2018 Master Table

Date	Author	Target	Description	
01/10/2018	Attackers linked to Saudi Arabia?	Canadian permanent resident and Saudi dissident Omar Abdulaziz	A report from The Citizen Lab reveals that the Canadian permanent resident and Saudi dissident Omar Abdulaziz was targeted by an attack infecting his phone with NSO's Pegasus spyware.	Malware/
01/10/2018	?	Apollo	Apollo, a sales engagement startup boasting a database of more than 200 million contact records, is hacked and sends an email to its affected customers.	Unknown
01/10/2018	Roaming Mantis	iOS Users	Kaspersky discover that the Roaming Mantis group is testing a new monetization scheme by redirecting iOS users to pages that contain the Coinhive in-browser mining script rather than the normal Apple phishing page.	Malicious
02/10/2018	Hidden Cobra AKA Lazarus Group	US Banks	A joint technical alert from the DHS, the FBI, and the Treasury warns about a new ATM cash-out scheme, dubbed "FASTCash," used by the Hidden Cobra APT.	Malware/
02/10/2018	?	SBM Holdings (State Bank of Mauritius India)	Mauritius banking group SBM Holdings unveils that its Indian operations suffered a cyber fraud earlier in the week, and that the bank has potentially lost up to $14 million worth. The bank is able to recover $10 million.	Fraudulen
02/10/2018	?	Individuals in the US	Researchers from ProofPoint discover a new DanaBot campaign spread through Malspam campaign installing the Hancitor malware.	Malware/
02/10/2018	?	Android Users in Japan and Korea	Researchers from Fortinet unveil a new round of attack carried on via the FakeSpy Android malware.	Malware/
02/10/2018	?	City of Regina	A city of Regina email is hacked, and used as a phishing tool to try and get passwords and emails from other city of Regina staff as well as external groups.	Account
02/10/2018	?	WhatsApp Users in Israel	A wave of reports about hijacked WhatsApp accounts in Israel has forced the government's cyber-security agency to send out a nation-wide security alert.	Account
03/10/2018	APT10 AKA Red Apollo, Stone Panda, POTASSIUM, MenuPass, Cloud Hopper, Red Leaves	Managed Service Providers	The US Department of Homeland Security issues an alert about "ongoing" cyber-attacks against managed service providers, indirectly attributed to APT10.	Targeted
03/10/2018	?	Black History Month Website	The Black History Month website falls victim to two cyber attacks in	DDoS

Date	Author	Target	Description	
			just 24 hours	
03/10/2018	?	Single Individuals	Researchers from Cybereason unveil a peak of multiple Betabot, aka Neurevt, infections over the past few weeks.	Malware/
03/10/2018	?	North American Risk Services	North American Risk Services, suffers a data breach between February 7 and March 27, when the company notices suspicious emails being sent from one of their employee's accounts.	Account
04/10/2018	China?	30 U.S. companies, including Amazon and Apple.	Bloomberg reports that an alleged attack by Chinese spies, carried out implanting a chip on Super Micro servers, reached almost 30 U.S. companies, including Amazon and Apple.	Targeted
04/10/2018	APT28, AKA Swallowtail, Fancy Bear, Sofacy	Military and Government Organizations in Europe and South America	Researchers from Symantec uncover a new espionage operation carried out by the infamous APT28 collective, targeting Military and Government Organizations in Europe and South America.	Targeted
04/10/2018	?	US Department of Defense	Roughly 30,000 DOD military and civilian personnel are believed to be affected by a cyber attack. A third-party contractor is compromised, granting the attackers access to the Pentagon network to steal travel data for DOD personnel.	Targeted
04/10/2018	Nomadic Octopus AKA DustSquad	High-value targets in several countries of Central Asia	Researchers from ESET and Kaspersky discover a new cyber espionage campaign carried out by Nomadic Octopus, active since at least 2015.	Targeted
04/10/2018	?	Assassin’s Creed Odyssey	Ubisoft's Assassin’s Creed Odyssey's launch is disrupted by a DDoS attack in the day of its release.	DDoS
04/10/2018	?	Square Enix	The same day Square Enix also announces to be fighting off a DDoS attack aimed towards its popular game, Final Fantasy XIV.	DDoS
04/10/2018	?	Tillamook Chiropractic Clinic	Tillamook Chiropractic Clinic reveals that on May 2016, malware was installed on the primary insurance billing system, which hackers then used as a staging area to collect patient records.	Malware/
05/10/2018	Russia-sponsored attackers	The Islam Channel	The Financial Times reveals that Russian military intelligence agents launched a 2015 cyber attack on UK-based TV station the Islam Channel, giving the Kremlin-backed hackers complete control	Targeted

Date	Author	Target	Description	
			over the broadcaster’s computer networks and infrastructure.	
05/10/2018	?	Multiple Targets in India	A new report from security company Banbreach reveals that a massive cryptojacking campaign, carried out via CoinHive, is ongoing in India, targeting 30,000 routers.	Malicious
05/10/2018	?	Single Individuals	Multiple Security companies reveal a spike in sextortion (sex extortion) campaigns targeting individuals via credentials collected from breach repositories.	Credentia
05/10/2018	?	Hetzner South Africa	The South African branch of Hetzner, a well-known web hosting provider, suffers a new security breach. The attacker manages to gain access to customer details such as names, email addresses, phone numbers, addresses, identity numbers, VAT numbers, and bank account numbers.	Unknown
05/10/2018	?	Assassin’s Creed Odyssey	Assassin’s Creed Odyssey's launch is disrupted by a DDoS attack.	DDoS
05/10/2018	?	City of St. Petersburg	The City of St. Petersburg publishes notifies a data breach of the third-party Click2Gov self-service payment which affected users who made payments between August 11, 2018, and September 25, 2018, using their credit cards.	Malware/
05/10/2018	AirNaine AKA TA545	Businesses in Canada	Researchers from Blueliv Team detect a new data stealer malware, dubbed ZeroEvil, targeting businesses in Canada.	Malware/
05/10/2018	?	National Ambulatory Hernia Institute	National Ambulatory Hernia Institute notifies almost 16,000 patients of Gamma ransomware attack	Malware/
06/10/2018	?	SpankChain	SpankChain, an adult industry focused cryptocurrency, has $38,000 worth of Ethereum stolen due to a smart contract bug.	Smart Co
06/10/2018	?	Anne Arundel County Public Library	Anne Arundel County Public Library officials announce that nearly 600 staff and public library computers have been hit by the Emotet virus. 4,768 customers who used public computers since September 17 are also notified;	Malware/
07/10/2018	Magecart	Cancer Research UK	The Magecart gang hit the Cancer Research UK back in 2016 with the same modus operandi.	Malicious
07/10/2018	?	Madison County Government Services	A ransomware attack hits Madison County Government	Malware/

Date	Author	Target	Description	
			services.	
07/10/2018	Ayyıldız Tim Cyber Army	Rep. Pete King’s campaign website	Rep. Pete King’s campaign website is defaced.	Defacem
09/10/2018	?	Single Individuals	Researchers from Trend Micro unveil a new phishing sophisticated campaign: the operators take over email accounts and insert the URSNIF banking trojan in conversation threads.	Malware/
09/10/2018	Magecart	Shopper Approved	Shopper Approved is the latest victim of the Magecart gang. The incident took place on September 15.	Maliciou
09/10/2018	?	Minnesota Department of Human Services	The Minnesota Department of Human Services falls victim of a phishing email scam. The attackers accessed the information of approximately 21,000 individuals in two incidents back in June and July.	Account
09/10/2018	?	City of Lake Worth Utilities	Customers of the City of Lake Worth Utilities who utilized the online option to pay their bill, between August 28 and October 9, may have experienced a possible breach of their credit card information.	Unknown
09/10/2018	?	Rebound Orthopedics & Neurosurgery	Rebound Orthopedics & Neurosurgery reports a data breach occurred back in May, when an employee's email account was improperly accessed. 2,800 employees and patients may have been compromised.	Account
09/10/2018	?	Cork City Council	5,000 people’s personal information, who used a parking app, collected by Cork City Council, is illegally accessed by a hacker.	Unknown
10/10/2018	Gallmaker	Entities in the government, military and defense sectors	Researchers from Symantec discover Gallmaker, a previously unknown cyber espionage group, targeting entities in the government, military and defense sectors since at least 2017.	Targeted
10/10/2018	FruityArmor?	Entities in Middle East	Researchers from Kaspersky reveal that the newly discovered Windows vulnerability CVE-2018-8453 is actively exploited for attacks targeting entities in Middle East.	Targeted
10/10/2018	?	Vulnerable Drupal Servers	Security researchers from IBM unveil a massive campaign targeting Drupal, exploiting	Drupal Vu

Date	Author	Target	Description	
			CVE-2018-7600 and CVE-2018-7602 to install a backdoor on the infected systems and take full control.	
10/10/2018	?	Sodexo Motivation Solutions	Sodexo Motivation Solutions' internal IT systems are hit by malware and as a consequence the Sodexo Engage's website lifestylehub.co.uk is pulled offline.	Malware/
11/10/2018	?	Single Individuals	Researchers from Palo Alto Unit 42 unveil a new malware campaign carried out via a fake Flash Player Trojan that installs a XMRig miner, but it also automatically updates his installed Flash Player.	Malware/
11/10/2018	?	Multiple Literary Agencies	Multiple literary agencies are hit by a sophisticated phishing campaign aimed to steal manuscripts. The most notable campaigns hit the Eccles Fisher Agency and Penguin Random House (PRH) North America.	Account
11/10/2018	?	Android Users	Researchers from Cisco Talos discover "GPlayed", a modular Android malware, still in testing phase, able to adapt itself and load multiple modules.	Malware/
12/10/2018	?	Iceland	Researchers from Cyren unveil the details of a massive phising campaign hitting Iceland, and distributing the Remcos remote access tool.	Malware/
12/10/2018	Black Energy	Information and telecommunication systems of Ukrainian government bodies	The Security Service of Ukraine (SBU) unveil a new targeted attack on the information and telecommunication systems of Ukrainian government bodies carried out by the Russia state-sponsored actor Black Energy.	Targeted
12/10/2018	?	Henderson School District	The Henderson school district in Texas is hit with a business email compromise (BEC) attack resulting in a $600,000 loss for the district. The attack took place on September, 26th.	Account
12/10/2018	?	Catawba Valley Medical Center (CVMC)	Catawba Valley Medical Center (CVMC) notifies patients of a phishing incident that took place back on August 2018.	Account
12/10/2018	?	Indio Water Authority (IWA)	Indio Water Authority (IWA) is another victim of the Click2Gov breach.	Malware/
13/10/2018	?	Onslow Water and Sewer Authority (ONWASA)	The Onslow Water and Sewer Authority (ONWASA) is hit by a targeted ransomware attack	Malware/

Date	Author	Target	Description	
			carried out via Ryuk.	
15/10/2018	?	EOSBet	Hackers are believed to have stolen $338,000 worth of EOS cryptocurrency from blockchain-powered gambling dApp EOSBet.	EOS Vuln
15/10/2018	?	35 million records belonging to US voters	A database containing an estimated 35 million records belonging to US voters appears on sale on a forum.	Unknown
15/10/2018	?	Multiple Targets	Researchers from Cisco Talos discover a new malware campaign distributing the information-stealing trojan "Agent Tesla," and other malware such as the Loki information stealer exploiting Microsoft Word vulnerabilities CVE-2017-0199 and CVE-2017-11882.	Malware/
05/10/2018	?	National Ambulatory Hernia Institute	National Ambulatory Hernia Institute notifies almost 16,000 patients of Gamma ransomware attack occurred on October 5.	Malware/
16/10/2018	?	New Share Counts	Researchers from Sucuri reveal that New Share Counts, a discontinued Tweet counter is hijacked, redirecting the users to scam pages.	Malicious
16/10/2018	Attackers linked to Hezbollah	Multiple Targets	The Czech Security Intelligence Service (BIS) reveals to have taken down the infrastructure used by Hezbollah operatives to target and infect users around the globe with mobile malware.	Malware/
16/10/2018	?	City of West Haven	The City of West Haven pays $2,000 after having 23 of its servers encrypted from a ransomware attack.	Malware/
17/10/2018	GreyEnergy	Energy companies and other high-value targets in Ukraine and Poland	Researchers from ESET uncover details of the successor of the BlackEnergy APT group, named GreyEnergy. Since December 2015, the group attacked energy companies and other high-value targets in Ukraine and Poland for the past three years.	Targeted
17/10/2018	?	A primary company in the Italian Naval Industry	Researchers from Yoroi discover a new targeted campaign against one of the most important companies in the Italian Naval Industry. The malware is dubbed MartyMcFly.	Targeted
17/10/2018	?	Vesta Control Panel (VestaCP)	Vesta Control Panel, the provider of an open-source hosting panel software reveals a security breach during which an unknown hacker contaminated the project's source	Malware/

Date	Author	Target	Description	
			code with malware. The malicious code was added on May 31, this year, and later removed two weeks later, on June 13.	
17/10/2018	?	Single Individuals	Researchers from Zscaler uncover a new SEO poisoning campaign, targeting keywords associated with the U.S. midterm elections. Attackers have hacked over 10,000 web sites in order to promote 15,000 different keywords	SEO Pois
17/10/2018	?	City of Muscatine	The City of Muscatine is hit with a ransomware attack on October 17. Financial and other servers are affected.	Malware/
17/10/2018	?	Facepunch	As reported by Troy Hunt's Have I Been Pwned breach notification service, the Facepunch game studio was the victim of a data breach in June 2016 which led to sensitive information of 396,650 users being exposed.	Unknown
18/10/2018	Oceansalt	Targets in US and Canada linked to South Korea	Researchers from McAfee discover a new attack targeting Korean-speaking victims, and borrowing code from a reconnaissance tool linked to Comment Crew, a Chinese nation-state threat actor exposed in 2013.	Targeted
18/10/2018	?	Indiana National Guard	The Indiana National Guard reports that a non-military server that contains the personal information of civilian and military personnel is hit with ransomware	Malware/
18/10/2018	Tick (or also Redbaldknight, or Bronze Butler)	Targets in South Korea and Japan	Researchers from Cisco Talos reveal the details of the latest campaign carried out by a group dubbed Tick (or also Redbaldknight, or Bronze Butler), targeting South Korea and Japan.	Targeted
19/10/2018	?	Healthcare.gov	The Centers for Medicare & Medicaid Services (CMS) announces that Healthcare.gov, the federally operated health insurance marketplace, has suffered a data breach. The CMS believes files for as many as 75,000 people were accessed,	Unknown
19/10/2018	?	Around 50 victims located in Russia, Iran and Egypt, related to nuclear energy, telecommunications, IT, aerospace and R&D.	Researchers from Kaspersky reveal a campaign targeting systems used in aerospace, nuclear energy, and other industries, using three tools leaked from the NSA: DarkPulsar, DanderSpritz, and Fuzzbunch.	Targeted
19/10/2018	APT-C-27	Countries in Middle East	Researchers from 360 Total	Targeted

Date	Author	Target	Description	
			Security reveal the details of a recent attack carried out by APT-C-27 and targeting Arabic countries.	
19/10/2018	?	Twitter users	Twitter shuts down a bot network pushing out pro-Saudi government tweets.	Social Ne
19/10/2018	?	Catawba Valley Medical Center	Catawba Valley Medical Center notifies patients of a phishing email incident occurred on August 13, 2018.	Account
19/10/2018	?	Investimer, or Hyipblock, or Mmpower	Researchers from Doctor Web expose an online scammer targeting thousands of victims interested in cryptocurrencies via a large and diverse business that includes phishing and fraud operations.	Account
20/10/2018	?	8 Adult Websites	Eight poorly secured websites are hacked, exposing megabytes of personal data. 1.2M users are exposed.	Unknown
21/10/2018	?	Trade.io	Cryptocurrency exchange Trade.io reveals a security breach: an unknown party withdraws over 50 million Trade tokens (TIO), worth over $7.5 million, from its cold storage wallets.	Unknown
21/10/2018	?	Python users	A malicious package is uploaded into the official repository of Python. The package is called “Colourama" and is able to inject a cryptocurrency clipboard hijacker.	Malware/
22/10/2018	?	Davos in the Desert	The website of the Saudi Arabian investment conference, referred to as “Davos in the Desert”, is defaced with anti-Saudi messages, to protest against the death of journalist Jamal Khashoggi.	Defacem
22/10/2018	?	Orange County Branch of the Girl Scouts of America	Hackers breach the Orange County, Calif. branch of the Girl Scouts of America, potentially exposing personal information for 2,800 members and their families.	Account
22/10/2018	?	Vulnerable IoT devices	Researchers from SophosLabs reveal the details of a new IoT botnet called Chalubo, targeting internet-facing SSH servers on Linux-based systems.	Account
23/10/2018	?	Axa Mexico	Insurer Axa reveals it suffered a cyber attack that prompted an alert from the Mexico central bank alert, however clients’ information and resources are safe and have not been affected.	Unknown
23/10/2018	?	Eurostar	Eurostar has reset its customers' login passwords after detecting	Unknown

Date	Author	Target	Description	
			attempts to break into an unspecified number of accounts taking place between 15 and 19 October.	
23/10/2018	Magecart	Vulnerable Magento Servers	The researcher Willem de Groot reveals that now the Magecart gang is targeting vulnerable Magento servers via 20 vulnerable extensions.	Vulnerab
23/10/2018	?	Ad Publishers	Google removes the apps and blacklists the websites employed in a massive ad scam that made millions for fraudsters using bots trained to mimic human user behavior.	Bots
23/10/2018	?	Single individuals in the UK, Italy, and Canada	Researchers from ProofPoint reveal the details of a malicious campaign, carried out via a new PowerShell downloader dubbed sLoad, characterized by sophisticated reconnaissance features.	Malware/
23/10/2018	?	Jones Eye Clinic and Surgery Center	40K users are affected by a ransomware attack, occurred on August 23, targeting Jones Eye Clinic and Surgery Center.	Malware/
23/10/2018	?	Internet Solutions	Internet Solutions (IS) sends a notice to clients to warn them about a breach, and urges them to change their passwords and take additional steps to secure their servers. Later the company confirms that its internal monitoring systems have detected “irregular activity” on some of its virtual services.	Unknown
23/10/2018	?	Children’s Hospital of Philadelphia (CHOP)	Children’s Hospital of Philadelphia (CHOP) notifies some of its current and former patients of two email incidents, both involving health information, occurred respectively on August 23, and September 6.	Account
24/10/2018	?	Cathay Pacific	Cathay Pacific announces to have discovered unauthorised access to some of its information system containing passenger data of up to 9.4 million people. The attack started in March and went undetected for some months.	Unknown
24/10/2018	?	Android users	The McAfee Mobile Research team identifies an active phishing campaign that traps users by sending an SMS to influence them on downloading and installing an Android malware app TimpDoor.	Malware/
25/10/2018	NARWHAL SPIDER	Japanese Users	Researchers from Crowdstrike uncover a new spam campaign carried out via the Cutwail botnet,	Malware/

Date	Author	Target	Description	
			targeting Japanese speaking victims, and using a mixture of malicious PowerShell and steganography to distribute the URLZone malware family (a.k.a. Bebloh).	
25/10/2018	?	Exposed Docker Engine API	Researchers from Trend Micro discover an unknown attacker scanning for exposed Docker Engine APIs and utilizing them to deploy containers that download and execute a coin miner.	Misconfi
25/10/2018	?	Vulnerable Hadoop Clusters	Researchers from Radware reveal the details of DemonBot, a botnet targeting Hadoop clusters to launch DDoS attacks.	Hadoop V
26/10/2018	China	Multiple Targets in US and Canada	An academic paper published by researchers from the US Naval War College and Tel Aviv University reveals that China Telecom has started abusing BGP hijacks after it entered into a pact with the US in September 2015 to stop all government-back cyber operations aimed at intellectual property theft.	BGP Hija
26/10/2018	Iran	Facebook users in the US and UK	Facebook announces to have removed 82 Pages, Groups and accounts for coordinated inauthentic behavior that originated in Iran and targeted people in the US and UK.	Social Ne
27/10/2018	?	Bank Islami	Karachi-based Bank Islami acknowledges of suffering a security breach of its payment cards system but denies reports of having lost an alleged $6 million in what local press have called the biggest cyber-attack in the country's history.	Unknown
27/10/2018	?	Python users	12 additional Python libraries uploaded on the official Python Package Index (PyPI) are found containing malicious code.	Malware/
28/10/2018	?	MapleChange	MapleChange, a Canadian crypto exchange, suffers a hack and looses all the funds (913 BTC, $6M worth), despite many accuse the exchange of attempting to stage an exit scam.	Vulnerab
28/10/2018	Anonymous	70 Gabon Government Websites	The hacktivist group Anonymous takes down 70 Gabon government websites as part of its “anti-dictatorships” campaign.	DDoS
28/10/2018	?	Tomorrowland Festival	Hackers breach computer security at the Tomorrowland festival organizers, and steal the data of 64,000 people who signed up for	Unknown

Date	Author	Target	Description	
			tickets for the 2004 edition.	
29/10/2018	LulzSec ITA and AntiSec ITA	Several Italian Universities	In name of Op #FifthOfNovember, the Italian branch of the Anonymous hacks several Italian Universities.	SQLi
29/10/2018	?	Mac Users	Researchers from Malwarebytes discover a malicious app, dubbed Coin Ticker, installing backdoor to unsuspecting Mac users for a purpose not completely clear.	Malware/
30/10/2018	?	FIFA	FIFA acknowledges that its computer systems were hacked earlier in March, for the second time, and officials from European soccer's governing body fear they also might have suffered a data breach.	Unknown
30/10/2018	?	US Voters	Researchers from Carbon Black reveal to have found 20 different state voter databases available for purchase on the dark web.	Unknown
30/10/2018	LulzSec ITA and AntiSec ITA	Websites affiliated to trade unions	In the second day of Op #FifthOfNovember, LulzSec ITA and AntiSec ITA target some websites affiliated to trade unions.	SQLi
30/10/2018	?	UK's leading construction, architecture and property firms	Over 600,000 breached corporate log-ins belonging to staff at the UK's leading construction, architecture and property firms are found for sale on the dark web.	Account
30/10/2018	?	Mobile Users	A mobile malvertising campaign recently found targeting three digital advertising platforms has been using a malware, dubbed JuiceChecker-3PC, which checks a phone's battery level as part of an unusual new technique for avoiding detection.	Malware/
31/10/2018	?	Iran	Iranian infrastructure and strategic networks are allegedly hit by a computer virus similar to Stuxnet but "more violent, more advanced and more sophisticated,"	Targeted
31/10/2018	?	Multiple Targets using Cisco Devices	Cisco reveals that attackers are actively exploiting CVE-2018-15454, a SIP vulnerability in the software of its firewall devices.	Vulnerab
31/10/2018	?	Radisson Hotel Group	The hotel chain Radisson Hotel Group suffered a security breach that exposed personal information of the members of its loyalty scheme. The incident happened on September 11, but was	Unknown

Date	Author	Target	Description	
			identified only on October first.	
31/10/2018	?	SIngle Individuals	Security researchers from Cisco reveal that two recent sextortion scam campaigns seem to rely on the Necurs botnet infrastructure to distribute the messages.	Malicious
31/10/2018	LulzSec ITA and AntiSec ITA	Federazione Italiana Medici Medicina Generale Pisa	Third day of Op #FifthOfNovember, and this time LulzSec ITA and AntiSec ITA deface a new target.	Defacem
31/10/2018	?	Single Individuals	According to a report from Kryptos Logic, the Emotet malware family has started mass-harvesting full email messages from infected victims in a new mysterious campaign.	Malware/
31/10/2018	?	NorthBay Healthcare Corporation	NorthBay Healthcare Corporation suffers a data breach affecting the information of everyone who applied for a position within the organization between December 2012 and May 2018.	Unknown
23/10/2018	MoneyTaker	Russian Banks	Researchers from Group-IB discover a first massive phising campaign in disguise of the Central Bank of Russia and FinCERT, the Financial Sector Computer Emergency Response Team.	Account
02/11/2018	?	Mac users using the Exodus wallet	Security researchers at F-Secure uncover a spam campaign aimed at delivering spyware to Mac users that use the Exodus wallet.	Malware
14/11/2018	Snake	Multiple targets in Germany, including: federal lawmakers, military facilities and German embassies	Hackers suspected of ties to Russia's government target Germany with a renewed cyber attack on political institutions, according to the country's domestic intelligence agency, BfV.	Targeted
14/11/2018	?	Vulnerable Linux Servers	Researchers at Dr.Web discover a malicious Monero cryptominer specifically designed for Linux named Linux.BtcMine.174.	DirtyCow and Linux Vulnerab
16/11/2018	Silence	Russian Banks	Researchers from Group-IB discover a second massive phising campaign in disguise of the Central Bank of Russia and FinCERT, the Financial Sector Computer Emergency Response Team.	Account
16/11/2018	?	New York Oncology Hematology	New York Oncology Hematology notifies nearly 130,000 patients and employees that it was the victim of a phishing attack occurred between April 20 and April 27.	Account
16/11/2018	?	OSIsoft LLC	OSIsoft LLC discloses a security breach which affected its	Account

Date	Author	Target	Description	
			employees, consultants, interns, and contractors. The credential theft involves 29 computers and 135 accounts.	
16/11/2018	Hades	Multiple targets	Researchers from Check Point discover a new spike of activity from Hades, the threat actor behind the Olympic Destroyer malware.	Targeted
16/11/2018	?	Center for Vitreo-Retinal Diseases	The Center for Vitreo-Retinal Diseases in Illinois notifies more than 20,300 patients after a ransomware attack.	Malware
17/11/2018	APT29 (aka The Dukes, Cozy Bear and Cozy Duke)	U.S. government agencies, businesses and think tanks	Researchers from Crowdstrike and FireEye uncover a malicious campaign, allegedly carried out by APT29, impersonating a State Department official, and targeting U.S. government agencies, businesses and think tanks.	Targeted
18/11/2018	?	Mékinac Regional County Municipality	The Quebec region of Mékinac pays a $30,000 Bitcoin ransom after its servers are hit by ransomware.	Malware
18/11/2018	TheDarkOverlord	Channel Ship Services	TheDarkOverlord claims to have hacked Channel Ship Services and have acquired personal data and information that can jeopardize maritime security.	Unknown
19/11/2018	Magecart Group	VisionDirect	VisionDirect, a popular contact lens online merchant, posts an advisory stating that their web site was compromised causing the theft of credit card and account information. The breach occurred between November 3rd and November 8th.	Malicious
19/11/2018	?	worldwish.org	Unknown attackers compromise worldwish.org, a website managed by a charitable organization, and implant the CoinIMP Javascript miner.	Drupalge
19/11/2018	?	Android users	Malware researcher Lukas Stefanko reveals that more than 560,000 users have been tricked into downloading malicious apps, which include a mix of luxury car and truck simulation apps.	Malware
19/11/2018	?	Vulnerable Drupal servers	According to researchers from Imperva, hackers are targeting vulnerable Drupal servers via Dirty Cow and Drupalgeddon 2 to get a foothold in the attached sites.	Drupalge vulnerabi
19/11/2018	?	East Tennessee State University	Two employees at East Tennessee State University fall for an email phishing scam and pave the way for a breach at the school.	Account

Date	Author	Target	Description	
19/11/2018	?	Spotify customers	Researchers from AppRiver discover a new phishing campaign targeting Spotify customers.	Account
20/11/2018	Sofacy, AKA APT28, AKA Fancy Bear	Targets in US and Europe	Researchers from Palo Alto Networks reveal the details of a new campaign carried out by the infamous APT28, AKA Fancy Bear, AKA Sofacy, via the Cannon malware.	Targeted
20/11/2018	Gamaredon group	Ukrainian government agencies	The Computer Emergency Response Team of Ukraine (CERT-UA) and the Foreign Intelligence Service of Ukraine detect a new strain of the Pterodo Windows backdoor targeting computers at Ukrainian government agencies.	Targeted
20/11/2018	Two different criminal groups	Brazilian Website of Umbro	Researchers from Malwarebytes reveal that two different groups compete to infect the Brazilian website of Umbro with the Magecart Card Skimming Group.	Malicious
20/11/2018	right9ctrl	BitPay and CoPay users	a NodeJS package that is used by the CoPay and BitPay is poisoned by its latest administrator with a malicious code allowing an attacker to swipe Bitcoin from Bitpay and Copay wallets.	Malicious
20/11/2018	OceanLotus AKA APT32 AKA APT-C-00	Multiple targets in Southeast Asia	Researchers from ESET discover a new watering hole campaign targeting 21 distinct websites in Southeast Asia carried out by OceanLotus.	Targeted
20/11/2018	Lazarus Group	Latin American financial institutions	Researchers from Trend Micro reveal that the advanced persistent threat group Lazarus has been observed using a modular backdoor to compromise a series of Latin American financial institutions.	Malware
20/11/2018	?	Johannesburg-Lewiston Area Schools (JLAS)	Johannesburg-Lewiston Area Schools (JLAS) falls victim to a ransomware attack.	Malware
20/11/2018	?	Vulnerable Wordpress sites	Researchers from WordFence reveal an ongoing campaign that utilizes the recently discovered vulnerabilities in the Wordpress AMP plugin to perform a XSS attack against the vulnerable WordPress sites.	XSS
20/11/2018	?	Multiple targets	Researchers from Cofense uncover a new Emotet-related campaign, carried out via elaborate phishing messages that spoof "a known and trusted organization."	Malware
20/11/2018	?	Multiple targets	Researchers from Agari uncover a BEC campaign trying to leverage	Account

Date	Author	Target	Description	
			the California wildfires to defraud their victims.	
21/11/2018	?	High Tail Hall	The website of High Tail Hall, an adult video game is hacked, with the information of nearly half a million subscribers stolen. The breach occurred back in August.	Unknown
21/11/2018	?	Vulnerable Linux Servers	Researchers from Netscout Asert discover what they believe is the first variant of Mirai targeting vulnerable Linux servers (Hadoop YARN).	Vulnerab
23/11/2018	?	East Ohio Regional Hospital and Ohio Valley Medical Center	A ransomware attack hits computer systems at the East Ohio Regional Hospital and Ohio Valley Medical Center reportedly disrupting the hospitals' emergency rooms.	Malware
23/11/2018	Nicholas Truglia	Robert Ross	In his latest SIM swap hack, Nicholas Truglia steals $1M worth in crypto currencies from Robert Ross, a Silicon Valley executive.	Account
23/11/2018	?	Drake’s Fortnite account	Drake’s Fortnite account is hacked and joins a charity livestream, yelling bad words during the event.	Account
23/11/2018	?	Knuddles.de	Following a hack that resulted in leaking about 808,000 email addresses and over 1.8 million usernames and passwords, a social network website in Germany received a fine of EUR 20,000 from the Baden-Württemberg Data Protection Authority.	Unknown
23/11/2018	?	Single Individuals	In two different analysis, researchers from Certego and Yoroi reveal the details of sLoad, a new malspam campaign hitting Italy.	Malware
26/11/2018	?	Android users	Researchers from analytics firm Kochava reveal that eight Android apps with a total of more than 2 billion downloads, have been exploiting user permissions as part of an ad fraud scheme that could have stolen millions of dollars.	Malware
27/11/2018	?	Atrium Health	Atrium Health says that data of about 2.65 million patients including addresses, dates of birth and SSN may have been compromised in a breach at its third-party provider AccuDoc Solutions. The breach occurred between Sept. 22 and 29.	Unknown
27/11/2018	?	Companies in Lebanon and the United Arab Emirates	Researchers from Cisco Talos discover DNSpionage, a new	Targeted

Date	Author	Target	Description	
		(UAE)	campaign targeting Lebanon and the United Arab Emirates (UAE) affecting .gov domains, as well as a private Lebanese airline company.	
27/11/2018	ScamClub	iOS users in the US	Researchers from Confiant uncover a massive malvertising campaign, targeting iOS users in the US, able to hijack over 300 million browser sessions over 48 hours.	Malvertis
27/11/2018	?	Single Individuals	Researchers from Trend Micro discover a new worm, dubbed njRAT/Njw0rm, which spreads a modern variant of the remote access tool Bladabindi.	Malware
27/11/2018	?	Android users	Researchers from Trend Micro uncover seven malicious Android apps posing as voice messaging. The malware strain is dubbed AndroidOS_FraudBot.OPS.	Malware
27/11/2018	?	PratenOnline.nl	Attackers manage to steal and hold for ransom 14,000 profiles and 16,000 chats from PratenOnline.nl, a website where young people with an anxiety and depression can chat anonymously with a professional.	Unknowr
28/11/2018	?	Dell	Dell releases an update on its website acknowledging that it warded off a possible hack happened on November 9th. According to the company, it is possible some information was removed from Dell’s network.	Unknowr
28/11/2018	?	Vulnerable devices	Researchers from Akamai discover a new variant of the UPnProxy vulnerability, named EternalSilence. The campaign has already compromised at least 45,000 routers.	EternalBl (CVE-201
28/11/2018	?	Targets primarily in China, India, Turkey, and the UAE	Researchers from ForcePoint unveil a long-lasting campaign (since 2014) carried out via malicious AutoCAD files.	Malware
28/11/2018	?	Georgia Spine and Orthopaedics of Atlanta	Georgia Spine and Orthopaedics of Atlanta notifies 7,012 patients after a phishing attack occurred on July 2018.	Account
29/11/2018	TA-505	Multiple targets	Researchers from Morphisec reveal the details of "Pied Piper", a new wave of phishing attacks by TA-505, aimed to infect victims with the FlawedAmmyy and Remote Manipulator (RMS) RATs.	Account
29/11/2018	?	North and South Korea	Researchers from Palo Alto Networks uncover Fractured Block, a phishing campaign	Targeted

Date	Author	Target	Description	
			targeting the Korean peninsula, using a malicious dropper called CARROTBAT.	
29/11/2018	?	Dunkin' Donuts	Dunkin' Donuts informs some of its DD Perks program members that their account information may have been exposed through a credential stuffing attack. The incident was discovered on October 31, 2018	Brute For
29/11/2018	?	Moscow Ropeway (MKD)	One day after opening to the general public, Moscow's first-ever cable car is forced to shut down after a reported ransomware cyberattack.	Malware
29/11/2018	Sofacy, AKA APT28, AKA Fancy Bear	Ministries of foreign affairs, political think-tanks, and defence organizations across Europe.	Researchers from Accenture uncover a campaign carried out by the infamous APT28 threat actor, exploiting Brexit to deliver malware.	Targeted
29/11/2018	?	Thundermist Health Center	Rhode Island's Thundermist Health Center is hit by ransomware.	Malware
29/11/2018	?	Town of Christiansburg	The information of 900 people of Christiansburg is compromised in a phishing scam.	Account
30/11/2018	?	Marriott	The records of 500 million customers of the hotel group Marriott International are compromised. In particular the guest reservation database of its Starwood division has been compromised by an unauthorised party since 2014.	Unknown
30/11/2018	TheHackerGiraffe	50,000 printers across the Globe	Nearly 50,000 printers across the globe are hacked by a hacker using the alias TheHackerGiraffe for the sake of promoting PewDiePie's YouTube channel and encouraging users to subscribe to the channel.	Printer m
30/11/2018	?	Microsoft IIS and SQL servers	Researchers from Check Point reveal the details of a new Monero miner called KingMiner, targeting Microsoft IIS and SQL Servers in particular, and running a brute-force attack to gain access.	Malware
30/11/2018	MuddyWater	Targets in Turkey	Security researchers at Trend Micro discover a PowerShell-based backdoor, active in Turkey, which resembles a malware used by MuddyWater threat actor.	Targeted
30/11/2018	Magecart Group	Sotheby's	Sotheby's Home website is the latest casualty of Magecart after a breach sees card-skimming code deployed by the cyber criminals.	Maliciou

