Cybersecurity threatscape

Q1 2021

ptsecurity.com

Contents

Summary

Highlights of Q1 2021 include:

- The number of attacks increased by 17% compared to Q1 2020, and compared to Q4 2020, the increase was 1.2%, with 77% being targeted attacks. Incidents involving individuals accounted for 12% of the total.
- Ransomware is still the malware that is most often used by attackers. In Q1, they demanded astronomical ransoms and refined their arsenal, including adding new ways to hide from security tools. There is a lot of new ransomware, for example, Cring, Humble, and Vovalex. And the good old WannaCry is running rampant again. Ziggy operators set a precedent: they returned the ransoms paid to the victims and "turned to the light side".
- The most popular vulnerabilities for attackers this quarter were breaches in the Microsoft Exchange Server software (ProxyLogon) and the outdated file sharing program Accellion FTA. Attackers used a zero-day vulnerability discovered in SonicWall VPN solutions not just to hack the company, but also to launch attacks on its customers. SonicWall presumably failed to notify its customers in time about the identified vulnerability or a need to implement protective measures. The incident supports the argument that software manufacturers should inform their customers as soon as possible about existing vulnerabilities and ways of protecting themselves until a patch is released.
- More and more cybercriminals are developing malware to conduct attacks on virtualization environments, and some are aggressively trying to exploit vulnerabilities already found in software for deploying virtual infrastructure. At the beginning of 2021, our security engineers helped to eliminate critical vulnerabilities in VMware products. We strongly recommend installing the security updates as soon as possible.
- The number of attacks targeting IT companies has remained consistently high for a second quarter in a row. In 15% of cases during Q1 2021, hackers targeted IT companies to conduct an attack on their customers or to steal customer data. At the beginning of 2021, there were still reports in the media about new victims of the attack on SolarWinds: the company's customers claim that their networks have been compromised.
- Telecom companies were twice as likely to be attacked as in Q4 2020. In 71% of the attacks, hackers aimed at obtaining data, with a particular interest in the 5G technology. Nine out of ten incidents saw attackers use malware—most frequently, RATs, which accounted for 55% of all attacks.

To protect from cyberattacks, follow our general recommendations for ensuring personal and corporate cybersecurity. Also, given the specifics of the attacks in the past quarter, we strongly recommend that you install security updates in a timely manner and pay special attention to protecting virtual infrastructure. You can strengthen security at the corporate perimeter by using modern security tools, for example, web application firewalls for protecting web resources. To prevent malware infection, we recommend using sandboxes to analyze the behavior of files in a virtual environment and detect malicious activity.

Statistics

The number of incidents in Q1 2021 increased by 17% compared to the same period in 2020, and compared to Q4 2020, increase was 1.2%, with 88% of the attacks targeting organizations. Cybercriminals typically attacked government institutions, industrial companies, research and education institutions. The main motive for attacks on both organizations and individuals remains acquisition of data. Attackers' main targets are personal data and credentials, and attacks on organizations are also aimed at stealing intellectual property.

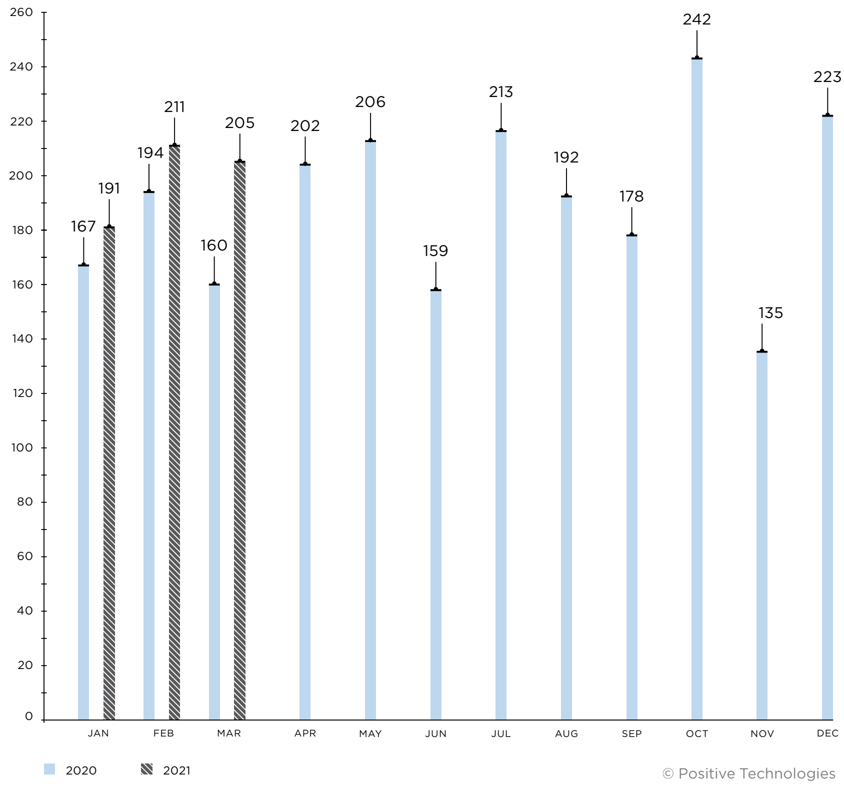
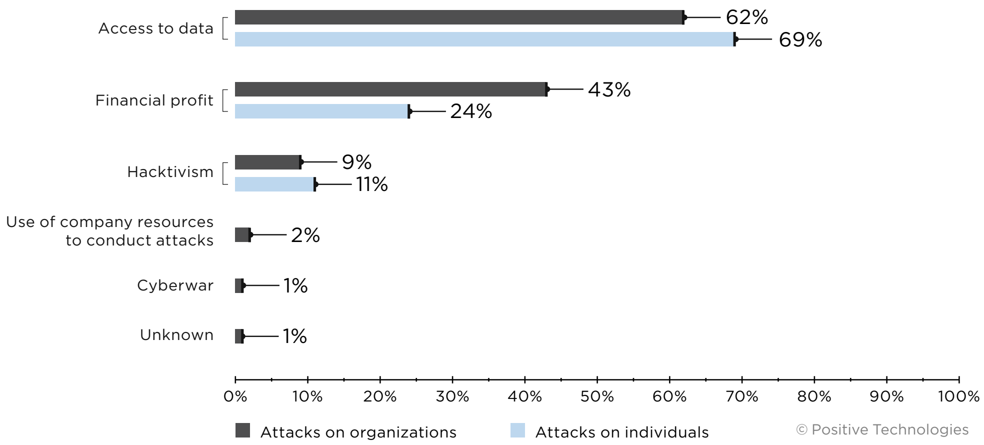
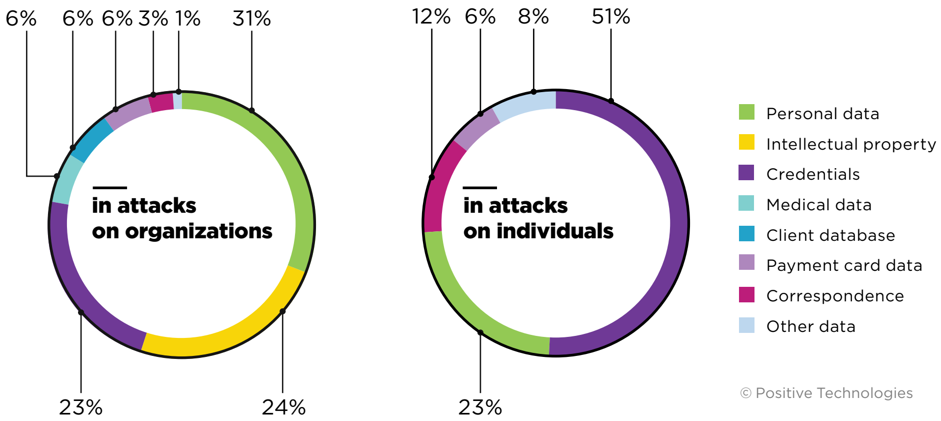


