Cybersecurity threatscape

Q4 2019

ptsecurity.com

Contents

Symbols used

Attack targets


Computers, servers, and network equipment


Web resources


Humans


POS terminals and ATMs


Mobile devices


IoT

Attack methods


Malware use


Credential compromise


Social engineering


Hacking


Web attacks

Victim categories


Finance


Government


Healthcare


Science and education


Military


Industrial companies


Online services


Hospitality and entertainment


Transportation


IT

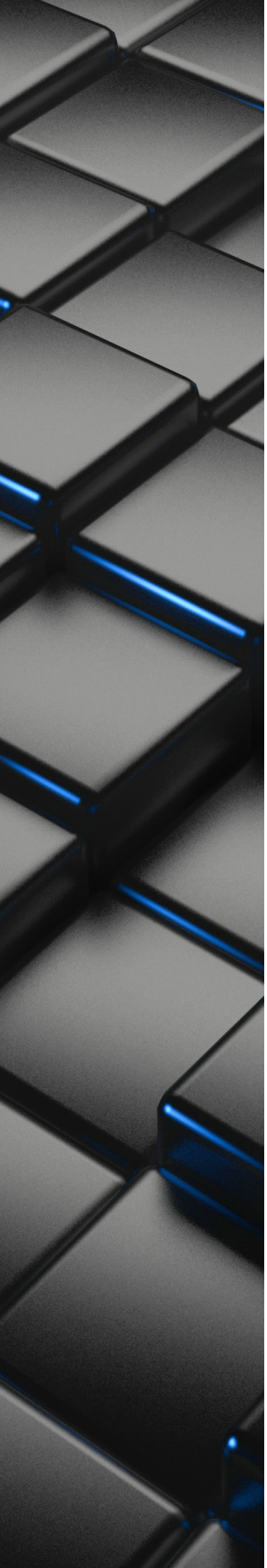

Retail


Individuals


Telecom


Blockchain


Other



Executive summary

Highlights of Q4 2019 include:

- Unique cyberincidents are growing, with a 12-percent increase in their number compared to the previous quarter.
- The share of targeted attacks increased by 2 percentage points versus the previous quarter, to 67 percent. This is due to a large number of APT attacks against individual organizations and entire industries.
- There were 11 very active groups. Their attacks targeted mostly government institutions, industry, and finance.
- Payment card information comprised a third of all data stolen from organizations (32%). This is 25 percentage points more than in the previous quarter. We believe the reason for this increase to be two-fold: the busy winter holiday purchasing season, plus the progressively growing number of MageCart attacks coupled with the second wave of attacks on Click2Gov.
- Ransomware attacks are highly dangerous. The share of such attacks among malware infections was 36 percent for organizations and 17 percent for individuals (in the previous quarter, these were 27% and 7%, respectively).
- A new trend in ransomware is to publish the stolen information if the victim refuses to pay up. We believe this is because more and more companies back up their data and have no need to pay for decryption. Malefactors are adjusting accordingly, and now threaten their victims with all the potential consequences of disclosure of personal data, which is subject to the protections of the European Union's General Data Protection Regulation (GDPR).

Statistics

In the last quarter of 2019 the percentage of attacks aimed at data theft and attacks for direct financial gain remained practically the same as in the previous quarter.

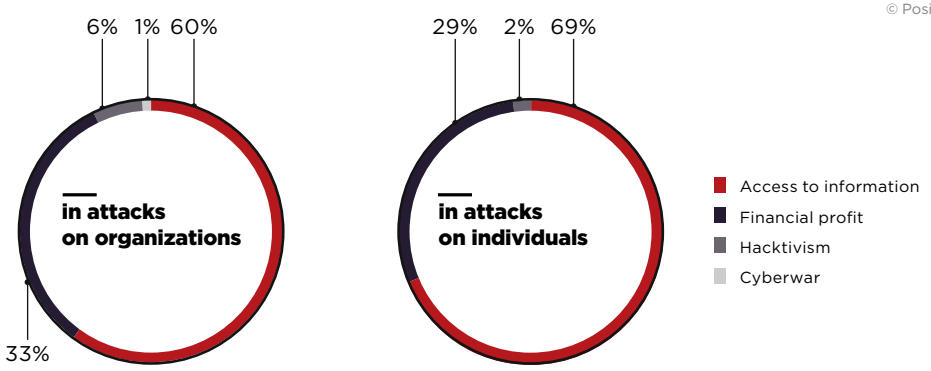


Figure 1. Attackers' motives

In the last quarter of 2019, payment card information made up a third (32%) of all information stolen from organizations. This is several times more than in the previous quarter (7%). This was to be expected. On the one hand, people make a lot of online purchases in the run-up to the winter holidays. On the other hand, this jump is related to the rapidly growing number of MageCart attacks on thousands of online stores, combined with a second wave of attacks on the Click2Gov service used by many Americans to pay their utility bills.

The percentage of attacks on individuals fell almost by half versus the previous quarter, and is now only 10 percent of all attacks. Credentials make almost half (40%) of all data stolen from individuals, same as in the previous quarter. One of the common ways of tricking users into disclosing their credentials is a phishing email with link to a fake log-in page. But email security gateway can block the link, which forces attackers to invent new schemes. For instance, instead of a link, they can attach an HTML file which is supposedly a payment document. If the user opens that file, JavaScript inside generates an authentication form in the user's browser, without any suspicious redirections to a different site. When the credentials are entered, the script sends the credentials to the attackers.

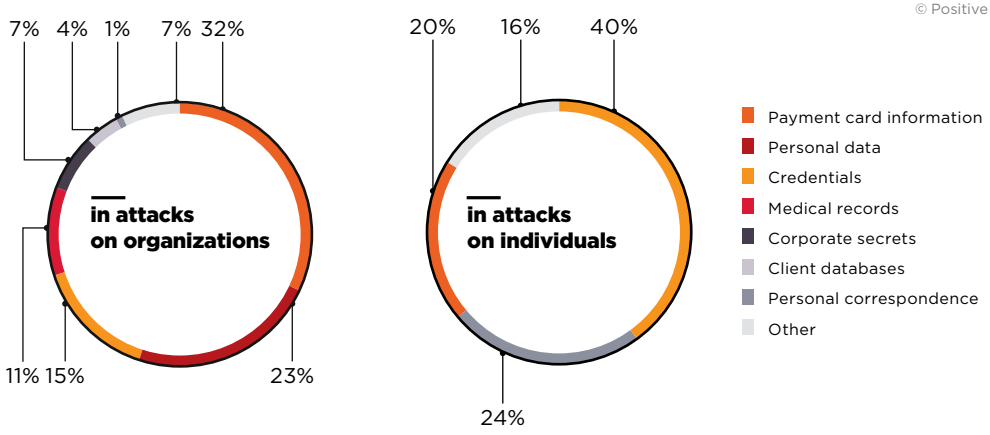


Figure 2. Types of data stolen

The percentage of targeted attacks remains high. Two-thirds of attacks (67%) were targeted. Hackers attacked specific companies or an industry of interest. As a result, we see fewer attacks in the "multiple industries" category (26 percent in early 2019 vs. 14 percent at year-end).

The list of the top five target industries remains stable: government, industry, healthcare, finance, and education. At the same time, we see a two-fold increase in attacks on IT companies and retail. We will talk about high-profile attacks of this kind later on.

Blockchains became less popular as a target as the year went on, approaching just 1 percent. But this does not mean that cryptowallet owners are free from danger. For instance, the site of the Monero cryptocurrency was compromised in the last quarter of 2019. Attackers uploaded malware masked as a legitimate cryptocurrency wallet. One user reportedly lost $7,000 in the attack.

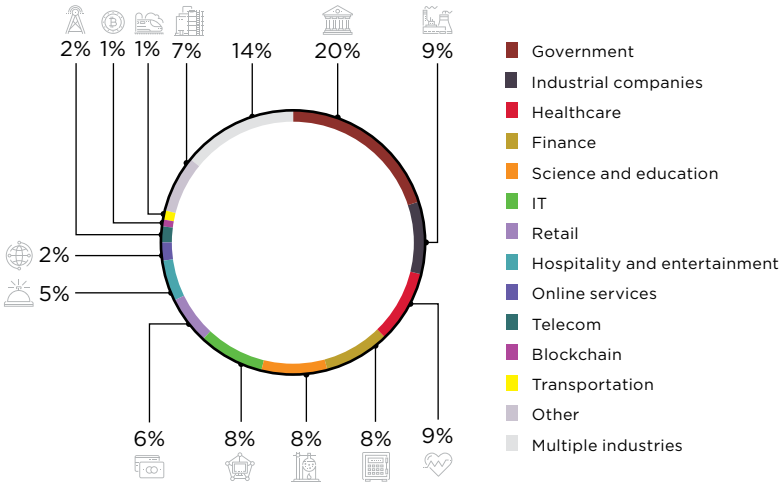


Figure 3. Victim categories among organizations

In almost a quarter of cases (23%), the threat for individuals came from their mobile devices. Users make things easier for attackers by downloading questionable software. In the last quarter of 2019, a number of Apple users who wanted to jailbreak their devices fell victim to cybercriminals. When the checkra1n utility was released in fall 2019, it allowed using a hardware vulnerability to jailbreak all iPhones up to iPhone X inclusive, as well as some iPads. Since checkra1n does not depend on the iOS version, this jailbreak method rapidly gained popularity with both mobile users and security researchers. We advise against performing any kind of jailbreak since doing so weakens device protections against malware. Cybercriminals were fast to make use of the popularity of checkra1n. Cisco Talos researchers discovered the fake website checkrain[.]com, which was used to distribute a mobileconfig file masked as checkra1n. When installed and launched, this file imitated the jailbreak procedure. Then users were informed that they needed to download certain mobile apps to complete the procedure. Hackers used the fake checkra1n to promote those apps and make more people download them.