Date	Author	Target	Description	
30/11/2018	?	1-800-FLOWERS	The Canadian operations of 1-800-FLOWERS discloses a four-year data breach affecting customers who purchased goods on its website. An unauthorized actor gained access to customers' payment card data from Aug. 15, 2014 through Sept. 15, 2018.	Unknown
30/11/2018	?	Ames Parking Ticket Payment System	The data breach to Click2Gov online payment system might have exposed information on 4,600 people who used Ames, Iowa, online ticket payment system between Aug. 10 to Nov. 19, 2018.	Malware
30/11/2018	?	Technic Forums	Technic Forums is compromised by an unknown third-party.	Malicious
02/11/2018	?	ASI Computer Systems	ASI Computer Systems notifies some of their customers after discovering that usernames and passwords on a support web site had been hacked prior to December 2016.	Account
29/11/2018	?	Mind & Motion	Mind & Motion notifies 16,000 after a ransomware attack.	Malware
01/12/2018	?	Targets in China	Over 100,000 computers in China are infected in just a few days by 'WeChat Ransom' since the ransom is payable via Tencent's WeChat payment service.	Malware
01/12/2018	?	Palermo Calcio	The Italian Football Team Palermo Calcio reveals to have suffered an intrusion with the consequent leak of fake news about the imminent sale of the team.	Unknown
03/12/2018	Turla and APT28 (Sofacy or Fancy Bear)	Czech Ministry of Foreign Affairs (MFA), Ministry of Defense, and the Army of the Czech Republic	The Czech Security Intelligence Service (BIS) that two Russian-linked cyber-espionage groups have hacked into the Czech Republic's government networks during 2016 and 2017.	Targeted
03/12/2018	?	Quora	Quora announces that one of their systems was hacked on November 30, and has led to the exposure of approximately 100 million user's data to an unauthorized third-party.	Unknown
03/12/2018	Magecart	OppoSuits	Customers of Dutch clothing company OppoSuits are warned to monitor their credit card accounts after the firm discovers the Magecart malware planted on its website could have stolen the details of 7,000 customers.	Malicious
03/12/2018	?	iOS Users	Apple removes two malicious iOS apps (Fitness Balance and	Malware

Date	Author	Target	Description	
			Calories Tracker) that tricked users into approving TouchID payments via misleading popups.	
03/12/2018	?	Cancer Treatment Centers of America	Cancer Treatment Centers of America notifies almost 42,000 patients of possible access to their protected health information after a phishing attack occurred on May 2 and discovered on September 26.	Account
04/12/2018	?	NRCC (National Republican Congressional Committee)	Politico reveals that the emails of top NRCC officials were hacked in a major 2018 hack occurred in April.	Account
04/12/2018	Russia?	Ukraine Telecommunications Network	The Security Service of Ukraine (SBU) reveals to have stopped a “massive” cyberattack against the country’s telecommunications network, and blames the Kremlin for the attempted hack.	Targeted
04/12/2018	?	BeatStars	BeatStars, a marketplace for selling music production beats, is mass-defaced.	Defacem
04/12/2018	?	Humble Bundle	The gaming subscription site Humble Bundle informs its customers of a data breach that may have exposed a person’s subscription status.	Vulnerab
04/12/2018	?	Vulnerable MicroTik routers	Security researchers discover over 415,000 MikroTik routers across the globe infected with malware designed to steal their computing power and secretly mine cryptocurrency.	Vulnerab
04/12/2018	?	San Francisco State University	Dozens of San Francisco State University student accounts are hacked in a phishing attack.	Account
04/12/2018	TheDarkOverlord	Caribbean Island Properties	Caribbean Island Properties is hacked by TheDarkOverlord	Unknowr
04/12/2018	TheDarkOverlord	Prime Staff Inc.	Prime Staff Inc. joins the list of the companies hacked by TheDarkOverlord. Thousands of employee's files are stolen.	Unknowr
05/12/2018	?	Vertcoin	The blockchain of Vertcoin is under a 51% attack. The attack could have resulted in a theft of over $100,000.	51% attac
05/12/2018	?	Linux Servers	Researchers from ESET details 21 "new" Linux malware families. All operate in the same manner, as trojanized versions of the OpenSSH client.	Malware
05/12/2018	?	Wordpress sites	Researchers from Defiant reveal the details of a botnet composed of over 20,000 WordPress sites, attacking other WordPress sites. The botnet propagates itself via	Dictionar

Date	Author	Target	Description	
			dictionary attacks.	
05/12/2018	State-sponsored actors from North Korea	Undisclosed academic institutions	Researchers from the ASERT Team of Netscout reveal the details of Stolen Pencil, a campaign allegedly originating from North Korea, targeting academic institutions since at least May 2018, using a malicious Google Chrome extension	Targeted
05/12/2018	Syrian Electronic Army	Multiple Targets	Researchers from Lookout uncover the latest waves of attacks carried out by the Syrian Electronic Army via SilverHawk, a mobile malware delivered through rogue apps (WhatsApp and Telegram spreading via watering hole websites and phishing emails.	Targeted
05/12/2018	?	High-profile online retail websites	Researchers from Symantec uncover a new payment information stealing campaign, using a new formjacking redirection method to compromise the checkout stage of high-profile online retail websites.	Formjack
06/12/2018	?	Devices in Russia, South Korea, the UK, and the US	Researchers from Anomali Labs discover a new malware, called "Linux Rabbit", targeting Linux servers and IoT devices. The campaign utilizes two strains of malware that share the same code base called Linux Rabbit and "Rabbot". The goal of this campaign is to install cryptocurrency miners.	Malware
06/12/2018	?	Android users	Researchers from Sophos discover a group of 22 Android applications from the Google Play store, used in an advertising clickfraud scheme, faking genuine ad traffic by randomizing the device and User Agent information. The apps were installed more than 2 million times by Android device owners.	Malware
06/12/2018	?	Redwood Eye Center	The Redwood Eye Center notifies 16,000 California residents their personal information may have been compromised when a company subcontractor (IT Lighthouse) suffered a ransomware attack on September 19.	Malware
06/12/2018	TA505	Retail, grocery, and restaurant chains in the US	Researchers from Proofpoint discover a new campaign carried out by TA505, targeting almost exclusively retail, grocery, and restaurant chains. This campaign distributed tens of thousands of	Malware

Date	Author	Target	Description	
			messages.	
07/12/2018	DarkVishnya	At least eight banks in Eastern Europe	Researchers from Kaspersky reveal the details of DarkVishnya: Cyber-criminal gangs are believed to have stolen tens of millions of dollars from at least eight banks in Eastern Europe, leaving malicious devices connected to the bank's network.	Maliciou
07/12/2018	@kitlol5	Linux.org	The Linux.org website is defaced via a DNS hijack.	DNS Hija
07/12/2018	?	Chrome users	ExtraHop, a real-time IT analytics firm, detects malicious code hidden inside a Chrome estension called Postman, raising concerns about a possible about a possible industrial espionage campaign, being the extension able to collect browsing history.	Maliciou
07/12/2018	?	City of Topeka	Another possible Click2Gov breach: Topeka's third-party payment vendor is breached possibly exposing the personal information of about 10,000 residents.	Malware
07/12/2018	?	Mac users	Researchers from Malwarebytes detect a fake Adobe piracy app (Adobe Zii) that infects Mac users with a one-two combination of the EmPyre backdoor/post-exploitation agent and the XMRig cryptominer. The malware is called OSX.DarthMiner.	Malware
07/12/2018	?	Multiple targets primarily in the United States	Researchers from Proofpoint observe a new sextortion campaign involving thousands of messages sent to a variety of targets primarily in the United States. However the message contains a link that leads to a GandCrab infection.	Malware
07/12/2018	?	Cape Cod Community College	The Cape Cod Community College notifies its employees that Hackers stole more than $800,000 when they infiltrated the school's bank accounts.	Account
09/12/2018	?	University of Maryland Medical System	The University of Maryland Medical System is hit by a ransomware attack, affecting about 250 of the system's 27,000 devices.	Malware
10/12/2018	APT33	SAIPEM	Italian oil services company SAIPEM is hit by a new version of the Shamoon malware. The attack started in India and hit the servers in Saudi Arabia, the United Arab Emirates and Kuwait. Fingers are pointed to Iran.	Targeted

Date	Author	Target	Description	
10/12/2018	Seedworm AKA MuddyWater	Government Agencies, Oil & Gas, NGOs, Telecoms, and IT Firms	Researchers from Symantec shed light on a recent series of cyber attacks carried out by the Seedworm (AKA MuddyWater) actor, designed to gather intelligence on targets spread primarily across the Middle East as well as in Europe and North America.	Targeted
10/12/2018	?	Baylor Scott & White Medical Center	Baylor Scott & White Medical Center notifies approximately 47,000 patients or guarantors that their payment information, including partial credit card information, may have been subject to a computer intrusion to a third-party credit card processing system.	Unknown
10/12/2018	?	North Bend	The city of North Bend is hit by a ransomware attack which temporarily locks out city workers from their computers and databases.	Malware
10/12/2018	?	Internet-exposed Ethereum wallets and mining equipment	Bad Packets LLC reveals that a massive campaign is ongoing, scanning Internet-exposed Ethereum wallets and mining equipment with port 8545 exposed online.	Misconfig
11/12/2018	?	Single targets in multiple sectors	Researchers from Cylance uncover a cybercriminal phishing operation lasting since three years, and designed to infect victims with a malicious backdoor, using command-and-control domains that intentionally spoofed the real-life domains of various Russian critical infrastructure firms.	Targeted
11/12/2018	?	PayPal Users	Researchers from ESET discover a new trojan capable of defeating the multifactor authentication required to access the official PayPal app.	Malware
11/12/2018	?	Governments of 30 countries, including Italy (52%), Portugal (22%) and Saudi Arabia (5%).	Researchers at Group-IB discover 40,000 credentials for various global government websites and portals and believe they could have been sold on dark web forums or leveraged in attacks designed to steal money or sensitive data.	Account
11/12/2018	?	Ramsey County Social Services	A cyber attack on the Ramsey County Social Services, occurred in August, may have comprised hundreds of clients' private health information.	Account
11/12/2018	?	Multiple Targets	Researchers from Netskope discover a new CapitalInstall	Malware

Date	Author	Target	Description	
			malware strain distributed with the help of Microsoft Azure blob storage instances.	
11/12/2018	?	Home or small office routers	Researchers from Trend Micro identify a new exploit kit named Novidade that targets home or small office routers by changing their Domain Name System (DNS) settings via cross-site request forgery (CSRF).	DNS Hija
12/12/2018	?	Multiple targets in the nuclear, defense, energy, and finance.	Researchers from McAfee discover Operation Sharpshooter a new global campaign targeting nuclear, defense, energy, and financial companies.	Targeted
12/12/2018	?	Ronin Gallery	Ronin Gallery notifies customers of payment card breach when unauthorized code is inserted in their web site able to capture customers' data.	Maliciou
12/12/2018	?	AOS 77	Former and current employees of AOS 77 in Washington County are made aware of a data breach in the school department's central office.	Unknown
12/12/2018	?	Vulnerable Linux Servers	Researchers from Trend Micro and ISC discover a malware campaign scanning the Internet for exploitable Elasticsearch instances running on Linux machines, aimed to drop a variant of the XMRig cryptocurrency miner.	Vulnerab and CVE-
13/12/2018	?	French Ministry of Europe, and Foreign Affairs (Ministère de l'Europe et des Affaires étrangères)	The personal information of 540,563 individuals is stolen from an emergency contact database after the website of the French Ministry of Europe, and Foreign Affairs is hacked.	Unknown
13/12/2018	?	Schenectady County	Schenectady County, shuts down its government website after a cyberattack via malware.	Malware
13/12/2018	Charming Kitty	Individuals involved in economic and military sanctions against the Islamic Republic of Iran	Researchers from Certfa unveil a new campaign carried out by the Charming Kitty targeting individuals involved in economic and military sanctions against the Islamic Republic of Iran.	Targeted
13/12/2018	?	Save the Children	Save the Children reveals to have been hit last year with a business email compromise scam that cost the charity $1 million. The incident took place in May 2017.	Account
13/12/2018	?	Brazilian mobile banking users	According to researchers from Doctor Web, more than 2,000 mobile banking users in Brazil	Malware

Date	Author	Target	Description	
			have unknowingly downloaded an Android malware, dubbed Android.BankBot.495.origin, that controlled devices and stole their confidential data.	
14/12/2018	Hackers linked to China	Contractors working for the US Navy	According to a new report, classified military information including missile plans have been stolen from contractors working for the US Navy by hackers linked to China.	Targeted
14/12/2018	?	Single Individuals	Researchers from Trend Micro discover a new malware strain, dubbed TROJAN.MSIL.BERBOMTHUM.AA, featuring a C&C service hidden into Twitter memes.	Malware
14/12/2018	?	Multiple targets including airline travel, retail, food, and entertainment	Researchers from Akamai publish a report on the "Three Questions Quiz" phishing campaign.	Account
14/12/2018	?	Tivit	Brazil-based IT services and business process outsourcing provider Tivit has data from many of its large customers leaked online, after nine members of staff have suffered a phishing attack.	Account
07/12/2018	?	Titan Manufacturing and Distributing	Titan Manufacturing and Distributing notifies consumers that its computer system had been compromised by malware during the period of November 23, 2017 to October 25, 2018.	Maliciou
16/12/2018	TheHackerGiraffe	100 Internet-connected printers worldwide	TheHackerGiraffe does it again, and this time, around 100,000 printers are hijacked, once again, to promote PewDiePie's YouTube channel. This time the attacker claims that he is able to destroy the printers.	Printer m
16/12/2018	?	Individual human right defenders spread across the Middle East and North Africa.	Amnesty International identifies several campaigns of credentials phishing, likely operated by the same attackers, targeting hundreds of individuals spread across the Middle East and North Africa. Attackers were able to bypass Gmail, Yahoo 2FA.	Account
16/12/2018	?	CCRM Dallas-Fort Worth	CCRM Dallas-Fort Worth becomes aware of a potential data security incident that may have resulted in the inadvertent exposure of patients' personal and health information, after a former nurse's email account is hacked.	Account
17/12/2018	China and Saudi Arabia?	Twitter users	Twitter shares fall seven percent after the social network giant reveals to have become aware of strange activity from China and Saudi Arabia, suggesting a	Targeted

Date	Author	Target	Description	
			possible state-sponsored attack, and involving one of its account help form APIs back on Nov. 15.	
17/12/2018	?	The Wall Street Journal’s website	The Wall Street Journal’s website is defaced with a post containing a fake apology supporting YouTube megastar PewDiePie, previously accused of antisemitism by the same paper.	Defacem
17/12/2018	?	University of Vermont Health Network – Elizabethtown Community Hospital	University of Vermont Health Network – Elizabethtown Community Hospital notifies 32,000 patients after an employee’s email account is accessed without authorization. The incident occurred on October 9, 2018,	Account
18/12/2018	?	NASA	NASA alerts its employees of a possible compromise of NASA servers containing personally identifiable information. The breach was discovered on October 23, and affects NASA Civil Service employees from July 2006 through October 2018.	Unknown
18/12/2018	?	Click2Gov	According to a new report published by Gemini Advisory, in the wake of the Ckick2Gov breach, at least 294,929 payment records have been compromised in 46 U.S. cities and sold in the Dark Web.	Malware
18/12/2018	?	Barnes-Jewish Company HealthCare	At least 5,850 people are alerted about a possible breach of credit card information through Barnes-Jewish Company HealthCare’s online payment portal. The breach was discovered on Nov. 19 and involved the injection of malicious code into their website.	Malicious
19/12/2018	Chinese Strategic Support Force (SSF)	European Diplomatic Network	A report by Area 1 Security reveals that a successful phishing attack on the Ministry of Foreign Affairs of Cyprus, an EU member nation, compromised the diplomatic communication network for the European Union (COREU).	Targeted
19/12/2018	?	The Wellcome Trust	The Wellcome Trust reveals in its annual report, that the email of four senior executives was compromised and sensitive information monitored for several months.	Account
19/12/2018	?	Financial sector employees in the U.S. and UK	Researchers from Menlo Security uncover a new phishing campaign, targeting financial sector employees in the U.S. and UK with remote access trojan payloads (Houdini - aka H-Worm -,	Account

Date	Author	Target	Description	
			as well as jRAT and Qrat), stored on a Google Cloud Storage domain.	
19/12/2018	?	California Department of Consumer Affairs	The California Department of Consumer Affairs suffers a malware attack, affecting workstations and disrupting computer networks.	Malware
19/12/2018	?	Hammer Nutrition	Hammer Nutrition notifies customers after discovering a malicious script into their website as a consequence of the compromise of their third-party website provider.	Malicious
19/12/2018	?	Steelite International	Steelite International discovers that hackers had encrypted its servers to cause "maximum disruption" to its payroll systems.	Malware
19/12/2018	Digital Revolution	Kvant Scientific Research Institute	The Digital Revolution group claims to have hacked the servers of Moscow-based Kvant Scientific Research Institute, and gathered evidence of a neural networks tool used to analyze activities on social networks.	Unknown
20/12/2018	APT10 AKA Red Apollo, CVNX, Stone Panda, POTASSIUM, MenuPass	Nine MSPs worldwide including Hewlett Packard Enterprise and IBM	Hackers working on behalf of China's Ministry of State Security breached the networks of Hewlett Packard Enterprise Co and IBM, then used the access to hack into their clients' computers in 12 countries including Brazil, Germany, India, Japan, the United Arab Emirates, Britain and the United States. The campaign is called Operation Cloudhopper.	Targeted
20/12/2018	?	Caribou Coffee	US coffee store chain Caribou Coffee announces a security breach after it discovered unauthorized access of its point of sale (POS) systems. The breach was discovered on November 28, and the company listed 239 stores of its total 603 locations as impacted.	Pos Malv
20/12/2018	?	Warby Parker	Warby Parker discloses that roughly 198,000 of its customers may have been affected by a credential stuffing attack targeting the eyeglass retail chain. The unauthorized activity started on Sept. 25 and continued through late November.	Credentia
20/12/2018	?	UK Taxpayers	Security researchers warn of a new HMRC scam using a threatening automated message in a bid to trick taxpayers into paying a 'fine.'	Account
20/12/2018	?	DrBenLynch.com	DrBenLynch.com notifies	Malicious

Date	Author	Target	Description	
			customers of payment card compromise after detecting a code injection into their web site that captured order information placed between September 8 and October 2,	
20/12/2018	?	The Podiatric Offices of Bobby Yee	The Podiatric Offices of Bobby Yee notifies 24,000 patients after ransomware attack.	Malware
21/12/2018	?	Electrum Bitcoin wallets	A clever phishing attack targeting Electrum Bitcoin wallets results in the theft of more than $750,000 worth of cryptocurrency.	Account
21/12/2018	?	San Diego Unified School District (SDUSD)	The San Diego Unified School District (SDUSD) reveals that PII of more than a half million students and staff were compromised as the result of a phishing attack that may have occurred as early as January 2018.	Account
21/12/2018	?	Saint John online parking payment system	Another consequence of the Click2Gov breach: the city of Saint John shuts down its online system used to pay parking tickets after discovering a data breach that could have exposed customer names, addresses and credit card information.	Malware
21/12/2018	?	Victorian Government	The work details of 30,000 Victorian public servants have been stolen in a data breach, after part of the Victorian Government directory was downloaded by an unknown party after an employee's email account is compromised.	Account
21/12/2018	?	Over 45,000 Chinese websites	Over 45,000 Chinese websites are under attack after Chinese cyber-security firm VulnSpy posts a proof-of-concept exploit for ThinkPHP, a Chinese-made PHP framework. The attacks aims to spread a new Mirai variant called Miori.	ThinkPHI
23/12/2018	?	Evercore	Thousands of sensitive documents have been stolen by hackers in a cyber-attack on the influential investment bank Evercore, after an employee in London falls victim of a phishing attack.	Account
24/12/2018	Anonymous	Some Italian Public Healthcare Organizations	In name of #AntiSecIta, hackers from the Anonymous collective breach the database of some Italian healthcare organizations.	SQLi
24/12/2018	?	Hayley Atwell	"Captain America" actress Hayley Atwell's nude photos are allegedly hacked and those behind it	Account

Date	Author	Target	Description	
			threatened to release the images, according to reports.	
24/12/2018	?	LiveBox ADSL modems from Orange	Honeypot systems at Bad Packets detect a scan targeting devices from Orange, trying to exploit a vulnerability that allows an attacker to retrieve their SSID and WiFi password in plaintext.	Router Vu
26/12/2018	?	News sites of Bulatlat, Kodao and Pinoy Weekly	The news sites of Bulatlat, Kodao and Pinoy Weekly are taken down by a DDoS attack, after stories on the Communist Party of the Philippines’ 50th anniversary were posted.	DDoS
26/12/2018	?	Windows, Linux and MacOS servers	Bleeping computer reveals that a ransomware called JungleSec is infecting victims through unsecured IPMI (Intelligent Platform Management Interface) cards since early November.	Malware
26/12/2018	?	Netflix Users	The Federal Trade Commission (FTC) warns consumers of a Netflix-based phishing scam that tells users they need to update their payment details.	Account
27/12/2018	?	Tribune Publishing's Southern California	A malware attack is suspected of preventing production of several newspapers, including the Wall Street Journal and Los Angeles Times. The suspected malware attack affected the computer systems at Tribune Publishing's Southern California printing plant. The Ryuk malware is suspected.	Malware
27/12/2018	?	Companies in the Italian automotive sector	Researchers at Cybaze-Yoroi ZLab reveal the details of Roma225, a campaign targeting companies in the Italian automotive sector.	Targeted
27/12/2018	?	BevMo	Alcohol retailer BevMo discloses to the California Attorney General’s office that its website was breached, compromising the credit card data of nearly 15,000 customers: a “malicious code” placed on the checkout page, compromising data between Aug. 2 and Sept. 26.	Malicious
28/12/2018	South Korea?	North Gyeongsang resettlement centre	Almost 1,000 North Korean defectors have their personal data leaked after a computer at the North Gyeongsang resettlement centre is hacked.	Targeted
28/12/2018	?	Family Physicians Group	Family Physicians Group notifies more than 8,000 patients about a phishing attack on an employee’s email account. Patient data may have been exposed between Aug. 7 and Aug. 21, 2018, when the company discovered the attack.	Account

Date	Author	Target	Description	
28/12/2018	?	College of Eastern Idaho	College of Eastern Idaho notifies a security incident discovered on September 5, 2018, when suspicious email activity was detected within an employee’s email account.	Account
28/12/2018	?	Westminster College	Westminster College in Salt Lake City, Utah notifies people after eleven of their employees fell prey to phishing attacks.	Account
28/12/2018	?	Several high profile Twitter accounts including Eamonn Holmes and Louis Theroux.	Several high-profile Twitter accounts are briefly hijacked by a security company (Insinia Security) to expose alleged flaws in the service.	Account
28/12/2018	?	Dental Center of Northwest Ohio	Dental Center of Northwest Ohio reveals that a ransomware attack affecting its local third-party IT vendor (Arakyta) may have endangered personal data belonging to current and former patients and employees.	Malware
29/12/2018	?	Dataresolution.net	Cloud hosting provider Dataresolution.net struggles to bring its systems back online after suffering a Ryuk ransomware infestation on Christmas Eve.	Malware
29/12/2018	?	City of Lake Charles	City of Lake Charles reports security breach of its information technology systems	Unknown
30/12/2018	Anonymous	Italian Trade Union of State Police Officers (silpcgil.it)	Hackers from the Anonymous collective release the contact information of over 200 Italian police officers, including their full names and personal email addresses. Hackers also post the user login name and password of 26 website administrators.	Unknown
31/12/2018	TheDarkOverlord	Several insurance groups including Hiscox Syndicates Ltd, Lloyds of London, and Silverstein Properties	TheDarkOverlord announces it had breached a law firm handling cases related to the September 11 attacks, and threatened to publicly release a large cache of related internal files unless their ransom demands were met. To provide evidence, the group publishes a link for a 10GB archive of files it allegedly stole.	Unknown
31/12/2018	?	Choice Rehabilitation	Choice Rehabilitation notifies patients after hack of corporate email account. The suspicious activity occurred from July 1, 2018 through September 30, 2018.	Account
01/01/2018	?	Faye Brookes	2018 begins with a new round of Fappening leaks. This time the victim is Faye Brookes, whose explicit video is leaked on several	Unknown

Date	Author	Target	Description	
			video sharing websites.	
17/10/2018	?	Tallahassee Memorial Hospital	Tallahassee Memorial Hospital reports the information of job applicants who applied to the facility may be at risk after a breach at Jobscience, a recruiting firm it uses.	Unknown
01/01/2018	?	Rockingham County Schools	Rockingham County Schools servers are compromised by the Emotet malware after an employee opens a phishing email.	Malware/
01/11/2018	?	Austal	Australian defence shipbuilder Austal is the victim of a data breach and an extortion attempt. The attackers gain access to ship designs and to some staff email addresses and mobile phone numbers. Fingers point to Iran.	Unknown
02/01/2018	Andariel	Unnamed South Korean Company	Bloomberg reveals that a hacking unit called Andariel seized a server at a South Korean company in the summer of 2017 and used it to mine about 70 Monero coins, worth about $25,000 as of Dec. 29.	Unknown
01/11/2018	Outlaw	Multiple Targets	Researchers from Trend Micro uncover an operation of a hacking group dubbed “Outlaw” involving the use of an IRC bot built in Perl Shellbot.	Malware
02/01/2018	@0x55Taylor	thefly.com	A hacker using the twitter handle @0x55Taylor posts some screenshots of a breach affecting all users who registered at thefly.com a leading digital publisher of real-time financial news between 2006 and 2015. The leak contains the data of 100,000 individuals, and the credit card details of 27,000 among them.	SQLi?
01/11/2018	LulzSec ITA and AntiSec ITA	Some Italian News Websites	In name of Op #FifthOfNovember, the Italian branch of the Anonymous hacks several news websites.	SQLi
03/01/2018	?	Uber Users	Symantec researchers discover a new malware strain, dubbed Android.Fakeapp, that sneakily spoofs Uber’s Android app and harvests users’ passwords, allowing attackers to take over users’ accounts.	Malware/
01/11/2018	?	St. Francis Xavier University	Canadian St. Francis Xavier University shuts down the entire network following a cryptojacking attack which attempted to use its systems' computing power to mine for Bitcoin.	Malware

Date	Author	Target	Description	
03/01/2018	?	Android Users	Researchers from Trend Micro discover 36 apps on Google Play in disguise of security tools, but in reality able to secretly harvesting user data, tracking user location, and aggressively pushing advertisements.	Malware/
01/11/2018	?	Single Individuals	Researchers from trend Micro discover a new Trickbot module adding password stealing capabilities.	Malware
03/01/2018	?	City of Farmington	The city of Farmington is hit by a variant of the SamSam ransomware.	Malware/
01/11/2018	?	Episcopal Health Services	Episcopal Health Services notifies patients after employee email accounts are hacked.	Account
03/01/2018	?	Linux Servers	Researchers at F5 discover a new Linux crypto-miner botnet dubbed PyCryptoMiner spreading over SSH. The Monero miner botnet is based on Python and leverages Pastebin as command and control server when the original C&C isn't available.	Malware/
02/11/2018	?	HSBC	A data breach at HSBC Bank allows attackers to gain access to a limited amount of customer's information such as account numbers, balances, addresses, transaction history, and much more. The attack affects about 1% of U.S. accounts and occurred between October 4th, 2018 and October 14th, 2018.	Credentia
03/01/2018	?	Bank customers globally	Researchers from security company Quick Heal reveal the detail of Android.banker.A9480, an Android banking trojan targeting more than 232 banking apps of financial institutions globally.	Malware/
02/11/2018	?	Facebook Users	Hackers appear to have compromised and published private messages from at least 81,000 Facebook users' accounts.	Malicious
03/01/2018	?	Big Line Holiday	Big Line Holiday, a Hong Kong travel agency, reveals that hackers might have broken into its database a day before and gained possession of some of its customers' personal information.	Malware/
02/11/2018	AnonPlus	Society of Authors and Publishers	AnonPlus hacks the website of the Italian Society of Authors and Publishers (SIAE) and leak 4Gb of data.	SQLi
04/01/2018	?	Ukrainian users	Researchers from Cisco Talos reveal that unknown attackers have compromised the official	Malware/

Date	Author	Target	Description	
			website of Ukrainian accounting software developer Crystal Finance Millennium to distribute a new variant of the malicious Zeus banking trojan. The compromised website hosts the payload retrieved by a dropper distributed via a spam campaign.	
02/11/2018	?	Ingerop	Hackers access confidential documents about nuclear plants and prisons in a cyberattack on the French Ingerop and leak 65Gb of data. The attack occurred back in June.	Unknown
04/01/2018	?	City of Belle Fourche	The city of Belle Fourche is hit by a ransomware attack.	Malware/
02/11/2018	Magecart	Kitronik	Educational electronics outlet Kitronik is the latest victim of the Magecart gang. The hack occurred between August and September.	Malware
04/01/2018	?	Goldjoy	Goldjoy, another travel agency in Hong Kong, reveals that unauthorised parties accessed its customer database containing personal information such as names and ID card numbers, passport details and phone numbers, asking for a ransom.	Malware/
02/11/2018	?	Five Guys	Five Guys notifies employees of data breach after an employee falls victim for a phishing attack.	Account
05/01/2018	?	Android Users	Security researchers from Check Point uncover LightsOut, a new mobile adware program hidden in 22 fake applications on the Google Play Store. According to the researchers, the apps were downloaded between 1.5 million and 7.5 million times.	Malware/
02/11/2018	?	Hobart's Henry Jones Art Hotel and Saffire Freycinet	Guests of two Tasmania's luxury hotels are notified that their personal data may have been accessed by an unauthorised third party.	Account
05/01/2018	?	Reddit	Reddit confirms that one of its email providers, Mailgun, has been breached, resulting in the hacks of user profiles and their linked cryptocurrency accounts.	Account
02/11/2018	?	Android Users	Security researchers reveal that two botnets, Fbot and Trinity, are fighting to take control over as many unsecured Android devices	Malware

Date	Author	Target	Description	
			as they can to use their resources and mine cryptocurrency.	
05/01/2018	?	Beautyblender	Beautyblender notifies 3,673 individuals that their information might have been compromised after the discovery of a malware on its online shop.	Malware/
03/11/2018	?	StatCounter	Researchers from ESET reveal that attackers successfully breached StatCounter, a leading web analytics platform, inject a malicious bitcoin stealer script to compromise gate.io	Malicious
05/01/2018	?	Oklahoma State University Center for Health Sciences (OSUCHS)	Oklahoma State University Center for Health Sciences notifies an undisclosed number of affected patients of an unauthorized third party occurred on November 2017.	Unknown
03/11/2018	LulzSec ITA and AntiSec ITA	Some Local Government Websites	In name of Op #FifthOfNovember, the Italian branch of the Anonymous hacks some local government websites.	SQLi
05/01/2018	@0x55Taylor	Creditseva	After defacing it, @0x55Taylor manages to gain access to creditseva main website server and a copy of the s3 bucket credentials.	Unknown
03/11/2018	LulzSec ITA and AntiSec ITA	Multiple Italian targets.	In the final round of their Op #FifthOfNovember, the Italian hacktivists dump multiple database from ministries, political parties, and other websites.	SQLi
05/01/2018	The Dark Overlord	Columbia Falls School District Number 6	The Columbia Falls School District Number 6 in Montana, sends out letters to notify the breach occurred after the attack carried on by The Dark Overlord begun on September 1st, 2017.	Unknown
05/11/2018	?	Twitter users	A widespread scam pretending to be from Elon Musk and utilizing a stream of hacked Twitter accounts and fake giveaway sites earns scammers over 28 bitcoins or approximately $180,000 in a single day.	Fake Twi
06/01/2018	?	Olympic Games in South Korea	Researchers from McAfee uncover a campaign, dubbed Operation PowerShell Olympics, targeting organizations involved with next month's Games in South Korea, with the aim of controlling infected machines.	Targeted
05/11/2018	?	Facebook and Instagram Users	30 Facebook accounts and 85 Instagram profiles have been removed by Facebook following suspicions of "coordinated	Social Ne

Date	Author	Target	Description	
			inauthentic behavior"	
06/01/2018	?	BlackBerry Mobile Site	The Blackberry Mobile site is hacked exploiting a vulnerability of Magento. The attackers install a Monero miner using the Coinhive library.	Magento
05/11/2018	?	www.myidentifiers.com	After unauthorized charges are done with cards used on www.myidentifiers.com, a site responsible for issuing ISBNs, an investigation reveals that unauthorized code was added to the checkout page affecting transactions between May 1 and October 23.	Malicious
06/01/2018	?	Florida's Agency for Health Care Administration (FAHCA)	A phishing attack on an employee at Florida's Agency for Health Care Administration (discovered in November 20, 2017) results in the exposure of sensitive information on 30,000 Medicaid patients.	Account
05/11/2018	Iran	Israel	Iran indirectly blames Israel for a series of attempted cyber attacks that it says targeted its communication infrastructure over the last few days.	Targeted
07/01/2018	?	CVE 2017-10271 Vulnerable Machines	A report published by the SANS Technology Institute reveals that attackers are exploiting a critical Oracle WebLogic flaw (CVE 2017-10271) to inject Monero cryptocurrency miners on victim's machines.	Malware/
05/11/2018	?	Telegram and Instagram users in Iran	Researchers from Cisco Talos reveal the details of Persian Stalker, a wave of campaigns against Telegram and Instagram users in Iran, leveraging the hijack of traffic through the BGP protocol.	BGP Hija
08/01/2018	?	Health South-East RHF	Health South-East RHF, a healthcare organization that manages hospitals in Norway's southeast region, announces a security breach. A hacker or hacker group might have stolen healthcare data for more than half of Norway's population. (over 2.9 million individuals)	Unknown
05/11/2018	?	EZECOM SINET Telcotech Digi	Several of Cambodia's biggest internet service providers (EZECOM, SINET, Telcotech, and Digi) are hit by large-scale DDoS attacks.	DDoS
08/01/2018	?	Single Individuals	Alien Vault reveals to have found malware that appears to install code for mining Monero cryptocurrency, sending any mined coins to a server at a North	Malware/

Date	Author	Target	Description	
			Korean university.	
05/11/2018		Pathé Twitter Account	The official account of Pathé, the world's second oldest operating film company and Europe's second largest studio, has been hacked to spread malicious Bitcoin giveaway links.	Account
08/01/2018	?	Onco360	Onco360 notifies a phishing incident involving an employee's email account and affecting potentially 53,000 users.	Account
06/11/2018	?	Megacable	Megacable notifies its users of a cyber attack.	Unknown
08/01/2018	?	Caremed Specialty Pharmacy	Caremed Specially Pharmacy is victim of the same event affecting Onco360	Account
06/11/2018	?	Twitter account of India's National Disaster Management Authority (NDMA)	The Twitter account of India's National Disaster Management Authority (NDMA) is hijacked to promote fake bitcoins giveaways.	Account
09/01/2018	Turla	Embassies and consulates in East Europe	Researchers from ESET unveil the details of a new operation carried on by the Turla cyber espionage group, targeting embassies and consulates in East Europe using a fake Adobe Flash updater.	Targeted
07/11/2018	?	Vulnerable Home Routers	Researchers from Qihoo 360's Netlab discover a massive botnet BCMUPnP_Hunter infecting 100,000 home routers worldwide.	UPnP Vu
09/01/2018	?	Android Users	Researchers at Trend Micro find in the Google Play Store the first Android malware designed to steal information, carry out click ad fraud, and sign users up to premium SMS services without their permission, written using the Kotlin programming language.	Malware/
07/11/2018	?	Bankers Life	Bankers Life notifies more than 566,000 individuals after the hack of some employees' email results in a breach of PHI. The breach occurred between May 30 and September 13, 2018.	Account
09/01/2018	?	Single Individuals	Malwarebytes reveal the details of a RIG exploit campaign distributing malware coin miners delivered via drive-by download attacks from malvertising, exploiting the RIG Exploit Kit.	Malvertis
07/11/2018	?	Spanish banks users	Researchers from Trend Micro discover a malicious app called Movil Secure, claiming to be connected to Banco Bilbao Vizcaya Argentaria (BBVA).	Malware
10/01/2018	Pawn Storm AKA Fancy Bear	International Olympic	APT28 AKA Pawn Storm AKA	Unknown

Date	Author	Target	Description	
	AKA APT28	Committee	Fancy Bear publish a set of apparently stolen emails purportedly belong to officials from the International Olympic Committee, the United States Olympic Committee, and third-party groups associated with the organizations.	
07/11/2018	Erwincho	Mobile World	A hacker dubbed Erwincho leaks a file containing more than 5.4 million email addresses and 31,000 bank card numbers (six digits covered), claiming they belong to clients of Mobile World.	Unknown
10/01/2018	?	Android Users	Researchers from Symantec discover a fake Telegram (Teligram) app on the Google Play Store that claims to be a new, updated version of the popular encrypted messenger app, but whose real purpose is to distribute malware.	Malware/
08/11/2018	?	Banking Customers in Brazil	Researchers from Cisco Talos identify two ongoing malware distribution campaigns used to infect victims with banking trojans, specifically financial institutions' customers in Brazil.	Malware
10/01/2018	?	Russian Bank Customers	Researchers at Trend Micro discover a new mobile malware that primarily targets Russian banking customers, taking over victims' SMS capabilities, allowing cybercriminals to intercept text messages that contain bank security codes, The malware is dubbed FakeBank.	Malware/
08/11/2018	?	Vulnerable ColdFusion Servers	Researchers from Volexity discover a new campaign carried out by a suspected Chinese APT group aimed to exploit vulnerable ColdFusion servers (CVE-2018-15961) to upload the China Chopper webshell.	CVE-2018
10/01/2018	?	Netflix Users	Netflix users are warned to avoid clicking on any suspicious email links after a phishing scam is uncovered by security firm Mailguard, which security experts say is designed to steal credit card details.	Account
08/11/2018	?	Vulnerable Wordpress Sites	Researchers from Wordfence discover a vulnerability in the popular plugin WP GDPR Compliance (more than 100,000 installs), exploited in the wild.	Wordpres
11/01/2018	?	Unpatched Windows and Linux servers	Researchers from Check Point and Certego reveals the details of a new campaign distributing a	Malware/

