→ New Botnets → Affiliate Programs → Network Compromise

HI-TECH CRIME TRENDS 2020 / 2021

NOVEMBER 2020

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains recommendations on how to protect against future attacks. The details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. Any information outlined in the report is not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

TABLE OF CONTENTS

INTRODUCTION

As the world continues to be rocked by an unpredictable pandemic, with borders still closed, businesses struggling to stay afloat, and political confrontations becoming increasingly hostile, one thing has remained constant: The steady growth of cybercrime.

For 17 years, Group-IB has dedicated its efforts to investigating cybercrime, monitoring the evolution of attackers' tactics and instruments, and developing innovative technologies to hunt for and eliminate cyber threats. The company actively shares its insights and investigations with the expert community and general public, and this expertise culminates in the annual Group-IB Hi-Tech Crime Trends report.

In their new report, **Hi-Tech Crime Trends 2020-2021**, Group-IB experts name the key changes that have occurred in the field of high-tech crime, revealing the inner workings of the cybercrime underground, communication between different threat groups, and affiliate programs that sell malware and other malicious services. Traditionally, Group-IB investigates not only attacks on the commercial sector but also those on critical infrastructure. The latter are typically the result of covert activities conducted by the special services of various countries around the world.

Hi-Tech Crime Trends gives you access to the most complete trove of strategic data and detailed information on active cyber threats. By reading the report, you will get the answer to these burning questions:

— Who are your enemies in cyberspace?
— How do they operate today?
— How will their toolkits adapt for future attacks?
— How can you protect yourself against them?

Armed with this knowledge, companies worldwide, regardless of industry, will be able to build more effective cybersecurity strategies.

The paralysis of entire economic sectors, mass transition to remote work, and widespread layoffs have led to a surge in cybercriminal activity. Threat actors have taken advantage of the unique global situation and become more creative, developing increasingly elaborate schemes to achieve their illicit goals. In the spring of 2020, Group-IB experts predicted that there would be a growth in the number of financial crimes, and cyberattacks on the computers, computer equipment (routers, web cameras), and unprotected networks of at-home workers. Those employees working in financial institutions, telecom operators, and IT companies would be the primary targets. Unfortunately, the predictions were right.

During the pandemic, Group-IB analysts noticed a spike in the number of cyberattacks originating from state-sponsored threat actors and criminals using spyware, ransomware, and backdoors to exploit people's fears and anxiety over the coronavirus. The analysts also noted that attackers actively looked for ways get into enterprise networks, a goal they achieved by infecting the computers of remote workers with malware.

While the overall number of successful targeted attacks on banks went down, Group-IB analysts discovered a shocking increase in the use of social engineering to commit fraud. The main attack vectors are vishing and phishing, whose victims are mainly bank customers. The fraudsters' main goal is still to steal money and information that can be sold, but they go about it in a new way.

The past year saw the majority of cybercriminal groups switch to working with ransomware. With ransomware in their arsenal, attackers are able to earn no less than they would in a successful bank attack and with a much easier technical execution. Big Game Hunting, or attacking large companies with the aim of collecting the largest possible ransom, is gaining momentum. New groups are joining the game and creating dangerous affiliations and partnerships in the cybercrime underworld.

The market for Cybercrime-as-a-Service is actively developing. The phenomenon directly correlates with the renting out of computer networks that are infected with malware (botnets) and used for organizing DDoS attacks, sending phishing emails, and providing proxy servers. There have emerged new sellers of network access who form partnerships with ransomware operators and APT groups that have shifted their focus from bank theft to working with private affiliate programs. State-sponsored threat actors have likewise jumped on bandwagon, opening the doors of corporate infrastructure to ransomware. This threat has become larger than life and can no longer be ignored by any company, no matter its industry or geographic location.

We are confident that with the constant exchange of information, joint efforts to maintain stability in the global cyberspace, and the creation and development of partnerships between private companies and international law enforcement agencies, we can effectively combat cybercrime. By raising the global community's awareness of cybercrime, we can help preserve and protect the opportunities cyberspace give us.

KEY FINDINGS AND FORECASTS

Ransomware attacks

Current threats

The main goal:

create access to corporate networks for ransomware purposes

Ransomware affiliate

programs shape the market of corporate network access for sale

— Over the past year, seven new ransomware affiliate programs have emerged (bringing the total to 15), which has shaped the market of corporate network access for sale.
— Between H2 2019 and H1 2020, the number of access for sale offers has increased 2.6-fold (from 138 to 362) compared to the previous period.
— There are more and more users who actively sell access to corporate networks. In 2019, there were 50 active sellers; in the first half of 2020, Group-IB identified 63.
— Owners of the banking botnets TrickBot, Qbot, Silent Night, and RTM have started using their botnets to deploy ransomware.
— The cybercriminal groups Cobalt and Silence, which had previously focused on targeted attacks on banks, have presumably joined ransomware affiliate programs.
— Primitive errors (such as vulnerable software versions in public services or weak passwords) pose one of the most serious risks to companies. If a vulnerable system is compromised, adversaries will usually attempt to inflict as much damage to the business as possible, followed by extortion.
— Ten ransomware affiliate programs involve brute-force attacks on servers accessible externally through Remote Desktop Services. Three programs exploit vulnerabilities in VPN services.
— New botnets that perform distributed brute-force attacks on remote access interfaces (RDP, SSH, VPN) and other services have been identified.
— One of the most common ways that victims are tricked into paying ransoms is stealing data from the network and threatening to leak the information online.
— In an effort to increase their profits, some groups have conducted auctions to sell stolen data instead of publishing it online.
— Ransomware proved so popular that criminals began to publish ready-made ransomware-as-a-service (RaaS) projects for Linux, MacOS, and Windows (e.g., the RAASNet project) on websites such as GitHub.
— Cybercriminals have mainly used two post-exploitation frameworks to move laterally and gain control over targeted corporate networks: a free tool called Metasploit and a cracked version of Cobalt Strike. Less often, adversaries used the frameworks PoshC2 and Koadic. During the reporting period, Group-IB experts identified more than 10,000 hosts with these frameworks installed. Between H2 2018 and H1 2019, Group-IB researchers identified around 6,000 such hosts.
— The countries attacked the most often were the USA, the UK, Canada, France, and Germany. They suffered 381 attacks out of 505, i.e. 75%.
— The most attacked sector was manufacturing. Half of all attacks targeted entities in the manufacturing, trade, government, healthcare, construction, and academic sectors.
— Group-IB identified cases of threat actors using new ransomware designed to disrupt processes associated with industrial network applications. Such tools help cybercriminals encrypt valuable data at manufacturing plants more effectively.

Forecasts

— Group-IB expects that specialized trading platforms will emerge for exhibiting lots with access to corporate networks, which may lead to even more related incidents.
— We expect that there will be more demand for Linux malware designed to achieve persistence in the network and escalate privileges.
— IoT botnet owners may start selling access to devices installed on corporate networks.
— New botnets and related criminal services for distributed brute-force attacks on remote control interfaces will emerge.
— The number of ransomware affiliate programs will grow for a brief time only. Group-IB expects that the market will stabilize and that numbers will stop increasing by the end of 2020.
— There may be cases of ransomware attacks targeting company mail systems. Hackers are likely to steal data from local mail servers and disable the mail system — bearing in mind that stable email communications are critical to businesses. This may lead to cloud mail services becoming more popular and the on-prem mail storage model being abandoned.
— Groups that focus on attacks on SCADA systems at industrial enterprises in order to manipulate production processes may emerge.
— Intelligence services may be interested in owners of affiliate programs and use them to access networks of interest.
— To inflict maximum damage on entities and divert attention away from their attacks, special services may start mimicking criminals by spreading documents that undermine the attacked organization's business operations or by selling access to the affected corporate networks.

Military operations

Current threats

More and more often espionage is replaced by active attempts

to destroy infrastructure facilities

High-profile attack targets include

nuclear facilities in Iran and India and Israel's water supply system

— Intelligence agencies are attacking more aggressively. Their goal is now not only to spy on targets covertly but also destroy critical infrastructure facilities.
— During the reporting period, seven new APT groups were identified. Group-IB also identified six known threat groups that had remained unnoticed for many years.
— As part of an APT operation, adversaries shut down power units at nuclear power plants and physically destroyed the surrounding infrastructure.
— A major cyberattack on a water management facility was thwarted. During the incident, threat actors attempted to poison water by altering water chlorine levels. Had it been successful, the civilian population in the country would have been seriously affected.
— Some country leaders began openly announcing successful attacks on other countries.
— Hacker arsenals were actively replenished with tools designed for attacks on air-gapped networks. Over the past year, four tools using USB for bridging the air gap have been identified.

Forecasts

— Against the backdrop of rising tension in the Middle East, attacks on the control systems of transport ships in the Persian Gulf may be carried out.
— Group-IB expects more sabotage operations against Iran's critical infrastructure facilities, especially those related to nuclear energy.
— Security vendors have begun developing features for detecting backdoors at the UEFI level more actively. Such tools will help detect new UEFI malware leveraged during military operations.
— New achievements made by Elon Musk's companies in the space industry may attract the attention of special services, both for espionage purposes and in order to gain control over the control systems of his satellite internet constellation.

Threats to the telecommunications sector

Current threats

State-sponsored groups
show an interest in the telecom sector and conduct sophisticated attacks against it

2.3 Tb per second and 809 million packets per second
new records in DDoS attack power

— During the reporting period, six groups linked to special services actively attacked the telecommunications sector.
— China is expanding its capacities in spying on mobile operators. To this end, it has developed a special Trojan for Linux servers that intercepts SMS messages based on specific criteria.
— Threat actors have set new records in DDoS attack power: 2.3 Tb per second and 809 million packets per second.
— 5G networks have not been widely deployed yet, which explains why the predictions relating to associated threats that we made in our previous report have not come true. They are relevant for the next period, however.
— BGP hijacking and route leaks remain a serious problem. Over the past year, nine significant cases have been publicized.

Forecasts

— As interstate conflicts continue to escalate, it is expected that threat actors will attack telecom operators for the first time in order to cause logical network congestion, which would lead to a cascading effect and affect multiple industries.
— The COVID-19 pandemic has forced a significant number of people to work from home, and many of them will become permanent work-from-home employees after the pandemic ends. As such, the number of attacks on home routers and storage systems will continue to increase given that they help advanced crime groups and state-sponsored actors access corporate data without infiltrating an organization's perimeter.

Threats to the energy sector

Current threats

Both state-sponsored groups and organized crime actors

disrupt facilities and encrypt data in order to demand ransoms

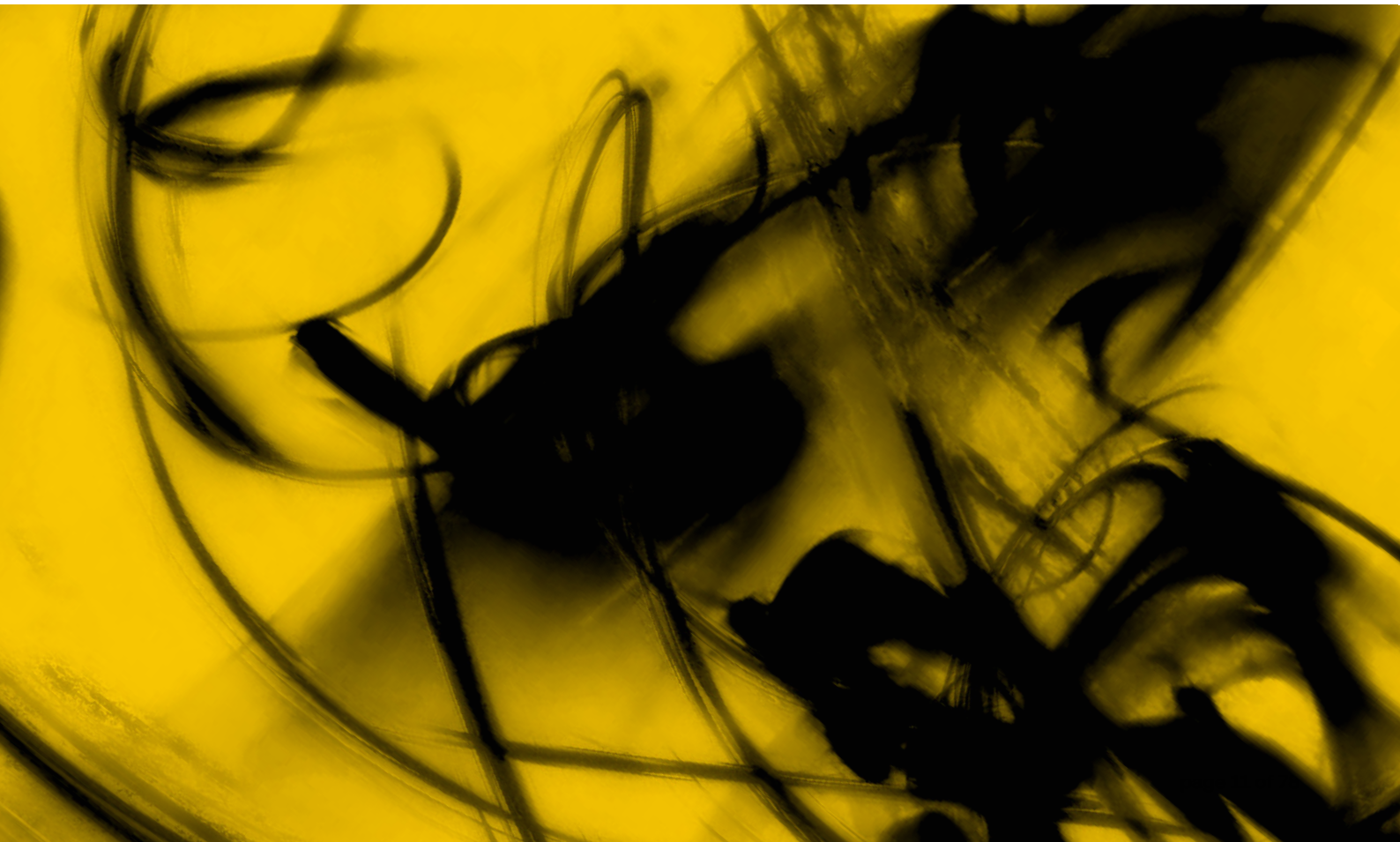
Air gap bypassed:

new tools for attacks on isolated networks discovered

- Adversary arsenals were actively replenished with tools designed for attacks on air-gapped networks. Over the past year, four tools using USB flash drives to bridge the air gap have been identified.
- Nuclear power has become an obvious target for attackers. No such attacks were reported in the past year. In the reporting period, however, Iran's nuclear energy facilities were sabotaged, while facilities in India were subject to espionage attacks. Threat actors are particularly interested in India because the country is developing nuclear technology and thorium-based reactors.
- No new frameworks able to influence technological processes were identified in the reporting period, which suggests that threat actors have become more careful about concealing their use of such tools.
- Organized crime groups have begun showing an active interest in energy companies. Targeted attacks are carried out to seize control over entire networks and infect infrastructure with ransomware.
- During the reported period, nine groups linked to intelligence services attacked the energy sector. Seven hackers reportedly sold access to energy networks. In addition, eleven successful attacks involving ransomware were conducted on the sector in question.
- Many types of ransomware have been equipped with new capabilities to detect processes associated with industrial control systems, which has led to substantial losses of critical data and increased ransom amounts for recovering access to such data. This is especially true for data stored on Historian servers.

Forecasts

- Espionage will remain the primary goal of state-sponsored threat actors.
- Sabotage attacks on the energy sector will be carried out in the Middle East or in countries with emerging military conflicts.
- To conduct attacks more effectively, threat actors will target not only large energy companies but also last-mile energy distributors and small suppliers that offer additional services to energy corporations.
- 5G networks will connect a large number of devices to global networks, including those belonging to energy and industrial enterprises. As a result, the attack surface will increase dramatically.
- Cybercriminals (mainly sophisticated hackers) will use the vector of initial infection through vulnerable network equipment more often. Less skilled criminals will use common phishing techniques.



Threats to the banking sector

Current threats

Targeted thefts are becoming rare cases

relevant only for poorly protected banks

Hackers gaining access and encrypting data to obtain hefty ransoms

is a trend in the banking sector

- In 2020, there have so far been no public reports on thefts through SWIFT, ATM Switch, payment gateways or ATMs when they were accessed through a bank's network.
- Nevertheless, the hacker group Lazarus reportedly continued to carry out theft attempts through SWIFT. To gain initial access, the hackers used a banking botnet called Trickbot controlled by Russian-speaking cybercriminals. Moreover, Group-IB researchers detected activity by another threat group that used publicly available Trojans, keyloggers, and unmodified exploits. Such toolsets are effective only against banks with a minimum level of security. Alternatively, during incident response, security teams may have made mistakes that prevented them from identifying more sophisticated tools.
- In the second half of 2019, only the group Silence carried out successful thefts without using SWIFT. They stopped attacking the financial sector in 2020, however.
- The Philippine government-controlled United Coconut Planters Bank (UCPB) was robbed in September 2020. The threat actors gained access to the card processing system and changed withdrawal limits. They also gained access to InstaPay, an interbank transfer system. As a result, they siphoned 167 million pesos (USD 3.44 million) from the bank.
- Tools used for attacks on ATMs have evolved slightly. During the reporting period, the following utilities were identified: ATMDtrack developed by Lazarus and a new version of the ATM Trojan developed by Silence. It has not been confirmed whether either utility has been successfully used in thefts.
- Cobalt and Silence have presumably joined ransomware affiliate programs, but they have shifted their focus from banks.

Forecasts

- Next year, there will probably be no traditional attacks on banks for theft purposes. There may be rare incidents, but this type of activity will no longer be as widespread as it used to be.
- As with other sectors, ransomware operators will pose the biggest threat to the financial vertical. This hypothesis is confirmed by the increasing number of offers selling access to corporate networks belonging to financial institutions.
- However, stealing information about financial transactions of VIP clients and publishing it online may become a more serious threat than data encryption. Such attacks may cause significant financial damage and make banks pay ransoms to threat actors more readily.
- Disclosing financial transaction data could launch a series of investigative journalism cases similar to the Panama Papers case in 2015 (a massive exposure of confidential financial files belonging to Mossack Fonseca, a Panamanian law firm), in which some intelligence agencies are likely to be interested.
- Another trend may be threat actors threatening to send (fake) alerts to financial regulators notifying that a bank has security issues. Threatening to send such notifications may act as an incentive for banks to pay higher amounts to extortionists.

Threats to retail

Current threats

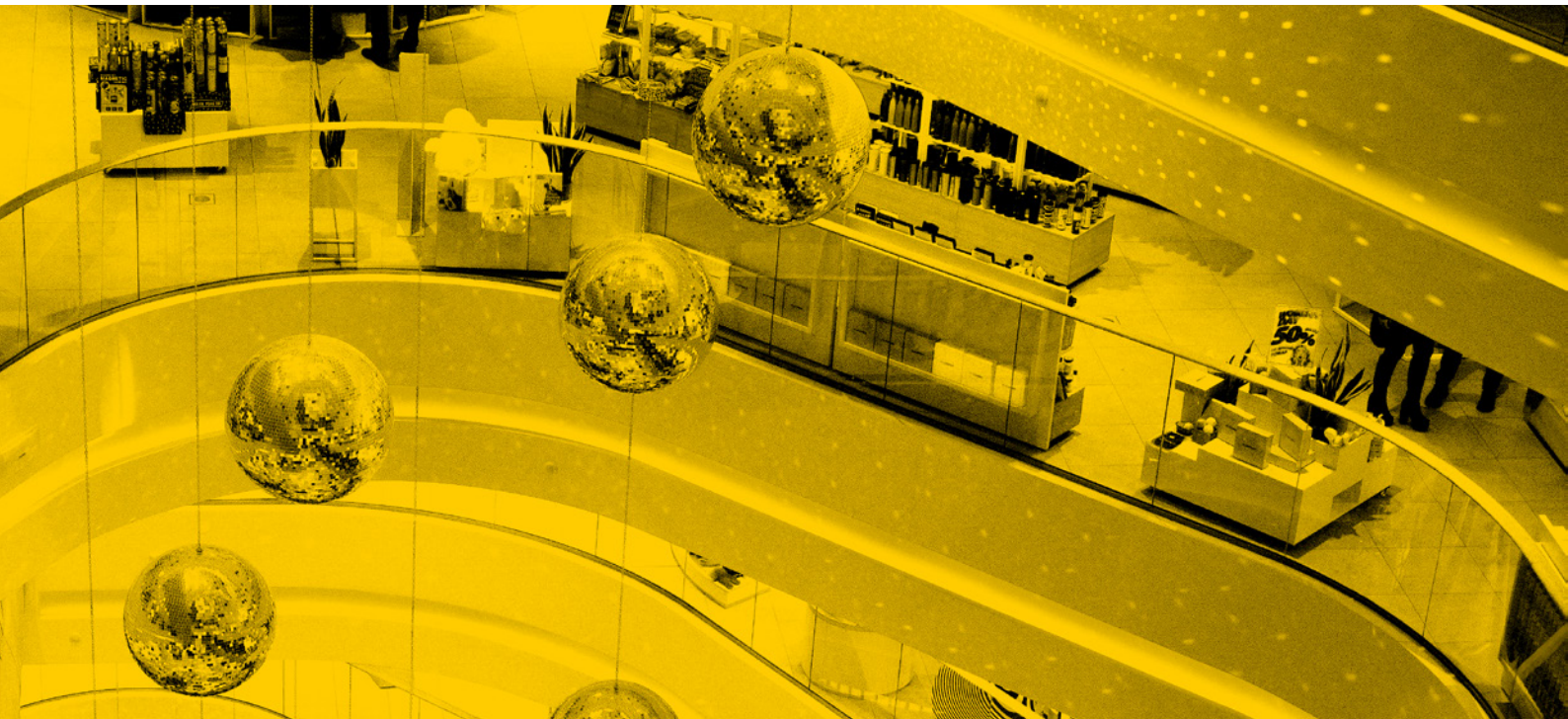
96 JS sniffer families
are currently being tracked by Group-IB experts

156% more bank card dumps
stolen using POS Trojans were offered for sale compared to the previous period

- It is possible to single out four main threats targeting retailers that may damage businesses: JS sniffers, attacks on POS terminals, credential stuffing, and ransomware.
- The number of known JS sniffer families has grown from 38 to 96 compared to the previous year.
- The state-sponsored threat group Lazarus has started using JS sniffers. The threat actor uses a JS sniffer variant that automatically steals funds from Bitcoin wallets.
- Techniques that prevent JS sniffers from being detected on web resources have improved greatly.
- The carding market has doubled from $880 million to $1.9 billion compared to the previous year.
- During the reporting period, 14 POS Trojans were found to be active. They were used to compromise and sell 63.7 million bank card dumps, which is 156% more than in the previous year.
- The amount of bank card textual details offered for sale has increased from 12.5 million to 28.3 million. The largest bank card data leaks are due to US retailers being compromised.
- During the reporting period, 19 compromised retailer networks were identified, compared to 17 in the previous year.
- Scammers primarily targeted bank cards issued in the United States, which accounts for more than 92% of all card dumps, followed by India and South Korea.
- Although many vendors offer solutions for protecting against bots and attacks such as credential stuffing, threat actors continue to actively use bots without browsers, which offers opportunities to create more advanced tools for bypassing defenses as well as possibilities to develop the cybercrime market in this direction.

Forecasts

- Many online resources are hacked every day. Currently, the main monetization methods used by hackers are selling databases and hosting phishing pages. However, damage to businesses may increase drastically, and along with it the profits made by cybercriminals if the latter begin actively cooperating with ransomware developers.
- Hacker groups using JS sniffers will pose a major threat to online retailers, especially in the US. At the same time, the main business risks will be associated with fines for security violations rather than with compensation for damage to customers or reputational losses.
- Attacks on computers with connected POS terminals aimed at collecting bank card dumps will remain a major threat in the United States.
- Scammers often use a fraudulent scheme as part of which they perform financial transactions in a given location, then use access to POS terminals to cancel the operations in other countries. The actions restore the card balance, and the cybercriminals can continue to perform fraudulent financial transactions. We may see similar new schemes involving access to online resources that accept card payments.
- The carding market keeps growing. However, arrests of main players may stop this growth and redistribute carding activity between criminals.
- The main schemes for obtaining bank cards and the list of popular target countries are unlikely to change.
- Carders may become more active in Latin America, where there is a large community of hackers with experience in using financial Trojans.



Banking Trojans

Current threats

19 PC Trojans and 10 Android Trojans
have been active this year

Owners of banking botnets
are switching to ransomware

— Latin America, particularly Brazil, has become the main source of new banking Trojans.
— Russian-speaking owners of the largest banking botnets (Trickbot, Dridex, Qbot, and Silent Night) have been following the main trend and switching to ransomware.
— A total of 19 PC banking Trojans were active this year, 12 of which were written by Russian-speaking developers. Six Trojans were developed by Latin American authors. One tool could not be attributed.
— In total, 10 Android banking Trojans were active this year. Five of them are brand new.

Forecasts

— Russian-speaking owners of banking botnets for both PCs and Android devices will reduce their activity even further. Eventually, such botnets will cease to exist.
— As banking Trojans become more active in Latin America, some of their owners are likely to be arrested, which will also reduce this threat significantly.
— Every year, three to five banking botnets for PCs disappear from the market. At this rate, the market for PC banking Trojans may become nonexistent in three to five years. A similar situation may occur with the market for Android Trojans, which are becoming less and less effective year after year.

Web phishing and social engineering

Current threats

A 118% growth
in phishing compared to the previous year

New trend:
using one-time links
to phishing websites

— Over the period investigated, 118% more phishing resources were identified and taken down compared to the previous reporting period.
— The COVID-19 pandemic has encouraged more cybercriminals to become involved in phishing attacks, which is one of the key reasons for the above-mentioned rise.
— Phishing attacks targeting bookmakers increased in Q2 2020, amounting to 6% versus 2% in the previous quarter.
— Another attack type that increased by 9% was phishing used to collect accounts for various online services such as Microsoft, Netflix, Amazon, eBay, and Valve Steam.
— Phishing resources targeting cryptocurrency projects have disappeared almost completely.
— So far, the main trend in 2020 is the use of one-time unique links that become inactive after the user opens them. This approach helps cybercriminals keep web phishing resources from being detected.
— In Russia, the main reason for the significantly higher numbers of phishing attacks is the emergence of various affiliate programs for hackers wanting to make money off phishing related to fake bank rewards programs, lottery draws, paid surveys, etc.
— Phishing-as-a-Service projects have become widespread in Russia.

Forecasts

— Phishing affiliate programs that have become more popular in Russia will be more actively used in other regions.
— Phishing attacks have become automated and longer-lasting thanks to the emergence of scams propagated through the Phishing-as-a-Service model. We expect that such projects will be actively developed and distributed.
— One of the greatest challenges for the cybersecurity industry will be hackers using one-time web phishing links.

