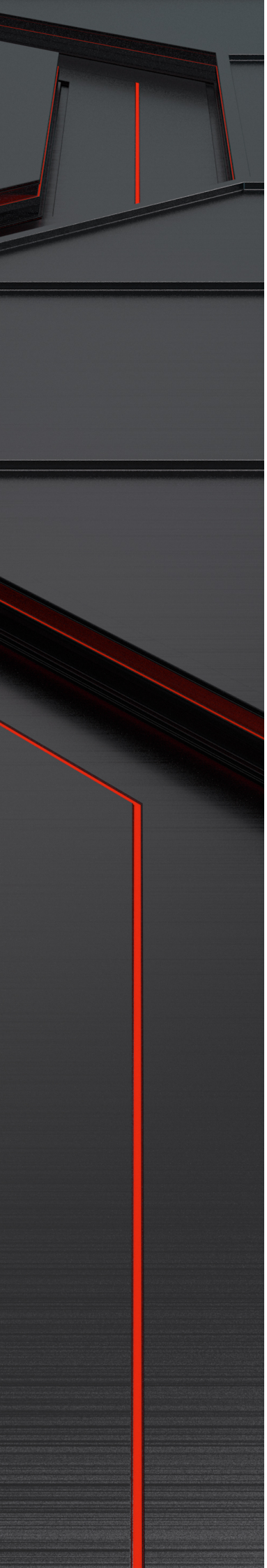
Cybersecurity threatscape

Q1 2020

ptsecurity.com

Contents



Executive summary

Highlights of Q1 2020 include:

- The number of cyberincidents is growing rapidly. In Q1 2020, we detected 22.5 percent more attacks than in Q4 2019.
- The share of targeted attacks remains unchanged from Q4 2019 (67%).
- In Q1 2020, there were 23 very active APT groups. Their attacks targeted mostly government agencies, industry, finance, and medical institutions.
- About 13 percent of all phishing emails of Q1 2020 were related to COVID-19. Of those, about a half (44%) targeted individuals. One out of every five mailings was sent to government agencies.
- More than a third (34%) of all attacks on organizations using malware were attacks with ransomware. Sodinokibi, Maze, and DoppelPaymer were the most active ones. Operators of these and some other ransomware created their own websites where they publish stolen data if the victims refuse to pay the ransom.
- The share of attacks against individuals was 14 percent. Logins and passwords make up half of the data stolen. This is because malware campaigns against individuals contained a large percentage of spyware (56%).

We expect that the number of attacks against remote workstations will be growing globally. Because people are working from home now, companies may soon see an increased number of attempts to hack corporate credentials or exploit vulnerabilities in remote access systems. These threats are especially relevant for companies that have no strict password policy and no regular software updates.

Web application firewalls (WAFs) can block potential attacks against web applications on the network perimeter, including attacks against remote access systems, such as Citrix Gateway. To prevent infection of computers of the employees with malware, we recommend checking email attachments for malicious activity with sandboxes. We also recommend following the general recommendations for ensuring personal and corporate cybersecurity.

Statistics

In Q1 2020, we registered 22.5 percent more attacks than in Q4 2019. The beginning of the year was tough on the whole world. The COVID-19 pandemic messed up the global economy and the life of all ordinary people. The situation impacted the information security, too.

22.5% more cyberattacks than in Q4 2019

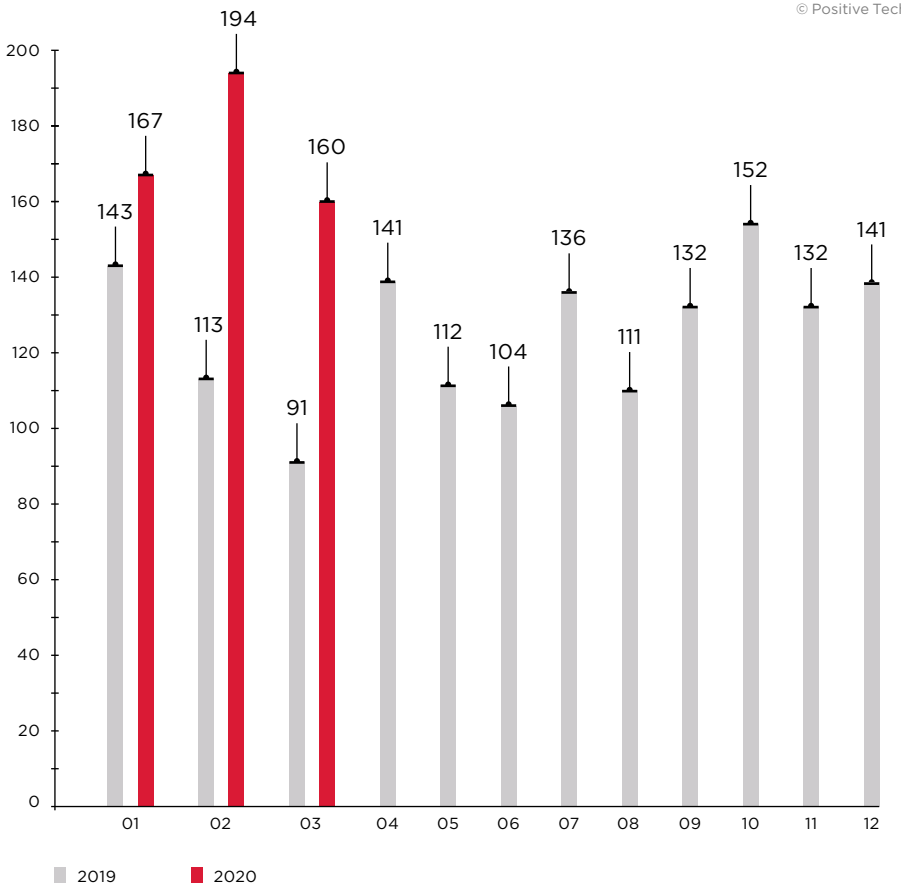


Figure 1. Number of attacks per month in 2019 and 2020 (1 = January, 12 = December)

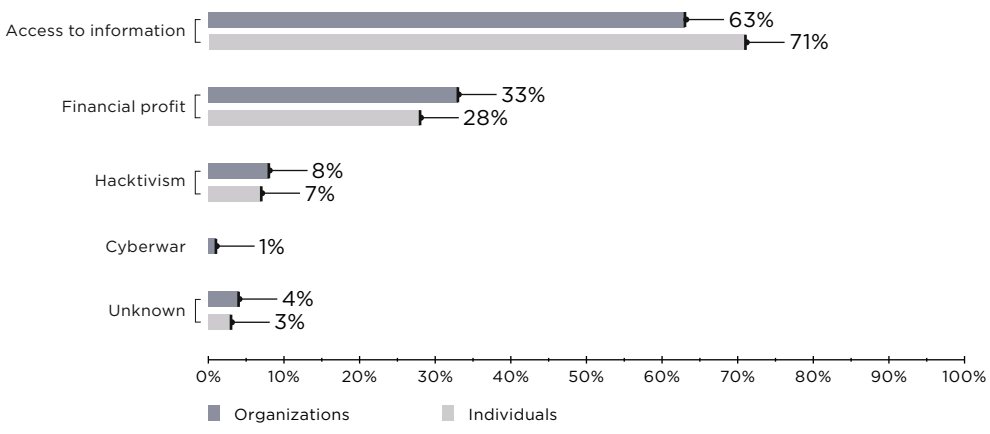


Figure 2. Attackers' motives (percentage of attacks)