Date	Author	Target	Description	
			malware dubbed RubyMiner, turning outdated web servers into Monero miners.	
08/11/2018	?	Media Prima Bhd	Media Prima Bhd is hit by a ransomware attack and asked to pay a ransom of 1,000 bitcoins	Malware
11/01/2018	?	German Users	German authorities warn about phishing emails trying to take advantage of the Spectre and Meltdown vulnerabilities, promising fake patches and distributing the Smoke Loader malware.	Malware/
08/11/2018	?	Altus Baytown Hospital (ABH)	Altus Baytown Hospital (ABH) is hit by a Dharma ransomware attack on September 3, 2018, with a lot of documents containing patient info being encrypted and the attackers requesting a ransom to unlock the hospital's data.	Malware
11/01/2018	?	Apple Mac users	Patrick Wardle, a security researcher, discovers OSX MaMi, a new, undetectable strain of malware affecting Apple Macs that can hijack a device's DNS settings and steal victims' personal data.	Malware/
08/11/2018	?	Linux Servers	Researchers from Trend Micro discover a cryptocurrency-mining malware dubbed Coinminer.Linux.KORKERDS.AB affecting Linux systems, bundled with a rootkit component (Rootkit.Linux.KORKERDS.AA) to make it hidden.	Malware
11/01/2018	?	North Korean defectors	Researchers at McAfee unveil the details of operation Sun Team, a campaign targeting North Korean defectors, along with those who help them, which aims to infect their devices with trojan malware for the purposes of spying on them.	Malware/
08/11/2018	?	Southwest Washington Regional Surgery Center	Southwest Washington Regional Surgery Center notifies 2,393 patients after phishing attack exposed their PHI.	Account
11/01/2018	?	Adams Health Network	Adams Health Network, which runs Adams Memorial Hospital, confirms that a ransomware attack targeted some of its computer servers.	Malware/
09/11/2018	?	Florida's Department of Health	Florida's Department of Health issues a notice of data breach detailing the compromise of an employee's Microsoft Outlook 365 account. The breach occurred between October 8 – October 16, 2018.	Account

Date	Author	Target	Description	
12/01/2018	Pawn Storm AKA Fancy Bear AKA APT28	US Senate	Researchers from Trend Micro reveal that the state sponsored hackers behind APT28 (AKA Pawn Storm AKA Fancy Bear) targeted the US Senate in mid-2017).	Targeted
09/11/2018	?	SIngle Individuals	Researchers from ESET discover a new spam campaign carried out via the Emotet banking trojan.	Malware
12/01/2018	?	Hancock Regional Hospital	The Hancock Regional Hospital, in the state of Indiana, confirms to be running on pen and paper following a SAMSAM ransomware attack, which hit the day prior. The hospital eventually pays up hackers $55,000 to restore control.	Malware/
09/11/2018	?	Metrocare Services	Metrocare Services notifies 1,804 patients after some employees' email is hacked. The incident occurred on September 4, 2018.	Account
12/01/2018	?	Android Users	Researchers from Check Point reveals the details of 'AdultSwine', a malware displays pornographic advertising on Android applications, found in 60 gaming apps on Google Play and downloaded between three and seven million times.	Malware/
09/11/2018	?	Huntsville Hospital	Huntsville Hospital also reports the information of job applicants who applied to the facility may be at risk after the breach at Jobscience.	Unknowr
13/01/2018	?	New Zealand Football	New Zealand Football says it is investigating a potential hack of its official website after a fake news article popped up "announcing" the resignation of its CEO Andy Martin.	Defacem
09/11/2018	?	LPL Financial	LPL Financial sends a notification about a third-party hack involving Capital Forensics, Inc.	Unknowr
13/01/2018	?	BlackWallet	An unidentified thief reportedly steals more than $400,000 in Stellar lumens after hacking the digital wallet provider BlackWallet.	DNS Hija
09/11/2018	?	Chesapeake Public Schools	A malware received via phishing emails take down the systems of Chesapeake Public Schools.	Malware
14/01/2018	?	Devices powered by ARC CPUs	Researchers from infosec group Malware Must Die discover a new variant of the Mirai botnet capable of infecting devices powered by ARC CPUs. The botnet is dubbed "Okiru", which means "wake up" in Japanese.	Malware/
10/11/2018	?	May Eye Care	May Eye Care notifies 30,000	Malware

Date	Author	Target	Description	
			patients after ransomware incident.	
14/01/2018	Ayyıldız Tim	Syed Akbaruddin's Twitter Account @AkbaruddinIndia	The verified Twitter account of Syed Akbaruddin. India's top diplomat to the United Nations, is briefly taken over by suspected Turkish hackers.	Account
12/11/2018	?	Android Users	Researcher Lukas Stefanko discovers a malware available on Google Play for download for almost a year, with over 5,000 installs.	Malware
14/01/2018	Ayyıldız Tim	Borge Brende's Twitter Account @borgebrende	The same hackers also manage to hijack the verified account of Borge Brende, the president of the World Economic Forum and former minister of foreign affairs for Norway.	Account
12/11/2018	?	Single Individuals	Researchers from McAfee reveal the details of WebCobra, a new Russian cryptojacking malware.	Malware
15/01/2018	?	OnePlus	Chinese smartphone manufacturer OnePlus launches an investigation after a number of customers who used its website to purchase products complain of attempted fraud. Few days after (January 19) the company confirms to have been hacked via a malicious script injected into its website, potentially compromising the payment card details of up to 40,000 customers.	Maliciou
12/11/2018	White Company (state sponsored actor)	Pakistan Air Force	Cylance uncover a sophisticated state-sponsored campaign, tracked as Operation Shaheen, against the Pakistan Air Force, carried out by a nation-state actor tracked as the White Company.	Targeted
15/01/2018	?	Chrome Users	Security researchers from ICEBRG find four malicious Chrome extensions available in the Chrome store, laced with suspicious code, and infecting more than 500,000 users across the globe, including workstations within major organizations.	Maliciou
12/11/2018	?	Multiple Twitter Accounts	Scammers hijack other verified Twitter accounts to promote fake cryptocurrency giveaway links. The victims include: the Australian branch of Capgemini, the Consulate General of India in Germany, California state senator Ben Allen, and Israeli politician Rachel Azaria.	Account
15/01/2018	?	Financial Organizations in Latin America	Researchers from Trend Micro spot a new variant of the KillDisk disk-wiping malware targeting	Malware/

Date	Author	Target	Description	
			companies in the financial sector in Latin America.	
12/11/2018	?	Health First, Inc.	Health First, Inc. notifies 42,000 patients after a phishing incident.	Account
12/01/2018	?	Monticello Central Strict District	Monticello Central School District warns of a sophisticated e-mail phishing attack occurred on November 1st, 2017. Potentially 2,598 individuals are affected.	Account
12/11/2018	?	Midlands State University	Midlands State University is forced to postpone its Student Representative Council Elections after hackers breach the security system.	Unknown
16/01/2018	Group 123	Multiple targets mainly in South Korea	Researchers from Cisco Talos reveal the details of the malicious activities of Group 123, a malicious actor linked to North Korea, author of at least six malicious campaigns focused on South Korean targets.	Targeted
13/11/2018	?	G Suite Twitter Account	Google's official G Suite Twitter account, which has more than 800,000 followers, is the latest victim of an increasingly widespread Bitcoin scam.	Account
16/01/2018	?	Several Italian Individuals	Researchers from Kaspersky Lab reveal the details of Skygofree, an Android malware, reminiscent of the Hacking Team surveillance malware, targeting some Italian individuals.	Malware/
13/11/2018	TEMP.Periscope	UK Engineering Company	Researchers from Recorded Future reveal the details of a spear phishing campaign carried out by the Chinese TEMP.Periscope group against a UK based engineering company, leveraging Russian APT Techniques.	Targeted
16/01/2018	Ayyıldız Tim	Eric Bolling (@ericbollingTR) and Greta Van Susteren (@greta) Twitter accounts	Former Fox News hosts Eric Bolling and Greta Van Susteren appear to have their Twitter accounts hijacked by a group of suspected Turkish hackers dubbed Ayyıldız Tim.	Account
13/11/2018	?	Users in Spain and France	Researchers from enSilo discover DarkGate, a sophisticated password stealer with multiple resilience and evasion capabilities.	Malware
16/01/2018	?	Several cryptocurrency exchanges such as Coinlink.	According to the security firm Recorded Future, the notorious North Korean hacking outfit Lazarus Group is behind cyberattacks that targeted South Korean cryptocurrency exchanges and users towards the end of	Account

Date	Author	Target	Description	
			2017, security researchers have found. However Coinlink denies the claims.	
13/11/2018	?	Target Twitter Account	Target’s Twitter account is hacked and its feed used to trick unsuspecting consumers into giving away cryptocurrency.	Account
16/01/2018	?	Singing River Health System	Unknown attackers try to break into the Singing River Health System’s network.	Unknown
13/11/2018	?	Android Users	Researcher Lukas Stefanko discover four additional malicious Android apps camouflaged as fake cryptocurrency wallets.	Malware
17/01/2018	?	Bank Customers in the UK, France and Australia	Security researchers at Forcepoint reveal a new improved version of the financial malware Dridex, targeting victims in the UK, France and Australia and using compromised FTP websites in phishing campaigns.	Malware/
14/11/2018	APT29 AKA Cozy Bear	Multiple Target in the US	Multiple security companies including Crowdstrike and FireEye reveal a new spear phishing campaign carried out by APT29 (after one year of silence) targeting multiple sectors in the U.S.	Targeted
17/01/2018	?	Several telecommunications, insurance and financial service firms.	Researchers from security firm FireEye reveal a new spam campaign delivering the Zyklon HTTP malware, and exploiting three relatively new Microsoft Office vulnerabilities. The attackers are targeting telecommunications, insurance and financial service firms. The malware comes with a variety of features, like password stealing, keylogging, DDoS and crypto mining.	Malware/
14/11/2018	?	Midlands Regional Hospital in Tullamore	Midlands Regional Hospital in Tullamore is hit by a ransomware attack	Malware
17/01/2018	?	Claymore mining rigs	A new variant of the Satori botnet springs back to life, targeting Claymore mining rigs, and replacing the device owner's mining credentials with the attacker's own.	Malware/
14/11/2018	?	Italian certified email accounts	Unknown hackers gain access to thousands of Italian certified email accounts, including those of magistrates and security officials.	Targeted
17/01/2018	?	Single Individuals	Necurs, the world's largest spam botnet, is back on track, sending millions of spam emails that push	Malware/

Date	Author	Target	Description	
			an obscure cryptocurrency named Swisscoin, used for Multi-Level-Marketing (MLM) Ponzi scheme.	
14/11/2018	Magecart	Infowars' online store	A Magecart credit card skimming attack is discovered on the online store for the Infowars web site.	Malware
18/01/2018	Dark Caracal	Victims inside governments, militaries, utility companies, financial institutions, manufacturing companies and defense contractors in 21 different countries	Security researchers from digital rights organization Electronic Frontier Foundation and security firm Lookout reveal a long lasting campaign allegedly carried on by attackers tied to the Lebanese government, able to steal hundreds of gigabytes from thousands of victims all over the world. The group is dubbed Dark Caracal.	Targeted
14/11/2018	?	Targets in Middle East	Security researchers from Kaspersky reveal that the CVE-2018-8589 Windows zero-day vulnerability addressed by Microsoft November 2018 Patch Tuesday has been exploited by an APT group in targeted attacks against entities in the Middle East.	Targeted
18/01/2018	?	Android Users	Google removes 53 apps from the official Play Store because they were spreading a new breed of Android malware named GhostTeam, active since April 2017, that could steal Facebook credentials and push ads to infected phones.	Malware/
15/11/2018	TA505	Single Individuals	Researchers from Proofpoint reveal a new campaign by the prolific actor TA505 aimed to deliver a new remote access trojan dubbed tRAT to victims in order to create a backdoor into PCs to steal credentials and banking information.	Malware
18/01/2018	?	Allscripts	A ransomware attack takes down some of the applications used by Allscripts.	Malware/
15/11/2018	?	HealthEquity	n intruder accesses the email accounts of two HealthEquity members, exposing protected health information (PHI)/ personally identifiable information (PII) of 20,906 subscribers. The breach dates back to September and October, and was discovered on October 5th.	Account
18/01/2018	?	Questar Assessment	A data breach at the company that develops New York State’s third-through-eighth grade reading and math tests allows an unauthorized user to access information about 52 students. Also students in	Unknown

Date	Author	Target	Description	
			another state are affected, but the company does not provide further details.	
15/11/2018	?	Multiple targets	Researchers from CenturyLink reveal a new waves of attacks carried out via the Mylobot botnet.	Malware
19/01/2018	?	IOTA	Malicious websites used to generate password details for the fintech network IOTA (online seed generators) are reportedly to blame for the theft of nearly $4m (£2.9m) from users' digital wallets.	Account
15/11/2018	?	Family Tree Relief Nursery	Some 2,000 clients of Albany-based nonprofit Family Tree Relief Nursery are notified of a ransomware attack occurred between June and August.	Malware
19/01/2018	?	Electronic Gas Stations	Russian authorities identify a distributed malware campaign targeting electronic gas stations using software programs at the pumps. Dozens of gas stations have been attacked with customers paying more for fuel (around 3 to 7% increment per gallon).	Malware/
15/11/2018	?	Misconfigured Docker services	Researchers at Juniper Networks discover that cybercriminals are currently taking advantage of misconfigured Docker services to add their own containers that run a Monero mining script.	Misconfig
19/01/2018	?	Westminster Ingleside King Farm Presbyterian Retirement Communities	Westminster Ingleside King Farm Presbyterian Retirement Communities notifies 5,228 Residents of a malware attack occurred on November 21, 2017	Malware/
15/11/2018	?	Daniel’s Hosting	Hackers compromise Daniel’s Hosting, one of the largest Dark Web hosting provider, and deleted 6,500+ sites.	PHP 0-Da
19/01/2018	?	Charlotte Housing Authority	341 employees of the Charlotte Housing Authority have their W-2 forms compromised after scammers sent CHA staffers an e-mail pretending to be from CEO.	Account
15/11/2018	Silence and MoneyTaker	Russian Financial Institutions	Group-IB identifies two major phishing campaigns targeting Russian financial institutions with emails purporting to come from the country's central bank and financial cybersecurity authorities.	Account
21/01/2018	?	Android Users	Security researchers at Russian cybersecurity company Dr.Web discover a dangerous Android malware hidden in several gaming apps on Play store stealing	Malware/

Date	Author	Target	Description	
			personal data from users by conducting phishing attacks. The malware is dubbed Android.RemoteCode.127.origin and has been downloaded more than 4,000,000 times.	
22/01/2018	?	Fire and Fury Readers	Researchers spot a copy of Michael Wolff's book Fire and Fury infected with malware.	Malware/
22/01/2018	Ayyıldız Tim	David Clarke Jr. Twitter Account	The Turkish Cyber Army hacking group strikes again and hijacks the Twitter account of vocal Donald Trump supporter and ex-Milwaukee County Sheriff David Clarke Jr.	Account
22/01/2018	?	Charissa Thompson	Fox Sports host Charissa Thompson is the latest celebrity whose nude photos are stolen by hackers and then published online as part of The Fappening scandal.	Account
22/01/2018	?	Apache Servers	Researchers from Trend Micro report a significant increase in the use of Apache Struts (CVE-2017-5638) and DotNetNuke (CVE-2017-9822) vulnerabilities to implant Monero miners.	Apache S
23/01/2018	?	Bell Canada	Police are investigating a new data breach at Bell Canada (the second in eight months), which says hackers have illegally obtained customer information, primarily subscriber names and e-mail addresses of up to 100,000 users.	Unknown
23/01/2018	?	Metrolinx	Ontario transit agency Metrolinx says it was the target of a cyberattack that originated in North Korea, but no personal information was compromised.	Unknown
23/01/2018	?	220,000 Malaysian organ donors.	Another data breach in Malaysia. A technology forum publishes details of a trove of data which includes the personal information of more than 220,000 organ donors.	Unknown
23/01/2018	Nexus Zeta	IoT Devices Worldwide	According to a new report by Newsky Security, the author of the infamous Satori IoT botnet has created two new variants of the predecessor Mirai, called Masuta and PureMasuta.	Malware/
23/01/2018	?	Turkish Defense Contractors	According to RiskIQ, an unknown actor purporting to be from the tax collection arm of the Turkish government is carrying out spear-phishing campaigns against Turkish defense contractors, using a RAT called Remcos.	Targeted

Date	Author	Target	Description	
23/01/2018	?	Twitter Users	Researchers from Malwarebytes reveal a fresh malware campaign spreading via a spamming Twitter accounts.	Malware/
23/01/2018	?	National Stores, Inc.	National Stores, Inc. announces that it has been the victim of a malware attack, enabling unauthorized parties to access payment card information. It appears that payment cards used by customers at some National Stores locations between July 16 and December 11, 2017 may be involved.	Malware/
23/01/2018	?	Unnamed company in Greenbay	Unknown hackers use a known vulnerability to get into a company's computer system, stealing personal information from human resources files, and then using that to steal what police call "significant amounts" of money from several people.	Undisclos
24/01/2018	?	Single Individuals	Researchers from Sucuri reveal a new campaign targeting more than 2,000 compromised websites and aimed to both mine Monero and stealing the users credentials.	Malicious
24/01/2018	?	Harris County	Harrys County lose almost $900K in a phishing scam. The attack dates back to September 2017.	Account
24/01/2018	?	Victims based primarily in Thailand, Vietnam and Egypt	Researchers from Palo Alto Networks discover A newly discover a malicious URL redirection campaign that infects users with the XMRig Monero cryptocurrency miner. The campaign has already victimized users between 15 and 30 million times.	Malvertis
24/01/2018	?	IoT Devices Worldwide	Bitdefender researchers uncover an emerging IoT botnet that uses advanced communication techniques to exploit victims and build its infrastructure. The bot is dubbed Hide 'N Seek (HNS)	Malware/
24/01/2018	?	5 universities, 23 private companies and several government organizations.	Security researchers from Comodo spot a new strain of sophisticated malware, dubbed Lebal, targeting a number of high-profile entities, including five universities, 23 private companies and several government organizations.	Targeted
25/01/2018	?	Single Individuals	Researchers from Crowdstrike discover a new strain of malware that uses the National Security Agency's EternalBlue exploit to	Malware/

Date	Author	Target	Description	
			hijack computers and secretly mine cryptocurrency. The malware is dubbed WannaMine.	
25/01/2018	?	Single Individuals	A new ransomware called MoneroPay is discovered that tries to take advantage of the cryptocurrency craze by spreading itself as a wallet for a fake coin called SpriteCoin.	Malware/
25/01/2018	OilRig	8 Middle Eastern government organizations, as well as one financial and one educational institution.	Researchers from Palo Alto Networks reveal a new operation of the Iran-linked cyber-espionage group tracked as OilRig, carried on using a backdoor dubbed RGDoor to target Internet Information Services (IIS) Web servers.	Targeted
26/01/2018	?	Financial Organizations in Latin America	NCR sends an advisory to its customers saying it had received reports from the Secret Service and other sources about jackpotting attacks against ATMs in the United States. Sources say the malware behind the attack is Ploutus.D.	Malware/
26/01/2018	?	YouTube Users	YouTube is caught displaying ads that covertly use visitors' CPUs and electricity to generate digital currency on behalf of anonymous attackers.	Malicious
26/01/2018	?	Coincheck	Japanese cryptocurrency exchange Coincheck confirms that some $524 million worth of digital coins (a cryptocurrency called NEM) has been stolen—likely making it the largest single hack on an exchange.	Unknown
26/01/2018	?	Users in the Middle East	Security researchers from Palo Alto Networks detect a fresh wave of attacks targeting users in the Middle East. Attackers use Arabic language documents related to current political events to download and run malicious malware. The campaign is called 'TopHat' and makes use of a malware dubbed 'Scote'.	Targeted
26/01/2018	?	Chrome Users	Trend Micro publishes a list of malicious Chrome extensions making use of a recently discovered technique called "Session Replay" attack.	Malicious
26/01/2018	?	phpBB	An unknown attacker compromises download links for the phpBB forum software, according to a statement released today by the phpBB development team.	Unknown
27/01/2018	?	ABN Ambro	ABN Ambro is the victim of a sustained DDoS attack. The wave	DDoS

Date	Author	Target	Description	
			of cyberattacks comes just days after local media reported that Dutch intelligence agency AIVD spied on Russia-linked hacker group Cozy Bear, also known as APT29, as early as 2014.	
27/01/2018	?	ING	During the same weekend, also ING is targeted.	DDoS
28/01/2018	?	Experty	A hacker tricks Experty ICO participants into sending Ethereum funds to the wrong wallet address. He is able to do this by sending emails with a fake pre-ICO sale announcement to Experty users who signed up for notifications. The bounty amounts to $150,000 worth of Ethereum.	Account
28/01/2018	?	Ontario Progressive Conservative Party	The Ontario Progressive Conservative Party’s internal database is locked up by a ransomware attack in early November. The incident is first being acknowledged now.	Malware/
29/01/2018	?	Rabobank	Rabobank is the third of the big Dutch banks to be targeted by a DDoS attack.	DDoS
29/01/2018	?	Dutch tax authority	The Dutch Tax Authority is also taken down by a DDoS attack.	DDoS
29/01/2018	?	DigID	The Dutch official online signature system DigID is also reportedly hit by the same wave of DDoS attacks.	DDoS
29/01/2018	Suspected malicious actor tied to Pakistan	Android Users in India	Security researchers from Trend Micro unveil the details o a cyber espionage campaign targeting Android users in India, using the PoriewSpy and Droid.jack malware.	Malware/
29/01/2018	?	Ransomware victims	The operators of at least one Tor proxy service are caught replacing Bitcoin addresses on ransomware payment sites, diverting funds meant to pay for ransomware decrypters to the site's operators. In this way the victims are damaged twice.	Tor Traffi
29/01/2018	?	Chester County School District	Chester County School District posts on its Facebook page that ransomware hit the district’s servers over the weekend.	Malware/
30/01/2018	?	Ukrainian Individuals	Researchers from Palo Alto Networks uncovered a two-year-old cyber espionage campaign	Targeted

Date	Author	Target	Description	
			that's been infecting Ukrainians with either a newly discovered remote access tool called Vermin or the more established Quasar RAT.	
30/01/2018	?	ABN Ambro	ABN Ambro is targeted by a new DDoS attack. Now the fingers are pointed to Russia.	DDoS
30/01/2018	?	ING	And during the same wave of DDoS attacks, also ING is targeted (once again).	DDoS
30/01/2018	?	Single Individuals	Security researchers from Malwarebytes uncover a new strain of ransomware called GandCrab that is being distributed through two separate exploit kits: the RIG EK and GrandSoft EK.	Malware/
30/01/2018	?	Spartanburg Public Library	The Spartanburg Public Library system is shut down after it is hit with a ransomware attack.	Malware/
31/01/2018	?	More than 526,000 infected Windows hosts	Researchers from Proofpoint reveal the details of the Smominru botnet. A Monero miner, active since May 2017, exploiting the Eternal Blue (CVE-2017-0144) and EsteemAudit (CVE-2017-0176) vulnerabilities to spread.	Malware/
31/01/2018	?	Users participating to the ICO of the Bee Token Crypto Currency	Users who were aiming to buy Bee Tokens during a Token Generation Event (i.e., an initial coin offering) are tricked into sending the money to scammers instead. The attackers steal nearly $1M worth of cryptocurrency.	Account
31/01/2018	?	GoGet	Car-sharing company GoGet discloses a major data breach seven months after it was first detected in June 2017 as the alleged hacker is arrested by Australian police this week. In an email sent to customers, the firm says its IT team identified "unauthorised activity" on its system on 27 June last year and immediately launched a full internal investigation.	Unknown
31/01/2018	?	Firefox Users	A Firefox extension called Image Previewer is discovered, injecting a Monero in-browser miner into Firefox. While we have seen numerous Chrome.	Malicious
31/01/2018	North Korea	South Korea	South Korea’s Internet & Security Agency (KISA) warns of a Flash zero-day vulnerability (CVE-2018-4878) reportedly exploited in attacks by North Korea’s hackers.	Targeted
01/02/2018	?	Single Individuals	The FBI warns hackers have been	Account

Date	Author	Target	Description	
			impersonating a federal online crime complaint portal to trick victims into divulging their personal and sensitive information in a new phishing scam.	
01/02/2018	Iron Tiger	Institutions in the government, technology, education and telecommunications sector in Asia and the US.	Security researchers from BitDefender discover a custom-built piece of malware wreaking havoc in Asia for several months that could signal the return of the notorious Chinese hacker group - Iron Tiger. The campaign is called Operation PZChao, and has been targeting institutions in the government, technology, education and telecommunications sector in Asia and the US.	Targeted
01/02/2018	?	Google Chrome Users	Security researchers from Trend Micro uncover 89 malicious Google Chrome extensions on the official Chrome store that can inject ads, code to secretly mine cryptocurrency, and load a tool to record and replay a person's browsing activities. According to researchers, this collection of extensions affected over 423,000 users and was used to form a new botnet called "Droidclub."	Malware/
01/02/2018	?	IoT Devices	Researchers from cyber-security firm Radware discover a new IoT DDoS botnet, built by San Calvicie, an operator of a gaming server rental business. The botnet is called JenX. The botnets borrows parts of different other IoT botnets (for instance CVE-2014-8361 and CVE-2017–17215).	Vulnerab
01/02/2018	?	City of Pittsburg in Kansas	The City of Pittsburg in Kansas reveals to have been subjected to a sophisticated phishing scheme targeting employee payroll data. The attack results in the release of sensitive information for current and former city employees who received a W-2 for the 2017 fiscal year.	Account
01/02/2018	?	HORNE LLP	HORNE LLP notifies an incident affecting the security of protected health information of certain Forrest General Hospital patients. On November 1, 2017, the company discovered that the email account of one of its employees was sending phishing emails.	Account
01/02/2018	?	City of Batavia	The city of Batavia reports employees’ personal and financial	Account

Date	Author	Target	Description	
			information was compromised through an email phishing of W-2 tax forms. The information includes names, social security numbers, addresses and earnings.	
01/02/2018	?	Kinetics Systems	Kinetics Systems falls victim of a phishing attack. The personal information of 11 residents of New Hampshire, including their W-2 forms, is compromised.	Account
01/02/2018	?	Purchase Line School District	The Purchase Line School District is the victim of a email spoofing attack by an individual pretending to be a school district employee.	Account
01/02/2018	?	Coastal Cape Fear Eye Associates	Coastal Cape Fear Eye Associates notifies HHS of a ransomware incident that impacted 925 patients.	Malware/
01/02/2018	?	Aperio	Aperio informs of a data breach that occurred when two employees' email accounts were compromised by successful phishing attacks that resulted in auto-forwarding email from those accounts to two external accounts.	Account
02/02/2018	?	Redis and OrientDB servers	Researchers from Qihoo 360 discover a new Monero-mining botnet targeting Redis and OrientDB servers, infecting nearly 4,400 servers and able to mine over $925,000 worth of Monero since March 2017. The botnet, called DDG, targets Redis servers via a credentials dictionary brute-force attack; and OrientDB databases by exploiting the CVE-2017-11467 remote code execution.	Brute For Executior
02/02/2018	?	Mac Users	Researchers from Malwarebytes reveal that the MacUpdate site has been hacked to distribute the OSX.CreativeUpdate Monero miner via maliciously-modified copies of the Firefox, OnyX, and Deeper applications.	Malware/
02/02/2018	?	Ron's Pharmacy Services	Ron's Pharmacy Services notifies certain patients of the unauthorized access to certain limited pieces of patient information, including patient names, Ron's Pharmacy internal account numbers, and payment adjustment information, after an employee email account was compromised in October 2017.	Account
03/02/2018	?	Android Users	Researchers from Qihoo 360 discover an additional botnet, targeting Android devices by	Malware/

Date	Author	Target	Description	
			scanning for open debug ports so it can infect victims with malware that mines the Monero cryptocurrency. The botnet targets port 5555, which on devices running the Android OS is the port used by the operating system's native Android Debug Bridge (ADB). The malware is dubbed ADB.Miner.	
04/02/2018	?	Reddit Users	Security Researcher Alec Muffett discovers a clone of the popular social news aggregation and discussion site Reddit on the reddit.co domain.	Account
04/02/2018	?	City of Keokuk	The City of Keokuk says a data breach resulted in the release of personal information of current and former city employees and elected leaders. An unauthorized party was able to obtain 2017 W-2 tax forms through the use of a “criminal phishing email.”	Account
05/02/2018	?	Waldo County	A phishing attack compromised the information of 100 Waldo County employees	Account
05/02/2018	?	City of Keokuk	The city of Keokuk has disclosed that a cybercriminal used a phishing scam to fraudulently obtain an electronic file containing the 2017 W-2 tax forms of current and former employees and elected officials.	Account
05/02/2018	?	Partners HealthCare System	Partners HealthCare System reveals to have discovered a malware attack, occurred in May, 2017 that may have exposed 2,600 patients’ information.	Malware/
05/02/2018	?	University of Northern Colorado	The private information of 12 University of Northern Colorado employees is compromised lafter an “unknown person or group” accessed their profiles on Ursa, UNC’s online portal.	Unknown
06/02/2018	Hidden Cobra, aka Lazarus Group	Multiple Targets	The Department of Homeland Security (DHS) and FBI jointly release two new reports analyzing trojan malware attributed to Hidden Cobra, aka Lazarus Group -- a threat actor widely believed to be sponsored by the North Korean government. The two malware packages, referred to as HARDRAIN and BADCALL, can install a remote access tool (RAT) payload on Android devices, and force infected Windows systems	Targeted

Date	Author	Target	Description	
			to act as a proxy server.	
06/02/2018	AnonPlus	Italian Democratic Party (PD)	The AnonPlus hacker group says they have hacked the Florence branch of the Italian centre-left Democratic Party (PD) and leaked data regarding leader Matteo Renzi online.	Unknown
06/02/2018	AnonPlus	Province of Milan	The same hackers also claim to have hacked the website of Provincia di Milano (Province of Milan) in Italy.	SQLi
07/02/2018	?	Swisscom	Swisscom, the biggest telecom company in Switzerland, suffers a data breach that resulted in the compromise of personal data of some 800,000 customers, i.e., nearly ten percent of the entire Swiss population. The breach dates back to Autumn 2017 and the data accessed includes the first and last names, home addresses, dates of birth and telephone numbers of Swisscom customers.	Account
07/02/2018	?	The Sacramento Bee	The Sacramento Bee deletes two databases hosted by a third party after a ransomware attack exposed the voter records of 19.5 million California voters and 53,000 current and former subscribers to the newspaper.	Malware/
07/02/2018	?	Nova Poshta	Personal data of 500,000 Nova Poshta clients, the largest private delivery company in Ukraine, is allegedly leaked to dark web.	Unknown
07/02/2018	?	City of Enumclaw	The city of Enumclaw accidentally sends an email to an "individual pretending to be a member of City administration" and compromises the W-2s of hundreds of employees.	Account
07/02/2018	?	Twitter Users	Online scammers have made over $5,000 worth of Ethereum in one night alone, creating fake Twitter profiles for real-world celebrities and spamming the social network with messages tricking users to participate in "giveaways."	Fake Twi
07/02/2018	?	Targets in Middle East	Researchers from Cisco Talos reveal the details of a campaign targeted against entities with an interest in the geopolitical context of the region.	Targeted
07/02/2018	?	Business Wire	Press release network Business Wire admits suffering an ongoing Distributed Denial of Service (DDoS) attack lasting a week.	DDoS

Date	Author	Target	Description	
07/02/2018	?	Smith Dental	Smith Dental notifies of a ransomware attack affecting 1,500 patients.	Malware/
08/02/2018	?	Undisclosed Water Utility Company	Researchers from Radiflow discover the first example of a malware attacking the operational network of a water utility company in order to mine the Monero cryptocurrency,	Malware/
08/02/2018	?	Decatur County General Hospital	Decatur County General Hospital in Parsons, Tenn., publicly discloses that an unauthorized party accessed the server for its electronic medical record system and secretly implanted cryptomining malware.	Malware/
08/02/2018	?	Single Individuals	Researchers from Trend Micro reveal the details of a malicious spam campaign aimed to distribute the Loki malware.	Malware/
08/02/2018	?	Mikaela Hoover	The Fappening scandal continues even in 2018, and Guardians of the Galaxy actress Mikaela Hoover appears to be the most recent victim.	Account
08/02/2018	?	Multiple Targets	Researchers from ForcePoint discover a new strain of point-of-sale (PoS) malware that disguises itself as a LogMeIn service pack and steals payment card information through a DNS server.	Malware/
08/02/2018	?	Cisco ASA Users	Five days after details about a vulnerability in Cisco ASA software (CVE-2018-0101) becomes public, Cisco reveals to be "aware of attempted malicious use of the vulnerability."	Cisco AS
08/02/2018	?	Single Individuals	A new malspam campaign is underway, installing the GandCrab ransomware on a victim's computer. This is done through a series of malicious documents that ultimately install the ransomware via a PowerShell script.	Malware/
09/02/2018	?	Single Individuals	A new ransomware is discovered called Black Ruby. The ransomware encrypts the files on a computer, scrambles the file name, and then appends the BlackRuby extension. To make matters worse, Black Ruby also installs a Monero miner. The malware only encrypts computer not from Iran.	Malware/
10/02/2018	Vietnamese Hacker	Newtek Business Services Corp.,	Newtek Business Services Corp., a Web services conglomerate that operates more than 100,000 business Web sites and some	DNS Hija

Date	Author	Target	Description	
			40,000 managed technology accounts, has several of its core domain names stolen over the weekend.	
10/02/2018	?	BitGrail	Italian cryptocurrency exchange BitGrail reports a loss of 17 million Nano, valued at over $170 million at the time of the hack. However, conflicting reports surface with some believing the exchange to be insolvent for a number of months.	Unknown
11/02/2018	?	Pyeongchang Winter Olympics	Pyeongchang Winter Olympics organizers confirm that the Games had fallen victim to a cyber attack during Friday's opening ceremony, but they refused to reveal the source. Researchers from Cisco Talos call the malware Olympic Destroyer and confirm that the only purpose is to disrupt systems.	Targeted
11/02/2018	?	4,275 sites	4,275 sites are injected with an in-browser Monero miner after a popular accessibility script, BrowseAloud by TextHelp.com, is compromised. The list of the affected sites includes government websites such as uscourts.gov, ico.org.uk, & manchester.gov.uk.	Malicious
12/02/2018	?	Wordpress Websites	Two malicious plug-ins are recently discovered by Sucuri, injecting obfuscated JavaScript into WordPress websites, in order to generate advertisements that appear if a visitor clicks anywhere on the page.	Wordpres
12/02/2018	?	Android Users	Malwarebytes researchers detect a series of attacks that began around November 2017 in which millions of Android devices were targeted redirecting to a specifically designed page performing in-browser cryptomining of Monero virtual currency.	Drive-By
12/02/2018	Hidden Cobra, aka Lazarus Group	Bitcoin users and global financial organizations.	Researchers from McAfee discover an aggressive Bitcoin-stealing phishing campaign by the international cybercrime group Lazarus that uses sophisticated malware with long-term impact. The campaign is dubbed HaoBao and targets Bitcoin users and global financial organizations.	Targeted
12/02/2018	?	Single Individuals	A new variant of Rapid Ransomware is currently being distributed using malspam that pretends to be from the Internal	Malware/