KEY TRENDS

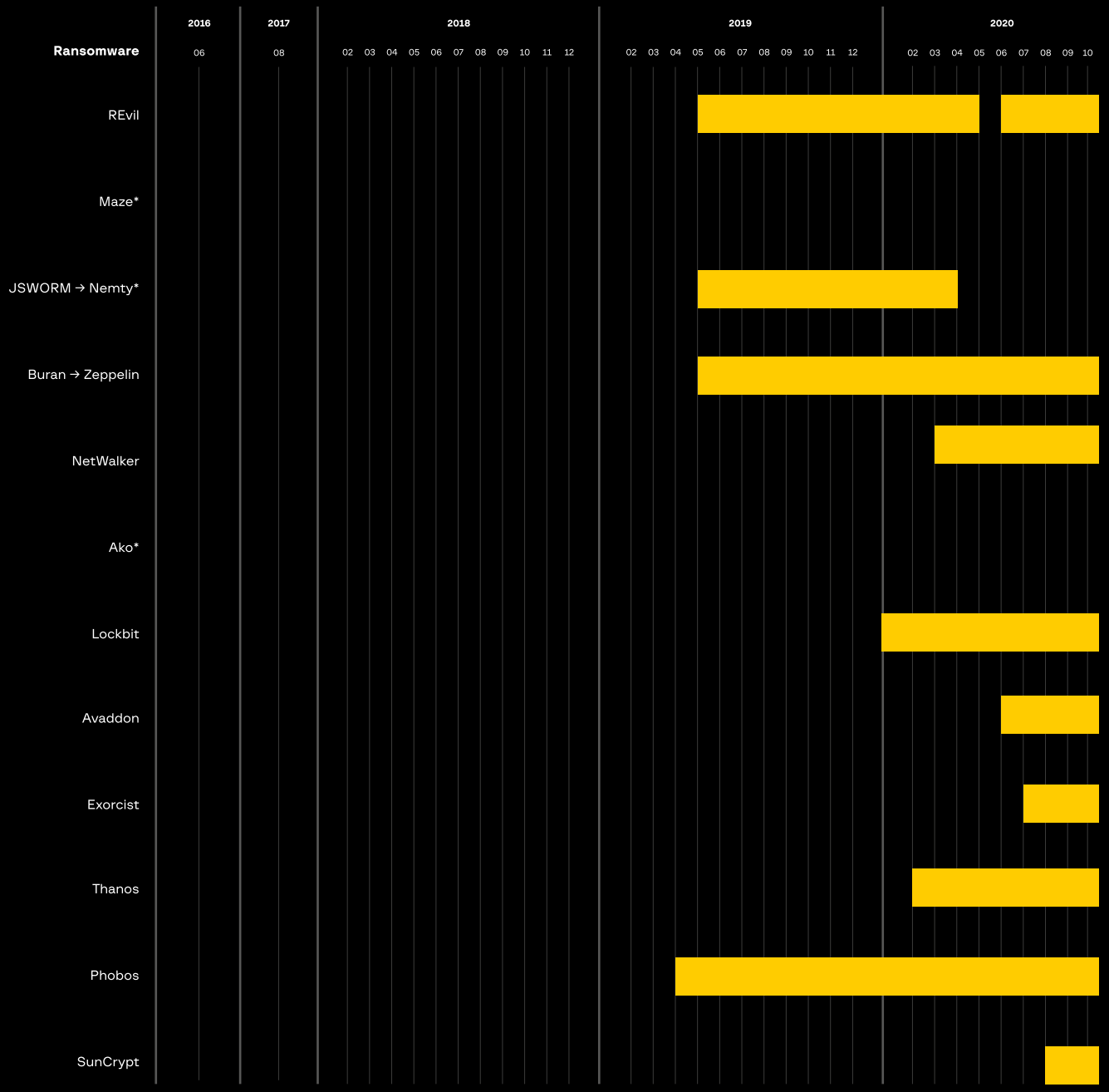
Gaining access to corporate networks for ransomware purposes

The emergence of ransomware affiliate programs

Going into 2019, many ransomware operators shifted their focus from ordinary users to companies, government agencies, and other victims that would help them pocket more money. Yet ransomware developers often lacked the tools and capabilities to infiltrate corporate networks. As a way to get around this problem, they began setting up affiliate programs. The scheme works as follows: threat actors who specialize in penetrating corporate networks monetize their actions by distributing ransomware. After the victim pays the ransom, the ransomware authors send a cut to their affiliates.

There are two types of affiliate programs: public and private. Public programs first emerged in mid-2019. Their distinctive feature is that the developers look for affiliates on underground forums. Private affiliate programs, on the other hand, are not advertised and are intended to bring together other types of threat actors (e.g. APT groups) and trusted users.

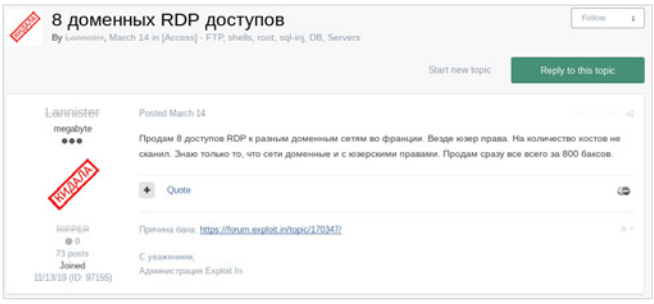
The table below contains information on affiliate programs related to the most popular ransomware.



* Private affiliate program

Many affiliates prefer to keep their activities under the radar. However, analyzing their activity in the hacker community and information obtained during incident response procedures has made it possible to identify some of them. Some users who showed an interest in affiliate programs on underground forums were involved in either selling access or working with various malware (including stealers). Examples of access are presented below.

Figure 1-2. Access for sale offers on underground forums

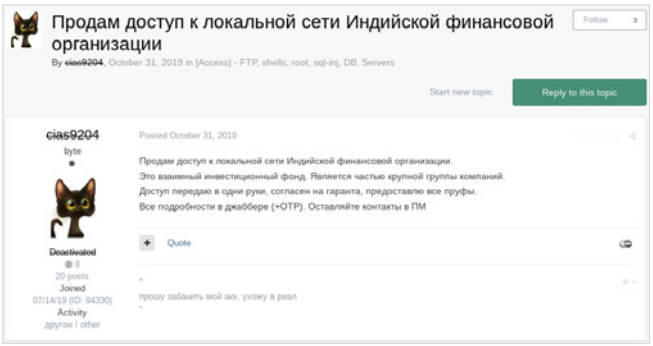


~~Lannister~~
Megabyte

Scammer

73 posts
Joined
11/13/19

8 domain RDP accesses
Posted March 14
I'm selling 8 RDP accesses to various domain networks in France. All have user access. I haven't scanned them for hosts. I just know that they are domain networks and have user rights.
I want to sell them all together for just $800
Reason for ban: [link]
Respectfully,
Exploit.In administration



~~cias9204~~
byte

~~Deactivated~~

20 posts
Joined
07/14/19
Activity
Other

Access to a local network of an Indian financial institution
Posted October 21, 2019
I'm selling access to the local network of an Indian financial institution. This is a mutual investment fund that belongs to a large group of companies. I will sell this access to a single customer and agree to work through an escrow service. I will provide all the proof required. All details will be provided in jabber (+OTP). Please share your contact details via PM.
Please ban my account as I want to leave the forum.

Initial compromise vectors

Most often, the initial intrusion vector was a malicious email campaign, a brute-force attack against Remote Desktop Protocol (RDP), or the exploitation of public-facing applications (including VPN-related).

In addition, other methods of distributing ransomware included exploit kits, VPNs, botnets, and other malware (e.g., downloaders). Supply-chain attacks are extremely rare (the case of REvil). In general, the above delivery methods are also relevant for ransomware distributed without affiliate programs.

The table below contains information about ransomware affiliate programs and the initial compromise methods used by their operators.

Ransomware	Phishing	Exploit Public-Facing Application	External Remote Service	Supply Chain Compromise
REvil	●	●	●	●
MegaCortex	●		●	
Maze	●	●	●	
Dharma			●	
JSWORM → Nemty	●	●	●	
Buran → Zeppelin	●	●	●	
NetWalker	●		●	
Ako	●	●	●	
Lockbit			●	
Avaddon	●	●		
Thanos	●		●	

Post-compromise

Once inside, many ransomware operators first attempt to escalate privileges by using exploits or post-exploitation frameworks. They then gain access to other accounts using various software (e.g., Mimikatz, LaZagne) or brute-force attacks.

Threat actors then perform network reconnaissance using legitimate network scanners or frameworks such as Cobalt Strike and Metasploit. They collect information about the system, groups, network resources, password policy, domain trust relationships, and more. The table below shows what frameworks were used by ransomware operators.

Ransomware	Cobalt Strike	Metasploit	CrackMapExec	PoshC2	Koadic	PowerShell Empire
Ryuk	●	●				●
REvil		●	●			
MegaCortex	●					
Maze	●					
DoppelPaymer				●	●	
Clop	●	●				
Lockbit			●			

Stealing and publishing data

In the early days, cybercriminals only encrypted data and demanded ransoms from victims. Since the end of 2019, however, many have started using a new technique: before encrypting all the information, they copy it to their servers for further blackmailing. They usually use the HTTP, HTTPS, and FTPprotocols and legitimate cloud storage services. On rare occasions, they use email and instant messengers.

In such cases, if the victim fails to pay the ransom, then in addition to the data being stolen, the ransomware operators will publish them online. To do so they create special websites, usually in the Tor network. An example of such a website is shown below.

Figure 3. Stolen data goes online

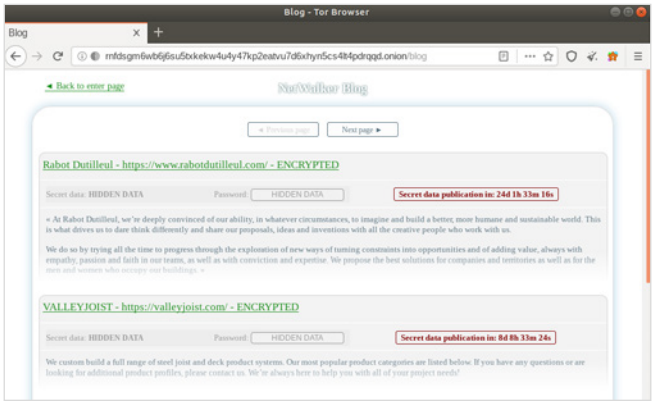
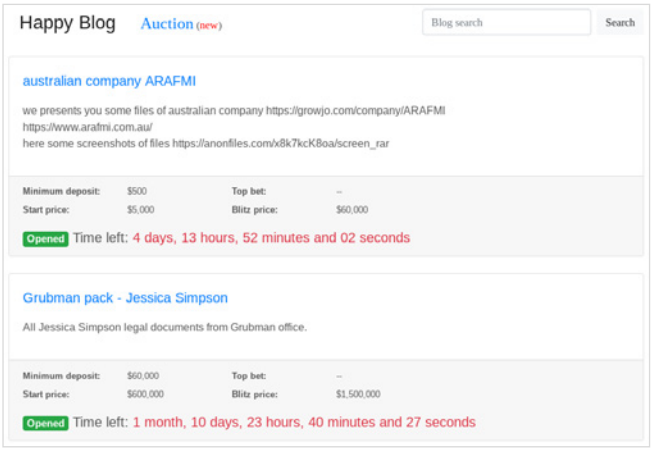


Figure 4. REvil auction



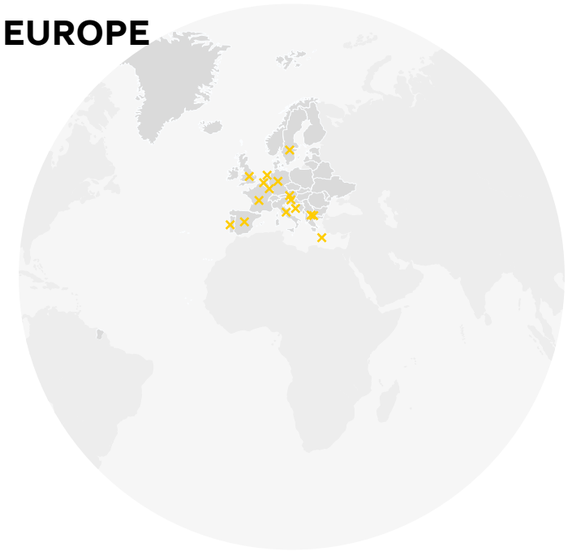
Attack statistics

Ransomware victims include both small local companies and international giants. Over the last year, there have been reports of more than 500 successful attacks using well-known ransomware on companies in more than 45 countries. The total number of successful attacks is much higher, but either the companies affected decided not to publicize the incident and pay the ransomware or the attack did not involve publishing data stolen from the victim's network.

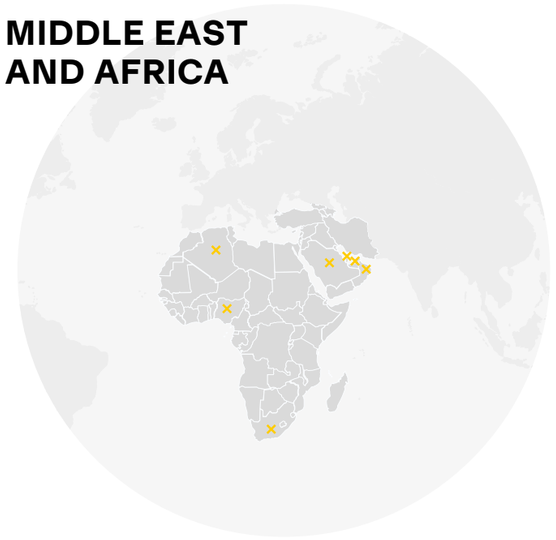
The most popular targets (about 60%) were US companies. European countries accounted for only about 20% of all attacks. About 10% were countries in North and South America (excluding the USA) and Asia (7%).

NORTH AND SOUTH AMERICA

EUROPE



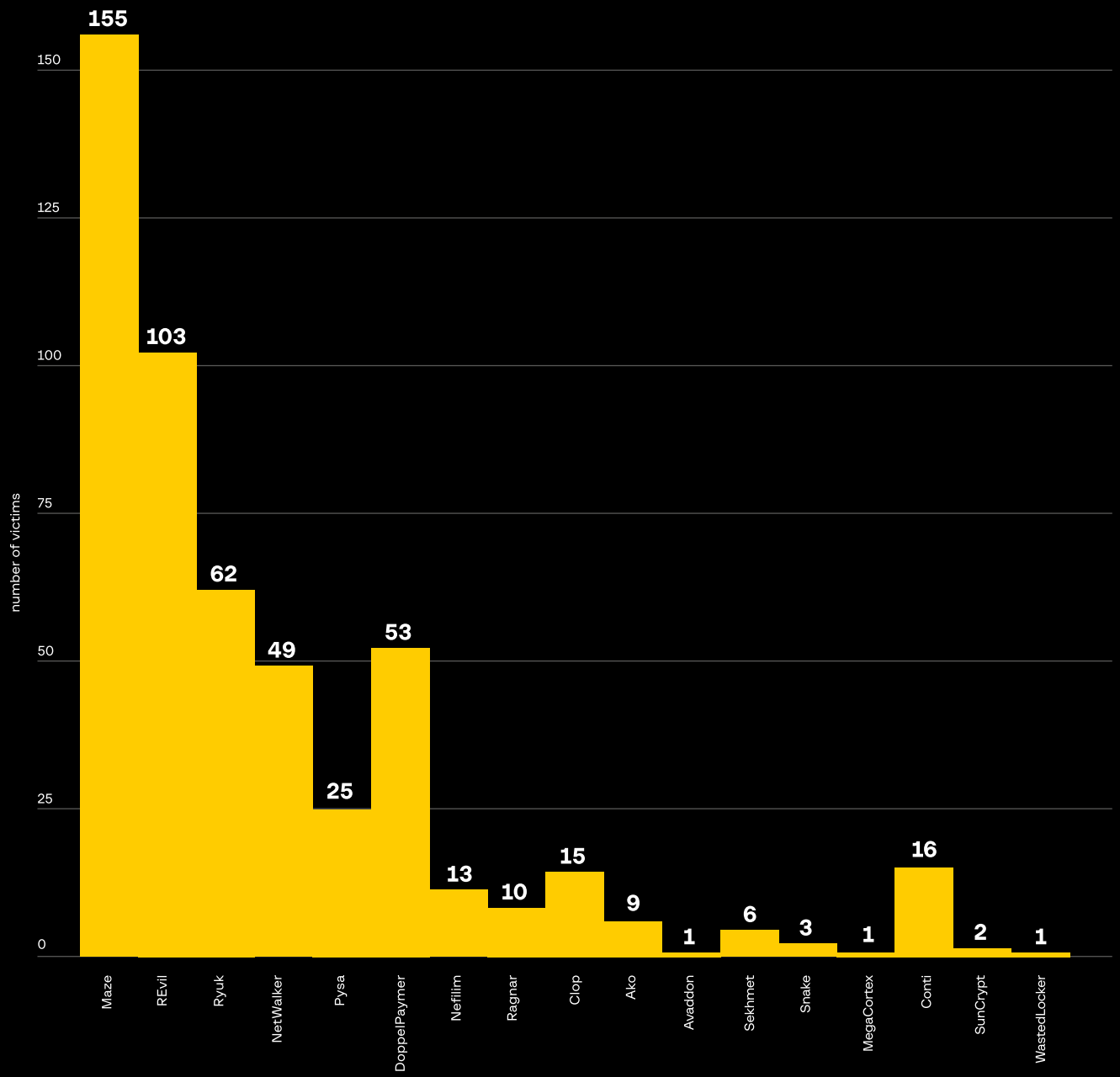
MIDDLE EAST AND AFRICA



SOUTHEAST ASIA AND AUSTRALIA

Statistics by country	
Country	Number of victims
USA	313
UK	25
Canada	24
France	20
Germany	17
Australia	13
Spain	11
Brazil	9
Italy	9
Switzerland	7
UAE	6
India	6
South Africa	5
Mexico	4
China	4
Colombia	4
Belgium	3
Saudi Arabia	3
Costa Rica	3
Thailand	2
Austria	2
Hong Kong	2
South Korea	2
Japan	2
Argentina	2
Oman	2
Kosovo	1
Singapore	1
Qatar	1
Philippines	1
Portugal	1
Chile	1
Dominican Republic	1
Jamaica	1
Unknown	1
Sweden	1
Slovenia	1
Cayman Islands	1
Sri Lanka	1
New Zealand	1
Cyprus	1
Algeria	1
Nigeria	1
Puerto Rico	1
Luxembourg	1
Macedonia	1
Croatia	1
Netherlands	1
Vietnam	1
Total	523

Statistics by sector	
Sector	Number of victims
Manufacturing	94
Trade	51
Government	39
Health Care	38
Construction	30
Educational Services	29
IT	28
Legal Services	20
Transportation and Warehousing	18
Administrative and Support and Waste Management and Remediation Services	14
Telecommunications	12
Accounting	11
Conglomerate	3
Consulting	9
Engineering	9
Data Processing, Hosting, and Related Services	9
Design	8
Real Estate and Rental and Leasing	8
R&D	7
Insurance	7
Investments	6
Lending	6
Mining, Quarrying, and Oil and Gas Extraction	6
Other	6
Agriculture, Forestry, Fishing and Hunting	5
Energy	5
Bank	4
Marketing	4
Non-Profit	4
Newspaper publisher	3
Travel Agency	3
Unknown	3
Hospitality	3
Arts, Entertainment, and Recreation	2
Broadcasting	2
Gambling	2
Aviation	2
Auction	1
Automobile	1
Food	1
Management of Companies and Enterprises	1
Transport	1
Professional Organization	1



155

TARGETED ATTACKS

were conducted by Maze ransomware operators

Maze and REvil have been the most active ransomware since late 2019, accounting for over 50% of successful attacks. Ryuk, NetWalker, DoppelPaymer are in the second tier.

The most often attacked sector was manufacturing. Half of all attacks targeted entities in the manufacturing, trade, government, healthcare, construction, and academic sectors. Although they currently focus on the above industries, affiliates usually seek easier targets, which explains the wide distribution of attacks across different verticals.

Ransomware **Maze** — Victims **155**

Top 5 attacked countries

USA	93
Canada	8
France	6
Italy	6
UK	6

Top 5 attacked sectors

Manufacturing	30
Trade	19
Construction	15
Administrative and Support and Waste Management and Remediation Services	8
Health Care	7

Ransomware **REvil** — Victims **103**

Top 5 attacked countries

USA	63
UK	7
Australia	5
Switzerland	4
Canada	3

Top 5 attacked sectors

Manufacturing	20
Trade	17
IT	10
Legal Services	6
Government	4

Ransomware **Ryuk** — Victims **62**

Top 5 attacked countries

USA	53
Spain	5
Australia	1
UK	1
Germany	1

Top 5 attacked sectors

Government	16
Educational Services	14
Health Care	14
Newspaper publisher	3
IT	3

Ransomware **NetWalker** — Victims **49**

Top 5 attacked countries

USA	28
France	6
Canada	4
UK	2
Austria	1

Top 5 attacked sectors

Manufacturing	14
Health Care	6
Educational Services	5
Trade	4
Transportation and Warehousing	3

Ransomware **Pysa** — Victims **25**

Top 5 attacked countries

USA	5
UK	3
Canada	2
France	2
Mexico	2

Top 5 attacked sectors

Health Care	5
Government	3
Manufacturing	3
Construction	2
Educational Services	2

Ransomware **DoppelPaymer** — Victims **53**

Top 5 attacked countries

USA	35
France	5
Canada	3
Saudi Arabia	1
Qatar	1

Top 5 attacked sectors

Trade	8
Government	7
Manufacturing	6
Transportation and Warehousing	4
Construction	3

Ransomware **Nefilim** — Victims **13**

Top 5 attacked countries

Brazil	3
India	3
Germany	1
France	1
Switzerland	1

Top 5 attacked sectors

Manufacturing	4
Construction	2
Mining, Quarrying, and Oil and Gas Extraction	2
Transportation and Warehousing	1
Administrative and Support and Waste Management and Remediation Services	1

Ransomware **Ragnar** — Victims **10**

Top 5 attacked countries

USA	7
Portugal	1
Germany	1
Singapore	1
—	—

Top 5 attacked sectors

Marketing	2
Legal Services	2
IT	1
Manufacturing	1
Construction	1

Ransomware **Clop** — Victims **15**

Top 5 attacked countries

Germany	7
USA	2
Spain	1
Austria	1
UK	1

Top 5 attacked sectors

Manufacturing	6
IT	2
Transportation and Warehousing	2
Gambling	1
Government	1

Ransomware **Ako** — Victims **9**

Top 5 attacked countries

USA	6
UK	2
Canada	1
—	—
—	—

Top 5 attacked sectors

Construction	2
Legal Services	1
Design	1
Engineering	1
Manufacturing	1

Ransomware **Avaddon** — Victims **1**

Top 5 attacked countries

USA	1
—	—
—	—
—	—
—	—

Top 5 attacked sectors

Construction	1
—	—
—	—
—	—
—	—

Ransomware **Sekhmet** — Victims **6**

Top 5 attacked countries

USA	3
Brazil	1
UK	1
Spain	1
—	—

Top 5 attacked sectors

Manufacturing	2
Legal Services	1
IT	1
Insurance	1
Transportation and Warehousing	1

Ransomware **Snake** — Victims **3**

Top 5 attacked countries

Germany	1
Argentina	1
Japan	1
—	—
—	—

Top 5 attacked sectors

Health Care	1
Energy	1
Conglomerate	1
—	—
—	—

Ransomware **MegaCortex** — Victims **1**

Top 5 attacked countries

USA	1
—	—
—	—
—	—
—	—

Top 5 attacked sectors

Data Processing, Hosting, and Related Services	1
—	—
—	—
—	—
—	—

Ransomware **Conti** — Victims **16**

Top 5 attacked countries

USA	13
Canada	2
Spain	1
—	—
—	—

Top 5 attacked sectors

Manufacturing	3
Hospitality	2
IT	1
Insurance	1
Health Care	1

Ransomware **SunCrypt** — Victims **2**

Top 5 attacked countries

USA	1
Canada	1
—	—
—	—
—	—

Top 5 attacked sectors

Manufacturing	1
Design	1
—	—
—	—
—	—

Ransomware **WastedLocker** — Victims **1**

Top 5 attacked countries

USA	1
—	—
—	—
—	—
—	—

Top 5 attacked sectors

Manufacturing	1
—	—
—	—
—	—
—	—

Estimated damage

Unfortunately, it is difficult to establish the exact damage caused by ransomware groups. This is because the amount should include the ransoms paid by victims, losses caused by system downtime, and expenses of recovering internal systems. In addition, it is difficult to obtain information about all attacks because many companies pay ransoms without making this fact public.

What's more, the amount often varies from company to company:

— For example, the ransoms demanded by the group REvil depend on the size of the company and the number of infected hosts. If only one computer on the network is infected, the ransom amount is about $48,000; but if several machines within the company's network are infected, then the average ransom amount is $470,000. There were several cases when the amount exceeded $1,000,000. The average ransom amounts to $260,000.

— A group called Maze usually demands extremely high ransoms, i.e. beyond one million dollars. The average ransom is $2,420,000.

— Some groups such as WastedLocker carried out very few attacks, but the ransom amount exceeded $10 million.

— The same applies to MegaCortex ransomware. The exact number of attacks it has been involved in is unknown, but the ransoms reportedly vary from 20,000 to $5,800,000.

The table below details past ransom amounts

Group	Average ransom ($)	Number of victims	Potential damage ($)
Ako	300,000	9	1,800,000
Avaddon	7,500	1	7,500
Clop	400,000	15	6,000,000
Conti	200,000	16	3,200,000
DoppelPaymer	1,143,500	53	60,605,500
Maze	2,420,000	155	375,100,000
Nefilim	100,000	13	1,300,000
NetWalker	720,000	49	35,280,000
Pysa	None	25	None
Ragnar	7,750,000	10	77,500,000
REvil	300,000	103	30,900,000
Ryuk	1,451,500	62	89,993,000
Snake	None	3	None
SunCrypt	400,000	2	800,000

This means that if combined publicly known attacks and experts estimations of possible ransomware incidents, the total potential damage could exceed one billion dollars ($1,005,186,000).

The data above only covers known incidents and shows the lower end of the damage. It is just the tip of the iceberg. For example, only 62 incidents involving Ryuk and spread using the banking Trojan Trickbot have been reported.

According to Group-IB's statistics, however, the owners of the Trickbot botnet have successfully encrypted more than 2,500 different networks over the past year using ransomware such as Ryuk (later Conti), Kraken, and Thanos. This means that the 62 known incidents represent only 2.5 percent of all incidents. The actual damage is likely to be much greater.

As regards Dharma ransomware, its source code was put up for sale last year and could have been used by many groups. Given the circumstances, it is difficult to establish the damage caused.

$1 BLN

estimated total potential damage

Increasingly larger market for selling access to corporate networks

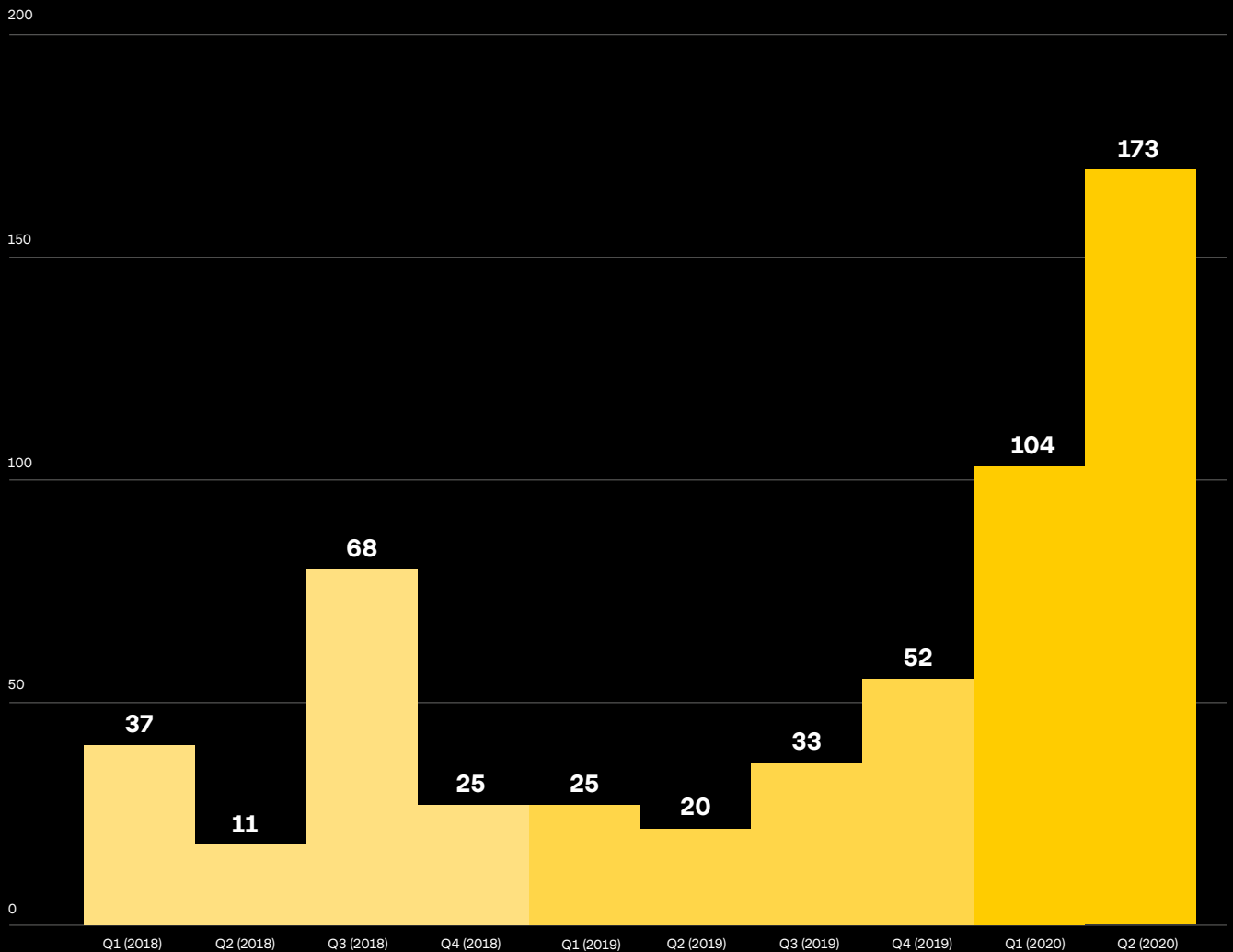
Sales of credentials are widespread on underground forums and have taken place since the early days of such communities. For a long time, cybercriminals did not perform additional reconnaissance after finding servers and gaining access to them, nor did they understand that the compromised servers could belong to large companies and that access to them could be capitalized on.

