Cybersecurity threatscape

Q2 2021

ptsecurity.com

Contents

Summary 3

Statistics 4

Malware targeting virtualization tools 7

Transformations of ransomware 10

Backups are at risk 14

Check for updates 14

Attacks on governmental institutions 15

New cybersecurity threatscape for retail 16

Threats to industry 17

About the research 19

Summary

Highlights of Q2 2021 include:

- The number of attacks increased by only 0.3% compared to Q1 2021. Such a slowdown should have been expected, since companies managed to adapt to work amidst the pandemic, including taking measures to protect their network perimeter and remote access systems.
- The number of targeted attacks is growing every quarter. In Q2, 77% of attacks were targeted. The percentage of attacks targeting individuals remained at the level of the previous quarter (12%).
- Attacks involving malware still rank first in the cybercriminals' arsenal. Compared to Q1 2021, the increase in Q2 was 15 percentage points, accounting for 73%. We note that the trend toward creating malware targeting Unix systems, virtualization tools, and orchestrators has taken hold.
- In Q2, the number of ransomware attacks reached stratospheric levels, accounting for 69% of all attacks involving malware. This number was increasing most in April. However, in early May, criminals attacked the Colonial Pipeline (the largest US pipeline system) and the police of the District of Columbia, which attracted the attention of law enforcement agencies. As a result, cybercriminals began to change their approaches to attacks and modify their partner programs. We believe that ransomware operators may soon abandon partners as a separate role and start supervising distributors directly.
- In Q2, owners of QNAP devices had to be on the alert, since these devices aggregate large amounts of data from companies and individuals and, in so doing, are of great value to attackers. QNAP clients were mainly attacked using ransomware, for example, AgeLocker and eCh0raix.
- The percentage of attacks on governmental institutions (among all attacks on organizations) soared from 12% in Q1 2021 to 20% in Q2. Ransomware distributors were involved in 73% of malware-related incidents. PT ESC discovered Tomiris, a new loader; this malware comes with functions for gaining persistence and can send encrypted information about the workstation to an attacker-controlled server.
- The cybersecurity threatscape for the retail industry has changed. In Q2, we noted, on the one hand, a decrease in the number of MageCart attacks, and, on the other, an increase in the share of ransomware attacks. Whereas previously cybercriminals pursued the goal of data theft, now they are seeking direct financial gain.
- In Q2, the industrial sector was also affected by ransomware distributors particularly often. They were involved in 80% of malware attacks. Cases of hacking became more frequent: the percentage of such attacks increased from 29% to 34%. PT ESC discovered B-JDUN, a new type of a remote administration tool (RAT), used in an attack on an energy company.

To protect against cyberattacks, we advise following our recommendations for personal and corporate cybersecurity. Taking into account the specifics of the attacks in this quarter, we strongly recommend installing security updates in a timely manner. We also advise conducting thorough investigations of all major incidents to identify the points of compromise and vulnerabilities that the attackers exploited. In addition, make sure that the criminals did not leave any backdoors for themselves. 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 that analyze file behavior in a virtual environment and detect malicious activity.

Statistics

The number of attacks increased by 0.3% against Q1 2021. The percentage of attacks aimed at compromising computers, servers, and network equipment increased from 71% to 87%, which is associated with an increase in the number of ransomware attacks. The percentage of attacks motivated by financial gain increased as well (from 43% to 59%). Most often, criminals attacked medical and governmental institutions and industrial companies.

In attacks on individuals, the primary motive was data theft. Compared to Q1 2021, its share increased by 9 percentage points to 78%, while the volume of stolen payment data more than doubled.

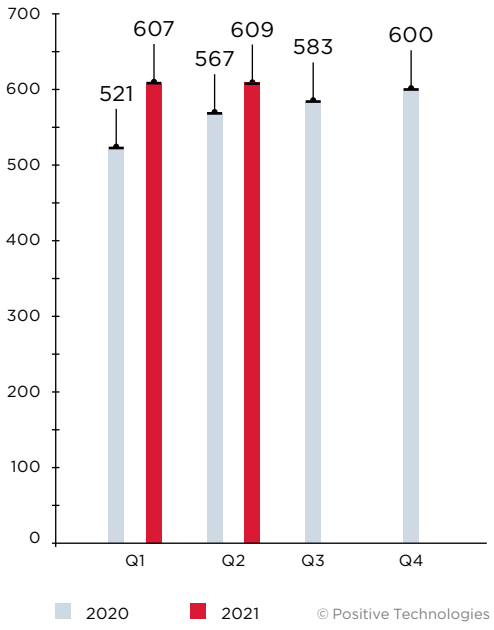

Figure 1. Number of attacks in 2020 and 2021 (per quarter)