Date	Author	Target	Description	
			Revenue Service.	
12/02/2018	?	Single Individuals	Researchers from IBM's X-Force reveal the details of a new campaign leveraging the Necurs botnet to send Valentine's Day-themed spam emails. The campaign reaches over 230 million spam messages within a matter of two weeks.	Malware/
12/02/2018	?	Idaho Transportation Department (ITD)	A hack of two email accounts at the Idaho Transportation Department (ITD) potentially exposes the personal information of commercial truckers whose rigs are registered in Idaho, including Social Security and credit card numbers. About 114 individuals are notified.	Account
12/02/2018	?	Entergy	Entergy notifies employees of a W-2 breach involving the TALX portal (a wholly-owned subsidiary of Equifax). The breach involves 2016 W-2 data.	Unknown
13/02/2018	?	Telegram Users	Researchers from Kaspersky reveal that malware authors have used a zero-day vulnerability in the Windows client for the Telegram instant messaging service to infect users with cryptocurrency mining malware (Monero, Zcash, and Fantomcoin primarily).	Zero-Day Telegram
13/02/2018	?	Android Users	Researchers from Trend Micro detect a new variant of Android Remote Access Tool (AndroRAT) (identified as ANDROIDOS_ANDRORAT.HRXC) that has the ability to inject root exploits. The AndroRAT targets CVE-2015-1805, a publicly disclosed vulnerability in 2016.	Malware/
13/02/2018	?	Military personnel and businessmen, among others, in various South Asian countries	Valentine's Day is approaching, and researchers from Trend Micro reveal that criminals from the Confucius gang are targeting military personnel and businessmen, among others, in various South Asian countries, persuading them into downloading malware hidden in chat apps.	Targeted
13/02/2018	?	Vulnerable Firewalls	Researchers from NewSky Security discover a new IoT botnet, dubbed DoubleDoor, exploiting CVE-2015–7755 and CVE-2016–10401 to bypass respectively Juniper and Zyxel firewalls.	Malware/
13/02/2018	?	Advertisement Screen in	And the last victim of the	Malware/

Date	Author	Target	Description	
		London	cryptocurrency frenzy is an advertisement screen in London that is infected by a miner.	
14/02/2018	?	Staybridge Suites Lexington Hotel	The Staybridge Suites Lexington Hotel is hit with what appears to be a point of sales data breach that occurred when several devices at the hotel were hit with malware.	Malware/
14/02/2018	?	Single Individuals	Researchers from Trustwave reveal a new multi-stage email word attack, exploiting CVE-2017-11882, but not making use of any macro.	Malware/
14/02/2018	?	Single Individuals	A Ukrainian cybercrime operation has made an estimated $50 million by using Google AdWords to lure users on Bitcoin phishing sites. The operation is temporarily disrupted by the Ukrainian cyber police, acting on information received from Cisco's Talos security division. The campaign is dubbed Coinhoarder.	SEO Pois
14/02/2018	?	Bitmessage users	Maintainers of the Bitmessage P2P encrypted communications protocol have released a fix after discovering that hackers were using a zero-day in attempts to steal Bitcoin wallet files from users' computers.	Zero-Day Bitmessa
14/02/2018	?	Atos	Reports emerge that the Olympic Destroyer malware might be used months before to target Atos, the IT provider of Winter Olympics.	Targeted
14/02/2018	?	Western Union	Western Union warns that some customers' information may have been accessed without authorization as a result of a computer intrusion against an external vendor system formerly used by Western Union for secure data storage	Unknown
15/02/2018	?	Jenkins CI Servers	Researchers from Check Point reveal the details of Jenkins Miner, a massive operation targeting Jenkins CI servers, via CVE-2017-1000353, aimed to mine Monero cryptocurrency. The Criminals are able	Malware/
15/02/2018	?	Retina-X Studios	A vigilante hacker claims to have wiped 1 Terabyte of data from Retina-X Studios, a company that sells spyware products.	Unknown
15/02/2018	GOLD LOWELL	Multiple Targets	Researchers from SecureWorks reveal the detail of a threat actor dubbed GOLD LOWELL using the SAMSAM ransomware for opportunistic attacks.	Malware/

Date	Author	Target	Description	
15/02/2018	?	Single Individuals	Researchers from IBM's X-Force discover a new variant of the infamous TrickBot malware repurposed to steal bitcoins.	Malware/
13/02/2018	?	US Taxpayers	The Internal Revenue Service warns taxpayers of a quickly growing scam involving erroneous tax refunds being deposited into their bank accounts.	Account
13/02/2018	?	City of Allentown	The city of Allentown is hit by the Emotet Trojan. The City believes that the cost of remediation is close to $1 million.	Malware/
13/02/2018	?	City of Savannah	The city of Savannah is in recovery mode after being hit by a malware attack when a city worker most likely opened a malicious email.	Malware/
14/02/2018	?	poorly secured Linux servers	According to researchers from GoSecure, attacks are launching SSH brute-force attacks on poorly secured Linux servers to deploy a backdoor dubbed Chaos backdoor	Brute-For
16/02/2018	?	Unnamed Russian Bank	The Russian Central Bank reveals that unknown hackers stole 339.5 million roubles ($6 million) from a Russian bank last year in an attack using the SWIFT international payments messaging system.	Unknown
16/02/2018	?	Snapchat Users	Details emerge on a phishing attack occurred on July 2017 able to score credentials for 50,000 Snapchat users.	Account
16/02/2018	rmsrf	Roomsurf	Roomsurf notifies his users of a data breach in which the attacker has been able to obtain usernames, phone numbers, and email addresses.	Unknown
16/02/2018	?	Davidson County	The Davidson County computers are hit by an unspecified ransomware.	Malware/
16/02/2018	?	Jemison Internal Medicine	Jemison Internal Medicine notifies 6,550 patients of a ransomware attack. However the investigation reveals that the systems had already been compromised.	Malware/
16/02/2018	?	Laufer Group International	Laufer Group International is the victim of a W-2 scam.	Account
16/02/2018	?	White and Bright Family Dental	White and Bright Family Dental notifies patients of a hack occurred on January 30 2018.	Unknown

Date	Author	Target	Description	
17/02/2018	?	Mac Users	Researchers from Digita Security warn users about the Coldroot remote access Trojan that is going undetected by AV engines since more than one year and targets MacOS computers.	Malware/
18/02/2018	?	India's City Union Bank	India's City Union Bank reveals that cyber criminals have been able to hack its systems and transfer nearly $2 million through three unauthorized remittances to lenders overseas via the SWIFT financial platform.	Unknown
18/02/2018	Flight Sim Labs (FSLabs)	Microsoft Flight Simulator Players	Mod developer Flight Sim Labs (FSLabs) has been accused of embedding malware in its flight simulation add-ons to steal pirates' Chrome passwords.	Malware/
19/02/2018	?	Blac Chyna	American model and entrepreneur Blac Chyna falls victim of The Fappening, having intimate content posted online.	Account
20/02/2018	?	Tesla	Researchers at security firm RedLock say hackers accessed one of Tesla's Amazon cloud accounts and used it to run currency-mining software. The breach started with a Kubernetes console left exposed.	Account
20/02/2018	APT37 AKA Reaper	Multiple Targets	Security Firm FireEye reveals the details of a lesser-known North Korean cyberespionage group targeting Korean Peninsula, Japan, Vietnam and the Middle East in 2017.	Targeted
20/02/2018	?	The Colorado Department of Transportation (CDOT)	CDOT is hit with a ransomware attack, attributed to SamSam, which forces the organization to shut down 2,000 computers.	Malware/
20/02/2018	?	Los Angeles Times	Troy Mursch, a security researcher at Bad Packets Report, finds cryptojacking code hidden (based on Coinhive) on the Los Angeles Times' interactive Homicide Report webpage.	Malicious
20/02/2018	?	HardwareZone (HWZ) Forum website	The HardwareZone (HWZ) Forum website is hacked and approximately 685,000 user profiles are affected. A senior moderator's account has been compromised by an unidentified hacker, and used to access the user profiles since September 2017.	Account
20/02/2018	APT28 AKA Fancy Bear	Multiple Targets in Middle East and Asia	Researchers from Kaspersky Lab publish a new report highlighting a shift in the activities of the infamous APT28 from Nato and	Targeted

Date	Author	Target	Description	
			Ukraine to Middle East and Central Asia.	
21/02/2018	?	Facebook Users	Researchers at Avast report a sophisticated campaign in which attackers use Facebook and Facebook messenger to trick users into installing a highly sophisticated Android spyware. The operation is dubbed Tempting Cedar.	Malware/
21/02/2018	?	SWIFT	IT security researchers at Comodo Labs discover a new phishing scam targeting SWIFT financial messaging service. The scam does not only aim at stealing banking credentials but also infects victims computers with the Adwind RAT.	Account
21/02/2018	Attackers of likely Nigerian origin	Multiple Fortune 500 companies	Researchers from IBM X-Force uncover an active Business Email Compromise campaign targeting multiple Fortune 500 companies.	Account
21/02/2018	?	IoT and networking equipment	Security researchers from Fortinet spot a new variant of the Mirai malware (dubbed Mirai OMG) that focuses on infecting IoT and networking equipment with the main purpose of turning these devices into a network of proxy servers used to relay malicious traffic.	Malware/
21/02/2018	?	University of Virginia Health System (uvahealth.com)	The University of Virginia Health System notifies almost 2,000 patients that their health records may have been exposed when an unauthorized third party implanted malware on a staffer's computer active between May 2015 and December 2016.	Malware/
21/02/2018	?	ASCD	ASCD is the victim of a W-2 scam.	Account
22/02/2018	?	The Los Angeles Philharmonic	The Los Angeles Philharmonic falls victim to a cyberattack that results in the theft of W-2 information for everyone that worked there in 2017. The security beach happened as the result of a "spear phishing" attack.	Account
22/02/2018	LulzSecITA	Matteo Salvini Blog	The Italian elections are approaching, so Hacktivists from the collective LulzSecITA hack the blog of Matteo Salvini, the leader of right-wind Italian party "La Lega" and dump 70,000 emails.	Unknown
22/02/2018	?	University of Alaska	Dozens of current and former employees and students of the University of Alaska are unable to access their Alaska.edu accounts.	Account

Date	Author	Target	Description	
			According to the investigation, user passwords have been changed by a third party.	
22/02/2018	?	Mobistealth	A hacker breaks into two consumer spyware companies, Mobistealth and Spy Master Pro and dumps a large cache of data.	Unknown
22/02/2018	?	Spy Master Pro	A hacker breaks into two consumer spyware companies, Mobistealth and Spy Master Pro and dumps a large cache of data.	Unknown
22/02/2018	?	Curtis Lumber	Curtis Lumber is the victim of a spear phishing attack	Account
22/02/2018	?	Punjab National Bank (PNB)	10,000 Credit Cards details from Punjab National Bank are leaked in the dark web.	Unknown
22/02/2018	?	Harper’s Magazine	Harper’s Magazine, the monthly longform journalism and essay publication, warns subscribers that their passwords may have been stolen by hackers.	Unknown
23/02/2018	?	About one dozen Connecticut government agencies	About one dozen Connecticut government agencies are hit with what one published report says is a WannaCry attack that knocks about 160 computers offline.	Malware/
23/02/2018	OilRig APT	An insurance agency and a financial institution in the Middle East	Researchers from Palo Alto Networks reveal that the Iran-linked OilRig APT group is now using a new Trojan called OopsIE in recent attacks against an insurance agency and a financial institution in the Middle East.	Targeted
23/02/2018	?	Chinese Websites	Researchers from Malwarebytes unveil the details of a drive-by attack targeting Chinese websites, and dropping an updated version of the Avzhan DDoS bot.	Malware/
23/02/2018	?	Children’s Aid Society of Oxford County Family and Children’s Services of Lanark, Leeds and Grenville	Two Ontario children’s aid societies are hit by Ransomware.	Malware/
24/02/2018	Anonymous	Matteo Salvini Facebook Page	And after the personal blog, hacktivists from Anonymous also deface Matteo Salvini's blog page.	Defacem
24/02/2018	?	Teesside University	Students at Teesside University are warned about a possible email security breach and urged to reset their university password.	Unknown
24/02/2018	?	Wallace Community College Selma	Personal and financial information of current and former employees of Wallace Community College Selma is leaked through a phishing scam.	Account
24/02/2018	?	Single Individuals	According to security researchers from Qihoo 360 Netlab, an advertising network is hiding in-	Malicious

Date	Author	Target	Description	
			browser cryptocurrency miners (cryptojacking scripts) in the ads it serves since December 2017.	
25/02/2018	?	Jorgie Porter	English actress and model Jorgie Porter is the latest victim of The Fappening hackers, who manage to steal her intimate pictures and videos and post them online.	Account
25/02/2018	Anonymous	Some Ohio State Websites	In name of #opUSA, hacktivists from the Anonymous collective take down some Ohio State websites.	DDoS
25/02/2018	?	Inland Revenue Department	Thousands of Inland Revenue files are locked up after New Zealand’s tax department becomes the target of a Cryptolocker attack in November.	Malware/
26/02/2018	Deep Panda	Some UK think tanks	Crowdstrike reveals that some UK think tanks specializing in international security were hacked by China-based group 'Deep Panda' beginning in April 2017.	Targeted
26/02/2018	?	Four British Schools	Hackers break into CCTV systems of at least four British schools and stream footage of pupils live on the internet.	Unknown
26/02/2018	?	Porsche Japan	The Japanese arm of Porsche says more than 28,000 email addresses have been leaked via a hack.	Unknown
26/02/2018	?	Vulnerable Oracle WebLogic Servers	Security researchers from Trend Micro uncover a new campaign, which involves hackers exploiting an Oracle server vulnerability (an Oracle WebLogic WLS-WSAT flaw CVE-2017-10271) to deliver two cryptominers: a 64-bit variant and a 32-bit variant of the XMRig Monero miner.	Malware/
26/02/2018	Hackers with connections to Iran	Unnamed Australian Universities	Australian universities have been targeted by hackers with connections to Iran in recent months, and "a number of investigations" are in progress, according to cybersecurity firm Crowdstrike.	Targeted
26/02/2018	?	Travel Corporation	Travel Corporation falls victim of a W-2 Scam.	Account
26/02/2018	?	U.S. Residents in 20 states	According to federal court documents, russian hackers operating in Colorado and 15 other states used data-mining viruses to steal thousands of credit card numbers from U.S. residents in 20 states and sold them on the darknet for more than	Malware/

Date	Author	Target	Description	
			$3.6 million.	
27/02/2018	?	Android Users	Security Firm Wandera reveals the details of RedDrop, a sophisticated strain of mobile malware targeting Android devices can extract sensitive data and audio recordings, run up premium SMS charges and then tries to extort money from victims.	Malware/
27/02/2018	?	Single Individuals	Researcher from cybersecurity firm Morphisec reveal the details of a new campaign carried on via spam messages delivering a malicious Word document. The document attempts to exploit an Adobe Flash Player bug (CVE-2018-4878) to let the attackers take control of the infected machines.	Malware/
27/02/2018	?	Wordpress, Joomla and CodeIgniter websites	Security researchers from SiteLock warn WordPress and Joomla admins of a sneaky new malware strain masquerading as legitimate ionCube files. The malware, dubbed ionCube Malware creates backdoors on vulnerable websites. The malware has been found on over 800 sites.	Malware/
27/02/2018	?	Tim Hortons	A computer virus is suspected of crashing cash registers at over 1,000 Tim Hortons coffee and donuts fast food restaurants.	Malware/
27/02/2018	?	FastHealth	FastHealth reveals that in mid-August 2017, an unauthorized party gained access to their web server and obtained patient data.	Unknown
28/02/2018	?	Financial Services Information Sharing and Analysis Center (FS-ISAC)	The Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry forum for sharing data about critical cybersecurity threats facing the banking and finance industries, reveals that a successful phishing attack on one of its employees was used to launch additional phishing attacks against FS-ISAC members.	Account
28/02/2018	APT28 AKA Fancy Bear	Various German government agencies	According to a report issued by the German news agency dpa, malicious actors from APT28 AKA Fancy Bear infiltrated several German government agencies for more than a year.	Targeted
28/02/2018	APT28 AKA Fancy Bear	Undisclosed North American and European foreign ministry agency	And nearly in contemporary, researchers from Palo Alto Networks reveal that the same attackers from APT28 targeted a North American and European	Targeted

Date	Author	Target	Description	
			foreign ministry agency.	
28/02/2018	?	GitHub	GitHub suvives the largest DDoS attack recorded (so far), reching a stunning 1.35 terabits/sec. leveraging memcached servers.	DDoS
28/02/2018	?	Undiclosed Brazilian public sector management school.	Researchers from Cisco Talos identify two different versions of a RAT, dubbed CannibalRAT, written entirely in Python, impacting users of a Brazilian public sector management school.	Targeted
28/02/2018	Chafer	Entities across the Middle East	Researchers from Symantec reveal the detalils of an Iranian hacking outfit, dubbed Chafer, previously focused on domestic surveillance, expanding its scope and cyber arsenal to target entities across the Middle East.	Targeted
28/02/2018	?	Single Individuals	Researchers from Malwarebytes reveal the details of a malvertising campaign using decoy websites pushing cryptocurrencies and to redirect users to the RIG exploit kit.	Malvertis
28/02/2018	?	rTorrent Client users	Researchers from F5 detect an attack actively exploiting the rTorrent client through a previously undisclosed misconfiguration vulnerability on XML-RPC for deploying a Monero (XMR) crypto-miner operation.	Malware/
28/02/2018	?	Single Individuals	A bulk breach dump is discovered totaling over 3.4 billion credentials.	Unknown
01/03/2018	?	NIS America	Japanese gaming developer Nippon Ichi Software reveals that its American arm, NIS America, has suffered a major data breach compromising the personal and financial data of online customers. The breach, due to malware implanted in the checkout page, took place sometime between 23 January and 26 February.	Malware/
01/03/2018	?	FS-ISAC	The Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry forum for sharing data about critical cybersecurity threats facing the banking and finance industries, reveals that a successful phishing attack on one of its employees was used to launch additional phishing attacks against FS-ISAC members.	Account
01/03/2018	?	Hope Hicks	Hope Hicks tells the House Intelligence Committee that one of her email accounts was hacked,	Account

Date	Author	Target	Description	
			according to people who were present for her testimony in the panel's Russia probe.	
01/03/2018	?	ASI Constructors, Inc.	ASI Constructors, Inc. reveals to have suffered a phishing attack targeting employees' 2017 W-2 forms. The attack occurred on January 31, 2018.	Account
01/03/2018	?	Greyhealth Group	Greyhealth Group reveals to have suffered a phishing attack compromising the personal information of 683 individuals.	Account
01/03/2018	?	Scottsboro City Board of Education	The Payroll Department of the Scottsboro City Board of Education falls victim of a phishing scam. The attackers requested W-2 information from all employees.	Account
01/03/2018	?	Rockdale Independent School District	An email phishing scheme causes several Rockdale ISD employees' taxes to be falsely filed and compromises confidential tax information for all employees.	Account
01/03/2018	?	b-tor[.]ru Users	Researchers from Palo Alto Networks discover a Russian BitTorrent Site distributing a Monero Miner.	Malware/
01/03/2018	?	Colorado Department of Transportation (CDOT)	For the second time in two weeks, the computers at the Colorado Department of Transportation Agency shut down 2,000 computers after a ransomware infection.	Malware/
01/03/2018	?	Primary Health Care	Primary Health Care notifies patients after discovering hack of employee email accounts.	Account
02/03/2018	?	Android Phone Buyers	Security Firm Dr.Web publishes a list of 42 Android phones sold already infected with the Triada banking trojan.	Malware/
02/03/2018	?	160 Applebee’s Restaurants	RMH Franchise Holdings reveals that PoS systems at the Applebee’s network of restaurants were infected with a PoS malware. 160 restaurants are affected. The breach was discovered on February 13, and took place between November 23, 2017, and January 2, 2018.	Malware/
02/03/2018	?	Humanitarian Aid Groups	McAfee uncovers Operation Honeybee, a malicious document campaign targeting Humanitarian Aid Groups, using North Korean political topics as bait.	Targeted
02/03/2018	?	St. Peter's Surgery & Endoscopy Center	St. Peter's Surgery & Endoscopy Center reveal that hackers potentially compromised medical records of about 135,000 patients	Malware/

Date	Author	Target	Description	
			earlier this year.	
04/03/2018		Peter Andre and wife Emily MacDonagh	The intimate photos of singer Peter Andre and wife Emily MacDonagh have reportedly been stolen and published online as part of a new episode from the Fappening saga.	Account
05/03/2018	?	Unidentified US Service Provider	Few days after GitHub suffered a massive 1.3 Tbps DDoS attack, Arbor Networks unveil the details of a new record DDoS attack that clocked at 1.7 Tbps. The attack was aimed at a yet-to-be-identified "US service provider."	DDoS
05/03/2018	?	Single Individuals	Researchers from Palo Alto Networks and Proofpoint discover a new malware, dubbed Combojack, that steals cryptocurrency and other electronic funds by surreptitiously modifying wallet or payment information whenever victims copy it to their devices' clipboards.	Malware/
05/03/2018	?	Single Individuals	A new report from Kaspersky Lab reveals that one cryptomining gang tracked by researchers over the past six months minted $7 million with the help of 10,000 computers infected with mining malware.	Malware/
05/03/2018	?	ABC Bus Companies, Inc.	An employee falls victim of a phising email and delivers to the attacker the personal information of ABC employees.	Account
06/03/2018	?	Single Individuals	Researchers from Cisco Talos reveal a surge of campaigns distributing the Gozi ISFB financial malware.	Malware/
06/03/2018	?	Flexible Benefit Service Corporation	Flexible Benefit Service Corporation notifies 5,123 of a phishing incident occurred on February 16.	Account
07/03/2018	?	Binance	A large scale phishing campaign causes a massive unauthorized cryptocurrency sell-off activity for the users of Binance, a Chinese cryptocurrency trader.	Account
07/03/2018	?	Individuals in Russia, Turkey and Ukraine	Microsoft says to have discovered and stopped a large attack that attempted to use variants of the Dofoil, or Smoke Loader, trojan to spread a cryptocurrency miner. In total more than 400,000 instances were recorded: 73 percent, hitting Russians with Turkey,18 percent, and the Ukraine 4 percent being the other main targets. The attack was carried on via an update server that replaced a BitTorrent	Malware/

Date	Author	Target	Description	
			client called MediaGet with a near-identical but back-doored binary.	
07/03/2018	?	Pinelands Regional School District	The Pinelands Regional School District is hit by the Emotet malware.	Malware/
08/03/2018	?	Italian Ministry of Education	The Italian branch of the Anonymous collective leaks from the Italian Ministry of Education, 26,000 emails of teachers belonging to all level of schools. They also leak 200 administrative staff addresses.	Unknown
08/03/2018	Hidden Cobra	Several Financial Turkish Institutions	Researchers from McAfee reveal that the reputed state-sponsored North Korean hacking group Hidden Cobra has once again been fingered in a malware attack against financial organizations, this time apparently targeting Turkish institutions in a spear phishing campaign in early March, leveraging CVE-2018-4878.	Targeted
08/03/2018	?	Misconfigured Redis servers, and Windows servers vulnerable to the EternalBlue NSA exploit.	Researchers from Imperva reveal a new unusually sophisticated cryptojacking attack attempting to install cryptominers on both database and application servers by targeting misconfigured Redis servers, as well as Windows servers that are susceptible to the EternalBlue NSA exploit. The Campaign is dubbed RedisWannaMine.	Malware/
08/03/2018	?	Dutch women's handball team	According to local reports in the Netherlands, hackers manage to breach the surveillance camera system in a dressing room of a sauna hosting the women handball team, and post the recordings on adult websites last December.	Unknown
08/03/2018	?	Former Tennessee Gov. Phil Bredesen's Senate campaign	Former Tennessee Gov. Phil Bredesen's Senate campaign tells the FBI in a letter that it fears it was hacked.	Unknown
09/03/2018	Slingshot APT	Targets in the Middle East and Africa	Kaspersky Lab reveal the details of Slingshot, an extremely sophisticated cyber espionage campaign, leveraging malware to spy on international targets for six years. The APT group exploited zero-day vulnerabilities (CVE-2007-5633; CVE-2010-1592, CVE-2009-0824) in routers used by the Latvian network hardware provider Mikrotik.	Targeted
09/03/2018	Turkish Government	Turkish Nationals	Security researchers from Citizen Lab publish a report where they reveal how deep packet inspection	Malware/

Date	Author	Target	Description	
			middleboxes are being used either to expose Turkish nationals to nation-state spyware or to redirect Egyptian Internet users to ads and browser cryptocurrency.	
09/03/2018	?	14 unnamed countries	ESET researchers reveal to have discovered a new version of the infamous Hacking Team surveillance tool, dubbed RCS (Remote Control System), active in 14 countries.	Malware/
09/03/2018	?	Multiple Industries	Researchers at Kroll Cyber Security reveal the details of a new family of point-of-sale malware, dubbed PinkKite, very tiny in size, potentially devastating for POS endpoints.	Malware/
09/03/2018	APT15	UK government contractor	Researchers at NCC Group reveal to have discovered multiple backdoors on a UK government contractor's computer designed to steal sensitive government and military data. The hack is tied to China-linked cyber espionage group APT15. According to researchers, the attackers were able to deploy three backdoors – identified as RoyalCli, RoyalDNS and BS2005. The networks were compromised from May 2016 until late 2017 and infected over 30 contractor controlled hosts.	Targeted
09/03/2018	APT28 AKA Fancy Bear AKA Sofacy	Far East Targets	Researchers at Kaspersky Lab reveal a new analysis on the infamous APT28 indicating that the group is shifting its interest to Far East Targets	Targeted
09/03/2018	?	Single Individuals	Researchers from Proofpoint reveal the details of a remote access tool dubbed FlawedAmmyy, developed using the leaked source code of Ammyy Admin, a legitimate remote desktop software.	Malware/
09/03/2018	?	Unpatched Apache Solr Servers	Researchers from the ISC SANS discover a campaign targeting Apache Solr servers that hadn't received patches for the CVE-2017-12629 vulnerability. The campaign is aimed to install miners.	Malware/
09/03/2018	$2a$45	Florida Virtual Learning School (FVLS)	Florida Virtual Learning School notifies 368,000 current and former students, after an individual with the moniker $2a $45 uploads information of 35,000 students on a forum. Leon County Schools is among the affected organizations.	Unknown

Date	Author	Target	Description	
09/03/2018	herbapproach@protonmail.com	JJ Meds	JJ Meds, a medical marijuana delivery service in Canada, goes offline after having received an extortion demand.	Unknown
10/03/2018	?	National Rifle Association (NRA)	According to a report released by Netlab, three different National Rifle Association (NRA) websites experienced Distributed Denial of Service (DDoS) attacks.	DDoS
10/03/2018	?	Mississippi Valley State University	Mississippi Valley State University's campus was temporary without internet service this week after university officials said the school was hit by a SamSam ransomware attack.	Malware/
12/03/2018	MuddyWater AKA TEMP.Zagros	Targets in Turkey, Pakistan and Tajikistan	Researchers from Palo Alto Networks and FireEye reveal that the Iran-Linked MuddyWater campaign (AKA TEMP.Zagros) appears to be still active against targets in Turkey, Pakistan and Tajikistan.	Targeted
12/03/2018	?	ATI Physical Therapy	ATI Physical Therapy notifies patients of a security incident that appears to have targeted employees' email accounts.	Account
12/03/2018	?	Okaloosa Water and Sewer	Okaloosa Water and Sewer warns its users of a security breach involving external vendors which process electronic credit/debit card payments for water and sewer bills.	Unknown
13/03/2018	OceanLotus APT aka APT32 aka APT-C-00	Targets in East Asian countries such as Vietnam, the Philippines, Laos and Cambodia	Researchers from ESET reveal that the suspected Vietnamese APT group OceanLotus has added a new backdoor to its repertoire of malicious tools – one that includes capabilities for enabling file, registry and process manipulation, and also downloading more malicious files.	Targeted
13/03/2018	?	Uyghurs	Researchers from Palo Alto Networks reveal the details of a new Android malware family dubbed "HenBox", targeting the Uyghurs, a minority Turkic ethnic group living in China.	Malware/
13/03/2018	?	Multiple Targets	Researchers from Imperva identify a new but unusually distributed Monero cryptominer scam campaign hidden in a picture of Scarlett Johansson.	Malware/
13/03/2018	?	Single Individuals	Researchers from AVAST reveal the details of a campaign where Criminals hosted their cryptominers in forked projects on GitHub.	Malware/
13/03/2018	?	Port of Longview	The Port of Longview is hit by a	Unknown

Date	Author	Target	Description	
			cyber attack that may have affected hundreds of past and current employees and dozens of vendors.	
13/03/2018	?	Gwent Police	Gwent Police is being investigated after failing to inform up to 450 people that hackers may have accessed their confidential reports to the force.	Unknown
14/03/2018	?	Fortnite	Several news reports surface of the suspected hacking of player accounts of popular video game Fortnite, with some gamers apparently faced with large credit card charges from fraudulent purchases.	Account
14/03/2018	?	Visitors of download.cnet.com	ESET researchers discover three trojanized applications (bitcoin stealing malware) hosted on download.cnet.com, the163th most visited site in the world according to Alexa rankings. The researchers estimate that as of March 13, the attacker managed to steal the equivalent of $80,000 USD. The malware had been hosted since May 2, 2016 and had been downloaded more than 4,500 times in total.	Malware/
14/03/2018	?	Android Users	Researchers from Check Point reveal the details of RottenSys, a massive botnet composed of 5 million Android smartphones, active primarily in China.	Malware/
14/03/2018	?	Multiple Targets	Researchers from Forcepoint publish a detailed analysis of the Qrypter Remote Access Tool. The analysis reveals that 243 organizations worldwide have been hit by the RAT.	Malware/
14/03/2018	?	Queensland Transport Department	ABC News reveals that overseas hackers breached the Queensland Transport Department's security network last year, before attempting to steal information from staff members from other sections of government.	Unknown
15/03/2018	Dragonfly	West's energy utilities and other critical infrastructures	The US Department of Homeland Security and the Federal Bureau of Investigation issued an alert warning of ongoing cyber-attacks against the West's energy utilities and other critical infrastructures by individuals acting on behalf of the Russian government. The report points the finger at the Dragonfly group.	Targeted
15/03/2018	APT28 AKA Fancy Bear AKA Sofacy	Unnamed European Government	Researchers from Palo Alto Networks reveal a new campaign	Targeted

Date	Author	Target	Description	
			carried on by the infamous APT28 (AKA Fancy Bear AKA Sofacy) targeting an unnamed European Government, exploiting an updated version of DealersChoice, a platform that exploits a Flash vulnerability to stealthily deliver a malicious payload of trojan malware.	
15/03/2018	?	Meghan Markle	The Fappening saga continues with new photo leaks published online. The most recent victim is none other than Meghan Markle, the soon-to-be Mrs. Prince Harry. Some believe ISIS could be involved in the hack, even if no official claim is made.	Account
15/03/2018	?	Single Individuals in South Korea	Researchers from Symantec reveal the details of a new version of the infamous FakeBank trojan distributed via malicious Android apps in South Korea.	Malware/
15/03/2018	?	Unnamed Petrochemical Company in Saudi Arabia	The New York Times reveals that back in August, a petrochemical company with a plant in Saudi Arabia was hit by a cyberattack aimed to sabotage the firm's operations and trigger an explosion.	Targeted
15/03/2018	?	Single Individuals	Security researchers from Kaspersky reveal that the PoS Malware Prilex has now evolved into a comprehensive tool suite that lets cybercriminals steal chip and PIN card data and create their own functioning, fraudulent plastic cards.	Malware/
15/03/2018	?	Nampa School District	The Nampa School District informed its employees of a potential security issue involving personally identifiable information of about 3,983 of its current and past employees.	Unknown
15/03/2018	?	Svitzer	The shipping company Svitzer suffers a significant data breach affecting almost half its Australian employees when three employees have had emails auto-forwarded in the past 11 months.	Account
16/03/2018	TEMP.Periscope AKA Leviathan	U.S. Maritime Entities	Security firm FireEye reveals the details of TEMP.Periscope, a Chinese group focused on U.S. maritime entities that were either linked to -- or have clients operating in -- the South China Sea.	Targeted
16/03/2018	?	UK National Lottery	The UK National Lottery advises all 10.5million people with online accounts to change their	Brute For

Date	Author	Target	Description	
			passwords following an attempt by hackers to access accounts using credential stuffing.	
16/03/2018	?	Atrium Hospitality	Atrium Hospitality notifies 376 hotel guests of a ransomware attack occurred on December 2017.	Malware/
16/03/2018	?	Frost Bank	Frost Bank investigates a breach after the company discovered unauthorized access to digital images stored in those customers' commercial image archives.	Unknown
16/03/2018	?	TheDarkOverlord	TheDarkOverlord claims to have breached H-E Parts Morgan. The breach seems to have occurred in November.	Unknown
18/03/2018	?	Russian Central Election Commission	The Russian Central Election Commission is hit by a DDoS attack.	DDoS
20/03/2018	?	Orbitz	Orbitz, a subsidiary of online travel agency Expedia Inc reveals that hackers may have accessed personal information from about 880,000 payment cards. The breach may have occurred between Jan. 1, 2016 and Dec. 22, 2017 for its partner platform and between Jan. 1, 2016 and June 22, 2016 for its consumer platform.	Unknown
20/03/2018	?	David Nott	David Nott, a British surgeon who helped carry out operations in Aleppo, reveals that the hacking of his computer could have led to a hospital being bombed by suspected Russian warplanes.	Targeted
20/03/2018	?	Puerto Rico's Power Utility, PREPA	Puerto Rico's Power Utility, PREPA reveals to have been hacked over the weekend, but customer information was not compromised.	Unknown
20/03/2018	?	Trusted Quid	Trusted Quid reports a theft of data from unauthorised access to its website. The incident relates to data directly entered by people applying for a loan only on the Trusted Quid website between 1 July 2016 and 17 February 2018. Up to 65,925 people may have been affected.	Unknown
20/03/2018	?	Finger Lakes Health	Finger Lakes Health is functioning the old-fashioned way while its computer system remains locked up by an unspecified type of ransomware.	Malware/
21/03/2018	?	Uttar Haryana Bijli Vitran	Uttar Haryana Bijli Vitran Nigam	Malware/

Date	Author	Target	Description	
		Nigam Limited (UHBVNL)	Limited (UHBVNL), a power distribution company suffers a cyber attack on its Automatic Meter Reading System (AMR) in which billing data of about 4,000 industrial consumers are encrypted. The attackers demand a ransomware equivalent to $150,000.	
21/03/2018	?	Vulnerable Cacti Servers	Researchers from Trend Micro reveal that a hacker group has made nearly $75,000 by installing a Monero miner on Linux servers after exploiting a five-year-old vulnerability in the Cacti "Network Weathermap" plugin (CVE-2013-2618). The researchers believe this is the same group that recently exploited CVE-2017-1000353 to inject Monero miners into vulnerable Jenikins installations.	Malware/
21/03/2018	?	SIngle Individuals	Researchers from security firm Webroot reveal the details of a new variant of the well-known Trickbot financial trojan.	Malware/
21/03/2018	OilRig APT	A number of organizations across the Middle East	According to a new analysis by security firm Nyotron, the Iran-linked OilRig APT is back with a new more advanced malware toolkit.	Targeted
22/03/2018	?	Russian Defense Ministry	The Russian Defense Ministry reveals that a total of 7 DDoS attacks are carried out against its website during the final vote of the general elections.	DDoS
22/03/2018	?	City of Atlanta	IT systems used by the City of Atlanta, are hit by a SamSam ransomware attack, cutting off some online city services and potentially putting the personal information of employees and citizens at risk.	Malware/
22/03/2018	?	Android Users	Researchers from SophosLabs reveal the details of Andr/HiddnAd-AJ, a malicious app in disguise of an Ad blocker, downloaded more than 500,000 times before being pulled off the Google Play Store.	Malware/
22/03/2018	?	Some Government Agencies	Researchers from FireEye discover a new spear phishing campaign targeting government agencies with an evolved version of Sanny malware, a five-year-old information-stealer that now features a multi-stage infection process, whereby each stage is downloaded from the attacker's	Targeted