Sales of corporate network access are increasing from year to year. The peak of sales occurred in 2020, which is associated with an increase in the number of new ransomware affiliate programs. Between H2 2019 and H1 2020, the number of access for sale offers increased 2.6-fold (from 138 to 362) compared to the previous period.

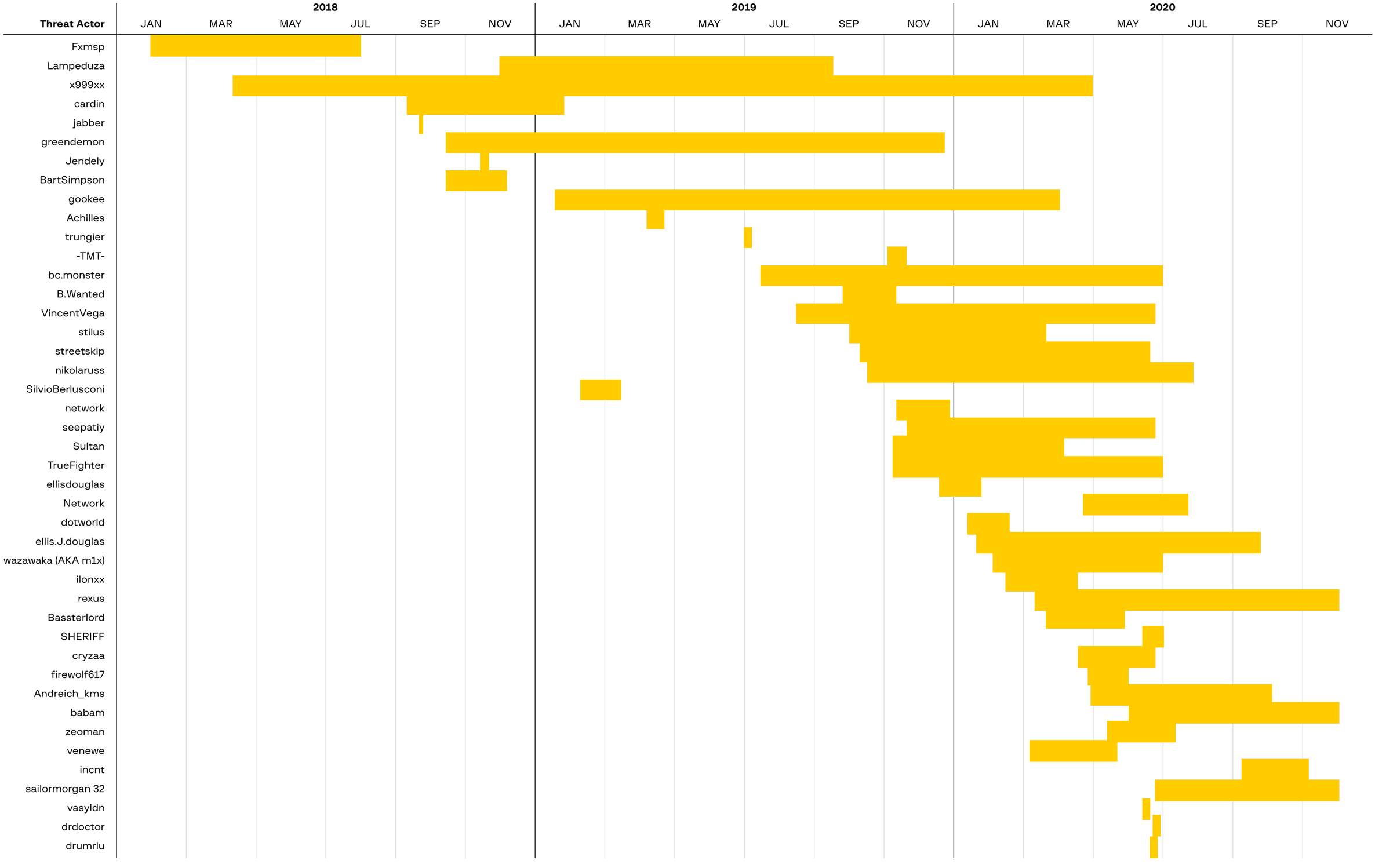
2018			
Q1	**Q2**	**Q3**	**Q4**
37	11	68	25
H1		**H2**	
48		93	
TOTAL			
141			

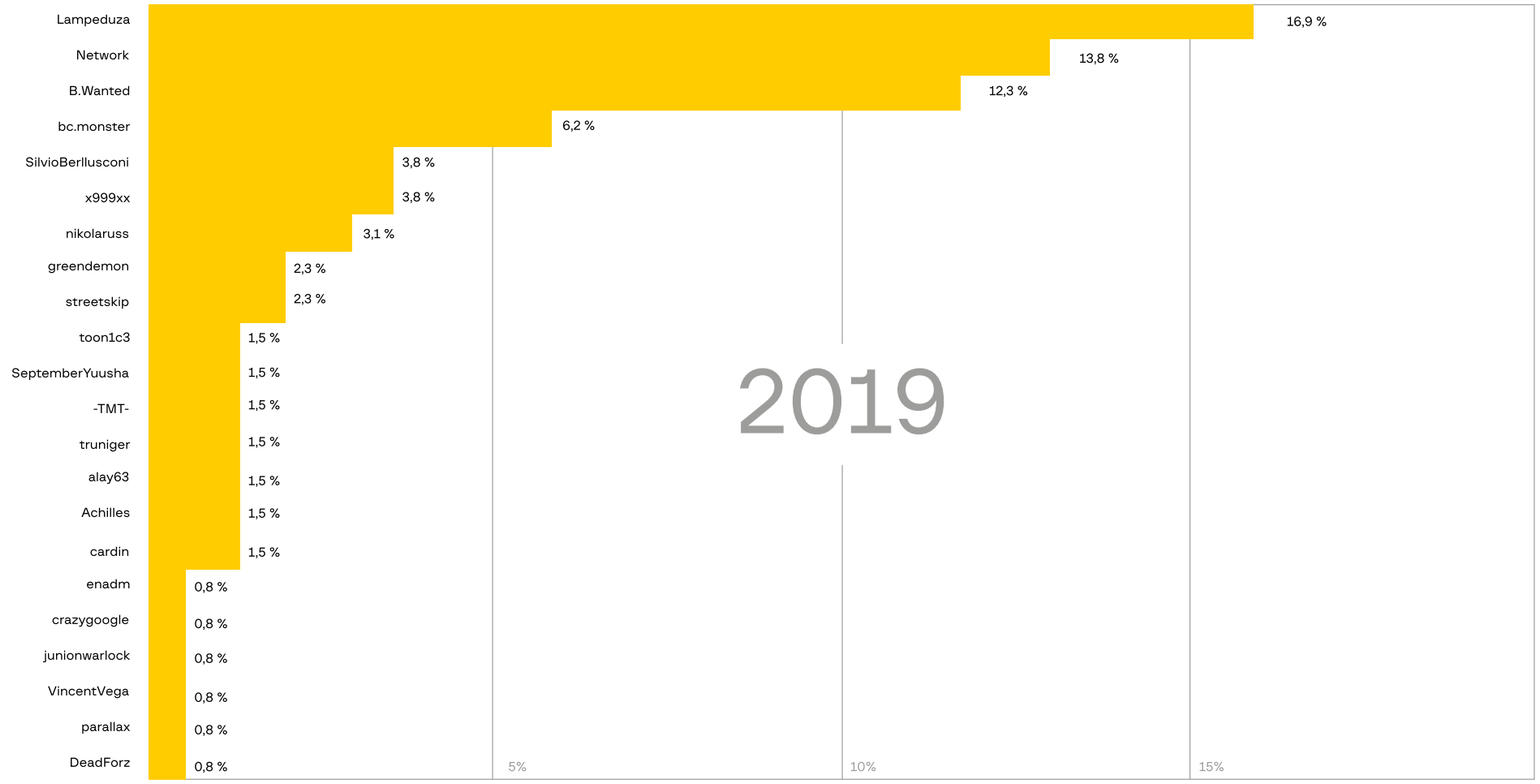
2019			
Q1	**Q2**	**Q3**	**Q4**
25	20	33	52
H1		**H2**	
45		85	
TOTAL			
130			

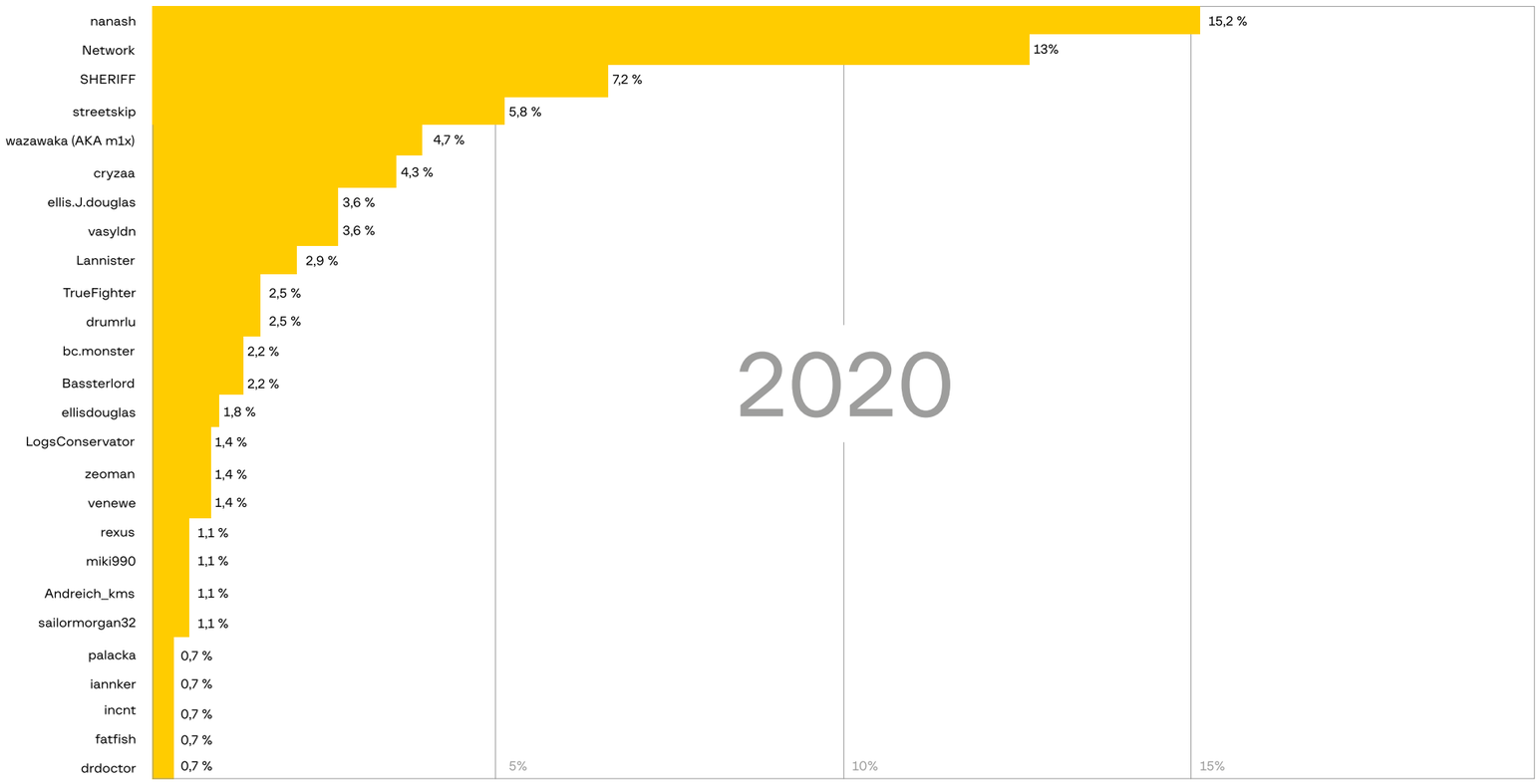
2020			
Q1	**Q2**	**Q3**	**Q4**
104	173	—	—
H1		**H2**	
277		—	
TOTAL			
277			



The table below shows active sellers of access to corporate networks on underground forums in 2018-2020 (only those who posted several offers).







Number of access sellers

37 in 2018

50 in 2019

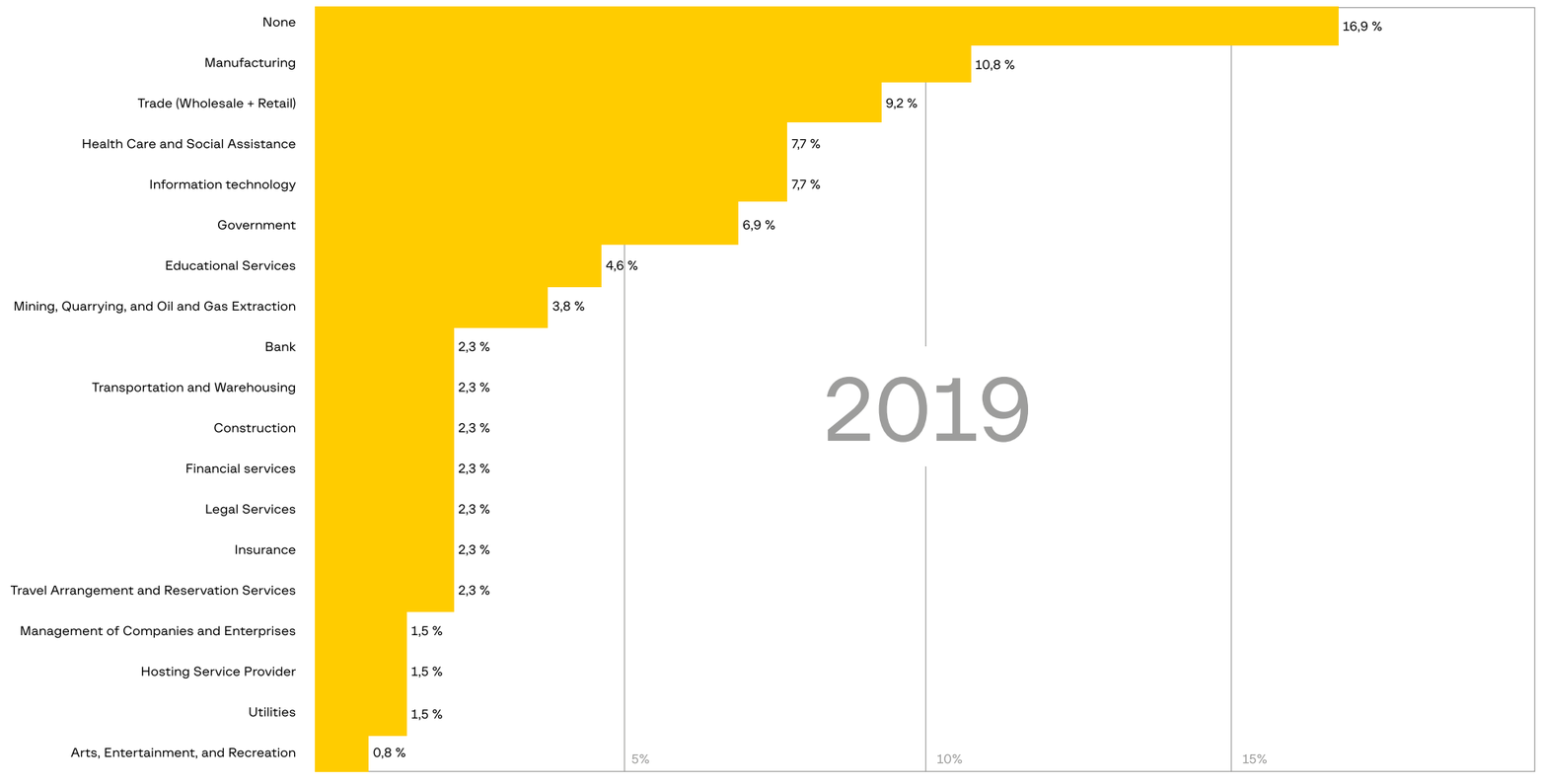
63 in 2020

In 2018, only 37 access sellers were active.

In 2019, Group-IB researchers identified 50 active access sellers, who offered access to 130 companies. Moreover, 44 of them were newcomers.

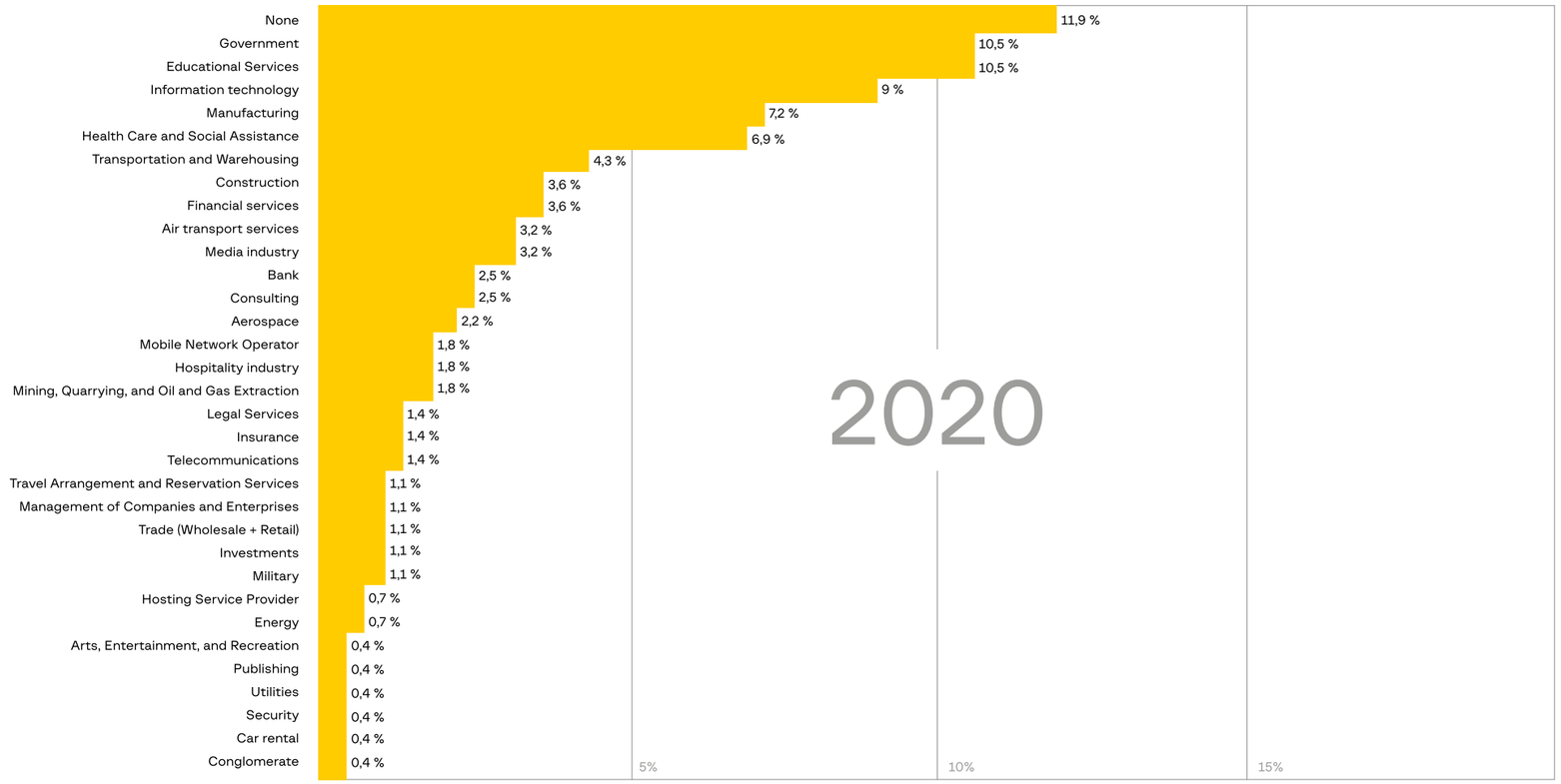
In H1 2020, 277 offers of access to corporate networks were put up for sale on underground forums. The number of sellers has also grown. During the above period, 63 sellers were active, and 52 of them began selling access in 2020. For comparison, during all of 2018, only 37 access sellers were active.

The market remains as fragmented as it was in 2019, and new sellers are replacing well-known ones. The diagrams to the left illustrate this trend.



2019 **main victims of attacks — production**

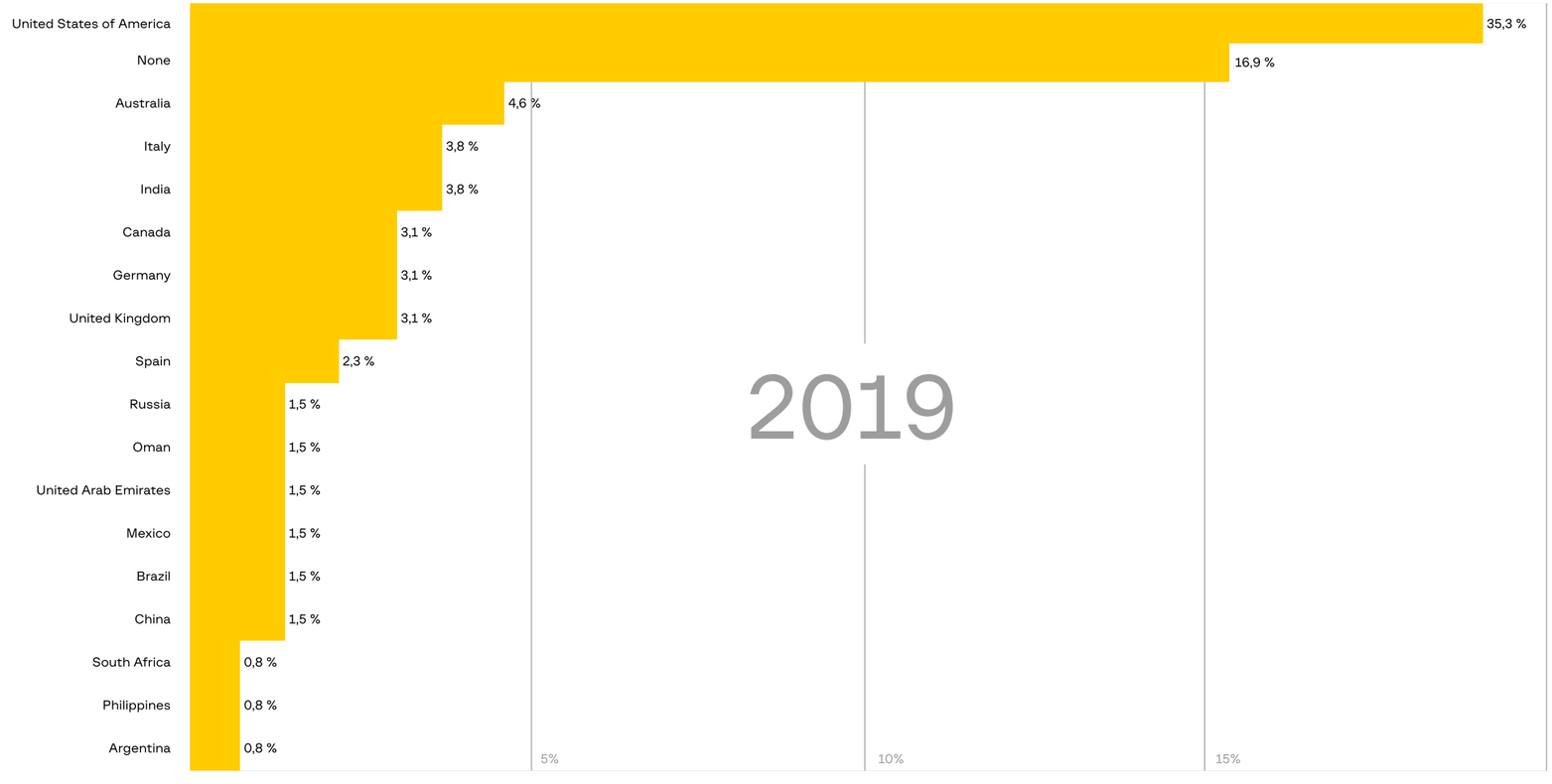
2020 **main victims of attacks — state-owned companies**

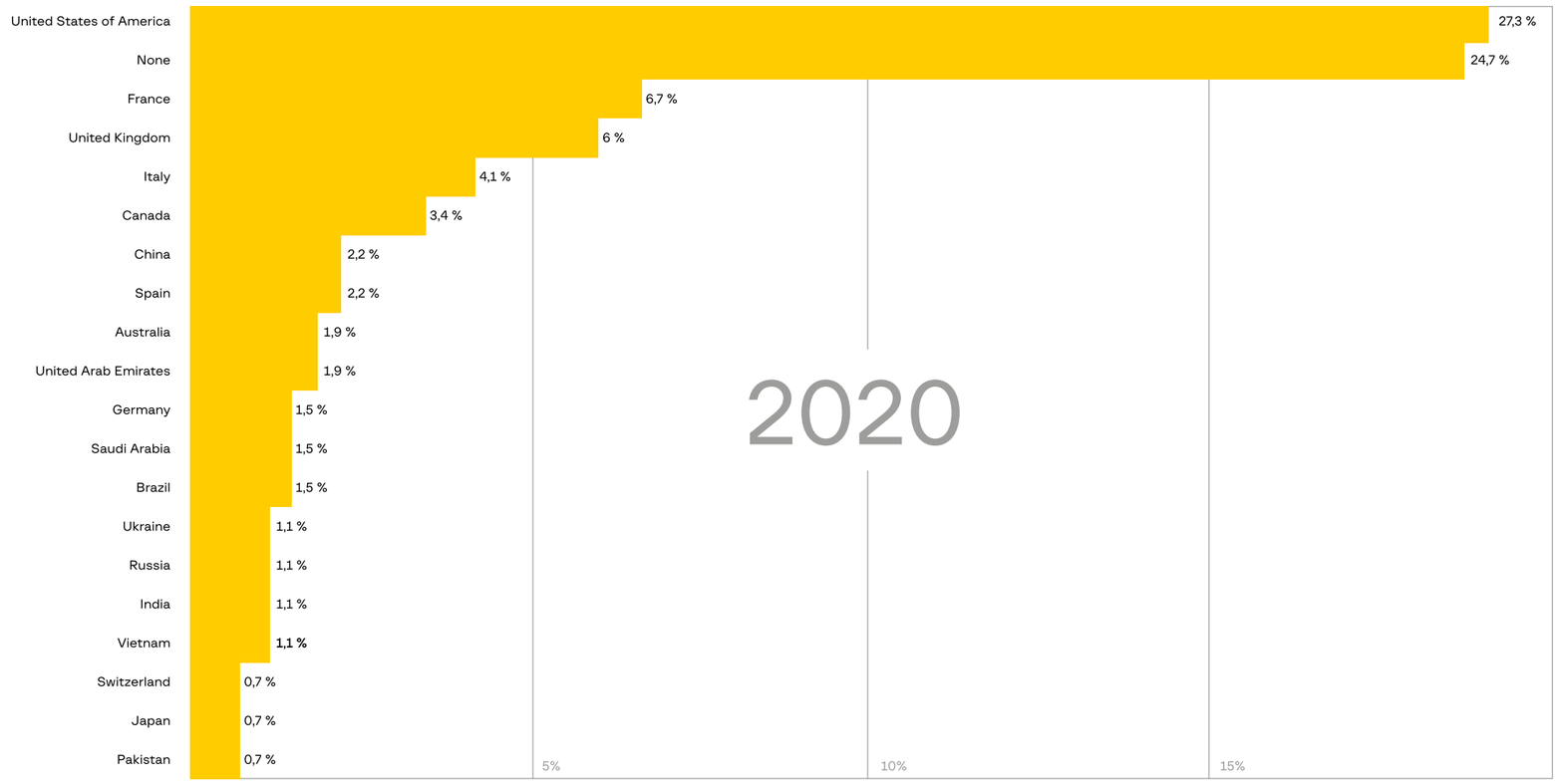


In 2019, cybercriminals stopped mentioning full company names when selling access, revealing only the country or industry. The full company name was indicated in only 27% of ads.