Figure 1. Number of incidents per month in 2020 and 2021



© Positive Technologies

Figure 2. Attackers' motives (percentage of attacks)

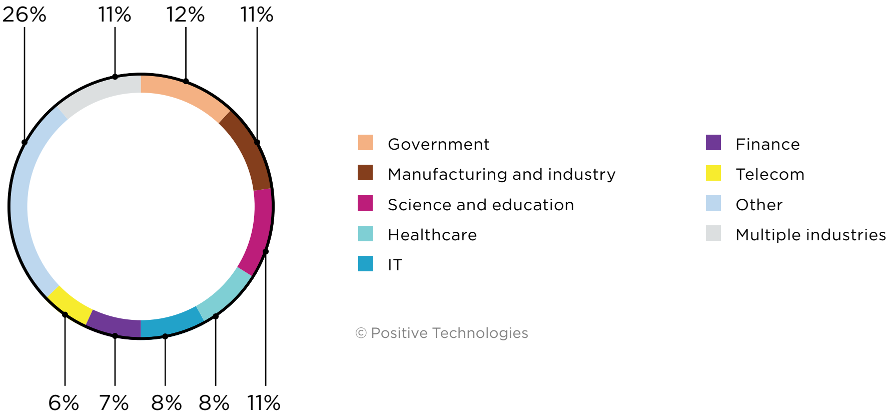


© Positive Technologies

Figure 3. Types of data stolen

77% of attacks were targeted

12% of attacks were directed at against individuals



© Positive Technologies

Figure 4. Victim categories among organizations

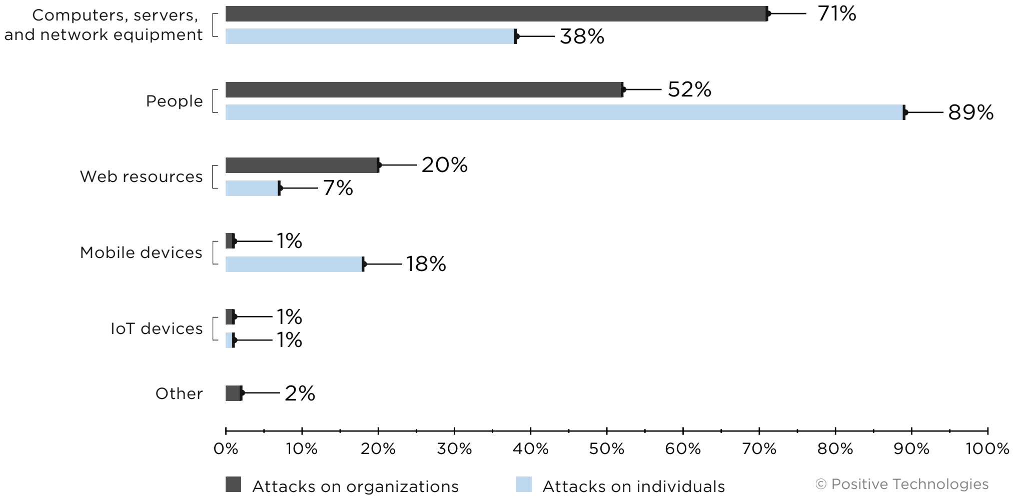


Figure 5. Attack targets (percentage of attacks)

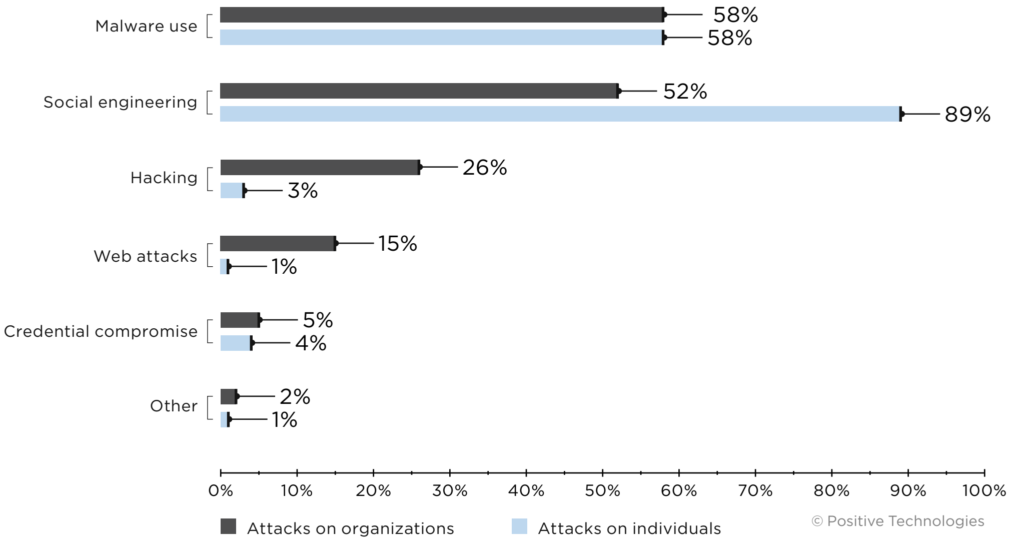


Figure 6. Attack methods (percentage of attacks)

Per-industry classification of cyberincidents by motive, method, target, and victim categories

		Victim categories									
		Government	Finance	Manufacturing and industry	Healthcare	IT	Science and education	Telecom	Other	Multiple industries	Individuals
	Total	**63**	**36**	**58**	**42**	**41**	**60**	**34**	**141**	**58**	**74**
Target	Computers, servers, and network equipment	47	21	48	32	29	44	31	88	39	28
	Web resources	16	4	5	4	11	4	17	36	11	5
	People	35	25	33	34	13	33	6	72	27	66
	Mobile devices	1							1	1	13
	IoT devices					2				3	1
	Other		2			1	4		5		
Method	Malware use	40	15	39	28	16	34	31	75	33	43
	Social engineering	35	25	33	34	13	33	6	72	27	66
	Credential compromise	1	1	5	3	2	6	1	5	5	3
	Hacking	13	8	17	4	21	18	1	34	20	2
	Web attacks	14	3	2	3	6	2	16	27	7	1
	Other	2	1						5	5	1
Motive	Access to data	38	29	39	24	27	22	24	98	31	51
	Financial profit	26	13	27	27	11	31	12	67	17	18
	Hacktivism	6	1	5		5	17		10	6	8
	Cyberwar	3							1		
	Use of company resources to conduct attacks			1		6			1	5	
	Unknown	1		1	1				1		

Darker colors indicate a greater proportion of attacks within a particular industry for each victim category

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

Elusive malware

Ransomware is predictably the most popular type of malware. Its share, among other malware used in attacks on organizations, increased by seven percentage points compared to Q4 2020 and is now 63%. Emailing remains the prevailing method of delivering malware: attackers used it in six out of ten malware attacks on organizations. Individuals are still most often attacked by banking trojans, spyware, and malware that provides remote access to the device.