Date	Author	Target	Description	
			server.	
24/03/2018	?	Baltimore's Automated Dispatch System.	Unknown actors temporarily cause a shutdown of Baltimore's automated dispatch system, impacting the messaging functions within the Computer Aided Dispatch (CAD) system used by both of the city's 911 and 311 services.	Unknown
26/03/2018	APT28 AKA Fancy Bear	UK Anti-Doping Agency	The UK Anti-Doping Agency revels to have foiled an attempted cyberattack during the weekend that tried to access confidential medical and drug testingdata.	Targeted
26/03/2018	?	Vulnerable Linux-based systems	Researchers from Cisco Talos reveal the details of GoScanSSH, a new strain of malware that targets vulnerable Linux-based systems, avoiding government and military networks.	Malware/
27/03/2018	Alleged Nigerian Hackers	Naukri.com	Nigerian hackers hack into Naukri.com's servers, stealing 100,000 resumes and contacting 10,000 job seekers for fake interviews.	Unknown
27/03/2018	?	Stormont (Northern Ireland Parliament)	Stormont (the Northern Irish Parliament)issues a warning to all staff, including political parties, after discovering its email service was hit by a cyber attack.	Targeted
27/03/2018	?	YouTube Users	Researchers at Russian anti-virus vendor Dr. Web discover a dangerous malware campaign spread by cybercriminals from comments posted on YouTube. The malware is dubbed Trojan.PWS.Stealer.23012.	Malware/
28/03/2018	?	Android Users	Researchers from Trend Micro discover HiddenMiner, a new type of Android malware that infects devices and untetheredly mines Monero in the phone's background until the battery is exhausted or the device gives out.	Malware/
28/03/2018	?	Boeing	A Boeing facility in South Carolina is hit by the Wannacry ransomware.	Malware/
28/03/2018	?	Vulnerable MicroTik devices	Another IoT Botnet: a new Hajime variant infects MicroTik devices vulnerable to an exploit known as "Chimay Red".	Malware/
28/03/2018	?	Single Individuals	Researchers from security company Cybereason reveal the details of "Fauxpersky", a simple and efficient keylogger impersonating the Russian antivirus software Kaspersky.	Malware/
28/03/2018	?	S.S. Lazio	Italian newspaper "Il Tempo"	Account

Date	Author	Target	Description	
			reports that Italian football team Lazio have fallen for an email scam and paid £1.75m (€2m) of the final instalment for defender Stefan de Vrij's transfer from Dutch club Feyenoord to fraudsters.	
28/03/2018	?	Indian Bank Customers	A complaint reveals that 1,020 bank accounts in different banks were used by fraudsters to receive money from victim's bank accounts through phishing.	Account
29/03/2018	?	Under Armour	Under Armour, Inc. announces that it is notifying users of MyFitnessPal - the company's food and nutrition application and website, about a data security issue. On March 25, the MyFitnessPal team became aware that an unauthorized party acquired data associated with MyFitnessPal user accounts in late February 2018. The company investigation reveals that approximately 150 million user accounts were affected by this issue.	Unknown
29/03/2018	?	Bank Negara Malaysia	Bank Negara Malaysia reveals to have foiled cyberattack in which fraudulent messages to transfer funds were sent on the SWIFT transactions platform.	Unknown
29/03/2018	?	Unnamed Bestiality Website	Thousands of user account details—many related to a bestiality website—are circulating on public image boards, according to data obtained by Motherboard.	Unknown
30/03/2018	?	CareFirst BlueCross BlueShield	A phishing email attack on Baltimore-based CareFirst BlueCross BlueShield may have comprised nearly 6,800 members' personal data. The insurer learned on March 12 that one of its employees fell victim to a phishing email that compromised his or her email account. The hacker used the email account to send spam messages to an email list of individuals not associated with CareFirst.	Account
01/04/2018	?	Guardian Pharmacy of Jacksonville	Guardian Pharmacy of Jacksonville notifies 11,521 patients of email compromise of protected health information.	Account
01/04/2018	JokerStash AKA Fin7 AKA Carbanak	Hudson's Bay Company	Retailer Hudson's Bay Company discloses that it was the victim of a security breach that compromised data on payment cards used at Saks and Lord &	Unknown

Date	Author	Target	Description	
			Taylor stores in North America. Millions of cards may have been compromised (5 millions are already offered for sale).	
02/04/2018	?	Four U.S. pipeline companies (Oneok Inc, Energy Transfer Partners LP, Boardwalk Pipeline Partners LP, Eastern Shore Natural Gas)	At least four U.S. pipeline companies have seen their electronic systems for communicating with customers shut down, with three confirming it resulted from a cyberattack to Latitude Technology, a third-party provider. It is not clear is the outage is the result of a ransomware or DDoS attack.	Unknown
02/04/2018	?	1,000 Magento Sites	Security researchers from FlashPoint say they've identified at last 1,000 Magento sites that have been hacked by cybercriminals and infected with malicious scripts that steal payment card details, perform cryptojacking, or redirect the visitors to malware distribution sites.	Brute-For
02/04/2018	?	Android Users	Researchers from Trustlook reveal the details of a new strain of Android malware specifically aimed at stealing private conversations on IM applications like Facebook Messenger, Skype, Telegram, Twitter, Viber, and others.	Malware/
02/04/2018	?	Government of Sint Maarten	The entire government of Sint Maarten, an independent country within the Kingdom of the Netherlands, is taken down for a week by a cyber attack.	Unknown
03/04/2018	?	Vadim Lavrusik Twitter and Flipboard accounts	Less than an hour after tweeting about being safe during the active shooting at YouTube's headquarters, the Twitter and Flipboard accounts of Vadim Lavrusik, a product manager at Youtube, are hit by hackers.	Account
03/04/2018	Dark-Coder or Th3Falcon.	More than a dozen major Israeli websites	In name of OpIsrael, more than a dozen major Israeli websites, belonging to hospitals, local authorities, the Israeli Opera, Israel Teachers Union and the IDF Widows and Orphans Organization are defaced apparently in response to clashes between the IDF and Gazan protesters the previous weekend.	Defacem
03/04/2018	Lazarus AKA Hidden Cobra	Online Casino in Central America	Researchers from ESET reveal that the infamous Lazarus Group, a malicious actor linked to North Korea, has used a new toolset, including the destructive KillDisk,	Targeted

Date	Author	Target	Description	
			to target the network of an online Casino in Central America.	
04/04/2018	APT32 AKA OceanLotus	Multiple Targets	Researchers from Trend Micro reveal the details of a new backdoor affecting MacOS linked to the OceanLotus threat group. The backdoor is called OSX_OCEANLOTUS.D.	Targeted
04/04/2018	?	Single Individuals	Researchers from Trend Micro discover a campaign aimed to inject the widely-used Coinhive code into an ad supplied by the AOL advertising network, in order to mine crypto currency.	Malicious
04/04/2018	?	Verge Cryptocurrency	An unknown attacker has exploited a bug in the Verge cryptocurrency network code to mine Verge coins at a very rapid pace	Unknown
04/04/2018	?	Facebook Users	Facebook reveals that "malicious actors" took advantage of search tools on its platform, making it possible for them to discover the identities and collect information on most of its 2 billion users worldwide.	Vulnerab
04/04/2018	?	Japan Ministry Employees	The Japanese government's cybersecurity center reveals that the email addresses and passwords of thousands of ministry employees have been leaked and are being sold on the Internet.	Unknown
04/04/2018	?	Oakton High School	A police investigation reveals that hackers attempted to change grades at Oakton High School, using an attack carried on via a malicious email.	Account
05/04/2018	?	[24]7.ai	[24]7.ai, a firm providing online customer support services based on artificial intelligence and machine learning, is breached. As consequence other companies using its services suffer a theft of customer payment information. The breach occurred between September 26, 2017 and October 12, 2017. The list of the victims include Sears, Kmart, and Delta Airlines. Even Best Buy is involved.	Unknown
05/04/2018	?	Several Financial Firms	Researchers from Recorded Future reveal the details of the IoTroop botnet, a botnet made up of hijacked internet-connected televisions and web cameras used to target financial firms with DDoS attacks.	DDoS
05/04/2018	?	Multiple Financial Targets	Researchers from Netskope	Malware/

Date	Author	Target	Description	
			discover a new ATM jackpotting malware dubbed ATMJackpot. The malware seems to have originated from Hong Kong and to be still in development.	
05/04/2018	?	Multiple Targets	Researchers from Fortinet discover a new variant of the Agent Tesla spyware, spreading via weaponized Microsoft Word Documents.	Malware/
06/04/2018	Suspected Chinese Hackers	India's Ministry of Defence	The website of India's Ministry of Defence is defaced by suspected Chinese attackers.	Defacem
08/04/2018	?	Drake Bell	Drake Bell appears to be the most recent victim of hackers as part of another episode of the Fappening saga.	Account
08/04/2018	?	Natalie Cassidy	EastEnders star Natalie Cassidy is the latest celebrity to have her intimate pictures leaked online in yet another evolution of the Fappening 2018 scandal.	Account
09/04/2018	JHT	Cisco switches around the world	The Iranian IT Ministry reveals that Hackers have attacked networks in a number of countries including data centers in Iran where they left the image of a U.S. flag on screens along with a warning: “Don’t mess with our elections”. The attack, exploiting CVE-2018-0171, affected 200,000 router switches across the world in a widespread attack, including 3,500 switches in Iran.	Vulnerab
09/04/2018	?	Armed Forces Recreation Center Edelweiss Lodge and Resort	The Armed Forces Recreation Center Edelweiss Lodge and Resort investigates a data breach that left some guests open to identity theft. At least 18 guests — primarily soldiers and retirees — who stayed at the resort between November 2017 and February 2018 reported that their credit cards were misused after their stays.	Malware/
09/04/2018	?	Sodexo Filmology	Sodexo food services and facilities management company notifies a number of customers that it was the victim of a targeted attack on its cinema vouchers platform Sodexo Filmology.	Targeted
09/04/2018	?	Telco companies in Brazil, Columbia and other Latin American countries	Researchers from Flashpoint observe a spike of activity in Telegram messaging channels being used to exchange HTTP injectors. HTTP injectors can be used to obtain free mobile internet	HTTP Inj

Date	Author	Target	Description	
			access.	
10/04/2018	?	Vulnerable CMS Systems.	Security researchers at Malwarebytes report to have uncovered evidence of a sophisticated campaign of thousands of compromised websites running vulnerable CMS' and abused to distribute malware to visiting users via fake updates. The campaign is called FakeUpdates and is used to distribute the ZeusVM variant Chtonic banking malware or a NetSupport Remote Access Tool	Malicious
10/04/2018	Kuroi'SH and Prosox	Vevo Youtube Account	Two hackers manage to deface several popular YouTube music videos, changing titles and thumbnail images. The list of the victims include the most-viewed YouTube video of all time, "Despacito". The two claim to have done it for Palestine.	Defacem
10/04/2018	?	Single Individuals	Researchers from Barracuda reveal the details of a recent spate of attacks using phishing, social engineering, exploits, and obfuscation to spread a Quant Loader trojan capable of distributing ransomware and password stealers. The attack uses a ".url" file extension claiming to be billing documents but actually lead to remote script files using a variation of CVE-2016-3353	Malware/
10/04/2018	?	Victoria Independent School District	Victoria independent School District notifies employees that some email accounts were inappropriately accessed between July and October 2017. Some of the emails in those accounts contained employees' personal information.	Account
11/04/2018	?	Great Western Railway	Great Western Railway reset more than a million customer accounts after discovering hackers had successfully breached a small percentage of them. According to the operator, about 1,000 of its passengers' details have been exposed.	Brute-For
12/04/2018	UK	Islamic State	The director of the intelligence agency GCHQ, Jeremy Fleming reveals that the UK has conducted a "major offensive cyber-campaign" against the Islamic State group.	DDoS
12/04/2018	?	Governments and high-level officials in the Middle East	Kaspersky Labs details a large-scale nation-state backed	Targeted

Date	Author	Target	Description	
		and North Africa (MENA)	malware campaign called Operation Parliament that is targeting governments and high-level officials in the Middle East and North Africa (MENA) regions and more specifically Palestine.	
12/04/2018	?	Single Individuals	Researchers from Menlo Security reveal the details of a new multi-stage campaign using malicious attachments to infect the endpoint with content hosted on a remote host (and exploiting CVE-2017-8570 to drop the executable in the endpoint), The campaign is used to deliver the Formbook malware.	Malware/
12/04/2018	?	Sucuri	The California based website security provider Sucuri suffers a series of massive DDoS attacks causing service outage in West Europe, South America and parts of Eastern United States.	DDoS
12/04/2018	?	Coinsecure	Cryptocurrency exchange Coinsecure, India's second exchange, announces that it has suffered a severe issue, 438 bitcoin, $3,3 million worth, have been transferred from the main wallet to an account that is not under their control.	Vulnerab
13/04/2018	?	Diagnostic Radiology & Imaging	Diagnostic Radiology & Imaging notifies 800 patients of phishing incident occurred in November 2017.	Account
13/04/2018	?	Vulnerable Drupal CMS Systems	After the publication of PoC code, attackers start to exploit the Drupalgeddon2 vulnerability (CVE-2018-7600).	Vulnerab
13/04/2018	?	Vulnerable routers	Security researchers at Akamai discover a proxy botnet composed of more than 65,000 routers exposed to the Internet via the Universal Plug and Play (UPnP) protocol.	Vulnerab
13/04/2018	?	Inogen	Inogen, a California-based medical device manufacturer, reports that 30,000 former and current customers may have had their personal information exposed when a company employee's email account was compromised sometime between Jan. 2, 2018, and Mar. 14, 2018.	Account
13/04/2018	?	Mise En Place Restaurant Services	Mise En Place Restaurant Services announces that it was subject to a ransomware attack, which may have potentially exposed some information of clients and individuals.	Malware/

Date	Author	Target	Description	
14/04/2018	?	Texas Health Resources	Texas Health Resources reveals that an unauthorized party may have gained access to patient information back in October 2017 by compromising some of the organization's email accounts. The breach was discovered in January 4,000 and might impact 4,000 users.	Account
15/04/2018	?	UnityPoint Health	UnityPoint Health notifies patients of a phishing attack occurred between November 1, 2017 and February 7, 2018	Account
04/04/2018	?	Single Individuals	Researchers from Palo Alto Networks reveal the details of Rarog, a previously unseen cryptomining trojan.	Malware/
12/04/2018	?	IIS 6.0 Vulnerable servers	Researchers from F5 discover a massive campaign exploiting an old IIS 6.0 vulnerability (CVE-2017-7269) to mine Electroneum.	Vulnerab
16/04/2018	Russian state-sponsored actors (Grizzly Steppe)	Government and private-sector organizations, critical infrastructure providers, and the internet service providers (ISPs)	The UK NCSC (National Cyber Security Centre), FBI (Federal Bureau of Investigation) and DHS (Department of Homeland Security) issue a joint Technical Alert about malicious cyber activity carried out by the Russian Government. The attackers use compromised routers to conduct man-in-the-middle attacks.	Man-in-th
16/04/2018	APT-C-32	Middle Eastern Individuals	Researchers from Lookout reveal the details of an espionage campaign using two malware strains called Desert Scorpion and FrozenCell, to spy on targets in Palestine. The attackers are thought to be linked to Hamas.	Targeted
16/04/2018	mobile APT (mAPT)	Several targets	Researchers from Lookout reveal a new campaign using a modified version of the infamous ViperRAT hosted in Google Play.	Targeted
16/04/2018	?	TaskRabbit	TaskRabbit, a web-based service owned by IKEA that connects freelance handymen with clients in various local US markets, emails customers admitting it suffered a security breach. The company takes down its app and website while investigating the incident and later admits that some personal information might have been compromised.	Unknown
16/04/2018	?	Android Users	Researchers from Kaspersky Lab reveal the detail of Roaming Mantis, an operation where malware authors have hijacked DNS settings on vulnerable	DNS Hija

Date	Author	Target	Description	
			routers to redirect users to sites hosting Android malware on clone apps of Google Chrome and Facebook.	
16/04/2018	?	Multiple Targets	According to multiple sources, hackers have started to actively exploit the Drupalgeddon 2 Drupal CMS vulnerability CVE-2018-7600 to inject cryptominers.	Vulnerab
16/04/2018	?	African Embassy in Dublin	Researchers from Lastline reveal that an African ambassador in Dublin was compromised by cyber criminals with hackers gaining access to entire nation's digital data.	Targeted
16/04/2018	?	Hong Kong Broadband Network	Hong Kong Broadband Network, the city's second largest fixed-line residential broadband provider, discovers that an inactive customer database has been accessed without authorization. The personal data of some 380,000 customers, including details for more than 40,000 credit cards, are compromised.	Unknown
16/04/2018	?	Irvington School District	Partial social security numbers of more than 1,200 employees at Irvington schools are distributed via email to an unknown number of recipients by an unidentified attacker.	Unknown
17/04/2018	?	Chrome Users	Researchers from AdGuard uncover five malicious ad-blocker extensions on the Chrome Web Store that were installed by 20 million Chrome users before Google removed them.	Malware/
17/04/2018	?	TheBottle	Researchers from Palo Alto Networks reveal the details of SquirtDanger, a new strain of malware that allows hackers to take action screenshots, steal passwords, download files and even steal the contents of cryptocurrency wallets.	Malware/
17/04/2018	?	Minecraft users	According to Avast's Threat Labs, nearly 50,000 Minecraft users have been infected with a malware aiming at reformatting hard drives, wiping out backup data from the targeted system along with deleting other important files.	Malware/
17/04/2018	AnoaGhost	insights.london.nhs.uk	An NHS website is defaced	Defacem
18/04/2018	Gold Galleon	Multiple Maritime Shipping	Researchers from Secureworks	Account

Date	Author	Target	Description	
		Firms	discover a previously unidentified "Gold Galleon" threat group, specialized in business email compromise (BEC) and business email spoofing (BES) fraud against maritime shipping firms in order to try and steal millions of dollars on an annual basis.	
18/04/2018	?	Single Individuals	Security researchers from Radware spot a new information stealer that collects Chrome login data from infected victims, along with session cookies, and appears to be looking for Facebook and Amazon details in particular. The malware is called Stresspaint and has infected so far more than 40,000 users.	Malware/
18/04/2018	?	California's Center for Orthopaedic Specialists (COS)	California's Center for Orthopaedic Specialists (COS) discloses to have been hit by a ransomware attack. The incident impacts the records of approximately 85,000 patients across three facilities in West Hills, Simi Valley and Westlake Village.	Malware/
18/04/2018	?	Ian Balina	Ian Balina, a well-known sponsored YouTube blogger is hacked, while streaming, loosing roughly $2 million in tokens.	Account
18/04/2018	?	Sangamo Therapeutics	Sangamo Therapeutics announces a data security incident involving compromise of a senior executive's company email account.	Account
18/04/2018	?	Minecraft and Counter-Strike: Global Offensive players	Researchers discover two strains of a fake ransomware targeting players of Minecraft and Counter-Strike: Global Offensive (CS:GO)	Malware/
18/04/2018	?	Questar	Annual tests in several states are delayed by what appears to be a suspected hack to Questar, a K12 assessment solutions provider.	Unknown
19/04/2018	HighTech Brazil Hackteam	Supreme Court of India	The website of Supreme Court of India is defaced.	Defacem
19/04/2018	?	Single Individuals	Researchers from Trend Micro discover a spam campaign delivering the Adwind RAT bundled with the XTRAT and DUNIHI Backdoors.	Malware/
19/04/2018	?	Single Individuals	Researchers at MalwareHunterTeam discover a new strain of ransomware, targeting Brazilian users, called RansSIRIA, which encrypts victim's files and then states it will	Malware/

Date	Author	Target	Description	
			donate the ransom to Syrian refugees. The malware target Brazilian victims.	
20/04/2018	?	Multiple Targets	Security researchers from antivirus maker Qihoo 360 Core discover a new Internet Explorer 0-day exploited by a state-sponsored threat actor. The vulnerability is called "double kill".	Targeted
20/04/2018	?	Multiple Targets	Researchers from Qihoo 360 Netlab and GreyNoise Intelligence discover a botnet made up of servers and smart devices exploiting the severe Drupal CMS vulnerability CVE-2018-7600 also known as Drupalgeddon 2. The botnet is dubbed Muhstik.	Malware/
21/04/2018	?	Equihash mining pools	Security researchers at 360 Core Security detect a new type of attack which targets some Equihash mining pools.	Vulnerab
21/04/2018	?	City of Hamilton	The emails of about 1,100 Hamilton residents have been compromised following a data breach of two waste collection apps, according to the city of Hamilton.	Unknown
22/04/2018	AnonPlus	ilgiornale.it	Hackers from AnonPlus deface ilgiornale.it, one of the main newspapers in Italy, with a fake news about Mr. Silvio Berlusconi in jail.	Defacem
22/04/2018	Prosox Shade	Red Bull Website	The Red Bull website is defaced twice in few hours, probably exploiting the Drupalgeddon 2 vulnerability.	Defacem
23/04/2018	?	Prince Edward Island (PEI) Government Website	A ransomware attack takes down the Prince Edward Island Government website.	Malware/
23/04/2018	Orangeworm	Healthcare organizations in the United States, Europe and Asia	Researchers from Symantec reveal the details of Orangeworm, a threat group targeting healthcare organizations in the United States, Europe and Asia via a custom backdoor dubbed Kwampirs.	Targeted
23/04/2018	?	Careem	Careem, Uber’s main ride-hailing app rival in the Middle East, is hit by a cyber attack that compromises the data of 14 million users. The breach was discovered on January 14.	Unknown
23/04/2018	APT10	Japanese defense companies	According to FireEye, the Chinese group APT10 has targeted Japanese defense companies,	Targeted

Date	Author	Target	Description	
			possibly to get information on Tokyo’s policy toward resolving the North Korean nuclear impasse.	
23/04/2018	Hunter butt	Thai Airways Website	The official website of Thai Airways is hacked by a Pakistani with the moniker “Hunter butt”. The hacker uploads a deface page on 23 subdomains.	Defacem
24/04/2018	?	MyEtherWallet.com	A hacker (or group of hackers) hijacks the Amazon DNS servers of MyEtherWallet.com, a web-based Ether wallet service. Users accessing the site are redirected to a fake version of the website. Those who logged in had their wallet private keys stolen, which the attacker used to empty accounts. The total bounty is $152,000.	DNS Hija
24/04/2018	?	Ukraine's Energy Ministry Website	Unknown hackers use ransomware to take the website of Ukraine's energy ministry offline and encrypt its files.	Malware/
24/04/2018	?	Single Individuals	Researchers from FortiGuard Labs uncover a new python-based Monero cryptocurrency mining malware, dubbed "PyRoMine" that uses the ETERNALROMANCE exploit to spread.	Malware/
24/04/2018	?	Brazilian companies	Researchers from FireEye identify a widespread spam campaign, dubbed Metamorfo, targeting Brazilian companies with the goal of delivering banking Trojans.	Malware/
24/04/2018	?	Americas Cardroom	Poker tournaments are disrupted after a spite of DDoS attacks on Americas Cardroom.	DDoS
24/04/2018	?	Multiple industries including critical infrastructure, entertainment, finance, health care, and telecommunications	Researchers from McAfee uncover a global data reconnaissance campaign assaulting a wide number of industries including critical infrastructure, entertainment, finance, health care, and telecommunications. The campaign is dubbed Operation GhostSecret.	Targeted
24/04/2018	?	WebLogic Servers	Attackers start to exploit Oracle WebLogic servers for CVE-2018-2628.	Vulnerab
25/04/2018	?	HPE Users	Threat actors target internet accessible HPE Integrated Lights-Out 4 (HPE iLO 4) remote management interfaces with ransomware.	Malware/
26/04/2018	?	Single Individuals	Researchers from Vade Secure	Account

Date	Author	Target	Description	
			reveal the details of a massive phishing campaign targeting more than 550 million email users globally since the first quarter of 2018.	
26/04/2018	?	Single Individuals	Researchers from Trend Micro discover a new variant of the infamous Necurs botnet using .url files (internet shortcuts) to bypass conventional detection methods.	Malware/
26/04/2018	The Invincible The Martian	Several targets in India	Researchers from Cisco Talos unveil the details of GravityRAT, a tool being used in targeted attacks, allegedly coming from Pakistan, against India with sophisticated anti-evasion techniques.	Targeted
26/04/2018	Team Kerala Cyber Warriors	Pakistan	Team Kerala Cyber Warriors, a hacking group based out of India, begin to install ransomware on web sites based out of Pakistan. The ransomware is called KCW Ransomware.	Malware/
26/04/2018	?	Sen. Richard Pan, D-Sacramento	Sen. Richard Pan, D-Sacramento, claims that thieves hacked his email account and stole $46,000 from his re-election campaign in a "sophisticated" scheme earlier this year.	Account
27/04/2018	?	Three banks in Mexico (Grupo Financiero Banorte, Banco del Bajio SA, and Bancomext)	Three banks in Mexico (Grupo Financiero Banorte, Banco del Bajio SA, and Bancomext) are targeted by a cyber attack aimed to penetrate Mexico’s electronic payment systems (SPEI).	Unknown
27/04/2018	?	Zippy's Restaurants	The Hawaii-based Zippy's Restaurants reports that its point-of-sale system at 25 of its locations have been compromised exposing customer data from November 23, 2017, to March 29, 2018.	Malware/
27/04/2018	?	Highway Sign in Arizona	Someone hacks a highway sign in Arizona and defaces it with 'Hail Hitler' text.	Unknown
27/04/2018	?	Leominster Schools District	Leominster Schools District pays $10,000 worth of Bitcoins ransom following a cyberattack on their system.	Malware/
27/04/2018	AnonPlus	City of Bologna	The website of the City of Bologna is defaced by AnonPlus	Defacem
27/04/2018	?	Scenic Bluffs Community Health Centers	Scenic Bluffs Community Health Centers notifies 2,889 patients of a potential breach of personal patient information after	Account

Date	Author	Target	Description	
			discovering March 1, 2018, that one staff email account had been hacked on Feb. 28, 2018, by an unauthorized party.	
27/04/2018	?	Billings Clinic	Billings Clinic notifies 949 patients of a breach affecting its email security system causing an unknown individual to access patients' information back in February.	Account
30/04/2018	?	Single Individuals	Researchers from Trend Micro reveal the details of FacexWorm, a malicious Chrome extension, targeting cryptocurrency trading platforms via Facebook Messenger in order to steal account credentials for Google MyMonero and Coinhive.	Malware/
01/05/2018	?	Rail Europe North America	Rail Europe, a site used by Americans to buy train tickets in Europe, reveals a three-month data breach of credit cards and debit cards. Hackers implanted credit card-skimming malware on its website between late-November 2017 and mid-February 2018.	Malware/
01/05/2018	APT28 AKA Fancy Bear	Lojack Users	Security researchers from Arbor Networks reveal that malware with suspected links to Russian cyber-espionage group Fancy Bear is turning up in installations of Lojack, an anti-computer theft program used by many corporations to guard their assets.	Targeted
01/05/2018	?	Vulnerable servers	Researchers from AlienVault reveal the details of MassMiner, a new wave of cryptocurrency-mining malware using exploits for vulnerabilities such as CVE-2017-10271 (Oracle WebLogic), CVE-2017-0143 (Windows SMB), and CVE-2017-5638 (Apache Struts).	Vulnerab
01/05/2018	SB315	City of Augusta Calvary Baptist Church Georgia Southern University, Two Augusta restaurants: Blue Sky Kitchen and Soy Noodle House	A group of vigilante hackers going by SB315 deface some Georgia sites and threaten retaliation if the bill becomes law. The list of the targets include: the City of Augusta (that denies the hack), the website of Calvary Baptist Church, Georgia Southern University, the sites for two Augusta restaurants, Blue Sky Kitchen and Soy Noodle House.	Defacem
01/05/2018	?	Knox County's website	The Tennessee county's website is taken down by a DDoS attack on election night.	DDoS

Date	Author	Target	Description	
02/05/2018	?	Drupal Servers	Researchers from Imperva/ Incapsula discover another strain of malware, dubbed Kitty, aimed to exploit Drupalgeddon 2.0 (CVE-2018-7600) to mine cryptocurrency	Vulnerab
02/05/2018	Allanite	Business and ICS networks at electric utilities in the US and UK.	Researchers from Dragos unveil the details of a threat actor dubbed Allanite, active at least since May 2017 and still targeting both business and ICS networks at electric utilities in the US and UK.	Targeted
02/05/2018	?	Fredericksburg School System	A Fredericksburg school system employee falls for phishing attack	Account
02/05/2018	Akincilar	Greek Foreign Ministry Athens-Macedonia News Agency (ANA) Greek Handball Federation Suzuki-Greece	The Turkish hacker group Akincilar ("Invaders") starts its offensive against Greece and defaces four websites (Greek Foreign Ministry, Athens-Macedonia News Agency - ANA -, the Greek Handball Federation, and Suzuki-Greece) in response to Athens' refusal to hand over the Turkish officers who fled to Greece in July 2016.	Defacem
02/05/2018				Defacem
02/05/2018				Defacem
02/05/2018				Defacem
03/05/2018	?	Targets in Middle East	Researchers from Kaspersky reveal the details of ZooPark, a cyberespionage operation that has been focusing on Middle Eastern targets since at least June 2015. The threat actors behind the operation infect Android devices using several generations of malware.	Targeted
03/05/2018	?	World Rugby Training and Education Website	World Rugby is forced to suspend its training and education website after the governing body is the target of a cyber attack that sees hackers obtain personal data from thousands of subscribers.	Unknown
03/05/2018	?	JavaScript users	The Node Package Manager (npm) team discovers and blocks the distribution of a backdoor inside getcookies, a popular, albeit deprecated, JavaScript package.	Malware/
03/05/2018	?	Airbnb users	Researchers from Redscan	Account

Date	Author	Target	Description	
			discover a GDPR-related phishing scam with emails claiming to be from Airbnb.	
03/05/2018	?	Several Florida Hospital Websites	Several Florida Hospital Websites are taken offline after being affected by a malware that could have compromised patient information. The list of the affected hospitals include: FloridaBariatric.com, FHOrthoInstitute.com and FHExecutiveHealth.com.	Malware/
03/05/2018	Anonymous	24TV Turk Telekom	As a retaliation for the attacks of the Turkish collective Akincilar, Greek hackers from Anonymous paralyze the 24TV Live website for several hours. They also claim to have hacked 12,987 routers of Turk Telekom.	DDoS
03/05/2018	?	Meituan Dianping	Meituan Dianping, the internet giant backed by Tencent, China's most valuable tech corporation, begins investigating reports of a data breach that exposed the private information of tens of thousands of users. This happens after tens of thousands of data snippets -- everything from names and mobile numbers to home addresses -- on food-delivery customers went on sale online.	Unknown
03/05/2018	?	Fleetcor Technologies	Fleetcor Technologies, a company specializing in fuel cards and workforce payment products and services, publicly discloses that its gift card systems were accessed last month by an unauthorized party. A "significant number" of gift cards that are at least six months old, as well as PIN numbers, were accessed.	Unknown
04/05/2018	?	Copenhagen city's bicycle sharing system "Bycyklen"	Unknown hackers disrupt the Copenhagen city's bicycle sharing system "Bycyklen", erasing the data of 1,860 bicycles.	Unknown
04/05/2018	AnonPlus	K9 Web Protection	Hackers from the collective AnonPlus, a splinter cell of Anonymous, deface the website of K9 Web Protection (belonging to Symantec).	Defacem
04/05/2018	?	Riverside Fire and Police department	Ransomware infects the servers of the Riverside Fire and Police department for the second time in a month.	Malware/
04/05/2018	?	W.S. Neal High School	While finalizing end-year school rankings, W.S. Neal High School realizes that someone has been changing grades since 2016.	Unknown

Date	Author	Target	Description	
04/05/2018	?	City of Tulsa	The City of Tulsa confirms that computer hackers broke into several City controlled accounts but says it appears there have been no effects on city systems.	Unknown
04/05/2018	?	Northwest University	The email account of the Northwest University's CFO is hacked. As a consequence $60,000 are stolen.	Account
04/05/2018	?	Banco Inter	Shares in Banco Inter fall as much as 11 percent after reports that a hacking attack had obtained sensitive data pertaining to clients. Banco Inter reveals it was "the victim of attempted extortion."	Unknown
05/05/2018	?	Vulnerable Drupal Servers	Researcher Troy Mursch discovers another campaign aimed to exploit Drupalgeddon 2.0 (CVE-2018-7600 and CVE-2018-7602). In this campaign more than 350 servers are compromised to inject cryptominers.	Vulnerab
05/05/2018	?	Mason Law Office	Mason Law Office discovers evidence of unauthorized access to their mycase.com instance by an unknown individual or group of individuals. Client data is potentially accessed.	Unknown
06/05/2018	?	Canon Security Cameras	"I'm Hacked. bye2"— That's the message left behind on most of the 60 hacked Canon security cameras in Japan with many more hacked in the previous weeks.	Unknown
06/05/2018	?	Android and Windows Users	Researchers from Trend Micro identify a new spyware distributed via adult games. Dubbed as Maikspy spyware (from a famous adult film actress). The main target of this malicious new campaign are Android and Windows users, and the primary objective is to steal sensitive personal data. The malware is dubbed AndroidOS_MaikSpy.HRX.	Malware/
07/05/2018	?	SSH Decorator (Python Module) users	SSH Decorator, a Python module, is compromised by unknown attacker who inject a backdoor.	Malware/
07/05/2018	?	Roseburg Public Schools	A ransomware attack targets Roseburg Public Schools, blocking access to the district's email, website and software.	Malware/
07/05/2018	Akincilar	Honda Greece	Turkish hackers from Akincilar launch a new cyber attack against Honda Greece. The automaker's website in Greece is infiltrated with a message condemning the	Defacem

Date	Author	Target	Description	
			country for “partnering” with terrorists.	
08/05/2018	?	Marketing/Advertising/Public Relations and Retail/ Manufacturing industries	Proofpoint observes a campaign targeting Marketing/Advertising/ Public Relations and Retail/ Manufacturing industries with a new malware called Vega Stealer. The malware contains stealing functionality targeting saved credentials and credit cards in the Chrome and Firefox browsers, as well as stealing sensitive documents from infected computers.	Malware/
08/05/2018	?	Sheffield Credit Union	Sheffield Credit Union is the victim of a Cyber attack, which is believed to have taken place on 14 February 2018 but only recently comes to light after a blackmailing attempt by the attackers. The personal data of about 15,000 members is compromised.	Unknown
08/05/2018	SilverTerrier	Multiple Targets Around the World	Researchers from Palo Alto Networks reveal the details of a ring of Nigerian criminals dubbed SilverTerrier, conducting hacking campaigns against targets around the world. The researchers have attributed 181,000 attacks, using 15 families of malware, to the group in the last year, with expected losses estimated more than $3B.	Malware/
08/05/2018	?	City of Goodyear	The City of Goodyear announces that its bill pay system may have been compromised. The possible breach could expose 30,000 utility customers.	Malware/
09/05/2018	?	Several financial targets in the US	Researchers from F5 reveal a new campaign carried on via the infamous Panda malware targeting US financials targets.	Malware/
09/05/2018	?	The Sun	The Sun calls in the UK's cybersecurity authorities after detecting Russian hackers trying to access the tabloid newspaper's internal computer systems.	Targeted
09/05/2018	?	Morinaga Milk Industry Co.	After receiving a report from a credit card issuer, Morinaga Milk Industry Co. says that credit card or other personal information of up to 120,000 online customers may have leaked.	Unknown
09/05/2018	?	The Oregon Clinic	The Oregon Clinic announces that a data security incident may have affected protected health information (PHI) after an unauthorized third party accessed an internal email account.	Account

Date	Author	Target	Description	
10/05/2018	Anonymous	Official website of Russia’s Federal Agency for International Cooperation (Rossotrudnichestvo)	The Anonymous deface several subdomains of the official website of Russia’s Federal Agency for International Cooperation (Rossotrudnichestvo) against the ongoing censorship in the country especially the recent ban on Telegram.	Defacem
10/05/2018	?	Multiple Targets	Researchers from Radware reveal the details of Nigelthorn, a crypto-mining malware abusing Chrome extensions, and using Facebook to spread. The analysis reveals that the group has been active since at least March of 2018 and has already infected more than 100,000 users in over 100 countries.	Malware/
10/05/2018	?	Vulnerable Dasan GPON routers	Researchers from Qihoo 360 Netlab reveal that at least five IoT botnets are targeting Dasan GPON routers, exploiting the two recently discovered vulnerabilities CVE-2018-10561 and CVE-2018-10562. The five botnets are known under codenames such as Hajime, Mettle, Mirai, Muhstik, and Satori.	Vulnerab
10/05/2018	?	Wasaga Beach	Wasaga Beach pays the ransom to hackers who took over its computer system earlier this month.	Malware/
10/05/2018	?	Malley’s Chocolates	Malley’s Chocolates reveals that its website has been hacked, and the card information of 3,400 online customers has been breached.	Unknown
11/05/2018	?	Android Users	Researchers from Symantec discover a new wave of 45 malicious on the Android store known under the definition of Android.Reputation.1. Of these apps, 7 are rebranded versions of previously removed apps, whereas 38 are completely new,	Malware/
11/05/2018	?	Chili's Restaurant	Chili's Restaurant reveals that some restaurants have been impacted by a data incident, which may have resulted in unauthorized access or acquisition of payment card data between March and April 2018.	Malware/
11/05/2018	?	Ubuntu Users	A user has spots a cryptocurrency miner hidden in the source code of an Ubuntu snap package hosted on the official Ubuntu Snap Store. The app's name is 2048buntu, a clone of the popular	Malware/