As regards the targeted sectors, in 2019 production companies remained the main victims. However, many healthcare organizations (usually hospitals and clinics) were also targeted.

In 2020, the list of attacked industries changed drastically. Various state-owned companies and educational institutions came to the fore. Manufacturing companies accounted for only 7.2%.





USA

the most attacked region

It is difficult to assess the size of the market for selling access, however, as offers published on underground forums often do not include the price.

$1,609,930

the total market size for access sold from H2 2018 to H1 2019 (the sum of the prices of all access information published on the forums)

$6,189,388

the market size in the current period, H2 2019 to H1 2020 (it has almost quadrupled)

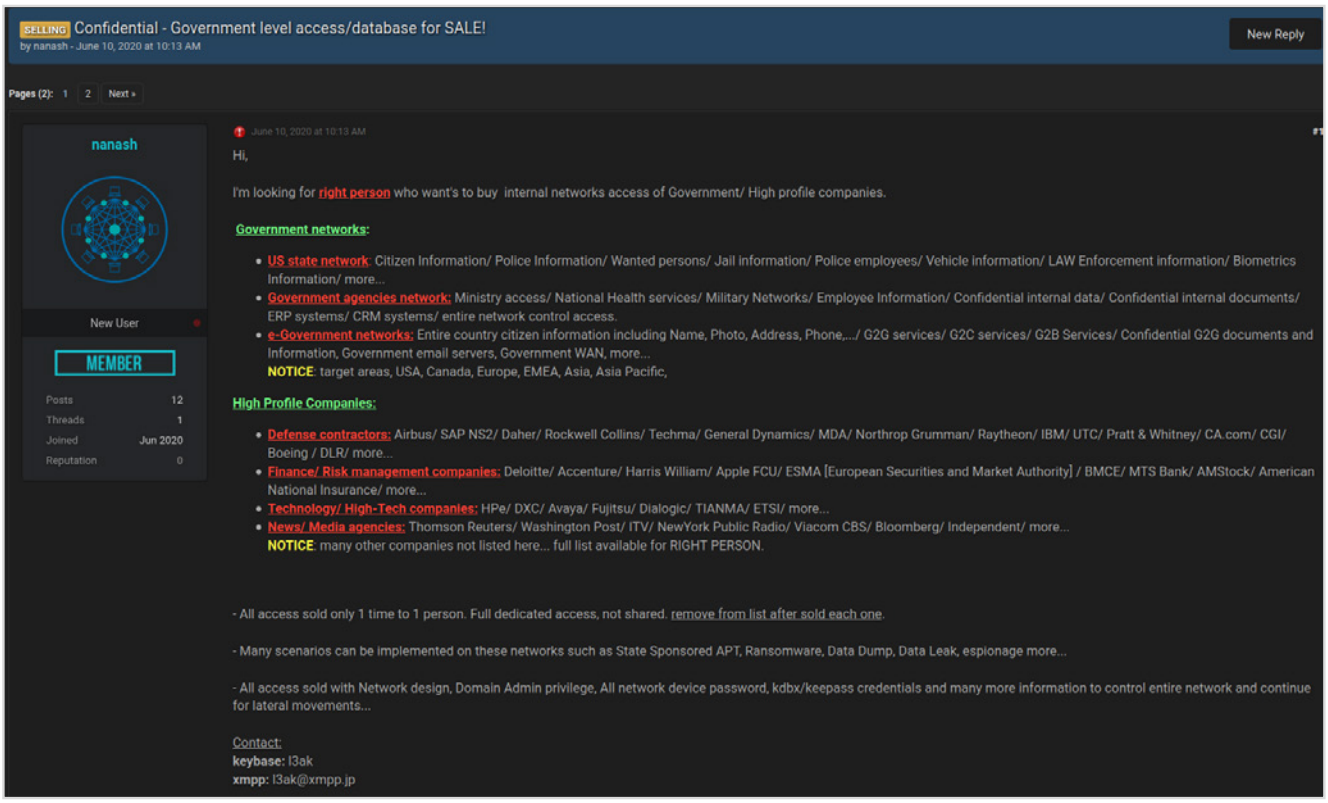
The United States remains the most often attacked region. It is worth highlighting, however, that it has become increasingly difficult to establish the name and location of the companies to which access is being sold without communicating with the cybercriminals involved.

Nation-state actors sell access to networks and use ransomware

In an effort to increase their profits, some state-sponsored groups began selling access to corporate networks or even using ransomware like regular cybercriminals.

A perfect example is an ad published by a user with the nickname nanash in June 2020. The seller offered access to many networks, including some belonging to US government departments, defense contractors (Airbus, Boeing, etc.), IT giants, and media companies. The figure below contains the full text of the ad.

Figure 5. A user nicknamed nanash offering access to various companies



Although the message looks suspicious, further investigation revealed that its author had access to at least two companies from the list above. Group-IB experts obtained screenshots and a video demonstration of LDAP access as evidence.

In the ad, the seller specifies that the price of access to each company is 11 BTC (USD 125,000). Access is sold directly with partial prepayment: after the customer has transferred 5 BTC, the seller provides additional evidence and the second transaction occurs.

In the message, the author did not mention all the companies they have access to, but the cost of accesses to companies listed explicitly is close to $5 million.

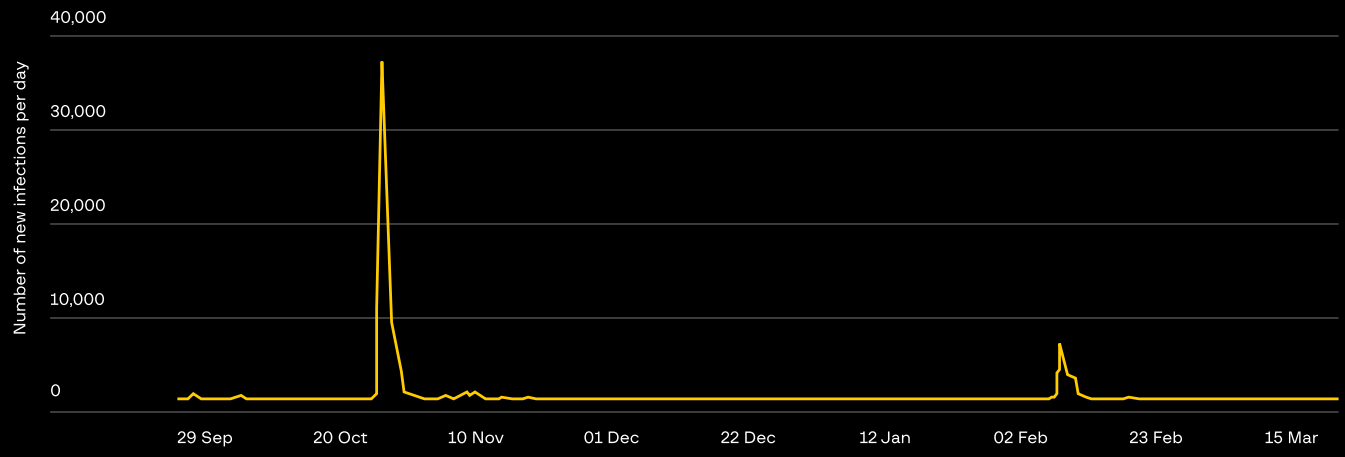
Another way for state-sponsored groups to make money is to use ransomware:

— Taiwanese authorities suspect that Chinese hackers from APT41 were behind a ransomware attack on Taiwan's energy and technology companies in May 2020. The notice included CPC Corp., a Taiwanese company that delivers petroleum products throughout the island, among the victims. While the attack did not affect CPC's manufacturing processes, it prevented customers from using CPC Corp.'s payment cards to buy gas. During the wave of attacks on Taiwanese targets, threat actors used a new ransomware called ColdLock. Malware analysis revealed similarities between the program and two known ransomware families: Freezing and EDA2, an open-source ransomware originally created for educational purposes.

— The hacker group Lazarus has resumed developing ransomware. The fact was brought to light during attacks on European companies involving ransomware called VHD Ransomware. The hackers gained access through a vulnerable VPN gateway, obtained administrator privileges, and installed the DacIs backdoor. They moved across the victim's network and encrypted files with a combination of AES-256 in ECB mode and RSA-2048.

— Another group of Chinese hackers, IronTiger, was behind the attack involving HybirdRansom ransomware against companies in the Asia-Pacific region in the fall of 2019 and the spring of 2020. The ransomware has three components that consequently launch each other to lock the machine and encrypt file: Locker, Loader, and Cryptor.

Compromised hosts by time (2019-2020)



Large companies under increasing threat from massive hacks

In the past, massive attacks did not cause serious damage to large companies. This was because brute-force attacks or exploiting vulnerabilities in widespread software led to their infrastructure being used to distribute or manage malicious code, mine cryptocurrencies, conduct DDoS attacks, or proxy traffic.

However, the market for the sale of access to corporate networks, the number of ransomware attacks, and APT group activity have all increased, so the cost of an error on a company's external perimeter has surged as well.

Ten out of 15 ransomware affiliate programs focus on brute-force attacks on RDP. Three programs actively exploit vulnerabilities in VPN services.

APT groups performed similar actions. For example, APT29 (aka Cozy Bear) actively exploited the following vulnerabilities with public exploits:

— CVE-2019-19781 (Citrix)
— CVE-2019-11510 (Pulse Secure)
— CVE-2018-13379 (FortiGate)
— CVE-2019-9670 (Zimbra)

The APT group BlackEnergy (aka Sandworm) exploited CVE-2019-10149 (a vulnerability in the Exim mail server) to install an SSH backdoor.

Ordinary criminal groups carried out similar actions. For example, the group Clownz responsible for leaks from GoDaddy and 247.ai also used CVE-2019-10149 (Exim) to install an SSH backdoor. For several months of activity, the group infected 80,000 servers.

As mentioned above, one of the main ways to gain access to corporate networks is to conduct brute-force attacks on remote access interfaces (RDP, SSH, VPN). How effective such an attack is will determine how many companies will be compromised as a result and how much money the fraudsters will make. Another key change is the emergence of new types of botnets. Their main purpose is to help perform distributed brute-force attacks from a large number of infected devices, including servers.


Брутфорс ботнет / Bruteforce botnet

By Ivanushk23, April 7 in [Software] - malware, exploits, bundles, crypts

Start new topic | Reply to this topic

Ivanushk23
kilobyte

Posted April 7

After 1+ year of work I want to announce new distributed bruteforce/scanner.

Друзья после более года работы рад представить вам распределеный брутфорс сканер.
Распределенный сканер / Брутфорсер это программный комплекс который может распределить задачу на несколько компьютеров, используя задачу скана / брутфорса паралельно,в результате чего достигается высокая скорость.

Paid registration
1
37 posts
Joined
10/17/18 (ID: 89629)

Возможна ли работа на найденых пк ?

-Да возможна, при использовании руткит модуля.

Figure 6. Example of the sale of a service based on a bruteforcer, a distributed scanner for establishing passwords

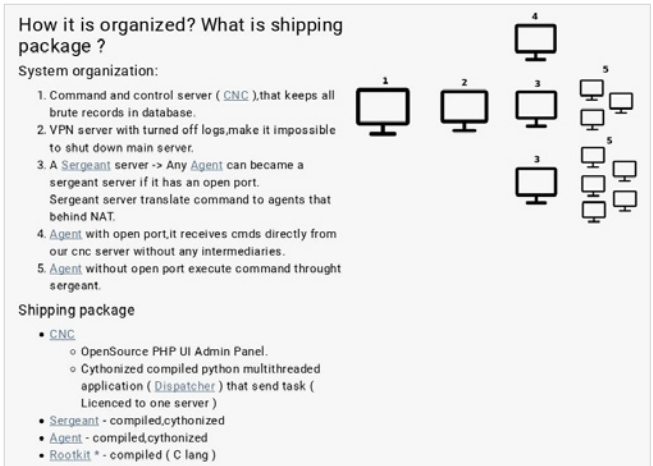
Ivanushk23
kilobyte

Paid registration
37 posts
Joined
10/17/18

Brute-force botnet
After 1+ year of work, I want to announce a new distributed bruteforce/scanner.

Hey friends,
After one year of work, I'm happy to present a distributed brute-force scanner.
The distributed scanner/ bruteforcer is a software that distributes tasks to several computers to scan/brute-force simultaneously. This speeds up the process significantly.

Can the solutions be used on computers found?
Yes, when using a module rootkit.


How it is organized? What is shipping package ?

System organization:

1. Command and control server (CNC),that keeps all brute records in database.
2. VPN server with turned off logs,make it impossible to shut down main server.
3. A Sergeant server -> Any Agent can became a sergeant server if it has an open port. Sergeant server translate command to agents that behind NAT.
4. Agent with open port,it receives cmds directly from our cnc server without any intermediaries.
5. Agent without open port execute command throught sergeant.

Shipping package

- CNC
  - OpenSource PHP UI Admin Panel.
  - Cythonized compiled python multithreaded application (Dispatcher) that send task (Licenced to one server)
- Sergeant - compiled,cythonized
- Agent - compiled,cythonized
- Rootkit * - compiled (C lang)

Growing activity of post-exploitation frameworks

Conducting a successful attack on a corporate network requires tools for lateral movement and privilege escalation. The growth of the access sales market has led to post-exploitation frameworks being used more often. Such frameworks are used by ransomware affiliates and operators, organized crime groups, and state-sponsored actors.

Group-IB regularly detects new infrastructure for various post-exploitation frameworks. From H2 2019 to H1 2020, more than 10,000 hosts used by such frameworks were discovered. In contrast, 6,000 such hosts were discovered in the same period last year.

	Threat actor	Cobalt Strike	Metasploit	Covenant	CrackMapExec	PoshC2	Koadic
Ransomware	Ryuk	●	●				
	REvil		●		●		
	MegaCortex	●					
	Maze	●					
	DoppelPaymer					●	●
	Clop	●	●				
	Lockbit				●		
Cybercrime	Cobalt	●					
	Silence		●				
	Fxmsp		●				
	FIN6	●	●				
APT	Lazarus	●					
	OilRig	●	●	●			
	APT41	●	●				
	APT32	●					
	Gamaredon		●				
	Chimera	●					
	Mustang Panda	●					
	Chafer		●				
	APT10	●					
	APT33					●	

10,000 HOSTS

used by post-explotation frameworks

MILITARY OPERATIONS

Seven new APT groups were discovered during the reporting period

Six known groups that remained unnoticed in recent years resumed their attacks

New tools and destructive consequences

Power units shut down, infrastructure destroyed, and air-gapped networks attacked

Asia-Pacific countries are becoming one of the key "arenas"

and are attracting the attention of cybercriminals from China, North Korea, Iran, and Pakistan

A changing threat landscape

Multiple attacks were carried out in the Asia-Pacific, a region in which the main active groups from China, North Korea, Iran and Pakistan showed interest.

During the reporting period, seven new APT groups were discovered. Group-IB researchers also unveiled the activity of six known groups that remained unnoticed for the past few years.

APAC

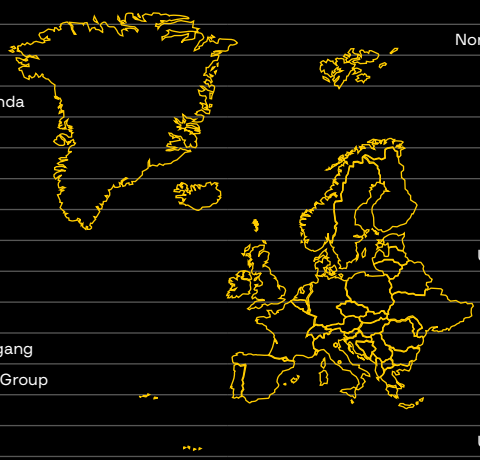
APT10	China
DarkHotel	North Korea
OceanLotus	Vietnam
TA428	China
Kimsuky	North Korea
APT37	North Korea
FruityArmor	UAE
BITTER	India
Patchwork	India
Emissary Panda	China
Poison Carp	China
Rancor	China
Lazarus	North Korea
IronTiger	China
APT41	China
Mustang Panda	China
Higaisa	South Korea
APT33	Iran
Platinum	China
APT-C-35	Unknown
APT20	China
BlackTech	China
Tick	China
SideWinder	India
APT40	China
Transparent Tribe	Pakistan
Cycldek	China
Tonto Team	China
TwoSail Junk	China
Naikon	China
Tropic Trooper	China
Chimera	Unknown
APT30	China
Orangeworm	Unknown

America

Gorgon Group	Pakistan
Kimsuky	North Korea
IronTiger	China
APT41	China
APT35	Iran
Oilrig	Iran
APT33	Iran
APT20	China
APT37	North Korea
Gaza Cybergang	Gaza
TA410	China
APT5	China
Tortoiseshell	Iran
Orangeworm	Unknown
Transparent Tribe	Pakistan

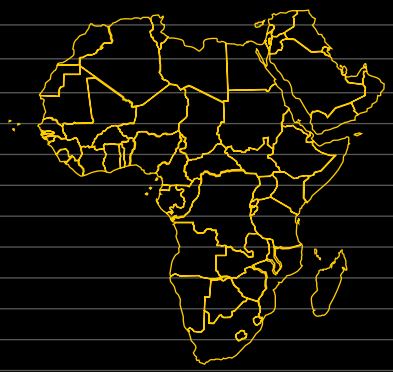
EUROPE

APT 10	China
APT15	China
Gorgon Group	Pakistan
Kimsuky	North Korea
FruityArmor	UAE
Lazarus	North Korea
APT41	China
Mustang Panda	China
APT29	Russia
Turla	Russia
Oilrig	Iran
Avivore	China
APT-C-35	Unknown
APT20	China
APT35	Iran
Gaza Cybergang	Gaza
Gamaredon Group	Russia
APT33	Iran
InvisiMole	Unknown
APT5	China
Orangeworm	Unknown
Transparent Tribe	Pakistan



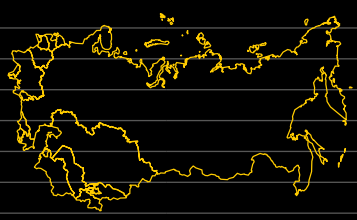
MIDDLE EAST & AFRICA

APT10	China
Oilrig	Iran
MuddyWater	Iran
Gorgon Group	Pakistan
FruityArmor	UAE
Tortoiseshell	Iran
APT41	China
Mustang Panda	China
APT33	Iran
APT-C-37	Unknown
Domestic Kitten	Iran
APT35	Iran
APT-C-23	Gaza
Gaza Cybergang	Gaza
Chafer	Iran
StrongPity	Turkey
WildPressure	Unknown
Orangeworm	Unknown



POST-SOVIET COUNTRIES

APT28	Russia
MuddyWater	Iran
Gamaredon Group	Russia
IronTiger	China
Turla	Russia
Golden Falcon	Kazakhstan
APT37	North Korea
Kimsuky	North Korea
Tonto Team	China



New APT groups

Tortoiseshell

Geography	Initial infection	Tools
America Middle East	Phishing Drive-by compromise	Backdoor.Syskit Infostealer

The group Tortoiseshell has remained under the radar since July 2018. Since then, it has attacked at least eleven IT companies, most of which are located in Saudi Arabia.

In at least two organizations, evidence was found that attackers gained access at the domain administrator level, which resulted in several hundred computers on the network being compromised. It was probably a forced measure to find the device of greatest interest to them given that infecting an IT provider opens up opportunities to access client systems.

To achieve their goal, the group created a unique malware called Backdoor. Syskit, developed in versions in the Delphi and .NET languages. With this backdoor in hand, the criminals were able to download and execute additional tools and commands. The malware was later identified in an attack involving a phishing website targeting US military veterans.

Poison Carp

Geography	Initial infection	Tools
Tibet Uyghur	Drive-by compromise Exploit public-facing application Spearphishing	MOONSHINE INSOMNIA IRONSQUIRREL

The group Poison Carp has remained unnoticed since 2018. The threat actor is believed to have links to China due to the chosen attack targets: senior figures in Tibetan and Uyghur groups. Poison Carp uses eight Android browser exploits, one iOS exploit chain, and a spyware suite for Android and iOS.

Posing as journalists or officials, the hackers attacked high-profile officials by first contacting them via the messaging service WhatsApp. After gaining their trust, the hackers sent the victims a link that installed spyware on the target devices.

Malicious software called MOONSHINE helped the hackers obtain access to calls, messages (including messengers installed on the gadget), and geolocation data. It also allowed them to control the smartphone's microphone and camera and install programs on the phone.

Higaisa

Geography	Initial infection	Tools
APAC Europe Russia	Spearphishing	GHOST RAT Keylogger InfoStealer

Since 2016, the group Higaisa has remained unnoticed. The adversary carries out phishing campaigns, delivering executable files most often disguised as legitimate installers, images or documents. Congratulatory texts or important news are used as decoys. The attackers use the following tools:

— A modified version of GHOST RAT
— A keylogger
— A malicious program designed to steal passwords from Outlook
— Android Trojans (capable of taking screenshots, capturing GPS location and SMS messages, recording calls, stealing phone book data, and downloading files).

AVIVORE

Geography	Initial infection	Tools
Europe UK	Supply Chain	Mimikatz PlugX Living-off-the-land

In the past, it was believed that hacker groups such as China-based APT10 organized attacks on European multinationals in the aerospace and defense industries. In fact, the threats came from previously unknown hackers such as AVIVORE. The group has been active since 2015, but their activities peaked in 2019. AVIVORE is reported to be behind recent attacks on Airbus, a European aerospace giant. Airbus was attacked four times in 2019, most recently in September.

The adversary infiltrated Airbus' global network of suppliers through the British engine manufacturer Rolls-Royce, which supplies aircraft engines, and the French technology consultancy Expleo. In addition, two unidentified contractors working for the aerospace company were compromised. The main malicious tool used by the group is PlugX.

Nuo Chong Lions

Geography	Initial infection	Tools
Middle East	Spearphishing Watering hole	AndroRat SandroRat Droidjack SpyNote MobiHok

Although the group Nuo Chong Lions was not active in 2019 and 2020, now that its leader has changed it is likely to become more active again. The group is also known as SilencerLion, and its attacks from 2013 to 2018 were used to spy on and control critics of the Saudi government at home and abroad. The group reportedly recruited two Twitter employees to gather confidential personal data about dissidents and radicals, including phone numbers and IP addresses. On November 11, 2015, Twitter issued a security notice to dozens of account holders viewed by one of the former Twitter employees.

Saud al-Qahtani, a former top aide to Crown Prince Mohammed bin Salman, is suspected of being involved in the above. He also allegedly hired the Israeli company NSO Group to spy on activists and journalists critical of Riyadh.

During their attacks, the hackers used watering hole and spear phishing methods. Nuo Chong Lions employed four mobile RATs, including an open source tool called AndroRat and three commercial RATs (SandroRat, SpyNote, and MobiHok).

Chimera

Geography	Initial infection	Tools
Taiwan	External remote services	SkeletonKeyInjector Cobalt Strike ChimeRAR

This hacker group attacked several Taiwanese semiconductor companies in 2018 and 2019. Experts named the threat actor Chimera. Their attacks were aimed at stealing as much intellectual property as possible, including documents on integrated circuits (ICs), software development kits, IC designs, and source code.

The motive behind the attacks is likely competitors (or possibly even nation-states, given the advanced nature of the attacks) seeking to gain a competitive advantage. The networks were initially compromised through VPN servers and valid accounts were used. The hackers most likely obtained credentials for the VPN access from compromised accounts. The group is known for deploying a skeleton key malware that makes it possible to log in without valid credentials.

WildPressure

Geography	Initial infection	Tools
Middle East	Unknown	Milum

The group WildPressure does not overlap with other APT groups and uses new malware. The hackers attacked Middle Eastern organizations, with at least a few operating in the industrial sector. The hackers distribute a fully-fledged C++ Trojan called Milum. Inside the encrypted communications within the HTTP POST requests, Group-IB researchers found the malware version 1.0.1. Such a version number indicates an early stage of development. Other fields suggest the existence of plans for non-C++ versions at the very least. This means that the group is likely to continue their attacks in the future.

Well-known groups remaining undetected for a long time

The year was also marked by long-term and covert attacks carried out by well-known groups that once seemed to have left the stage. On the one hand, this reaffirms that APT groups and their sophistication should never be underestimated. On the other hand, continuously training systems to detect malicious infrastructure and software at an early stage makes preventive measures much more effective, and means that more and more attacks can be tracked. Most such groups have their own unique style or use self-developed tools.

Golden Falcon

An unexpected discovery in 2019 was the activity of the group Golden Falcon (aka APT-C-34), which became known after one of the group's C&C servers was detected.

The group hacked private companies and government organizations in Kazakhstan. They mainly used two tools. The first was a version of RCS (Remote Control System), a surveillance kit sold by an Italian vendor called HackingTeam. The second was a backdoor named Harpoon that appears to have been developed by the group itself. Documentation about the latter in Russian was found on a C&C server, which suggests that the group hired third-party developers to write the malware according to the group's own technical specifications.

The group's activities resemble those of the group DustSquad, which has been active since 2017. They also orchestrate espionage campaigns in Kazakhstan, for which they used the Octopus Trojan. The group may be backed by Kazakhstan's special

services or individuals interested in monitoring the situation in the country.

Naikon

The prize for the most stealthy and long-term campaign goes to the Chinese group Naikon for its five-year campaign against top government agencies in target countries in the APAC region. Naikon used a new backdoor called Aria-body that creates and deletes files and directories, takes screenshots, searches for files, and collects data (file metadata, system information, and location data). Even though the threat actor uses common initial intrusion vectors (emails with malicious attachments), their attacks are highly effective.

APT20

For two years, the group APT20 remained undetected while attacking companies and government agencies. The threat actor stole passwords and bypassed two-factor authentication to collect target data. Their large-scale campaign called Operation Wocao affected multiple industries including aviation, construction, finance, healthcare, insurance, gambling, and energy.

The criminals effectively covered their tracks by regularly removing data-stealing tools from infected computers.

APT5

Another surprise comeback came from the group APT5 (aka Manganese). The group has been active since 2007 and consists of several subgroups with specific tactics and infrastructure. The criminals infiltrate organizations across various verticals. Their primary interest appears to be telecommunications and technology organizations, with a particular affinity for satellite communication firms.

During the reporting period, APT5 created an infrastructure designed to scan the web for Fortinet and Pulse Secure enterprise VPN servers. The criminals then exploited the CVE-2018-13379 vulnerability in Fortinet and the CVE-2019-11510 vulnerability in Pulse Secure. These arbitrary file reading vulnerabilities make it possible for an unauthenticated remote attacker to read the content of files on vulnerable devices.

APT30

It was uncovered that the group APT30 has been upkeeping its 10-year-old tools (BACKSPACE and NETEAGLE) and has used them in attacks on Southeast Asia. In addition, the hackers continued with their old approaches to organizing network resources and tested new software: RHttpCtrl and RCtrl.

Cycldek

The hacker group Cycldek also made an appearance. The threat actor uses the USBCulprit Trojan, which is designed to steal data from corporate networks and helps gain access to disconnected and physically isolated devices. The malware had gone undetected since 2014, with new samples appearing in 2019. The group focused on government organizations in several countries in Southeast Asia.

Significant operations

Attacks on nuclear facilities

India, 2019

In September 2019, Group-IB experts discovered an archive containing Dtrack, a remote administration tool attributed to the North Korean group Lazarus. Analysis revealed that the logs contained data from a compromised machine running Windows that belonged to an employee of the Nuclear Power Corporation of India Limited (NPCIL).

All the files in the archive were compiled at different times, but the main file with the compromised data is dated January 30, 2019, i.e. more than six months before they were detected. This suggests that the hackers remained unnoticed in the victim's network for a long time.

Analysis revealed that the attack against NPCIL was taken even further and led to Kudankulam Nuclear Power Plant (situated in the south of the state of Tamil Nadu) being compromised. On October 19, 2019, the power plant's second power unit was shut down. Group-IB believes that these events may be linked.

According to the company officials, the reason for the power unit being shut down was a low SG level:

"The most important SG parameter subjected to regulation is the SG level. If the level is too low, the insufficient heat removal by the secondary side may cause evaporation of the reactor coolant, thus overheating of the reactor core."

In other words, the pressure in the steam generator, which is responsible for transferring heat from the core to the generator's turbine, was low. This could have led to the core overheating.

