Cybersecurity threatscape

Q2 2019

ptsecurity.com

Contents

Symbols used

Attack targets

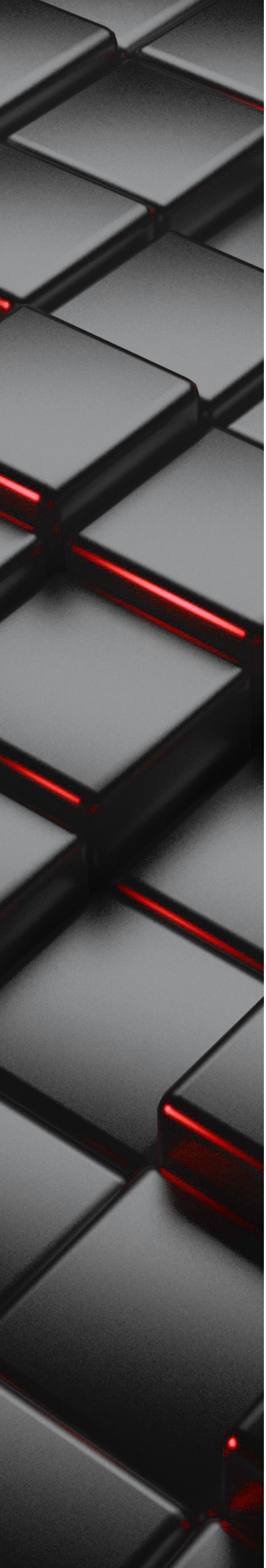
- Computers, servers, and network equipment
- Web resources
- Humans
- POS terminals and ATMs
- Mobile devices
- IoT

Attack methods

- Malware use
- Credential compromise
- Social engineering
- Hacking
- Web attacks

Victim categories

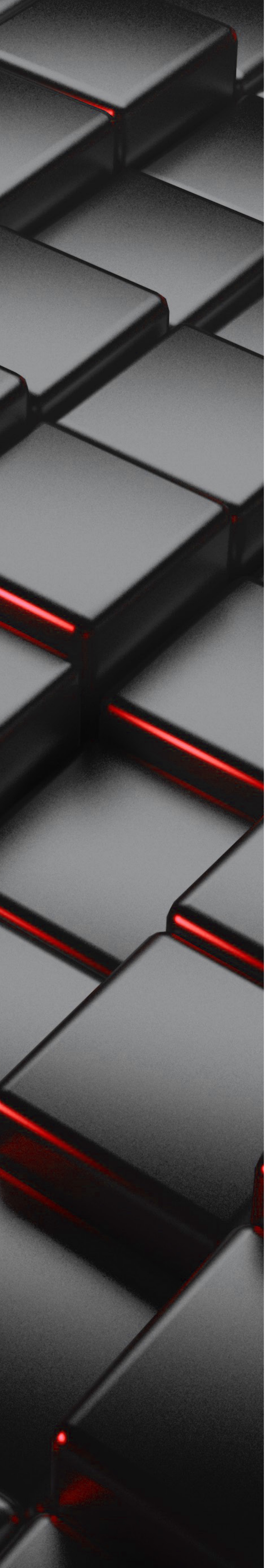
- Finance
- Government
- Healthcare
- Science and education
- Military
- Industrial companies
- Online services
- Hospitality and entertainment
- Transportation
- IT
- Retail
- Individuals
- Telecom
- Blockchain
- Other



What is a cyberthreat?

As computers have permeated all aspects of life, the benefits have been immense for many areas of the economy, including finance, retail, industry, healthcare, education, and science. Today, business and government policy alike are difficult to imagine without information technologies. But criminals have learned to use these systems for unlawful purposes. The result is a constant battle between cyberoutlaws and security professionals. To survive, criminals constantly refine their methods and tools, leaving greater numbers of digital threats in their wake.

By cyberthreat, we refer to a confluence of factors and conditions with the potential to compromise information security. In this report, we will consider cyberthreats from the standpoint of the actions performed by criminals in cyberspace with the intention to breach an information system for stealing data or money, or performing other acts with the potential to cause harm to governments, businesses, or individuals. Criminals may pursue these aims by targeting corporate IT infrastructure, workstations, mobile devices, other software and equipment, or humans themselves.



Trends and forecasts

Positive Technologies keeps monitoring the most important IT security threats. Cybercriminals are not slackening: they seize on news of fresh vulnerabilities, react to cryptocurrency price changes, and continue to refine their techniques.

Summarizing our findings from the second quarter of 2019, we note the following trends:

- The number of unique cyberincidents remains high, standing at three percent higher than in Q1 2019.
- Mass attacks are less common than targeted ones, which make up 59 percent of the total (12% higher than in Q1).
- Over half of all cybercrimes have data theft as their goal. Direct financial gain motivated 42 percent of attacks on individuals and 30 percent of attacks on organizations.
- In attacks on organizations, most stolen information consisted of personal data (29%). Individuals stood to lose their credentials and payment card information (44% and 34%, respectively, of all information stolen from individuals).
- Growth in the value of Bitcoin has inspired a revival of hidden mining.
- MageCart attacks are becoming more common. Experts have noted the increased presence of JS sniffers even on sites that do not handle payments.
- Malware infections have become more common among government targets (62% compared to 44% in Q1 2019). Last quarter, governments most frequently were hit by ransomware.
- IT companies often serve as a stepping-stone in supply chain attacks. Email addresses from hacked IT vendors are actively used by attackers in phishing messages.

Statistics

As in past quarters, data theft is the top goal of most cyberattacks. Direct financial gain, by contrast, is sought in 30 percent of attacks on organizations and in 42 percent of attacks on individuals. The high rate of financially motivated attacks on individuals owes to several factors: regular mass infections by adware (including on mobile devices), infection by miners and other malware on dubious sites, and extortion campaigns in which the victim is threatened with compromising information.

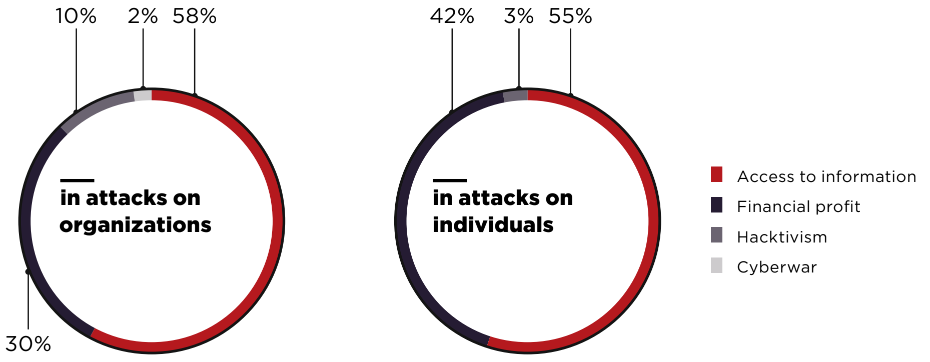


Figure 1. Attackers' motives

Personal data and credentials are the most frequent item of interest for attackers targeting organizations. This is no surprise, since companies can keep huge databases of clients' personal data and credentials. In addition, attackers may be interested in the credentials of the employees of the victim company.

Social media accounts can also be of value to an attacker, especially if an account is highly popular with a large number of subscribers. At the same time, users often fail to take basic precautions for securing their accounts. They use weak passwords or re-use passwords across sites, enter their passwords without making sure of site authenticity, and give out information that could help to guess their password. These factors explain the high rate of stolen credentials (44%) among attacks on individuals. For instance, computer game fans form a high-risk category. In Q2, attackers lured Steam users to websites with the false promise of a free new game, as long as the users would enter their Steam credentials first. Similar ruses can also be found on gaming forums. A number of websites distributed the TurtleCoin cryptocurrency mining Trojan, which was disguised as a ZIP file supposedly containing cheat codes.

Since payment cards and financial details are usually protected cryptographically, attackers' method of least resistance is to trick people into disclosing this information via social engineering. Among attacks on individuals, 34 percent of stolen data consists of payment card information.