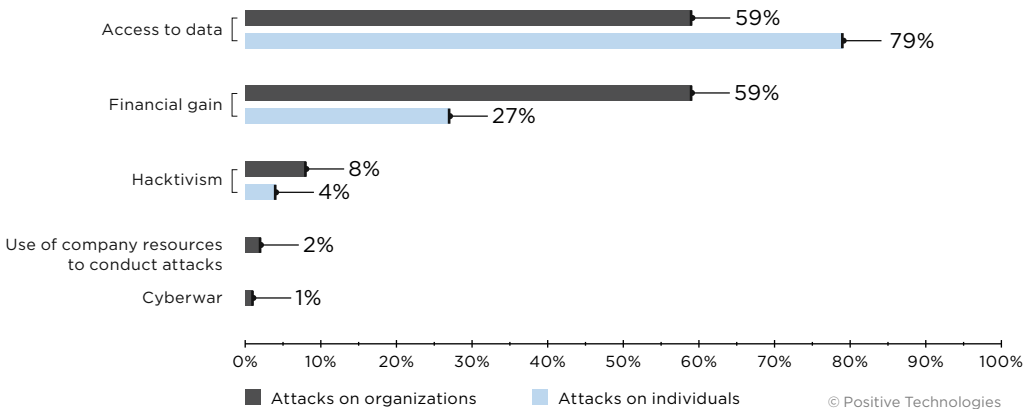

Figure 2. Attackers' motives (percentage of attacks)

77% of attacks were targeted

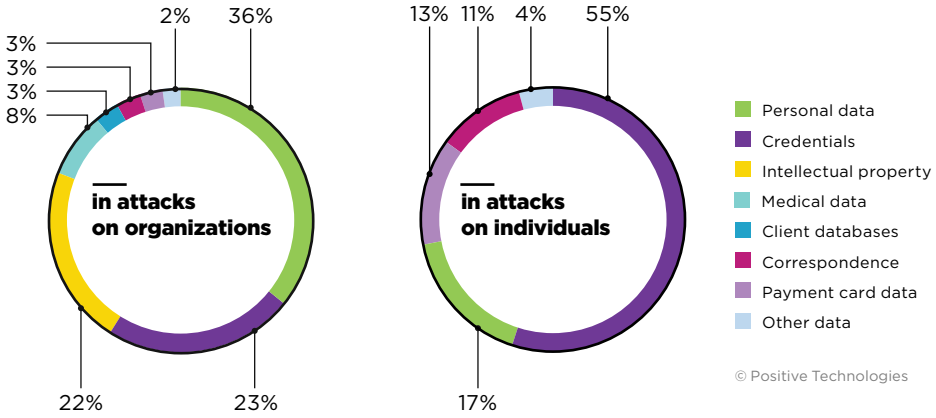

Figure 3. Types of data stolen

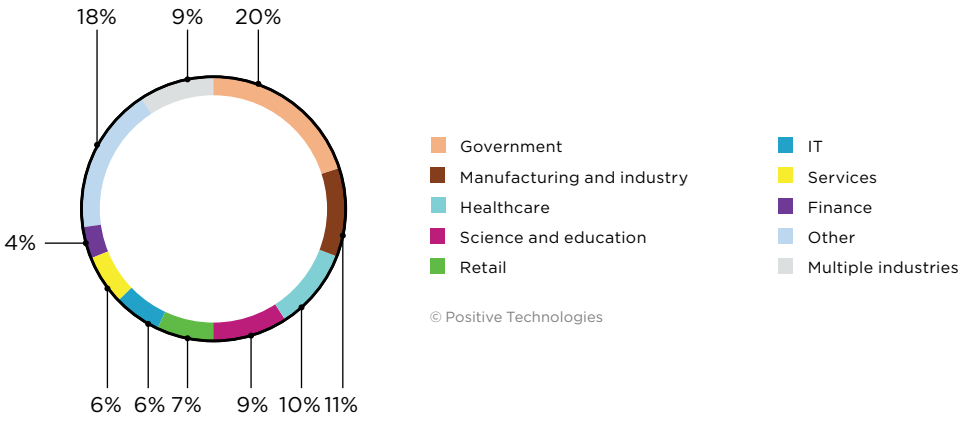

Figure 4. Victim categories among organizations

12% of attacks were directed at individuals

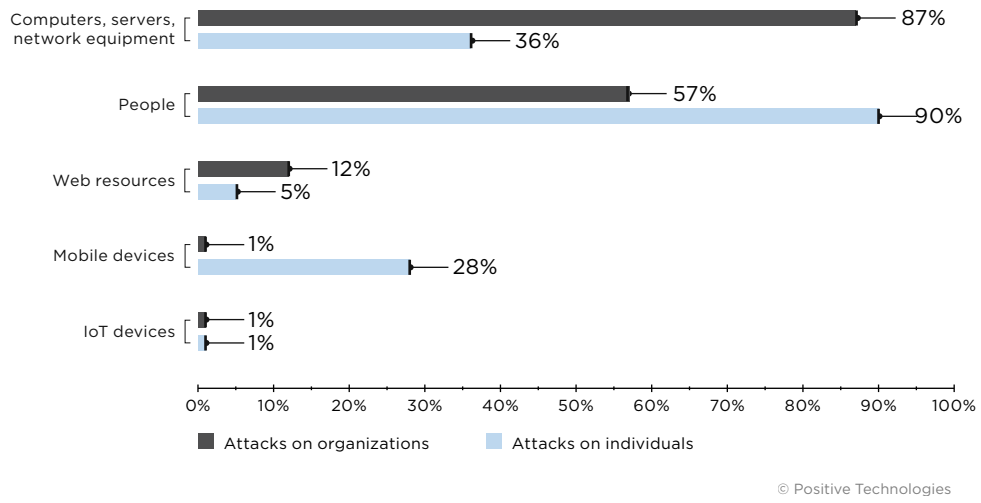

Figure 5. Attack targets (percentage of attacks)