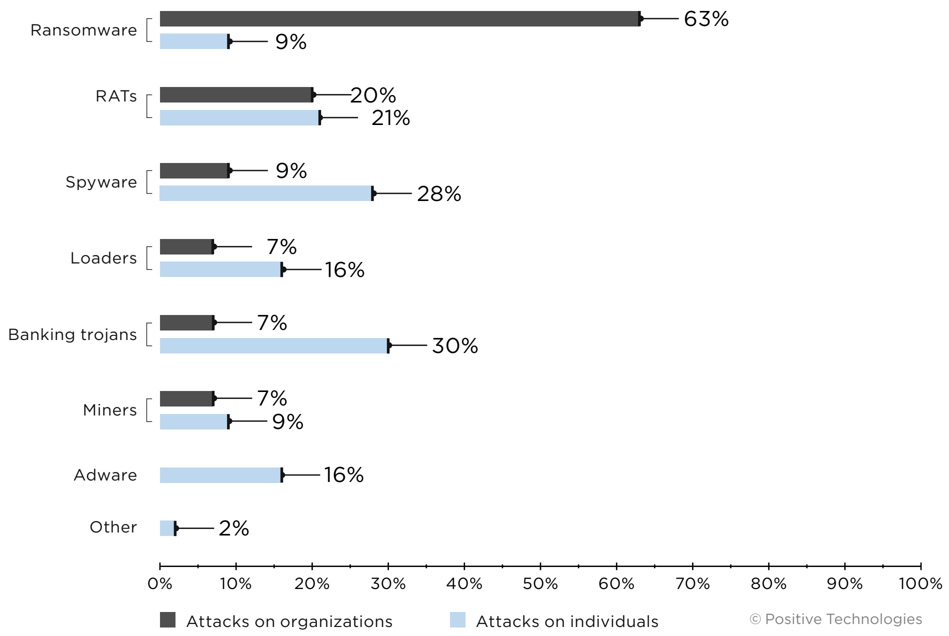


Figure 7. Types of malware (percentage of malware attacks)

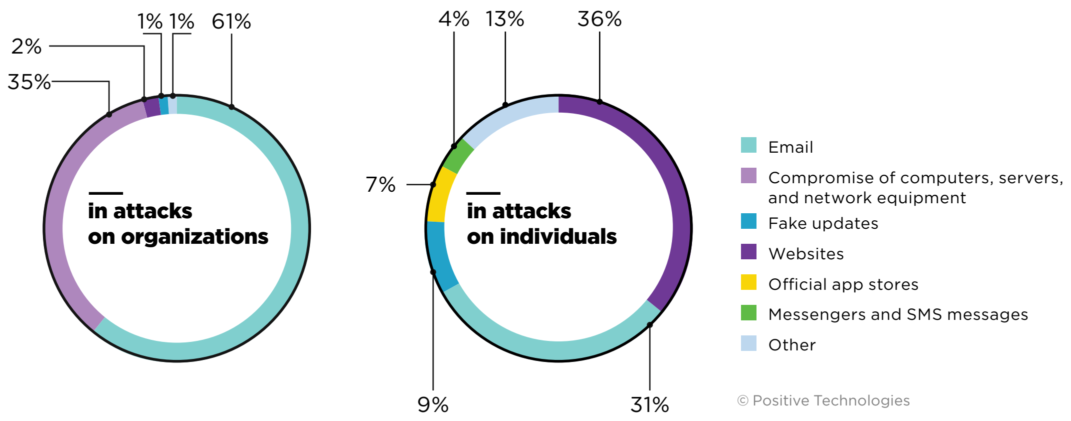


Figure 8. Methods used for malware distribution

Malware developers continue to look for new ways of bypassing security measures. To achieve that goal, attackers, for example, use unpopular programming languages, as in the case of BazarBackdoor (RAT), which was rewritten in Nim; the ransomware operators of Vovalex and RobbinHood chose such uncommon languages as D and Golang, respectively, from the get-go.

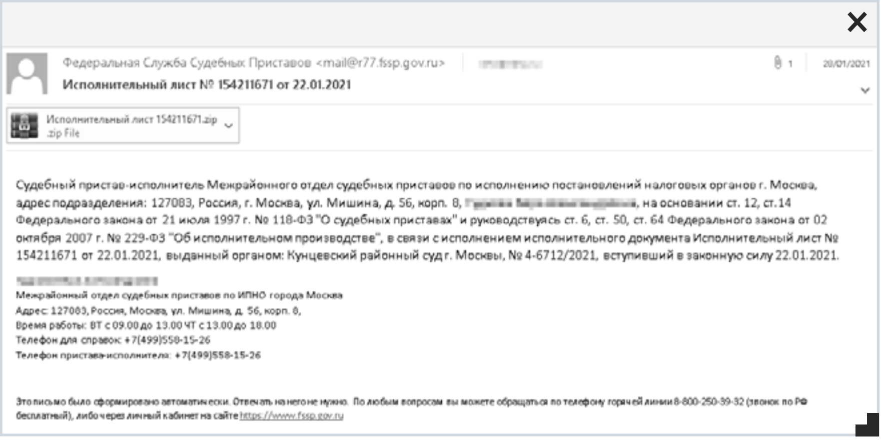
Some attackers have upgraded their tools with features that erase traces of malicious activity—as seen in such miners as OSAMiner, Black-T and Pro-Ocean. The code of the OSAMiner cryptominer, which targets macOS-based devices, contains a function that allows killing the Activity Monitor process, along with other monitoring and antimalware tools. Activity Monitor is the Mac equivalent of Task Manager. The Black-T miner, which targets Unix systems, clears bash history after deploying its payload and erases all traces of its own activity. The added openly accessible function for hiding the process is called libprocesshider; if detected, it may lead security experts to assume the presence of a malicious load. This tool is also used by attackers who distribute the Pro-Ocean miner, which attacks Apache ActiveMQ, Oracle WebLogic, and Redis servers, and checks the target environment before installation. At this stage, it determines whether to hide the malware, and if, for example, the malware finds itself in the Tencent Cloud or Alibaba Cloud environment, it starts the process of deleting monitoring agents.

Another way to hide the destructive load is to split the malware into archives. An example is the Masslogger trojan designed to collect credentials. Attackers use email to deliver the malware, and to bypass the security measures, they split the executable file into multivolume archives with such extensions as .r00, .r01, and so on.

Having analyzed the latest attacks by the RTM APT group, the PT ESC team found that the attackers were using packers as a service to bypass security tools. This approach greatly complicates a search for known signatures, but behavioral analysis of files in the sandbox allows detecting malicious activity. In addition, the use of cryptors does not affect interaction between the malware and management servers, which means that they can be detected by analyzing network traffic.