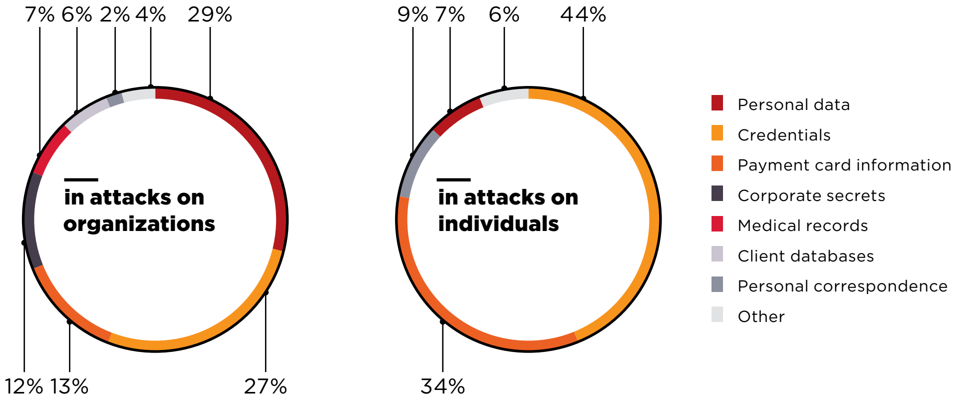


Figure 2. Types of data stolen

In Q2 2019, the share of targeted attacks climbed significantly compared to the previous quarter (59% in Q2 vs. 47% in Q1). The share of cyberincidents targeting individuals was 24 percent. Among organizations (see Figure 3), the most frequent targets were governments, industrial companies, healthcare institutions, banks, and other financial entities. In Q2 we saw supply chain attacks on major IT companies with clients in a variety of sectors, meriting a closer look in our discussion of IT attacks.

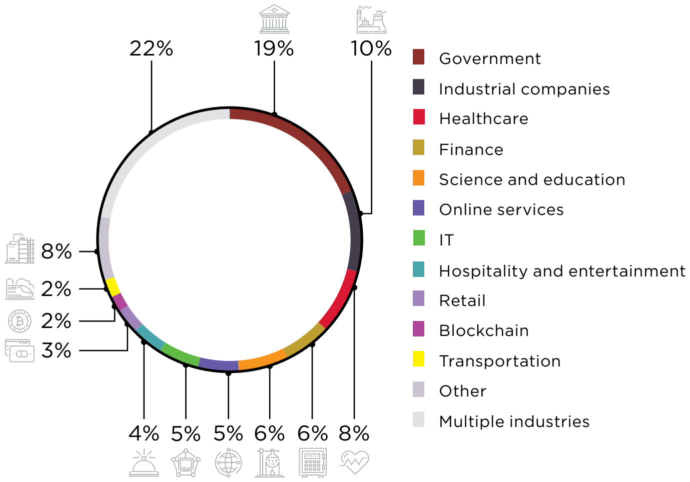


Figure 3. Victim categories among organizations

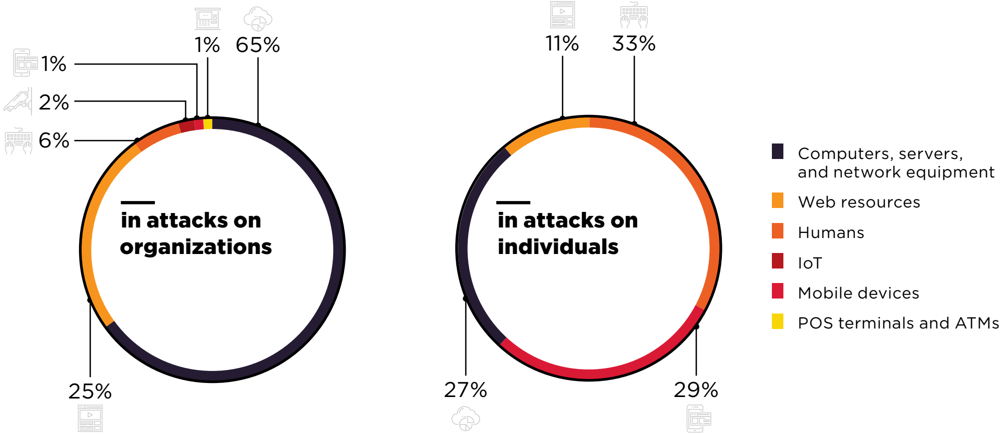


Figure 4. Attack targets

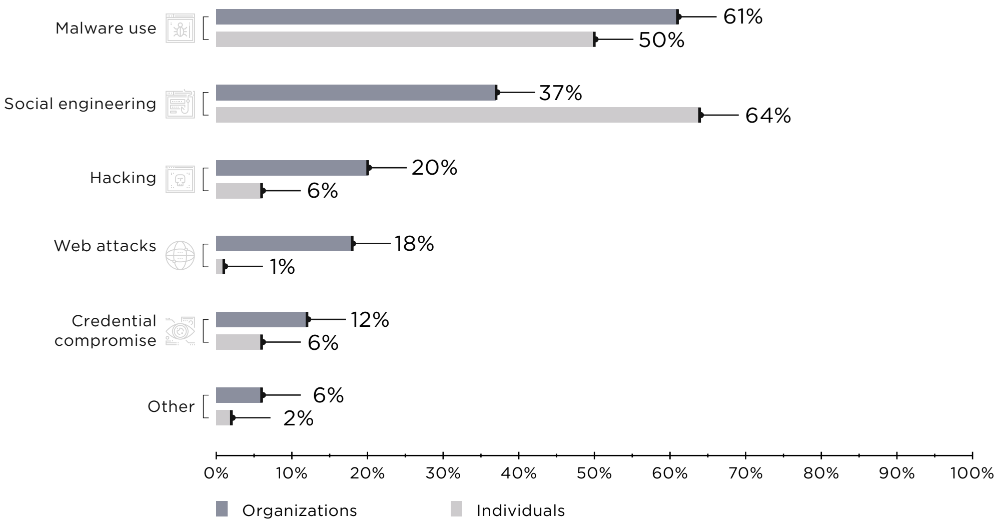


Figure 5. Attack methods

Per-industry classification of cyber-incidents by motive, method, and target

		Industry													
		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Science and education	Retail	Transportation	Blockchain	Other	Multiple industries	Individuals
	Total	**53**	**16**	**27**	**22**	**14**	**10**	**14**	**17**	**9**	**5**	**5**	**21**	**60**	**84**
Target	Computers, servers, and network equipment	37	14	26	11	5	4	10	8	2	3	4	15	39	23
	Web resources	9	1	1	5	8	5	4	9	7	2		5	13	9
	Humans	5			6	1						1	1	2	28
	Mobile devices	2												1	24
	POS terminals and ATMs		1				1								
	IoT													5	
Method	Malware use	33	14	26	9	2	2	6	7	2	2	1	13	48	42
	Social engineering	22	11	21	8	1	1		3	2	1	1	9	15	54
	Credential compromise	6		1	4	2	4	3	3	1			3	7	5
	Hacking	6	1	1	1	2	2	5	1		1	4	1	29	5
	Web attacks	6		2	2	8	3	3	5	6	1		4	9	1
	Other	7	1			2		1	1			1	1	1	2
Motive	Financial profit	19	6	1	6	2	1	5	1	1	1	4	8	28	35
	Access to information	25	10	25	16	10	9	9	13	8	2	1	7	24	46
	Hacktivism	6		1		2			3		2		5	8	3
	Cyberwar	3											1		