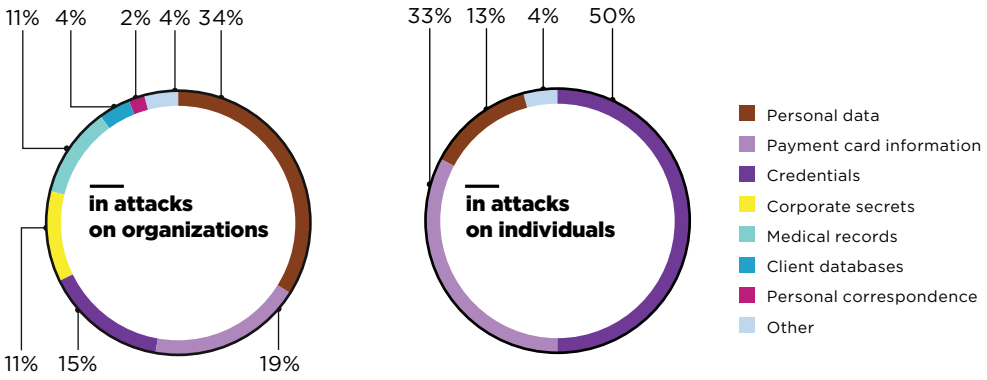


Figure 3. Types of data stolen

67% of attacks are targeted

14% of attacks target individuals

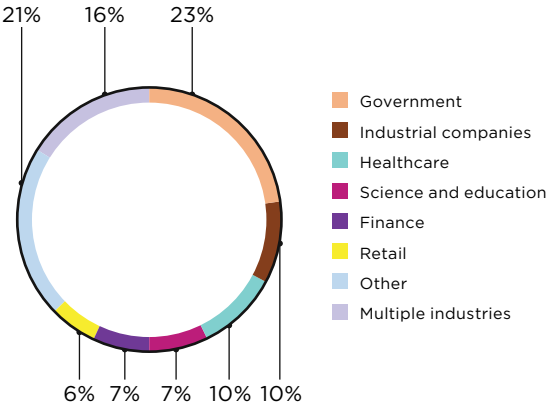


Figure 4. Victim categories among organizations

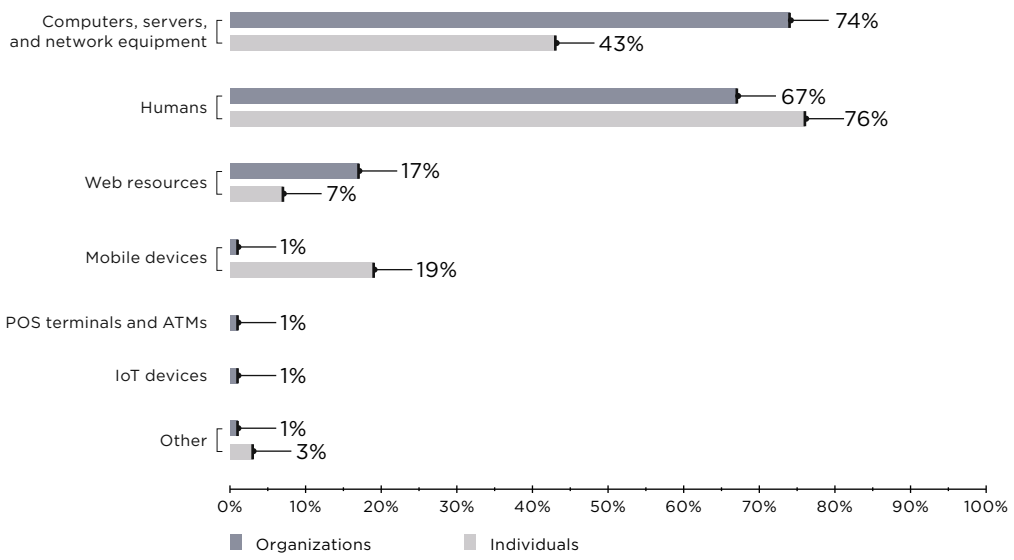


Figure 5. Attack targets (percentage of attacks)

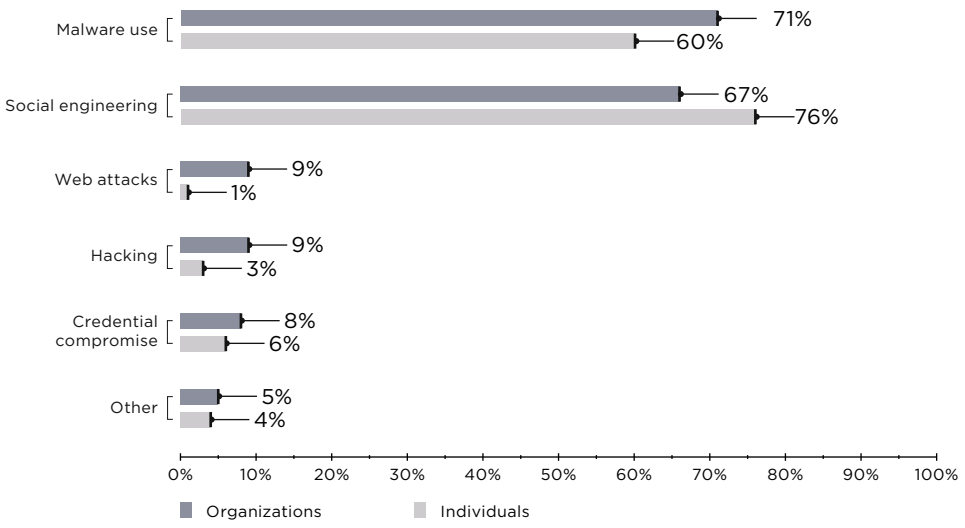


Figure 6. Attack methods (percentage of attacks)

Victim categories

	Per-industry classification of cyberincidents by motive, method, target, and victim categories	Government	Finance	Industrial companies	Healthcare	Science and education	Retail	Other	Multiple industries	Individuals
	Total	**103**	**30**	**47**	**45**	**32**	**29**	**92**	**71**	**72**
Target	Computers, servers, and network equipment	87	26	42	31	23	9	60	54	31
	Web resources	12	3	3	3	5	18	20	11	5
	Humans	80	23	40	35	27	9	45	42	55
	Mobile devices							1	2	14
	POS terminals and ATMs		1				1	1		
	IoT devices			1					3	
	Other							3		2
Method	Malware use	83	25	43	27	23	9	56	51	43
	Social engineering	81	23	41	35	27	9	46	42	55
	Credential compromise	2	1		5	3	3	17	5	4
	Hacking	6	4	3	3	1		10	14	2
	Web attacks	6	2	2		3	15	6	6	1
	Other	7	1		3		1	10	1	3
Motive	Access to information	67	19	36	32	8	28	56	39	51
	Financial profit	25	10	15	18	21	3	37	19	20
	Hacktivism	10	2		1	3		11	8	5
	Cyberwar	1		1				2	1	
	Unknown	2	1		1	2			10	2