A cryptor (packer)

Is a program that uses cryptographic methods to package malware in order to hide it from security tools during signature analysis.



Федеральная Служба Судебных Приставов <mail@r77.fssp.gov.ru> [redacted] 1 20/01/2021

Исполнительный лист № 154211671 от 22.01.2021

Исполнительный лист 154211671.zip
.zip File

Судебный пристав-исполнитель Межрайонного отдел судебных приставов по исполнению постановлений налоговых органов г. Москва, адрес подразделения: 127083, Россия, г. Москва, ул. Мишина, д. 56, корп. 8, [redacted], на основании ст. 12, ст.14 Федерального закона от 21 июля 1997 г. № 118-ФЗ "О судебных приставах" и руководствуясь ст. 6, ст. 50, ст. 64 Федерального закона от 02 октября 2007 г. № 229-ФЗ "Об исполнительном производстве", в связи с исполнением исполнительного документа Исполнительный лист № 154211671 от 22.01.2021, выданный органом: Кунцевский районный суд г. Москвы, № 4-6712/2021, вступивший в законную силу 22.01.2021.

[redacted]
Межрайонный отдел судебных приставов по ИПНО города Москва
Адрес: 127083, Россия, Москва, ул. Мишина, д. 56, корп. 8,
Время работы: ВТ с 09.00 до 13.00 ЧТ с 13.00 до 18.00
Телефон для справок: +7(499)558-15-26
Телефон пристава-исполнителя: +7(499)558-15-26

Это письмо было сформировано автоматически. Отвечать на него не нужно. По любым вопросам вы можете обращаться по телефону горячей линии 8-800-250-39-32 (звонок по РФ бесплатный), либо через личный кабинет на сайте https://www.fssp.gov.ru

Figure 9. Phishing email from the RTM group that mimics a warning from bailiffs

Since the beginning of 2021, RTM has added the Quoter ransomware to their arsenal. According to researchers, if the banking trojan has failed to complete its tasks and collect information from the infected host, the attackers launch Quoter onto the company's network as Plan B. Following the example of other ransomware operators, RTM employs the strategy of double extortion in their attacks. The group still uses social engineering methods as the main method of delivery, sending phishing emails to victims.

The group's activity in Q1 2021 decreased compared to Q4 2020, but this may indicate that the attackers are busy developing new attack techniques or refining existing tools for now.

Ransoms keep going up

Every third attack in Q1 involved ransomware operators. At the end of 2020, healthcare was the most frequently attacked sector, but in Q1 2021, the first place was shared by industrial, scientific and educational organizations. They amounted to 30% of all incidents involving ransomware; 28% of the attacks were directed at governmental and medical institutions.

In about seven out of ten ransomware attacks on organizations, email was used as a method of delivering the malware, and in a quarter of cases, attackers exploited vulnerabilities and searched for unprotected resources accessible from the Internet.

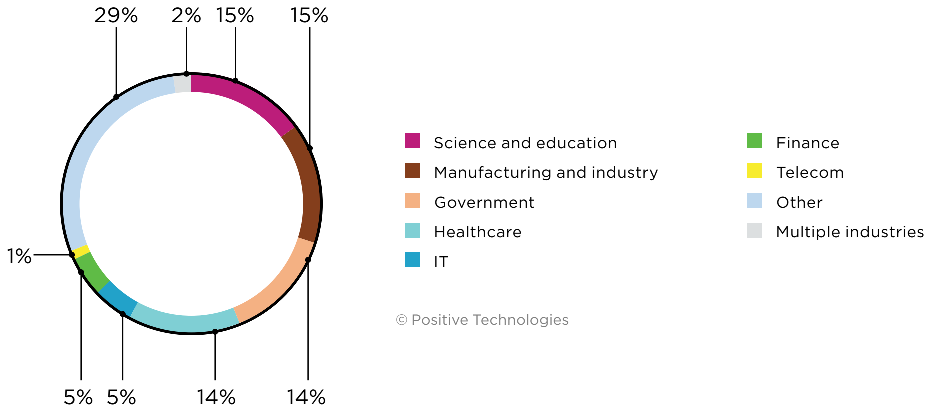


Figure 10. Categories of victims attacked by ransomware in Q1 2021

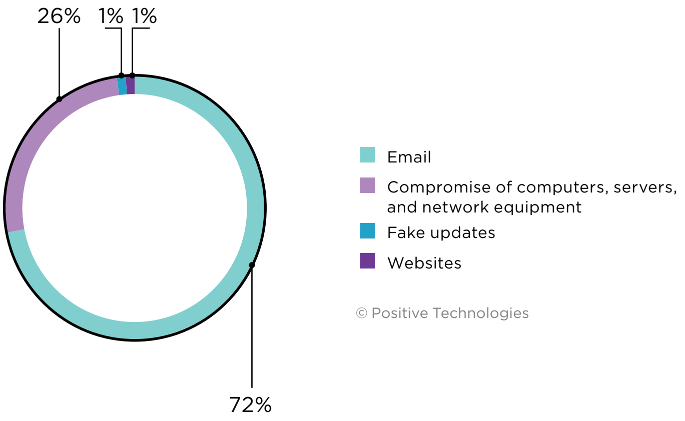


Figure 11. Ways of distributing ransomware inside organizations

The 5 most active ransomware programs in Q1 2021

1. REvil
2. Clop
3. Conti (Ryuk)
4. Babuk Locker
5. DoppelPaymer

New players appearing on the scene

In early 2021, several new ransomware programs appeared: Cring, Vovalex, Babuk Locker, Phoenix CryptoLocker, Hog, and Humble.

Hog

Hog is currently targeting individuals. Its operators decrypt the victims' devices only if they connect to their Discord server. The use of Discord was previously seen in other hackers' attacks and is becoming a frequent practice. Hog operators could be testing new techniques.

Astronomical ransoms

In Q1 2021, REvil operators broke all records in ransom demands. They demanded $50 million after attacking the IT company Acer, and, after encrypting the network of the pan-Asian retail chain Dairy Farm Group, demanded 30 million in exchange for a decryptor and nondisclosure of the stolen data. Such large amounts are due to the ask-more-to-get-more tactic. The incident with the retailer FatFace speaks to the success of the campaign. In early January, Conti (Ryuk) operators penetrated the company's network by conducting a phishing attack, and after seven days of reconnaissance, extracted 200 GB of data and started the encryption process. Initially, the attackers demanded $8 million. However, during the negotiations, the amount was reduced to 2 million, which satisfied both parties.

Due to the fact that some companies refuse to pay the ransom, ransomware operators are forced to come up with new tactics. These days, if the company is refusing to pay, the attackers threaten to report the attack and the data theft to its customers. The fraudsters expect that the customers will persuade the company to pay a ransom to prevent the disclosure of their data.