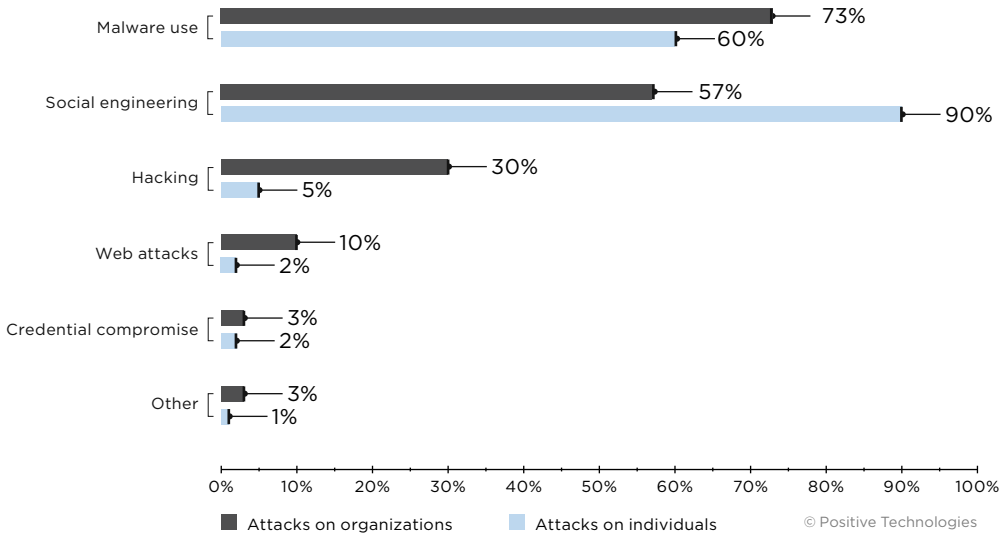

Figure 6. Attack methods (percentage of attacks)

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

		Sector										
		Government	Finance	Manufacturing and industry	Healthcare	IT	Science and education	Retail	Services	Other	Multiple industries	Individuals
	Total	**102**	**23**	**56**	**50**	**32**	**47**	**34**	**29**	**94**	**48**	**94**
Targets	Computers, servers, and network equipment	88	20	49	45	32	45	26	26	81	39	35
	Web resources	19	1	2	3	2	3	7	4	16	5	5
	People	60	15	33	34	8	34	18	17	54	19	85
	Mobile devices	2								1		26
	IoT devices										3	1
Method	Malware use	78	15	41	37	20	38	20	21	71	37	56
	Social engineering	60	15	33	34	8	34	18	17	54	19	85
	Credential compromise	4	1	2		1	1		2	4	2	2
	Hacking	24	4	19	13	21	10	9	8	23	24	5
	Web attacks	15	1	1	3		3	7	4	14	5	2
	Other	4	3	1		1				4	1	1
Motive	Access to data	56	14	33	35	18	20	18	20	61	29	74
	Financial gain	60	11	38	34	16	32	21	17	54	23	26
	Hacktivism	8	4	6	2	1	5	4	2	7		4
	Cyberwar	1		1			1					
	Use of company resources to conduct attacks			1		3			1	2	6	
	Unknown					1						

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

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

Malware targeting virtualization tools

Compared to Q1 2021, the percentage of attacks using malware and attacks targeting organizations increased by 15 percentage points to 73%. Ransomware is still the most popular type of malware used in attacks on organizations. The percentage of ransomware attacks increased from 63% to 69% in Q2. Compared to Q1, the percentage of attacks using loaders more than doubled.

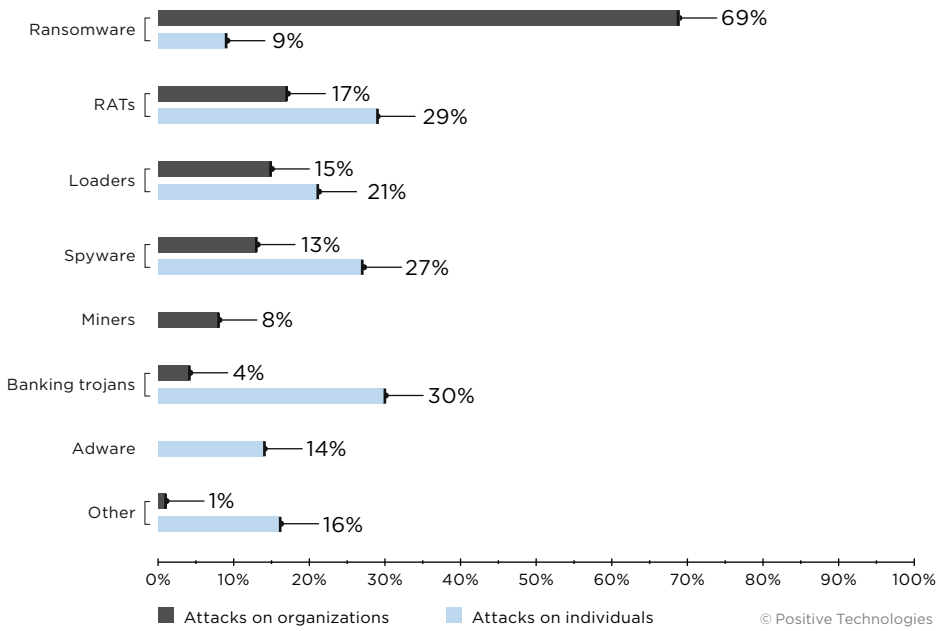

Figure 7. Types of malware (percentage of malware-related attacks)