Darker colors indicate a greater proportion of attacks within a particular category of victims

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

Hiding from the antivirus: attacks with malware

Over time, malware infection risks keep increasing. Cybercriminals don't stop at using a single type of malware. They use multifunctional trojans or inject compromised devices with a whole bunch of assorted malware. Hackers keep looking for ways to bypass antiviruses and security tools embedded in the OS. For instance, since early 2020 we keep seeing attempts to use the new vulnerability CVE-2020-0601 in Windows CryptoAPI for signing malware. This vulnerability allows bypassing certificate checks. Another example is SysUpdate remote access trojan. This is a unique tool developed by BronzeUnion APT group. The hackers use it to deliver payload to the devices under their control. Usually this payload is not detected by antiviruses, because the file has an indefinite format and the antivirus can't recognize it. Another example is FakeChmMsi, a malware with a complex chain for delivering the Gh0st trojan. Along the chain, DLL hijacking is used twice, complicating analysis of the malware by any antivirus. Modern malware can bypass antiviruses, firewalls, IPS, mail and web gateways, but it can be efficiently countered with sandboxes. Those are solutions allowing one to launch a file in an isolated virtual environment and analyze it for malicious activity.

The greatest number of malware attacks on corporate infrastructure came from ransomware. Individuals were mostly attacked with infostealers, keyloggers, and banking trojans.

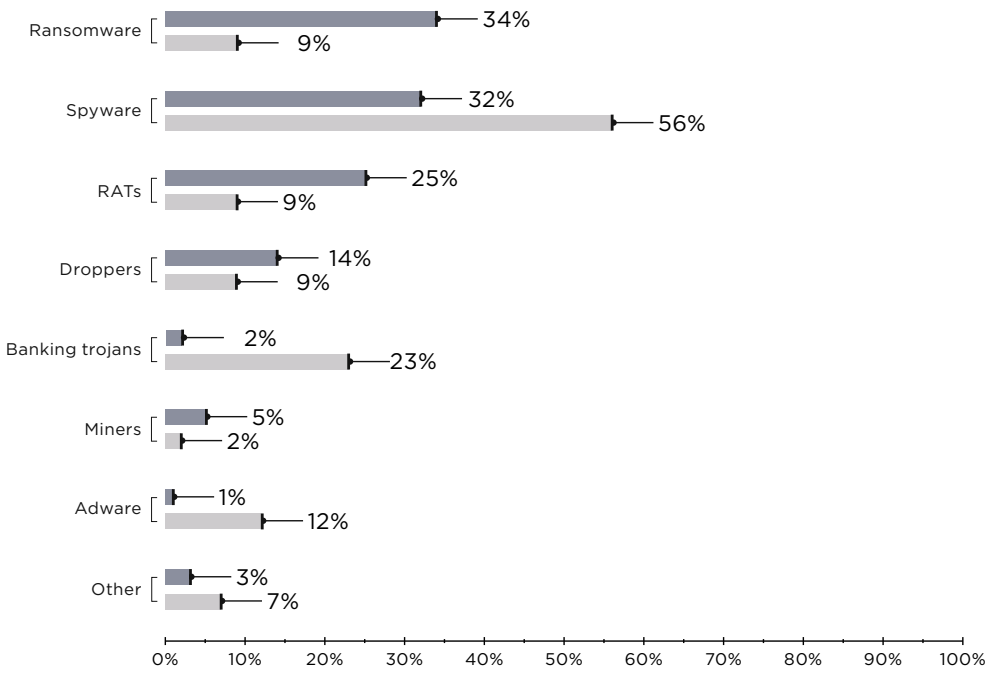


Figure 7. Types of malware (percentage of attacks using malware)

Same as before, eight out of ten malware campaigns against organizations started with emails with attachments. Individuals risk getting their computers infected not only via emails, but also by visiting sites and downloading software from untrusted resources. For instance, in Q1 the hackers have compromised a number of WordPress sites and redirected the visitors to phishing sites spreading a backdoor disguised as a Chrome browser update. The malware was downloaded over 2,000 times.

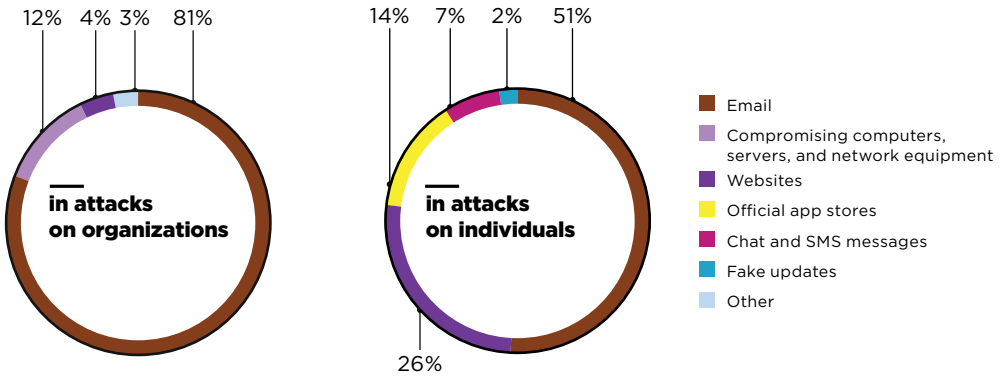


Figure 8. Malware distribution methods

Phishing emails about COVID-19

The hackers were quick to use the common concern about the new coronavirus for their phishing emails. According to our estimates, in Q1 2020 about 13 percent of social engineering attacks were related to the coronavirus.

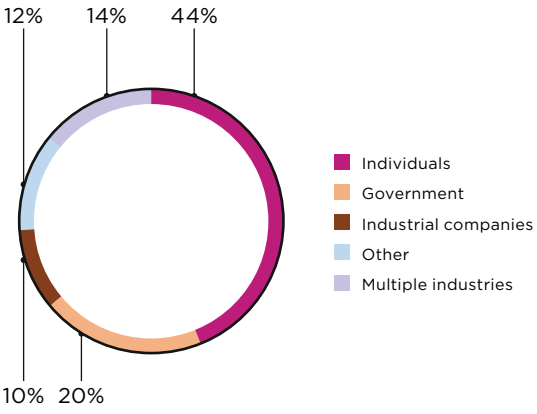


Figure 9. Categories of victims of phishing emails about COVID-19

Starting from the second half of January, we see an increase in the number of phishing emails related to COVID-19. The pandemic situation was used both for mass malware campaigns and for APT attacks. In Q1, Emotet, Remcos, AZORult, Agent Tesla, LokiBot, TrickBot, and many other trojans were distributed in the guise of official information about infection statistics, a vaccine, and prevention measures, allegedly coming from the authorities and medical institutions.