Old players making a comeback

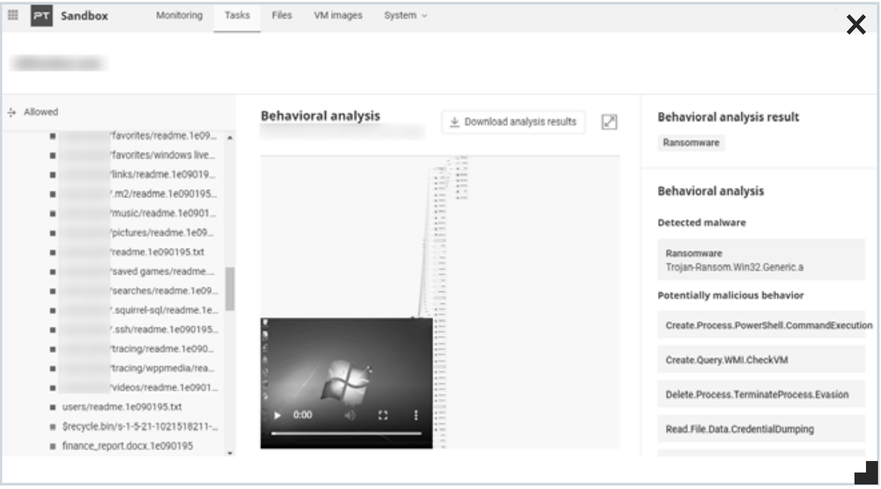
The WannaCry ransomware that thundered around the world four years ago is back in the game. According to Check Point, the number of affected organizations in March 2021 increased fortyfold compared to October 2020. The malware is being distributed using the EternalBlue exploit. The extortionists mostly attack government institutions and defense contractors, while the industrial sector ranks second, and financial organizations and medical institutions rank third and fourth, respectively.

New features

REvil has acquired a new feature: the ability to run the encryption process in Windows safe mode, which enables the malware to bypass security measures. Conti (Ryuk) developers have supplemented it with the ability to spread to other devices within the domain. It is distributed over the network through shared network resources, where it creates copies of itself, and files are launched by creating tasks in the Windows task scheduler.

Secure storage of stolen data

DarkSide operators, who attacked the Brazilian electric power company Companhia Paranaense de Energia (Copel), stealing about 1 TB of sensitive information, use their own method of data storage. They do not store stolen information on specially created private websites, as this is not safe. Instead, they have developed a distributed database: the data is stored on different servers. This helps to limit the number of individuals who can look at the data and avoid losing access to stolen information due to possible blockages.



- 'favorites/readme.1e09...
- 'favorites/windows live...
- 'links/readme.1e09019...
- '.m2/readme.1e090195...
- 'music/readme.1e0901...
- 'pictures/readme.1e09...
- 'readme.1e090195.txt
- 'saved games/readme....
- 'searches/readme.1e09...
- '.squirrel-sql/readme.1e...
- '.ssh/readme.1e090195...
- 'tracing/readme.1e090...
- 'tracing/wppmedia/rea...
- 'videos/readme.1e0901...
- users/readme.1e090195.txt
- $recycle.bin/s-1-5-21-1021518211-...
- finance_report.docx.1e090195

Behavioral analysis result

Ransomware

Behavioral analysis

Detected malware

Ransomware
Trojan-Ransom.Win32.Generic.a

Potentially malicious behavior

Create.Process.PowerShell.CommandExecution

Create.Query.WMI.CheckVM

Delete.Process.TerminateProcess.Evasion

Read.File.Data.CredentialDumping

Figure 12. DarkSide ransomware tool detected using PT Sandbox

Fear of liability

Ziggy operators, in the wake of the news about the capture of the attackers who distributed Netwalker and the destruction of the Emotet botnet infrastructure by law enforcement agencies, announced the end of their hacking career and promised the victims who paid them a ransom to return the money.

Insecure software

The first quarter of 2021 will be remembered for aggressive exploitation of vulnerabilities in the Microsoft Exchange Server software (ProxyLogon vulnerabilities) and Accellion FTA. The ProxyLogon vulnerabilities were exploited by distributors of the Black Kingdom and DearCry ransomware tools, Lemon_Duck cryptocurrency miner operators, and other APT groups.

Vulnerabilities in the outdated Accellion FTA data transfer software were exploited by Clop operators and the cybercriminal group FIN11: about 100 organizations were affected. About a quarter of these organizations suffered from major data breaches: the Singapore-based mobile operator Singtel, law firm Jones Day, universities in Miami and California, U.S. Bureau of Shipping, rail operator CSX, and aircraft manufacturer Bombardier. Centene, which was also affected by the vulnerabilities, filed a lawsuit against Accellion. The claim demands reimbursement of expenses associated with recovering from the attack.

The vulnerability CVE-2015-1427 in Elasticsearch allows attackers to bypass the sandbox protection mechanism and execute arbitrary commands. This quarter, it was used by operators of three botnets: z0Miner, Skidmap, and WatchDog. Another botnet, FreakOut, expanded with the help of vulnerabilities in TerraMaster (CVE-2020-28188), Zend Framework (CVE-2021-3007), and Liferay Portal (CVE-2020-7961).

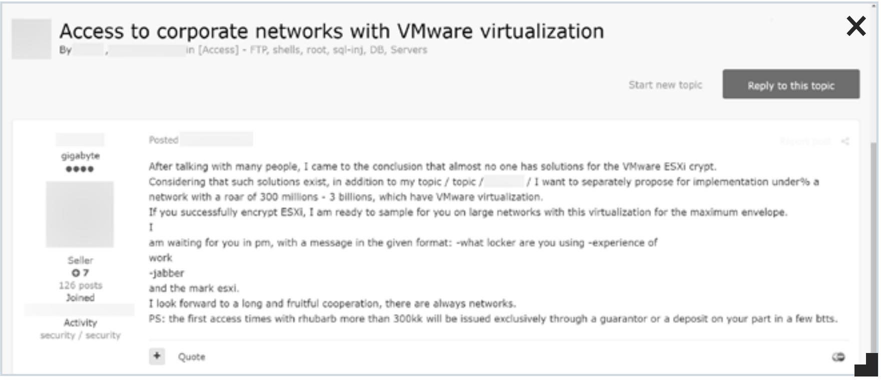
Speaking of vulnerabilities, we cannot fail to mention the incident with SonicWall, the manufacturer of information security systems, which was hacked via a zero-day vulnerability in the NetExtender and Secure Mobile Access VPN products in late

January. It was followed by media reports of attacks on the company's customers who were using the vulnerable solutions. For example, this opportunity was used by the UNC2447 group, which distributes the FiveHands ransomware (an updated version of DeathRansom) through the WarPrism loader or the SombRAT backdoor. According to researchers, the attackers were exploiting the vulnerability even before a security update appeared. Presumably, SonicWall did not alert its customers on time to the identified breach or a need to take protective measures.

Targeting virtual infrastructure

Q4 2020 saw a trend for attackers gearing their malware toward attacks on virtual infrastructure, and in Q1 2021, this trend consolidated. We can link this primarily to the global process of moving corporate IT infrastructure into a virtual environment. Attackers carefully monitor information about new vulnerabilities and try to find a use for these in their attacks as soon as possible. In early 2021, our experts helped to eliminate several critical vulnerabilities in VMware products, including CVE-2021-21972 in vCenter Server, which allowed remote code execution. At the time of publication, we estimate that the number of devices vulnerable to CVE-2021-21972 worldwide exceeded 6,000. After the vendor's security updates appeared in early February and the bulletin was published, Bad Packets researchers discovered multiple network scans conducted to find vulnerable hosts.