Emailing remains the main method of spreading malware in attacks on organizations (58%). The percentage of using websites to distribute malware in organizations increased from 2% to 8%. For example, this method was used by spyware distributors targeting programmers who work with Node.js. The malware imitated the Browserify component in the npm registry.

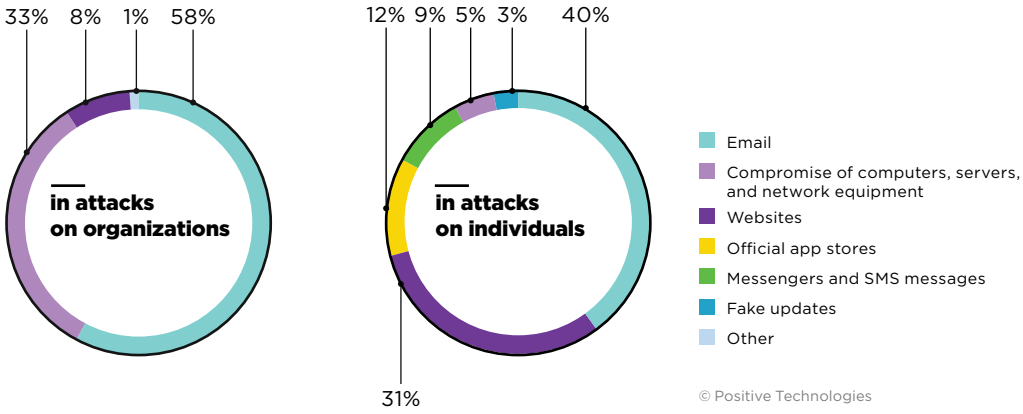

Figure 8. Methods used for malware distribution (percentage of malware-related attacks)

Targeting Unix systems and virtualization tools

It was previously thought that attackers distributing malware posed a danger mainly to Windows systems. Now we see that the trend toward creating malware for attacks on Unix systems, virtualization tools, and orchestrators has taken hold.

In Q1 2021, we wrote that many attackers targeted virtual infrastructure. In Q2, they were joined by ransomware operators. REvil, RansomExx (Defray), Mespinoza, GoGoogle, DarkSide, Hellokitty, and Babuk Locker are ready to be used in attacks on virtual infrastructure based on VMware ESXi.

Trend Micro analyzed the new in-development DarkRadiation ransomware, and found it to be tailored for attacks on Red Hat, CentOS, and Debian Linux. The malware itself is a bash script that can stop or disable all running Docker containers. Attackers use compromised accounts and the SSH protocol as a way to distribute this ransomware.

In addition, attackers targeting Unix systems distribute:

- Sysrv miner and botnet miner, which abuse legitimate DevOps tools (Ansible, Chef, SaltStack)
- RotaJakiro backdoor, which remains invisible to antivirus mechanisms
- Facefish backdoor, together with a rootkit to access the Linux-based hosting management interface Control Web Panel
- FreakOut multiplatform malware with a rootkit in user mode targeting Windows- and Linux-based VMware vCenter virtual servers. FreakOut has functions for conducting DDoS attacks using victims' equipment, download other malware, including miners, and intercept network traffic.

In this context, we should mention the distributors of a RAT called Siloscape targeting Windows containers. The criminals' overall goal is the compromise of both individual containers and entire Kubernetes clusters to facilitate subsequent attacks on their users (for example, supply chain attacks).

How to complicate the life of developers

In Q2, we discovered an interesting incident involving distributors of cryptocurrency miners. The criminals abused free access to continuous integration services (GitHub, Microsoft Azure, LayerCI, TravisCI, Sourcehut, CloudBees CodeShip and CircleCI), using their computing capacity to host and launch miners. Thus, they were able to generate cryptocurrency during the access trial period.

As soon as the affected companies found out about this scheme, they introduced additional restrictions, requiring payment card data during registration or completely terminating free access to their services.

Big comebacks

The TrickBot botnet returned with the new Diavol ransomware. Its developers used asymmetric encryption algorithms and hid the source code in bitmaps.

The financially motivated APT group FIN7, notorious for its Carbanak malware, also reappeared with an updated version of the Tirion loader, known as Lizar. The new malware is distributed under the guise of a security analysis tool. Victims of the new malicious campaign included several educational institutions, a gambling establishment, pharmaceutical companies in the U.S., an IT company headquartered in Germany, and a financial institution in Panama. Lizar has plenty of functions for

collecting information about the infected system, launching various plugins, including for collecting credentials, and loading additional software, for example, Mimikatz and the Carbanak backdoor. The modular structure of the malware allows attackers to easily add new plugins.