After cybersecurity expert Puhraj Singh tweeted about the attack, the nuclear power plant's administration released a statement in which Singh's words were called "false information" and denied that an attack had occurred, stating that "any cyber-attack on the Nuclear Power Plant Control System is not possible."

The Nuclear Power Corporation of India Limited, however, later confirmed that the plant had been attacked. NPCIL's official statement said that the malware infected one computer connected to the nuclear power plant's administrative network, but did not reach its critical internal network used to control the power plant's nuclear reactors.

South Korea, 2020

In April 2020, Lazarus sent malicious emails to a company in the energy sector in South Korea. The hackers disguised themselves using a document with a description of a vacancy at KHNP (Korea Hydro & Nuclear Power Co., Ltd.).

KHNP is a subsidiary of Korea Electric Power Corporation. It operates large nuclear and hydroelectric plants in South Korea, which supply about 30% of the country's electric power.

In addition, since October 2019, the North Korean groups Lazarus and Kimsuky have been actively attacking South Korea's defense enterprises. The attacks have intensified since April 2020.

Iran, 2020

On July 3, 2020, it transpired that the Israeli authorities were suspected of carrying out a cyberattack on Iran's nuclear facilities. The incident occurred on July 2 at Iran's largest uranium-enrichment facility in Natanz and caused a fire and explosion. Before the incident was made public, a group calling itself the Homeland Cheetahs sent a statement to BBC Persian journalists and claimed to be behind the attack. The group allegedly consists of "former members of the Iranian security forces who have decided to fight against the authorities."

Iran's officials said the incident had caused significant damage that could slow the development of advanced uranium enrichment centrifuges, but that there had been no casualties.

Attacks on Israel's water supply facilities

In April 2020, the Israeli National Cyber-Directorate (INCD) issued a security alert urging staff at companies in the energy and water sectors to change passwords for all Internet-connected systems. According to the alert, the agency had received reports of intrusion attempts at wastewater treatment plants, water pumping stations, and sewers, which was confirmed by the Israeli authorities. Details of the attacks were not disclosed, but INCD Head Yigal Unn said they could have led to some damage to the civilian population and even temporary water shortages. Israeli officials said that the attacks had targeted SCADA systems of wastewater treatment facilities, but that they had been successfully thwarted.

Initial reports played down the April attack, but a Financial Times report a few month later cited its sources as claiming that the hackers had gained access to some of Israel's water treatment systems and tried altering water chlorine levels before being detected and stopped. If the sabotage attack had been successful, attackers could have poisoned the local population served by the treatment facility affected.

In addition, the Israeli Water Authority warned that in June 2020 water supply and water treatment systems were attacked again. The incidents reportedly did not cause any damage to Israel's water system.

The first attack affected agricultural water pumps in upper Galilee, while the second one targeted water pumps in the central province of Mateh Yehuda, local media reported.

"These were specific, small drainage installations in the agriculture sector that were immediately and independently repaired by the locals, causing no harm or any real-world effects," the Water Authority said in a statement.

Attacks on Iran's critical facilities

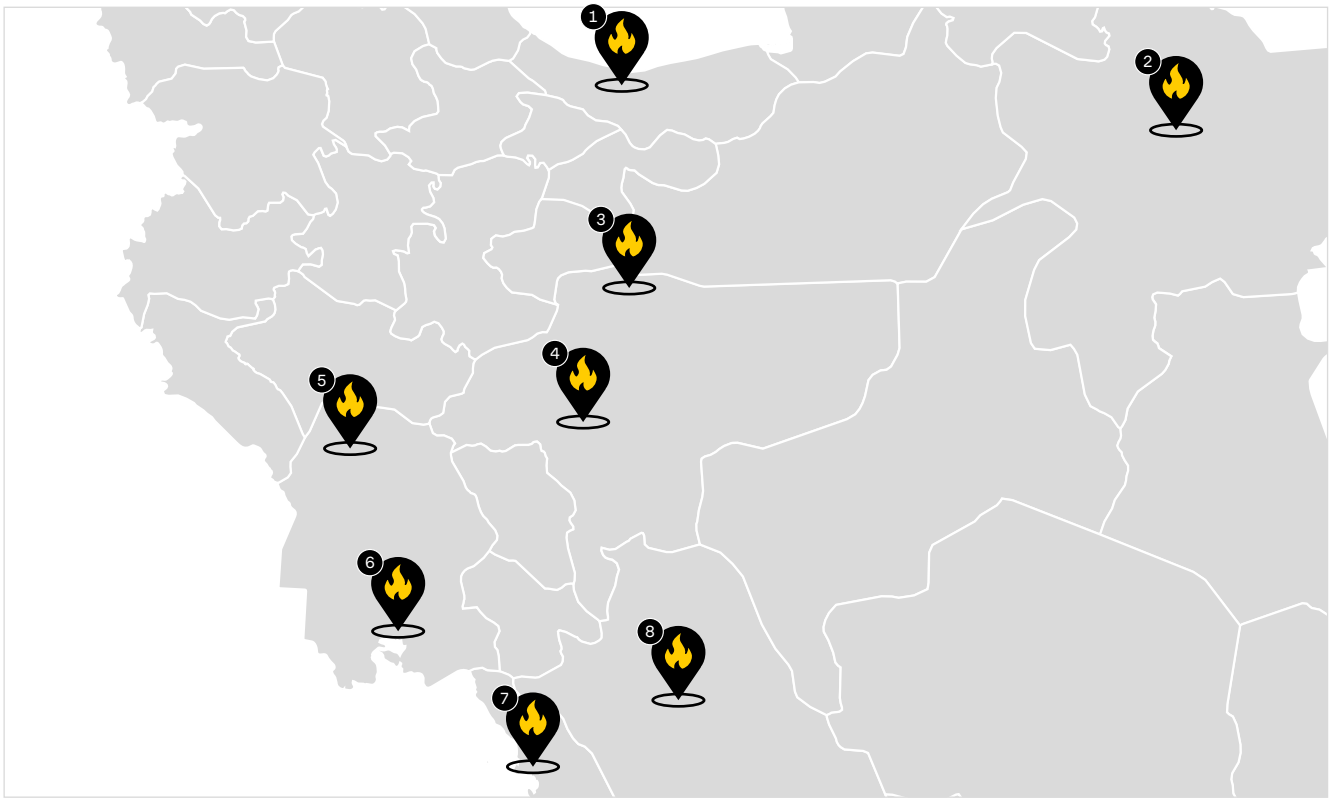
On May 9, 2020, hackers carried out a cyberattack on the systems of Iran's Shahid Rajaee port in the city of Bandar Abbas. According to Iran's Ministry of Roads and Urban Development officials, the attack affected a limited number of private operating resources in the port and did not cause significant damage.

It was later revealed, however, that computers regulating the flow of vessels, trucks, and goods all crashed at the same time, creating massive backups on waterways and roads leading to the facility.

The attack was presumably in response to an alleged Iranian attempt to hack into Israel's water infrastructure systems.

The attack was followed by a series of accidents and explosions at some of Iran's critical facilities, including petrochemical plants, uranium enrichment facilities, power plants, and ports.

Figure 7. Map of shutdowns and explosions in Iran



1. **June 26 →** Khojir SSM facility
   June 30 → Sina Athar Clinic in Shariati Avenue
   July 13 → Shian forest
   July 9 → Garnadareg explosion
   July 12 → Enghelab fire
2. **July 13 →** Kavian Friman industrial complex
3. **July 2 →** Natanz nuclear enrichment facility
4. **July 13 →** Najafabad fire
   July 19 → Isfahan power plant
5. **July 4 →** Zargan power plant
   July 4 → Karoon petrochemicals plant
6. **July 12 →** Shahid Tondgooyan petrochemical plant in Khyzestan province
7. **July 15 →** Bushehr ships fire
8. **July 3 →** Shiraz fire

On June 26, a large explosion occurred near Tehran region. The Iranian government was quick to dismiss the episode as a gas explosion at the Parchin military base. Satellite photographs, however, revealed that the explosion happened at the Khodjir missile production facility (part of the Shahid Hemmat Industrial Group). The base is laced with underground tunnels and has long been suspected of being a major site for Iran's growing arsenal.

Iran linked the attack to a power outage in the city of Shiraz, nearly 600 miles to the south. Shiraz also has major military facilities, and the explosion and the outage happened almost at the same time. American and Israeli intelligence officials insist they were not involved.

Figure 8. Satellite image of the explosion site in the mountains in the east of Tehran

THREATS TO THE TELECOMMUNICATIONS SECTOR

6 State-sponsored groups

show an interest in the telecom sector and conduct sophisticated attacks against it

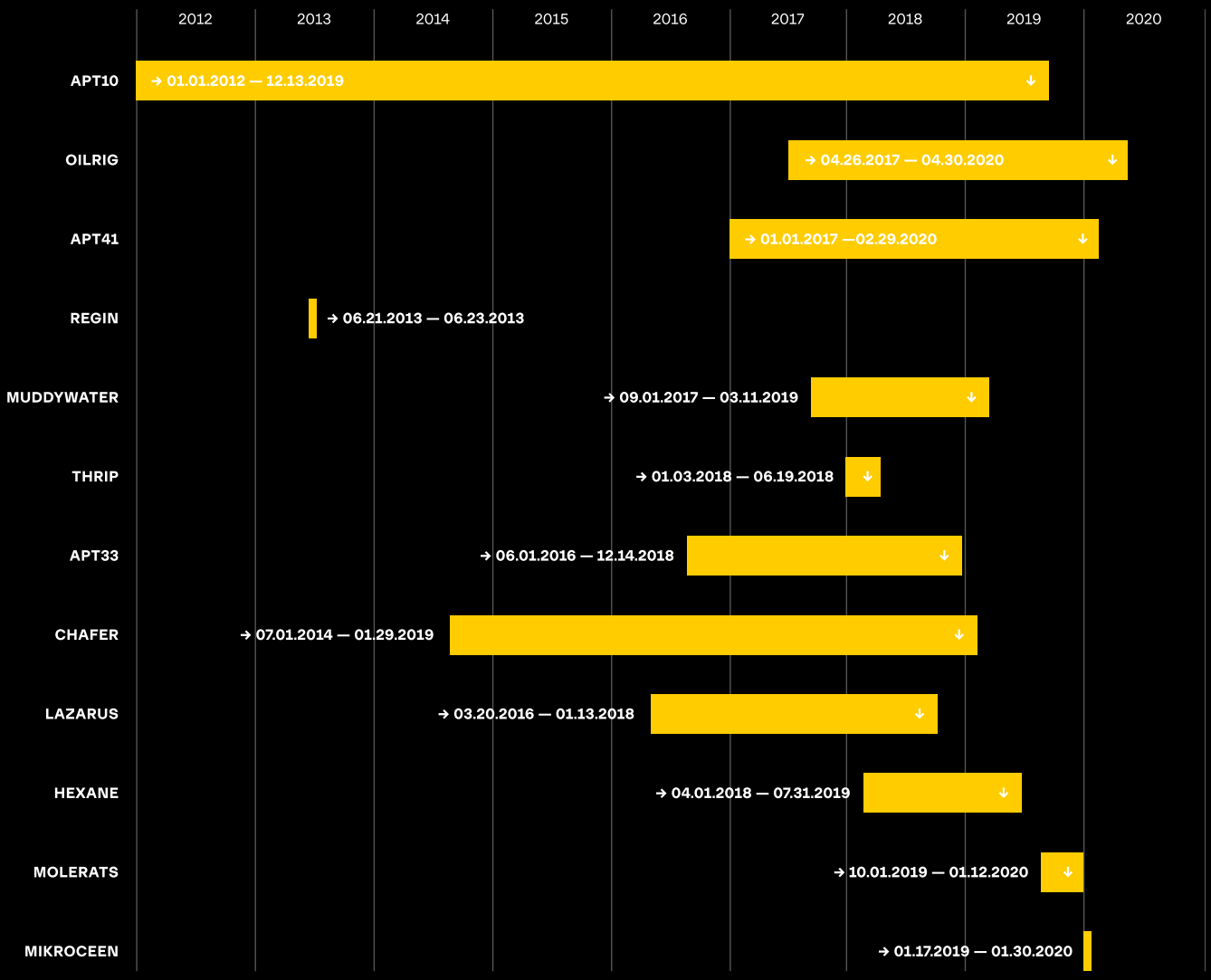
2.3 Tb per second and 809 million packets per second

new records in DDoS attack power

Special services pose the greatest threat to telecom companies. During the reporting period, six groups linked to special services actively attacked the telecommunications sector, targeting both fixed and mobile operators.

The traditional problems faced by operators are BGP route leaks and DDoS attacks. Such attacks are becoming increasingly effective and are setting new records.

Nation-state actors attacking the telecom sector



95 MONTHS

of attacks on the telecom sector conducted by an active hacker group

APT41

The hacker group APT41 carried out a number of attacks recently. In February 2020, the hackers successfully exploited a Cisco RV320 router at a telecommunications organization. It is unknown what specific exploit was used, but there is a Metasploit module that combines CVE-2019-1653 and CVE-2019-1652 to enable remote code execution on such routers. It also uses wget to download specified payloads.

APT41 also exploited the CVE-2020-10189 vulnerability in Zoho ManageEngine, which allows unauthenticated remote attackers to execute arbitrary code with SYSTEM/root privileges. The day after CVE-2020-10189 was fixed, the threat actors attacked over a dozen systems and compromised at least five. They then deployed a trial version of the Cobalt Strike BEACON loader and used another backdoor to download VMProtected Meterpreter.

OilRig

The Iranian group OilRig has been directly involved in two campaigns affecting the telecommunications sector.

One of the campaigns lasted three years and was dubbed Fox Kitten by security researchers. During the campaign, the threat actors gained access to and ensured persistence in the networks belonging to numerous companies and organizations from various sectors, including telecommunications.

In most cases, target organizations were initially infected through one-day vulnerabilities in various VPN services such as Pulse Secure VPN, Fortinet VPN, and Palo Alto Networks' Global Protect. Once inside the company, the attackers would try to maintain access to networks by opening a variety of communication tools, including opening RDP links over SSH tunneling. At the final stage, after successfully infiltrating the organization, the attackers performed the routine process of identifying, examining and filtering sensitive valuable information from every targeted organization.

The second campaign affected telecom providers in South Asia and was discovered in April 2020. During the campaign, the threat actors used post-exploitation frameworks and tools such as Covenant, Cobalt Strike, Metasploit, and Mimikatz. In addition, the group used legitimate tools such as Plink, Bitvise, and Bitsadmin. The threat actors used phishing emails to gain initial access. The campaign's main aim was to steal user credentials and gain access to database servers using the obtained credentials.

The attacks were long-term: the threat actors may have infiltrated the network of one organization as early as in October 2019. The first activity was detected on October 11, 2019, when a malicious PowerShell command was executed to install a Cobalt Strike Beacon module. The threat actors then executed a PowerShell command that launched Metasploit for achieving persistence in the system.

The group's activities resumed on February 6, 2020, when a PowerShell command was executed to search for files similar to web.config. For each file found, the threat actors extracted username and password details where possible. They may use the credentials to access organizational resources such as SQL servers.

On March 11, the threat actor attempted to connect to a database server via PowerShell, presumably using stolen credentials. The hackers also used an SQL command to obtain information about the database server version, possibly to verify credentials and connectivity.

Molerats

Between October 2019 and early December 2019, security researchers identified multiple instances of phishing attacks likely related to a threat group called Molerats (also known as Gaza Hackers Team and Gaza Cybergang). The group targeted organizations in the telecommunications, insurance, and retail industries and government agencies, eight in total, all in six countries.

All the attacks involved spear-phishing emails with malicious documents that required the recipient to carry out certain actions. The social engineering techniques involved misleading images that tricked users into enabling content to run macros. The hackers also threatened to release compromising pictures to the media as a way of coercing users into clicking a link and downloading malicious payloads. During most such attacks, the payload was a backdoor called Spark, which allows threat actors to open applications and run command line commands on the compromised system.

Mikroceen

Security experts analyzed a Trojan used by an unknown Chinese APT that spied on undisclosed companies in the telecommunications and gas industries as well as a government entity in Central Asia. The analysts called this campaign Mikroceen.

As part of their operations, the threat group used backdoors to gain permanent access to corporate networks. Based on the data obtained, Group-IB researchers believe that the same group was involved in other attacks, including Microcin against Russian military personnel, BYEBY against the Belarussian government, and Vicious Panda against the Mongolian public sector. The group has been active since at least 2017.

The experts justify this theory by the fact that the hackers used Gh0st RAT, which has been used by Chinese APTs often and for a long time. In addition, the analysts discovered clear similarities in the malware codes.

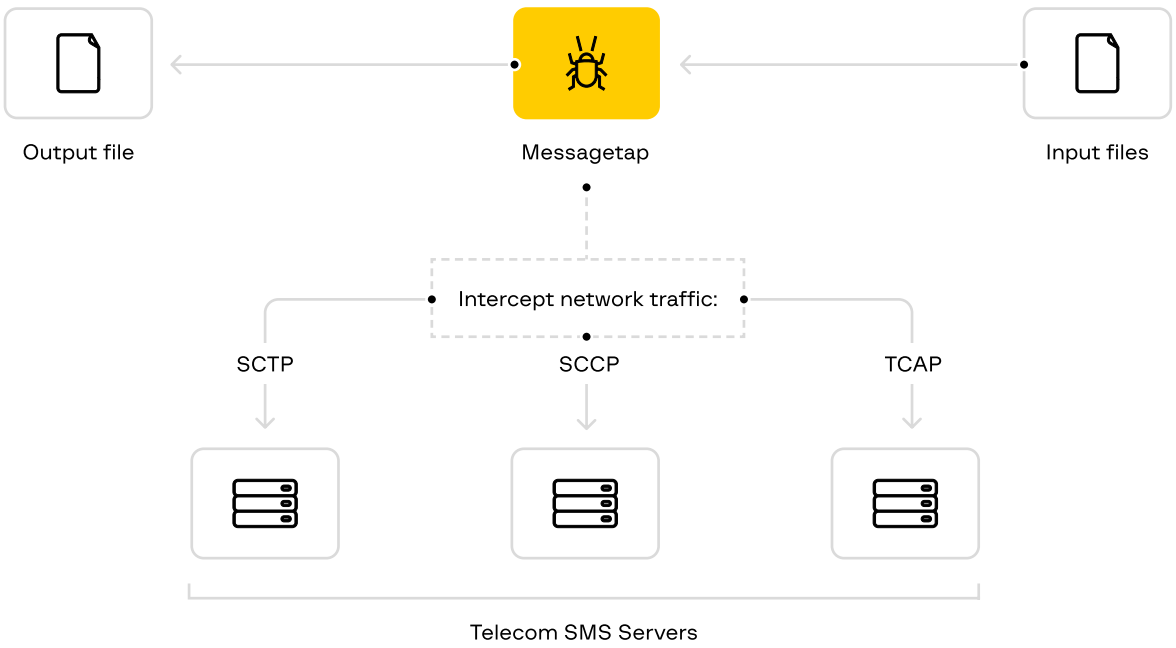
Attacks on mobile operators

APT41, a Chinese state-sponsored threat group, was highly active during the investigated period. The group actively deployed malware called MESSAGETAP.

The malware is designed for Linux devices and meant to be installed on Short Message Service Center (SMSC) servers located inside mobile operator networks that handle SMS communications. After compromising a cluster of Linux servers belonging to an unidentified telecom provider, the group would intercept messages sent by individuals of interest to the Chinese government. The criminals then searched for messages based on the keyword list containing items of geopolitical interest for Chinese intelligence services. Sanitized examples include the names of political leaders, military and intelligence organizations, and political movements at odds with the Chinese government.

MESSAGETAP also sets aside SMS messages if they are sent from or to particular phone numbers, or from or to a device with a particular International Mobile Subscriber Identity (IMSI) unique identifier. When it was discovered, the malware was tracking thousands of device phone numbers and IMSI codes at a time.

During attacks, the threat actor also interacted with call detail record (CDR) databases to query, save, and steal records about individuals of interest. Targeting CDR information provides a high-level overview of phone calls between individuals, including time, duration, and phone numbers.



MESSAGETAP is a 64-bit ELF data miner initially loaded by an installation script. Once installed, the malware checks for two files: keyword_parm.txt and parm.txt, which contain instructions for MESSAGETAP to target and save SMS message content. Both files are deleted from the disk once the configuration files are read and loaded into the memory. After loading the keyword and phone data files, MESSAGETAP begins monitoring all network connections to and from the server. It uses the libpcap library to listen to all traffic and extracts SMS message metadata, including SMS message content, IMSI numbers, and source and destination phone numbers.

Based on the above information, users and organizations must consider the risk of unencrypted data being intercepted several layers upstream in their cellular communication chain. This is especially critical for frequently targeted individuals such as dissidents, journalists, and officials who handle highly sensitive information.

BGP Hijacking

BGP hijacking remains a serious problem. Attacks and deliberate interruptions often occur because companies fail to correctly set configurations or prefix filters.

Date	Name	Brief description
07/21/2020	AS 264462 Comercial Conecte Sem Fio Ltda me, Brazil	13,046 prefixes leaked. The affected ISPs belong to India, Russia, South Korea, Vietnam
06/09/2020	IBM Cloud	IBM Cloud (cloud data center) malfunctioning because an external provider sent incorrect routes
04/23/2020	AS205310 Beiersdorf Shared Services GmbH, Germany	90,000 prefixes compromised: Routes were redirected to AS15943 instead of AS8220
04/22/2020	AS263444 Open X Tecnologia Ltda, Brazil	9,328 prefixes leaked from 1250 AS, including Akamai, Cloudflare, Vodafone, NTT, Amazon, NVIDIA
04/05/2020	AS7552 Viettel, Vietnam	4,825 prefixes of 326 operators leake
04/01/2020	AS12389 Rostelecom, Russia	8,870 prefixes leaked from nearly 200 AS including Akamai, Cloudflare, Hetzner, Digital Ocean, Amazon AWS
03/31/2020	AS50048 NEWREAL-AS, Russia	Leak of 2,658 prefixes in Tier-2 ISP Transtelecom. The prefixes belonged to Orange, Akamai, and Rostelecom
02/16/2020	AS139070 Google Asia Pacific Pte. Ltd., Singapore	—
02/07/2020	AS8359 "MTS", Russia	225 prefixes leaked from 36 AS

Growing power of DDoS attacks

An increase in the number of Internet of Things (IoT) devices has led to more and more hosts being added to infamous botnets such as Mirai. In addition, new botnets have emerged.

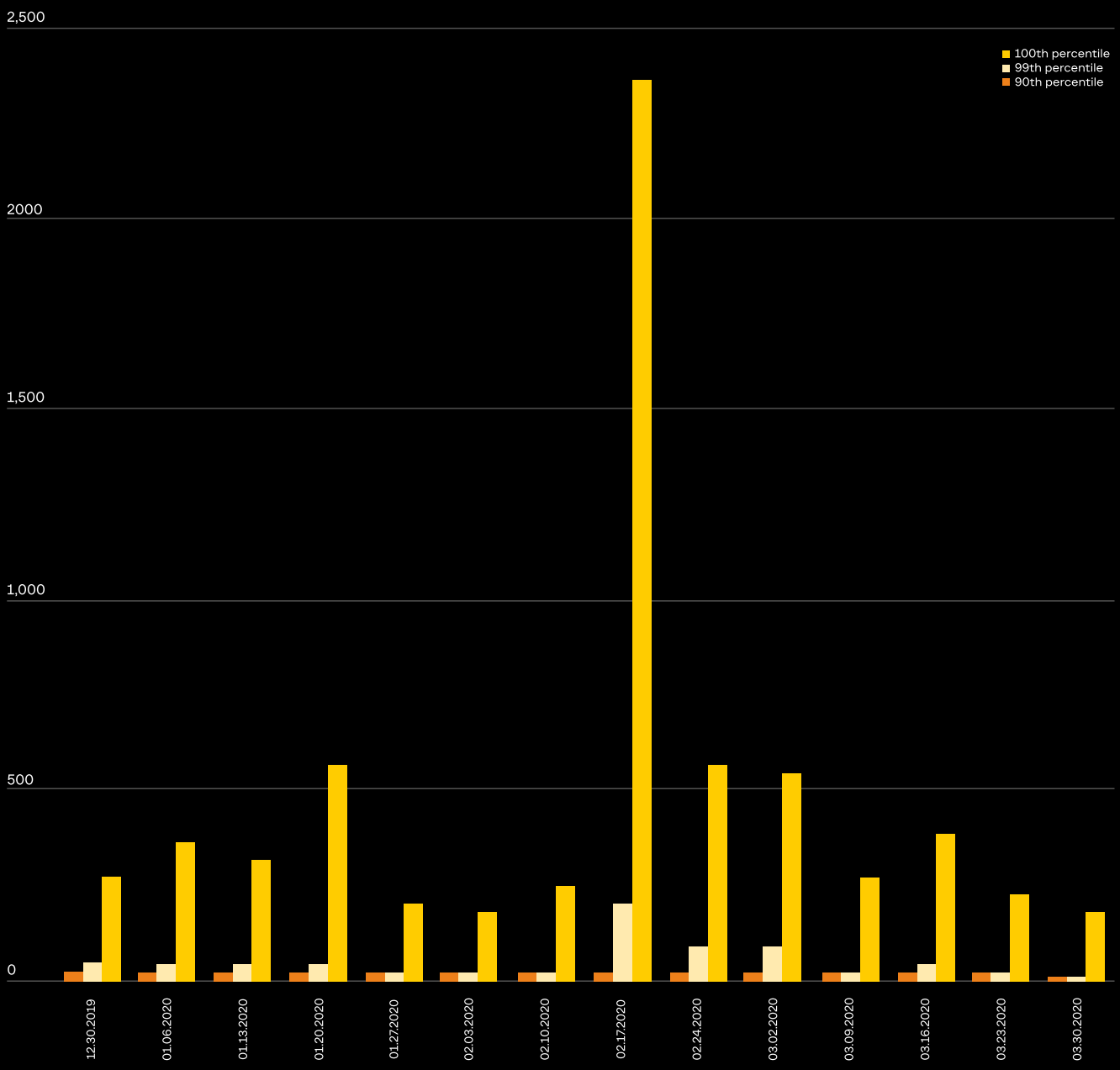
As regards DDoS attack techniques, SYN floods still remain the most common type of attack. ICMP flood attacks rose from last to second place in popularity, and HTTP floods finished in last place — they have become less widespread since January 2019.

In 2020, denial-of-service attacks became more effective. In the first half of 2020, threat actors set new records for DDoS attack power.

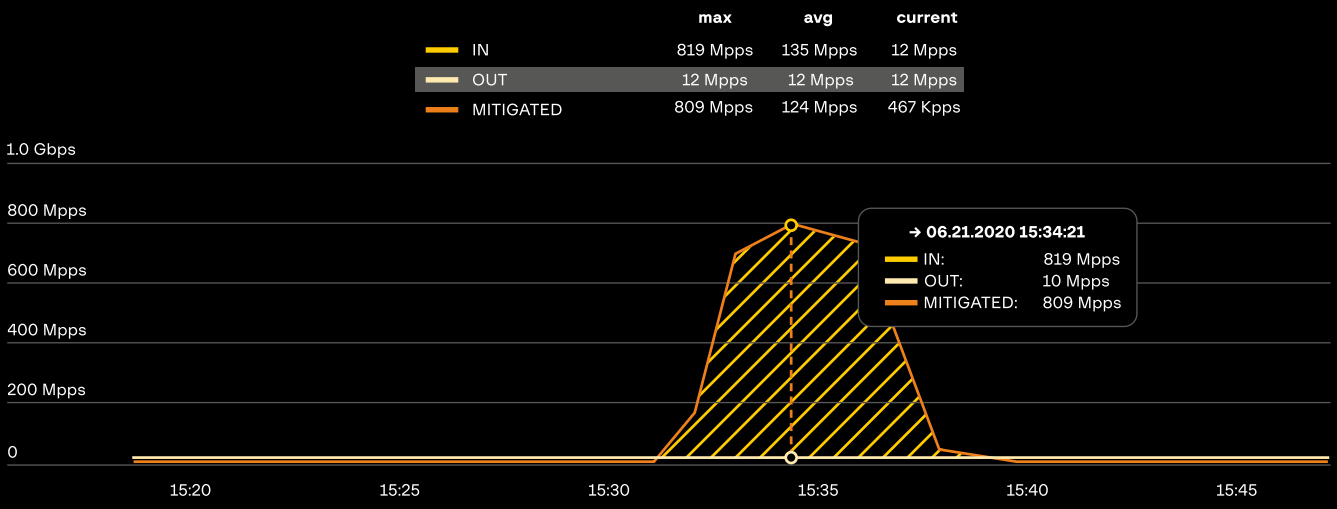
Largest Gbps DDoS attack ever recorded

According to Amazon's Q1 2020 threat report, its AWS Shield service mitigated the largest DDoS attack ever recorded, stopping a 2.3 Tbps attack in mid-February this year. The company did not disclose the attack's target or origin. The attack was carried out using hijacked CLDAP web servers and lasted three days. CLDAP (Connectionless Lightweight Directory Access Protocol) is an alternative to the older LDAP protocol that has been abused for DDoS attacks since 2016. CLDAP servers are known to amplify DDoS traffic by 56 to 70 times its initial size, making it a highly sought-after protocol and a common option provided by DDoS-for-hire services.