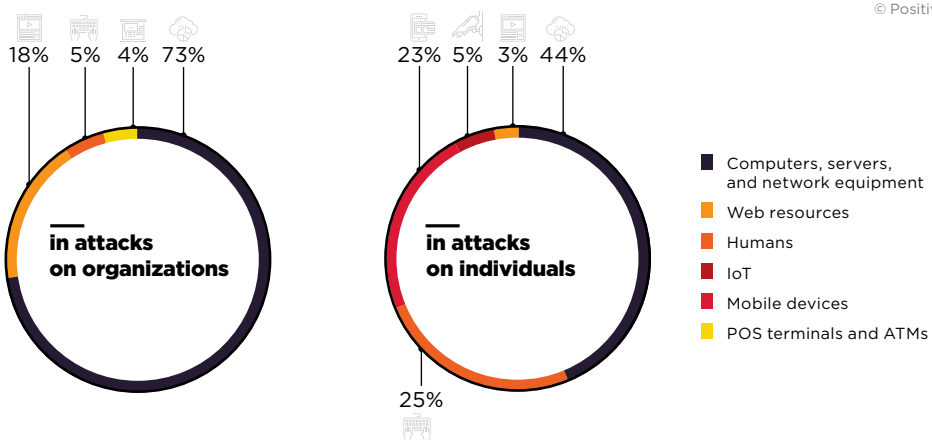


Figure 4. Attack targets

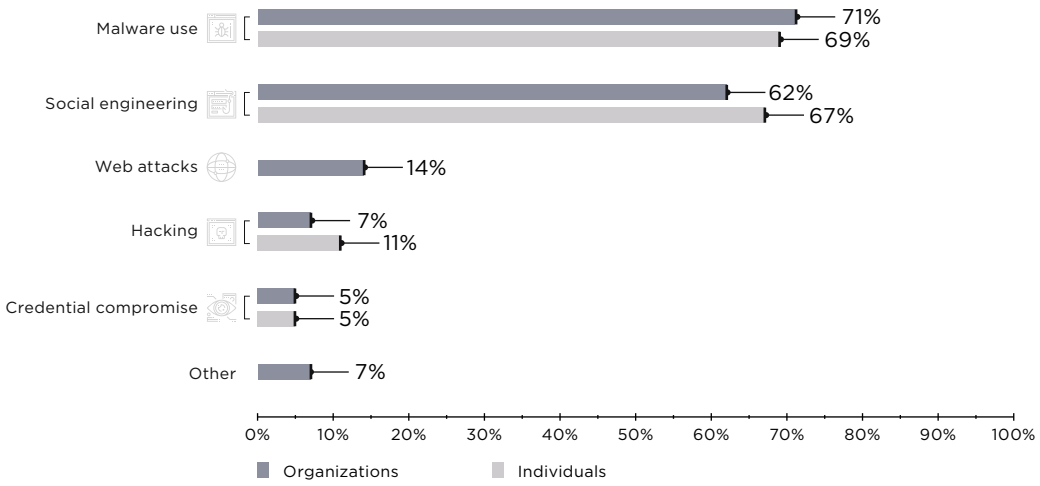


Figure 5. Attack methods

Industry

Per-industry classification of cyberincidents by motive, method, and target		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Science and education	Retail	Telecom	Transportation	Blockchain	Other	Multiple industries	Individuals
	Total	**74**	**31**	**33**	**32**	**7**	**17**	**28**	**30**	**22**	**6**	**3**	**4**	**24**	**53**	**61**
Target	Computers, servers, and network equipment	51	31	31	18		4	23	27	7	5	3	2	18	47	27
	Web resources	18		2	8	7	2	4	2	13	1		2	5	3	2
	Humans	5			6			1	1					1	3	15
	Mobile devices															14
	POS terminals and ATMs						11			2						
	IoT															3
Method	Malware use	49	29	30	18		15	17	26	9	3	3		18	42	42
	Social engineering	49	29	29	22		4	14	25	8	1	3		16	25	41
	Credential compromise	1		2	4			2	1	2				1	4	3
	Hacking	5	1	1	1			3	1	1			2		12	7
	Web attacks	15		1	1	4	2	3	2	11	3		1	3	5	
	Other	5	2	3		3		4			2		1	2	4	
Motive	Access to information	54	14	28	17	3	14	14	10	18	4		1	9	34	42
	Financial profit	13	17	4	15	1	3	12	19	3		3	2	11	18	18
	Hacktivism	6		1		3		2	1	1	2		1	3	1	1
	Cyberwar	1												1		

Darker colors indicate a greater proportion of attacks within a particular industry

0% 10% 20% 30% 40% 100%

Attack number

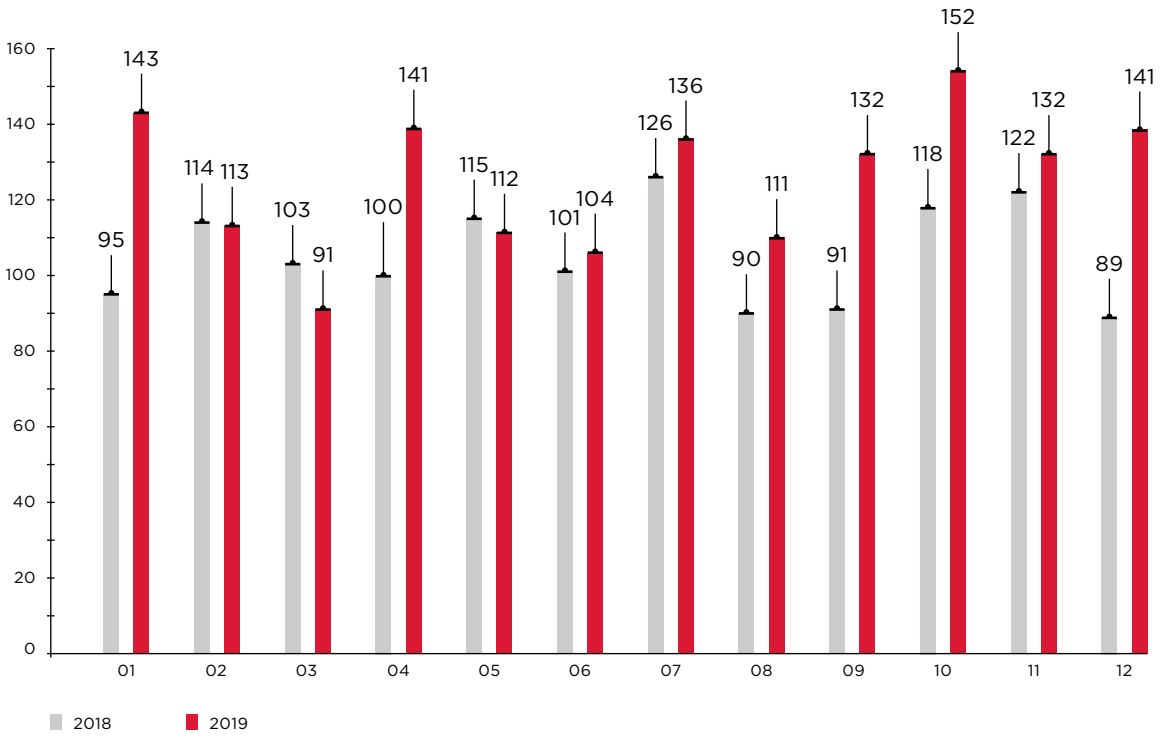


Figure 6. Number of incidents per month in 2018 and 2019 (1 = January, 12 = December)

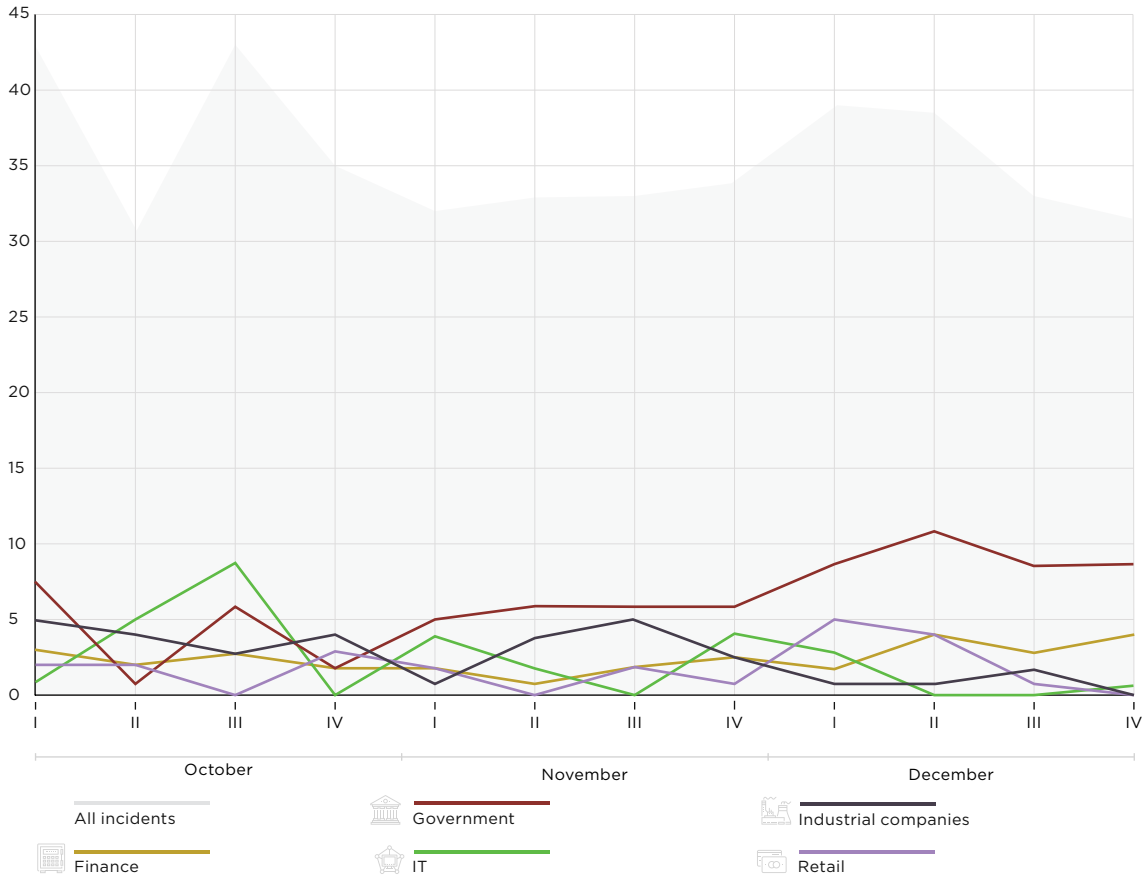


Figure 7. Number of incidents in Q4 2019 (by week)

Attack methods

Here we will describe the attack methods used by criminals, based on some of the highest-profile cyberincidents in Q4 2019.

Malware use

Ransomware continues to hit companies all over the world. In Q4 2019, victims included schools, medical institutions, industrial facilities, governments, and IT companies. The most aggressive ransomware operators were Sodinokibi, Maze, Ryuk, and Bitpaymer. In Spain alone, at least three companies (consulting firm Everis, radio company Cadena SER, and manufacturing company TECNOL) fell victim to the latter two groups.

More and more companies realize the threat of ransomware and are paying more attention to making backups in case of an attack. As a result, ransomware operators have to keep thinking of new ways to make their victims pay the ransom. For instance, the operators of Maze copy sensitive data to their servers before encrypting it, and then threaten to disclose it to the general public unless the victim pays up. Two such victims are Allied Universal, with a requested ransom of 300 bitcoins, and Southwire, whose data was "valued" at 850 bitcoins. In both cases, the companies refused to pay the ransom, and the attackers followed through on their threat. The files of both companies ended up on the web.

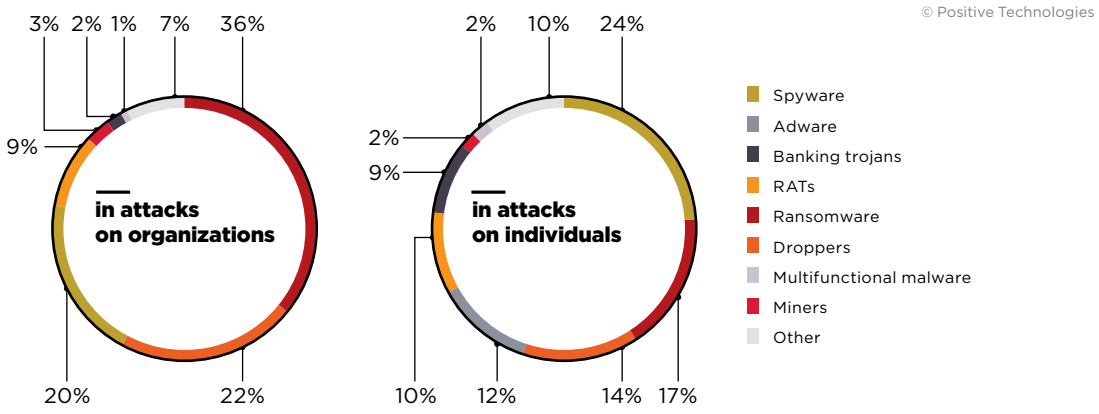


Figure 8. Types of malware

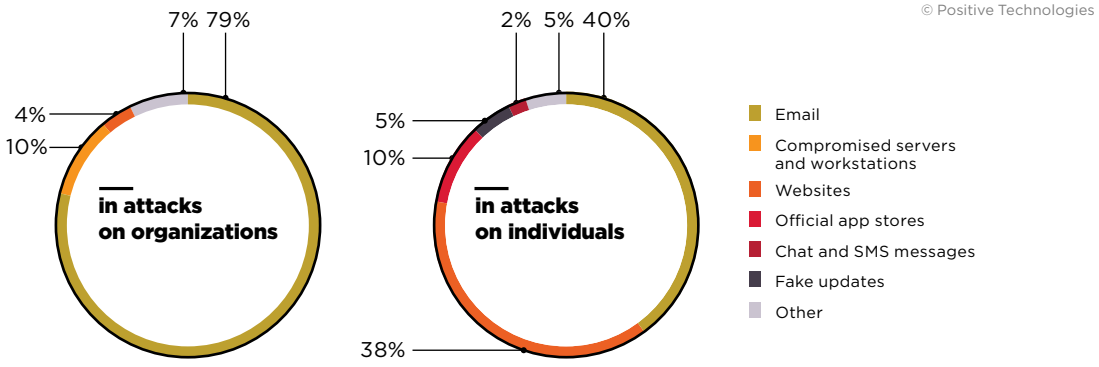


Figure 9. Malware distribution methods

The majority (79%) of malware infections at companies started with phishing emails. These emails can be sent as a part of a mass attack or tailored to the target. Company-specific phishing emails usually come from APT groups. As part of threat monitoring and research, the Positive Technologies Expert Security Center (PT ESC) recorded attacks by such APT groups as TA505, Sofacy (APT28), Donot (APT-C-35), Cloud Atlas, Bronze Union (LuckyMouse, APT27), Leviathan (APT40), Bisonal, Gamaredon, SongXY, Cobalt, and RTM throughout the last quarter of 2019. Some of these groups send malicious documents with very believable decoy texts. For instance, attacks by the Cloud Atlas group featured a text in Russian about the geopolitical confrontation between China and the United States in the field of artificial intelligence.