Darker colors indicate a higher proportion of attacks in a particular industry

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

Attack number

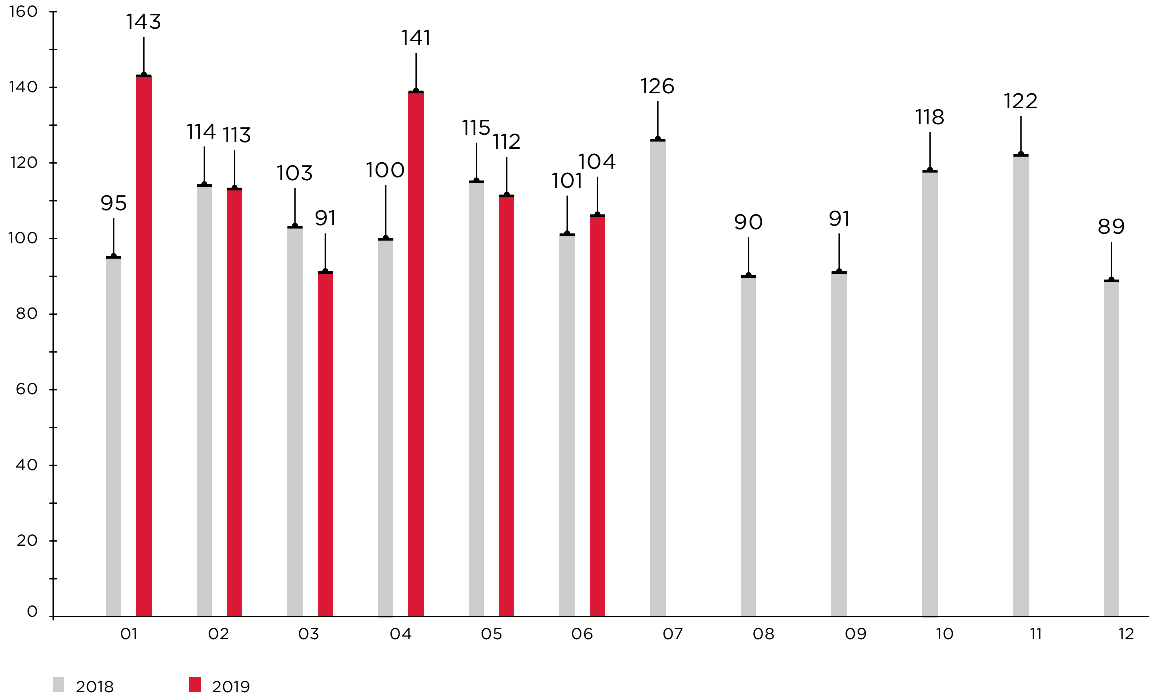


Figure 6. Number of incidents per month in 2018 and 2019 (1 = January, 12 = December)

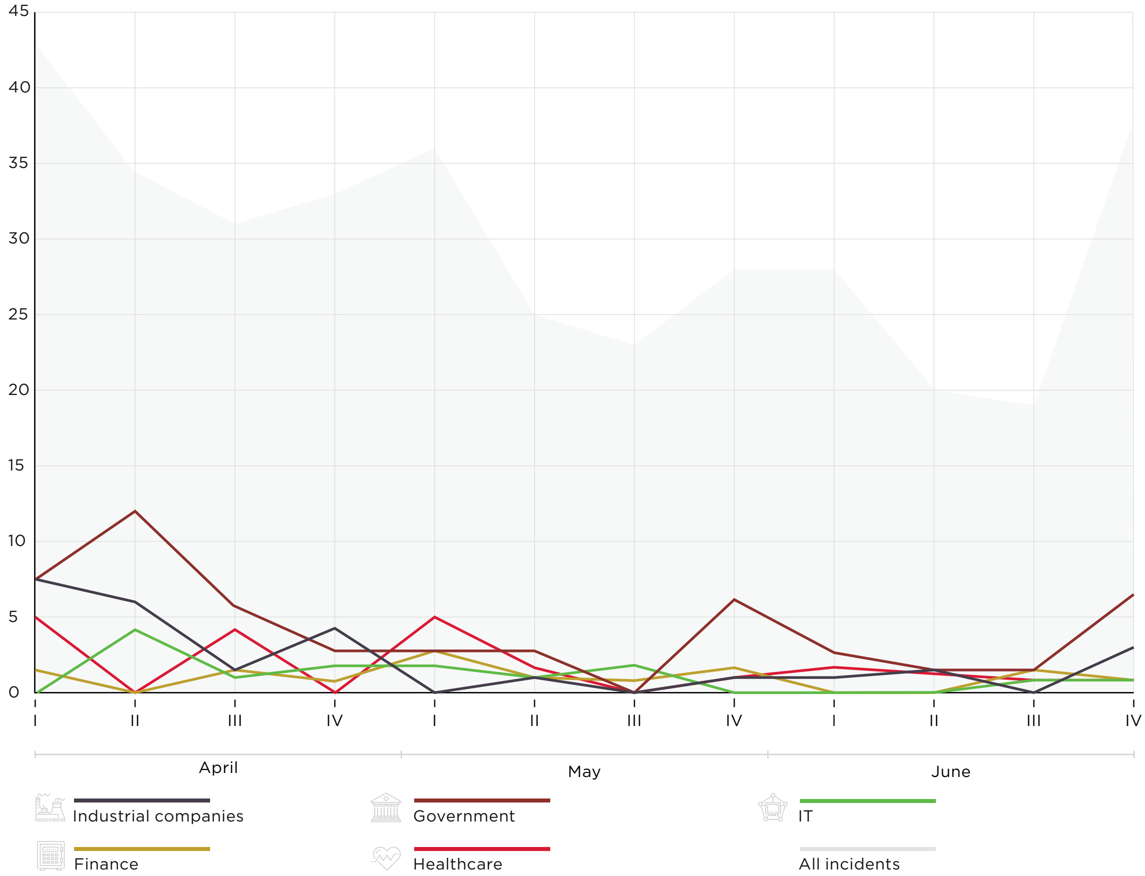


Figure 7. Number of incidents in Q2 2019 (by week)

Attack methods

We will take a closer look at each attack method and indicate which targets and industries were most affected.

Malware use

Multifunctional Trojans constitute a growing share of attacks. For example, the DanaBot modular Trojan we wrote about in Q1 now has ransomware capabilities. By comparison, another well-known piece of ransomware, GandCrab, wound down and its operators announced the end of the malicious campaign. Several weeks after reports indicated the end of development of the ransomware, security researchers disclosed they had obtained access to the GandCrab servers. With the help of the encryption keys stored there, it was possible to make a decryption program for the latest version of GandCrab so that victims could recover their encrypted files.

Despite these events, the rate of ransomware attacks remains high. Creating a simple strain of ransomware does not even require custom code development. Most new ransomware is very similar to what already exists. Instead of developing code from scratch, cybercriminals can now just acquire ready-to-use code or pay for a subscription (ransomware as a service) on the darkweb. So even with minimal upfront investment, ransomware can bring a sizable income.

Reports have periodically appeared since April 2019 of attacks by new Sodinokibi ransomware. At least three IT service providers have fallen victim to it. Cybercriminals have used remote administration tools (Webroot and Kaseya) to install ransomware on the systems of clients of the compromised IT service providers. But Sodinokibi has a few other tricks up its sleeve, in addition to supply chain attacks. It also is spread via vulnerabilities in Oracle WebLogic Server and in phishing messages.

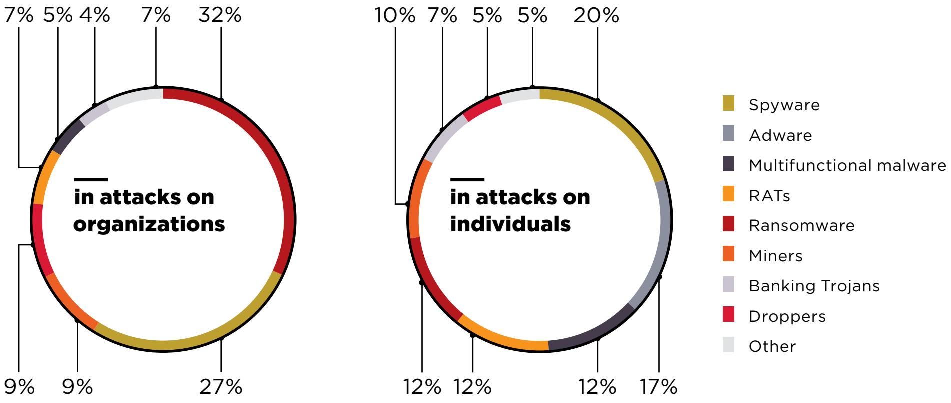


Figure 8. Types of malware

Email continues to be the most popular method for delivering malware. In Q2, experts noticed an uptick in cases of Trojans being spread in the ISO disk image format. This trick has been used by AgentTesla, LokiBot, and NanoCore. ISO images are often not scanned by antivirus software, since they may be whitelisted. One giveaway is the file size: a malicious disk image will be smaller than 2 megabytes, while a legitimate one will usually be much larger.