The previous record for the largest DDoS attack ever recorded was 1.7 Tbps. It was mitigated by NETSCOUT Arbor in March 2018. The attack abused Memcached servers exposed to the Internet and reached massive bandwidths.



Largest Mpps DDoS attack



Source: Akamai (https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html)

Largest Mpps DDoS attack

A bank in Europe was hit by a massive, distributed denial-of-service (DDoS) attack that generated a record 809 million packets per second (PPS). The record DDoS attack was mitigated by Akamai on June 21, 2020. The company did not disclose the bank's name.

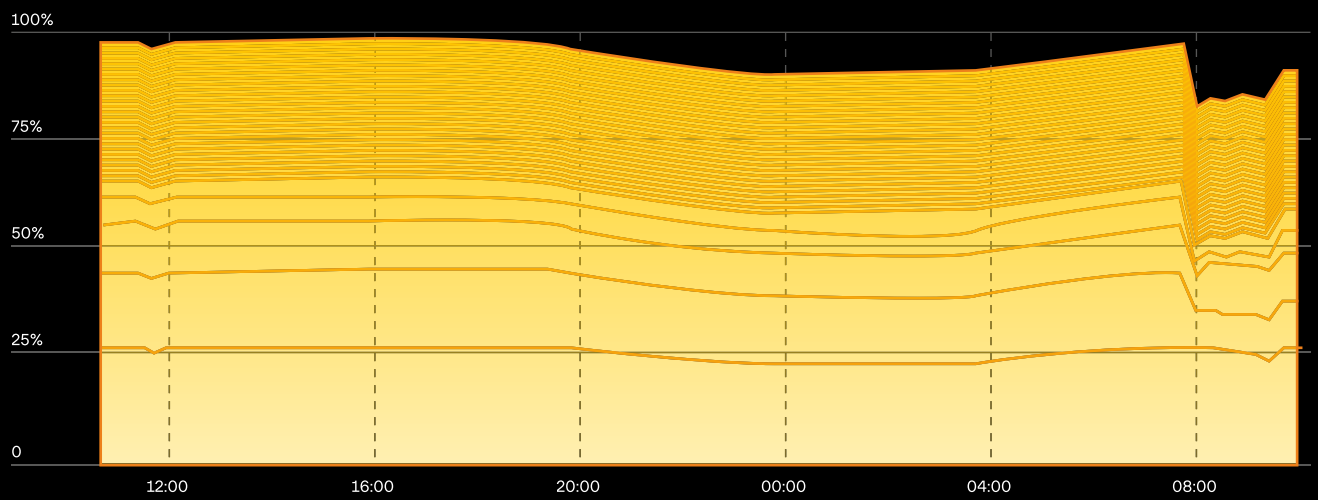
It was unusual that 96.2% of the IP addresses involved in the attacks were not being tracked as recent attacks, which suggests that a new botnet emerged. The June 21 attack was remarkable not only for its size, but also because of how quickly it reached its peak. The attack grew from normal traffic levels to 418 Gbps in seconds before reaching its peak size of 809 Mpps in approximately two minutes. In total, the attack lasted just under 10 minutes.

Nation-level accessibility issues

In early February 2020, Iran's infrastructure came under a large-scale DDoS attack, which left 25% of users in Iran without Internet. The NetBlocks Internet observatory, which maps Internet security and freedom in real-time, confirmed that there was extensive disruption to the Iranian telecommunications network that began on the morning of February 8 at 11:45 local time.

The consequences of the massive DDoS attack left the country's major network operators unable to operate for one to seven hours.

Nation-level accessibility issues



Netblocks.org: Network Connectivity, Iran: → 02.07.2020 — 02.08.2020 UTC

THREATS TO THE ENERGY SECTOR

Iran and India

Nuclear power facilities in these countries were targeted this year

Bypassing Air gaps

New tools for attacks on physically isolated networks have appeared

9 groups

linked to special services have showed an interest in the energy sector

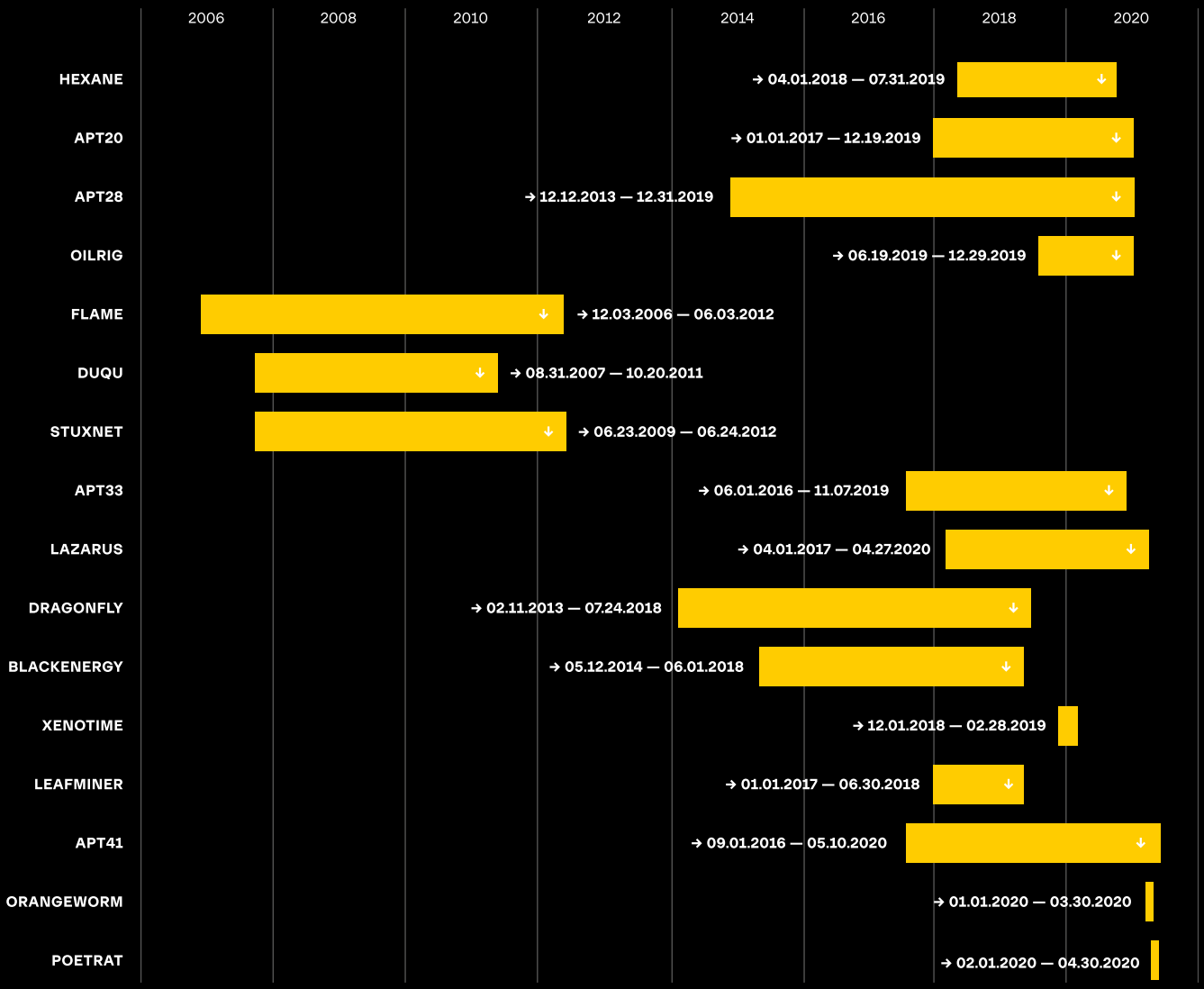
It has been a challenging year for the energy sector. The most notable threats occurred in the nuclear power industry. For more details, please refer to the "Military Operations" section of this report. As part of their operations, adversaries shut down power units at nuclear power plants and physically destroyed the surrounding infrastructure.

In the reporting period, Iran's nuclear energy facilities were sabotaged, while facilities in India were subject to espionage attacks. Threat actors are particularly interested in India because the country is developing nuclear technology and thorium-based reactors.

Apart from special services, organized crime groups also began to pose a serious threat to energy companies. Both can disrupt production using ransomware to obtain a ransom.

During the reported period, 9 groups linked to intelligence services actively attacked the energy sector. At the same time, some of these groups (e.g. China-based APT41) actively used ransomware to disable networks.

Nation-state actors attacking the energy sector



9 GROUPS

linked to intelligence services actively attacked the energy sector during H2 2019 — H1 2020

APT20

The Chinese-backed hacker group APT20 attacked companies in ten countries as part of a campaign called Operation Wocao. The group's attacks affected various industries, including the energy sector.

The hackers compromised target networks via vulnerable web servers managed by a company or government entity. The threat actor then propagated across the network looking for system administrator credentials with privileged access to the infrastructure's most critical parts.

APT20 installed keyloggers on computers used by administrators in order to capture keystrokes and steal passwords. The campaign involved tools such as web shells for file upload and command execution, a script for scanning the system for information, the custom XServer backdoor, CheckAdmin to identify if administrators are logged in, and others.

APT28

The group APT28 is believed to have been behind a phishing attack against the Ukrainian oil and gas group company Burisma in early November 2019.

The threat actors registered lookalike domains that mimicked legitimate websites belonging to Burisma's subsidiaries and partners. In particular, domains targeting the following subsidiaries were discovered: KUB-Gas LLC, Esko-Pivnich, and CUB Energy Inc.

To carry out the attack, the threat actors sent employees emails with links to login pages. The links looked legitimate. In addition, the attackers set up sender authentication records using SPF and DKIM. After victims followed the link and entered their credentials, the attackers gained access to them and could use them to further the attack. Some employees entered their credentials on the fake webpages, which allowed the threat actors to stealthily operate within the organization and obtain the information they needed.

APT41

The group APT41 used a new ransomware family called ColdLock to conduct a series of attacks against several organizations in Taiwan. Analysis of the malware revealed similarities between ColdLock and the previously known Freezing ransomware family as well as the EDA2 "educational" ransomware kit. For example, Freezing and ColdLock have a similar method of propagating within networks (compromised AD servers), similar reflective injection methods, and a similar internal module architecture.

ColdLock terminates the following services on the system before encrypting their files:

— mariadb
— msexchangeis
— mssql
— mysql
— oracleservice

It also terminates the Outlook process and checks the Windows version running on the system. If the system is running Windows 10, the ransomware carries out several Windows 10-specific routines. Windows Defender is disabled, as is the ability to send feedback/malware samples to Microsoft. Push notifications are disabled as well.

According to media reports, the campaign struck the computer systems of Taiwan's state-owned energy company, CPC Corp., which delivers oil products throughout Taiwan. Although the attack did not affect the company's energy production, it did reportedly prevent some customers from using CPC Corp.'s payment cards to purchase gas.

PoetRAT

A new remote access Trojan named PoetRAT was discovered in February 2020. The attacks affected Azerbaijan's government agencies and industrial companies, mainly in the energy sector. The investigation revealed that cybercriminals are particularly interested in SCADA systems used in the electricity sector, specifically in wind turbine systems.

RAT is written in Python and has all the features specific to this type of malware. It gives the operators complete control over the compromised system.

The attackers sent malicious Microsoft Word documents, some of which were made to look like messages from Azerbaijani government agencies or from the Defense Research and Development Organization of India. Some of the file names mentioned COVID-19.

The threat actors monitored specific directories, which meant that they wanted to exfiltrate specific information about the victims. The attackers likely wanted to get a full picture of the victims by using keyloggers, browser credential stealers, and Mimikatz and pypykatz for further credential harvesting.

OilRig

Iranian hackers were once again found to be using wipers, but this time the attacks are attributed to the OilRig group (aka APT34). A new Trojan called ZeroCleare was used in a recently discovered targeted attack on an oil and gas company.

The attack most likely started in the fall of 2018 with reconnaissance scanning from various low-cost/free VPN providers and gaining access to one of the accounts that was later involved in the attack. During the summer of 2019, the attackers used a password spray from a system on the local network to gain access to additional accounts, install ASPX web shells, and gain domain administration privileges.

After the device was compromised through a vulnerable driver, the wiper spread to other devices in the network for further destructive attacks. The malware then overwrote the master boot record (MBR) and disk partitions on Windows-based machines using a legitimate driver, EldoS RawDisk. While Group-IB researchers could not determine the exact number of organizations that were impacted, at least 1,400 hosts were affected by ZeroCleare.

Later, a new strain of ZeroCleare data-wiping malware called Dustman was detected on the network belonging to Bapco, Bahrain's national oil company. A common component of the malware is EldoS RawDisk. Dustman differs from other wipers by the fact that the necessary drivers and loaders are supplied in one executable file and not two, as is the case with ZeroCleare. Dustman also overwrites the volume, while ZeroCleare erases it by overwriting it with junk data (0x55).

In this case, however, OilRig was most likely trying to cover its tracks as the hackers had previously made mistakes that revealed their presence on the network.

Orangeworm

Since January 2020, a wave of attacks involving the Kwampirs Trojan has been identified. The malware has been linked to the Orangeworm group, which used the Trojan to attack companies in the healthcare sector, in particular software supply chain companies.

After penetrating the system, Kwampirs collects basic data about the device and sends it to a remote server. Attackers then gain access to sensitive data using the backdoor on the infected machine. If the compromised system is identified as potentially interesting, the data is stolen and the malware is copied to all available machines and network resources.

This year, the threat actor has been conducting supply-chain attacks against software vendors, but the group's ultimate interest has changed. They now attempt to gain access to organizations that support industrial control systems (ICS) for the global production, transmission, and distribution of energy.

Orangeworm is not officially associated with any country. The FBI has said, however, that the Kwampirs source code shows that the Trojan is similar to the infamous Shamoon wiper developed by the Iranian hacker APT33, though the latter does not have a wiper component.

Attackers most often use the following methods to bypass air gaps:

Many industrial networks are “air gapped” and to some extent isolated from other internal networks. But even protected networks can be breached.

Attackers most often use the following methods to bypass air gaps:

— Trusted USB devices
— Connected Raspberry Pi devices
— Supply-chain attacks

During the reporting period, new tools for jumping the air gap emerged:

Group	Trojan	Modus operandi
Cycldek (China)	USBCulprit	USBCulprit is delivered using another Trojan (NewCore RAT), which initially reaches users via spear phishing emails, usually politically themed. Once it is in the system, USBCulprit scans paths to executable files, collects documents with certain extensions, and exports them to USB drives connected to the system. When a USB drive infected with USBCulprit is connected to a computer, the Trojan will copy stolen files either to or from the removable drive.
Tropic Trooper (China)	USB worm USBferry	The threat actors ferry a malware installer via USB into an air-gapped host. The malware checks for network connectivity. If it determines that the network is unavailable, it tries to collect information from the target machine and copy the collected data to USB storage. After that, the Trojan exfiltrates information and uploads it to the C&C server.
DarkHotel (South Korea)	Ramsay 1 September 2019) Ramsay 2.a (early March 2020) Ramsay 2.b (end of March 2020)	All versions of the malware differ from each other and infect victims in different ways. Versions 1 and 2.b exploit a vulnerability in .doc (CVE-2017-0199), .rtf (CVE-2017-11882), and Visual Basic mechanisms integrated into Word. Version 2.a is disguised as a 7zip installer. The persistence mechanism is selected based on the Ramsay version used. Some have a special Spreader component that copies Ramsay to all PE files located on disks, including removable drives, in order to eventually reach isolated systems. The threat actor exfiltrates the collected data using an external component that has not yet been detected.
Turla	COMpfun	The hackers have updated the classic COMpfun remote access Trojan by adding the ability to check whether a USB drive is connected to the infected host. Security experts believe that this mechanism is used by Turla to infect physically isolated systems and spread the Trojan automatically.
Transparent Tribe	USBWorm component of the Crimson Trojan	USBWorm is a component developed for stealing files from removable drives and spreading malware across systems by infecting removable media. To steal data, the malware enumerates all the files stored on the device and copies those with an extension matching a predefined list. As part of the infection process, the malware lists all directories. Then, for each directory, it creates a copy of itself in the drive root directory using the same directory name and changing the directory attribute to “hidden”. This results in all the actual directories being hidden and replaced with a copy of the malware using the same directory name. Moreover, USBWorm uses an icon that mimics a Windows directory, tricking the user into executing the malware when trying to access a directory.

Analysis of these attacks reveals that threat actors usually apply the following techniques to attack the energy sector:

Attack vector	Modus operandi
Reconnaissance via OPC	Attackers use the OPC protocol to gather information about the equipment being used and to identify its topology.
Access to SCADA HMI	Since HMI workstations have a small attack surface, in addition to standard methods of gaining access to computers running Windows, hackers actively investigate vulnerabilities in the HMI. Exploiting such vulnerabilities means that malicious code can be executed.
Controller management	Attack frameworks (e.g., Idustroyer) are being supplemented with modules that allow threat actors to manage controllers using standard protocols such as IEC 60870-5-101, IEC 60870-5-104, and IEC 61850.
Control over emergency shutdown systems	Control over emergency shutdown systems allows hackers to stop production, so attackers have developed specialized modules for this purpose (e.g., the Triton framework).
Infiltration through home routers and NAS	In order to detect industrial networks, the threat actors load modules for traffic analysis and Modbus protocol detection (e.g., the VPNFilter framework) on network devices.

Organized crime targeting the energy sector

Crime groups conduct two main types of attack on the energy sector:

— Active sale of access, including to networks belonging to energy companies

— Ransomware attacks

Many types of ransomware have been equipped with new capabilities to detect processes associated with industrial control systems. This has caused substantial losses of critical data and higher ransom amounts for recovering access to such data. This is especially true for data stored on Historian servers.

Sale of access

In 2019, cybercriminals stopped publish full company names very often, making it more difficult to categorize a compromised company. Based on the descriptions presented, six companies in the energy sector were identified. Five of them are associated with the extraction of energy resources.

In 2020, Group-IB did not observe an increase in the sale of access to networks belonging to energy companies. This year, access to seven companies was offered for sale. Two companies are involved with energy directly and five are associated with production. The only company whose name has been published is Entrust Energy.

2019

Date	Seller	Industry	Name	Domain	Region	Price ($)
03/04/2019	Achilles	Mining, quarrying, and oil and gas extraction	None	None	None	None
04/28/2019	Lampeduza	Mining, quarrying, and oil and gas extraction	Stevin Rock LLC	stevinrock.com	United Arab Emirates	900
08/10/2019	bc.monster	Energy	None	None	None	4,600
09/15/2019	B.Wanted	Mining, quarrying, and oil and gas extraction	None	None	USA	4,600
09/21/2019	Gabrie1	Mining, quarrying, and oil and gas extraction	None	None	USA	24,000
11/11/2019	nikolaruss	Mining, quarrying, and oil and gas extraction	None	None	Turkey	3,500

2020

Date	Seller	Industry	Name	Domain	Region	Price ($)
02/08/2020	ellis.J.douglas	Energy	Entrust Energy	entrustenergy.com	USA	1,600
03/16/2020	rexus	Mining, quarrying, and oil and gas extraction	None	None	China	10,000
04/18/2020	cryzaa	Mining, quarrying, and oil and gas extraction	None	None	None	3,000
04/27/2020	Network	Mining, quarrying, and oil and gas extraction	None	None	None	None
05/14/2020	zeoman	Mining, quarrying, and oil and gas extraction	None	None	Netherlands	2,000
06/11/2020	fatfish	Energy	None	None	Canada	500
06/30/2020	drumrlu	Mining, quarrying, and oil and gas extraction	None	None	United Arab Emirates	2,000

Ransomware attacks on energy companies

Over the past year, eleven attacks against energy companies have been detected. Five of the targeted companies are linked to energy directly and six are related to production. At the same time, there is no specific type of ransomware used in this industry: the attacks involved eight different ransomware families.

Date	Ransomware	Industry	Name	Domain	Region
11/11/2019	DoppelPaymer	Mining, quarrying, and oil and gas extraction	Pemex	pemex.com	Mexico
01/14/2020	Maze	Energy	Electricaribe	electricaribe.co	Colombia
02/20/.2020	Clop	Mining, quarrying, and oil and gas extraction	INA Group	ina.hr	Croatia
04/02/2020	Nefilim	Mining, quarrying, and oil and gas extraction	Aban Offshore	abanoffshore.com	India
04/06/2020	Maze	Mining, quarrying, and oil and gas extraction	Groupement Berkine	Нет	Algeria
04/28/2020	Nefilim	Mining, quarrying, and oil and gas extraction	W&T Offshore, Inc.	wtoffshore.com	USA
05/26/2020	NetWalker	Energy	SolarReserve	solarreserve.com	USA
06/09/2020	Snake	Energy	Enel Argentina	enel.com.ar	Argentina
07/03/2020	REvil	Energy	Light S.A.	light.com.br	Brazil
07/06/2020	Ragnar	Energy	Energias de Portugal	edp.com	Portugal
07/24/2020	NetWalker	Mining, quarrying, and oil and gas extraction	Axens	axens.net	France

THREATS TO THE BANKING SECTOR

Focus shifted to ransomware

criminals use more convenient and profitable methods

Small and poorly protected banks

are still being successfully attacked for targeted theft of funds

Leaks including transaction history

are likely to pose risks to the sector, together with ransomware

The era of targeted attacks on banks to steal funds is over. Last year's report covered five active groups: Cobalt, MoneyTaker, Silence, SilentCards, and Lazarus, all of which successfully committed thefts through SWIFT, ATM Switch, card processing, and ATMs. In 2020, such thefts have almost stopped.

Recent thefts

SWIFT

Only Lazarus and Cobalt stole via SWIFT. The most recent public incident occurred in February 2019 at the Bank of Valletta in Malta.

The most interesting events always remain behind the scenes, however, and attempts to commit theft have not stopped entirely. Over the past year, Group-IB researchers detected incidents in several countries (Argentina, India, Kenya, Ghana, and Jordan) per quarter, but not all attempts were successful. Two groups were active during this period: NanoSwift and Lazarus.

NanoSwift

At least one known incident involving this group took place. Compromise was initially achieved using a legitimate remote access tool called RMS, which was installed using a VBS script:

install.vbs
c719a030434d3fa96d62868f27e904a6
f2f750a752dd1fda8915a47b082af7cf2d3e3655
2696ee4302a85c6b4101fc6d1ce8e38b94fd9c2bbd1acc73b553576b3aacb92f

This script has been “in the wild” for a long time and was first uploaded to VirusTotal on October 8, 2018.

For further propagation, the attackers used the well-known NanoCore Trojan, which was saved on the system as lanss.exe in the \LAN Subsystem\ lanss.exe directory, which is a typical NanoCore indicator known since 2018.

The following tools were used to escalate privileges:

Tool	Description
Invoke-MS16135.ps1	A privilege escalation exploit that is a part of PowerShell Empire
Invoke-MS16032.ps1	
RoguePotato.zip	Tools for running programs with SYSTEM privileges
SysExec.exe	
cve-2020-0796-local.zip	CoronaBlue exploit
Hooker_3.4.zip	Hooker keylogger by Den4b
rkfree_setup_2.26_password_123.exe	Revealer keylogger

Evidence suggests that the threat actor uses quite an old toolset. It is effective only if the hackers attack a bank with a minimum level of security and set “traps” for the incident response teams.

What is notable, however, is the use of CVE-2020-0796, which was made public in March 2020, and the first exploit was made available in the same month. A file named cve-2020-0796-local.zip was published on GitHub on April 3. This indicates that the incident took place between April and July 2020.

Lazarus

Lazarus mainly attacks small banks because they are an easy target.

In 2020, it transpired that the group purchases pay-per-install services from operators of the TrickBot botnet. This explains why, in the case of several incidents, it was noted that the TrickBot Trojan loaded into the memory malicious code developed by Lazarus, which was downloaded from external servers. The incidents involved two domains used by Lazarus from which malicious code was downloaded:

— util98[.]com, registered on April 24, 2019
— startmary[.]com, registered on January 13, 2020

Based on the dates when the domains were registered, the organizations were compromised in April 2019 and January 2020, but the thefts were attempted one to two months later.

Card processing

In the past, the groups Cobalt, MoneyTaker, and Silence were reported to attack card processing systems. However, recent attacks of this type were carried out by Silence only, in the first half of 2019.

The Philippine government-controlled United Coconut Planters Bank (UCPB) was robbed in September 2020. The reports mentioned that the attackers increased the ATM withdrawal limit from 20,000 pesos to 10 million pesos per day.

They also gained access to InstaPay, an interbank transfer system.
As a result, they siphoned 167 million pesos (USD 3.44 million) from the bank.

Following the investigation, four Nigerian citizens were arrested.

ATM Switch

The only group that leveraged ATM Switch access during the reporting period is Lazarus. In August 2020, US-CERT issued a security alert that this group had resumed its activity and that they had malicious code in their arsenal that could be used to steal funds through an ATM Switch running Windows. In the past, this code was used only to attack AIX operating system versions. Despite the alert, the most recent theft was detected in 2018.

ATM

Many groups (Cobalt, MoneyTaker, Silence, Lazarus) possess ATM Trojans, but they don't actively use these tools.

In September 2019, Group-IB researchers described a Trojan called Dtrack used by Lazarus, which was discovered back in 2018. Since then, it has not been used for theft purposes.

In the second half of 2019, Silence was the only group to carry out attacks on banks. They successfully infiltrated several banks in Chile, Costa Rica, and Bulgaria, but their attacks were thwarted at early stages.

In November 2019, two files were uploaded to VirusTotal from the Republic of Senegal: xfs.dll and dns.dll.

The xfs.dll file was compiled on October 19, 2019. It is likely that the ATM attack was carried out on this day, and this is evidence of the last such successful attack conducted by Silence. At the time, the main Trojan used by Silence was XDA.RAT.

The XDA.RAT source code is based on an open-source project: https://github.com/iagox86/dnscat2. The application supports the following commands:

— 0: ping command
— 1: create a cmd.exe process
— 2: execute a shell command
— 3: download a file
— 4: upload a file from the infected device to the C&C server
— 5: close all connections
— 6: change the interval of making requests to the server
— 7: save the %LOCALAPPDATA%\updatea.bin file
— 8: overwrite the <%XDA_path%>\updatea2.bin file
— 9: get information about the connected dispenser
— 10: carry out an ATM jackpotting attack

It is important to note that the functionality for working with ATMs has been borrowed from xfs-disp.exe, which we described in our report on Silence. The XDA.RAT source code is therefore based on two projects: dnscat2 and xfs-disp.exe.

When the Trojan receives the 9 command, it collects information in the same way as xfs-disp.exe:

1. It attempts to connect to the following dispenser service providers:

— CashDispenser (Nautilus)
— NXCdm (Nautilus)
— DBD_AdvFuncDisp (Diabold)
— CurrencyDispenser1 (NCR)
— CDM30 (WINCOR)
— GEN (WINCOR GEN)
— ATM (GENERIC)

2. It logs the maximum number of banknotes that can be dispensed in a single operation (using WFS_INF_CDM_CAPABILITIES).

3. It logs the current status of the dispenser (whether it is connected and busy), the state of the safe door, the state of the dispenser's logical cash units, the state of the shutter, etc. The format is as follows:

```
state=%d, safedoor=%d, dispenser=%d, stacker=%d
pos=%d, OutputPosition=%d, shutter=%d, transport=%d
...
pos=%d, OutputPosition=%d, shutter=%d, transport=%d
```

4. It logs information about the status and contents of ATM cassettes. The output is displayed as a format string:

```
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d][%d]
...
Id:%s(nr=%d)(l=%d,h=%d), %d|%d|%d of %d [%s][%d][%d],[%d][%d]
```

The application receives the following parameters with the 10 command:

— Flag.
  — If this value is 0, the application withdraws cash from a specific cash unit.
  — If this value is 1, the application withdraws cash from all cash units.
— Integer value: Cash unit index
— Integer value: Cash count

The application performs ATM jackpotting attacks in the same way as xfs-disp.exe. The only difference is that the application can extract a specific amount of money from a given cash unit.