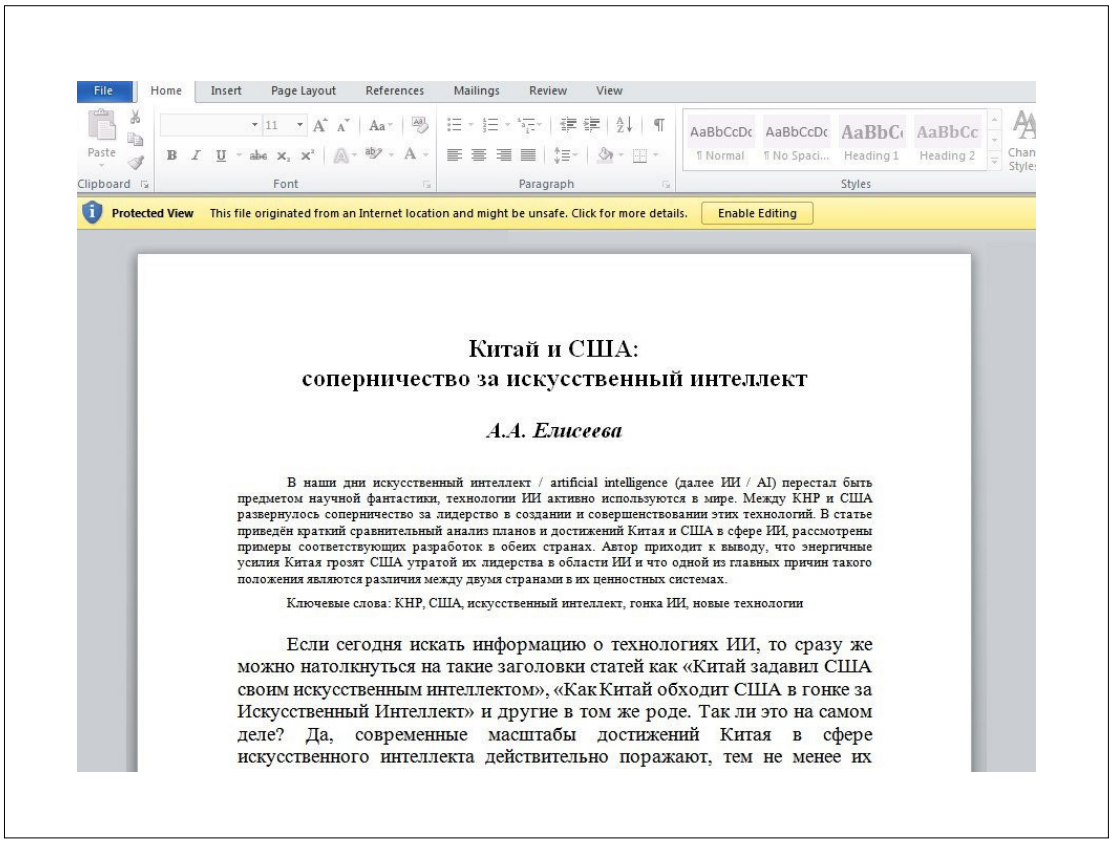


Figure 10. Fragment of document sent by Cloud Atlas

Social engineering

Oftentimes, attackers manipulate people's emotions to deliver malware. Emails are one way to accomplish this. In Q4 2019, 54 percent of attacks used social engineering combined with malware. Users need to be especially careful with their inboxes during the holiday season. Holidays are when attackers send phishing emails most actively. For instance, prior to Thanksgiving in the U.S., attackers sent out emails with supposed greeting cards. The attachments actually delivered malware, such as Emotet, to the victims' computers. Mass emails with fake party invitations containing Emotet were also sent out at Halloween and Christmas.

Even if you do not click suspicious links and do not open suspicious attachments, do not think you are immune. In Q4 2019, hackers took advantage of the workings of the Microsoft OAuth API to perform phishing attacks. The OAuth protocol allows issuing an access token to third-party apps without needing to know credentials. The attack went as follows. A phishing email contains a link to a file supposedly on OneDrive or SharePoint. But after clicking the link and entering credentials, the user gets a form requesting access to an Office 365 account. An inattentive victim can provide all requested rights with a single click. And then attackers receive access to the user's contact list, files, and correspondence.

Extortion emails are not a new trick, but they still pay off well. For instance, Check Point estimates that operators of the Phorpiex botnet made about $115,000 in five months by sending such emails. As proof of compromise, attackers obtain their victims' passwords from breached databases and include the passwords in the message. Payment for non-disclosure of sensitive data is usually in bitcoins. However, Cofense points out that attackers have started requesting payment in alternate currencies, such as litecoins (LTC). The reason is that messages containing bitcoin wallet addresses are often blocked by email security gateways precisely to prevent such extortion attempts. Some cybercriminals having taken to putting bitcoin wallet addresses in emails in the form of QR codes.

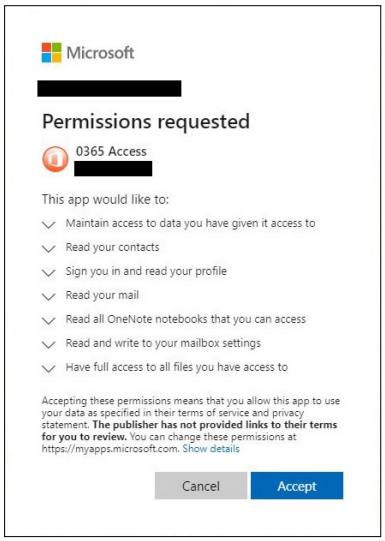


Figure 11. Request from phishing app O365 Access

Hacking

Vulnerability CVE-2019-0708 (also known as BlueKeep) is now being used in real attacks to deliver miners. However, we think that in the future this vulnerability could be used by hackers in other campaigns as well, including APT attacks.

In October, Wallarm experts reported a vulnerability in PHP 7 (CVE-2019-11043) allowing execution of arbitrary commands on nginx servers supporting PHP-FPM. Cloud storage company NextCloud, whose clients were at risk, released guidance on how to protect against the new threat. However, not all NextCloud administrators took security measures in time, and after a short while there were reports of NextCry ransomware attacks. This malware targets and infects NextCloud servers vulnerable to CVE-2019-11043. The vulnerability was new, so antivirus software could not detect the first NextCry attacks. This enabled infection to occur.

Hacking can be used together with social engineering, as in the case of browser vulnerabilities. In November, it was found that scammers were actively exploiting a vulnerability in Mozilla Firefox in attacks where they pretend to be technical support personnel. Users of the vulnerable browser were lured (such as by emails) to visit a hacker-controlled web resource. When the user visits, the browser is blocked with a pop-up window stating that the user must contact technical support or buy certain software. The trick is not new, but it still works.

Web attacks

Web resources remain a target for hacktivists. In the U.S. state of Ohio, hackers attacked an electronic voting system on election day, November 5, with an attempted SQL injection.

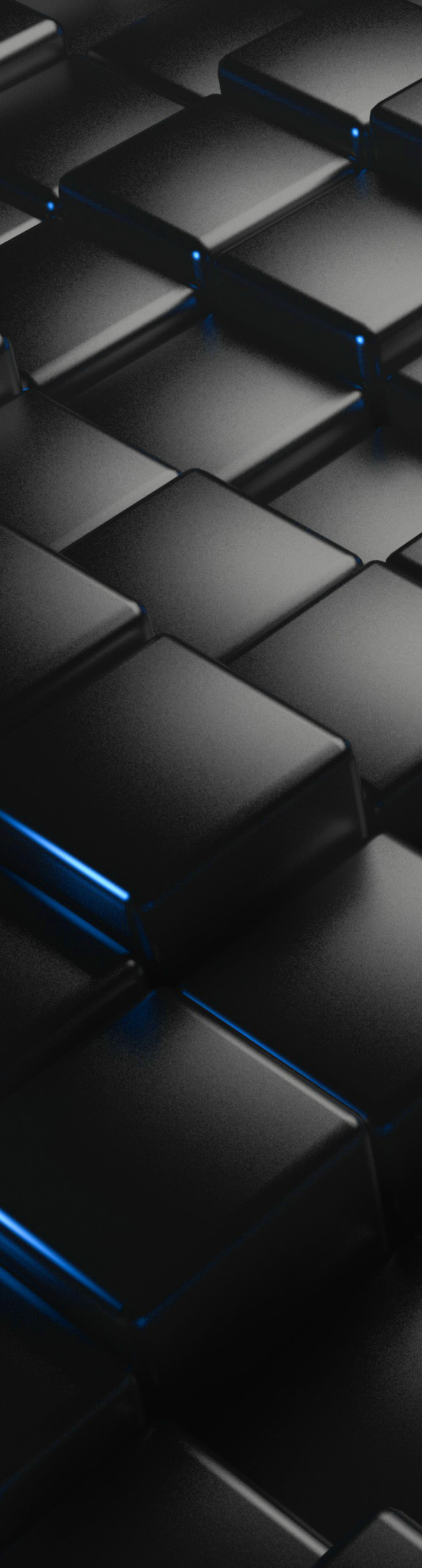
Corporate websites are also attractive to hackers. Attackers hope to obtain client databases, payment card information, and credentials of site users. If the attackers succeed in stealing sensitive data, the victim company has to notify the affected users and take measures to prevent further attacks. For instance, a breach of personal data of online store clients forced smartphone manufacturer OnePlus to launch a bug bounty program and partner with HackerOne. The breach was caused by a web vulnerability the details of which are still undisclosed.

Hackers can also use web vulnerabilities for denial of service (DoS) attacks. Cisco specialists reported an increase in attempts to exploit vulnerability CVE-2018-0296 in the Cisco Adaptive Security Appliance and Firepower Appliance firewall web administration interface. The vulnerability allows rebooting attacked devices remotely and without logging in, by sending specially crafted HTTP requests. It also allows reading system information with directory traversal. The vulnerability was reported back in mid-2018, but remains a workhorse for hackers.

Credential compromise

Attackers search the Internet for accessible network devices with weak passwords to infect with malware and add to their botnets for cryptocurrency mining or DoS attacks. A new botnet called Mozi searches for Netgear, D-Link, and Huawei routers with weak Telnet passwords and infects them with malware. The Muhstik botnet targets routers with Tomato firmware which have the default password "admin".

There are other ways for hackers to monetize credentials obtained in massive brute-force attacks. One option is to sell the data on the darkweb. But often attackers publish such databases for free. The owner of one DDoS-for-hire service published a list of credentials for Telnet for over 515,000 servers, routers, and IoT devices on a hacker forum. The explanation: instead of creating botnets, that person could rent high-performance servers from cloud service providers.



Victim categories

In this section, attacks on industries of special interest in Q4 2019 will be considered in greater detail.