In February, Positive Technologies Expert Security Center (PT ESC) detected an attack from TA428 group. As a decoy, the group sent out a document with coronavirus infection statistics. By the way, in January that group used the deteriorating relations between U.S. and Iran as the topic for their emails. Malicious documents delivered a loader with encrypted Poison IVY shell code to the victim's computer.

COVID-19
Daily update (FOR INTERNAL USE ONLY)
Ministry of Health Mongolia
Date: 17 February 2020, 01.00 pm (Ulaanbaatar time)

GLOBAL SITUATION(Table 1)

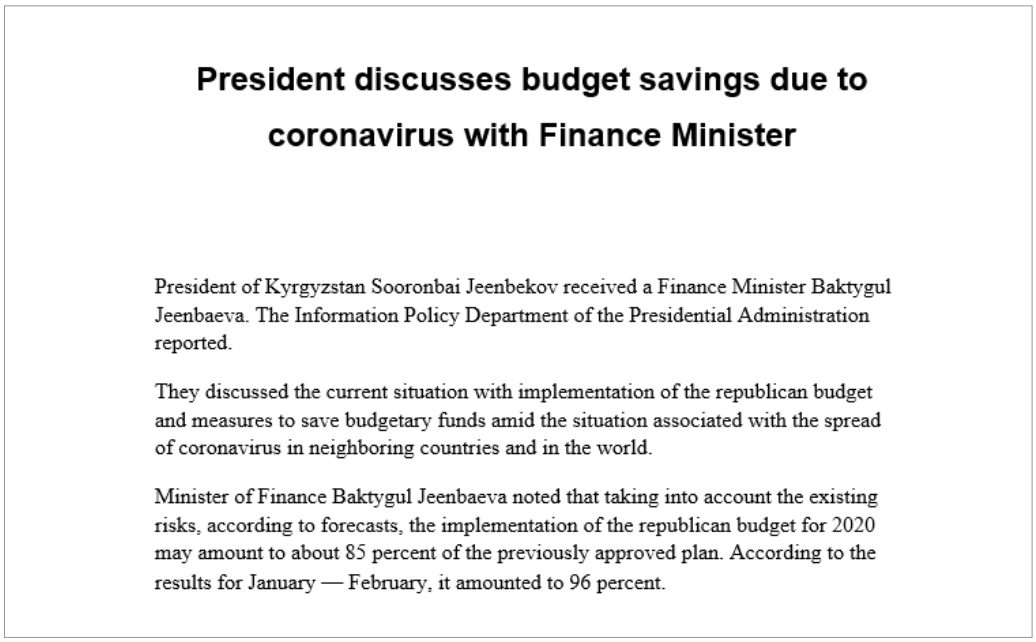
	WHO*		MOH, PRC**		MoH, Mongolia	
	total	new cases in the last 24 hours	total	new cases in the last 24 hours	Total	new cases in the last 24 hours
Number of confirmed cases	51857	1278	70586†	2002	-	-
Number of deaths	1666	142	1770	104††	-	-
Number of suspected cases	NA	NA	8228	-1918	137	1
Number of severe cases	NA	NA	11272	219	-	-
Number of recovered cases	NA	NA	10773	1348	-	-

†Clinically confirmed cases in addition to the lab confirmed cases
§Lab confirmed cases

A total of 683 (157 cases in the last 24 hours) confirmed cases have been reported in 25 countries outside China. Thirddeath outside China is reported in France. 355confirmed cases reported in Diamond Princess Ship docked in Yokohama, Japan.

Figure 10. Document with COVID-19 statistics from TA428 emails

In March, PT ESC registered four sets of phishing emails the hackers used to distribute the Chinoxy backdoor. In one of the documents, the attackers used a text related to saving the budget during the coronavirus pandemic.



President discusses budget savings due to coronavirus with Finance Minister

President of Kyrgyzstan Sooronbai Jeenbekov received a Finance Minister Baktygul Jeenbaeva. The Information Policy Department of the Presidential Administration reported.

They discussed the current situation with implementation of the republican budget and measures to save budgetary funds amid the situation associated with the spread of coronavirus in neighboring countries and in the world.

Minister of Finance Baktygul Jeenbaeva noted that taking into account the existing risks, according to forecasts, the implementation of the republican budget for 2020 may amount to about 85 percent of the previously approved plan. According to the results for January — February, it amounted to 96 percent.

Figure 11. The document from the Chinoxy email

Groups like TA505, Hades, Mustang Panda, APT36, Higaisa, and SongXY also sent out emails with malicious attachments related to the pandemic. We will discuss the last two in more detail in the section about attacks on government agencies.

The virus intervenes

Due to the pandemic, many countries sent schoolchildren and students to study from home, and employers were instructed to send their personnel to work from home, if they could. In this situation, many companies have to use VPN to arrange remote access to their corporate network for their employees. As you know, lately the attackers have been actively exploiting vulnerabilities in VPN solutions and remote access systems, such as products by Pulse Secure, Fortinet, Palo Alto, and Citrix. We recommend immediately installing the latest updates released by those manufacturers. Otherwise, the risk of compromise is quite high. For instance, the British company called Finastra fell victim to ransomware in March because they used unpatched versions of Citrix ADC and VPN by Pulse Secure.

Dangerous vulnerabilities in VPN solutions and remote access systems

CVE-2019-19781 **Citrix**
CVE-2019-11510 **Pulse Secure**
CVE-2019-11539 **Pulse Secure**
CVE-2018-13379 **Fortinet**
CVE-2018-13382 **Fortinet**
CVE-2018-13383 **Fortinet**
CVE-2018-1579 **Palo Alto Networks**

Attackers set on exploitation

- Operators of Sodinokibi ransomware
- APT5
- APT33
- APT34
- APT39
- APT41

Because of the large number of people shifting to home office, there are now more hosts accessible for RDP connection. We expect that companies all over the world will see an increase in attacks on RDP starting in Q2 2020. For instance, the famous banking trojan TrickBot already got a new module called rdpScanDll which bruteforces credentials for RDP connection.

When more people started using Zoom videoconferencing, the hackers started paying closer attention to it, too. Over 1,700 phishing domains related to the name of the popular platform were registered in Q1 2020. Active use of Zoom app revealed a number of vulnerabilities. Specialists from Check Point discovered that the platform had a vulnerability allowing the attackers to join someone's video conference without an invite. Unsanctioned breach of Zoom online conferences was dubbed Zoom-bombing. According to the FBI, a lot of such incidents occur in the US. Recordings of thousands of video calls ended up on YouTube and Vimeo. Private calls, recordings of business meetings, doctors' sessions, and classes were made public. In addition, at the end of Q1 news came about a UNC path injection vulnerability allowing the hackers to steal Windows credentials via Zoom.

With quarantine and self-imposed isolation, there is an increased demand for takeout food and food products delivery services. The hackers used this to stage a DDoS attack against takeaway.com, demanding 2 bitcoins for stopping it. Attackers also interfered with the work of medical institutions. We will discuss these attacks later, in the Industry Specific section.