Attacks on individuals

Malware was used in 60% of attacks on individuals. Most often, attackers distributed banking trojans (30% of attacks involving other malware), RATs (29%), and spyware (27%). Ransomware attacks account for only 9% of attacks involving other malware. The distribution of NitroRansomware is an example of a ransomware attack on individuals. Attackers spread this malware under the guise of a tool for generating free gift codes for Nitro, a Discord add-on. After launching, the malware collects data from the browser, then encrypts the files in the victim's system. To get a decryptor, the victim has to purchase a gift code for activating Nitro and give it to the criminals.

Transformations of ransomware

In Q2 2021, seven out of 10 malware attacks involved ransomware distributors, with an increase of 30 percentage points compared to Q2 2020 (their share was only 39% back then). The most common targets were governmental, medical, and industrial companies, and scientific and educational institutions.

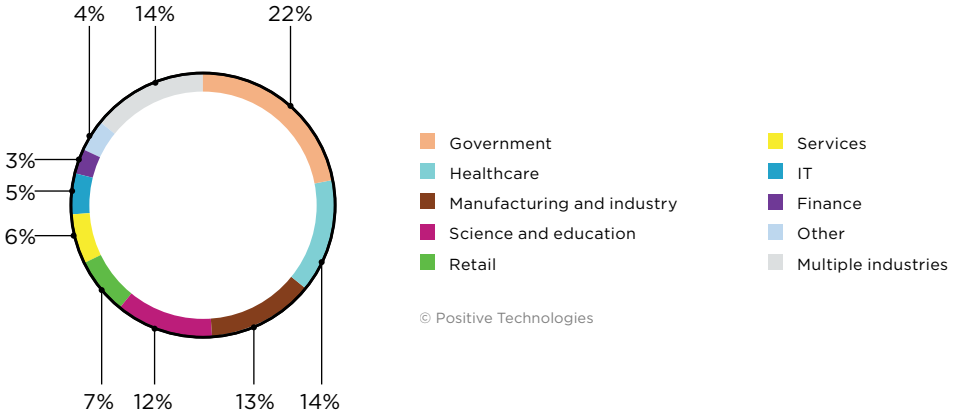

Figure 9. Ransomware attacks by industry

The most popular ransomware in Q2 2021

- REvil
- Avaddon (announced shutdown in June)
- DoppelPaymer
- PayOfGrief[1]
- Conti (Ryuk)

1 In July, researchers concluded that DoppelPaymer was now operating under the name PayOfGrief.

Transformations of ransomware operators

In April, we witnessed a record number of ransomware attacks: they accounted for 45% of the attacks detected that month. BlackFog also noted the explosive growth in the number of ransomware attacks at the beginning of Q2.

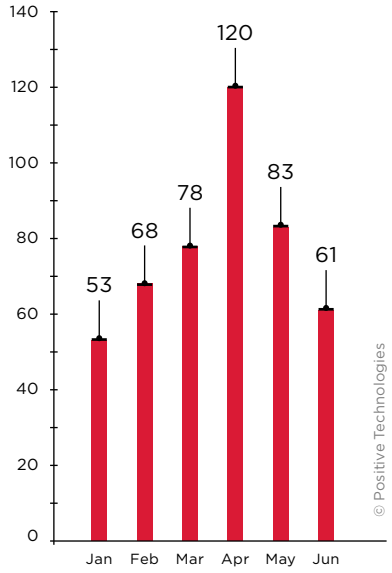

Figure 10. Number of ransomware attacks by month

The ransomware rampage culminated in an attack on the Colonial Pipeline, the largest U.S. pipeline system, which occurred in early May. Responsibility was claimed by DarkSide distributors. As a result, the company's network was encrypted, and the criminals became the owners of a large array of data. Colonial Pipeline Company was forced to suspend the operation of the fuel pipeline. Two days after the attack, the government declared a state of emergency in 17 states and the District of Columbia. The attackers requested $4.4 million for the decryptor.

Law enforcement agencies reacted quickly, and the DarkSide operators lost access to their servers in a matter of days. The criminals had no choice but to announce the termination of their activity. Other operators followed their example. Due to the mass exodus from the market, the boom of ransomware attacks observed in April began to gradually subside.

Another incident that attracted special attention of law enforcement agencies was the Babuk Locker attack on the District of Columbia Metropolitan Police. The Babuk Locker operators changed their attack approach after this incident. The new technique, called PayLoad Bin, entails stealing data without encrypting the victim's network infrastructure, followed by a ransom demand for nondisclosure of the stolen information. The ransomware operators claim that it has become difficult for them to control attacks by criminals who use their malware, for which reason victims can suffer repeat attacks, and tools provided for data recovery fail to work. The operators of Conti, LockBit, Black Kingdom, and REvil (Sodinokibi) ransomware have faced similar problems. After such publicity, it is difficult for them to demand high ransoms whilst boasting of an "impeccable reputation."

These incidents affected the activity of ransomware operators and distributors, and June saw a halving of such attacks. Some of them (for example, REvil operators) even changed their partner programs, introducing restrictions on the industry of target enterprises.

We also see disputes on dark web forums regarding the business of ransomware operators in general. Some forum users believe that ransomware operators should stop their current activities and find another way to earn money.

We think that ransomware operators responsible for high-profile attacks will find it hard to quit such a profitable business, and will instead wait for things to blow over before developing a new concept.