Government

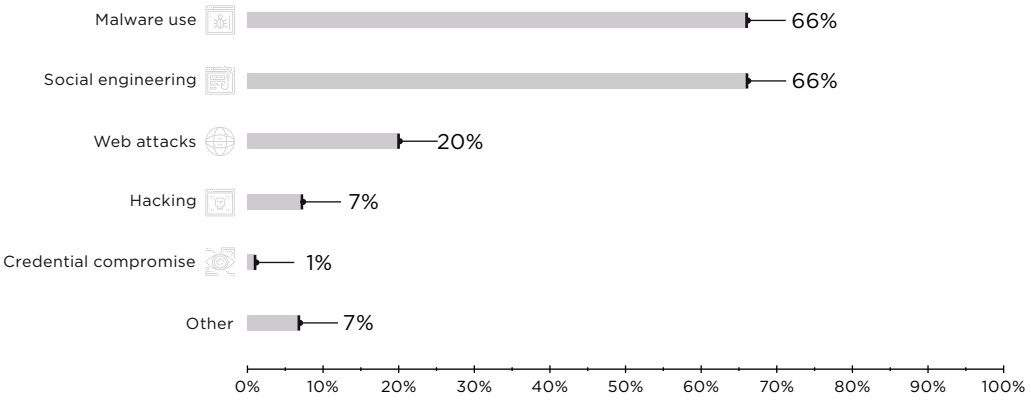


Figure 12. Government: attack methods used in Q4 2019

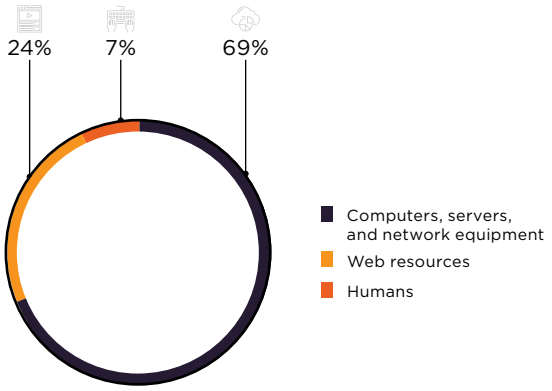


Figure 13. Attack targets

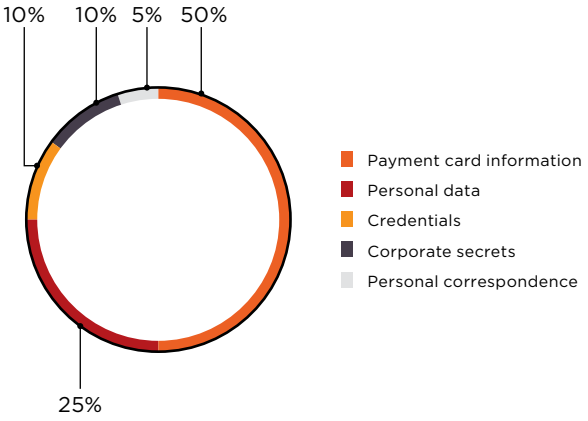


Figure 14. Data stolen

The U.S. was hit by a wave of attacks on the Click2Gov service. We described them in detail a year ago. In Q4 2019, these attacks occurred again. Authorities in eight cities stated that those who paid utility bills via the service between late August and November were affected.

Figure 15. Geographic distribution of attacks on Click2Gov (yellow: first wave of attacks, blue: new wave of attacks)

Government institutions are still targeted by APT groups. In the last quarter of 2019, the Gamaredon APT group remained active. In November and December, PT ESC registered 17 attacks by this group, targeting state institutions and military and defense-related organizations in Ukraine. The group now uses a different method of payload delivery. In their previous attacks, they sent documents with macros. At the end of the year, though, they used template injection, which allows avoiding antivirus detection. With this method, the document does not contain OLE objects or macros. Instead, it contains a link to a malicious template document automatically downloaded from the attackers' server. That documents contains a macro that saves a malicious Visual Basic script (VBScript) to the startup folder. The macro also modifies the registry value responsible for warning the user of macro execution. After this modification, all macro documents will run automatically.

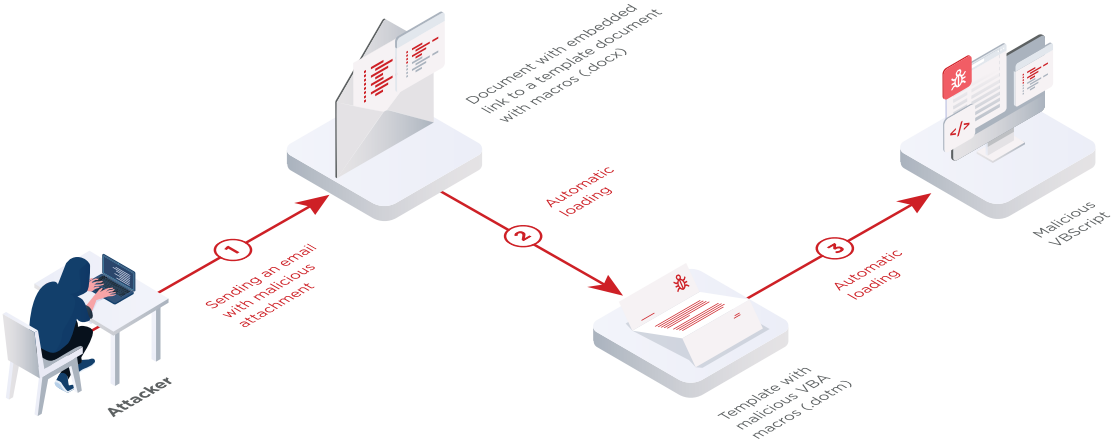


Figure 16. Infection with template injection as used in Gamaredon attacks


ICTV

МІЖНАРОДНА КОМЕРЦІЙНА ТЕЛЕРАДІОКОМПАНІЯ (ICTV)

Вих.№29/09-054

Служба зовнішньої розвідки України

Інформаційний запит

Телеканал «ICTV» та програма «Більше ніж правда» засвідчують Вам повагу. Просимо Вас доручити відповідальній особі надати нам коментар на камеру щодо наступних питань:

МІНІСТЕРСТВО ЗАКОРДОННИХ СПРАВ УКРАЇНИ

Михайлівська площа, 1, м. Київ, 01018, Україна

Тел.: (044) 238 17 48; факс: (044) 238 18 88
E-mail: zmfa@mfa.gov.ua
Web: http://www.mfa.gov.ua
Код ЄДРПОУ 00026620

MINISTRY OF FOREIGN AFFAIRS OF UKRAINE

1 Mykhailivska Square, Kyiv, 01018, Ukraine

24.12.2019 р. № 71/ПР/21-524/2-1791

Закордонні дипломатичні установи України

Щодо надання інформації

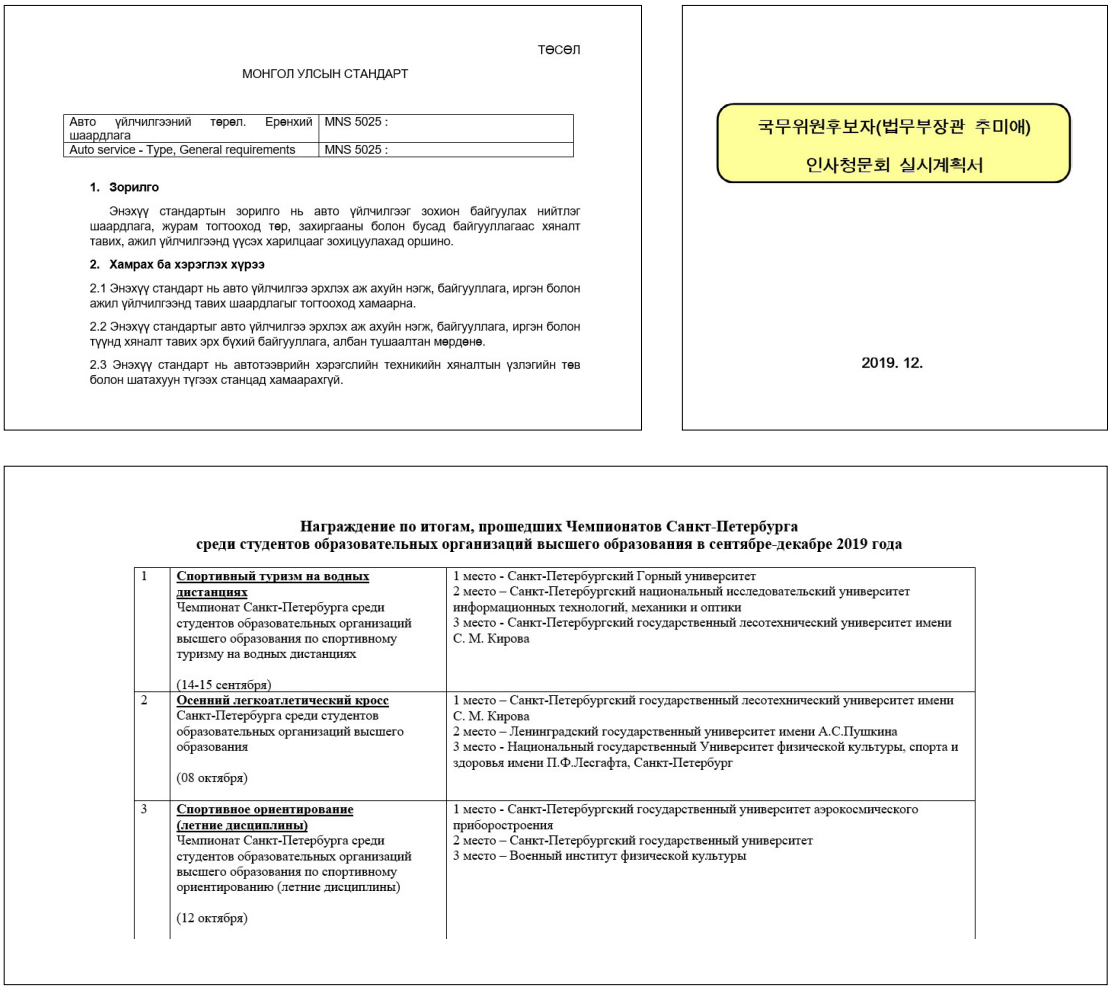
У зв'язку із запитом компетентних органів просимо здійснити наступні перевірки:
- щодо оформлення та видачі паспорта громадянина України для виїзду за кордон
- щодо оформлення паспорта громадянина України для виїзду за кордон або посвідчення особи на повернення в Україну на ім'я

За результатом просимо інформувати ДКС (gov.ua в копії: gov.ua) **до кінця робочого дня 25 грудня 2019 року, виключно у разі наявності запитуваної інформації,** а також надіслати копії заяви-анкети та документів, що слугували підставою оформлення зазначених паспортних документів.

Начальник Управління консульського обслуговування ДКС **підписано**

Figure 17. Documents from Gamaredon emails with embedded link to template document with macro

In December, PT ESC detected traces of three attacks on government institutions in Mongolia, South Korea, and Russia by the Bisonal group. Malicious emails from the group used RTF documents with an exploit for vulnerability CVE-2018-0798. The documents were generated with builder 8.t, which is also used by other APT groups such as Goblin Panda, IceFog, and SongXY.



ТӨСӨЛ

МОНГОЛ УЛСЫН СТАНДАРТ

Авто үйлчилгээний төрөл. Ерөнхий шаардлага	MNS 5025 :
Auto service - Type, General requirements	MNS 5025 :

1. Зорилго

Энэхүү стандартын зорилго нь авто үйлчилгээг зохион байгуулах нийтлэг шаардлага, журам тогтооход төр, захиргааны болон бусад байгууллагаас хяналт тавих, ажил үйлчилгээнд үүсэх харилцааг зохицуулахад оршино.

2. Хамрах ба хэрэглэх хүрээ

2.1 Энэхүү стандарт нь авто үйлчилгээ эрхлэх аж ахуйн нэгж, байгууллага, иргэн болон ажил үйлчилгээнд тавих шаардлагыг тогтооход хамаарна.

2.2 Энэхүү стандартыг авто үйлчилгээ эрхлэх аж ахуйн нэгж, байгууллага, иргэн болон түүнд хяналт тавих эрх бүхий байгууллага, албан тушаалтан мөрдөнө.

2.3 Энэхүү стандарт нь автотээврийн хэрэгслийн техникийн хяналтын үзлэгийн төв болон шатахуун түгээх станцад хамаарахгүй.

국무위원후보자(법무부장관 추미애)

인사청문회 실시계획서

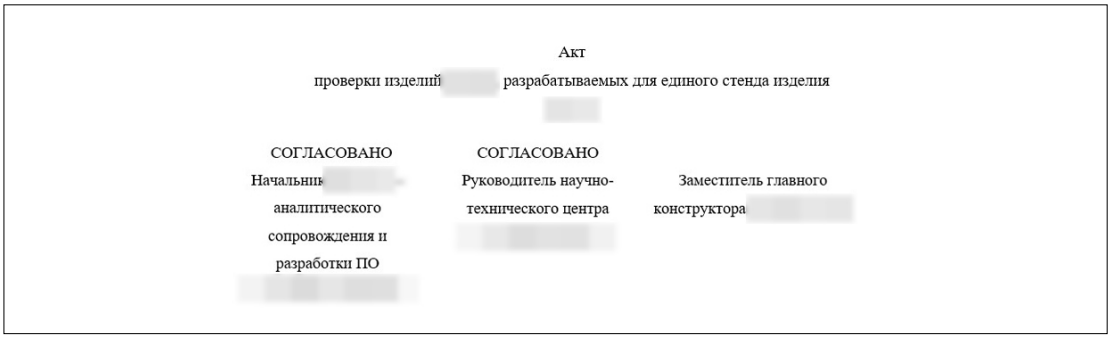
2019. 12.