Citrix vulnerability put to use

In Q1 2020, 12 percent of malware was delivered to the companies by compromising network equipment, servers, or workstations. One of the vulnerabilities currently used to deliver malware is a vulnerability in some Citrix products (CVE-2019-19781). The vulnerability became widely known back in the end of 2019. It is a critical vulnerability allowing an unauthorized attacker to run arbitrary code. The vulnerability affected about 80,000 organizations worldwide, with most of the victims in the state sector. The manufacturer released final patches on January 24, 2020.

In Q1 2020, the APT41 group used this vulnerability in targeted attacks against government agencies, finance, telecom, industry, healthcare, and the media. In addition, vulnerability CVE-2019-19781 was presumably exploited during attacks against the infrastructure of Potsdam and the Defence Signals Directorate in Australia.

In January, specialists from FireEye found that unknown perpetrators install a backdoor named NOTROBIN on vulnerable Citrix devices. Curiously, NOTROBIN can detect and block attempted exploitation of CVE-2019-19781 by other attackers, making sure its owners are the only ones in control of the compromised device.

Ransomware with a new blackmail strategy

In Q1 2020, there was an increase in ransomware attacks where the hackers demanded ransom for not disclosing the stolen data. The hackers now create their own sites where they publish the stolen data. Operators of Maze, Sodinokibi, Nemty, DoppelPaymer, Nefilim, CLOP, and Sekhmet already have their sites.

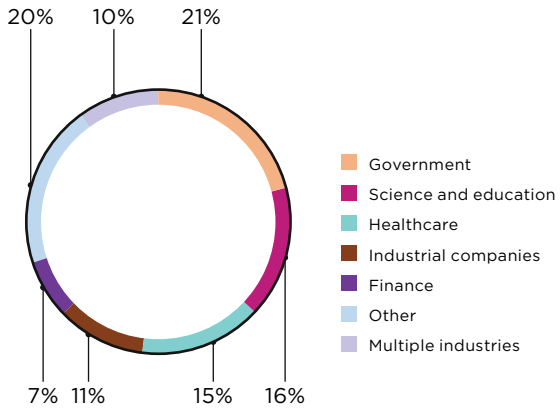


Figure 12. Ransomware victim categories among organizations

Operators of Sodinokibi are looking for new leverage over the compromised organizations. The hackers plan to notify the stock exchange about attacks on large companies if the latter refuse to pay the ransom. The attackers believe that the possibility of the victim's stock prices going down might be an additional reason to pay the ransom.

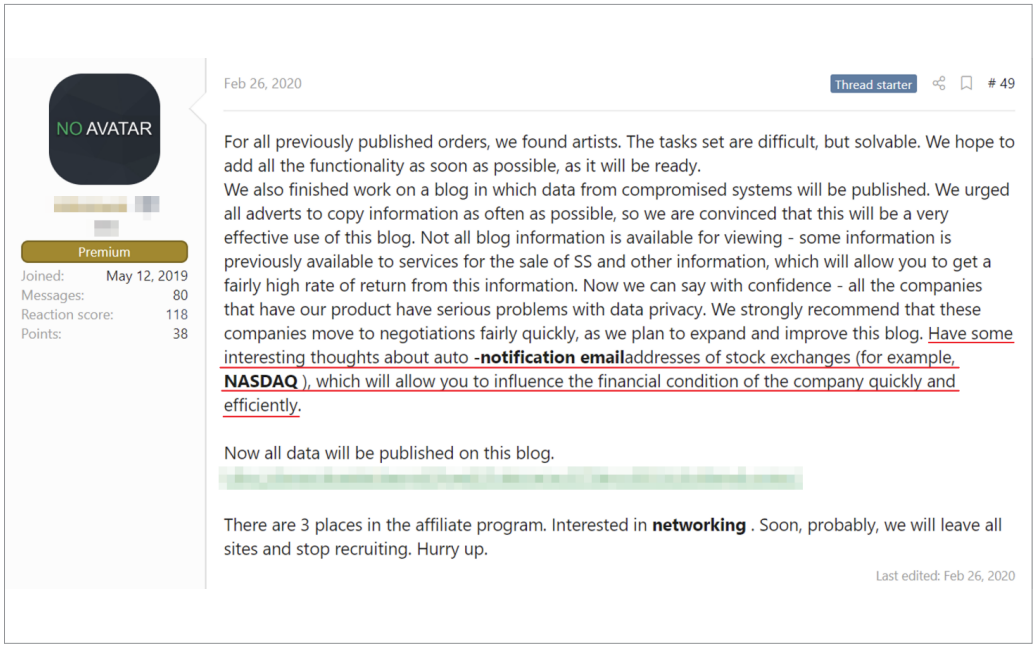


Figure 13. Sodinokibi notifying of their plans

Industry specific

In this section, attacks on industries of special interest in Q1 2020 will be considered in greater detail.

Government

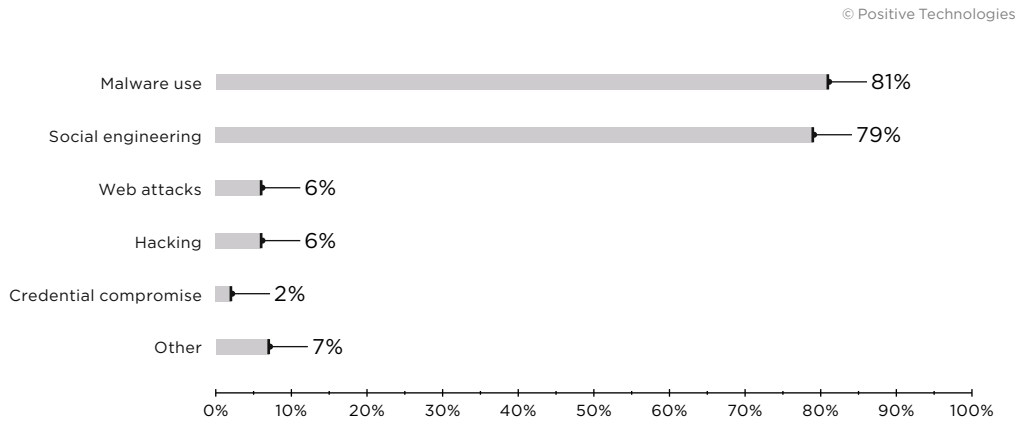


Figure 14. Attack methods (percentage of attacks on government agencies)