Dark web forums recently banned posts relating to ransomwares partner programs. This step, having further complicated the life of ransomware operators, could precipitate a change in their business structure.

One of these change scenarios may be the disappearance of so-called partners as a separate role—ransomware operators themselves will take over their tasks.

They will assemble teams of distributors and supervise them directly, rather than through an intermediary, and make more active use of access miners in their attack chains.

Clients on the access market

Increasingly often we hear that highly skilled attackers obtain initial access to target companies' networks independently, preferring to buy it on specialized dark web forums. For example, a CyberCX researcher reports that Avaddon distributors very often resort to access miners for assistance. The same method is used by the DarkSide distributors who attacked Brenntag.

In our research, we note that this trend in the initial access market is recalibrating the classical approach to attacker modeling. An outside intruder who gains initial access to a corporate network and a criminal who follows through with the attack once inside are completely different in terms of capability. In other words, attacks by highly skilled and motivated groups cannot be ruled out on the basis that "our company is of no interest to them."

Figure 11. Dark web ad selling access to various companies

Second-round attacks

Cybereason reports that 80% of organizations that paid a ransom to ransomware operators were attacked again; 46% of those who suffered second-round attacks believe that they were carried out by the same cybercriminals as the first time. Generally, if ransomware operators manage to cause significant damage to the IT infrastructure of a target company, this means that there are serious flaws in the company's security system. To reiterate, it is vital to conduct a thorough investigation to identify the points of compromise and vulnerabilities that the attackers exploited and make sure that the criminals did not leave any backdoors for themselves.

However, even if you have not been attacked a second time, there is no guarantee that you will recover the information lost during the attack. Indeed, 46% of respondents reported that after paying the ransom and using a decryptor, the information could not be restored.

Big entrance

Lots of new players appeared on the ransomware market in Q2, and quickly picked up steam. For example, the operators of Lorenz, Epsilon Red, PayOrGrief, Prometheus, and Xing Team. Each is remarkable in its own way. For example, Lorenz distributors sell access to the internal network of target companies along with stolen data. PayOrGrief distributors warn that their requested ransom amount is non-negotiable. Epsilon Red distributors actively exploit vulnerabilities on Microsoft Exchange servers in their attacks as the initial access vector. One of the victims, whose name is not disclosed, has already paid about $210,000 to Epsilon Red distributors.

Backups are at risk

In Q2 2021, we noticed a large number of attacks on QNAP network drives. These devices aggregate large amounts of data from companies and individuals and, in so doing, become of great value to attackers. QNAP devices were mainly attacked using ransomware, for example AgeLocker and eCh0raix.

During one of their campaigns, Qlocker operators used 7-Zip instead of their usual ransomware. The campaign targeted small and medium-sized businesses that used QNAP devices in their infrastructure, with an average ransom of $557—a readily affordable amount for the victim. As a result, the attackers "earned" $260,000 in five days. This ransomware is distributed by exploiting the vulnerabilities CVE-2020-2509, CVE-2020-36195, and CVE-2021-28799, which allow remote execution of 7-Zip, a built-in archiver.

Figure 12. Ad selling access to QNAP devices

If QNAP NAS appliances and Hybrid Backup Sync backup software are used in your company's infrastructure, update the version of Hybrid Backup Sync and install security updates for QNAP NAS. If you have a QNAP NAS with Roon Server version 2021-02-01 or earlier, we strongly recommend disabling the server and using QNAP NAS only on a local network without Internet access. Also follow general recommendations: do not use default port numbers, limit the number of attempts to enter credentials to connect to devices, and use strong passwords that comply with current password policies.

Check for updates

In general, attackers continue to exploit vulnerabilities in Microsoft Exchange Server (ProxyLogon vulnerabilities), which we discussed in more detail in our Q1 2021 report. This quarter, attackers exploited these vulnerabilities to distribute such RATs as Turian and Lemon_Duck, as well as the Epsilon Red ransomware, and the Monero miner.

If you still believe that the installation of security updates can be postponed on the grounds that the threat is not imminent, think again. On June 24, 2021, PT SWARM researchers published an exploit for the vulnerability CVE-2020-3580 in Cisco ASA, and on the same day, Tenable researchers reported that attackers had already begun to use this information to conduct attacks. Note that this vulnerability was detected a year earlier, in June 2020, and Cisco released the first security update in October 2020. Despite it being only a medium-severity vulnerability, attackers immediately began to exploit it in their attacks. From this, we can conclude that exploits for more serious vulnerabilities, once they appear, will also quickly come into play, so do not postpone the installation of security updates.

Attacks on governmental institutions

Compared to Q1 2021, the percentage of attacks on governmental institutions among all attacks on organizations increased from 12% to 20%. Most often, attackers use malware: the share of this method increased from 63% to 76% compared to the previous quarter.

The lion's share went to ransomware-based attacks (73% of all malware). Most commonly, these were Avaddon and DoppelPaymer (PayOrGrief) attacks. RATs, being the second most popular type of malware, were used in 16% of malware attacks. For example, BackdoorDiplomacy—both an APT group and a cross-platform RAT—was observed in attacks on the foreign ministries of various countries in Africa, the Middle East, Europe, and Asia. As an initial attack vector, the group used vulnerabilities on corporate network perimeters, including CVE-2020-5902 in F5 BIG-IP and ProxyLogon.