Награждение по итогам, прошедших Чемпионатов Санкт-Петербурга среди студентов образовательных организаций высшего образования в сентябре-декабре 2019 года

1	**Спортивный туризм на водных дистанциях** Чемпионат Санкт-Петербурга среди студентов образовательных организаций высшего образования по спортивному туризму на водных дистанциях (14-15 сентября)	1 место - Санкт-Петербургский Горный университет 2 место – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики 3 место - Санкт-Петербургский государственный лесотехнический университет имени С. М. Кирова
2	**Осенний легкоатлетический кросс** Санкт-Петербурга среди студентов образовательных организаций высшего образования (08 октября)	1 место – Санкт-Петербургский государственный лесотехнический университет имени С. М. Кирова 2 место – Ленинградский государственный университет имени А.С.Пушкина 3 место - Национальный государственный Университет физической культуры, спорта и здоровья имени П.Ф.Лесгафта, Санкт-Петербург
3	**Спортивное ориентирование (летние дисциплины)** Чемпионат Санкт-Петербурга среди студентов образовательных организаций высшего образования по спортивному ориентированию (летние дисциплины) (12 октября)	1 место - Санкт-Петербургский государственный университет аэрокосмического приборостроения 2 место – Санкт-Петербургский государственный университет 3 место – Военный институт физической культуры

Figure 18. Documents from emails by Bisonal

The SongXY group also attacks government institutions. PT ESC registered three attacks in Q4 2019: two on Ukrainian government institutions and one on Russian ones. Both Bisonal and SongXY used RTF documents with an exploit for vulnerability CVE-2018-0798. Attachments were generated by builder 8.t.



Акт

проверки изделий [redacted] разрабатываемых для единого стенда изделия

[redacted]

СОГЛАСОВАНО
Начальник [redacted]
аналитического
сопровождения и
разработки ПО
[redacted]

СОГЛАСОВАНО
Руководитель научно-
технического центра
[redacted]

Заместитель главного
конструктора [redacted]

Figure 19. Examples of malicious attachments from SongXY

Службові номери керівництва України

Структурнийпідрозділ	Прізвище, ім'я, по-батькові	Телефон
Директор		(приймальня)
Перший заступник Директора		відсутній (приймальня)
Заступник Директора		відсутній (приймальня)
Заступник Директора		(приймальня)
Головнийпідрозділдетективів		
Керівник Головного підрозділудетективів		(приймальня)

Розпорядження N 2098-р Директоравід 26 листопада 2019 року вакансіяконкурсоголошенняпровакансії

ЗАТВЕРДЖУЮ
Директор
(найменування посади, ініціали (ім'я), прізвище та підпис керівника державної служби у державному органі)

«26» листопада 2019 року

РозпорядженнямДиректора
2019 року № 2098-р оголошеноконкурсназайняттявакантнихпосад в
України (далі –).

Figure 20. Examples of malicious attachments from SongXY

Industrial companies

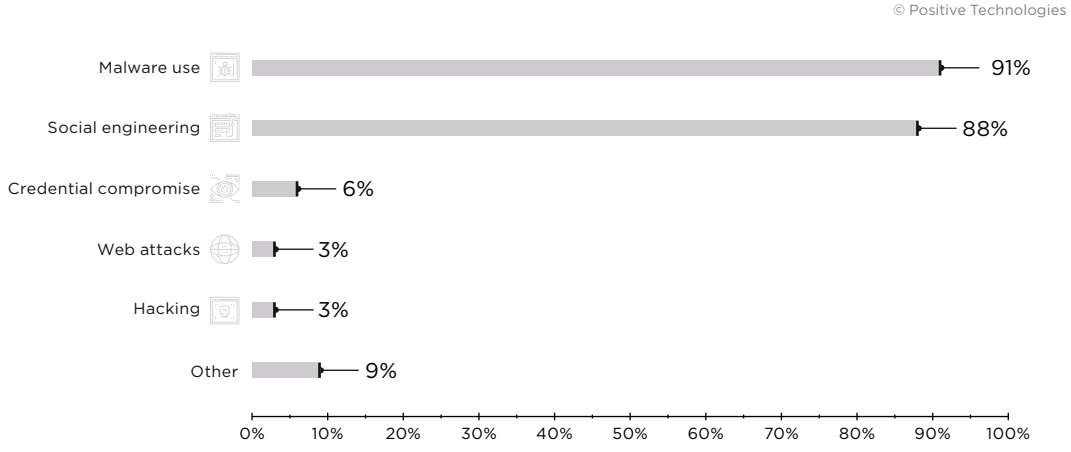


Figure 21. Industrial companies: attack methods used in Q4 2019

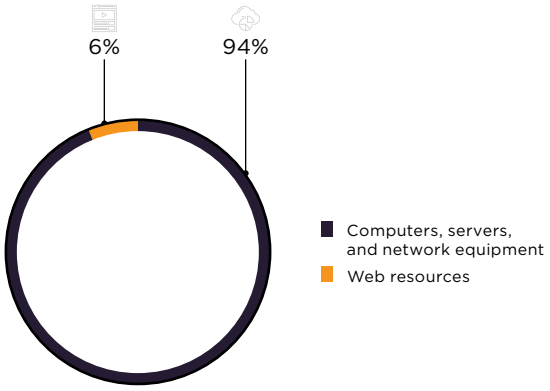


Figure 22. Attack targets

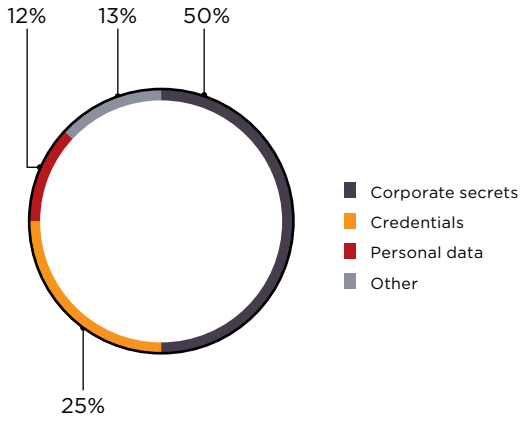


Figure 23. Data stolen

The RTM group is still actively attacking industrial companies in Russia and the CIS. However, they also send malicious emails to government institutions, banks, and scientific and educational institutions. PT ESC detected 25 malicious mailings by the group during the fourth quarter. Starting in June 2019, RTM started calculating the server IP address with logical operations based on the amount of a transaction received by a certain Bitcoin wallet. In mid-December 2019, RTM changed the algorithm for obtaining IP addresses. Now every malware sample contains two Bitcoin wallet numbers, and the calculation is based on the latest outgoing transactions from the first wallet to the second one. The change had a minimal effect on the group's code, but gave the attackers protection from spoofing of their C2 server addresses.

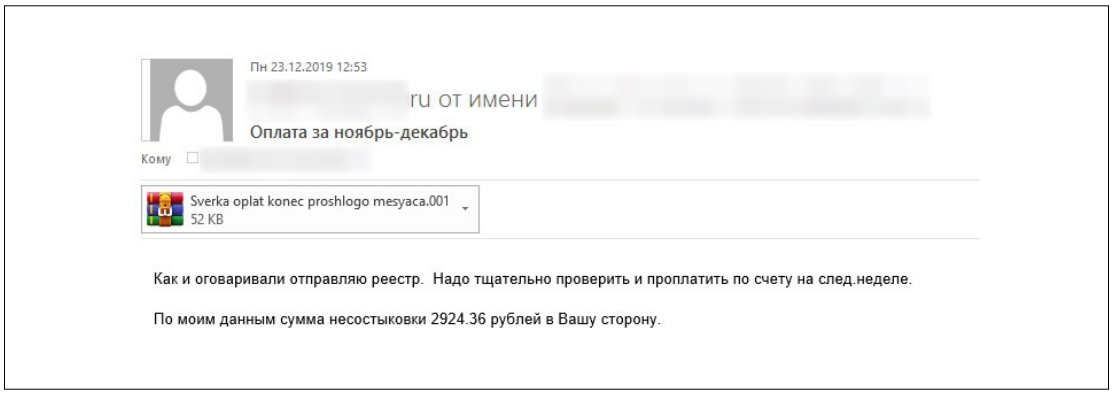


Figure 24. Phishing message from the RTM group to an industrial company

In Q4 2019, APT attacks targeted industrial companies not only in Russia and the CIS, but also in the United States, South Korea, Japan, Indonesia, Turkey, and Germany. Experts from Section 52 at CyberX detected targeted attacks on industry in which attackers sent phishing emails for delivering the Separ infostealer. It is believed that Separ can be used to steal intellectual property and passwords for accessing industrial systems.

The APT33 group is also actively attacking industrial companies. This group makes heavy use of password spraying, in which they test multiple weak passwords in attacks on a large number of accounts. At CyberwarCon, a Microsoft speaker presented findings from monitoring of the APT group. Experts say that in recent months the number of attacked organizations went down to 2,000, but the number of accounts the attackers tried to hack at each of these organizations increased dramatically.

Financial institutions

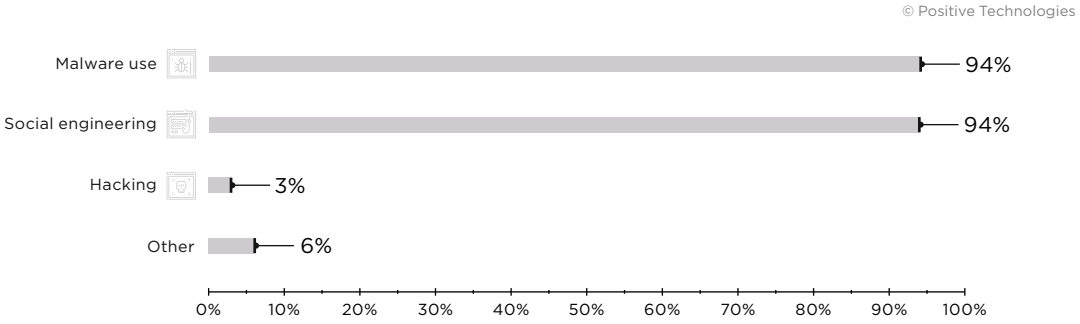


Figure 25. Financial institutions: attack methods used in Q4 2019

In Q4, PT ESC detected 12 mailings from the Cobalt group to financial institutions.

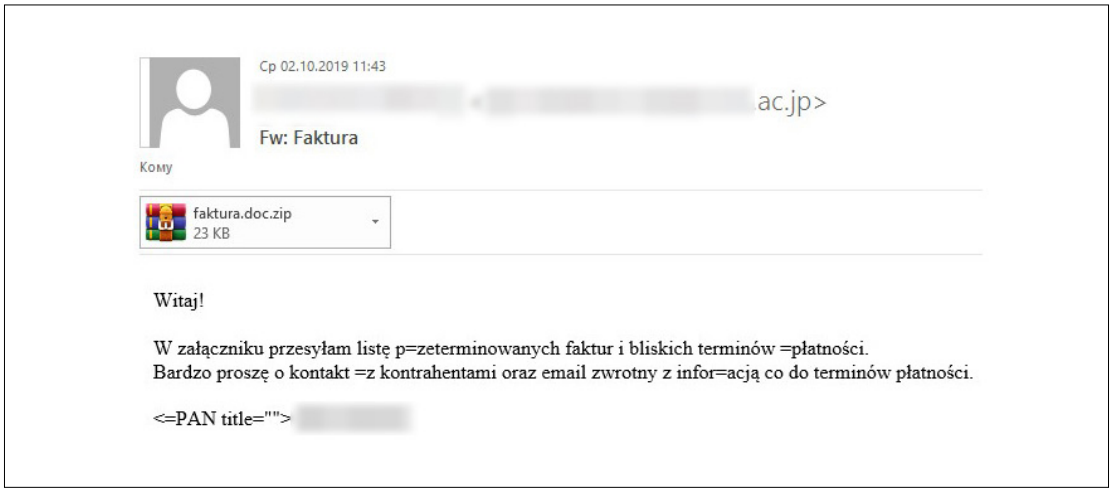


Figure 26. Phishing email from the Cobalt group

The group uses different types of malicious attachments, such as RTF documents with exploits, Microsoft Office documents with macros, and VHD (Virtual Hard Drive) files. The last one is a new format for Cobalt's malicious emails. It works only on Windows 7 and later. When the VHD file is opened, it is automatically mounted as a drive. Then Windows Explorer opens the malicious content, and all the user has to do is launch it. Payloads used by Cobalt in Q4 included CoolPlants, CobInt, COM-DLL-Dropper, and a JScript backdoor.