Shift in priorities

The main challenge that threat actors face when attacking banks is not how to gain access to the target system, but how to eventually withdraw and launder the stolen funds. If attackers find an opportunity to make the same amount of money while attracting less attention from law enforcement agencies with a higher chance of success, they shift their focus. This is what happened with Cobalt and Silence.

We still come across the unique malicious codes used by Cobalt and Silence, but no related thefts have been detected.

Presumably Cobalt or some of its members have joined the private Thanos ransomware affiliate program. This fact is confirmed by the use of a unique packer for Thanos ransomware. The same packer was used by Cobalt for their unique CobInt Trojan.

Silence did not end their activity in 2020, either. Group-IB discovered new C&C servers used in attacks against atypical targets: medical and industrial companies in Western Europe.

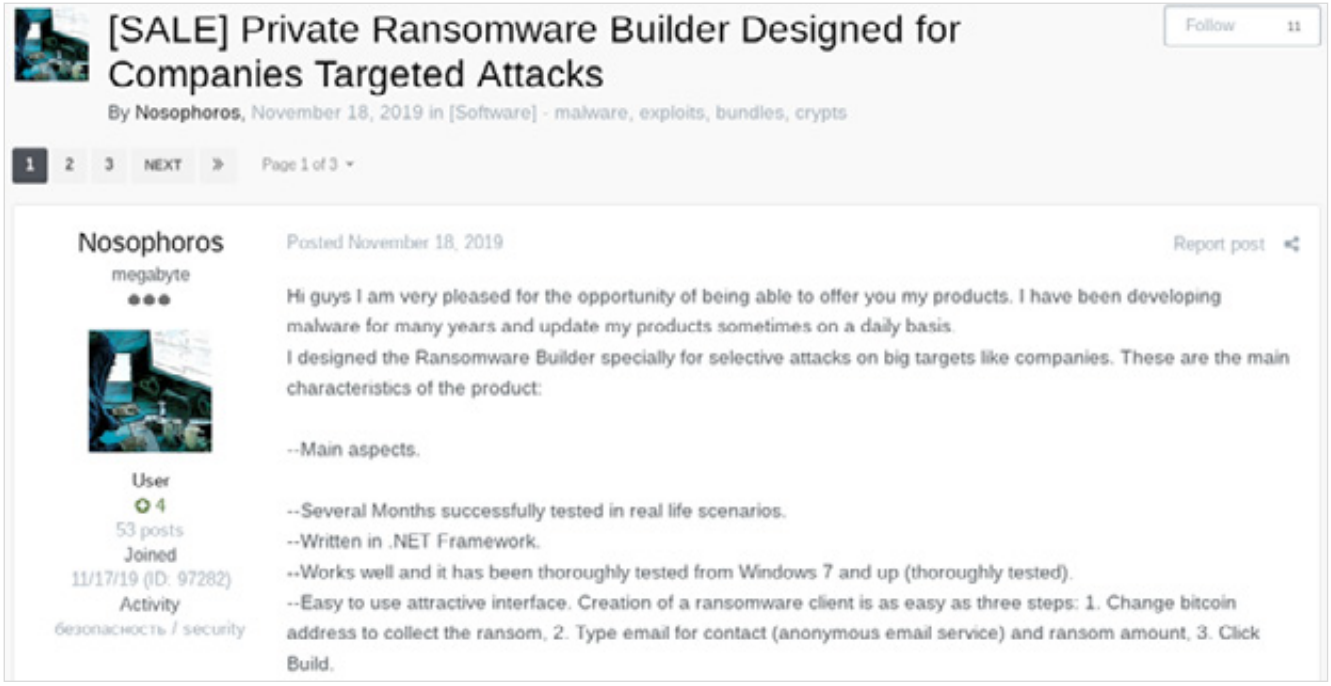


Figure 9. Sale of a ransomware builder

THREATS TO THE RETAIL SECTOR

2.5-fold increase
in the number of JS sniffers

63.7 million bank card dumps
obtained using POS Trojans were put up for sale

92% of all card dumps
were related to the United States

There are four main threats that could critically damage retail businesses:

— JS sniffers
— Attacks on POS terminals
— Credential stuffing
— Ransomware

Ransomware attacks are easy to understand and, as a rule, companies are aware of them. As such, we will discuss only the first three threats underlying the carding and mass fraud market.

General carding trends

The carding market can be divided into two main segments: sale of textual card data (number, expiration date, holder's name, address, CVV) and sale of dumps (contents of magnetic stripe cards).

Textual data is collected using phishing websites, PC/Android banking Trojans, and ATMs. Threat actors intercept such data also by hacking e-commerce websites and using JS sniffers. The latter were this year's main novelty and are becoming increasingly widespread among cybercriminals.

Dumps are obtained using skimming devices and Trojans for computers with connected POS terminals.

The carding market has grown from $880 million last year to $1.9 billion. The doubling applies to both text data and dumps. The amount of text data offered for sale has increased from 12.5 to 28.3 million cards, while dumps have surged from 41 to 63.7 million.

JS sniffers

Over the past year, the number of attacks on online stores has increased. This is because the use of JavaScript sniffers to steal bank cards has become one of the main techniques of obtaining large volumes of payment information. The increase in attacks was also caused by the trend of reselling access to various websites and organizations on underground forums.

Sniffer family	Price	Number of stolen cards
Inter Developed by an underground forum user with the nickname Sochi, who is also the developer of the Red Alert Android Trojan.	$990	—
CoffeMokko This sniffer family was developed independently by the criminal group that uses it. To monetize stolen data, the criminals created their own card shop.	N/A	180,000
ImageId This family was developed by an underground forum user with the nickname poter, who has been selling the solution since 2017. At the moment, the sniffer is not offered for sale anymore. One criminal group still uses a variant of it, however.	$5,000	22,000

The most popular JS sniffer families

The number of known JS sniffer families has grown from 38 to 96 compared to the previous year. Each of the new families deserves to be analyzed separately.

According to Group-IB's findings, over the past year nearly 460,000 bank cards compromised using JS sniffers. Additionally, 645,000 bank cards were put up for sale at card shops for a total of $3.6 million.

The top nine banks that issued the stolen cards are located in the US, with 170,000 cards in total. Cybercriminals are also interested in cards issued in Brazil, Australia, Canada, Spain, the United Kingdom, India, Singapore, and France.

Lazarus, JS sniffers, and Bitcoin theft

In July 2020, security researchers reported that the state-sponsored APT group Lazarus used JS sniffers to steal credit card data from 25 online stores worldwide.

Group-IB researchers identified two campaigns that involved infrastructure previously seen in attacks attributed to the North Korean group.

The first campaign began in May 2019. The attackers used the ClientToken sniffer family to infect 20 online stores.

The second campaign began in February or March 2020 and targeted large online stores. In total, three websites were infected with the Preloader sniffer. Group-IB found two websites that the attackers used to collect cards stolen during the Preloader campaign, which may indicate a greater number of victims.

Group-IB researchers also discovered the BTC Changer campaign, during which a modified version of ClientToken was used to spoof the address of a Bitcoin wallet at the time of payment on online stores that accept Bitcoin. Specialists found two websites infected during this campaign, which brought the attackers 0.66983720 BTC (approximately $7,800).

Sale of access to online stores

Access to hacked online stores — for the purpose of subsequently deploying a sniffer — can be purchased on underground forums. The price heavily depends on the country in which the store operates, the number of buyers per day, and the type of payment system used on the website. If payment is made in a separate window opened in an iframe or after being redirected to the payment system website, then it is more difficult to deploy a sniffer. Such lots will therefore be cheaper than websites on which card data is entered on the website itself.

To gain access to a store or install a JS sniffer, cybercriminals continue to use known vulnerabilities in popular e-commerce CMS. They also employ malicious software to steal passwords and conduct brute-force attacks on administrative control panels of stores or DBMS. For example, threat actors continue to conduct attacks using the GoBrut malware written in GoLang. The program is used to conduct distributed brute-force attacks on online stores and administrative panels of popular CMS such as Magento, OpenCart, phpMyAdmin, and cPanel. Subsequently, the threat actors leverage access to administrative panels and administration tools to install JS sniffers on the target websites.

Evasion techniques

To prevent malicious code from being detected and removed from the victim website, cybercriminals use several techniques.

- Most techniques are based on using JavaScript to load the main JS sniffer code when the user is on the checkout page. In the past, JS sniffers were often loaded from a link using the script tag.
- Another increasingly popular technique involves concealing the JS sniffer code within an image. The injector code downloads the image from the attackers' server, extracts the JS sniffer code, and executes it on the online store page.
- Criminals still use the code for detecting whether a browser's console is open to avoid being detected by researchers and security tools. The malicious code will not be run and will not execute the main load if it detects that the browser's developer console is open on the visitor's website.
- To avoid detection, JS sniffer families also use several different checks under the responsibility of the server-side sniffer: the main JS sniffer code will be obtained only if (i) the user's IP address does not belong to the network of a large cloud provider, (ii) the user's country (determined by IP address) corresponds to the country of the store, and (iii) the Referer field contains the address of the infected store's payment page. If at least one of these checks fails, a benign JS script of a legitimate library is returned in response to a sniffer code request.
- Loading the main sniffer code using JavaScript helps attackers conceal the address from which the code is loaded. The simplest code samples use Base64 to hide links to malicious JS files. However, we often find samples of malicious code in which the link to the JS sniffer is stored in encrypted form and as a concatenation of parts of a URL address or a string with a reverse character order.
- Group-IB Researchers also found samples of malicious code that used the Domain Generation Algorithm (DGA) to obtain the website address from which the main sniffer code will be downloaded. The actual address depended on the exact date that the attackers created one domain for each month. If one of the domains was blocked, all they had to do was wait and the flow of bank card data from the infected store would resume.

Attacks on POS terminals

The main product sold by carders is bank card dumps. In total, 63.7 million dumps were found for sale during the reporting period, which is 156% more than last year.

The main method of compromising magnetic stripe data is infecting computers with connected POS terminals with special Trojans that collect data from RAM. In total, 14 Trojans were found to be active during the reporting period:

- RtPOS
- TinyPOS
- UdPOS
- FighterPOS
- DiamondFox
- GratefulPOS
- FrameworkPOS
- MajikPOS
- DMSniff
- PinkKite
- BADHATCH
- Pillowmint
- GlitchPOS
- Alina POS

During the reporting period, Group-IB researchers established that 19 retail chains were compromised, as a result of which millions of bank cards were put up for sale.

Country	Number of dumps H2 2019 — H1 2020	Percent	Number of dumps H2 2018 — H1 2019	Difference (2020 vs 2019)
UNITED STATES	58,921,367	92.37%	39,895,064	1.48
INDIA	1,723,722	2.70%	17,246	99.95
SOUTH KOREA	644,672	1.01%	77,573	8.31
UNITED KINGDOM	584,519	0.92%	466,296	1.25
CANADA	565,535	0.89%	198,741	2.85
BRAZIL	447,412	0.70%	168,294	2.66
MEXICO	276,935	0.43%	43,832	6.32
FRANCE	234,076	0.37%	53,804	4.35
UNITED ARAB EMIRATES	208,089	0.33%	82,446	2.52
AUSTRALIA	182,263	0.29%	41,288	4.41

During the reporting period, Group-IB researchers established that 19 retail chains were compromised, as a result of which millions of bank cards were put up for sale.

Date	Compromised company	Database name on card shops	Number of cards
July 2019	Deer Valley Resort	—	—
August 2019	Hy-Vee (Hy-Vee Market Grilles, Market Grille Expresses and Wahlburgers)	SOLAR ENERGY	3,188,056
August 2019	Russell Stover's retail stores	—	—
September 2019	Krystal, Moe's, McAlister's Deli and Schlotzsky's	NEW WORLD ORDER	3,419,867
November 2019	North american fuel dispenser merchants (visa report)	—	—
November 2019	Church's Chicken	—	—
November 2019	Catch	—	—
November 2019	on the Border	—	—
December 2019	Noth american fuel dispenser merchants (visa report)	—	—
December 2019	WAWA	BIGBADABOOM-III	15,065,318
December 2019	Islands Restaurants	—	—
December 2019	Champagne French Bakery Cafe	—	—
January 2020	Landry's	—	—
January 2020	The crack shack	—	—
February 2020	—	NIRVANA BREACH	1,049,577
February 2020	Rutter's	—	—
February 2020	Quaker Steak & Lube	—	—
March 2020	Key Food	—	—
April 2020	Main Event	—	—

Despite how many services sell bank card dumps (card shops), most major databases were exposed on two well-known resources: Joker's Stash and Trump's Dumps. The surges clearly show that the number of compromised retail chains is much higher:

Date	Number of dumps	Database name	Card shop	Number of dumps in the specified database	Distribution by country in the database	The cost of the whole database
08/02/2019	471,540	GOOD-KARMA-DISCOUNT-SALE	Joker's Stash	320,518	USA (99.7%)	$961,554,00
08/20/2019	689,382	SUNRISE-01-US (SOLAR ENERGY BREACH)	Joker's Stash	481,071	USA (99.7%)	$12,099,755,00
08/20/2019	689,382	SUNRISE-01-EU (SOLAR ENERGY BREACH)	Joker's Stash	203,875	Lebanon (26.8%), France(9.08%), Brazil (8.72%) and other EU countries	$40,114,790,00
10/28/2019	1,727,559	INDIA-MIX-NEW-01	Joker's Stash	1,333,266	India (98%)	$133,326,600,00
11/22/2019	921,549	NEW-WORLD-ORDER-01-US (NWO BREACH)	Joker's Stash	225,242	USA (100%)	$4,541,410,00
11/22/2019	921,549	NEW-WORLD-ORDER-02-US (NWO BREACH)	Joker's Stash	485,113	USA (100%)	$9,517,595,00
01/27/2020	3,845,727	BIGBADABOOM-III-US-part1 (BBB3 BREACH)	Joker's Stash	974,877	USA (99.9%)	$20,415,497,00
01/27/2020	3,845,727	BIGBADABOOM-III-US-part2 (BBB3 BREACH)	Joker's Stash	974,829	USA (99.9%)	$20,408,637,00
01/27/2020	3,845,727	BIGBADABOOM-III-US-part3 (BBB3 BREACH)	Joker's Stash	1,237,912	USA (99.9%)	$25,922,342,00
01/27/2020	3,845,727	BIGBADABOOM-III-EU-part1 (BBB3 BREACH)	Joker's Stash	381,940	UK (21.8%), Australia (16.8%), Puerto Rico (16.3%) and other EU countries	$74,813,895,00
03/06/2020	598,510	BIGBADABOOM-III-US-part19 (BBB3 BREACH)	Joker's Stash	186,074	USA (99.9%)	$3,895,216,00
03/06/2020	598,510	DWELL-DISCOUNT-SALE	Joker's Stash	136,270	USA (94.2%), Korea (4.29%)	$681,350,00
03/06/2020	598,510	06.03_USA_ASIA_PIN_DISCOUNT	Trump's Dumps	66,929	Hong Kong (39.3%), China (26.3%), Taiwan (13.4%)	$996,435,00
03/23/2020	564,950	AURIFEROUS-DISCOUNT-SALE-5USD	Joker's Stash	292,121	USA (98.5%)	$1,460,605,00
03/23/2020	564,950	BIGBADABOOM-III-US-part25 (BBB3 BREACH)	Joker's Stash	189,945	USA (100%)	$3,973,479,00
04/09/2020	531,978	SCARFACE-DISCOUNT-SALE-5USD	Joker's Stash	397,465	Korea (49.9%), USA (49.3%)	$1,987,325,00
04/12/2020	461,865	12.04_USA	Trump's Dumps	431,542	USA (74.5%), Korea (22%)	$3,590,317,00
04/25/2020	455,377	CONSERVATIVE-DISCOUNT-SALE-5USD	Joker's Stash	382,643	USA (77.4%), Korea (21%)	$1,913,215,00
04/29/2020	1,061,346	STOCK-DISCOUNT-SALE-5USD	Joker's Stash	281,652	USA (98.8%)	$1,408,260,00
04/29/2020	1,061,346	29.04_USA	Trump's Dumps	223,864	USA (98.9%)	$1,953,469,50
04/29/2020	1,061,346	BIGBADABOOM-III-US-part35 (BBB3 BREACH)	Joker's Stash	186,883	USA (99.9%)	$3,915,851,00
04/30/2020	526,638	30.04_USA	Trump's Dumps	389,592	USA (78.4%), Korea (18.2%)	$3,264,337,00
05/01/2020	610,381	IRONY-DISCOUNT-SALE-5USD	Joker's Stash	365,602	USA (88.9%), UAE (9%)	$1,828,010,00
05/11/2020	1,007,295	ZONDER-DISCOUNT-SALE-3USD	Joker's Stash	613,333	USA (98.6%)	$1,839,999,00
05/12/2020	691,320	12.05_US_AE	Trump's Dumps	370,549	USA (88.8%), UAE (8.33%)	$2,953,153,25
06/11/2020	672,373	12.06_US_AE	Trump's Dumps	344,273	USA (91.5%), UAE (5.8%)	$3,258,824,00
06/22/2020	504,060	19.06_USA_ZIP_PIN_DISCOUNT	Trump's Dumps	257,547	USA (56.6%), UAE (10.1%)	$3,863,205,00
06/22/2020	504,060	BIGBADABOOM-III-US-part53 (BBB3 BREACH)	Joker's Stash	181,718	USA (99.9%)	$3,792,718,00
06/29/2020	566,534	XXXBBB-DISCOUNT-SALE-1USD	Joker's Stash	229,644	USA (99.9%)	$229,644,00
06/29/2020	566,534	BIGBADABOOM-III-US-part56 (BBB3 BREACH)	Joker's Stash	181,549	USA (99.9%)	$3,789,953,00
TOTAL						$352,602,650

Credential stuffing

One of the most common security issues is the credential stuffing technique, i.e. extracting login-password pairs from various leaks (email, phone number, and other identification data can be the login) for subsequent brute-force attacks.

The problem is that many users choose the same passwords for different resources, and if one resource becomes compromised, the same login credentials could be used on others. It is also worth noting that currently almost all major leaks are initially put up for sale, then become publicly available on underground forums, which makes it easy for attackers to collect databases for credential stuffing attacks. This applies to all retailers with personal accounts on online resources, but also to some bank accounts and e-wallets.

Types of monetization

Gaining access to bank accounts and e-wallets

Bank accounts and e-wallets are among the most obvious targets for cybercriminals. Hackers prefer attacking online resources that give direct access to the victim's money. Some banks provide access to online banking using the pair email:password or phone:password, which makes them attractive targets.

It is difficult for cybercriminals to directly withdraw funds from banks because such operations usually require confirmation (two-factor authentication) from the account holder. This explains why this monetization method is not the most popular one.

That being said, e-wallets do not usually involve such sophisticated security measures as those deployed to protect bank accounts. After gaining access to the electronic wallet, attackers attempt to either make purchases at the victim's expense or transfer the funds to another wallet, registered to a money mule, through various exchange services.

Monetizing reward points

Online and offline retailers often offer members of their loyalty programs cashback for purchases in the form of reward points or money. Reward points can usually be used to pay for only a part of a purchase, but in some cases they can be used to pay for an entire order.

— A common method of monetizing reward points is by purchasing goods that can later be resold. Criminals purchase gift cards for stores that sell digital content (e.g., PlayStation Store, Xbox Store), then resell the cards or use them to pay in-store.
— If attackers gain access to many user accounts, they can group reward points together and pay for a large number of purchases and/or buy more expensive goods.
— In some retail chains, bonus points can be used to pay at checkout in-store. In such cases, cybercriminals use virtual loyalty cards, barcodes, and discount coupons from the user's personal account to cash in bonus points and pay for purchases.

Monetizing funds for paid services

Some retailers offer services that can be paid for by topping up a personal account on the website.

If criminals gain access to a user account with a positive balance on their personal account, the threat actors can use these funds to obtain paid services from the retailer. In some cases, cybercriminals sell access to such accounts.

Receiving gift points or goods

Retailers offer users rewards and gifts for upgrading to a higher level of service or a more expensive tariff.

Attackers can take advantage of access to a user's account and independently transfer it to another level of service in order to receive a reward. The threat actor will then sell the reward.

Access to personal data

In the user's personal account on the retailer's website, attackers can gain access to the following personal data:

— full name
— contact information (phone number, email, delivery addresses)
— data about payment methods (bank card and/or account numbers, accounts in payment systems)

If personal user data in the retailer's accounts is poorly protected, attackers can exfiltrate it for subsequent social engineering attacks or to be sold to other interested parties.

Attack techniques

To carry out such actions, threat actors need:

— login-password lists from various leaks
— lists of proxy servers to bypass blocking due to a limited number of requests allowed from one IP address
— a program that will receive as input the lists of logins, proxies, and the address of the resource to check the existence of a user with such login and password details

Tools used to carry out the above attacks are of the greatest interest to threat hunters. They can be divided into three main categories:

— bots without browsers
— browser bots
— hybrid solutions

Bots without browsers

This is the most primitive way to implement such tools. Bots without browsers are extremely simple, they work reliably and quickly, but they cannot bypass anti-bot solutions.

There are many different offers of ready-made tools on the market, but one of the most widespread is OpenBullet, an open source tool. Its main advantage is extensibility. Threat actors must usually adapt the code for each online resource, which needs to be checked for certain user accounts. In OpenBullet, as in many other tools, the code is adapted in configuration files. This means that many users write configuration files for different resources, and the largest of them have long been on the list.

A distinctive feature of paid resources is a more comprehensive offer. Developers of paid tools constantly update proxy lists and write log parsers to extract contact and payment information from personal accounts.

Since it is easy to conduct attacks using bots without browsers, some scammers prefer to write their own scripts to perform attacks against specific resources.

Hybrid solutions

Since bots without browsers cannot pass CAPTCHAs and receive cookies, scammers have developed a hybrid solution.

Criminals launch the browser either automatically or manually and receive cookies. The cookies are then added to the bot configuration file, after which the bots check login and password details (without the need to launch a browser). This scheme is easy to implement and, most importantly, it works quickly and does not require many computing resources.

To bypass various types of CAPTCHAs, hackers can use either separate tools that solve the simple types or SaaS services for their solution. In the latter case, scammers automatically send the link to the service via the API and receive a cookie or a solution in response.

Hybrid methods can bypass almost all anti-bot solutions.

Browser bots

It is rare to find resources with reliable protection. More often than not, these are large social media or IT giants that use their own solutions to protect against bots. In such cases, scammers write unique browser bots for each resource.

Browser bots are full-fledged browsers that automatically start, open pages, run scripts, and emulate user behavior on a website.

This variant is much more expensive than the previous ones. It requires a great deal of customization, while running many browsers requires more server power and, most importantly, is much slower.

BANKING TROJANS

Latin America

remains the main source of this type of threat

12 out of 19 banking Trojans

were written by Russian-speaking developers

Switch to ransomware

Owners of banking botnets
are following the popular trend

Every year, several banking botnets disappear from the market and new ones rarely take their place. This year was no exception. At this rate, the market for PC banking Trojans may become nonexistent in three to five years.

Trojans for PC

A total of 19 PC banking Trojans were active this year, 12 of which were written by Russian-speaking developers. Six Trojans were developed by Latin American authors.

Russian-speaking owners of the largest banking botnets have also followed the main trend of switching to using ransomware. For example:

— Trickbot uses the following ransomware: Ryuk (later Conti), Kraken, Thanos
— Dridex uses WastedLocker, DoppelPaymer; it previously used BitPaymer, Locky, Bart, and Jaff
— Qbot (Quakbot) started using ProLock
— zLoader/Silent Night also switched to using an unidentified ransomware
— RTM, which is the only banking botnet active in Russia, uses Cerber

A shift in focus does not mean that threat actors stop committing thefts. If they see an opportunity to transfer a large amount of money, they will take it. But as a general rule, their main income now comes from ransomware.

This change in behavior has led to less damage from theft and changed the money laundering market.

Given that the most widespread banking Trojans used to be developed by Russian-speaking cybercriminals, the decrease in thefts has led to this segment degrading more significantly.

Old and active	Guildma (Astaroth), Grandoreiro, Javali, Melcoz, CamuBot, Metamorfo, Qbot, Gootkit, Trickbot, Gozi (ISFB, Ursnif, Dreambot), IcedID (Bokbot), Ramnit. Backswap, Dridex, LokiPWS, Retefe, RTM, Danabot
New	zLoader/Silent Night
Disappeared	TinyNuke (aka NukeBot), Panda Banker, Osiris, MnuBot

During the analyzed period, only one new banking Trojan developed by Russian-speaking authors appeared: Silent Night. It is an improved version of the old Axebot Trojan and was used in attacks on German Internet users. During the same period, another three Trojans created earlier by Russian-speaking authors stopped being used completely: TinyNuke, Panda Banker, and Osiris.

Russia

The only banking Trojan for PCs in Russia is RTM, which does not seem to be used much and will likely soon cease to exist. This banking botnet uses Cerber ransomware.

Latin America

Latin America has become the main source of banking Trojans. In 2020, five new Trojans emerged: Guildma (Astaroth), Grandoreiro, Javali, Melcoz, and Metamorfo. All have been active for several years, but attracted the attention of researchers only recently.

The developers of these Trojans live in Latin America and their Trojans are used locally, although some of them are starting to attack Europe and the United States.

USA and Canada

Traditionally, the US and Canada have been the primary targets for banking Trojans. Even Latin American developers have added American banks to their config files.

Currently, eleven Trojans for PCs pose a threat to clients of US and Canadian banks, ten of which were developed by Russian-speaking hackers: Metamorfo, zLoader/Silent Night, Gootkit, Trickbot, Gozi, IcedID, Danabot, Ramnit, Dridex, LokiPWS, and Qbot.

APAC

In the APAC region, banking Trojans have barely undergone any significant changes. The key targets are Japan and Australia, which are attacked using well-known Trojans: Trickbot, Gozi, Danabot, Ramnit.

Trojans for Android

The Android Trojan market is similar to the PC Trojan market. The main developers are Russian-speaking hackers. However, developers from Latin America are actively expanding to the market and use their tools to attack bank customers locally.

In total, ten Android banking Trojans were active this year, five of which are brand new.

An author of the Red Alert banking Trojan with the nickname Sochi stopped developing Trojans and switched to working with JS sniffers.

Authors of Android Trojans are not picky about names. For instance, Alien Bot appeared in 2020, but Trojans with the same name but from other developers had existed before.

Android Trojans mainly use web fakes, i.e. dialog boxes that request the information required (passwords, bank card numbers, etc.) from the victim. Services offering to develop such web fakes appeared in the Russian-speaking underground segment. As a result, banking Trojan authors no longer need to spend time supporting certain applications for collecting financial data. It is enough to buy a set of web fakes and the Trojan can be used in almost any region, which is what usually happens with Trojans created by Russian-speaking cybercriminals.

Old and active	Anubis, Flexnet, Gustuff, BasBanke (Coybot), Cerberus
New	Ginp, Alien Bot, BlackRock, Hydra, EventBot
Disappeared	Red Alert, Asacub

Russia

Only two Android Trojans were active in Russia: Flexnet and Anubis. They did not cause significant damage. For example, Flexnet spread more massively and was able to infect 50,000 devices and intercept data from just over 5,000 bank cards.

Anubis spread more selectively, using landing pages disguised a Russian bank brand, and infected about 400 clients in a targeted way.

Latin America

The locally developed BasBanke Trojan was most active in Latin America. BasBanke works as part of an affiliate scheme, i.e. several people can distribute it at once.

USA and Canada

Russian-speaking authors adhere to the unspoken rule that Android Trojans should not be used to attack US clients, although the authors of web fakes are actively creating windows to collect data from US financial institutions.

Only two Trojans pose a threat: the new Alien Bot and BlackRock.

APAC

Threats for the APAC region are posed by all Trojans developed by Russian-speaking hackers: Anubis, Gustuff, Cerberus, and the new Alien Bot.