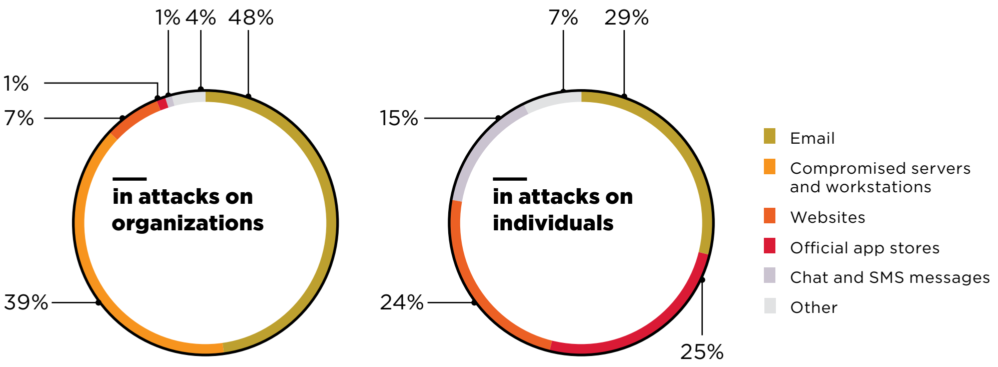


Figure 9. Malware distribution methods

We saw renewed criminal interest in cryptojacking in Q2 2019. With the Bitcoin price rising steadily, attackers continue to develop software for stealthy mining. Researchers at Sucuri discovered a miner with improved persistence mechanisms: a special cron job (which is run periodically according to a schedule) allows resuming mining even if the main malware module has been detected and removed from the infected system.

Attackers widely distributed the AZORult infostealer in the second quarter. For instance, the experts at the Positive Technologies Expert Security Center (PT ESC) in early April noted that the RTM group had started using AZORult instead of Pony. In addition, the AZORult Trojan spreads via websites under the guise of various utilities (such as the G-Cleaner system optimizer or Pirate Chick VPN client).

Social engineering

In Q2, criminals made active use of Azure App Service for different types of fraud involving social engineering. Azure can be used for quickly deploying phishing pages with fake login forms, as well as for creating fake Microsoft technical support pages with popups stating the visitor's computer has been infected by a non-existent virus. In addition, attackers send emails prompting to download a file after logging in via a fake form, which is hosted on Azure Blob Storage. The scale and success of this scam is caused in part by the domain (windows.net) and valid SSL certificate (belonging to Microsoft). But such scams are hardly new. Instructions are available to users with the details of how to automatically block such phishing emails.

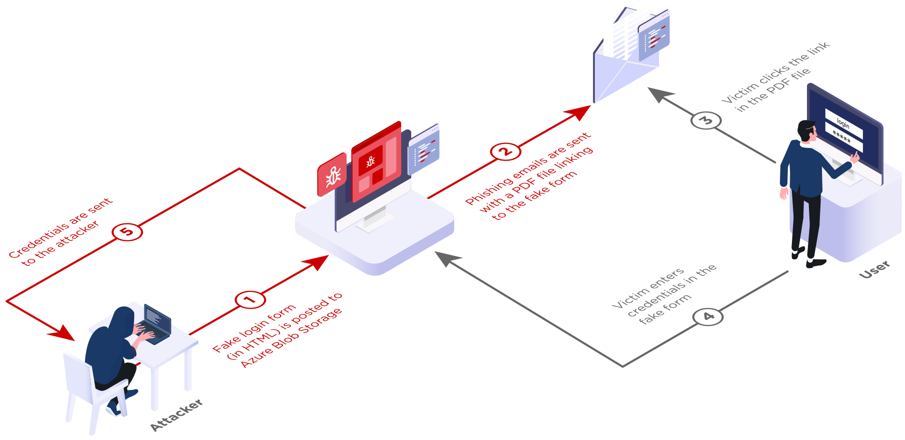

1
Fake login form (in HTML) is posted to Azure Blob Storage
2
Phishing emails are sent with a PDF file linking to the fake form
3
Victim clicks the link in the PDF file
4
Victim enters credentials in the fake form
5
Credentials are sent to the attacker
Attacker
User
login

Figure 10. Theft of Office 365 credentials with use of Azure Blob Storage

As noted already, the strong increase in Bitcoin value in Q2 sparked a return of interest in the cryptocurrency, including among the criminal community. In one iteration, fraudsters used a seemingly timeless scheme. They claimed to be famous people or organizations offering cash prizes, with a catch: the "winner" must first transfer a small amount of money for verification purposes. In this case, the cryptocurrency "prizes" were supposedly being handed out by John McAfee and Elon Musk.

YouTube's popularity has made video channels an attractive place to put malicious links. In one fraud campaign, viewers were shown links (in the video description) to materials allegedly teaching how to generate bitcoins for free. But in reality, clicking the link initiated download of the Qulab infostealer. Another such campaign used YouTube to spread the njRAT Trojan.

Hacking

The most discussed security issue of Q2 was BlueKeep (CVE-2019-0708), a critical Remote Code Execution (RCE) vulnerability in the RDS service in older versions of Windows. Although Microsoft released a patch on May 14, many computers around the world remain at risk. Attackers are actively probing for vulnerable hosts and developing exploits.

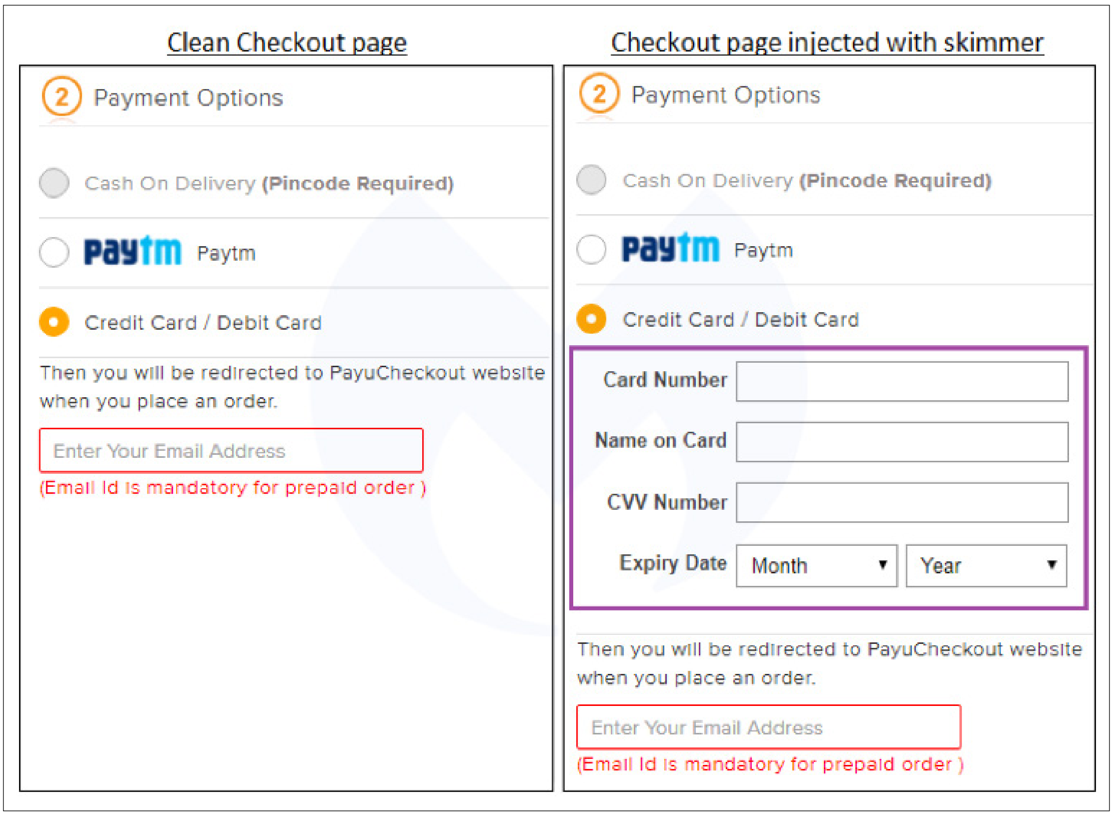
BlueKeep could be exploited to spread malware on the scale of WannaCry, which is why installing Windows updates is so important