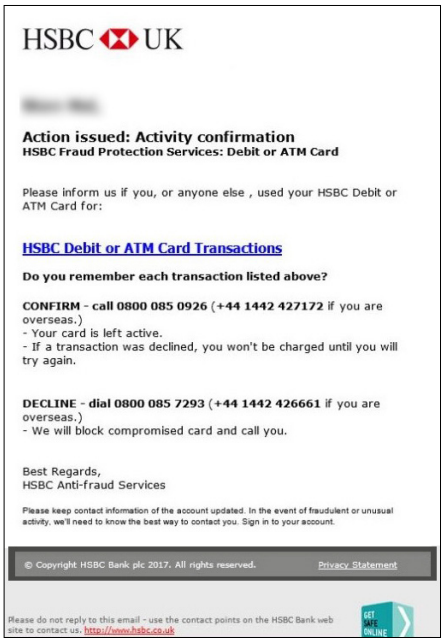


Figure 27. Malicious VHD image attachment

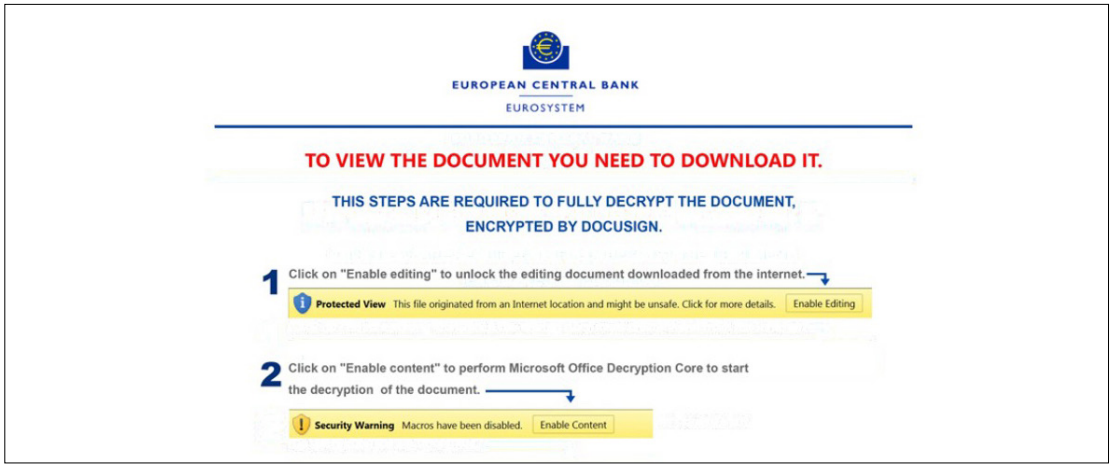


Figure 28. Document with embedded malicious macro

The TA505 group also attacks financial institutions. The attackers are not tied to any specific geographic location. According to PT ESC, in Q4 the group attacked financial institutions in the United States, Columbia, India, and the Czech Republic. Attachments to malicious emails from TA505 deliver the Get2 loader, which in turn downloads the FlawedGrace and SDBbot backdoors, as well as the Snatch loader, to infected computers.

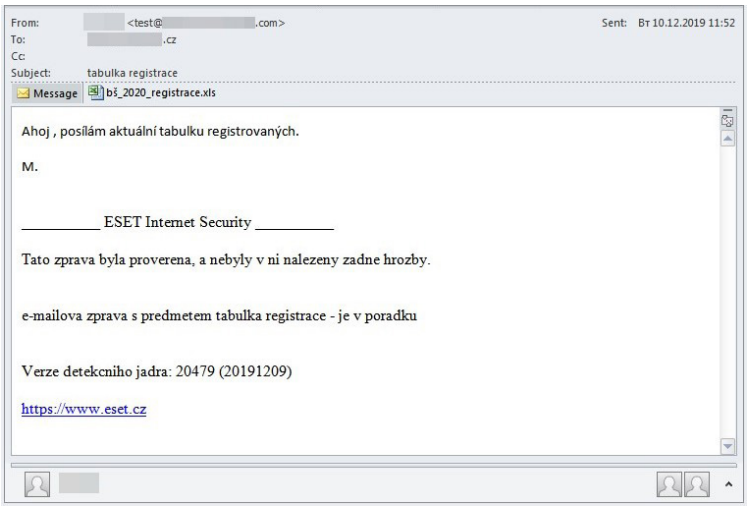


Figure 29. Phishing email from TA505 to a Czech bank

In addition to financial institutions, targets of TA505 included IT companies, industry, and universities. Besides the malware mentioned already, the group still uses CryptoMix ransomware, EmailStealer malware for filtering files by extension and stealing email accounts, a utility to disable Windows Defender and launch the payload, and a modified ServHelper backdoor. On top of that, TA505 has started using AZORult spyware.

A new infostealer called Raccoon appeared on the darkweb in April 2019 and is rising in popularity. In Q4 2019, operators of Raccoon attacked employees of banks. To avoid detection by email systems, attackers send phishing emails from a corporate account compromised earlier. In late October, emails contained a link to a malicious image hosted on Dropbox. Raccoon is distributed as MaaS (malware as a service) for $200 a month. Developers update the malware regularly and add new features.

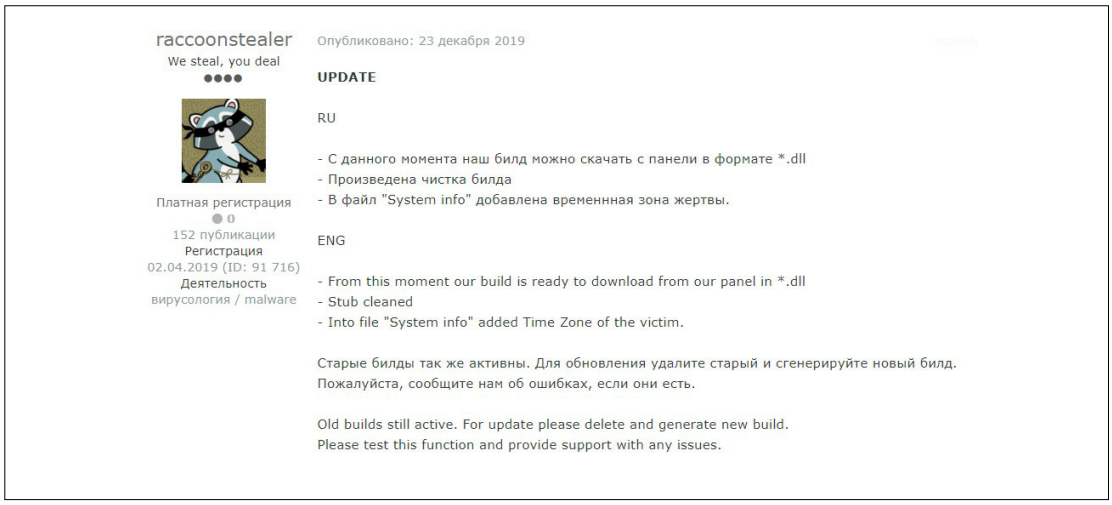


Figure 30. Update announcement from Raccoon developers

IT

In Q4, the percentage of attacks on IT companies increased to 8 percent of all attacks on organizations, compared to 3 percent in Q3. Large IT companies are an attractive target for ransomware operators, which is hardly surprising. If an IT service provider is compromised, the provider will lose clients, who will be concerned about infrastructure integrity. This danger is enough to make IT companies pay the ransom.

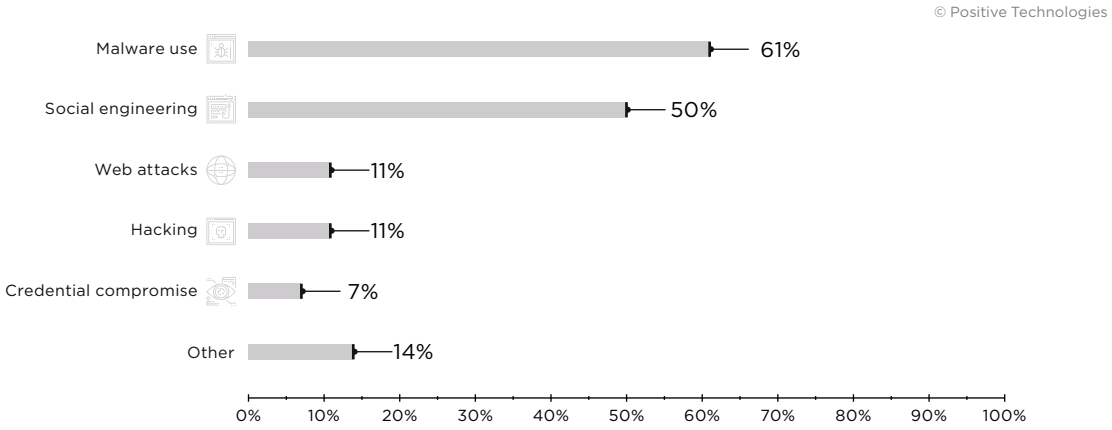


Figure 31. IT: attack methods used in Q4 2019

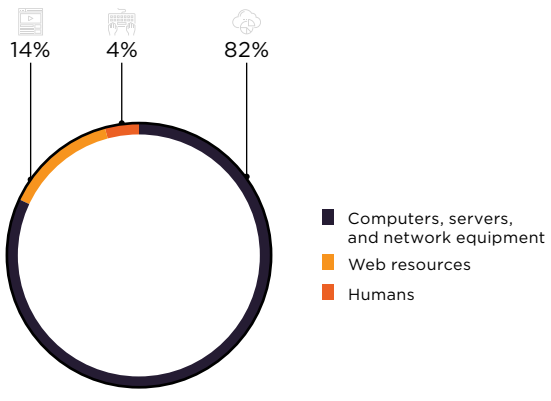


Figure 32. Attack targets

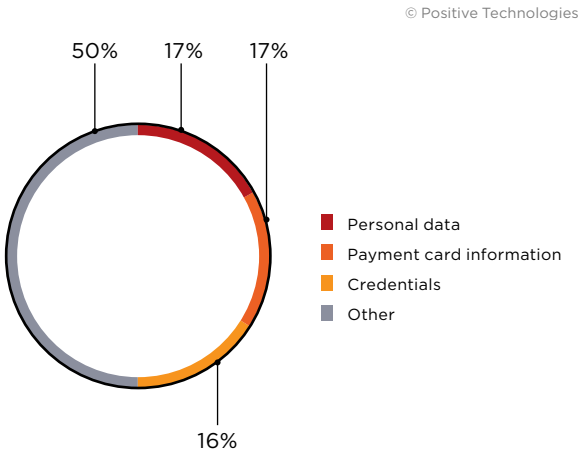


Figure 33. Data stolen

The General Data Protection Regulation states that personal data must be protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage (integrity and confidentiality). In Q4 2019, we saw a new trend. Ransomware operators force their victims to pay the ransom by saying that if the stolen personal data is disclosed, the company will pay much more under the GDPR. For instance, CyrusOne, one of the largest American hosting providers, was attacked with ransomware (presumably Sodinokibi). Attackers threatened to disclose the stolen data if the victim refused to pay.