Date	Author	Target	Description	
			2024 game.	
11/05/2018	?	DSB	The Danish state rail operator DSB is hit by a massive DDoS attack, paralyzing some operations, including ticketing systems and the communication infrastructure.	DDoS
11/05/2018	?	Bemus Point School District	Bemus Point School District Superintendent reveals that some students in the district might have been compromised amid the breach of Maia Learning by a competitor.	Unknown
12/05/2018	?	Capitol Administrators	Capitol Administrators notifies individuals of a phishing attack.	Account
12/05/2018	?	Five Mexican Banks including No. 2 Banorte	Thieves siphon 300 million pesos ($15.4 million) out of five Mexican banks, including No. 2 Banorte, by creating phantom orders that wired funds to bogus accounts and promptly withdrew the money.	Account
14/05/2018	Hackers linked to the Turkish Government	Turkish Dissident and Protesters	According to a new report by digital rights organization Access Now, hackers, apparently working for the Turkish government, attempted to infect a large number of Turkish dissidents and protesters by spreading the infamous FinFisher spyware on Twitter.	Malware/
14/05/2018	?	Family Planning NSW	Family Planning NSW tells customers their personal information may have been compromised after the not-for-profit fell victim to a ransomware attack. Around 8,000 users might be affected.	Malware/
15/05/2018	Stealth Mango	Government officials, members of the military, and activists in Pakistan, Afghanistan, India, Iraq and the United Arab Emirates	Researchers from Lookout discover a phishing campaign that infected Android devices with custom surveillance-ware bent on extracting data from top officials, primarily in the Middle East. The campaign is called Stealth Mango, and has been used to collect over 30 gigabytes of compromised data on attacker infrastructure	Malware/
10/05/2018	?	Nuance	Speech recognition software firm Nuance announces the breach of thousands of patient records after a former employee breached its servers and accessed the personal information of 45,000 individuals from several contracted clients between November 20 and December 9 of 2017.	Account

Date	Author	Target	Description	
11/05/2018	?	Multiple Users	Researchers from Qihoo 360 discover a miner campaign hidden behind a potentially unwanted program dubbed One System Care.	Malware/
11/05/2018	Satori Botnet	Exposed Ethereum Mining Rigs	The operators of the Satori botnet are mass-scanning the Internet for exposed Ethereum mining rigs, according to three sources in the infosec community who've observed the malicious behavior —SANS ISC, Qihoo 360 Netlab, and GreyNoise Intelligence.	Brute-For
15/05/2018	?	Multiple Users	Researchers from Qihoo 360 discover a particular miner dubbed IdleBuddyMiner, which asks nicely for permission to mine via a popup.	Malware/
16/05/2018	?	Securus	A hacker provides Motherboard with 2,800 login details for Securus, a company that buys phone location data from major telecom companies and then sells it to law enforcement. The company confirms the breach few days later.	Unknown
16/05/2018	?	Windows Users	Researchers from Qihoo 360 discover a massive malware campaign spreading a new coinminer, which appears to have made roughly 500,000 victims in three days alone. The miner is called WinstarNssmMiner.	Malware/
16/05/2018	?	Ethereum Wallets	Researchers from RiskIQ unveil the details of MEWKit, a sophisticated phishing campaign aimed at stealing credentials of Ethereum wallets, and in the same time, perform and automated transfer with the stolen details.	Account
16/05/2018	?	ZooPark APT Group	A vigilante hacker claims to have hacked the alleged Iran-linked group behind the ZooPark campaign discovered by Kaspersky earlier this month, and dumps the files purportedly stolen from a server controlled by the attackers.	Unknown
16/05/2018	?	LifeBridge Health and LifeBridge Potomac Professionals	LifeBridge Health and LifeBridge Potomac Professionals notify patients about a malware incident occurred back in March 18, 2018. The number of affected patients could be 500,000.	Malware/
16/05/2018	?	Wordpress Websites	A report from security firm Wordfence reveals that hackers have come up with a never-before-seen method of installing backdoored plugins on websites	Account

Date	Author	Target	Description	
			running the open-source WordPress CMS, and this new technique relies on using weakly protected WordPress.com accounts and the Jetpack plugin.	
16/05/2018	Racoon Hacker	Russian-speaking Telegram users	Researchers from Cisco Talos reveal the details of TeleGrab, a malware harvesting cache and key files from Telegram.	Malware/
16/05/2018	?	Android Users	Researchers from security company Avast discover 26 apps on the Google Play Store that include adware forcing ads on compromised systems.	Malware/
17/05/2018	?	blackphoenixalchemylab.com	blackphoenixalchemylab.com discovers malware inserted into the portion of the checkout page between May 1 and May 16.	Malware/
17/05/2018	?	Corporation Service Company (CSC)	Hackers steal the personally identifiable information of 5,678 customers of the Corporation Service Company (CSC), according to a notice the company sent to the California attorney general's office.	Unknown
17/05/2018	?	Fortnite Players	Researchers at Zscaler's ThreatLabZ discover malicious apps on Google Play, in disguise of a mobile version of the popular game Fortnite.	Malware/
17/05/2018	?	Vulnerable IoT devices	Researchers from Fortinet discover a new variant of the Mirai botnet dubbed 'Wicked Mirai'	Malware/
17/05/2018	?	Independent Like the North State Group Forum	An online forum designated for California's First Congressional District debate was hacked by unknown hackers, who take over the live stream to broadcast gay pornography.	Unknown
18/05/2018	Sun Team	North Korean defectors and journalists	Researchers from McAfee discover RedDawn, a new campaign on Google Play targeting North Korean defectors and journalists.	Targeted
18/05/2018	?	DrayTek routers	DrayTek, a Taiwan-based manufacturer of broadband CPE devices, announces that hackers are exploiting a zero-day vulnerability to change DNS settings on some of its routers.	Vulnerab
18/05/2018	?	University of Buffalo	University of Buffalo confirms to be investigating and responding to a breach of 2,690 UBITName accounts.	Account
18/05/2018	?	Tidal	Jay-Z's Tidal streaming platform announces to have enlisted an "independent, third party cyber-security firm" to investigate a	Unknown

Date	Author	Target	Description	
			possible data breach, after reports of inflated subscriber and streaming numbers.	
18/05/2018	?	Mobile Users	Researchers from Kaspersky reveal a new campaign carried on using the Roaming Mantis mobile trojan, targeting Europe and Middle East, and adding new features, like a phishing option for iOS devices, and crypto-mining capabilities for the PC.	Malware/
18/05/2018	?	Shona McGarty	Actress Shona McGarty, who plays Whitney Carter in EastEnders, is the latest celebrity to have intimate pictures leaked on the internet. Apparently her photos were stolen from the iCloud account.	Account
18/05/2018	?	Bitcoin Gold	An unidentified hacker performs several "double spend" attacks on the infrastructure of the Bitcoin Gold cryptocurrency and manages to amass over $18 million worth of BTG (Bitcoin Gold) coins in the process.	51% attac
19/05/2018	Two unidentified students	Bloomfield Hills High School	Two students from Bloomfield Hills High School are the main suspects of a recent hack discovered at the school. The two broke into the school's MISTAR Student Information System portal where they changed grades, attendance records, and attempted to refund lunch purchases.	Vulnerab
20/05/2018	?	200 million Japanese	A hacker suspected to be operating out of China has put on sale the data of around 200 million Japanese users on an underground cybercrime forum, according to a FireEye iSIGHT Intelligence report. The data appears to have been assembled by hacking up to 50 smaller Japanese sites.	Unknown
20/05/2018	?	Allied Physicians	Allied Physicians reports it was hit with a SamSam ransomware attack earlier this month (May 17).	Malware/
20/05/2018	?	Manuel Delia's Blog	Manuel Delia's blog (a Maltese journalist and blogger) is the target of a DDoS attack. Apparently the attack comes from Ukraine.	DDoS
21/05/2018	?	Gigabit Passive Optical Network (GPON) routers	Security researchers from Qihoo 360 Netlab discover that the operators behind the TheMoon botnet are now leveraging a zero-day exploit to target GPON routers.	Malware/

Date	Author	Target	Description	
21/05/2018	?	Gigabit Passive Optical Network (GPON) routers	Trend Micro researchers detect a new attack mimicking the Mirai botnet modus operandi, originating from Mexico and targeting Gigabit Passive Optical Network (GPON)-based home routers via two vulnerabilities (CVE-2018-10561 and CVE-2018-10562).	Vulnerab
21/05/2018	?	Twitter account of Charlie Lee	The Twitter account of Charlie Lee, the creator of Litecoin is hacked.	Account
21/05/2018	?	Bombas	Bombas notifies consumers of breach going back to 2015 when malware in the code of the e-commerce platform was identified and removed on February 9, 2015.	Malware/
22/05/2018	?	Verge Cryptocurrency	A hacker finds a way around a previous patch in the Verge cryptocurrency source code and takes advantage of the flaw to monopolize mining operations and create Verge coins (XVG) at a rapid pace. He is able to mine over 35 million XVG coins in just a few hours for a profit of $1.65 million.	51% attac
22/05/2018	?	Mac Users	According to researchers at Malwarebytes, many Mac users in the past weeks have been infected with a new strain of Monero miner. The owners of the infected Mac systems noticed the presence of a process named “mshelper” had been consuming a lot of CPU power and draining their batteries.	Malware/
22/05/2018	?	Monacoin	Monacoin suffers a 51% attack.	51% attac
23/05/2018	State sponsored attackers (Russia?)	500,000 organizations worldwide	Researchers from Cisco Talos unveil the details of VPNFilter, a massive campaign lasting since 2016 and carried on by nation-state hackers, infecting at least 500,000 victims in at least 54 countries. The known devices affected by VPNFilter are Linksys, MikroTik, NETGEAR and TP-Link networking equipment, as well as QNAP NAS devices. An update of June 6 reveals new capabilities, such as the possibility to perform MITM attacks, and other vulnerable devices (ASUS, D-Link, Huawei, Ubiquiti, UPVEL, and ZTE).	Malware/
23/05/2018	?	University of Vermont	University of Vermont officials say they have no reason to believe the personal information of 37,000 current and former faculty, staff	Unknowr

Date	Author	Target	Description	
			and students fell into the wrong hands following an intrusion of the school's computer systems.	
24/05/2018	Trisis, AKA Xenotime, AKA HatMan	Multiple Targets	Security researchers from CyberX reveal that the threat actor behind the Triton malware (aka Trisis, Xenotime, and HatMan) is now targeting organizations worldwide and safety systems.	Targeted
24/05/2018	?	Android Users	Avast reveals a list of 140 Android devices whose firmware is infected with a malware called Cosiloon.	Malware/
24/05/2018	?	Screens at the Mashhad airport in Iran	Hackers deface the screens at the Mashhad airport in Iran to protest against the Government and the military's activities in the Middle East.	Defacem
24/05/2018	?	Associates in Psychiatry and Psychology	Associates in Psychiatry and Psychology notifies 6,546 patients and the U.S. Department of Health and Human Services (HHS) of a ransomware incident that occurred in March.	Malware/
25/05/2018	?	Oxnard City	Oxnard city officials are contacted by a bank representative about fraudulent purchases being made with the cards people used to pay their utility bills	Account
25/05/2018	?	American Family Life Assurance Company of Columbus (Aflac)	American Family Life Assurance Company of Columbus (Aflac) issues a press release concerning the breach of independent contractor sales agents' email accounts. The breach occurred between Jan. 17 and April 2 and has reportedly affected some clients' personal information.	Unknowr
25/05/2018	?	Aultman Health Foundation	About 42,600 patients tied to AultWorks Occupational Medicine, Aultman Hospital, and some Aultman physician offices may have had personal health and identification information stolen in a data breach after unknown and unauthorized individuals gained access to certain email accounts in February and March.	Unknowr
26/05/2018	?	Afghan diplomats in Pakistan	Afghan diplomats in Pakistan are warned they are believed to be victims of "government-backed" digital attacks trying to steal their email passwords.	Targeted
26/05/2018	?	Arlo	Arlo advises its customers to change their passwords after credential-stuffing attempts detected.	Brute-For
27/05/2018	?	Goliath and Goliath	Comedy and entertainment	Account

Date	Author	Target	Description	
			agency Goliath and Goliath suffered a loss of more than 300,000 ZAR (22,000 USD worth) in what appears to be a phishing scam.	
28/05/2018	?	Bank of Montreal	Bank of Montreal, the country's fourth bank, announces to have been contacted by fraudsters claiming to have stolen personal and financial information of a limited number of the bank's customers. According to the bank, less than 50,000 c customers are affected by the incident.	Unknown
28/05/2018	?	Canadian Imperial Bank of Commerce (CIBC)	Also the Canadian Imperial Bank of Commerce (CIBC), the country's fifth largest bank is affected by the same incident, and they believe that 40,000 users could be possibly affected from its subsidiary Simplii Financial.	Unknown
28/05/2018	?	Taylor Cryptocurrency	The creators of the Taylor cryptocurrency trading app claim that an unidentified hacker has stolen around $1.35 million worth of Ether from the company's wallets.	Account
28/05/2018	Cobalt AKA Carbanak	Several Russian Banks	Group-IB reveals that, despite the alleged arrest of its leader, the Cobalt (AKA Carbanak) hacker group that's specialized in stealing money from banks and financial institutions is still active, even launching a new campaign.	Targeted
28/05/2018	?	Harare Institute of Technology	A database from the Harare Institute of Technology is leaked, containing 3,500 users.	Unknown
29/05/2018	Hidden Cobra	Multiple Targets	The FBI and Department of Homeland Security jointly release two technical alerts via the US-CERT, warning of two malware families dating back to at least 2009 that they say are tied to the suspected North Korea-sponsored APT group Hidden Cobra. The two malware families are the remote access tool (RAT) Joanap and the Server Message Block-based (SMB) worm Brambul.	Targeted
29/05/2018	?	Brazilian Individuals	Researchers from IBM X-Force uncover a new Brazilian, Delphi-based banking malware, dubbed MnuBot. The malware uses Microsoft SQL Server as ITS command and control server.	Malware/
29/05/2018	?	EOS Blockchain nodes	Threat Intelligence firm GreyNoise discovers that a mysterious attacker is scanning the Internet for EOS blockchain nodes that are	Brute-For

Date	Author	Target	Description	
			accidentally exposing private keys through an API misconfiguration.	
30/05/2018	IsHaKdZ	Ticketfly	The Ticketfly website is defaced with an image of V from the film V for Vendetta. Unfortunately, after refusing to pay a 1 BTC ransom, Ticketfly reveals that the personal information of 27 million accounts, including ticket buyers and venue operators, was accessed by the attacker.	Vulnerab
30/05/2018	?	Purdue University Pharmacy and the Family Health Clinic of Carroll County	Patients of the Purdue University Pharmacy and the Family Health Clinic of Carroll County receive notices that their information might be compromised because of a security breach. A malicious file was installed on some computers on September 1st.	Malware/
31/05/2018	North Korean APT actor Group123?	South Koreans	Researchers from Cisco Talos discover NavRAT, a remote access trojan that apparently went undiscovered for at least two years, targeting Koreans in a spam campaign using the possible upcoming U.S.-North Korea nukes summit as a phishing lure. The tool leverages the email platform from South Korea-based Naver Corporation to communicate with the attackers.	Targeted
31/05/2018	Andariel Group	South Koreans	Local media in South Korea reveal that a North Korean cyber-espionage group has exploited at least nine ActiveX zero-day vulnerabilities, including a new 0-day, to infect South Korean targets with malware or steal data from compromised systems.	Targeted
31/05/2018	?	Sooke School District	The Sooke School District warns parents about a privacy invasion after an employee's email was hacked.	Account
01/06/2018	?	Buffalo Wild Wings	A hacker manages to take control of the official Twitter account of Buffalo Wild Wings (@BWWings) and posts a number of crude and racist tweets, including one that claims to give out the "secret recipe" for the company's wings.	Account
01/06/2018	?	Several Rhode Island State Agencies	Rhode Island officials say several state agencies are targeted by malware. The list of victims include: the Department of Children, Youth and Families, the Department of Human Services, and the Department of Behavioral Healthcare.	Malware/
02/06/2018	?	Several Australian citizens	Several Australian citizens are the	Account

Date	Author	Target	Description	
			victims of a tech support scam, through which the attackers are able to take over their webcams and upload videos to YouTube.	
02/06/2018	Todd Davis aka Lifelock	Holland Eye Surgery & Laser Center	Holland Eye Surgery & Laser Center notifies 42,200 patients about a hack occurred in 2016.	Unknown
02/06/2018	?	Shiawassee County	The Shiawassee County financial administrator resigns after being caught in a phishing scam and mistakenly wiring $50,000 to an overseas bank account.	Account
03/06/2018	?	ZenCash	ZenCash, an upcoming privacy coin, is the victim of a 51% attack.	51% attac
03/06/2018	?	Booking.com users	According to multiple reports, unknown cybercriminals launch a phishing campaign targeting Booking.com customers whose information was illegally obtained, possibly by breaching certain partner hotels.	Account
04/06/2018	?	MyHeritage	MyHeritage, the genealogy website and DNA testing service, warns that the email addresses and hashed passwords of its customer database, approximately 92 million user accounts, have been found on a private server.	Unknown
04/06/2018	?	New York Giants defensive end Avery Moss	Explicit videos and pictures of New York Giants defensive end Avery Moss are posted on his Twitter timeline after his account is hacked.	Account
04/06/2018	?	Morinaga Milk Industry Co.	Morinaga Milk Industry Co. says that personal data on up to 92,822 customers may have been stolen as its health food shopping website was hacked. Credit card information belonging to up to 29,773 of the affected customers was leaked and that around 300 cases of illicit use of the information, involving some ¥20 million ($180,000), have been confirmed so far.	Unknown
05/06/2018	?	Undisclosed Japanese Syndicate Wallet	Shopin, a universal shopper profile using blockchain and Artificial Intelligence, releases an official statement indicating that a significant token distributor was hacked on June 1st, resulting in a loss of more than $10 million USD of a variety of tokens, including Ethereum, Level Up, Orbs, and Shopin Tokens.	Account
05/06/2018	?	WordPress Sites	Security researchers from Wordfence reveal the details of BabaYaga, a malware targeting WordPress sites characterized by	Malware/

Date	Author	Target	Description	
			sophisticated self-preserving mechanisms.	
06/06/2018	?	PageUp	Australia-based human resources firm PageUp confirms it found "unusual" activity on its IT infrastructure on May 23, which has resulted in the potential compromise of client data.	Malware/
06/06/2018	?	Multiple Targets	Researchers from the GuardiCore security team reveal the details of Operation Prowli, a gigantic botnet of over 40,000 infected web servers, modems, and other IoT devices, used for cryptocurrency mining, and for redirecting users to malicious sites.	>1
06/06/2018	Sofacy	Government organizations dealing with foreign affair	Researchers from Palo Alto Networks Unit 42 reveal the details of Zebrocy, a new campaign carried on by the Sofacy group via phishing attacks that contain malicious Microsoft Office documents with macros as well as simple executable file attachments.	Targeted
06/06/2018	?	Litecoin Cash	Litecoin Cash is the latest crypto currency to suffer a 51% attack.	51% attac
06/06/2018	?	Brazilian users of online banking services.	Researchers from Kaspersky Lab discover a malicious Chrome Extension available in the Chrome Web Store, targeting Brazilian users of online banking services.	Malware/
07/06/2018	?	High-profile targets in Russia and Ukraine	Researchers from ESET reveal the details of Invisimole, a campaign active since 2013 targeting entities in Russia and Ukraine.	Targeted
07/06/2018	?	Targets in Middle East	Researchers from ICEBRG and 360 Core Security reveal a wave of attacks leveraging the unpatched CVE-2018-5002 Adobe vulnerability.	Vulnerab
07/06/2018	?	Russian service centers offering maintenance and support for various electronic goods.	Security researchers from Fortinet spot a series of attacks targeting Russian service centers offering maintenance and support for various electronic goods.	Vulnerab
07/06/2018	?	City of Wellington	Wellington officials reveal to have been recently notified by Superion, their software vendor, about potential unauthorized charges on credit cards used by customers to pay their utility bills.	Vulnerab
07/06/2018	?	RISE Wisconsin	RISE Wisconsin formerly Community Partnerships and Center for Families) notifies its participants of a ransomware attack occurred on April 8, 2018.	Malware/
08/06/2018	Alleged State-sponsored	US Navy Contractor	Chinese government hackers have	Targeted

Date	Author	Target	Description	
	Chinese hackers		compromised the computers of a Navy contractor, stealing 600+ Gb of highly sensitive data related to undersea warfare, including secret plans to develop a supersonic anti-ship missile for use on U.S. submarines by 2020, according to American officials. The attack occurred in January and February.	
08/06/2018	?	Elmcroft Senior Living	The personal information of Elmcroft Senior Living residents and their family members, employees and others could have been stolen in a data breach that occurred in mid-May.	Account
08/06/2018	?	Terros Health	Terros Health warns that 1,600 patient records were exposed in a data breach earlier this spring. The breach, due to a phishing attack, was discovered on April 12 and happened November 16, 2017.	Account
08/06/2018	?	Multiple Targets	Researchers from Barkly reveal a malicious spam campaign distributing .IQY files, simple text files that open by default in Excel and are used to download data from the Internet. These files are highly evasive for AVs.	Malware/
08/06/2018	?	Undisclosed Italian Companies	Researchers from Yoroi reveal the details of DMOSK, a malware targeting specifically Italian firms.	Malware/
11/06/2018	?	Bank of Chile	Shares in the Bank of Chile are down after it confirms hackers siphon off $10 million of its funds, mainly to Hong Kong. However the bank says no client accounts have been impacted. Apparently a wiper malware was used to conceal the real purpose of the attack.	Fraudulen
11/06/2018	?	Coinrail	Coinrail, a South Korean cryptocurrency exchange, says that its systems have been hacked. It is believed that hackers stole about 40 billion won (US $37.2 million) worth of cryptocurrency from Coinrail, including 21 billion won worth of Pundi X and 14.9 billion won worth of Aston.	Unknown
11/06/2018	Lazarus Group	South Korean Think Tank	North Korea-linked Lazarus APT Group planted an ActiveX zero-day exploit on the website of a South Korean think tank focused on national security.	Targeted
12/06/2018	?	Misconfigured Ethereum Mining Rigs and applications	According to Chinese internet security firm Qihoo 360 Netlab, hackers have stolen $20 million in	Misconfig

Date	Author	Target	Description	
			ether from poorly configured Ethereum mining rigs and third-party applications.	
12/06/2018	One or more people in Russia?	Clarifai	A lawsuit filed by a former employee alleges that AI startup Clarifai's computer systems were compromised by one or more people in Russia, potentially exposing technology used by the US military. The lawsuit says Clarifai learned of the breach last November, but did not promptly report it to the Pentagon.	Targeted
12/06/2018	?	Mexican National Action Party (PAN)	The website of the Mexican National Action Party is hit by a cyber attack during the final television debate between presidential candidates ahead of the July 1 vote, after the site had published documents critical of the leading candidate.	DDoS
12/06/2018	?	Single Individuals	Researchers from Fortinet discover PyRoMineIoT, a new strain of crypto-currency miner that exploits the NSA-linked EternalRomance exploit to spread.	Malware/
12/06/2018	?	Multiple Targets	Researchers from Kromtech reveal that over a dozen malicious docker images have been available on Docker Hub for 30 days, allowing hackers to earn $90,000 in cryptojacking profits.	Malware/
12/06/2018	?	Massachusetts Clean Energy Center	An audit reveals that a scammer stole nearly $94,000 in public funds from the Massachusetts Clean Energy Center last year.	Account
12/06/2018	?	National Network and Electronic Services Agency (NASES) Slovak Hydro-meteorological Institute (SHMÚ) slovensko.sk	Several Slovakian websites are hit by a wave of DDoS attacks.	DDoS
13/06/2018	?	Dixons Carphone	Dixons Carphone has admitted a huge data breach involving 5.9 million payment cards and 1.2 million personal data records. The breach began in July last year and 105,000 cards without chip-and-pin protection have been leaked.	Unknown
13/06/2018	LuckyMouse AKA EmissaryPanda AKA APT27	Mongolia	Researchers from Kaspersky reveal that the Chinese hacking group LuckyMouse broke into a national data center in Mongolia late last year and planted the HyperBro malware into government websites.	Targeted
13/06/2018	?	Syscoin	Malicious actors replace the legitimate Windows installer for Syscoin's cryptocurrency with a	Malware/

Date	Author	Target	Description	
			version containing malware, which was available on the company's Github page for several days.	
13/06/2018	?	Single Individuals	Researchers from Qihoo 360 Total Security reveal the details of ClipboardWalletHijacker, a malware campaign infecting over 300,000 computers. The malware's purpose is to intercept content recorded in the Windows clipboard, look for strings resembling Bitcoin and Ethereum addresses, and replace them with ones owned by the malware's authors.	Malware/
13/06/2018	?	AcFun	According to a statement by the company, millions of user accounts of the Chinese video sharing platform AcFun are hacked. According to the same statement, the accessed data includes the user IDs, nicknames and passwords of nearly 10 million users. The company urges them to change their password.	Unknown
14/06/2018	Hidden Cobra	Multiple Targets	The US Department of Home Security issues a new warning over a new type of malware coming from the Hidden Cobra group. The new variant is known as “TYPEFRAME".	Targeted
14/06/2018	?	HealthEquity	About 23,000 accounts are compromised by a data breach that took place at HealthEquity in April when an employee fell for a phishing scam.	Account
14/06/2018	?	Multiple Targets	Researchers from Trend Micro reveal another version of the MuddyWater campaign using a Powershell-based PRB-Backdoor. The malware is dubbed W2KM_DLOADR.UHAOEEN.	Targeted
14/06/2018	?	Android users	Researchers from ThreatFabric discover a new malware strain still under development, dubbed MysteryBot, which blends the features of a banking trojan, keylogger, and mobile ransomware.	Malware/
14/06/2018	?	Med Associates	Med Associates, notifies of a security incident that may have compromised its patients protected information.	Malware/
15/06/2018	?	Vulnerable IoT devices	Researchers from Qihoo 360 Total Security discover a spike in traffic, coming from the infamous Satori botnet, and directed to port TCP 8000, attempting to exploit	Vulnerab

Date	Author	Target	Description	
			CVE-2018-10088.	
15/06/2018	?	Multiple Targets in Singapore	Researchers at F5 Labs and Loryka observe a spike in the number of cyber-attacks targeting Singapore from June 11 to June 12, in the wake of the meeting between U.S. President Donald Trump and North Korean President Kim Jong-un.	>1
06/06/2018	?	Danielle Lloyd	Danielle Lloyd, English model and former Miss England and Miss Great Britain, has her iCloud account hacked, with attackers stealing intimate images that were eventually posted online.	Account
13/06/2018	?	Black River Medical Center	Black River Medical Center in Missouri notifies an unspecified number of patients potentially affected by a phishing incident discovered on April 23.	Account
16/06/2018	?	Liberty Life	Liberty Life's IT system are attacked by unknown hackers, who reportedly obtain sensitive data about some of the insurer's top clients and ask for a ransom.	Unknown
17/06/2018	?	Andy Android Emulator users	A GPU Miner Trojan is installed along with the popular Andy Android emulator.	Malware/
18/06/2018	?	Carepartners	CarePartners' computer system is breached and as a result patient and employee information including personal health and financial information, are inappropriately accessed.	Unknown
19/06/2018	Thrip	Satellite operators, defense contractors and telecommunications companies in the United States and southeast Asia	Researchers from Symantec reveal the details of Thrip, a sophisticated hacking campaign launched from computers in China targeting satellite operators, defense contractors and telecommunications companies in the United States and southeast Asia, active from 2013.	Targeted
18/06/2018	?	Flightradar24	Users of the popular flight-tracking site flightradar24 are told to change their passwords after the site warns of a data breach. The breach may have compromised the email addresses and hashed passwords for a small subset of Flightradar24 users (those who registered prior to March 16, 2016).	Unknown
19/06/2018	?	Individuals in the US	Researchers at Bitdefender discover Zacinlo, a newly uncovered form of stealthy and persistent malware distributing adware to victims across the world while also allowing	Malware/

Date	Author	Target	Description	
			attackers to take screenshots of infected machines' desktops. The vast majority of Zacinlo victims are in the US, with 90 percent of those infected running Microsoft Windows 10.	
19/06/2018	?	Med Associates	Med Associates notifies its patients that the facility suffered a data breach on March 22, when unusual activity was detected, potentially exposing PII, including medical diagnosis and payment card information of about 270,000 patients.	Unknown
19/06/2018	?	Financial organizations in Russia, and biological and chemical threat prevention laboratories in Europe and Ukraine.	Researchers from Kaspersky Lab reveal to have detected Olympic Destroyer infections across Europe in May and June 2018. New victims include financial organizations in Russia, and biological and chemical threat prevention laboratories in Europe and Ukraine.	Malware/
19/06/2018	?	Android Users	Malware researchers from ESET discover a new strain of Android RAT, tracked as HeroRat, that leverages Telegram protocol for command and control, and data exfiltration.	Malware/
20/06/2018	?	Fortnite players	Malwarebytes reveal the details of a campaign carried on via a fake installer for the famous video game Fortnite.	Malware/
20/06/2018	?	Bithumb	South Korean cryptocurrency exchange Bithumb says that 35 billion won ($31.5 million) worth of virtual coins have been stolen by hackers.	Unknown
20/06/2018	?	Multiple Targets	Researchers from Deep Instinct reveal the details of Mylobot, a complex botnet that uses a never before seen combination of evasion techniques,	Malware/
20/06/2018	?	Unknown target (probably an embassy)	Researchers from AlienVault uncover a new Afghanistan-based attack disguised as a recent article from a Middle Eastern news, leveraging a Metasploit backdoor.	Targeted
20/06/2018	?	Road Sign close to ICE (U.S. Immigration and Customs Enforcement)	Someone hacks a road sign close to the ICE headquarter in Portland and defaces it with the “Abolish ICE” message.	Unknown
21/06/2018	?	Android Users	RiskIQ reveals the details of a new malicious Android app that has infected at least 60,000 devices, gaining the ability to extract some important information from each	Malware/

Date	Author	Target	Description	
			device along with installing some ad click malware.	
21/06/2018	?	Vulnerable Drupal servers	Researchers from Trend Micro observe a series of network attacks exploiting the Drupal vulnerability CVE-2018-7602 to turn affected systems into Monero-mining bots.	Vulnerab
21/06/2018	?	Magento sites	Researchers at Sucuri discover a very simple evasion technique to infect again Magento websites after their malicious code has been removed.	Malware/
21/06/2018	?	Humana	Health insurer Humana notifies an unspecified number of health plan members after detecting and blocking a credential stuffing attack against Humana.com and Go365.com. The attacks took place on June 3 and June 4 from overseas IP addresses.	Credentia
22/06/2018	?	Indian Businessman	The email of a city-based businessman is hacked and INR12.5 lakh (USD 18,230) stolen and transferred to two bank accounts in China.	Account
22/06/2018	?	PDQ	PDQ, a fast-casual dining restaurant warns customers about a cyber attack on its computer systems in which hackers were able to access or acquire personal information from the chain's customers who paid with credit cards. The breach lasted nearly a year, from May 19, 2017 to April 20, 2018.	Remote a
22/06/2018	?	Entities in South East Asia	Security researchers at Palo Alto Networks uncover a new cyber espionage group tracked as RANCOR that has been targeting entities in South East Asia, using two previously unknown strains of malware dubbed DDKONG and PLAINTEE.	Targeted
22/06/2018	?	cryptocurrency exchanges	Security researchers at AlienVault uncover a series of cyber attacks on cryptocurrency exchanges, carried on by the infamous Lazarus Group, and leveraging weaponized HWP documents (Hangul Word Processor documents). The researchers suspect the same actors are behind the attack to Bithumb,	Targeted
22/06/2018	Tick APT	South Korean defense company	Researchers from Palo Alto Networks uncover a new operation conducted by the cyber espionage group known as Tick APT. The campaign targets a	Targeted

Date	Author	Target	Description	
			secure USB drive built by a South Korean defense company.	
24/06/2018	?	Midwest City	Midwest City, Oklahoma, reports that about 2,300 customers are potentially affected by a breach involving Superion's software Click2Gov.	Vulnerab
26/06/2018	?	FastBooking	The personal details and payment card data of guests from hundreds of hotels, are stolen by an unknown attacker from FastBooking, a Paris-based company that sells hotel booking software to more than 4,000 hotels in 100 countries. The breach occurred on June 14.	Vulnerab
26/06/2018	?	Single Individuals	Security researchers at Kaspersky discover an adware written in Python targeting Windows-based computers. The adware is dubbed PBot (PythonBot) and is also able to install cryptocurrency miner and ad extensions in the browser.	Malware/
27/06/2018	?	Ticketmaster	Ticketing service Ticketmaster announces a data breach affecting roughly 5% of its entire customer base, resulting in the theft of customer data, Ticketmaster login information, and payment details. The breach didn't occur at Ticketmaster itself, but at Inbenta, a provider of AI-powered live chat widgets, which Ticketmaster was deploying on some of its localized sites across the world.	Unknown
27/06/2018	?	Red Hen Restaurant	Researchers from Malwarebytes discover that the Red Hen restaurant that refused to serve Sarah Sanders is hit by a SEO Spam cyberattack	SEO Spar
27/06/2018	Apophis Squad	ProtonMail	ProtonMail is hit by a DDoS attack	DDoS
27/06/2018	?	Connecticut Higher Education Trust (CHET)	Unauthorized individuals gain access to 21 accounts of the Connecticut Higher Education Trust (CHET) and make 44 withdrawals, for a total of $1,416,635, of which, $442,540 is recovered or stopped.	Account
27/06/2018	?	Z Energy Ltd	New Zealand-based fuel supplier Z Energy Ltd says it has been presented with evidence that customer data from its Z Card Online database was accessed by a third party in November 2017.	Unknown
27/06/2018	?	Cyanweb Solutions	Digital marketing and web provider Cyanweb Solutions	Unknown

Date	Author	Target	Description	
			looses nearly all customer data and backups after a “criminal hacking incident” that compromises one of its servers.	
28/06/2018	?	Adidas	Adidas alerts customers about a possible data breach on its U.S. website. On June 26, the company became aware that an unauthorized party claimed to have acquired limited data associated with certain consumers. A preliminary investigation found the leaked data includes contact information, usernames and encrypted passwords.	Unknown
28/06/2018	?	Official website of Ernakulam Siva Temple	The official website of Ernakulam Siva Temple is defaced with anti-national slogans and offensive language besides a Pakistan flag.	Defacem
28/06/2018	?	GitHub account of the Gentoo Linux distribution	An unknown hacker temporarily takes control over the GitHub account of the Gentoo Linux organization and embed malicious code inside the operating system's distributions that would delete user files. The malicious code fails to trigger properly and users' files remain safe.	>1
28/06/2018	?	Single Individuals	Researchers from FireEye discover for the first time one malware campaign using the innovative PROPagate technique to inject malware into legitimate processes.	Malware/
28/06/2018	?	Multiple Targets	After observing attacks on customers, Cisco tells users to install the fix for CVE-2018-0296, a denial-of-service flaw, discovered on June 6, affecting a number of its security appliances.	Vulnerab
28/06/2018	?	City of Midland	City of Midland is the latest municipality being breached because of a vulnerability in the Superion’s Click2Gov application.	Vulnerab
28/06/2018	?	Middletown school district	The Middletown School District is hit by a ransomware.	Malware/
28/06/2018	?	South Eastern Regional College (SERC)	Personal information of hundreds of staff at the South Eastern Regional College is compromised after detecting suspicious email activity as the consequence of a hack.	Account
29/06/2018	?	Typeform	Barcelona-based online survey and form building service Typeform announces a data breach after an unknown attacker downloaded a backup file	Unknown