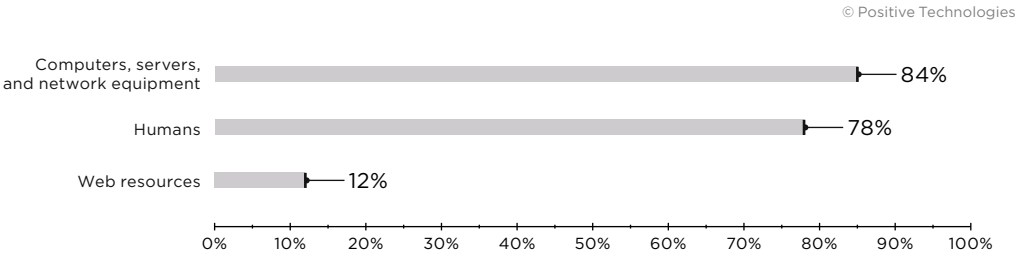
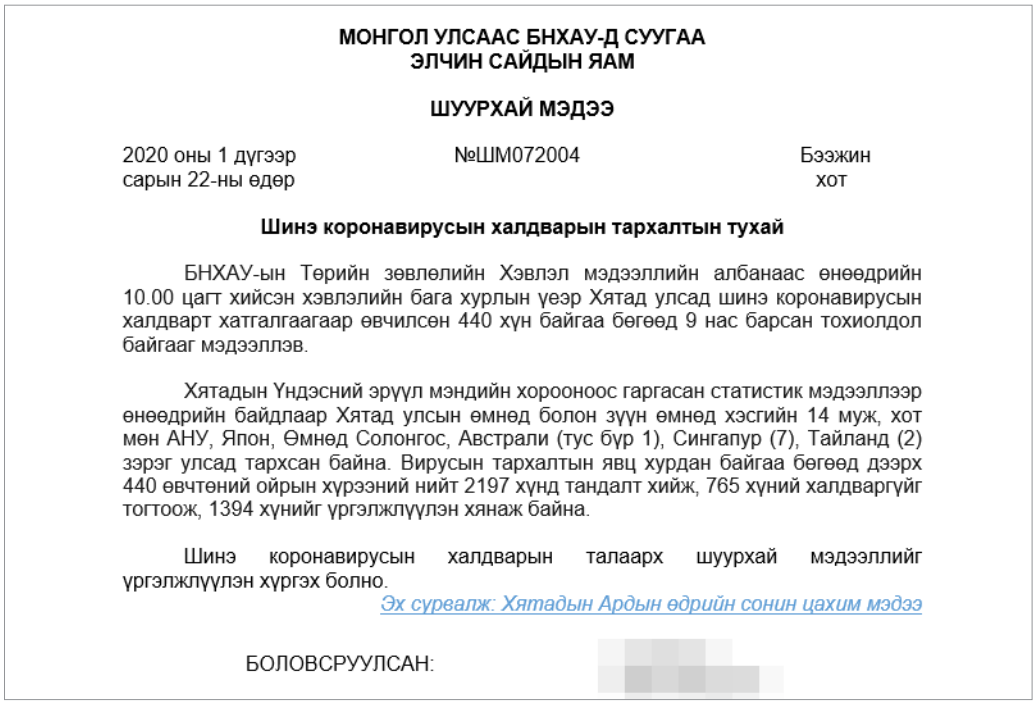


Figure 15. Attack targets (percentage of attacks on government agencies)

The percentage of malware and social engineering attacks against government agencies has increased significantly compared to Q4 2019. The pandemic may have been a factor. Many attackers sent emails to government agencies of various countries, with a malicious attachment related to the coronavirus infection. In January 2020, PT ESC registered two attacks by SongXY APT group. The attackers used a text in Mongolian, which very likely indicates that they target a specific region. The text contained information about COVID-19 outbreak in China. The RTF document with exploit for vulnerability CVE-2018-0798 saved an encrypted loader to the victim's hard drive, decrypted it, launched it, and then loaded the main payload.



МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр | №ШМ072004 | Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээний нийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

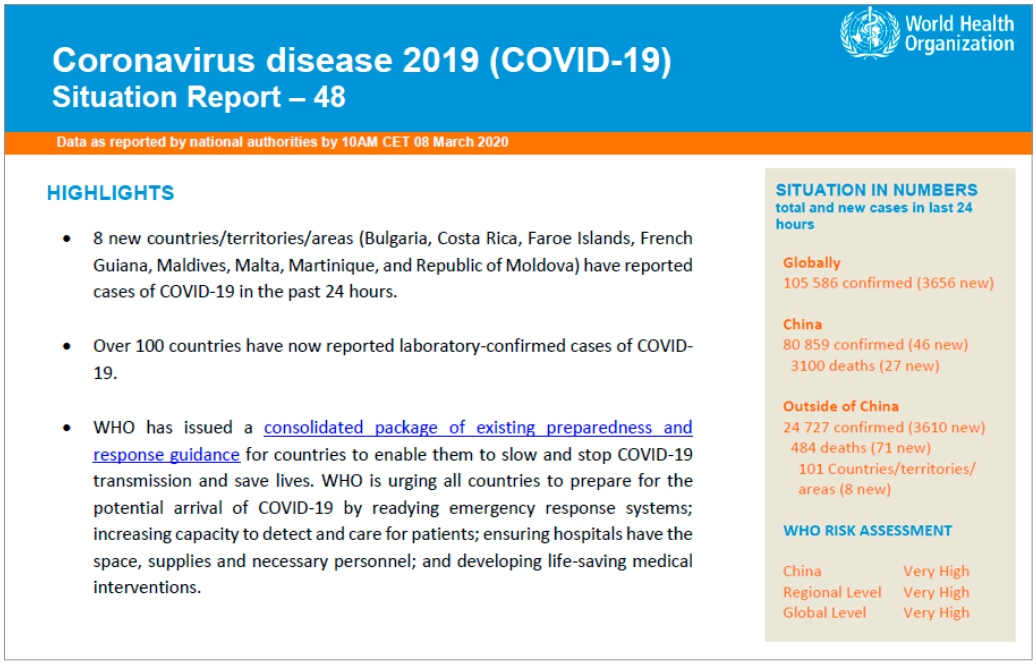
Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН:

Figure 16. The decoy text in RTF format about COVID-19 from the SongXY email

In Q1 2020, PT ESC detected two attacks by the Higaisa group. That group attacks government agencies, diplomatic missions, and organizations promoting human rights in China, North Korea, Japan, Nepal, Singapore, Russia, and other countries. Both campaigns started with phishing emails. The first one used a text about national holidays and current news in North Korea. In the second case, the group disguised the malicious LNK file as a PDF document about COVID-19.



World Health Organization

Coronavirus disease 2019 (COVID-19)
Situation Report – 48

Data as reported by national authorities by 10AM CET 08 March 2020

HIGHLIGHTS

- 8 new countries/territories/areas (Bulgaria, Costa Rica, Faroe Islands, French Guiana, Maldives, Malta, Martinique, and Republic of Moldova) have reported cases of COVID-19 in the past 24 hours.
- Over 100 countries have now reported laboratory-confirmed cases of COVID-19.
- WHO has issued a consolidated package of existing preparedness and response guidance for countries to enable them to slow and stop COVID-19 transmission and save lives. WHO is urging all countries to prepare for the potential arrival of COVID-19 by readying emergency response systems; increasing capacity to detect and care for patients; ensuring hospitals have the space, supplies and necessary personnel; and developing life-saving medical interventions.