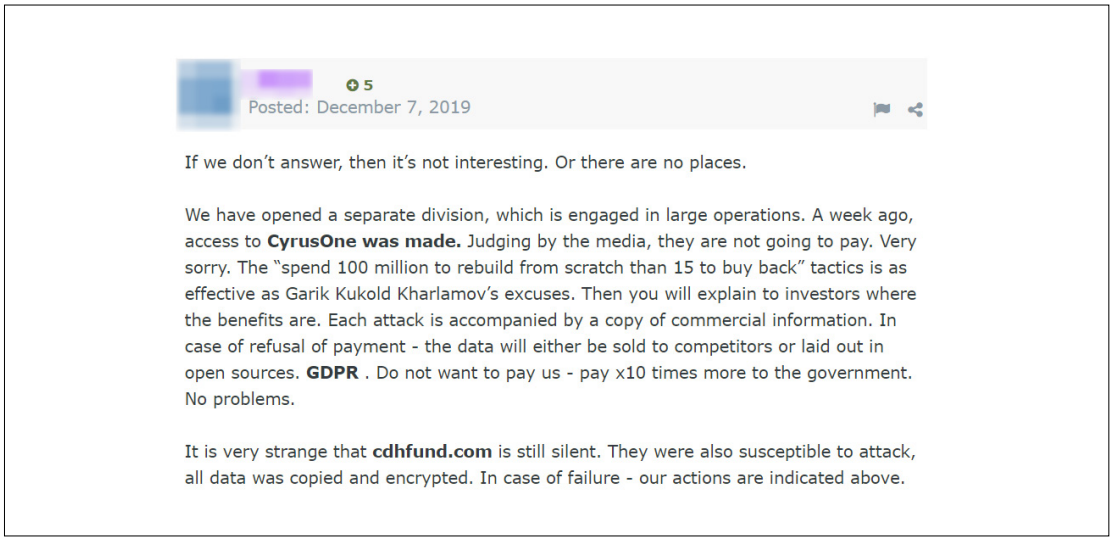


Figure 34. Announcement on the darkweb about attack on CyrusOne

IT companies, such as Synoptek and Complete Technology Solutions, were also hit by Sodinokibi in Q4.

At the start of the quarter, hackers attacked the website of Extendware, a company that develops extensions for sites run on the Magento CMS. Attackers injected a keylogger into the sales pages. Specialists believe this may be a supply chain attack. Hackers could have injected the malware not only into the Extendware site, but into the extensions as well. Such an attack could potentially compromise all Extendware clients. In mid-2019, we already wrote about supply chain attacks against IT companies. This trend persisted throughout 2019, and will probably continue in 2020. Another example of a supply chain attack was seen against Volusion, an e-commerce platform developer. We will go in to greater detail on the attack slightly later.

Retail

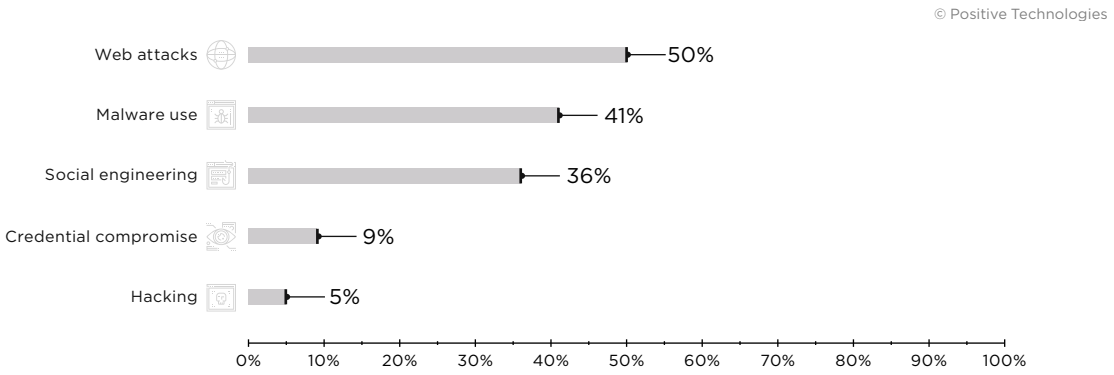


Figure 35. Retail: attack methods used in Q4 2019

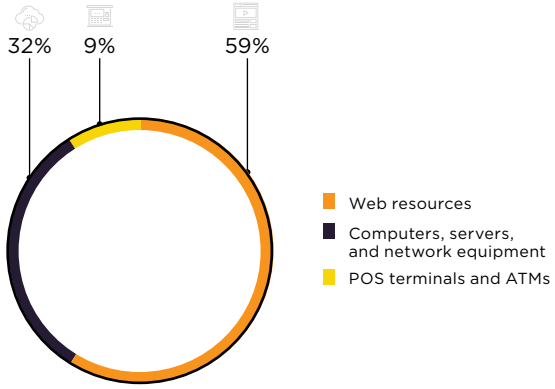


Figure 36. Attack targets

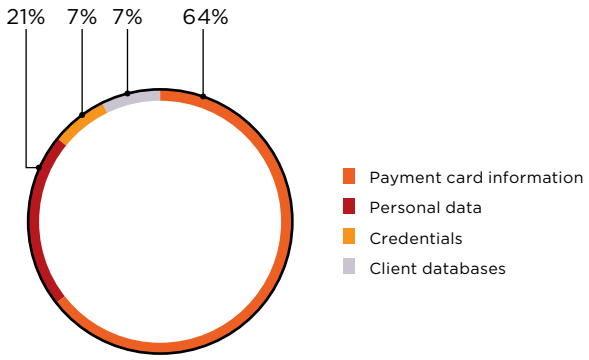


Figure 37. Data stolen

At the start of the quarter, hackers involved in attacks collectively referred to as MageCart compromised Sixth June, an online clothes store developed on Magento. Attackers injected a JavaScript sniffer (a scriptlet for stealing payment card information) into the site. To make the sniffer harder to detect, the hackers registered a domain name (mogento[.]info) that could be easily confused with that of Magento. The fake web resource was used to distribute malicious components and receive the stolen payment card information.

What is MageCart?

MageCart is a class of attacks on payment-enabled websites, such as online stores. MageCart is also used to refer to the hacker groups behind these attacks. In this attack, hackers compromise a site and inject a special JavaScript script ("sniffer") into the payment page. When a user enters payment card information on the compromised site, the sniffer sends this information to the hackers' server. These attacks are sometimes called web skimming.

Web skimming is so widespread now that different MageCart groups sometimes attack the same site independently of each other. For instance, PerimeterX concluded that sniffers similar to those found in the attack on Sixth June were installed on five other websites, including PEXSuperstore.com. Yet they also found another sniffer at PEXSuperstore.com, presumably installed by a different group of attackers.

Same as in the previous quarter, there were MageCart supply chain attacks. For instance, one group compromised the Google Cloud storage of Volusion and injected a sniffer which was automatically pushed to Volusion-based online stores. The estimated number of victims ranges from 6,500 to 20,000 sites.

When compromising online resources and installing JavaScript sniffers, attackers do their best to evade detection. For instance, in the case of Volusion, attackers used the domain name volusion-cdn[.]com to mask illegitimate data transfer as communication with Volusion servers. The same trick was used in attacks on Magento-based stores. Another trend in hiding JavaScript sniffers is to make their code as small as possible. In Q4 2019, Malwarebytes detected attacks in which just a single line of code was injected. That line downloaded a JavaScript sniffer from payment-mastercard[.]com, an address that belonged to the attackers.

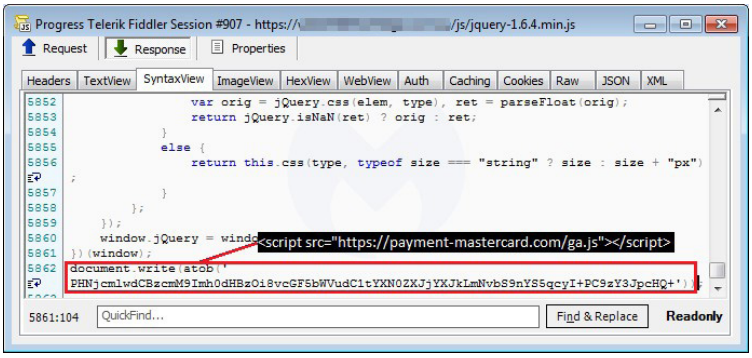


Figure 38. Link to a fake payment data input form injected into the compromised site

It was also found that the domain name payment-mastercard[.]com was involved in other attacks. That domain was used to load a fake form for payment data input, imitating the input form of a legitimate payment service provider. After the user entered payment information into the phishing form, the data went to the attackers' server, and the user was redirected to the original page of the provider.

Retail companies must keep in mind that they can become victims of ransomware just like any other industry. For instance, in Q4 2019 Arrigo Automotive Group lost $250,000 in this kind of attack.

APT groups attack retail companies, too. For example, PT ESC detected APT attacks by the TA505 group against retail companies in Japan.

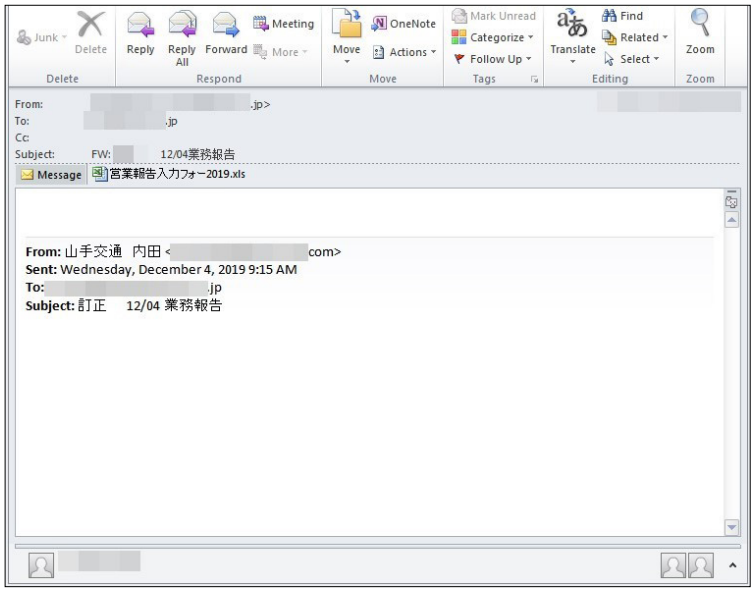


Figure 39. Email from TA505 to a Japanese retail company

What companies can do to stay safe

Use proven security solutions

- Centrally manage software updates and patches. To prioritize update plans correctly, the most pressing security threats must be taken into account.
- Install antivirus software with a sandbox for dynamically scanning files and the ability to detect and block threats in the corporate email system, such as malicious email attachments, before they are opened by employees. Ideally, antivirus software should simultaneously support solutions from multiple vendors and have the ability to detect signs of hidden or obfuscated malware, as well as block malicious activity across diverse data streams: email, web traffic, network traffic, file storage, and web portals. Whatever solution you select, it should be able to check files both in real time and retrospectively, by automatically re-scanning files when signature databases are updated to detect previously unknown threats.
- We also recommend using SIEM solutions for timely detection and effective response to information security incidents. This will help identify suspicious activity, prevent infrastructure hacking, detect attackers' presence, and enable prompt measures to neutralize threats.
- Automated tools for analyzing security and identifying software vulnerabilities.
- Deploy web application firewalls as a preventive measure.
- Detect sophisticated targeted attacks in real time and in saved traffic with deep traffic analysis. Using such solutions will allow you to detect previously unnoticed attacks and monitor network attacks in real time, including use of malware and hacking tools, exploitation of software vulnerabilities, and attacks on the domain controller. Such an approach quickly identifies attacker presence in the infrastructure, minimizes the risk of loss of critical data and disruption to business systems, and decreases the financial damage caused by attackers.
- Employ specialized anti-DDoS services.

Protect your data

- Encrypt all sensitive information. Do not store sensitive information where it can be publicly accessed.
- Perform regular backups and keep them on dedicated servers that are isolated from the network segments used for day-to-day operations.
- Minimize the privileges of users and services as much as possible.
- Use a different username and password for each site or service.
- Use two-factor authentication where possible, especially for privileged accounts.

Do not allow weak passwords

- Enforce a password policy with strict length and complexity requirements.
- Require password changes every 90 days.
- Replace all default passwords with stronger ones that are unique and meet strict password policy requirements.