Hackers are making use of a vulnerability in the Exim mail server (CVE-2019-10149) to remotely run OS commands with administrator privileges. One criminal group uses the vulnerability to place a backdoor on target systems, by downloading shell scripts to mail servers and adding an SSH key to the root account. In addition, criminals illegally install cryptocurrency miners on vulnerable servers. The vulnerability was fixed by the Exim developers in February 2019. But release of a vendor update often fails to solve the problem outright. Delays in installing updates give hackers a chance to successfully exploit even vulnerabilities that are five years old.

Throughout Q2, attackers searched for publicly available Docker API instances by scanning the Internet for hosts with open port 2375. Misconfigured Docker containers are used for a wide array of purposes. After discovering a working container, for example, hackers might install Dofloo on it. This is the same Trojan placed by attackers on systems running Atlassian Confluence. To do so, they exploit vulnerability CVE-2019-3396. Dofloo uses the victim's resources to perform DDoS attacks and hidden cryptocurrency mining.

Web attacks

In Q2, web vulnerabilities were exploited in 18 percent of attacks on organizations. The wave since Q1 of attacks on payment sites continues to build. MageCart attacks with JS sniffers (malicious scripts designed to steal payment card information) hit Forbes, Puma, and numerous online stores. The criminals regularly update their malicious scripts. The danger of JS sniffers is that the threat may stay unnoticed by users, since the malicious scripts are invisible to them. But one of the new methods used by MageCart to steal data may offer a way for attentive users to spot the threat. The attackers inject a form for entering card information into site pages. But normally this interface should be shown only after the user is redirected to the secure page of the payment provider. Entering card information twice (first on the site itself and a second time on the payment provider's page) should raise red flags among users.



Clean Checkout page

(2) Payment Options

○ Cash On Delivery **(Pincode Required)**

○ Paytm Paytm

● Credit Card / Debit Card

Then you will be redirected to PayuCheckout website when you place an order.

Enter Your Email Address

(Email Id is mandatory for prepaid order)

Checkout page injected with skimmer

(2) Payment Options

○ Cash On Delivery **(Pincode Required)**

○ Paytm Paytm

● Credit Card / Debit Card

Card Number	
Name on Card	
CVV Number	
Expiry Date	Month ▾ Year ▾

Then you will be redirected to PayuCheckout website when you place an order.

Enter Your Email Address

(Email Id is mandatory for prepaid order)

Figure 11. MageCart form for stealing payment card information

In Q2, Malwarebytes Labs discovered MageCart JS sniffers in libraries stored by site developers in private Amazon CloudFront CDN repositories. In addition, since April criminals have been injecting MageCart sniffers into files on Amazon S3, leading to compromise of 17,000 sites. Since not all compromised sites show a form for entering card information, experts gauge it likely that the hackers are using JS sniffers for so-called mass spray and pray attacks.

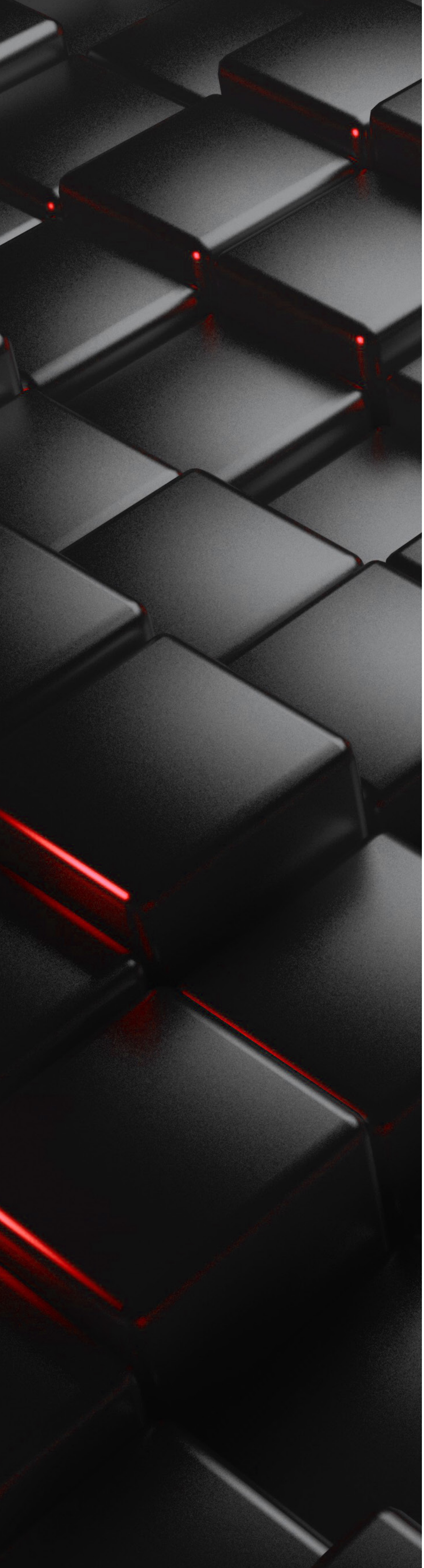
Not all of the sites targeted are used for online purchases. In June, the Social Engineered blog, developed on MyBB, was hacked. Attackers took advantage of an XSS vulnerability in MyBB that had become public several days prior. The attackers thus were able to obtain 55,000 sets of credentials and personal messages of forum users.

Credential compromise

Weak passwords remain a major security threat. Passwords for 300 employees of Ethiopia's Information Network Security Agency, charged with overseeing information security, proved to be weak and were subsequently hacked and posted online. Out of 300 passwords, 142 were "p@$$w0rd" and another 60 were "123".

Credential stuffing (attempts to log in to a system using sets of credentials stolen elsewhere) remains frequent. Such attacks resulted in the breach of around half a million user accounts for the Uniqlo and GU online stores.

Q2 also marked attacks by the new GoldBrute botnet to bruteforce RDP passwords. Over 1.5 million Windows devices have already been attacked. While the objectives of the attackers remain unclear, they likely include selling the stolen credentials on the darkweb. Mass attacks on weak credentials are a common occurrence for IoT devices as well. Silex malware, which attempts to log in to IoT devices using standard sets of credentials, made the news in June. As soon as Silex successfully guesses a password, it disables the device. Over 2,000 devices have incurred Silex's destructive power so far.



Victim categories

Here we will consider attacks on specific industries of interest during Q2 2019.