SITUATION IN NUMBERS
total and new cases in last 24 hours

Globally
105 586 confirmed (3656 new)

China
80 859 confirmed (46 new)
3100 deaths (27 new)

Outside of China
24 727 confirmed (3610 new)
484 deaths (71 new)
101 Countries/territories/areas (8 new)

WHO RISK ASSESSMENT

China	Very High
Regional Level	Very High
Global Level	Very High

Figure 17. Document from the email of Higaisa APT group

PT ESC also detected 14 attacks of Gamaredon group, targeting government agencies of Ukraine and Georgia. As usual, the group used template injection, a technique we discussed at the end of last year. This technique allows the hackers to deliver the malicious macro codes, which executes a VBScript (VBS). Starting mid-February, the group uses obfuscation to protect VBS from detection. The method of gaining a foothold on the infrastructure changed, too. The VBS now creates the RUN key in the Windows registry, ensuring it keeps functioning after reboot.

Figure 18. Document from the phishing email by Gamaredon group

Industrial companies

Malware infection is still a valid threat for the industry. The greatest threats are spyware and ransomware. They made 42 percent and 28 percent of all malware attacks on industry, respectively. In Q1 2020, we saw attacks on industry with Maze, Sodinokibi, Ryuk, and DoppelPaymer ransomware.

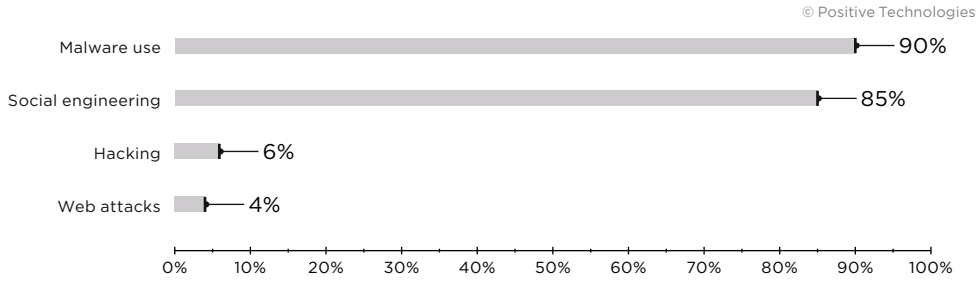


Figure 19. Attack methods (percentage of attacks on industry)

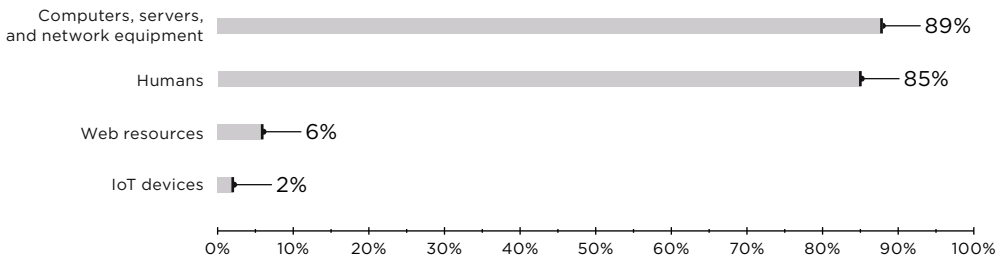


Figure 20. Attack targets (percentage of attacks on industry)

At the beginning of the year, many cybersecurity experts turned their attention to the new ransomware called Snake, capable of deleting shadow copies and stopping processes related to ICS operation. For instance, Snake can stop the processes of GE Proficy and GE Fanuc Licensing, Honeywell HMIWeb, FLEXNet Licensing Service, Sentinel HASP License Manager, and ThingWorx Industrial Connectivity Suite. The attackers presumably want to use Snake in targeted attacks against industry. The ransomware leaves a file on the compromises computer, instructing the victim what to do next, with bapcocrypt@ctemplar[.]com set as contact email. PT ESC theorized this may be a reference to the attack on Bapco company. At the end of 2019, it was attacked with Dustman malware designed to delete data. It is possible that Dustman and Snake are related, because the samples of the two became available to the public at about the same time, and both targeted industry.

Just like government agencies, industry is targeted by many APT groups worldwide. For instance, one of the APT attacks by Bisonal group in Q1 2020 targeted Russian aerospace organizations. PT ESC determined that in that particular attack, the remote control malware (RAT) was delivered by emails with malicious RTF documents as attachments. The group created those documents using the Royal Road exploit builder.

Aerospace & Defense Supplier Summit Seattle 2020 - международный саммит авиационно-космической промышленности

с 6 по 8 апреля

США, Сиэтл
Организатор: BCI Aerospace

О конференции Aerospace & Defense Supplier Summit Seattle 2020

Конференция Aerospace & Defense Supplier Summit Seattle 2020 проходит с 6 по 8 апреля в городе Сиэтл, США. Посмотреть, как проехать в место проведения конференции можно на сайте конгрессной площадки. Деловая программа Aerospace & Defense Supplier Summit Seattle 2020 может включать несколько потоков или секций и размещается на сайте мероприятия с подробным списком докладчиков. Спикеров конференции Aerospace & Defense Supplier Summit Seattle 2020 обычно окончательно утверждают за 1-2 месяца до начала конференции.

Figure 21. The document from the Bisonal email

In Russia and the CIS countries, the industry is still attacked by RTM group. PT ESC detected 29 malicious mailings by the group during the first quarter.

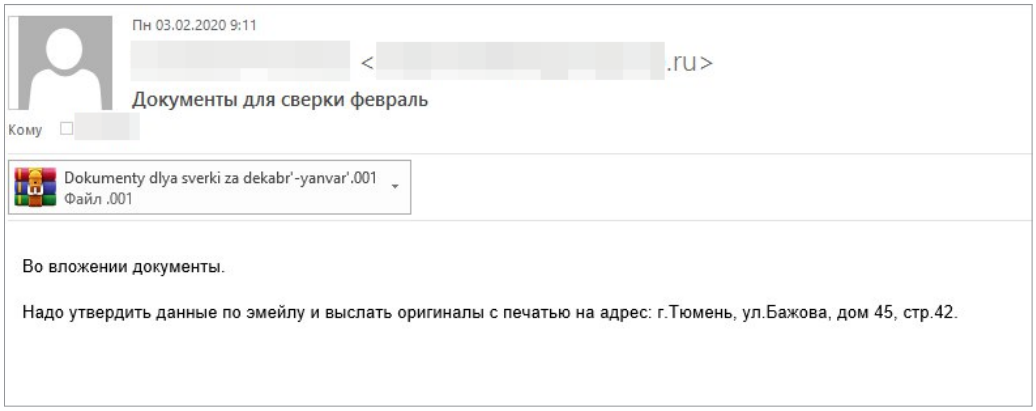


Figure 22. A message with malicious attachment sent by RTM to an industrial company

Healthcare

The number of attacks on healthcare has increased significantly compared to Q4 2019. This is because the cybercriminals took an increased interest in healthcare facilities currently on the front lines of coping with the coronavirus pandemic. With stress and heavy workload on the medical staff, we see more successful attacks, because the healthcare workers may not be so careful about the stream of emails they receive now.