Darkside, RansomExx, and Babuk Locker operators are aggressively exploiting other vulnerabilities in VMware products to encrypt data stored on virtual hard drives, such as the remote code execution vulnerabilities CVE-2019-5544 and CVE-2020-3992.



Access to corporate networks with VMware virtualization

By [redacted] , [redacted] in [Access] - FTP, shells, root, sql-inj, DB, Servers

gigabyte

Seller

7

126 posts

Joined [redacted]

Activity

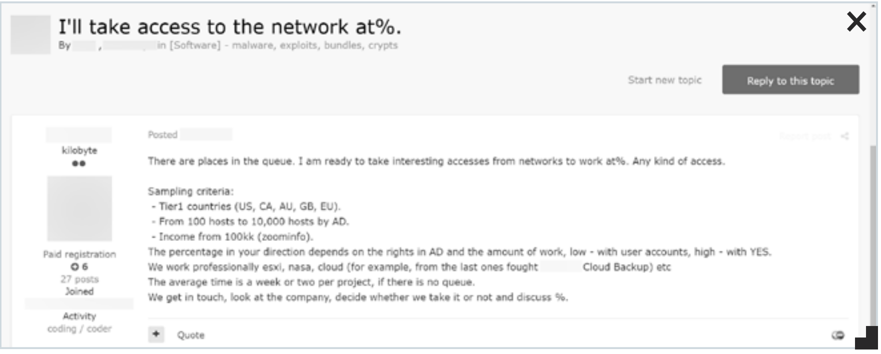
security / security

Posted [redacted]

After talking with many people, I came to the conclusion that almost no one has solutions for the VMware ESXi crypt.
Considering that such solutions exist, in addition to my topic / topic / [redacted] / I want to separately propose for implementation under% a network with a roar of 300 millions - 3 billions, which have VMware virtualization.
If you successfully encrypt ESXi, I am ready to sample for you on large networks with this virtualization for the maximum envelope.
I
am waiting for you in pm, with a message in the given format: -what locker are you using -experience of
work
-jabber
and the mark esxi.
I look forward to a long and fruitful cooperation, there are always networks.
PS: the first access times with rhubarb more than 300kk will be issued exclusively through a guarantor or a deposit on your part in a few btts.

Figure 13. Offer of access to networks using VMware ESXi

Attackers who distribute the Hildegard trojan purposefully attack Kubernetes environments. To hide their malware, they use several techniques at once, including encrypting the payload, masking the malicious process as the bioset process in Linux and using the Dynamic Linker Hijacking technique.



I'll take access to the network at%.

By [redacted], [redacted] in [Software] - malware, exploits, bundles, crypts

[redacted]
kilobyte

Paid registration
6
27 posts
Joined [redacted]
Activity
coding / coder

Posted [redacted]

There are places in the queue. I am ready to take interesting accesses from networks to work at%. Any kind of access.

Sampling criteria:
- Tier1 countries (US, CA, AU, GB, EU).
- From 100 hosts to 10,000 hosts by AD.
- Income from 100kk (zoominfo).
The percentage in your direction depends on the rights in AD and the amount of work, low - with user accounts, high - with YES.
We work professionally esxi, nasa, cloud (for example, from the last ones fought [redacted] Cloud Backup) etc
The average time is a week or two per project, if there is no queue.
We get in touch, look at the company, decide whether we take it or not and discuss %.

Figure 14. Ad for virtual or cloud infrastructure hacking services

Gaining access to virtual infrastructure and cloud services is a fairly popular topic on the darkweb. The services of so-called brokers are also used by ransomware operators for acquiring credentials to log in to the systems. In addition to ready-to-use access to certain companies, attackers post offers to hack companies to order on darkweb message boards.

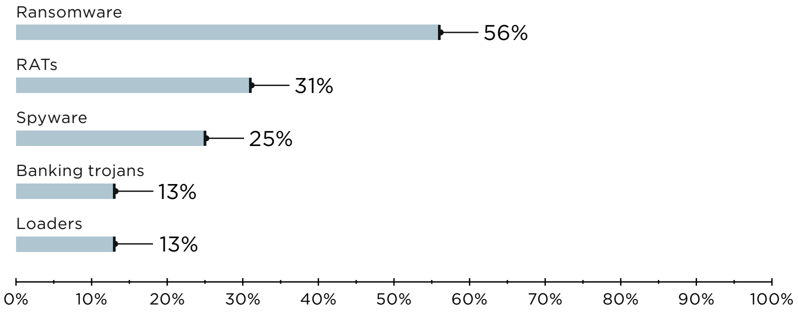
Targeting software developers and cloud services

The number of attacks on IT companies has not decreased since the beginning of Q4 2020. The main motive of hackers attacking this industry is to obtain data (66%). In 27% of the incidents, hackers sought financial gain, and in 15% of the cases, companies were hacked to facilitate subsequent attacks on their customers.

The consequences of the attack on SolarWinds were evident still even in early 2021. Thus, in early March, news about the attack on the IT company Robotron appeared in the media. The incident also affected the company's customers who installed malicious updates for the Werkzeugkasten backup server. The investigation revealed that the company's network was compromised as a result of the attack on SolarWinds. According to Robotron, the first victim to install malicious updates was a small company in the Netherlands (neither the name nor even the industry in which the company operates were disclosed). Under the guise of updates, the BlockKopieren ransomware was distributed.

Supply chain attacks did not spare information security companies. In early February, the French company Stormshield reported that its systems had been hacked. Attackers compromised the technical support portal. As a result of the incident, the source code of the Stormshield Network Security software firewall was stolen. It can be assumed that the attackers will examine the stolen code to find vulnerabilities in the software. In early January 2021, Malwarebytes, which produces information security tools, suffered due to a vulnerability in an application that has privileged access to Microsoft Office 365 and Azure. Note that in half of the attacks on this industry, attackers exploited software vulnerabilities.

Ransomware operators were involved in 56% of the malware attacks. The most significant incidents in terms of consequences occurred with the American IT service provider CompuCom and the Canadian IoT solution provider Sierra Wireless. In the first case, due to the attack using the DarkSide ransomware, the company suspended the provision of services to some customers. The company estimates that it will have to spend up to $20 million to eliminate all of the consequences, and the expected loss of revenue ranges from 5 to 8 million. Sierra Wireless, which was also affected by the ransomware attack, was forced to stop production, and the company's website was unavailable for two weeks. In addition, the company had to withdraw its financial forecast for Q1 2021, as it now needs to be adjusted.



© Positive Technologies

Figure 15. Malware types used in attacks on IT companies

The share of RATs increased by 23 percentage points compared to Q4 2020. In one of the campaigns, the attackers distributed it under the guise of Xcode, a free IDE for the Apple ecosystem. SentinelOne researchers discovered this malware in the legitimate project TabBarInteraction. The campaign is aimed at developers who will then inadvertently distribute remote control malware to their clients as part of the project. Another attack aimed at software developers involved hacking the official PHP Git repository and adding malicious commits. It is noteworthy that the attackers managed to add well-known developers' signatures to the commits.