Government

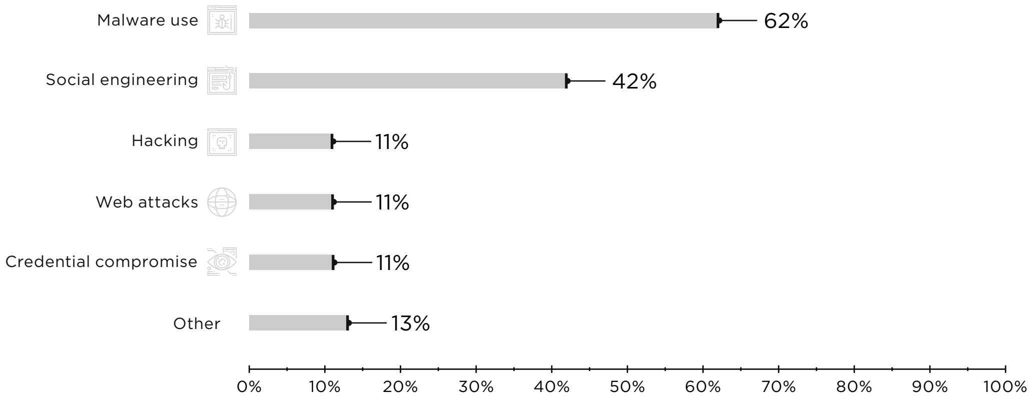


Figure 12. Government: attack methods used in Q2 2019

In Q2 2019, we saw a sharp rise in the share of malware in attacks on government organizations (62% in Q2 vs. 44% in Q1).

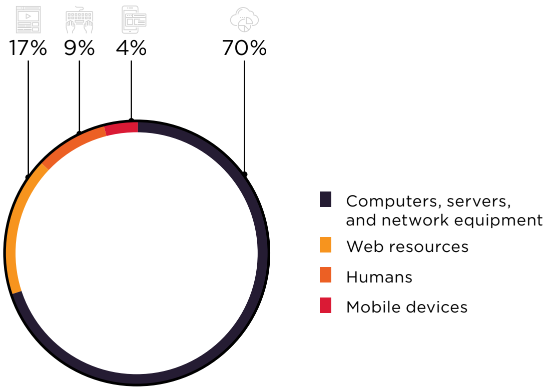


Figure 13. Attack targets

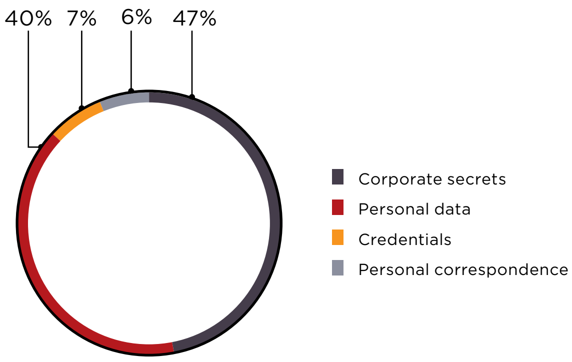


Figure 14. Data stolen

Most frequently, governments fall victim to ransomware. In the U.S. in early May, the entire IT infrastructure of Baltimore was inoperative for several weeks due to RobinHood ransomware. City authorities estimated losses at over $18 million. Baltimore was not RobinHood's first victim: in April, the same ransomware infected the systems of the city of Greenville, also in the U.S.

Faced with the threat of an entire city government's IT systems going down, authorities in several cases have had to give in to demands and pay a ransom. This is particularly the case in small cities with poorly developed IT infrastructure. The city council of Riviera Beach, Florida, unanimously voted to pay a ransom of 65 bitcoins (approximately $600,000) since the city lacked the backups necessary to get its systems running again.

Another Florida city, Lake City, was targeted by ransomware in early June. City information systems were infected as part of the large Triple Threat malicious campaign first described in April by Cybereason. The Triple Threat campaign received its name because of its three-part payload: phishing messages delivered three different Trojans (Emotet, TrickBot, and Ryuk) to victim computers. Although infected devices were disconnected from the city network as soon as possible, this was not fast enough to save most phone and mail systems. Lake City decided to meet the attackers' demand of 42 bitcoins (approximately $530,000), after which the city's IT director was fired.

Yet another Florida city, Key Biscayne, came in the sights of ransomware attackers in late June. But in this case the city refused to pay up.

Governments have suffered due to phishing as well. In one such attack in Canada, the city of Burlington lost $503,000.

Government-related websites continue to attract ill-wishers. A hack of three websites of the FBI National Academy Association resulted in posting of personal data for around 4,000 federal agents and law enforcement personnel online.

Industrial companies

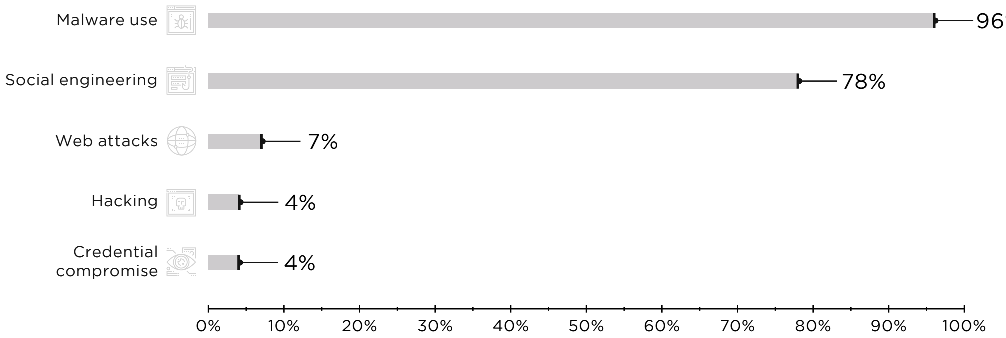
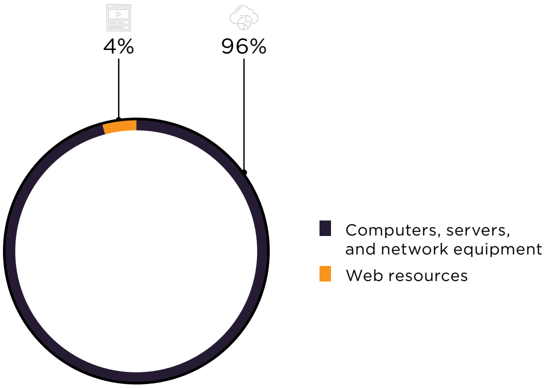


Figure 15. Industrial companies: attack methods used in Q2 2019



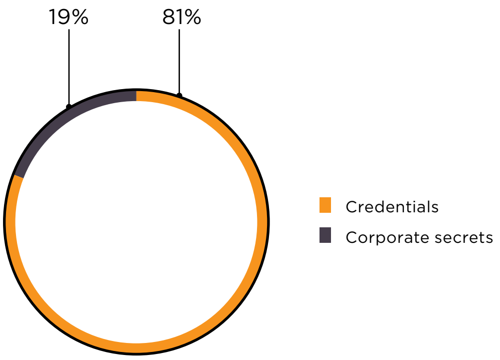


Figure 16. Attack targets

Figure 17. Data stolen

Almost all Q2 2019 attacks on industrial companies (96%) involved use of malware. The RTM group is actively attempting to penetrate the internal IT infrastructure of industrial companies. PT ESC detected 26 malicious mailings by the group during the second quarter. Recipients included financial institutions and over a dozen industrial entities in Russia and the CIS. All the messages were written in Russian and tend to have a financial focus, claiming to include invoices, accounting paperwork, or related documents, requesting to verify the documents, sign them, or make payment.

The RTM Trojan is classified as spyware: it steals credentials, records video, takes screenshots, and exfiltrates them to the attackers' server. Of interest, in June the group changed the method for getting the IP address of its command-and-control (C2) server. Now the address is obtained with the help of logic operations (AND and a right rotation) on the amount of a transaction received by a certain Bitcoin wallet.

Ransomware continues its assault on industry. Two such victims in Q2 included Aebi Schmidt, manufacturer of equipment for airports, and ASCO, a major aviation parts supplier.

Hackers frequently target the websites of industrial companies. Attackers placed the Emotet Trojan on the website of Uniden. The site of Petrobangla, an oil and gas company, was hacked twice in the same day. In the latter case, the attacker claimed to be pointing out security issues to the site owners.