Trojans for PC

	PT	CL	CA	BR	EC	DE	PE	FR	IT	ES	PL	AT	NL	AU	JP	NZ	GB	CH	US	NO	LI	LU	SE	MX
Latin American developments																								
Guildma (Astaroth)	●			●																				
Grandoreiro	●			●		●	●			●							●							●
Javali				●																				●
Melcoz		●		●						●														●
CamuBot				●																				
Metamorfo		●	●	●	●					●									●					●
Russian-language developments																								
zLoader/Silent Night			●			●											●		●					
Gootkit	●					●		●	●		●	●							●					
Trickbot			●			●				●	●			●	●		●		●					
Gozi (ISFB, Ursnif, Dreambot)			●			●			●		●			●		●			●					
IcedID (Bokbot)			●														●		●					
RTM*																								
Danabot						●			●		●	●		●										
Ramnit									●						●									
Dridex**																								
LokiPWS**																								
Retefe																		●		●	●	●	●	
Qbot													●						●					
Unidentified origin																								
Backswap										●														

Trojans for Android

	PT	CL	CA	BR	TR	DE	PE	FR	IT	ES	PL	AT	NL	AU	JP	IL	GB	CH	US	IN	MY	LU	TH	MX	CZ	HR	HU	BE	BG
Latin American developments																													
BasBanke (Coybot)	●	●		●					●	●														●					
Russian-language developments																													
Anubis**																													
Gustuff**																													
Cerberus**																													
Unidentified origin																													
Alien Bot			●		●	●	●	●	●	●			●	●	●	●	●		●	●	●	●	●		●				
Ginp										●	●						●												
BlackRock			●		●	●		●	●	●	●	●		●			●		●							●	●	●	●
Hydra																													
EventBot					●	●		●	●	●							●	●											

* Attacked CIS
** Global attacks

WEB PHISHING AND SOCIAL ENGINEERING

118% more phishing websites

were identified and taken down compared to the previous reporting period

Phishers are targeting sports betting and online services

increasingly often

Criminals are using new techniques and tools

to evade detection

Between H2 2019 and H2 2020, 118% more phishing resources were identified and taken down compared to the previous reporting period.

This significant growth can be explained by two main factors:

— **The pandemic**. During lockdowns, many attackers had more time to devote to malicious activity. In addition, phishing, as one of the simplest earning schemes, attracted the attention of a larger audience as many people lost their income due to the pandemic.

— On the other hand, lockdowns increased the demand for online shopping. More and more people began to order goods and services from home. Scammers quickly adapted to this trend and began carrying out phishing attacks on services and individual brands, which previously did not have much financial appeal to them.

— **Change of tactics**. In previous years, attackers ended their campaigns after fraudulent websites were taken down and quickly switched to other brands. Today, they are automating their attacks instead and replacing the blocked pages with new ones.

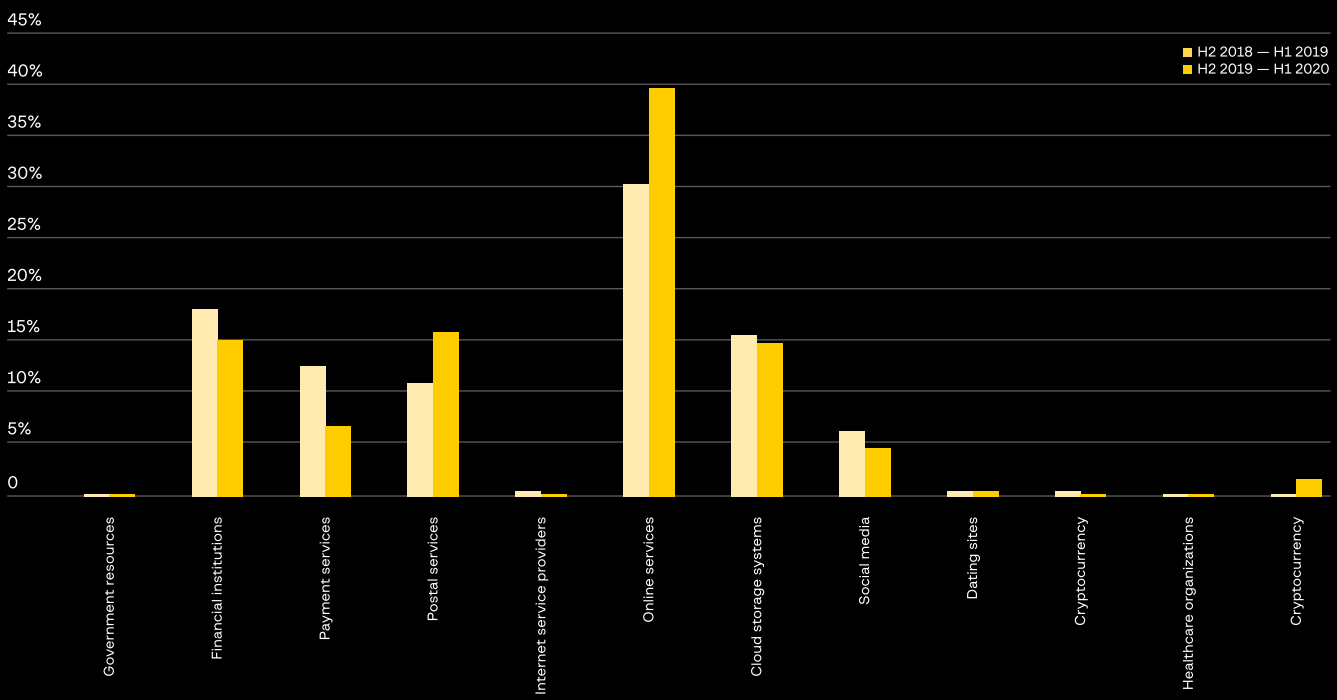
Phishing attacks targeting bookmakers increased in Q2 2020, amounting to 6% versus 2% in the previous quarter. Compared to H2 2018-H1 2019, phishing targeting bookmakers grew by more than 20% during the reporting period.

Postal services and financial institutions also remained a key target for attackers.

Another attack type that increased significantly was phishing used to collect accounts for various online services such as Microsoft, Netflix, Amazon, eBay, and Valve Steam.

Phishing resources targeting cryptocurrency projects have disappeared almost completely. The main reason lies in the waning interest in ICO projects, which were a key target for phishers in 2017 and 2018.

	H2 2018 — H1 2019	H2 2019 — H1 2020
Government resources	0.3%	0.1%
Financial institutions	18.3%	15.0%
Payment services	12.9%	6.6%
Postal services	11.6%	15.6%
Internet service providers	1.6%	0.7%
Online services	30.5%	39.6%
Cloud storage systems	15.8%	14.5%
Social media	6.0%	4.5%
Dating sites	1.4%	1.2%
Cryptocurrency	1.5%	0.0%
Healthcare organizations	0.1%	0.0%
Bookmaker offices	0.1%	2.2%



Phishing evasion techniques

So far, the main 2020 trend is the use of one-time unique links that become inactive after the user opens them. This means that if someone clicks on the link at least once, it will not be possible to obtain the same content again in order to collect evidence. This significantly complicates the process of taking down phishing resources.

Common evasion techniques used by phishers are listed below:

— **One-time links**. A unique one-time link is generated for each user.
— **Blocking by subnets**. The subnets of many companies that provide phishing page detection services are blacklisted, and if a request for a page comes from their subnets, phishing content will not be shown.
— **Blocking by user agent**. Attackers understand who their target audience is, and if it is clear from the user agent that this is not a real user, phishing content will not be shown. For example, if a criminal carries out an attack on mobile device users, all visitors with a PC browser will not receive the phishing page. Phishing kit scripts usually contain a list of keywords that are checked in the user agent field.
— **Blocking by region**. GeoIP databases are actively used by various criminals and phishing is no exception. If the target audience is located in Singapore, there is no point in showing the phishing page to users in the United States.
— **Redirects to official websites**. If some checks are failed, instead of phishing content visitors will be redirected to the attacked brand's official website or to websites belonging to other legal services.

Affiliate programs

Phishing scammers cannot do much damage on their own. As such, there are affiliate programs that bring together people who want to make money by phishing.

In Russia, the main reason for the significantly higher numbers of phishing attacks is the emergence of various affiliate programs for hackers wanting to make money off phishing involving fake bank rewards programs, lottery draws, paid surveys, and more. At the final stage of the scam, the victim is prompted to enter their payment details or make a transfer.

The affiliates distribute links to as many people as possible. Affiliate program organizers create landing pages, accept payments, and help launder money. For example, in a short period of time, one of the affiliate programs created more than 12,000 accounts of money mules to transfer stolen money.

So far, this trend has been observed only in Russia. Russia is often used as a testing ground, so similar schemes are likely to appear in other countries.

Automated management of phishing projects

Since the start of the year, there has been a rise in advanced social engineering, namely when multi-stage scenarios are used in a phishing attack. As part of such increasingly popular phishing schemes, threat actors first stake out the victim: they establish contact with the target individual (e.g., through a messenger), create an atmosphere of trust, and only then do they direct the victim to a phishing page.

Communications between members of such new criminal gangs are especially interesting. Hackers coordinate attacks, communicate, and distribute stolen funds through dedicated Telegram channels and bots. A typical infrastructure for such a project built around Telegram might include the following features:

— a bot for recruiting, where information about a new potential cybergroup member is entered (scamming experience, age, link to a profile on the forum, etc.)
— a bot for displaying information about successful thefts (nickname in Telegram, how much money was made and how)
— private channels for interaction/communication/support for members of the scam group
— bots for generating phishing links based on certain settings, which are introduced by group members during attacks

In addition to the traditional phishing kits, underground hacker forums nowadays offer ready-made management platforms designed to automate phishing projects. Thanks to such platforms distributed as SaaS, the number of groups that can be easily scaled is growing. The number of members in a group built around such platforms can reach several dozen people. Automating management of a criminal group in turn leads to the emergence and spread of more complex social engineering. The latter is slowly starting to be used in large-scale attacks and not only in targeted attacks as before.

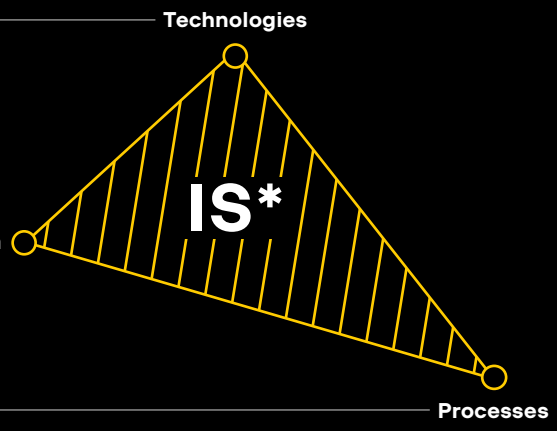
RECOMMENDATIONS FOR TOP MANAGEMENT

Three pillars of information security

Nowadays, threat actors are continuously innovating. Criminals implement new tools with more enthusiasm and much faster than many companies. This is what affects the balance of power on the information security battlefield. Take advantage of the latest developments and solution classes available on the market to prevent your opponent from gaining the upper hand.

Even the latest generation of automated security systems are managed by a team. It is this team of specialists that determines how much of the product's capabilities you use and therefore the effectiveness of the solution. Learning and innovation must become a continuous process.

The number of people in your response team and existence of playbooks is just as important as the coherence and interchangeability of each unit within that team. Consultants always advise you to assign roles in the team, but do you conduct "rehearsals" on a regular basis? Do all team members know how they should act in any given situation? Involve your team in creating a playbook and establish effective interaction between teams and employees.



*Information security

General recommendations

Threat hunting and proactive defense	Monitoring and proactive threat detection are not new for the cyber industry, but not everyone is managing to implement these processes. You need to constantly collect and match indicators of compromise and TTPs of attackers. Train your team in new techniques, improve their skills, and provide them with the latest tools.
Hygiene and hygiene	Phishing and social engineering have remained the most popular vectors of initial compromise. Ordinary employees hold their defenses behind their monitors and inboxes every day. Establishing a password policy and conducting training and social engineering testing will help protect against phishing and prevent corporate data leaks.
Trust MSS providers and partners	Product innovations aren't slowing down their momentum, and technical skills are always needed to ensure information security. Therefore, more companies are delegating part or most of their information security tasks to MSS providers. Doing so not gets best-in-class technical specialists at your side without hiring but also is beneficial for budget allocation.
Keep in touch with your competitors	To raise awareness of new threats, you need to go beyond professional trainings and start a dialogue with colleagues from your industry. Competitors could become your partners in the fight against common enemies: APTs, pro-state groups, ransomware attacks, and others.
Checkups and cyber risk insurance	Just as people need regular checkups, so do companies need to regularly assess their security infrastructures. Nowadays, this applies not only to infrastructure but also to teams and processes. The standard set of checkups should be supplemented with a third-party audit as well as an assessment of potential retrospective compromise. It is important to note that the above does not negate the importance of cyber risk insurance, especially when you are responsible for the information of your customers and employees.
Measuring performance	Information security is becoming more expensive for companies, which is why many are requesting that the effectiveness of solutions be measured and compared. The saturated market dictates the new rules: solutions should not just be modern and efficient but also advantageous for businesses. Comparing costs to the effectiveness of a tool in its pilot stage also requires defining business metrics that differ in one way or another from the size of the company and its infrastructure. Analysts from Gartner, Forrester, and other analytical agencies handle the market's requests to collect performance measurements and their metrics.

Recommendations for how to set up your technical infrastructure and train your information security team

— Hunt for traces of covert activity by threat actors in the company network. This helps stop an ongoing attack for which the initial stages were overlooked by the organization's security controls.

— Implement a Malware Detonation Platform that allows for suspicious files and links to be run in an isolated environment, be analyzed in detail, and subsequently blocked if found to be malicious.

— Use a Threat intelligence solution to identify threats, leaks, breaches, and other hacker activity before they can harm you.

— Back up regularly. Any backups must be separated from the main network so that they cannot be accessed by threat actors if administrator accounts become compromised.

— Conduct round-the-clock monitoring of information security events and be prepared to promptly respond.

— Each incident should be matched with its level of complexity. Incidents that require analysis should be investigated, the causes and consequences should be identified, and the problems that caused the incident should be fixed. For the second level of response, it is important to have a third-party incident response team with pre-negotiated agreement that can assist in stopping a complex targeted attack.

— Make sure that your team has the necessary skills to perform threat hunting and collect threat intelligence.

— Conduct regular digital hygiene training for employees.

— Perform security assessments in a format that simulates real-life actions taken by cybercriminals. This approach will help identify weaknesses in the company's IT infrastructure and determine whether the company is ready to combat real cyberattacks.

— Conduct periodic fraud risk assessments to see if your solutions and procedures can defend against existing attacks and fraudulent schemes that use different attack channels. Identify the main risk factors, and start from existing and possible problems when choosing a fraud protection solution.

— Create a layered protection for your web portal using not only transaction analysis, but also solutions for session analysis of behavior and devices, and unveil fraudulent operations that occur on your web channel. Leave only legitimate users on your portal and take actions regarding blocking suspicious users or bots.

Unfortunately, it is not always possible to detect attacks at early stages: threat actors continuously improve their skills and implement new techniques to gain access to networks of various size. Detecting traces of compromise at different stages of the cyber kill chain requires an ia ntegrated approach. This approach involves creating a centralized data source about what is happening in the network infrastructure and isolating compromised hosts. XDR solutions can be used for these purposes, as they are able to detect malicious activity at various layers, regardless of the tactics, techniques, and procedures used by threat actors.

Reducing cyber attacker dwell time also requires not only high-quality response but also proactive analysis, which can be carried out both by the organization's employees with relevant competencies and by outsourced experts. The latter speeds up the investigation and improves the quality of analysis significantly.

Both reactive and proactive approaches require not only relevant competencies but also a significant amount of cyber threat intelligence data. Strategic, operational and tactical threat data help organizations identify attackers during the ongoing analysis and detect signs of compromise at the earliest stages.

Incident Response team capabilities

Log analysis
Firewall, Proxy, NetFlow, AV, EDR, EventLog, etc

Malware analysis

Endpoint digital forensics

Cyber Threat Intelligence

Infrastructure Manipulation and Maintenance
Windows (Active Directory), Unix/Linux, hypervisor, cloud

Incident management
Risk management, Crisis management

Cyber professions of the future are jobs built on skills that are in demand today. Such professions are not taught as part of traditional curricula.

1. **Digital Forensics Analyst**
   Windows Forensics, Network Forensics, Memory Forensics, Forensics Data Recovery Mobile Forensics
2. **Incident Responder**
3. **Threat Hunter**
4. **Malware Analyst**
5. **Threat Intelligence Analyst**

TECHNICAL RECOMMENDATIONS FOR COUNTERACTING CYBERATTACKS

Primitive errors: vulnerable software versions in publicly accessible services or weak passwords; vulnerabilities with public exploits

- Update software regularly.
- Automatically inventory software to identify outdated programs.
- Regularly conduct security assessments and penetration testing to identify weaknesses in the network and establish possible attack vectors.
- Enhance your password policy.
- Implement multi-factor authentication.
- Implement VPNs to protect services on the external network perimeter. If this is not an option, set up an SSO.

Distributed brute-force attacks on remote access interfaces (RDP, SSH, VPN) and other services (using new botnets)

IoT botnet owners selling access to devices installed on corporate networks

- Make an inventory of the external network perimeter, firewall rules, and network address translation (NAT) rules to prevent services from being externally accessible by mistake.
- Do not, under any circumstances or even temporarily, make devices that can easily be compromised accessible from the Internet. These include devices used for video surveillance, smart homes, office equipment (printers, scanners, and multifunctional devices), and storage such as NAS servers in the SOHO segment.
- Ensure that remote access services for operating systems are not accessible externally (e.g., RDP, SSH, VNC, SMB/RPC).
- If this cannot be avoided, change the SSH/RDP port to a non-default one and implement a white list of IP addresses that can access these services.
- Ensure that remote access meets the following requirements:
  - Multi-factor authentication.
  - Enhanced password policy.
  - The ability to restrict network access for the tasks of a specific account (e.g., contractors are granted access only to servers they need, not the entire segment or network).
- Set fields such as "expires at" for accounts and access rules in case manual revocation of remote access fails.
- Make an inventory of the external network perimeter, firewall rules, and network address translation (NAT) rules to prevent services from being externally accessible by mistake.
- Do not, under any circumstances and even temporarily, make devices that can be easily compromised accessible from the Internet: video surveillance devices, smart home devices, office equipment (printers, scanners, and multifunctional devices), and storage devices such as NAS servers in the SOHO segment.
- Ensure that remote access services for operating systems are not accessible externally (e.g., RDP, SSH, VNC, SMB/RPC, etc.).
  - If this cannot be avoided, change the SSH/RDP port to a non-default one and implement a white list of IP addresses that can access these services.
- Ensure that remote access meets the following requirements:
  - Multi-factor authentication.
  - Enhanced password policy.
  - The ability to restrict network access for the tasks of a specific account (e.g., contractors are granted access only to servers they need, not the entire segment or network).
  - Set fields such as "expires at" for accounts and access rules in case manual revocation of remote access fails.

Ransomware

— Be prepared to identify signs of initial compromise, methods used to achieve persistence in the system, and lateral movement. Although attack techniques are usually primitive and can be detected with the naked eye, more advanced attacks can be identified only by hunting for threats.
— Regularly check your infrastructure for known bad indicators of compromise.
— The success of ransomware affiliate programs depends on an organization's overall level of security. We recommend using security systems such as Group-IB Threat Hunting Framework and Group-IB Threat Intelligence & Attribution.

Post-exploitation frameworks: a free tool called Metasploit and a cracked version of Cobalt Strike. Less often, the frameworks PoshC2 and Koadic.

— Ensure that your security tools are able to detect tracks of popular post-exploitation frameworks.
— Ensure that a sufficient number of different and unique data sources are used when assessing the security level of your infrastructure and preparing for attacks.

Supply-chain attacks

— Ensure that your current security tools are able to detect anomalous activity when legitimate software is being used. Such activity may include launches of atypical processes, creation of files, and file system or registry modifications that are usually used to achieve persistence in the system.
— Common security tools are usually unable to handle such tasks, therefore we recommend considering Group-IB Threat Hunting Framework.

Privilege escalation using various software (e.g., Mimikatz, LaZagne) or brute-force attacks

To counteract Mimikatz, we recommend:

— Update your systems to Windows 10/2016 with the Credentials Guard feature.
— Use the Protected Users group for administrator accounts.
— Build a privileged access management system in accordance with Microsoft recommendations.
— If you believe that attackers may bypass the methods listed above, or if it is impossible to implement the above recommendations, ensure that the existing security controls are able to detect the use of Mimikatz (most often launched using post-exploitation frameworks).
— Log access to lsass.exe process memory and identify suspicious processes that may perform such activity.

Tools for attacks on physically isolated networks that use USB devices for jumping the air gap

Do not use untrusted USB devices or USB devices of unknown/questionable origin.

BGP hijacking and route leaks

How successfully you repel such attacks largely depends on other Internet users.

— Implement Group-IB Threat Hunting Framework and Threat Intelligence systems to check whether your organization has been compromised

Attacks on card processing and interbank transfer systems

The success of such attacks is highly dependent on your organization's level of security.

— Implement Group-IB Threat Hunting Framework and Group-IB Threat Intelligence & Attribution systems to check whether your organization has been compromised

JS sniffers

— Regularly update CMS and plugins, and control versions of website files.
— Enhance the password policy for administrative accounts on websites.
— Use Group-IB Fraud Hunting Platform to detect web injections.

Attacks on POS terminals

There are no specific recommendations, as the success of such attacks is highly dependent on your organization's level of security.

— Implement Group-IB Threat Hunting Framework and Group-IB Threat Intelligence & Attribution to check your organization for compromise.

Credential stuffing

— Prevent users from registering on any third-party services using corporate emails. Users tend to use the same password on multiple services or modify their passwords. If passwords are leaked from one service, a hacker can attack a given company directly.
— A threat actor can use a breached password to conduct a social engineering attack against a specific user.
— Check databases of leaked credentials for your accounts (e.g., using Group-IB Threat Intelligence & Attribution).

New records in DDoS attack volume: 2.3 Tb per second and 809 million packets per second

— Switch to using an external balancer or proxy service; increase architecture complexity; and move IP addresses to external services to protect your entire infrastructure.
— Increase bandwidth.
— Purchase filtering hardware.
— Switch to operators with relevant anti-DDoS capacities.

Banking botnets, Trojans (TrickBot, Qbot, Silent Night and others)

1. Attack on vulnerable software: browsers, operating systems

— Perform timely software updates
— Do not click on suspicious links
— Do not install software from untrusted sources

2. Phishing campaigns:

— Do not open suspicious emails and attachments.
— Use Group-IB Threat Hunting Framework and similar solutions.

Such Trojans are well known and leave specific traces in the target system. Make sure to install security tools that will detect and repel Trojans in your infrastructure.

Web phishing and social engineering

Recommendations for marketplace customers:

— Pay attention to domain names, especially those shown in search engine ads and conversations with sellers.
— Do not switch to communicating outside marketplaces, since chat histories will not be saved, and the resource's anti-fraud rules will not work.
— Pay attention to the seller rating.

Recommendations for marketplaces:

— Create a fraud prevention system.
— Use Group-IB Fraud Hunting Platform.

Recommendations for other websites, online stores, and their visitors:

— Check the date when the domain name was registered and whether the domain is spelled correctly.
— Check the website content, including product descriptions and user reviews.
— Be attentive to websites that appear on the top of advertising in search engines. Cybercriminals often buy such ads to promote their websites.
— Be attentive to websites where the price of products is set too low.
— Implement Group-IB Fraud Hunting Platform and Group-IB Digital Risk Protection.

Growing demand for Linux malware designed to achieve persistence in the network and escalate privileges

— Install packages only using official repositories
— Carefully check information about developers of packages that are not available in official repositories.
— Follow general cybersecurity recommendations of the Linux communities (e.g., remove SUID bits off unnecessary binaries).
— Use minimum privileges when using untrusted software.

Mobile RATs

— Do not install untrusted software
— Do not listen to intruders trying to persuade you to install TeamViewer and any other software to connect a tech support employee.
— Update software and operating systems in a timely manner.

For our clients: use Group-IB Fraud Hunting Platform, which is able to detect active RATs on mobile devices.

Gaining access to SCADA systems at industrial enterprises to manipulate production processes

- The success of such attacks is highly dependent on your organization's level of security.
- Implement Group-IB's Threat Hunting Framework and Group-IB Threat Intelligence & Attribution systems to check whether your organization has been compromised

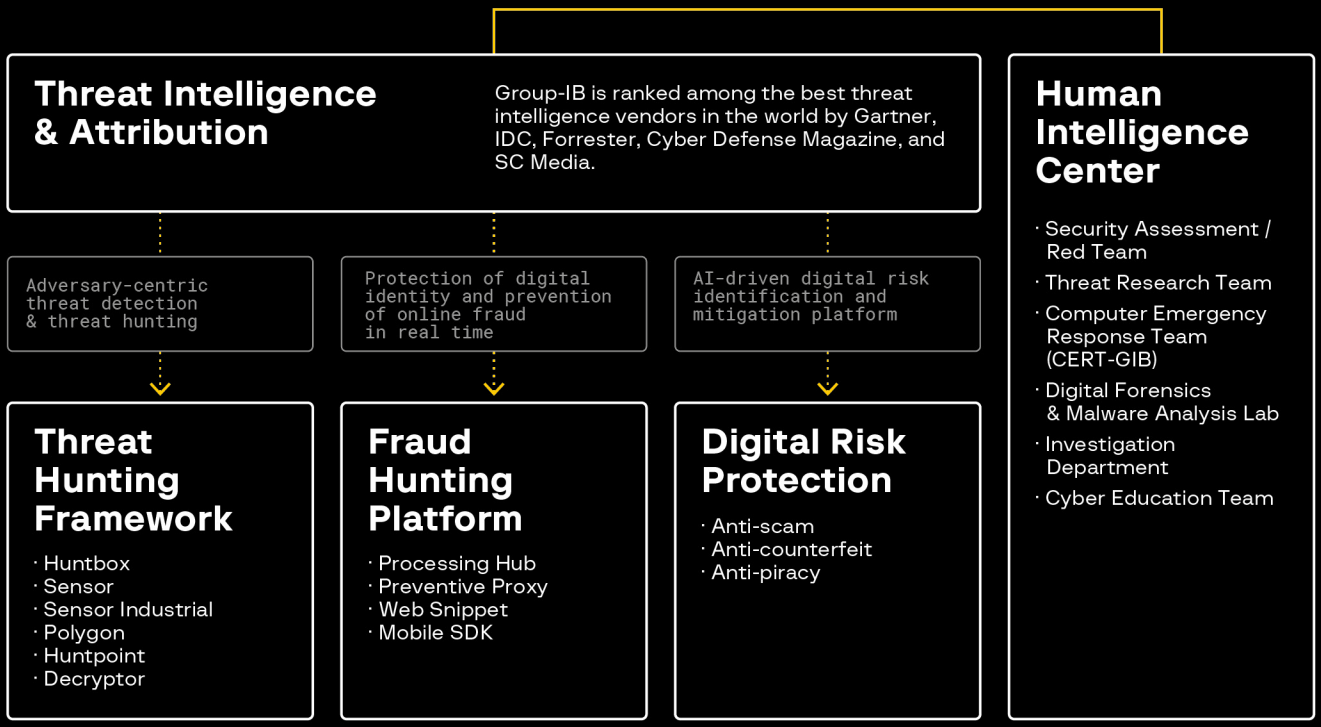
Exploits and spyware suits for Android and iOS

- Do not visit untrusted/suspicious websites.
- Do not install software from unverified sources.
- Perform timely updates of operating systems and software
- Separate personal and work devices.
- Use one device for work, the other for personal life, do not mix them.
- Use Group-IB Fraud Hunting Platform and Group-IB Threat Intelligence & Attribution (with notifications on new attacks, new software, and exploits).

Initial compromise through VPN servers

- Ensure that remote access meets the following requirements:
  - Multi-factor authentication
  - Enhanced password policy
  - The ability to restrict network access for the tasks of a specific account (e.g., contractors are granted access only to servers they need, not the entire segment or network)
  - Set fields such as "expires at" for accounts and access rules in case manual revocation of remote access fails.

ABOUT GROUP-IB



17 years	65,000+	1,200+	500+
of hands–on experience	hours of incident response	cybercrime investigations worldwide	world–class cybersecurity experts

Group–IB is ranked among the best threat intelligence vendors in the world by Gartner, IDC, Forrester, Cyber Defense Magazine and SC Media.

We have provided professional development training to Europol, INTERPOL, law enforcement agencies and corporate security teams on four continents.

INTERPOL EUROPOL

Official partners

Experiencing a breach?

Call us at +65 3159-4398
Email us at response@cert-gib.com
Fill out our incident response form

Group-IB experts will conduct incident response, investigate incidents, and collect evidence for subsequent submission to law enforcement agencies.

PREVENTING AND INVESTIGATING CYBERCRIME SINCE 2003

www.group-ib.com
group-ib.com/blog/
info@group-ib.com
twitter.com/groupib_gib
facebook.com/groupibHQ
linkedin.com/company/group-ib