Popular cloud services that facilitate interaction and simplify companies' IT infrastructure also became a favorite target for attackers. The reason for this phenomenon is that by attacking a cloud service provider, hackers can gain access to the customers' data, as it happened, for example, during the January incident with the Bonobos clothing store. The store suffered a data leak due to an attack on the cloud service provider that the company used to store customer credentials and personal data. A similar incident occurred with the network equipment manufacturer Ubiquiti.

According to the United States Cybersecurity and Infrastructure Security Agency, hackers managed to find a way to bypass two-factor authentication to compromise cloud services. This was achieved through a "pass the cookie" attack.

Pass the cookie

In this type of attack, attackers intercept the session of an already authenticated user or use stolen session cookies to authenticate with a web resource.

Wiretapping, interception of messages, and news about 5G

The number of attacks on telecom companies doubled compared to Q4 2020.

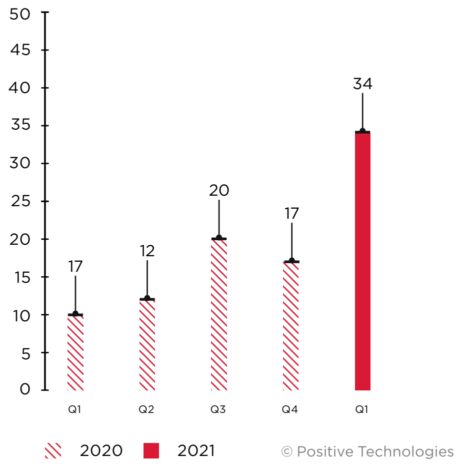


Figure 16. Number of attacks on telecom companies

In 71% of the attacks, the attackers pursued the motive of obtaining data. The 5G technology turned out to be a really interesting topic for hackers, perhaps due to the fact that they want to understand the features of its implementation in order to subsequently conduct attacks on subscribers. As part of a major cyberespionage campaign, hackers created a fake website that mimics Huawei's official job portal. Upon visiting this resource, a malicious Flash application was installed on the victim's computer, which acted as a loader for a subsequent installation of Cobalt Strike Beacon. At least 23 telecommunications companies fell prey to this campaign.

In early 2021, researchers from ClearSky reported on a campaign they identified, which collected sensitive data. Conducted by the Volatile Cedar cybercrime group, the campaign began in Q3 2020 and continues to this day. During the attacks, hackers exploit the web vulnerabilities CVE 2019-3396 (Atlassian Confluence), CVE 2019-11581 (Atlassian Jira) and CVE 2012-3152 (Oracle Fusion). Among the victims of this campaign were, for example, the American telecom company Frontier Communications, the Egyptian mobile operator Vodafone Egypt, the Israeli National Information Technology Center, as well as the telecom companies Mobily and Saudinet in Saudi Arabia, and other major companies in the industry.

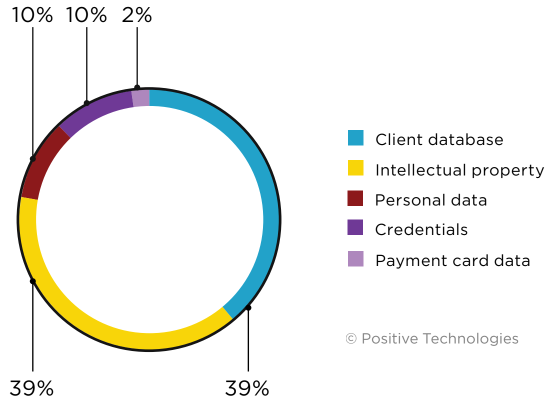
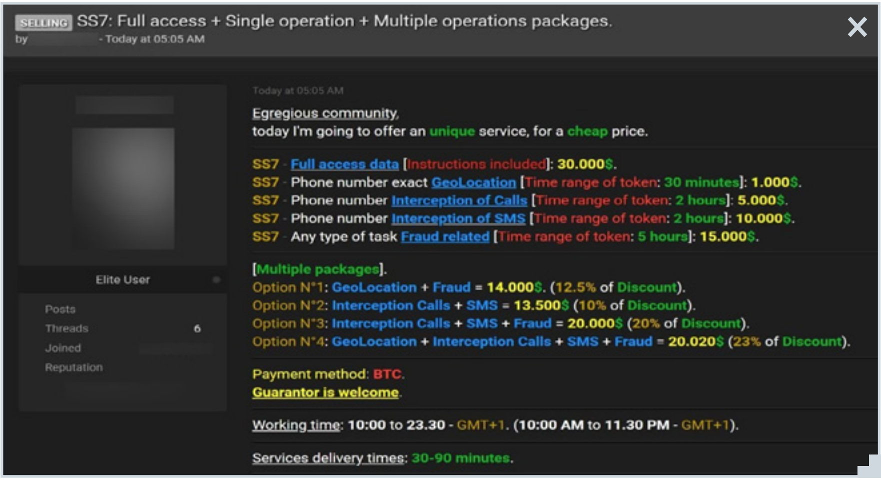


Figure 17. Data stolen in attacks on telecom companies

Malware was used in 91% of the attacks. Most of the incidents (55%) involved RATs, as in the case of USCellular. This fact may indicate that access to telecom companies is of high value to hackers: it can be sold on a darkweb forum or used in further attacks on subscribers.



SS7: Full access + Single operation + Multiple operations packages.
by [redacted] - Today at 05:05 AM

Today at 05:05 AM

Egregious community,
today I'm going to offer an unique service, for a cheap price.

SS7 - Full access data [Instructions included]: 30.000$.
SS7 - Phone number exact GeoLocation [Time range of token: 30 minutes]: 1.000$.
SS7 - Phone number Interception of Calls [Time range of token: 2 hours]: 5.000$.
SS7 - Phone number Interception of SMS [Time range of token: 2 hours]: 10.000$.
SS7 - Any type of task Fraud related [Time range of token: 5 hours]: 15.000$.

[Multiple packages].
Option N°1: GeoLocation + Fraud = 14.000$. (12.5% of Discount).
Option N°2: Interception Calls + SMS = 13.500$ (10% of Discount).
Option N°3: Interception Calls + SMS + Fraud = 20.000$ (20% of Discount).
Option N°4: GeoLocation + Interception Calls + SMS + Fraud = 20.020$ (23% of Discount).

Payment method: BTC.
Guarantor is welcome.

Working time: 10:00 to 23.30 - GMT+1. (10:00 AM to 11.30 PM - GMT+1).

Services delivery times: 30-90 minutes.

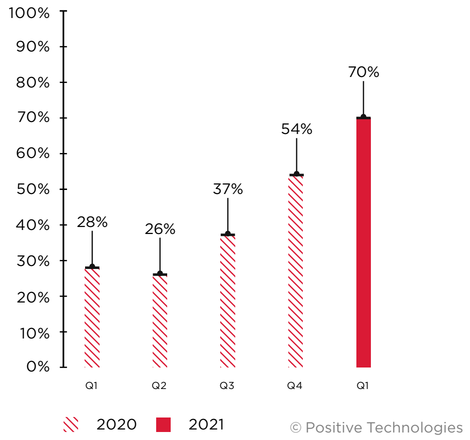
Figure 18. Ad for access to the SS7 network and cybercriminal services

Access to telecom equipment can allow attackers to intercept calls and messages of subscribers, track their location, and conduct fraudulent operations.