Healthcare

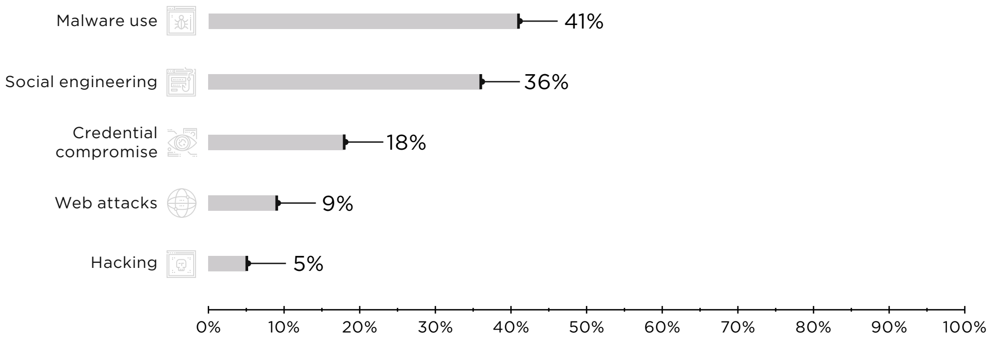
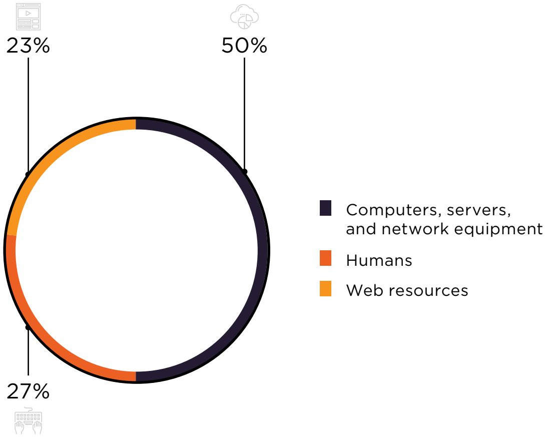


Figure 18. Healthcare: attack methods used in Q2 2019



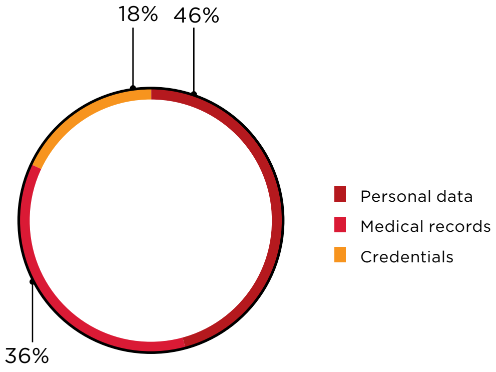


Figure 19. Attack targets

Figure 20. Data stolen

Business-disrupting malware is especially dangerous in the healthcare sector: such incidents have the potential to cause major harm to both institutions and patients. In April 2019, ransomware struck JFJ Eyecare, encrypting the personal data of patients.

Healthcare employees are the frequent victims of phishing attacks. One healthcare employee in Nova Scotia (Canada) fell for a message, supposedly from an IT department employee, requesting to send account credentials to prevent a freeze. The attacker succeeded in getting the employee's username and password, putting data for 3,000 patients at risk.

When targeting healthcare organizations, attackers can be interested not only in patients, but in employees as well. For example, for $500, it is possible on the darkweb to purchase sets of physician identity documents: medical diplomas, board recommendations, and medical licenses.

Financial institutions

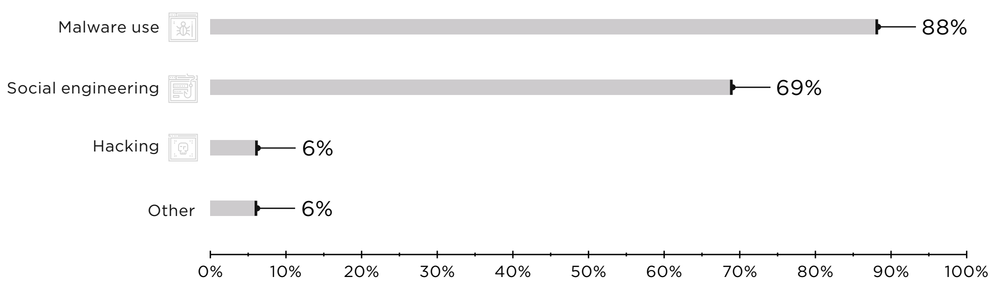
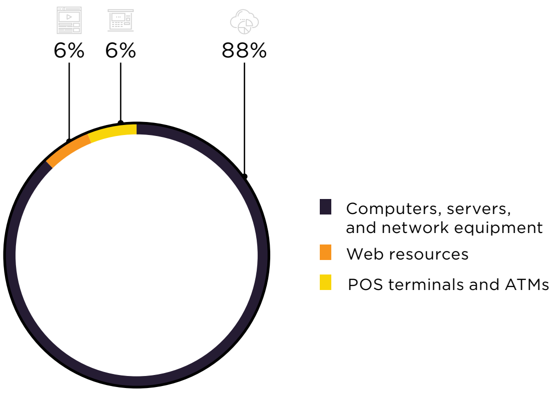


Figure 21. Financial institutions: attack methods used in Q2 2019



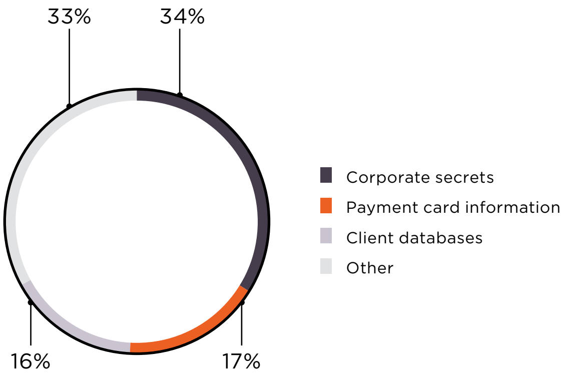


Figure 22. Attack targets

Figure 23. Data stolen

Several groups targeted financial institutions in phishing mailings in Q2. The Cobalt group continues its attacks, of which PT ESC noted two in the outgoing quarter. In the second attack, the group switched from tools it had used since late last year (COM-DLL-Dropper and a JavaScript backdoor) to using a modified version of CobInt, which had been in their arsenal already from August to November 2018.

In June, PT ESC detected a phishing mailing from the Silence group disguised as being from a bank client.

In May, PT ESC discovered phishing messages with encrypted archives containing an LNK file. When run on the victim's computer, the LNK file downloads a PowerShell script, which collects system information and sends it to the attackers. Based on this, the attackers chose which malware to install on the compromised computer. Network infrastructure allows us to identify this criminal group as FinTeam.

In Bangladesh, at least three banks were struck by hackers in Q2 2019: Dutch Bangla Bank Limited (DBBL), NCC Bank, and Prime Bank. According to reports, the cyberattack on DBBL resulted in losses of $3 million. Representatives of the other two banks reported no financial losses.