In May, a PT ESC threat analysis found an executable file named "List of allowed destinations to visit during annual vacations" with the .exe extension. During the analysis, this file turned out to be a loader written in Golang. It has functions for gaining persistence and can send encrypted information about the workstation to an attacker-controlled server. The server response is expected to contain a file to be run by the loader. The malware was named Tomiris after the functions in the code. Note that one variant of the loader was distributed from an IP address at which the government domains of a CIS country were located.

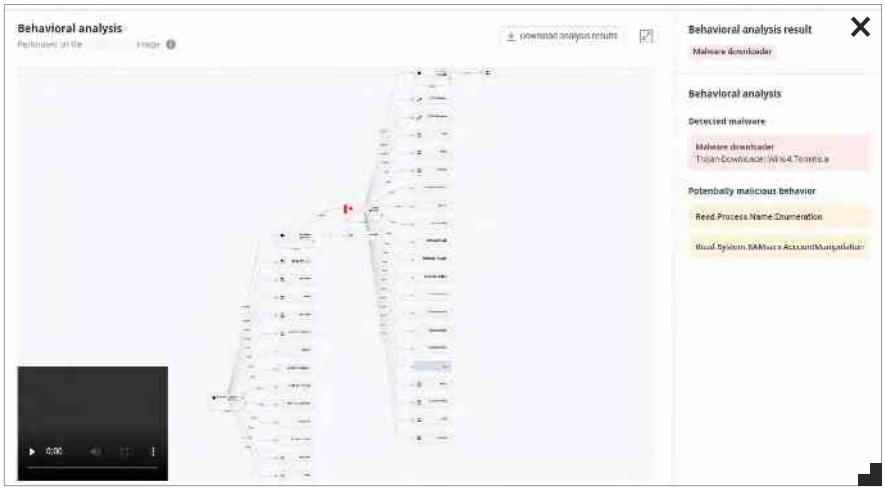

Figure 13. Detecting Tomiris using PT Sandbox

New cybersecurity threatscape for retail

The cybersecurity threatscape for retail has changed a lot over the past year. For example, we noted a decrease in the number of Magecart attacks. This was perhaps due to ransomware distributors' increased interest in retail and commerce: such malware was detected in six out of ten attacks. Operators of REvil, DarkSide, and ALTDOS were most commonly seen.

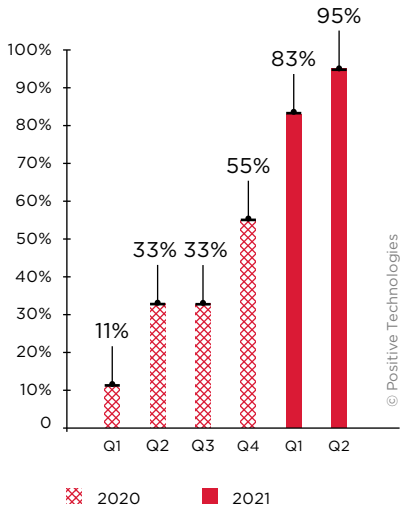

Figure 14. Percentage of ransomware attacks among malware attacks on retail and commerce

Previously, attackers' main purpose when targeting trading companies was to steal data: payment details, personal data, credentials. Now, however, with the increase in the number of ransomware attacks, criminals are increasingly pursuing direct financial gain, hoping to get large ransoms.

In Q2 2020, the percentage of malware attacks among other attack methods accounted for only 26%. In Q2 2021, this figure increased, standing at 59%. The percentage of social engineering attacks also increased from 36% in Q1 2021 to 53% in Q2.

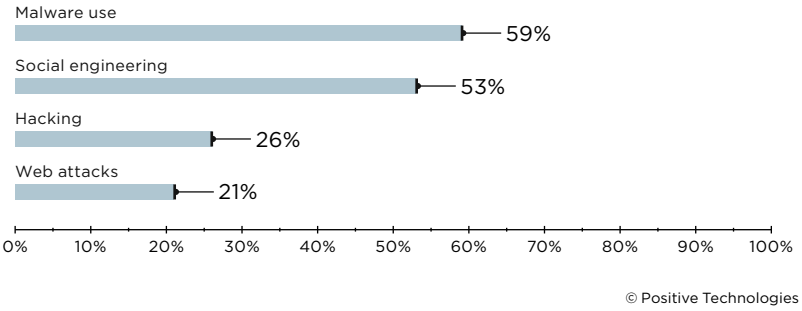

Figure 15. Methods of attacks on retail and commerce

In Q2, 21% of attacks were conducted by exploiting web vulnerabilities, for example, mass attacks on companies which used the Fancy Product Designer plugin on their e-commerce sites. Cybercriminals exploited a zero-day vulnerability (CVE-2021-24370) for bypassing authentication procedures to upload and execute arbitrary code, and gained full access to e-commerce sites of various companies. The attackers' goal was to obtain information about customers' orders, including their personal data. If you use the Fancy Product Designer plugin, we strongly recommend updating it to version 4.6.9.