Date	Author	Target	Description	
			containing sensitive customer information. The backup file contained data gathered by Typeform customers through surveys and online forms up until May 3, 2018.	
29/06/2018	?	Algonquin College	The Algonquin College publishes a note indicating that the education community is still not sure how many current and former students and employees could be affected by a cyber attack that happened weeks earlier. However the note suggests that the impacted people could be thousands.	Unknown
30/06/2018	?	Single Individuals	Researchers from Bleeping Computers discover a new Clipboard Hijacker Malware able to monitor 2.3 Million bitcoin addresses.	Malware/
30/06/2018	?	Single Individuals	Security researchers spot a new Mac malware family, dubbed OSX.Dummy, advertised on cryptocurrency-focused Slack and Discord channels.	Malware/
30/06/2018	?	Notre Dame de Namur University	Notre Dame de Namur University notifies some financial aid applicants that their information may have been compromised when an employee fell prey to a phishing attack on April 23, 2018.	Account
22/06/2018	?	Manitowoc County	Manitowoc County officials release more information about a data breach of a Manitowoc County email account in January, when an employee falls victim of a phishing attack.	Account
26/06/2018	?	Linux-Based servers	Researchers from Trend Micro uncover a malware bot that infects Linux-based servers and connected devices with a cryptominer that appears to transfer funds to the operators of a Chinese money-making scam website.	Malware/
29/06/2018	?	Klook Travel	Klook Travel informs its users about a data breach incident it suffered. The attackers exploited a malicious JS code associated with SOCIAPlus, a third-party tool integrated on the site.	Malicious
29/06/2018	?	Hunt Regional Medical Center	Hunt Regional Medical Center notifies patients of a possible breach due to the hack of an employee email occurred on May 1st, 2018.	Account
01/07/2018	?	Trezor	The team behind the Trezor multi-cryptocurrency wallet service	BGP Pois

Date	Author	Target	Description	
			discovers a phishing attack against some of its users that took place over the weekend, carried on via DNS poisoning or BGP hijacking.	
02/07/2018	?	Fortnum & Mason	Luxury retailer Fortnum & Mason is the latest big brand to be involved in a significant data breach after the company admits the details of around 23,000 competition and survey participants have been compromised in the wake of the Typeform breach.	Unknown
02/07/2018	?	Whitbread	Whitbread’s online recruitment system has suffered a data breach, affecting a number of the company’s brands including Premier Inn, and the UK outlets of Costa Coffee. The breach is a consequence of the attack to PageUp.	Malware/
02/07/2018	?	Fortnite players	Tens of thousands of Fortnite users are infected by malware after downloading a fake cheating app.	Malware/
03/07/2018	?	Taiwan Democratic Progressive Party's (DPP)	The Democratic Progressive Party's (DPP) official website is defaced by Chinese hackers and the website is replaced with pictures and words reading "Chinese netizens are supporting Tsai Ing-wen to run for re-election" in simplified Chinese characters.	Defacem
03/07/2018	?	Israeli Military	The Israeli military say it had uncovered a plot by Hamas militants to spy on soldiers by befriending them on social media and then luring them into downloading fake dating applications that gave Hamas access to their smartphones.	Account
03/07/2018	?	Domain Factory	German hosting provider Domain Factory experiences a data breach which has exposed customer data. After an unknown threat actor posts claims that suggest they had managed to compromise the firm's systems and access information, the company launches an investigation and finds the claims to be true and says that customer data "was accessed by an outside party without authorization" on 28 January 2018.	Vulnerab
03/07/2018	Charming Kitten, Newscaster, or Newsbeef.	Single Individuals	ClearSky Security reveals that the malicious actor Charming Kitten, which the company previously	Account

Date	Author	Target	Description	
			exposed, built a phishing website impersonating the company and attempting to spear-phish people interested in reading reports.	
03/07/2018	?	Single Individuals	Researchers from Cisco Talos discover a new version of Smoke Loader, a malicious application that can be used to load other malware.	Malware/
03/07/2018	?	Single Individuals	Researchers at Malwarebytes reveal the details of an operation leveraging shortlinks and traffic distribution system to infect users and mine Monero using the CPN Miner.	Malware/
03/07/2018	?	Single Individuals	Researchers from Trend Micro uncover an unusual malicious macro-based malware campaign that modifies infected users' shortcut files so that they secretly download a backdoor program.	Malware/
05/07/2018	?	Yatra.com	Online travel booking website Yatra.com is compromised and attackers steal 5 Million user records that include email address & physical addresses, phone numbers & plain text passwords & PINs. The breach happened back in 2013, and it came to light now.	Unknown
05/07/2018	?	MSK Group	MSK Group notifies patients of a data security incident that they discovered on May 7, due to an unauthorized access to certain parts of the network at times over several month.	Unknown
06/07/2018	Chinese Government	Australian National University	China-based hackers have successfully infiltrated the IT systems at the Australian National University, potentially compromising the home of Australia's leading national security college and key defence research projects.	Targeted
06/07/2018	?	CVE-2018-7600 Vulnerable servers	Researchers from Akamai reveal the details of DrupalGangster, yet another Monero-mining campaign based on XMRig and lukMiner exploiting the Drupalgeddon 2 vulnerability CVE-2018-7600.	Vulnerab
06/07/2018	?	B&B Hospitality Group	B&B Hospitality Group (B&BHG) announces that it has identified and addressed a payment card security incident that affected nine restaurants in the New York metropolitan area.	Malware/
06/07/2018	?	VSDC	Research from Qihoo 360 Total Security reveal that hackers have breached the website of VSDC, a popular company that provides	Malware/

Date	Author	Target	Description	
			free audio and video conversion and editing software. Three different incidents have been recorded during which hackers changed the download links on the VSDC website with links that initiated downloads from servers operated by the attackers.	
06/07/2018	?	Lake Oswego School District	Lake Oswego School District warns students about a phishing email after the District Twitter account and an employee email accounts are hacked.	Account
07/07/2018	?	Blizzard Entertainment	Blizzard Entertainment is hit by a DDoS attack. Players of Overwatch, Heroes of the Storm, and World of Warcraft are affected.	DDoS
08/07/2018	?	Timehop	Timehop discloses a security breach that has compromised the personal data of 21 million users (essentially its entire user base). Around a fifth of the affected users have also had a phone number that was attached to their account breached in the attack. The breach was discovered on July 4, while the attack was in progress.	Account
08/07/2018	Gaza Cybergang APT	Institutions across the Middle East, specifically the Palestinian Authority.	Researchers from Check Point reveal the details of Big Bang, an operation carried on by the Gaza Cybergang APT against institutions across the Middle East, specifically the Palestinian Authority.	Targeted
09/07/2018	?	Bancor	Token creation platform Bancor goes offline following a "security breach" that sees the platform lose millions of dollars worth of cryptocurrency. The company lost roughly $13.5 million in the hack and the value of the coin loses quickly 20%. The breach was carried on via the compromise of the free VPN service Hola.	Account
09/07/2018	?	Gas Station in Detroit	Police in Detroit are looking into an apparent hack at a gas station that allowed people to steal more than 600 gallons of gas, valued at over $1,800. Authorities believe the thieves used some sort of remote device to take control of the pump. At least 10 cars filled up for free during that time.	Remote D
09/07/2018	?	Macy's Inc.	Macy's Inc. warns customers that hackers compromised the login information of some users of the retailer's websites. The suspicious	Account

Date	Author	Target	Description	
			activity took place from April 26 to June 12. A third party obtained valid usernames and passwords through websites not related to macys.com or bloomingdales.com and used those to gain access to customers' accounts.	
09/07/2018	BlackTech	Multiple Targets	Researchers from ESET discover a new malware campaign misusing stolen digital certificates from D-Link Corporation and Changing Information Technology. Two different malware families that were misusing the stolen certificate – the Plead malware, a remotely controlled backdoor, and a related password stealer component, allegedly used by the cyberespionage group BlackTech.	Malware/
09/07/2018	Magecart APT	Inbenta Technologies	Researchers from RiskIQ reveal the real extension of the third-party breach that compromised the data of several Ticketmaster UK customers. More than 800 e-commerce sites were compromised.	Malicious
10/07/2018	?	Arch Linux	Yet another Linux distribution compromised. This time it's up to Arch Linux, which has three downloadable software packages in the AUR, short for Arch User Repository, rebuilt to contain malware.	Malware/
10/07/2018	TEMP.Periscope	Cambodia	Researchers from FireEye reveal a large scale operation from TEMP.Periscope, a Chinese cyber espionage group seeking to monitor the country's upcoming and contentious July 29 national elections.	Targeted
10/07/2018	?	U.S. Air Force	Security Firm Recorded Future identifies an attempted sale of what is believed to be highly sensitive U.S. Air Force documents pertaining to the MQ-9 Reaper drone. The attack was carried on via the default FTP authentication credentials in Netgear routers.	Vulnerab
10/07/2018	?	Turkish Android users	Researchers from IBM X-Force discover a campaign distributing the Marcher (aka Marcher ExoBot) and BankBot Anubis mobile banking Trojans via malicious apps in Google Play. It's believed that at least 10,000 people have downloaded the malware.	Malware/
10/07/2018	?	Career and Technology	Career and Technology Education	Unknown

Date	Author	Target	Description	
		Education Centers (C-TEC)	Centers (C-TEC) reveals it suffered a possible data breach earlier this year that could have exposed individuals' names and Social Security numbers. The breach happened on May 25 when an unauthorized person had access to a private file for several minutes.	
10/07/2018	?	Cass Regional Medical Center	Cass Regional Medical Center, a Missouri health care center, announces that they have been affected by an undisclosed ransomware. This incident affected their internal communications system and their electronic health record (EHR) system.	Malware/
11/07/2018	?	BP	BP emails about 60,000 people who applied for jobs in its retail stores since 2008 to notify them they could have had their personal information accessed by hackers. The company originally thought about 10,000 applicants' data had been breached. The breach is a consequence of the attack to PageUp.	Malware/
11/07/2018	?	Chlorine distillation plant in Ukraine	The Ukrainian Secret Service (SBU) reveals it stopped a cyber-attack with the VPNFilter malware on a chlorine distillation plant in the village of Aulska, in the Dnipropetrovsk region. The SBU accuses Russia of operating the malware and launching the attack.	Malware/
11/07/2018	?	Ammyy	Researchers from ESET reveal that on June 13 or 14, the Ammyy website was compromised to serve a malware-tainted version of this otherwise legitimate software bundling the Kasidet trojan. To add an interesting twist to the incident, the attackers tried to hide their malicious activity behind the brand of the ongoing FIFA World Cup.	Malware/
11/07/2018	?	Major International Airport	While researching underground hacker marketplaces, researchers from McAfee discover that access linked to security and building automation systems of a major international airport could be bought for only US$10.	Account
11/07/2018	?	Aviation ID Australia	Aviation ID Australia, the company that issues Aviation Security Identity Cards (ASICs) is hacked and notifies hundreds of people that their ASIC application information may have been stolen.	Unknown

Date	Author	Target	Description	
12/07/2018	?	Single Individuals	A hacker gains access to a developer's npm account and injects malicious code into eslint-scope, a popular JavaScript library, sub-module of the more famous ESLint, a JavaScript code analysis toolkit.	>1
12/07/2018	?	13 iPhones in India	Researchers from Cisco Talos identify an unprecedented highly targeted campaign against 13 iPhones which appears to be focused on India. The attacker deployed an open-source mobile device management (MDM) system to control enrolled devices.	Malicious
12/07/2018	?	Samsung service centers in Italy	Security researchers from TG Soft discover an ongoing malware campaign targeting Samsung service centers in Italy leveraging the CVE-2017-11882 Office Equation Editor vulnerability. The campaign appears to be the counterparts of attacks that have previously targeted similar electronics service centers in Russia this year.	Targeted
12/07/2018	?	Single Individuals	Researchers from Imperva pick up on a spike in SPAM activity directed at sites powered by WordPress, launched by a botnet, with linked sites offered betting services on 2018 FIFA World Cup matches.	Spambot
12/07/2018	?	UMC Physicians (UMCP)	UMC Physicians (UMCP) notifies patients who may have been affected by a recent data breach. On May 18, the UMCP IT team discovered an employee's email account was hacked on March 15, potentially compromising the personal health information of more than 18,000 patients.	Account
13/07/2018	?	Alive Hospice	Alive Hospice notifies patients whose personal and protected health information were in employee emails that were accessed by an unknown person or persons beginning on December 20, 2017 and again on April 5, 2018 after two employees fell prey to phishing attacks. The attacks were discovered on May 15, 2018.	Account
13/07/2018	?	Billings Clinic	Billings Clinic discloses a breach exposing details of 8,400 patients. The organization detected anomalous activity on one of the employees' email accounts on May 14, 2018. The investigation	Account

Date	Author	Target	Description	
			revealed the account was compromised while the employee was traveling overseas.	
13/07/2018	?	Pennsylvania Department of Health	A government spokesman reveal that the Pennsylvania Department of Health’s birth certificate system was shut down for nearly a week last month after someone hacked into an internal website but did not take or alter citizens records.	Unknown
14/07/2018	?	LabCorp	LabCorp, one of the US largest medical diagnostics companies, investigates a security breach that could have put health records of millions of patients at risk. The company, in a filing with the Securities and Exchange Commission, says it detected “suspicious activities” on its network over the weekend of July 14 and “immediately took certain systems offline as part of its comprehensive response to contain the activity.”	Unknown
14/07/2018	Anonymous	Sant' Andrea Hospital	Hackers from the Anonymous leak the usernames and passwords from 12,000 employees, patients, contractors from the Sant' Andrea Hospital in italy.	SQLi
15/07/2018	?	League of Legends Philippines'	League of Legends Philippines' confirms an unauthorized modification in their client lobby code resulting in the injection of the Coinhive Monero miner.	Malware/
15/07/2018	APT28 AKA Fancy Bear	Italian Military	Security researchers from the Z-Lab at CSE Cybersec reveal the details of Operation "Roman Holiday" an operation carried on by APT28 (AKA Fancy Bear) and targeting the Italian Military.	Targeted
12/07/2018	Joel Ortiz	Around 40 victims	California authorities arrest Joel Ortiz, a 20-year-old college student, who hijacked more than 40 phone numbers and stole $5 million in bitcoins and other crypto currencies.	SIM Hijac
15/07/2018	?	Mahatma Gandhi Mission Hospital	The Mahatma Gandhi Mission Hospital in Mumbai is hit by a ransomware attack.	Malware/
16/07/2018	?	Mega	Thousands of credentials for accounts associated with New Zealand-based file storage service Mega are published online. The text file contains over 15,500 usernames, passwords, and files names.	Credentia
16/07/2018	?	LabCorp	LabCorp, the US' biggest blood testing laboratories network,	Unknown

Date	Author	Target	Description	
			announces that hackers breached its IT network over the weekend.	
16/07/2018	Andariel Group	South Korean targets	Researchers from Trend Micro discover a new campaign from the Andariel Group carried out via the injection of a malicious script into four compromised South Korean websites for reconnaissance purposes.	Targeted
16/07/2018	?	Sunspire Health	Sunspire Health notifies an undisclosed number of individuals after several employee email accounts were accessed in a phishing attack between March 1, 2018 and May 4, 2018.	Account
16/07/2018	?	University of Pittsburgh Medical Center - Cole	UPMC Cole has notified 790 patients treated at UPMC Cole that their personal information may have been inappropriately accessed after two phishing attacks on June 7 and June 14.	Account
16/07/2018	?	City of Bozeman	The city of Bozeman says some customers that used its Click2Gov utility payment system in 2017 may have had their credit information stolen.	Malware/
16/07/2018	?	Single Individuals	Researchers from Kromtech discover an automated operation aimed to launder money from stolen credit cards, buying and selling goods for three popular games: Clash of Clans, Clash Royale, Marvel Contest of Champions.	Account
16/07/2018	?	Southern College of Optometry	The Southern College of Optometry notifies an undisclosed number of students whose student loan information and Social Security numbers were in an employee email account that was hacked	Account
17/07/2018	?	Ukrainian government institutions	Researchers from ESET reveal the details of a prolonged cyber espionage campaign active against the Ukrainian Government since 2015. and carried out via three different RATs: Quasar, Sobaken and Vermin.	Targeted
17/07/2018	Blackgear AKA Topgear and Comnie)	Organizations in Japan, South Korea, and Taiwan	Researchers from Trend Micro reveal a new activity of the Blackgear cyber espionage campaign (also known as Topgear and Comnie), targeting public sector agencies and telecommunications and other high-technology industries in Japan, South Korea, and Taiwan.	Targeted
17/07/2018	?	UK and European supply companies	Action Fraud warns that malicious actors are impersonating UK	Account

Date	Author	Target	Description	
			universities to defraud out of vast sums of money UK and European supply companies.	
17/07/2018	?	Ubisoft	Video game publisher Ubisoft suffers a series of massive DDoS attacks. As a result, several Ubisoft gaming servers face connectivity issues.	DDoS
18/07/2018	Anarchy	Vulnerable Huawei devices	Security researchers from NewSky Security reveal the detail of a botnet comprised of over 18,000 Huawei devices in one day, built exploiting the CVE-2017-17215 vulnerability.	Vulnerab
18/07/2018	?	Single Individuals	Denis Sinegubko, a security researcher from Sucuri unveils a malware distribution campaign where the GoogleUserContent CDN is used a malicious image hiding malware code in Exchangeable Image File Format (EXIF) data. The malicious code is used to steal PayPal security tokens.	Malware/
19/07/2018	?	ComplyRight	Cloud-based human resources company ComplyRight reveals that a security breach of its Web site may have compromised sensitive consumer information — including names, addresses, phone numbers, email addresses and Social Security numbers — from tax forms submitted by the company's thousands of clients on behalf of employees. The breach happened between April 20, 2018 and May 22, 2018.	Unknown
19/07/2018	?	Finland	Researchers from F5 Networks reveal a spike of attacks against IoT devices in Finland in the days leading up to the July 16 Helsinki summit between President Donald Trump and Russian President Vladimir Putin.	>1
19/07/2018	?	Dasan and D-Link routers	Security researchers from eSentire observe an increase in exploitation attempts targeting Small-Office/Home Office (SOHO) network devices manufactured by Dasan and D-Link. The attacks are carried out via a botnet composed of more than 3,000 source IPs.	Vulnerab
19/07/2018	?	Roblox	Roblox, a hugely popular online game for kids, is hacked by an individual who subverts the game's protection systems in order to have customized animations appear. This allows two male avatars to gang rape a	Malicious

Date	Author	Target	Description	
			young girl's avatar on a playground in one of the Roblox games.	
19/07/2018	?	Liverpool FC	Liverpool FC's fan database is hacked resulting in a serious data breach for around 150 supporters. The club confirms that season ticket holder information - including home addresses and bank details - were stolen from a club email account.	Account
19/07/2018	TA505	Single Individuals	Researchers from ProofPoint discover a malicious spam campaign carried out abusing the SettingContent-ms file format.	Malware/
20/07/2018	?	SingHealth	Singapore's largest health care group, SingHealth, reveals to have suffered a cyber attack to a company database in which attackers copied information belonging to roughly 1.5 million patients, including the country's prime minster, Lee Hsien Loong. The attack was discovered on July 4 and all patients who visited the clinics from May 1, 2015 through July 4, 2018 were affected.	Targeted
20/07/2018	?	Golden Heart Administrative Professionals	Golden Heart Administrative Professionals, a billing company and business associate of several healthcare providers in Alaska, notifies 44,600 individuals that some of their protected health information has potentially been accessed by unauthorized individuals as a result of a recent ransomware attack. Golden Heart Administrative Professionals.	Malware/
20/07/2018	?	Three U.S. congressional candidates	Microsoft reveals to have helped the U.S. government to fend off attempts by Russia to hack into the campaigns of three congressional candidates earlier this year.	Targeted
20/07/2018	MoneyTaker	PIR Bank of Russia	Cybercriminals part of the notorious hacking group MoneyTaker attack the PIR Bank of Russia and steal $1M. The hacking is carried out after infiltrating the bank's systems by compromising an old, outdated router. The router was installed at one of the regional branches of the bank. The attack took place on July 3.	Vulnerab
20/07/2018	?	MacOS Users	Researchers from Kaspersky Lab uncover Calisto, what appears to be an early developmental prototype of the Proton backdoor	Malware/

Date	Author	Target	Description	
			malware that typically infects macOS.	
20/07/2018	?	Boys Town National Research Hospital	Boys Town National Research Hospital discloses data breach that may have exposed PHI on 105,309 individuals. The hospital, on May 23, discovered unusual activity relating to an employee’s email account.	Account
20/07/2018	?	Single Individuals	Researchers from Fortinet reveal that the notorious Jigsaw ransomware has been repurposed to steal Bitcoin by altering the addresses of wallets and redirecting payments into accounts owned by the attacker.	Malware/
20/07/2018	?	Vulnerable IoT devices	Researchers from Palo Alto Networks Unit 42 find three malware campaigns built on publicly available source code for the Mirai and Gafgyt malware families that incorporate multiple known exploits affecting Internet of Things (IoT) devices.	Malware/
20/07/2018	?	NorthStar Anesthesia	NorthStar Anesthesia notifies patients after some employee email accounts are compromised between April 3 and May 24, 2018.	Targeted
20/07/2018	?	Clark University	Clark University in Massachusetts notifies some students whose personal information, including Social Security Numbers, were in an employee’s email account that had been accessed between March 19 and March 23rd, amid a phishing attack.	Account
20/07/2018	?	Ochre Health Wollongong	An unspecified cyber incident at Ochre Health Wollongong medical centre leaves patients without the possibility to access their patient data.	Unknown
23/07/2018	Dragonfly AKA Energetic Bear	U.S. Utility Control Rooms	Homeland Security Officials reveal that attackers from the malicious actor Dragonfly AKA Energetic Bear might have accessed the control rooms of U.S. Energetic Utilities.	Targeted
23/07/2018	?	Etherscan.io	Visitors of the popular Ethereum blockchain explorer Etherscan.io are shown a pop-up message showing "1337" indicating the website has been compromised.	Malicious
23/07/2018	APT-C-27 AKA Golden Rat	Targets in Syria	Researchers at CSE Cybsec ZLab discover a malicious code revealing that a long-term espionage campaign in Syria attributed to a APT-C-27 group, is still active.	Targeted

Date	Author	Target	Description	
23/07/2018	?	Department of Corrections, DOC	A “security incident” occurred on April 3 at a third-party vendor (Accreditation, Audit & Risk Management Security, LLC) may have compromised the personal information of employees, inmates and others involved with the state Department of Corrections.	Unknown
24/07/2018	?	The National Bank of Blacksburg	Brian Krebs reveals that hackers used phishing emails to break into a The National Bank of Blacksburg in two separate cyber intrusions over an eight-month period, making off with more than $2.4 million total. The breaches happened in May 2016 and June 2017.	Account
24/07/2018	?	Southern Baptist Convention's International Mission Board	The Southern Baptist Convention's (SBC) International Mission Board announces to have suffered a data breach earlier this year (on April 11) exposing the personally identifiable information on its current and former employees, volunteers and applicants.	Unknown
24/07/2018	?	Users in Germany, Poland and Japan	Researchers from Proofpoint discover an upgraded version of the Kronos banking trojan, targeting users in Germany, Poland, and Japan.	Malware/
24/07/2018	?	Vulnerable Oracle WebLogic Servers	Security researchers from ISC SANS and Qihoo 360 Netlab reveal to be currently tracking two separate groups who appear to have automated the exploitation of Oracle WebLogic CVE-2018-2893 vulnerability at a large scale.	Vulnerab
24/07/2018	EliteLands	Unpatched AVTech devices	Ankit Anubhav, a security researcher at NewSky Security discovers a botnet named "Death" composed of vulnerable AVTech devices.	Vulnerab
24/07/2018	?	Verified @AlmostHumanFOX Twitter Account	An apparent hacker is able to hack a discontinued TV show's verified Twitter account (@AlmostHumanFOX) to impersonate Justin Sun, the founder of the decentralized Tron currency and promote a cryptocurrency scam.	Account
25/07/2018	?	COSCO	A ransomware attack severely disables the U.S. network of COSCO (China Ocean Shipping Company), one of the world's largest shipping companies.	Malware/
25/07/2018	?	Securities Investors Association Singapore (SIAS)	The Securities Investors Association Singapore (SIAS)	Unknown

Date	Author	Target	Description	
			announces to have suffered a breach. The breach occurred in 2013 and that the NRIC numbers, home addresses, email addresses, mobile and landline numbers of 70,000 people were compromised in the incident.	
25/07/2018	Leafminer	Government organizations and business verticals in various regions in the Middle East	Researchers from Symantec uncover the operations of a threat actor named Leafminer targeting a broad list of government organizations and business verticals in various regions in the Middle East since at least early 2017.	Targeted
25/07/2018	OilRig group (AKA APT34, Helix Kitten)	Unnamed technology services provider and government entity	Researchers from Palo Alto Networks Unit 42 reveal to have detected multiple attacks by the OilRig group appearing to originate from a government agency in the Middle East. The attacks delivered a PowerShell backdoor called QUADAGENT.	Targeted
25/07/2018	?	Vulnerable SAP and Oracle ERP software	A joint report from Onapsis and Digital Shadows forces the Department of Homeland Security's US-CERT to issue a security advisory warning organizations that attackers are increasingly exploiting vulnerabilities in Enterprise Resource Planning (ERP) software from companies like SAP and Oracle.	Vulnerab
25/07/2018	?	Targets in the information technology, healthcare, and retail industries.	Researchers from ProofPoint discover a new remote access Trojan (RAT), dubbed Parasite HTTP.	Malware/
25/07/2018	?	Kasikornbank (Kbank) and Krungthai Bank (KTB)	Computer systems of Kasikornbank (Kbank) and Krungthai Bank (KTB) are compromised, affecting the security of the personal and corporate data of more than 120,000 customers.	Unknown
25/07/2018	?	City of Medford	1,842 Medford residents are impacted by a City of Medford data breach after the city's online utility billing service is infected with malware. The breaches happened between February 18th through March 14th and March 29th through April 16th.	Malware/
25/07/2018	Shadow Brokers	Some Banks in Chile	Hackers from the Shadow Brokers gain access to some 14,000 credit card numbers in Chile and publish them on social media.	Unknown
26/07/2018	APT28 AKA Fancy Bear	Sen. Claire McCaskill	Sen. Claire McCaskill is the target of a spear phishing campaign	Targeted

Date	Author	Target	Description	
			allegedly orchestrated by the infamous Fancy Bear AKA APT28.	
26/07/2018	?	KICKICO	KICKICO, an Initial Coin Offering (ICO) project suffers a security breach. Attackers access the private key of the smart contract and as a result, steal more than 70 million KickCoins which is around $7.7 million.	Vulnerab
26/07/2018	?	Yale University	Yale University notifies members of breach that took place between 2008 and 2009, when a threat actor managed to access a database and exfiltrate names, Social Security numbers, and dates of birth. The breach was discovered on June 16 this year.	Unknown
26/07/2018	?	Blue Springs Family Care	Healthcare provider Blue Springs Family Care discloses a ransomware attack resulting from an authorized access that may have also compromised 44,979 patients records.	Malware/
26/07/2018	?	Vulnerable client and servers	Researchers from Kaspersky Lab reveal the details of PowerGhost, a mining campaign based on a PowerShell script able to spread using the EternalBlue exploit.	Malware/
26/07/2018	?	Individuals in Ukraine	Researchers from FireEye reveal the details of a new wave of attacks related to the FELIXROOT campaign, targeting individuals in Ukraine, and carried out via a malicious email containing a weaponized document leveraging the CVE-2017-0199 and CVE-2017-11882 exploits.	Targeted
26/07/2018	?	Single Individuals	Security researchers from Trend Micro reveal the details of Underminer, a new exploit kit, currently active mainly in Asian countries, used to spread rootkits and cryptocurrency-mining (coinminer) malware. The campaign exploits three vulnerabilities: CVE-2015-5119, CVE-2016-0189, CVE-2018-4878.	Malware/
26/07/2018	?	Undisclosed PDF Editor Application	Microsoft reveals that hackers compromised a font package installed by a PDF editor app and used it to deploy a cryptocurrency miner on users' computers, tampering the shared infrastructure in place between the vendor of a PDF editor application and one of its software vendor partners.	Unknown
26/07/2018	?	Prison-issued tablets	Idaho prison officials announce in	Vulnerab

Date	Author	Target	Description	
			a press release that they've identified 364 inmates who have exploited a vulnerability in their prison-issued tablets and have used it to assign nearly $225,000 worth of digital credits to their tablet accounts.	
27/07/2018	?	Several U.S. state and local government agencies	Several U.S. state and local government agencies report receiving strange letters via conventional mail that include malware-laden compact discs (CDs) apparently sent from China.	Malware/
27/07/2018	?	Single Individuals	Ivan Kwiatkowski, a French security researcher, discovers an adware delivery scheme that involves clone websites that use legitimately-looking domain names to trick victims into downloading famous apps, but which are actually laced with adware.	Malware/
27/07/2018	DarkHydrus	Government agency in the Middle East	Researchers from Palo Alto Networks Unit 42 unveils a targeted attack against a government agency in the Middle East carried out by a threat actor dubbed DarkHydrus.	Targeted
27/07/2018	Coaches for the football team at Braden River	Hudl football team	Coaches for the football team at Braden River (Bradenton, Fla.), are caught using a college Hudl account to access opponents' game and practice videos.	Account
27/07/2018	Dohaeragon	Kaiser Permanente's Health Innovations	Kaiser Permanente's Health Innovations website is defaced by	Defacem
28/07/2018	@fs0c131y	Telecom Regulatory Authority of India (TRAI) chairman R S Sharma	Alleged personal details of the Telecom Regulatory Authority of India (TRAI) chairman R S Sharma are leaked after he tweeted his 12-digit Unique Identification Authority of India or UIDAI number and challenged hackers.	Account
28/07/2018	?	Confluence Health	Confluence Health discloses a patient data breach after an employee email account is hacked on March 30 and May 28, 2018.	Account
28/07/2018	?	Some Banks in Chile	Additional 55,106 cards are leaked in Chile.	Unknown
30/07/2018	?	UnityPoint Health	UnityPoint Health warns 1.4 million patients their information might have been breached by email hackers after a phishing attack.	Account
30/07/2018	?	Vulnerable MikroTik Routers	Security researchers discover a massive cryptojacking campaign that targets MikroTik routers and	Vulnerab

Date	Author	Target	Description	
			changes their configuration to inject a copy of the Coinhive in-browser cryptocurrency mining script in some parts of users' web traffic.	
30/07/2018	Sandsworm	Spiez Laboratory	The state-run Spiez laboratory near Bern, which analyzed the nerve agent samples from Salisbury, reveals to have been targeted by hackers believed to be linked to the Russian government ahead of a conference of chemical and biological warfare.	Targeted
30/07/2018	?	Single Individuals	Researchers from Palo Alto Networks Unit 42 discover 145 Google Play apps infected with Windows malware and available since October 2017. The apps are removed by Google.	Malware/
30/07/2018	?	Single Individuals	Researchers from Check Point reveal the details of a massive malvertising campaign dubbed Master134 attempting 40,000 infections per week and distributing crypto miners.	Malvertis
30/07/2018	?	Single Individuals	Researchers from Proofpoint discover a large email campaign distributing an enhanced version of the AZORult information stealer and downloader.	Malware/
30/07/2018	?	Hāwera High School	An anonymous computer hacker demands US$5000 from a provincial high school to return course work they are holding for ransom.	Malware/
31/07/2018	?	Single Individuals	Valve Corporation, the company behind the gaming website Steam, suddenly pulls a game called Abstractism from its store. Customer complaints and the game’s performance metrics point to another instance of crypto jacking.	Malware/
31/07/2018	?	Borough of Matanuska-Susitna	The Borough of Matanuska-Susitna is hit by CryptoLocker. The attack took place on July 24 but was maybe dormant since May. The IT systems are not operation with some users starting to use typewriters.	Malware/
31/07/2018	?	City of Valdez	Also the City of Valdez is hit by CryptoLocker.	Malware/
31/07/2018	?	Single Individuals	Researchers from Sucuri discover a new crypto mining campaign using the Crypto-Loot cryptominer and abusing RawGit, a CDN for	Malicious

Date	Author	Target	Description	
			GitHub files.	
31/07/2018	?	Jersey Mike's Subs	Jersey Mike's Subs warns some of their customers to change their account passwords to ensure account security. According to the email, the firm suspected a possible data breach at some third party.	Unknowr
20/07/2018	?	MedSpring Urgent Care	MedSpring Urgent Care notifies 13,000 patients after a phishing attack occurred on May 8.	Account
30/07/2018	?	Altex Exchange	Altex Exchange acknowledges that a double-counting bug in Monero (XMR) cryptocurrency did result in a major undisclosed financial loss.	Monero V
01/08/2018	?	Reddit	Reddit discloses a breach of its systems that compromised user data including some current email addresses and salted and hashed passwords from a 2007 database backup. The attacker gained access to several employee accounts via SMS intercept between June 14 and June 18.	Account
01/08/2018	?	Companies and organizations associated with industrial production	Kaspersky Lab ICS CERT identifies a new wave of phishing emails with malicious attachments targeting primarily companies and organizations associated with industrial production. The malware used in these attacks installs legitimate remote administration software – TeamViewer or Remote Manipulator System/Remote Utilities (RMS). Around 800 computers in more than 400 countries are targeted.	Malware/
01/08/2018	?	Amnesty International	Amnesty International reveals to have been targeted by a campaign carried out via the surveillance malware developed by the Israel surveillance vendor, NSO Group.	Targeted
01/08/2018	booloop	recruitmilitary.com	A user called booloop a publishes a database containing over 850,000 US military officers personal information.	Unknowr
01/08/2018	?	Hong Kong's Department of Health	Three Hong Kong's Department of Health computers are hit by ransomware.	Malware/
02/08/2018	Gorgon	Governmental organizations in the United Kingdom, Spain, Russia, and the United States.	Researchers from Palo Alto Networks Unit 42 uncover Gorgon, a threat actor allegedly operating from Pakistan and targeting governmental organizations in the United Kingdom, Spain, Russia,	Targeted

Date	Author	Target	Description	
			and the United States leveraging spear phishing emails with Microsoft Word documents exploiting CVE-2017-0199.	
02/08/2018	RASPITE	Entities in the US, Middle East, Europe, and East Asia	Researchers from Dragos identify a new activity group targeting access operations in the electric utility sector, called RASPITE.	Targeted
02/08/2018	DarkCoder AKA @Th3Falcon	Elbit Systems	DarkCoder AKA @Th3Falcon leaks 10,000 credentials for users and administrators from Elbit Systems.	SQLi
03/08/2018	?	TSMC (Taiwan Semiconductor Manufacturing Co.)	A computer virus, later reported to be a variant of WannaCry, halts several Taiwan Semiconductor Manufacturing Co. factories, the sole maker of the iPhone's main processor.	Malware/
03/08/2018	?	Mention	Mention CEO Matthieu Vaxelaire informs users of the occurrence of a data security breach involving a third-party provider. The breach occurred in July and Mention promptly reported details to the French data protection authorities.	Unknown
03/08/2018	?	Datawire, Vantiv, Mercury Payment Systems	Researchers from Oracle publish the details of three DNS Hijacks against three payment processors.	DNS hijac
04/08/2018	?	RAF Airwoman	An RAF airwoman has her Tinder profile hacked. The attackers use the hacked profile to steal secrets of Britain's new F-35 Lightning II stealth fighter.	Account
04/08/2018	?	Livecoin	Livecoin crypto exchange announces that it met considerable losses because crucial bug in Monero code, allowing to manipulate transaction amounts. The total amount of the funds lost is 15108 XMR (more than $1,8 million).	Vulnerab
06/08/2018	?	Single Individuals	Security from Duo Security release a report detailing the operations of a Twitter bot composed of 15.000 fake accounts promoting cryptocurrency giveaway scams.	Twitter B
07/08/2018	?	PGA of America	PGA of America's computers are locked by a ransomware.	Malware/
07/08/2018	DarkHydrus	Government entities and educational institutions in the Middle East.	Researchers from Palo Alto Networks Unit 42 reveal the detail of a new credential harvesting attack carried out by the DarkHydrus Threat Actor.	Account
08/08/2018	?	US Political Organizations	LinkedIn reveals to have uncovered and restricted a group	Linkedin