Monitor the security situation

- Keep software up to date. Do not delay installing patches.
- Test and educate employees regarding information security.
- Make sure that insecure resources do not appear on the network perimeter. Regularly take an inventory of Internet-accessible resources, check their security, and remediate any vulnerabilities found. It is a good idea to monitor the news for any new vulnerabilities: this gives a head start in identifying affected resources and taking necessary measures.
- Filter traffic to minimize the number of network service interfaces accessible to an external attacker. Pay special attention to interfaces for remote management of servers and network equipment.
- Regularly perform penetration testing to identify new vectors for attacking internal infrastructure and evaluate the effectiveness of current measures.
- Regularly audit the security of web applications, including source-code analysis, to identify and eliminate vulnerabilities that put application systems and clients at risk of attack.
- Keep an eye on the number of requests per second received by resources. Configure servers and network devices to withstand typical attack scenarios (such as TCP/UDP flooding or high numbers of database requests).

Help clients to stay safe

- Improve security awareness among clients.
- Regularly remind clients how to stay safe online from the most common attacks.
- Urge clients to not enter their credentials on suspicious websites and to not give out such information by email or over the phone.
- Explain what clients should do if they suspect fraud.
- Inform clients about security-related events.

How vendors can secure their products

- All the measures described for organizations, plus:
- Implement a secure development lifecycle (SDL).
- Regularly audit the security of software and web applications, including source-code analysis.
- Keep web servers and database management systems up to date.
- Do not use libraries or frameworks with known vulnerabilities.

How users can avoid falling victim

Do not skimp on security

- Use only licensed software.
- Maintain effective antivirus protection on all devices.
- Keep software up to date. Do not delay installing patches.

Protect your data

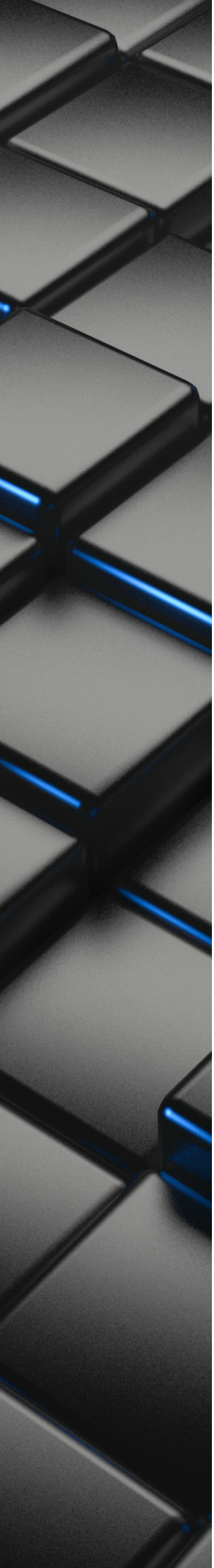
- Back up critical files. In addition to storing them on your hard drive, keep a copy on a USB drive, external disk, or a backup service in the cloud.
- Use an account without administrator privileges for everyday tasks.
- Use two-factor authentication where possible, such as for email accounts.

Do not use trivial passwords

- Use complex passwords consisting of at least eight hard-to-guess letters, numbers, and special characters. Consider using a password manager (secure storage with password generation feature) to create and store passwords securely.
- Do not re-use passwords. Set a unique password for each site, email account, and system that you use.
- Change all passwords at least once every six months, or even better, every two to three months.

Be vigilant

- Scan all email attachments with antivirus software.
- Be mindful of sites with invalid certificates. Remember that data entered on such sites could be intercepted by criminals.
- Pay close attention when entering passwords or making payments online.
- Do not click links to unknown suspicious sites, especially if a security warning appears.
- Do not click links in pop-up windows, even if you know the company or product being advertised.
- Do not download files from suspicious sites or unknown sources.

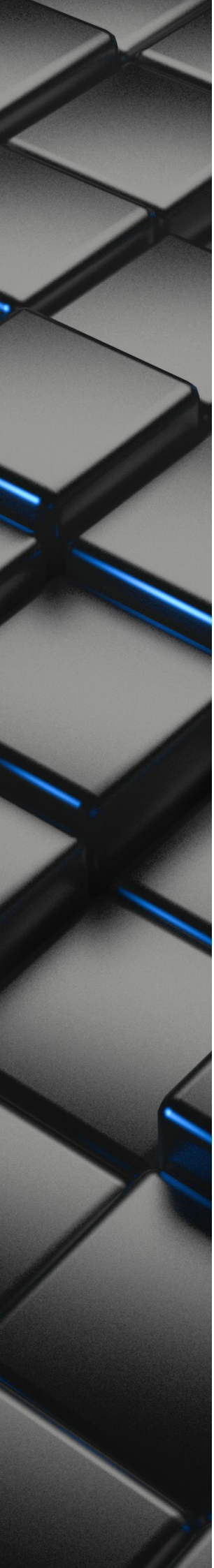


About the research

In this annual report, Positive Technologies shares information on the most important and emerging IT security threats. Information is drawn from our own expertise, outcomes of numerous investigations, and data from authoritative sources.

For the purposes of this report, any particular mass incident (such as a virus attack in which criminals send phishing messages to a large number of targets) is counted as one unique security threat. Terms used in this report:

- A cyberthreat is a combination of factors and circumstances that create the risk of information security compromise. In this report, we look at cyberthreats in terms of the actions of malefactors in cyberspace who attempt to breach an information system in order to steal money or data, or with other intentions potentially causing harm to government, business, or individuals. Attacker actions may be directed against the target company's IT infrastructure, workstations, mobile devices, other equipment, or at people as a factor in cyberspace.
- A cyberattack consists of unauthorized actions targeting information systems by cybercriminals leveraging techniques and software to obtain access to information, impair the normal functioning or availability of systems, or to steal, alter, or delete information.
- An attack target is the target of unauthorized actions by cybercriminals. In cases when social engineering is used to obtain information directly from an individual, client, or employee, the attack target is "Humans." On the other hand, when social engineering is part of an attempt to place malware on corporate infrastructure or on the computer of an individual, the attack target is "Computers, servers, and network equipment."
- Attack motive is the overall goal of cybercriminals. If an attack results in theft of payment card information, the motive is "data theft."
- Attack methods are a set of techniques used to achieve a goal. For instance, an attacker might perform reconnaissance, detect vulnerable network services available for connection, exploit vulnerabilities, and get access to resources or information. For the purposes of this report, such a process is referred to as "hacking." Credential compromise and web attacks were placed in separate categories for greater granularity.
- Victim categories are the economic sectors in which the attacked companies operate (or individuals, if the attack was indiscriminate with respect to employer). For example, the "Hospitality and entertainment" category includes companies providing paid services, such as consulting agencies, hotels, and restaurants. The "Online services" category includes platforms where users can fulfill their needs online, such as ticket and hotel aggregator websites, blogs, social networks, chat platforms and other social media resources, video sharing platforms, and online games. Large-scale cyberattacks affecting more than one industry (most often, malware outbreaks) have been placed in the "Multiple industries" category.



In our view, the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity by hacker groups are unable to perform a precise count. This research is conducted in order to draw the attention of companies and ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

Group profiles

APT-C-35 (Donot, SectorE02), active since 2016, attacks organizations in South Asia: Pakistan, Bangladesh, Sri Lanka, Maldives, Myanmar, Nepal, and countries of the Shanghai Cooperation Organization. The attackers take the guise of governmental institutions, military entities, and telecom companies.

APT28 (Fancy Bear, Sofacy), a cyberespionage group, has been active since at least 2004. The group became widely known after a series of attacks in the leadup to the 2016 U.S. presidential elections. In 2017 and 2018 the group attacked international organizations, military and defense contractors, and government institutions in Europe and South America. The group uses a variety of tools, including some of their own making.

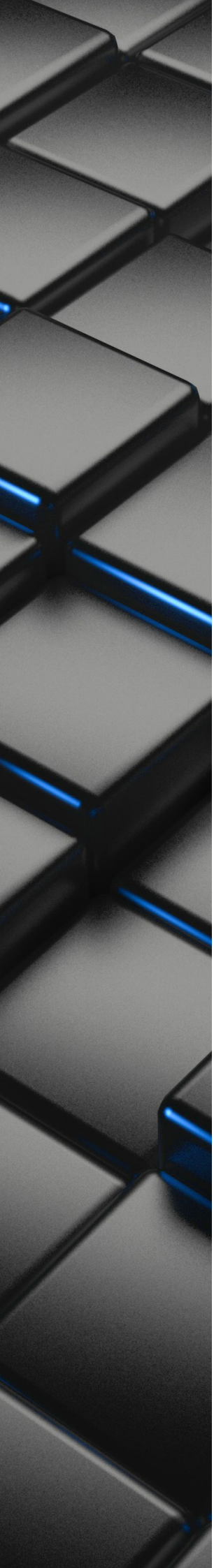
APT40 (Leviathan, TEMP.Jumper, TEMP.Periscope) has been known for spyware campaigns since 2013. This group attacks transport and government, science, education, and IT companies in Western Europe, North America, and Southeast Asia.

Bisonal is known for developing the malware of the same name. Its history dates back to 2014. The group attacks companies mostly in Russia, South Korea, and Japan.

Bronze Union, also known as TG-3390, LuckyMouse, APT27, or Emissary Panda, has been involved in cyberespionage attacks since 2010. To gain a foothold on networks, the group often uses watering hole attacks: they target the websites frequented by targeted users and place malware on the websites in order to automatically infect visitors' computers. Currently the group targets governmental entities and companies involved in industry, military manufacturing, energy, aerospace, and other high-tech fields around the world.

Cloud Atlas has been known since 2014 for their attacks on various companies in Russia, Central Asia, and Europe (especially Portugal).

Cobalt has been known since 2016 for its attacks on financial institutions. The group started off by stealing from banks in CIS countries. Since 2017, it has expanded its range of targets to include banks in Eastern Europe and Southeast Asia. The group was named after Cobalt Strike, the penetration testing software used by the group to develop attacks within target networks. Its primary method of breaching corporate networks is phishing messages with malicious files in various formats: executable files, Microsoft Office documents with macros or exploits, LNK files, and passworded archives containing executable files.



Gamaredon has been active since 2013. The attackers focus exclusively on Ukrainian governmental entities: the C2 servers perform filtering by geographic region. In their attacks, the group uses a chain of scripts to download the Ultra VNC remote management utility to the victim's computer. They use a self-developed framework named Pteranodon for full-fledged management of infected hosts. With it, the attackers can collect information about the system and users, steal passwords, run scripts and commands, and exfiltrate information to remote servers.

The history of **RTM** dates back to 2016. The group attempts to access corporate bank accounts and steal funds. They use phishing messages to obtain access to corporate networks. Since the very start, the group has used a consistent format in such messages. Positive Technologies data indicates that in 2018 alone, the group carried out 59 mailings, the recipients of which included financial institutions. In 2019, the group moved to use of the Bitcoin blockchain. Most targets are financial institutions, although cases have also included industry, government, and IT-related organizations. In addition, the group has used .bit domains for some of their C2s. The .bit zone is powered by the Namecoin blockchain, which acts as a censor-proof and confiscation-resistant alternative to traditional DNS registrars. Experts at the PT Expert Security Center were able to use the blockchain architecture to devise an algorithm for monitoring registration of new domains by RTM and changes in their IP addresses. This enabled warning financial institutions and the security community of new C2 servers in a matter of minutes (or sometimes even before) they entered use by the attackers.

SongXY was discovered in 2017 by Positive Technologies experts. The group's victims include at least 17 companies from Russia, Japan, Mongolia, Belarus, the United States, Tajikistan, Uzbekistan, Kyrgyzstan, Kazakhstan, and Ukraine. The group attacks defense and industry. They use emails to deliver Lurid and Gh0st malware that can steal data, take screenshots, and record audio from the victim's microphone.

TA505 has operated since 2014. The group's targets include major financial, manufacturing, transportation, and governmental entities in Canada, South Korea, the United Kingdom, the United States, and dozens of other countries. Phishing messages are the group's main method for penetrating target networks. With each new wave of attacks, the group has made qualitative changes to its toolkit and advanced to more sophisticated techniques for maintaining stealth. Since 2014, the group's arsenal has included the Dridex banking Trojan, Neutrino botnet, and several families of ransomware, including Locky, Jaf, and GlobeImposter. Since spring 2018 the group has used the FlawedAmmyy remote access Trojan, and since late 2018, the new ServHelper backdoor.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

ptsecurity.com
info@ptsecurity.com

Cybersecurity_threatscape-2019-Q4_A4.ENG.0002.03