Governmental institutions are the most frequently attacked organizations

Since 2017, governmental institutions have topped our rankings of the most frequently attacked organizations. For their malicious actions, hackers mainly used malware (63% of attacks) and social engineering techniques (56%). The exploitation of web vulnerabilities ranks third: the share of this method (22%) increased by 13 percentage points compared to Q4 2020. Most often, attackers exploited vulnerabilities that were popular in Q1 2021, such as the ProxyLogon vulnerability used, for example, in the incident with the Norwegian parliament and a vulnerability in Accellion FTA, which affected the audit service of the state of Washington. The APT groups LuckyMouse, Tick, and Calypso, which target organizations in the United States, Europe, Asia, and the Middle East, including governmental agencies, were also seen exploiting the ProxyLogon remote code execution vulnerability (CVE-2021-26855). The purpose of these campaigns was to obtain data.

The share of ransomware operators in attacks on governmental institutions is increasing: they were found in 70% of malware attacks. In addition to ransomware, attackers also used banking trojans (18% of malware attacks), RATs (13%), and spyware (8%).

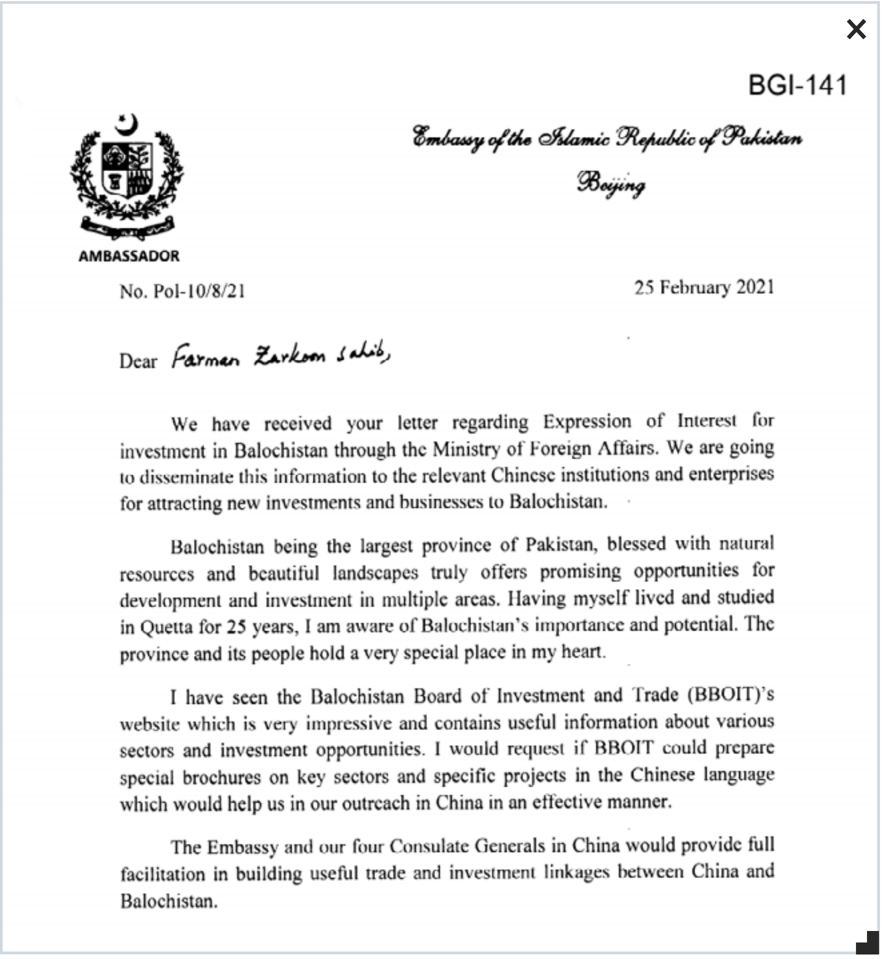


© Positive Technologies

Figure 19. Ransomware attacks on governmental institutions (percentage of malware-related attacks)

In this context, we should note the February attack on smart city systems in India. The Economic Times stressed that this is the first attack ever on the infrastructure of a smart city. The ransomware operators demanded $646,000 for troubleshooting the problems they created. An equally interesting example is the attack by the hacker group Hotarus Corp, which managed to hack the network of the Ministry of Economy and Finance of Ecuador and distribute their ransomware Ronggolawe (AwesomeWare). The peculiarity of this ransomware is that it is written in PHP and encrypts the files of the victim company's web applications. During this attack, the credentials of more than 6,500 users were compromised, and sensitive information, including emails and personal data of employees, was stolen.

Social engineering techniques were used in 56% of the incidents. For example, the APT group SideWinder, whose activities were monitored by PT ESC, uses these to deliver malware. Attacks by this group on governmental institutions in Southeast Asia were recorded throughout Q1 2021. As the first step of the attacks, the hackers attached a file with a .lnk extension a phishing email. If the user opened the file, the mshta.exe utility ran, displaying a stub document to the victim to allay its suspicions, while the main script deployed the trojan. This technique is used by many APT groups that we talked about in Q2 2020 and Q3 2020.



BGI-141

Embassy of the Islamic Republic of Pakistan
Beijing

AMBASSADOR

No. Pol-10/8/21

25 February 2021

Dear Farman Zarkoon sahib,

We have received your letter regarding Expression of Interest for investment in Balochistan through the Ministry of Foreign Affairs. We are going to disseminate this information to the relevant Chinese institutions and enterprises for attracting new investments and businesses to Balochistan.

Balochistan being the largest province of Pakistan, blessed with natural resources and beautiful landscapes truly offers promising opportunities for development and investment in multiple areas. Having myself lived and studied in Quetta for 25 years, I am aware of Balochistan's importance and potential. The province and its people hold a very special place in my heart.

I have seen the Balochistan Board of Investment and Trade (BBOIT)'s website which is very impressive and contains useful information about various sectors and investment opportunities. I would request if BBOIT could prepare special brochures on key sectors and specific projects in the Chinese language which would help us in our outreach in China in an effective manner.

The Embassy and our four Consulate Generals in China would provide full facilitation in building useful trade and investment linkages between China and Balochistan.

Figure 20. Sample the phishing email from the APT group SideWinder for a targeted attack on the Embassy of Pakistan in China

About the research

In this quarterly report, Positive Technologies shares information on relevant global cybersecurity threats. The information draws on our own expertise, the outcomes of investigations, and data from authoritative sources.

We believe that the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity of hacker groups are unable to do a precise count of threats. This research aims to draw the attention of companies and common citizens who concern themselves with the state of information security to the key motives and methods of cyberattacks, and to highlight the main trends in the changing cyberthreat landscape.

In this report, each mass attack—for example, when attackers send phishing emails to multiple addresses—is counted as a single incident. Definitions of terms used in this report are available in the glossary on the Positive Technologies site.

About Positive Technologies

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

For 19 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.