Date	Author	Target	Description	
			of less than 40 fake accounts that appeared to be engaged in efforts to connect with members in political organizations.	
08/08/2018	?	Multiple Organizations	Researchers from Check Point discover a massive proxy botnet, called Black, infecting 100,000 machines in two months, and used as a relay to the infamous Ramnit malware.	Malware/
09/08/2018	Hidden Cobra	US Organizations	The US-CERT issues an alert for the KeyMarble Trojan, a new threat attributed to the infamous North Korean Hidden Cobra Actor.	Targeted
09/08/2018	?	Hennepin County	Officials reveal that cyber attackers have infiltrated e-mail accounts for about 20 Hennepin County employees since late June, and may have accessed the private information of people who rely on the county's services.	Account
10/08/2018	?	Butlin's	Butlin's has confirmed that the records of up to 34,000 guests have been accessed by hackers. The stolen data does not include payment details, but customers' names, holiday dates, postal and email addresses and telephone numbers.	Account
10/08/2018	?	Brazilian Bank Customers	The Radware Threat Research Center identifies a hijacking campaign aimed at Brazilian bank customers via their IoT devices, attempting to gain their bank credentials via DNS hjiacking against D-Link routers.	DNS hjiac
10/08/2018	?	Adams County	Adams County officials release a media statement and a detailed notification regarding a security breach affecting 258,120 individuals in the Adams County. The investigations revealed that the breach, due to an unauthorized access, lasted for around six years: from January 2013 to March 2018.	Unknown
11/08/2018	?	Cosmos Bank	Cyber criminals hack the systems of India's Cosmos Bank and siphon off nearly 944 million rupees ($13.5 million) through simultaneous withdrawals across 28 countries. Unidentified hackers stole customer information through a malware attack on its ATM server.	Malware/
11/08/2018	?	Hundreds of Instagram accounts	Hundreds of Instagram accounts are hijacked in a coordinated attack.	Account
13/08/2018	?	Single Individuals in	Multiple researchers identify a	Malware/

Date	Author	Target	Description	
		developing countries	dangerous new variant of the KeyPass ransomware, featuring a manual-control functionality, and according, targeting developing countries.	
14/08/2018	?	Office 365 Users	Researchers from Avanan discover a new phishing campaign, dubbed PhishPoint, targeting the 10% of Office 365 users globally.	Account
15/08/2018	?	Michael Terpin	Michael Terpin, a bitcoin investor is suing AT&T for $240m after it allegedly ported his phone number to a hacker, allowing the criminal to steal $24m in cryptocurrency.	SIM Swa
15/08/2018	?	Customers of large banks	Researchers at Cyberbit announce they have discovered a new variant of Trickbot, a modular malware and well-known financial Trojan that targets customers of large banks and steals their credentials.	Malware/
15/08/2018	?	Hans Keirstead	Rolling Stone reveals that the U.S. Federal Bureau of Investigation is investigating a series of cyberattacks over the past year that targeted Dr. Hans Keirstead, a Democratic candidate in California.	Targeted
16/08/2018	Malicious Actors from China	Alaska Communications Systems Group Inc Ensco Plc's Atwood Oceanics, The Alaska Department of Natural Resources The Alaska governor's office Regional internet service provider TelAlaska	Cybersecurity firm Recorded Future said the Hackers operating from China's Tsinghua University targeted U.S. energy and communications companies, as well as the Alaskan state government, in the weeks before and after Alaska's trade mission to China.	Account
16/08/2018	?	Augusta University Health	Augusta University Health discloses a breach affecting 417,000 patients as a consequence of two phishing attacks occurred on September 11, 2017 and July 31, 2018.	Account
16/08/2018	?	Several Financial Institutions	Proofpoint researchers discover a new downloader malware in a fairly large campaign (millions of messages) primarily targeting financial institutions. The malware, dubbed "Marap" ("param" backwards), is notable for its focused functionality that includes the ability to download other modules and payloads.	Malware/
17/08/2018	?	Eastern Maine Community College	Eastern Maine Community College in Bangor warns of a possible data breach that could have	Malware/

Date	Author	Target	Description	
			exposed the personal information of current and former staff and students. School officials notify 42,000 current and former students and employees that certain computers were recently infected with malware and may have been hacked. Officials said the problem could apply to students dating back to 1998, and faculty dating to 2008.	
17/08/2018	?	Individual Users	Researchers from Trustwave Spiderlabs and Cofense reveal the details of a malicious spam campaign, targeting the banking industry, and using unusual Microsoft Publisher documents, originating from the Necurs botnet.	Malware/
17/08/2018	?	Compromised Wordpress Sites	Researchers from Sucuri uncover a malicious campaign targeting up to 3,000 infected Wordpress sites, carried out via a URL shortener, a fake plug-in and a malicious popuplink.js.	Malicious
18/08/2018	?	David Min	Reuters reveals that the U.S. Federal Bureau of Investigation is investigating a cyber attack on the congressional campaign of David Min, a Democratic candidate in California.	Targeted
18/08/2018	?	Bossier City	Some Bossier City water customers may have had their information compromised due to a possible breach of an online billing payment system.	Malware/
20/08/2018	?	Legacy Health	Legacy Health notifies 38,000 patients that a phishing attack may have breached their data. Officials discovered unauthorized access to some employee email accounts on June 21. However, the access began several weeks before in May 2018.	Account
20/08/2018	?	Superdrug	Superdrug confirms that hackers claim to have obtained the personal details of almost 20,000 individuals who shopped online at Superdrug.	Credentia
20/08/2018	?	Single Individuals	A new malicious spam campaign is underway that pretends to be an invoice for an outstanding payment. When these invoices are opened they install the AZORult information stealing Trojan and the Hermes 2.1 Ransomware onto the recipient's computer.	Malware/
20/08/2018	?	South Korean users	Researchers from Trend Micro discover a malicious spam	Malware/

Date	Author	Target	Description	
			campaign targeting South Korean users, carried out distributing the GrandCrab ransomware through files with .egg extension.	
20/08/2018	?	Animoto	Animoto, a cloud-based video maker service for social media sites, reveals a data breach. The breach occurred on July 10 but was confirmed by the company in early August, and later reported to the California attorney general. Names, dates of birth and user email addresses were accessed by hackers	Unknowr
21/08/2018	APT28 AKA Fancy Bear	U.S. Senate, two conservative think tanks and Microsoft's OneDrive cloud storage	Microsoft claims it thwarted a Russian-backed phishing attack by seizing control of fake copies of right-leaning American think tanks' websites – including one led by a prominent Donald Trump critic.	Account
21/08/2018	Malicious actors from Iran	US, UK, Middle East and Latin America	FireEye identifies a suspected influence operation that appears to originate from Iran aimed at audiences in the U.S., U.K., Latin America, and the Middle East. This operation leverages a network of inauthentic news sites and clusters of associated accounts across multiple social media platforms to promote political narratives in line with Iranian interests.	Fake Nev Network
21/08/2018	?	Organizations in South Korea	Researchers from Trend Micro and IssueMakersLab uncover the details of Operation Red Signature, an information theft-driven supply chain attack targeting organizations in South Korea. The threat actors compromised the update server of a remote support solutions provider to deliver a remote access tool called 9002 RAT.	Targeted
21/08/2018	?	Several Organizations Worldwide	Researchers from Check Point reveal the details of Ryuk, a new ransomware strain able to net over $640,000 worth of Bitcoin in a recent activity surge.	Malware/
21/08/2018	?	Mexican Individuals	Researchers from Kaspersky Lab reveal the details of Dark Tequila, a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars.	Malware/

Date	Author	Target	Description	
22/08/2018	Lazarus Group	Undisclosed cryptocurrency Exchange	Kaspersky Lab reveals the details of Operation AppleJeus, an attack against cryptocurrency exchanges carried out via a trojanized cryptocurrency trading application distributing the Fallchill malware.	Targeted
22/08/2018	?	Cheddar Scratch Kitchen	Restaurants in 23 states belonging to Cheddar Scratch Kitchen are affected by a cyberattack that exposed payment card information. The amount of impacted card details is estimated to be 567,000 and were stolen between November 3, 2017, and January 2, 2018, the cybercriminals accessed the Cheddar Scratch Kitchen network.	Malware/
22/08/2018	Turla AKA Snake AKA Uroburos	Foreign offices of two European countries Network of a major defense contractor	Researchers from ESET reveal that three more entities have been hit by the infamous Turla APT.	Targeted
22/08/2018	?	Six Banks in Spain	Researchers from IBM X-Force reveal that the relatively new trojan BackSwap is now targeting six banks in Spain.	Malware/
22/08/2018	?	Vulnerable Wordpress Sites	Researchers from Sucuri uncover what they describe as a massive WordPress redirecting campaign targeting vulnerable tagDiv themes and Ultimate Member plugins.	Malicious
23/08/2018	?	T-Mobile	T-Mobile reveals that hackers stole some of the personal data of 2 million people in a new data breach. The intrusion took place on August 20 when hackers part of “an international group” accessed company servers through an API that “didn’t contain any financial data or other very sensitive data.	Illegitima
23/08/2018	?	Vulnerable IoT devices	Researchers from Symantec discover another Mirai variant leveraging the Aboriginal Linux open source project to infect multiple devices.	Malware/
23/08/2018	?	Android Users	Security researchers from Bitdefender discover a new Android spyware framework dubbed Triout that could be used to create malware with extensive surveillance capabilities.	Malware/
24/08/2018	TA555	Single Individuals	Researchers from Proofpoint discover a new malicious spam campaign carried on via a previously undocumented downloader called AdvisorsBot.	Malware/
24/08/2018	COBALT DICKENS	76 universities located in 14	Secureworks Counter Threat Unit	Account

Date	Author	Target	Description	
		countries	(CTU) researchers discover a URL spoofing campaign carried out by Iranian actors. The campaign involves Sixteen domains contained over 300 spoofed websites and login pages for 76 universities located in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States.	
24/08/2018	?	Vulnerable Apache Struts Servers	Greynoise Intelligence and Volexity, say they've detected threat actors scanning for Struts servers vulnerability CVE-2018-11776.	Vulnerab
26/08/2018	Anonymous Catalonia	Banco de España	Hacktivists from Anonymous Catalonia claim to have taken down the website of Banco de España.	DDoS
27/08/2018	?	Atlas	Atlas, a popular Brazilian cryptocurrency investment platform is hacked. The personal information of over 264,000 of its customers is leaked, including 4,500 records that detail users' balances on the platform.	Unknown
28/08/2018		Huazhu Group Ltd.	Shanghai police launches an investigation into the alleged massive data breach of Huazhu Group Ltd., one of China's largest hotel operators. An online post emerges, containing nearly 500 million pieces of information related to the hotel group's customers, including registration information, personal data and booking records of the group's wide range of hotel brands.	Unknown
28/08/2018	L.M.	TheTruthSpy	A hacker breaks into the servers of TheTruthSpy, one of the most notorious stalkerware companies out there, and stole logins, audio recordings, pictures, and text messages, among other data. The breach occurred on February 2018.	App Vuln
28/08/2018	?	Single Individuals	A new malicious spam campaign is underway that pretends to be shipping documents and contains an attachment that installs the DarkComet remote access Trojan	Malware/
28/08/2018	?	Multiple Targets	Security researchers from Booz Allen Hamilton discover RtPOS, a previously unseen and undocumented malware strain that targets point-of-sale (POS) systems.	Malware/
29/08/2018	?	Air Canada	Air Canada says the personal	Unknown

Date	Author	Target	Description	
			information for about 20,000 customers "may potentially have been improperly accessed" via a breach in its mobile app, so the company has locked down all 1.7 million accounts as a precaution until customers change their passwords. The airline detected unusual log inbehavior with Air Canada's mobile App between Aug. 22 24,2018.	
29/08/2018	?	Android Users	Researchers from Doctor Web find dozens of malicious applications on Google Play designed to generate illegal revenue. Authors of these applications spread them under the guise of well-known and useful software and use them in different fraudulent schemes.	Malware/
29/08/2018	?	Android Users	Researchers from Kaspersky Lab reveal the detail of BusyGasper, a new, unsophisticated Android Spyware.	Malware/
29/08/2018	?	University of Missouri	The University of Missouri suspends email delivery after a Missouri State Democratic Party email seeking interns helps jumpstart a phishing attempt.	Account
29/08/2018	?	University of Oregon	University of Oregon is target of a phishing campaign.	Account
29/08/2018	?	West Vancouver	West Vancouver warns thousands of its residents after discovering hackers installed malicious software on the district server used to store personal information collected through its website. The attack was discovered on July 31.	Malware/
29/08/2018	?	Cloquet School District	Cloquet school district is hit by a ransomware attack second time in the past three years.	Malware/
30/08/2018	?	Sweden	The Swedish Security Service reveals that there has been a proliferation of new “bots” on Twitter supporting the nationalist, anti-immigration Sweden Democrats and attacking the ruling Social Democrats.	Twitter B
30/08/2018	Cobalt AKA TEMP.Metastrike	NS Bank Patria Bank	Researchers from NetScout Arbor reveal the details of a new campaign carried out by the Cobalt Group via spear phishing.	Targeted
30/08/2018	?	Family Orbit	An anonymous hacker is able to find the key to the cloud servers of Family Orbit and leaks 281 Gb of pictures and videos.	Account
30/08/2018	?	Vulnerable Magento Servers	The MagentoCore Skimmer campaign reveals all its extent. A single group is responsible for	Malware/

Date	Author	Target	Description	
			planting skimmers on 7339 individual stores in the last 6 months.	
30/08/2018	?	Individuals in China	Researchers from Check Point uncover a new ongoing campaign aimed to distribute the CEIDPageLock browser hijacker, distributed via the RIG Exploit Kit. The victims are located primarily in China.	Malware/
30/08/2018	?	Single Individuals	Researchers from Symantec uncover a new attack chain which exploits the Windows Management Instrumentation Command-line (WMIC) utility and eXtensible Stylesheet Language (XSL) files to be undetected and steal data.	Malware/
30/08/2018	?	Single Individuals	Researchers from Cisco Talos warn of a Chinese-language threat actor leveraging a wide array of Git repositories to infect vulnerable systems with Monero-based cryptomining malware.	Malware/
31/08/2018	?	Americans with access to government and commercial secrets	William Evanina, the U.S. counter-intelligence chief reveals that Chinese espionage agencies are using fake LinkedIn accounts to try to recruit Americans with access to government and commercial secrets.	LinkedIn
17/08/2018	?	Dallas County Community College	Dallas County Community College discloses a breach after some employees' emails credentials are compromised by a phishing attack from September 14, 2017 to December 18, 2017.	Account
24/08/2018	?	Schneider Electric	Schneider Electric finds a malicious code on the USB drives that have been shipped with Conext ComBox and Conext Battery Monitor products.	Malware/
24/08/2018	?	Coweta County	Coweta County restores most of its computer servers, nearly two weeks after hackers demanded $341,000 in bitcoins.	Malware/
29/08/2018	GOBLIN PANDA	Vietnam	Researchers from security firm CrowdStrike have observed a new campaign associated with the GOBLIN PANDA APT group, targeting Vietnam via a spear phishing campaign using weaponized documents.	Targeted
30/08/2018	"@joshua" from group Fatal Error Crew	C&A	The Brazilian operation of international fashion retail clothing chain C&A confirms a cyberattack to its gift card platform. Data from 36,000	Unknown

Date	Author	Target	Description	
			customers who purchased gift cards is leaked on Pastebin.	
01/09/2018	?	Town of Midland	The small Canadian town of Midland, Ontario plans to pay off a $35,000 ransom to the malicious actors who shut down the municipalities compute system with a ransomware attack.	Malware/
02/09/2018	?	Single Individuals	Researchers discover a new ransomware that only encrypts .EXE files on a computer. It then displays a screen with a picture of President Obama that asks for a "tip" to decrypt the files.	Malware/
03/09/2018	?	South African Department of Labour	The South African Department of Labour confirms a DDoS attack which disrupted the government agency's website.	DDoS
03/09/2018	?	Vulnerable IoT devices	A new IoT botnet called Hakai comes out online.	Malware/
03/09/2018	?	Hoopeston Area School District	The Hoopeston Area School District website is hacked with pictures and repeated emergency callout messages to district families.	Unknown
03/09/2018	?	Hoopeston Area School District	The Hoopeston Area School District website is hacked with pictures and repeated emergency callout messages to district families.	Unknown
04/09/2018	?	Vulnerable Apache Struts 2 servers	Researchers from F5 detected threat actors exploiting the CVE-2018-11776 Apache Struts 2 namespace vulnerability in a new Monero crypto-mining campaign.	Apache S
04/09/2018	?	Mega.nz	The official Chrome extension for the MEGA.nz file sharing service is compromised with malicious code that steals usernames and passwords, but also private keys for cryptocurrency accounts	Malware/
04/09/2018	?	Major Brazilian banks	IBM X-Force researchers discover a new financial malware that targets major Brazilian banks through their customers. The malware is dubbed CamuBot because it attempts to camouflage itself as a security module required by the banks it targets.	Malware/
04/09/2018	Iran-Linked OilRig APT	Undisclosed government in the Middle East	Researchers from Palo Alto Networks Unit 42 report on a wave of OilRig attacks delivering the OopsIE trojan involving a Middle Eastern government agency.	Targeted
04/09/2018	Fatal Error	Boa Vista SCPC	Brazilian credit bureau Boa Vista SCPC investigates a possible	Unknown

Date	Author	Target	Description	
			hack, after a group of hackers called Fatal Error claimed it accessed the database of the company which has more than 350M personal data.	
05/09/2018	Silence	Financial institutions in Russia and Eastern Europe.	Researchers from Group-IB reveal the details of a new Russian-speaking "Silence" group, having spent the last three years mounting silent cyber-attacks on financial institutions in Russia and Eastern Europe, stealing $800,000.	Targeted
05/09/2018	FIN6	PoS systems across the United States and Europe.	Researchers from IBM X-Force IRIS uncover a new malware campaign targeting point-of-sale (PoS) systems across the United States and Europe. The attacks have been attributed to the FIN6 cybercriminal group.	Malware/
05/09/2018	rogue0	Rousseau	Rousseau, the online platform of the Italian Five Star Movement is hacked again by rogue0, who leaks private data related to the donors.	Unknown
06/09/2018	Magecart Group	British Airways	British Airways notifies authorities, after being hacked between August 21 and September 5, with 380,000 payments compromised.	Malicious
06/09/2018	PowerPool	Targets in Chile, Germany, India, Philippines, Poland, Russia, United Kingdom, United States, and Ukraine.	Researchers from ESET identify a group dubbed PowerPool exploiting the recently discovered Windows ALPC LPE 0-day vulnerability.	Malware/
06/09/2018	?	Cork City Park by Phone	A data breach at Cork City Park by Phone service in Ireland affects more than 5,000 people. The unauthorized access started in May.	Unknown
06/09/2018	?	Victims in the Middle East, Asia Pacific, and Southern Europe	Researchers from FireEye report a new Exploit Kit, dubbed Fallout, used to deliver GandCrab to victims in the Middle East, while also targeting the Asia Pacific region and Southern Europe with additional malware.	Malware/
07/09/2018	Domestic Kitten	240 individuals from Iran including Kurdish and Turkish natives and ISIS supporters	Researchers from Check Point uncover a mobile-based attack targeting Iranian citizens that operates under the radar of detection since 2016.	Targeted
07/09/2018	?	U.S. State Department	The State Department suffers a breach of its unclassified email system, and the compromise exposes the personal information of a small number of employees.	Targeted
07/09/2018	Big Bang	Palestinian Authority and other targets in the Middle	Researchers from Check Point detect a new surveillance attack	Targeted

Date	Author	Target	Description	
		East.	carried out by the Big Bang gang against the Palestinian Authority and other targets in the Middle East.	
09/09/2018	?	C-CEX	Cryptocurrency exchange C-CEX is hacked. The attackers are successfully able to withdraw all Litecoin (LTC) and Dogecoin (DOGE) from company servers.	Vulnerab
09/09/2018	?	Vulnerable Apache Struts 2 servers	Researchers from Palo Alto Networks, for the first time discover a variant of the Mirai Internet of Things botnet that targets Apache Struts CVE-2017-5638 vulnerability.	Malware/
09/09/2018	?	Vulnerable versions of the Global Management System (GMS) from SonicWall	The same researchers from Palo Alto Networks reveal a new version of the Gafgyt botnet (AKA Bashlite), targeting versions of the Global Management System (GMS) from SonicWall vulnerable to CVE-2018-9866.	Malware/
10/09/2018	?	Vulnerable MikroTik Routers	Researchers find an additional 3,700 MikroTik routers running injecting CoinHive in secret. The total number of compromised devices detected exceeds 280,000, an increase of 80,000 in just over 30 days.	MikroTik (CVE-201
10/09/2018	runningsnail	DEOSGames	Betting platform DEOSGames is drained of a significant chunk of its operating funds in a heist that netted one ‘lucky’ punter almost $24,000.	EOS Vuln
10/09/2018	?	European countries particularly France	Researchers from Trend Micro spot a ransomware imitating Locky, dubbed PyLocky, characterize by strong evasion capabilities, and being spread via spam emails targeting European countries particularly France.	Malware/
10/09/2018	LuckyMouse	Multiple Targets	Kaspersky Lab discovers several infections from a previously unknown Trojan, likely related to the infamous Chinese-speaking threat actor – LuckyMouse. The most peculiar trait of this malware is its driver, signed with a legitimate digital certificate.	Targeted
10/09/2018	?	Vulnerable MikroTik Routers	Security researcher Troy Mursch reveal that the infected MikroTik routers abused for the CoinHive redirection campaign, are now abused for a new cryptojacking operation.	MikroTik (CVE-201
10/09/2018	?	FreshMenu	The Indian online food platform FreshMenu admits to have hidden a data breach affecting 110K users for two years. The data	Unknown

Date	Author	Target	Description	
			breach happened on July 1, 2016	
11/09/2018	Cobalt	Russian and Romanian banking customers	Researchers from ProofPoint reveal that the Cobalt Gang cybercrime group has launched a new round of phishing campaigns targeting primarily Russian and Romanian banking customers with CobInt, a recently discovered malicious backdoor and downloader.	Malware/
11/09/2018	Cobalt	Remotely accessible and unprotected MongoDB databases	A new attack called Mongo Lock is discovered. The new attack targets remotely accessible and unprotected MongoDB databases, wiping them, and then demanding a ransom in order to get the contents back.	Misconfig
11/09/2018	?	Vulnerable Wordpress Sites	Researchers from security firm Defiant reveal an uptick in scan attempts for Wordpress installations with the vulnerable plugin Duplicator.	Wordpres
11/09/2018	?	University of Louisville	Nearly 250 University of Louisville faculty and staff enrolled between 2007 and 2014 have their personal info stolen through the “Get Healthy Now” program.	Unknown
11/09/2018	?	Pakistani WhatsApp users	WhatsApp accounts of multiple Pakistani citizens are hacked by an anonymous group of hackers asking for money to get their accounts back.	Account
11/09/2018	?	City of Tyler	The city of Tyler is the latest victim of the Click2Gov payment system breach.	Vulnerab
12/09/2018	Magecart Group	Feedify	Customer engagement service Feedify is hit by Magecart attackers, who repeatedly modified a script that it serves to a few hundred websites to include payment card skimming code.	Malicious
12/09/2018	?	Edinburgh University (ed.ac.uk)	The website of Edinburgh University is down after the institution suffered a major DDoS attack.	DDoS
12/09/2018	?	Monroe County School District	A GandCrab ransomware attack forces Monroe County School District in Florida to shut down its computer systems for at least three days.	Malware/
12/09/2018	?	Users of the Jaxx cryptocurrency wallet site	Researchers from Flashpoint take down a website spoofing the official Jaxx cryptocurrency wallet site after discovering a number of infections linked to the operation.	Malware/
12/09/2018	Iran-Linked OilRig APT	Undisclosed government in	Researchers from Palo Alto	Targeted

Date	Author	Target	Description	
		the Middle East	Networks' Unit 42 uncover a new campaign by the OilRig APT targeting members of an undisclosed government in the Middle East with an evolved variant of the BondUpdater trojan.	
13/09/2018	?	Single Individuals	ESET researchers discover three third-party add-ons for the popular open-source media player Kodi (XvBMC, Bubbles and Gaia), being used to distribute Linux and Windows Monero cryptocurrency-mining malware.	Malware/
13/09/2018	?	Fetal Diagnostic Institute of the Pacific (FDIP)	Honolulu-based Fetal Diagnostic Institute of the Pacific (FDIP) announces to have been hit by a ransomware attack that may have compromised patient data.	Malware/
13/09/2018	APT10	Japanese media sector	Researchers from FireEye reveal a new campaign carried out by the Chinese APT10 group, targeting the Japanese media sector via the UPPERCUT backdoor.	Targeted
13/09/2018	?	Single Individuals	A huge database with 42M email addresses, passwords in clear text, and partial credit card data is uploaded to kayo.moe, a free, public hosting service.	Unknown
14/09/2018	aabbccddeefg	EOSBet	A gambling application that is based on the EOS blockchain has a flaw in its smart contract system exploited. The attacker is able to make off with $200,000 worth of EOS due to the vulnerability.	DEOS Vu
14/09/2018	?	Bristol Airport	Flight information screens are blacked out over the weekend at the Bristol Airport. Airport officials blame the incident on a ransomware infection that affected the computers running the airport's in-house TV.	Malware/
14/09/2018	?	Colorado Timberline	Colorado Timberline, a Colorado printing company claims to have been forced out of business after being hit with a severe ransomware attack from which it could not recover.	Malware/
14/09/2018	?	Victims in Japan, France, and other locations	The Fallout Exploit KIT starts to distribute a new ransomware called SAVEfile via malicious spam campaigns.	Malware/
14/09/2018	?	Guardant Health	Guardant Health suffered a phishing attack in July 2018 according to an SEC filing for the firm's initial public offering, where private information from about 1,100 individuals was compromised.	Account

Date	Author	Target	Description	
14/09/2018	LulzSecITA	Italian National Institute for Social Assistance (INAS)	The portal of the Italian National Institute for Social Assistance (INAS) is hacked, compromising the information of 37,500 individuals.	Unknown
12/09/2018	?	SMEG UK	The UK branch of the appliance manufacturer SMEG reveals to have been hit by a "targeted cyber attack".	Unknown
14/09/2018	Magecart	Groopdealz	Groopdealz joins the list of the victims of the Magecart group.	Malware/
17/09/2018	?	Saverspy.com	Bob Diachenko, a security researcher, identifies an unsecured MongoDB server leaking the personal details of nearly 11 million users. The database seems to have been ransomed back in June.	Unsecure
17/09/2018	LulzSecITA	Unuci.org (Union of Italian Retired Military Officials)	LulzSecITA leaks the personal details of about 300 retired military officials.	Unknown
17/09/2018	Iron cybercrime group (AKA Roke)	Vulnerable Windows and Linux Servers	Researchers from Palo Alto Networks discover a new malware strain dubbed XBash that combines features from four types of malware categories: ransomware, coinminers, botnets, and worms.	Malware/
17/09/2018	?	Multiple targets	Researchers from Qihoo's 360Netlab discover Fbot, a strange botnet based on Satori, which instead of infecting devices, appears to be actually wiping them clean of cryptocurrency mining malware. The botnet also hides its C&C behind a blockchain-based DNS service.	Malware/
17/09/2018	?	Perth Mint	A data breach at Perth Mint sees hackers take the personal details of about 3200 customers, far more than initially suspected. The breach occurred on the system of a third-party technology provider and only involved 13 customer initially.	Unknown
17/09/2018	?	Multiple government websites in India.	Security researchers discover that multiple government websites in the country are infected with cryptojackers.	Malware/
17/09/2018	?	Nonresident aliens in the U.S.	Researchers at Fortinet discover a phishing campaign claiming to be from the IRS but reportedly sent from a server originating in Italy. The campaign appears to be targeting nonresident aliens.	Account
18/09/2018	Magecart	ABS-CBN	213 customers of ABS-CBN, a Filipino media conglomerate, have	Malware/

Date	Author	Target	Description	
			their financial data stolen data due to a payment skimmer discovered in the broadcaster's online store.	
18/09/2018	?	45 countries, including the US, France, Canada, Switzerland, and the UK	A report published by Citizen Lab researchers reveals the existence of 36 different groups who deployed the Pegasus spyware against targets located in 45 countries, including the US, France, Canada, Switzerland, and the UK.	Malware/
19/09/2018	Magecart	Newegg	Researchers from RiskIQ, together with Volexity, reveal that California-based retailer Newegg is the latest well-known merchant to succumb to the Magecart group.	Malware/
19/09/2018	?	Click2Gov	FireEye has revealed reveals that a yet-to-be-identified hacker group is behind the hack against the Click2Gov servers, used to plant malware that stole payment card details.	Malware/
19/09/2018	?	3,000 breached websites	Researchers from Flashpoint reveal that hackers are selling access to over 3,000 breached websites on an underground hacking forum called MagBO for Russian-speaking users.	Unknown
19/09/2018	?	Android Users	ESET researchers discover malicious apps impersonating various financial services and the Austrian cryptocurrency exchange Bitpanda on Google Play.	Malware/
19/09/2018	?	City of Beatrice	A virus shuts down many city operations including phone and internet services for several departments.	Malware/
20/09/2018	?	Zaif	Yet another Japan-based cryptocurrency exchange is hacked, losing a 6.7 billion yen (about $60 million worth of cryptocurrency), including 5,966 bitcoins.	Unknown
20/09/2018	?	Port of Barcelona	The land operations of the Port of Barcelona are impacted by a ransomware attack.	Malware/
20/09/2018	?	Multiple platforms	Security researchers discover a new botnet dubbed Torii, able to infect multiple hardware platforms. The botnets has no clear purpose.	Malware/
20/09/2018	?	Vulnerable Wordpress Systems	Researchers from Malwarebytes reveal a massive campaign compromising vulnerable WordPress sites and redirecting users to tech scams.	Malicious

Date	Author	Target	Description	
20/09/2018	?	Arran Brewery	Arran Brewery says it was locked out of its own computer system after being duped into opening an email attachment that contained a ransomware. The attackers then demanded a 2BTC ransom.	Malware/
20/09/2018	Lucy Gang	Multiple Targets	Researchers uncover a new Russian-speaking threat actor hawking a proprietary cyber-weapon, malware-as-a-service, dubbed “Black Rose Lucy.”	Malware/
21/09/2018	?	Some European Countries	Researchers from ESET discover a new DanaBot campaign targeting a number of European countries.	Malware/
21/09/2018	?	AdGuard	AdGuard, a popular ad blocker for Android, iOS, Windows, and Mac, resets all user passwords, after suffering a brute-force attack during which an unknown attacker tried to log into user accounts by guessing their passwords.	Credentia
21/09/2018	?	Infinite Campus	Infinite Campus, one of the largest student information management systems used by schools in America, is coping with the latest in a string of Distributed Denial-of-Service (DDoS) attacks.	DDoS
21/09/2018	?	freelance workers	MalwareHunterTeam discovers a new campaign targeting freelance workers spreading malware via malicious documents masquerading as job briefs and offers.	Malware/
21/09/2018	?	Single Individuals	Researchers from Trend Micro reveal the detail of Virobot, a multi-strain malware working as ransomware, keylogger, and botnet.	Malware/
21/09/2018	?	Bryan Caforio’s website	A DDoS attack takes down California Democratic Bryan Caforio’s website just hours before he steps onto the debate stage to face fellow Democrats.	DDoS
24/09/2018	?	Android Users	Researchers from Sophos discover two-dozen Android apps able to urns users' phones into cryptocurrency miners. Combined, they have been downloaded more than 120,000 times.	Malware/
24/09/2018	?	Targets in Turkey	Researchers from Cisco Talos and ReversingLabs reveal the detail of a new spam campaign spreading the Adwind 3.0 remote access tool (RAT).	Malware/
24/09/2018	?	Oklahoma City Public School District	The Oklahoma City Public School District is affected by a DDoS attack on their parent portal.	DDoS

Date	Author	Target	Description	
25/09/2018	?	Port of San Diego	Service to the public in the Port of San Diego are impacted by a ransomware attack.	Malware/
25/09/2018	?	NewsNow	Online news aggregation service NewsNow admits that it has suffered a security breach and an encrypted version of the passwords may have been accessed.	Unknown
25/09/2018	?	Doordash	Food delivery startup DoorDash receives dozens of complaints from customers who say their accounts have been hacked. The users are the target of a credential stuffing attack.	Credentia
25/09/2018	?	Chegg	Educational technology company Chegg resets the passwords for 40 million of its users after news broke that the firm was breached in April of this year.	Unknown
25/09/2018	?	RWE	Unknown attackers launch a large-scale DDoS attack that takes down RWE's website.	DDoS
25/09/2018	?	Aspire Health	Aspire Health, is hacked earlier this month and loses at least some patient information to an unknown cyber attacker.	Unknown
26/09/2018	?	pigeoncoin	The developers behind the pigeoncoin cryptocurrency confirm that an unknown attacker successfully took advantage of a bitcoin bug, printing 235 million pigeoncoins worth about $15,000.	Bitcoin V
26/09/2018	?	Several Android Users in Europe	Researcher Lukas Stefanenko from ESET reveals the details of a malicious app impersonating a phone call recording utility in Google Play Store (Qrecorder) able to steal thousands of euros from a couple of bank customers in Europe.	Malware/
26/09/2018	?	Multiple businesses in the city of Conway	Multiple businesses in Conway, Arkansas, are hit by ransomware.	Malware/
27/09/2018	?	Facebook	Facebook says a breach affected 50 million people on the social network. The vulnerability stemmed from the "view as" feature, which lets people see what their profiles look like to others. Attackers exploited code associated with the feature that allowed them to steal access tokens.	"view as"
27/09/2018	APT28 (AKA Fancy Bear, Sednit, Strontium, and Sofacy)	Undisclosed Target	Researchers from ESET find the first evidence of a rootkit, called LoJax, for the Unified Extensible Firmware Interface (UEFI) being	Targeted

Date	Author	Target	Description	
			used in the wild by the infamous APT28.	
27/09/2018	Malicious Actors from North Korea?	Politically-motivated victims in Eurasia and Southeast Asia.	Researchers from Palo Alto Networks publish an analysis of NOKKI, a new RAT named so because of the significant links with KONNI, a previously discovered threat. The operation shows similarities with the modus operandi of Reaper, a malicious actor tied to North Korea.	Targeted
27/09/2018	?	Vulnerable RDP servers	The Internet Crime Complaint Center (IC3), in collaboration with the Department of Homeland Security and the FBI, issues a security alert regarding attacks being conducted through the Windows Remote Desktop Protocol.	RDP Vulr Misconfig
27/09/2018	Cobalt	High-value financial organizations around the world	Researchers from the Secureworks Counter Threat Unit (CTU) disclose the latest operation of the Cobalt threat actor, targeting high-value financial organizations around the world through the SpicyOmelette malware.	Targeted
27/09/2018	?	Single Individuals	Researchers discover a new campaign aimed to distribute the GandCrab ransomware via the Phorpiex worm.	Malware/
28/09/2018	?	Single Individuals	Motherboard reveals that hackers have hijacked the accounts of at least four high profile Instagrammers recently, locking them out and demanding a bitcoin ransom.	Account
28/09/2018	?	SHEIN	A criminal cyber-attack is thought to have affected roughly 6.42 million customers of fashion brand SHEIN. The attack took place on August 22, and gained access to email addresses and encrypted password credentials of customers who registered on the company website.	Malware/
28/09/2018	?	Toyota Industries North America	Toyota Industries North America notifies individuals of a phishing incident, potentially impacting approximately 19,000 current/ former employees and health plan participants.	Account
28/09/2018	?	Recipe Unlimited	Recipe Unlimited, a Canadian restaurant chain that operates over 20 restaurant brands, suffers a country-wide outage of its IT systems over the weekend in a ransomware incident.	Malware/
28/09/2018	?	Developers of Google Chrome	Developers of Google Chrome	Account

Date	Author	Target	Description	
		extensions	extensions are targeted by a massive phishing campaign.	
29/09/2018	CyberSecurity & Intelligence (CSI)	Virat Kohli’s official website	Following the defeat of the Bangladeshi cricket team against India at the 2018 Asia Cup final, a group of Bangladeshi hackers defaces Virat Kohli’s official website (the current captain of India's team) to protest against an 'unfair decision' during the match.	Defacem
29/09/2018	?	Customers of Brazilian Banks	Security researchers from Qihoo 360 NetLab uncover an ongoing hacking campaign leveraging the GhostDNS malware. Attackers have already hijacked over 100,000 home routers (70+ types). The malicious code allows to modify DNS settings to hijack the traffic and redirect users to phishing websites.	Malware/
29/09/2018	baidu3250617231	Gwinnett Medical Center (GMC)	Gwinnett Medical Center(GMC) is hacked and the patient data is posted online.	Unknown
30/09/2018	FIN7	Burgerville	Burgerville reveals a data breach impacting the chain which may have led to the theft of detailed credit card information belonging to customers.	Malware/