Threats to industry

Manufacturing ranks second among other industries in terms of number of attacks. Compared to 2020, we see an increase in the share of hacking from 29% to 34% in Q2 2021. The share of malware attacks increased by 6 percentage points compared to Q1 2021, accounting for 73%.

Eight out of ten malware attacks were conducted by ransomware distributors. Most often, attacks on industrial companies involved REvil and DarkSide. The most high-profile attacks using them affected JBS Foods (a food manufacturer), Colonial Pipeline (largest pipeline system in USA), European subsidiaries of Toshiba, Brenntag (a distributor of chemicals), as well as one of Apple's suppliers, from which blueprints of new products were stolen. During the attack on Brenntag, DarkSide distributors stole 150 GB of data; the company paid a ransom of $4.4 million. JBS Foods also decided to pay a ransom of $11 million (in this case, to REvil operators).

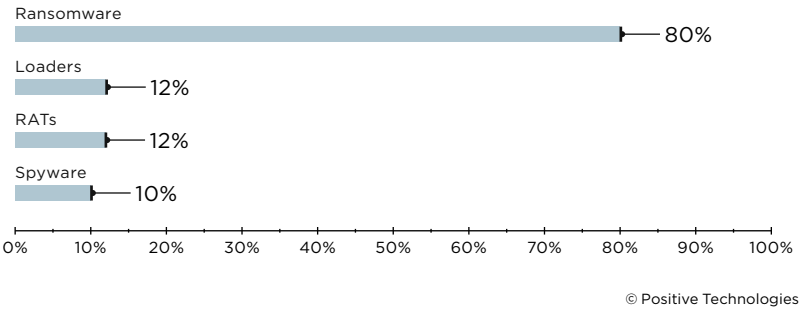

Figure 16. Types of malware in attacks on industry (percentage of malware-related attacks)

In Q2, PT ESC discovered B-JDUN, a new RAT used in attacks on energy companies. A notable feature of this backdoor is that it waits for a special identifier from the C2 before commencing interaction with it and executing commands. The value of this ID is set in the malware source code. If the ID sent by the server does not match, the malware interrupts the connection. The attack began with sending an email to victims with a document containing an exploit for a remote code execution vulnerability in Microsoft Office (CVE-2018-0798). To generate this document, the attackers used Royal Road, which is popular with Chinese groups.

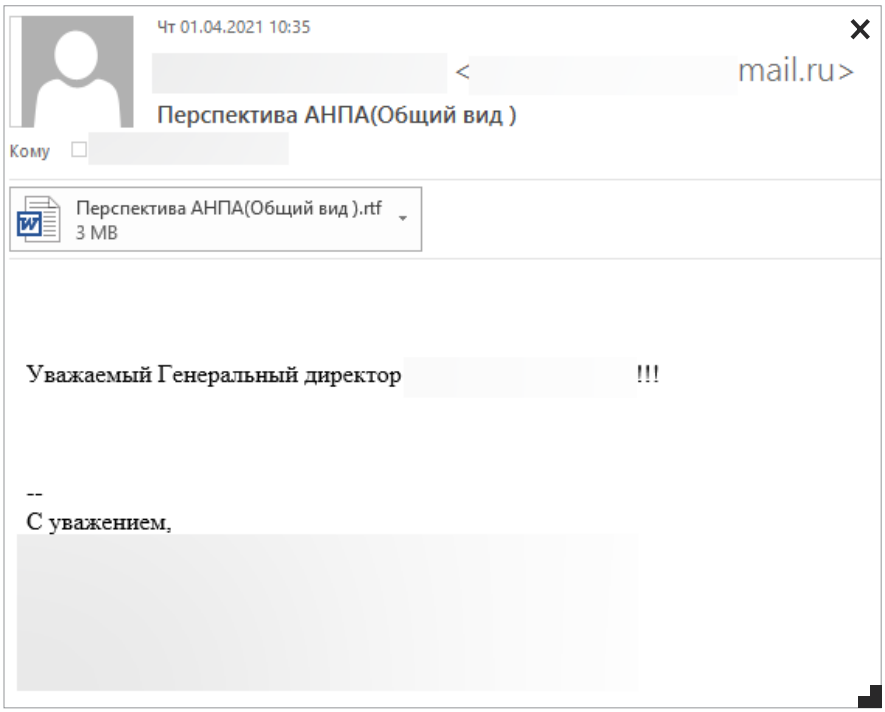

Figure 17. Phishing email from B-JDUN trojan distributors

The goal of approximately six out of 10 attacks on industry is data theft; this applies, for example, to the APT group RedFoxtrot, whose cyberespionage campaign was discovered by Recorded Future's Insikt Group. In its attacks, the group uses a whole variety of RATs: IceFog, ShadowPad, Royal Road, PCShare, PlugX, and Poison Ivy.

About the research

This quarterly report Positive Technologies addresses current relevant global IT security threats. The information provided draws on our own expertise, the outcomes of 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 hacker activity are unable to do a precise count of the number of threats. Our research, aimed at companies and individuals with a keen interest in information security, seeks to draw attention to cybercriminal methods and motives and highlight the main trends in the changing cyberthreat landscape.

This report counts each mass attack—for example, a phishing email sent to multiple addresses—as a single incident. Definitions of terms used in this report are available in the glossary on the Positive Technologies site.