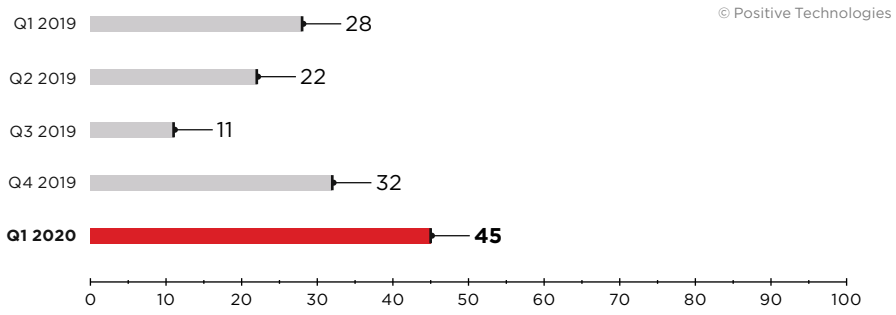


Figure 23. Number of attacks against healthcare

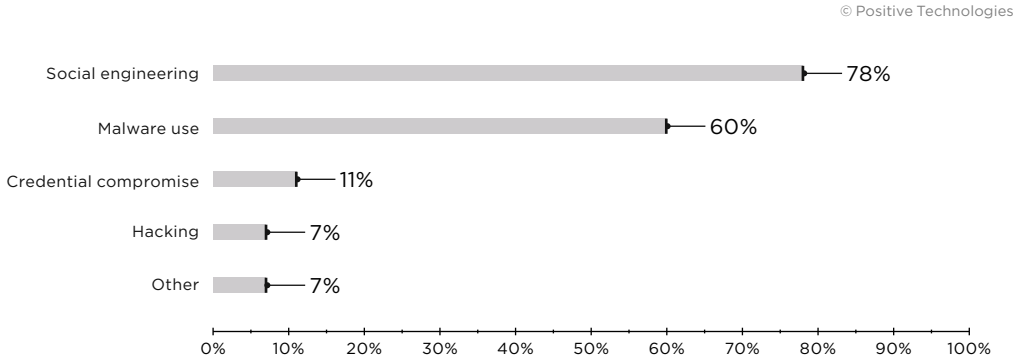


Figure 24. Attack methods (percentage of attacks on healthcare)

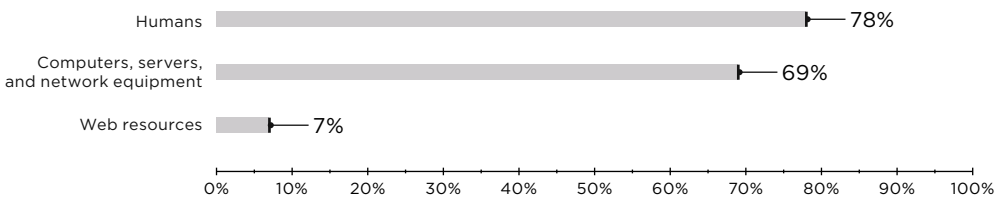


Figure 25. Attack targets (percentage of attacks on healthcare)

In 78 percent of attacks on healthcare, the hackers used social engineering. Attackers would send phishing emails to convince the staff to enter corporate credentials in a fake authentication form.

Malware infection threat is just as real. In the early hours of March 13, a cyberattack by unknown perpetrators crashed the network of a large medical center in Brno (Czech Republic) testing people for coronavirus infection. A day later, Hammersmith Medicines Research, a British company preparing to test a coronavirus vaccine, was attacked by Maze ransomware. Remember that the hackers behind the Maze attacks were among the first to demand a ransom for not disclosing the data stolen before encryption. That time, the victim refused to pay and restored their system quickly. A few days later, Maze operators promised to stop attacking healthcare institutions during the pandemic. However, after that promise was made, they published the data stolen from Hammersmith Medicines Research. This proves yet again that one can never trust cybercriminals. Their promises do not guarantee that the stolen data will be recovered and that it will not end up on the Net.

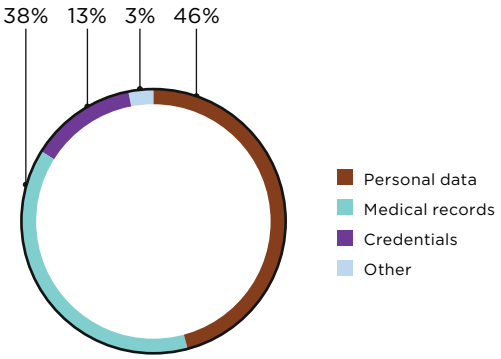


Figure 26. Data stolen

About the research

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

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

In this report, every mass attack (where the attackers send out a phishing email to many addresses, for instance) was considered as one incident. Terms used in this report:

A **cyberthreat** is a combination of factors and circumstances that create the risk of information security compromise. We look at cyberthreats in terms of the actions of malefactors in cyberspace who attempt to breach an information system in order to steal money or data, or with other intentions potentially causing harm to government, business, or individuals. Attacker actions may be directed against the target company's IT infrastructure, workstations, mobile devices, other equipment, or at people as a factor in cyberspace.

A **cyberattack** consists of unauthorized actions targeting information systems and their users by cybercriminals leveraging techniques and software to obtain access to information, impair the normal functioning or availability of systems, or to steal, alter, or delete information.

A **mass attack** is a cyberattack against a wide range of companies or individuals. In a mass attack, attackers may not restrict themselves to a single industry, or may even ignore the industries of their targets entirely—their objective is to compromise as many victims as they can.

A **targeted attack** is a cyberattack targeting a specific company, a certain industry, or a limited number of individuals. A targeted attack usually involves reconnaissance to gather information about the target.

An **APT attack** (advanced persistent threat attack) is a well-organized and well-planned multistage targeted attack. APT attacks are performed by criminal groups (APT groups) consisting of highly skilled people. Because of this, APT groups have significant financial resources and technical capabilities.

An **attack target** is the target of unauthorized actions by cybercriminals. For instance, this could be web resources, computers, servers, network equipment, mobile devices, or the IoT. People can be an attack target too, if the attackers use social engineering.

Attack methods are the set of techniques used by attackers to achieve their goal.

Hacking means exploitation of vulnerabilities and security flaws to gain access to resources or information. For greater granularity, some hacking methods have been placed in separate categories. For instance, bruteforcing credentials to accessible services is considered separately from exploitation of vulnerabilities in web applications.

About Positive Technologies

For 18 years, Positive Technologies has been creating innovative solutions for information security. We develop products and services to detect, verify, and neutralize the real-world business risks associated with corporate IT infrastructure. Our technologies are backed by years of research experience and the expertise of world-class cybersecurity experts.

Over 2,000 companies in 30 countries trust us to keep them safe.

Follow us on social media (LinkedIn, Twitter) and the News section at ptsecurity.com.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Cybersecurity_threatscape-2020-Q1_A4.ENG.0004.01.