IT

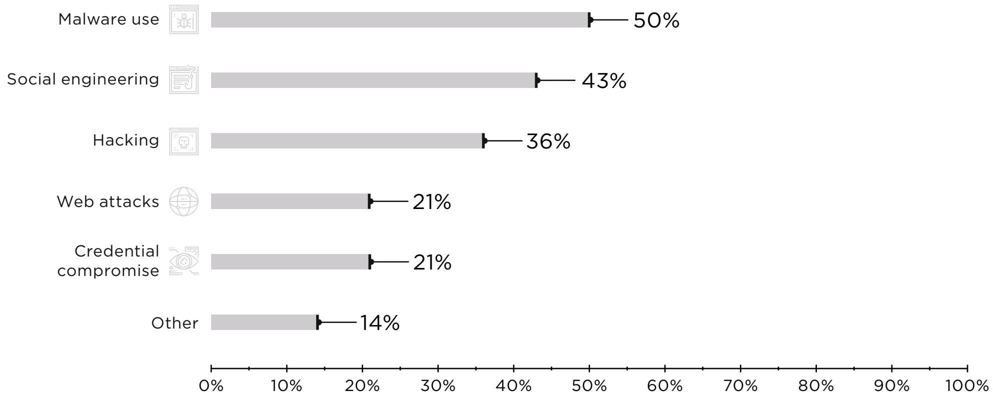


Figure 24. IT: attack methods used in Q2 2019

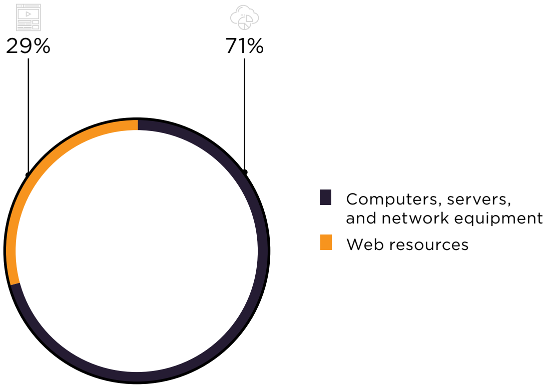


Figure 25. Attack targets

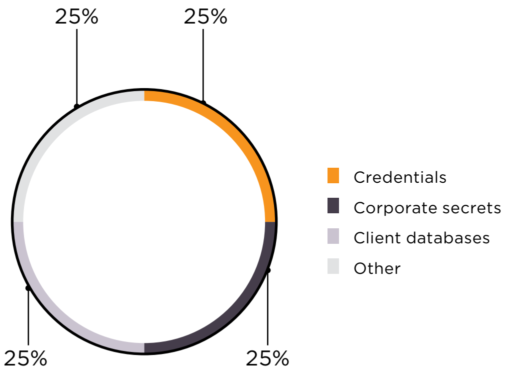


Figure 26. Data stolen

In the first half of April, vulnerabilities in an out-of-date Jenkins version yielded access to the infrastructure of Matrix, the decentralized messaging platform developer. Attackers' haul included unencrypted messages, hashes of user passwords, and access tokens.

IT companies are frequent victims of supply chain attacks. Hackers broke into the systems of Wipro, one of the largest Indian IT service providers with clients in the healthcare, telecom, and finance industries. As the result of successful phishing attacks on Wipro infrastructure, over a dozen of the company's clients received emails (seemingly sent by Wipro employees) with malicious attachments. According to Flashpoint, which performed investigation of the incident, one of the motivations for the attackers was gift card fraud.

In mid-May, a supply chain attack hit cloud provider PCM. The attackers obtained access to the administrator account used at PCM to manage clients' Office 365 accounts. In this case, too, the motivation for the theft included gift card fraud.

What companies can do to stay safe

Use proven security solutions

- Implement a system for centralized management of updates and patches. To prioritize update plans correctly, the most pressing security threats must be taken into account.

- Install antivirus software with a sandbox for dynamically scanning files and the ability to detect and block threats such as malicious email attachments before they are opened by employees. Ideally, antivirus software should simultaneously support solutions from multiple vendors and have the ability to detect signs of hidden or obfuscated malware, as well as block malicious activity across diverse data streams: email, web traffic, network traffic, file storage, and web portals. The solution must not only check files in real time, but also automatically analyze files that have already been checked; this will allow detecting new threats when signature databases are updated.

- We also recommend using SIEM solutions for timely detection and effective response to information security incidents. This will help identify suspicious activity, prevent infrastructure hacking, detect attackers' presence, and enable prompt measures to neutralize threats.

- Use automated software audit tools to identify vulnerabilities.

- Use web application firewalls as a preventive measure to protect websites.

- Implement systems allowing deep network traffic analysis in order to detect advanced persistent threats in real time and in saved traffic. Using such solutions will allow you to detect previously unnoticed attacks and monitor network attacks in real time, including use of malware and hacking tools, exploitation of software vulnerabilities, and attacks on the domain controller. Such an approach quickly identifies attackers' presence in the infrastructure, minimizes the risk of loss of critical data and disruption to business systems, and decreases the financial damage caused by the attackers.

- Employ specialized anti-DDoS services.

Protect your data

- Encrypt all sensitive information. Do not store sensitive information where it can be publicly accessed.

- Perform regular backups and keep them on dedicated servers that are isolated from the network segments used for day-to-day operations.

- Minimize the privileges of users and services as much as possible.

- Do not use identical username–password combinations for multiple systems.

- Use two-factor authentication where possible, especially for privileged accounts.

Do not allow weak passwords

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

Monitor and stay current

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

Keep clients in mind

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

How vendors can secure their products

- Follow all of the recommendations given in the section on corporate security.
- Implement a secure development lifecycle (SSDL).
- Regularly audit the security of software and web applications, including source-code analysis.
- Keep web servers and database software up to date.
- Do not use libraries or frameworks with known vulnerabilities.

How users can avoid falling victim

Invest in security:

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

Protect your data:

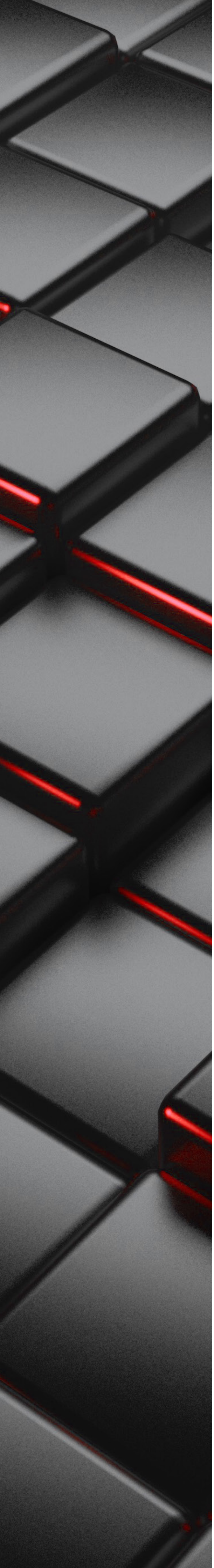
- Back up critical files. In addition to storing them on your hard drive, keep a copy on a USB drive, external disk, or a backup service in the cloud.
- Use an account without administrator privileges for everyday tasks.
- Use two-factor authentication where possible, such as for email accounts.

Do not use weak passwords:

- Use complex passwords consisting of at least eight hard-to-guess letters, numbers, and special characters. Consider using a password manager to create and securely store passwords.
- Set a different password for each site, email address, or other account that you use.
- Change all passwords at least once every six months, or even better, every two to three months.

Be vigilant:

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



About the research

In this 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.

Any particular mass incident, such as a phishing campaign using malware, is considered in this report as a single unique information security threat. Each event is characterized by the following parameters:

- **Attack target** is the target of destructive actions by cybercriminals. In cases when social engineering is used to obtain information directly from an individual, client, or employee, the attack target is "Humans" On the other hand, when social engineering is part of an attempt to place malware on corporate infrastructure or on the computer of an individual, the attack target is "Computers, servers, and network equipment."
- **Attack motive** is the ultimate goal of cybercriminals. If an attack results in theft of payment card information, the motive is "data theft."
- **Attack methods** are a set of techniques used to achieve a goal. An attacker can perform reconnaissance, detect vulnerable network services available for connection, exploit vulnerabilities, and get access to resources or information. For the purposes of this report, this process is referred to as "hacking." Credential compromise and web attacks are put in separate categories for greater granularity.
- **Victim categories** are the economic sectors in which the attacked companies operate (or individuals, if the attack was indiscriminate). For example, the "Hospitality and entertainment" category includes companies providing paid services, such as consulting agencies, hotels, and restaurants. The "Online services" category includes platforms where users can fulfill their needs online, for example ticket and hotel aggregator websites, blogs, social networks, chat platforms and other social media resources, video sharing platforms, and online games. Large-scale cyberattacks affecting more than one industry (most often, malware outbreaks) have been placed in the "Multiple industries" category.

We believe that in most cases cyberattacks are not made public because of reputational risks, which makes it hard even for companies involved in incident investigation and analysis of hacking groups to calculate the precise number of threats. 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.

About Positive Technologies

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

ptsecurity.com
info@ptsecurity.com