POSITIVE TECHNOLOGIES

Cybersecurity threatscape

Q1 2019

Contents

Symbols used

Attack targets

- Infrastructure
- Web resources
- Users
- 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
- Industrial companies
- Military
- Online services
- Hospitality and entertainment
- Transportation
- IT
- Retail
- Individuals
- Telecom
- Blockchain
- Other

Trends and forecasts

Positive Technologies keeps monitoring the most important IT security threats. Experts all over the world are working to combat cybercriminals, fueling an arms race in which hackers continue to refine their tools. In early 2019, companies in a wide range of industries suffered from cyberattacks.

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

- The number of unique cyberincidents continued to grow, exceeding the equivalent year-ago period (Q1 2018) by 11 percent.
- Malware combining multiple types of Trojans is becoming more and more widespread. Due to its flexible modular architecture, this malware can perform many different functions. For example, it can display advertising and steal user data at the same time.
- The share of hidden mining keeps decreasing (7% compared to 9% in Q4 2018). Hackers have started to upgrade miners, turning them into multifunctional Trojans. Once inside a system with low computational power on which mining is uneconomical, such Trojans start acting as spyware and steal data.
- Infections by cryptolockers increased from 9 percent of total incidents in Q4 2018 to 24 percent in Q1 2019. This malware is often used in combination with phishing, with hackers constantly inventing new ways of deceiving users and making them pay a ransom.
- Healthcare has proved to be a favorite target of cryptolockers. Medical institutions are more likely to pay a ransom compared to other businesses, perhaps because of patients' lives and health being at stake.
- Cyberattacks against government are mainly aimed at data theft, with attackers using custom self-developed spyware, or at hacking government websites in order to infect users with malware.
- Malware remains a serious threat for large industrial companies. When it comes to such companies, the objective of most attacks is to obtain business secrets. It is possible that ransomware attacks on industry could be aimed at covering the traces of previous incidents.
- Leaks of millions of user credentials put online services at risk. Attackers extensively use publicly available data for credential stuffing attacks.
- Injection attacks with malicious JavaScript code (JS sniffers) steal payment card information and jeopardize the security of users of online stores and services that support online payments.

We predict growth in the number of attacks in Q2 2019. Malware and social engineering will remain the favored tools of attackers.

It is no secret that cryptocurrency is in high demand by criminals. However, mining is becoming increasingly difficult, which is forcing hackers to search for alternative ways of obtaining cryptocurrency. As a result, the share of ransomware Trojans will remain high so long as there are people willing to pay a ransom.

Statistics

In the first quarter of 2019, we saw a growing number of attacks aimed at obtaining data. In fact, more than half of attacks were aimed at theft of information. Attackers chase a wide range of data, including personal correspondence and trade secrets. However, the most in-demand information remains credentials, personal data, and payment card data.

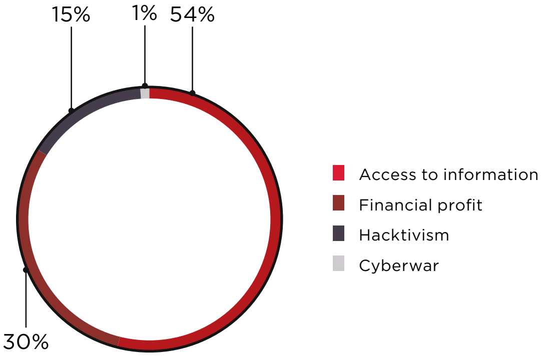


Figure 1. Attackers' motives

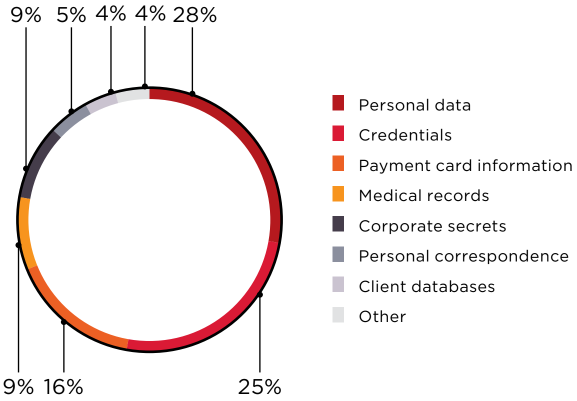


Figure 2. Types of stolen data

The share of targeted attacks fell from 62 percent in Q4 2018 to 47 percent in Q1 2019. This is caused by an increasing number of attacks affecting more than one industry—most often, malware campaigns. The share of incidents affecting individuals remained almost the same (21% compared to 22% in Q4 2018). As for organizations, attackers most often hit government agencies, medical institutions, industrial companies, banks, and other financial firms. Later in this report, we will examine these attacks in detail. In addition, Q1 2019 saw a growing number of attacks against online services. We will also try to explain why hackers are so interested in this particular target.

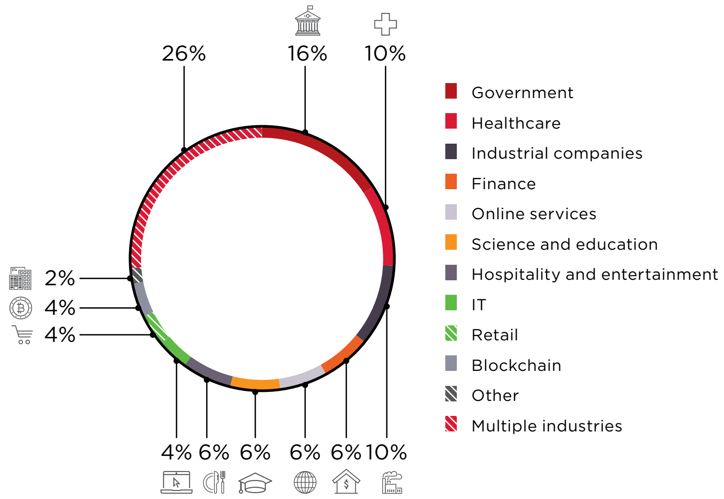


Figure 3. Victim categories among organizations

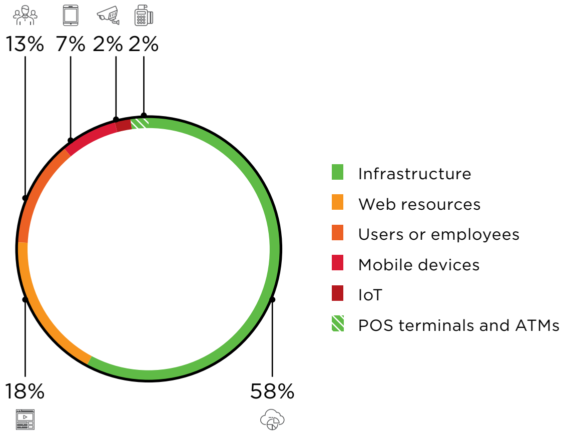


Figure 4. Attack targets

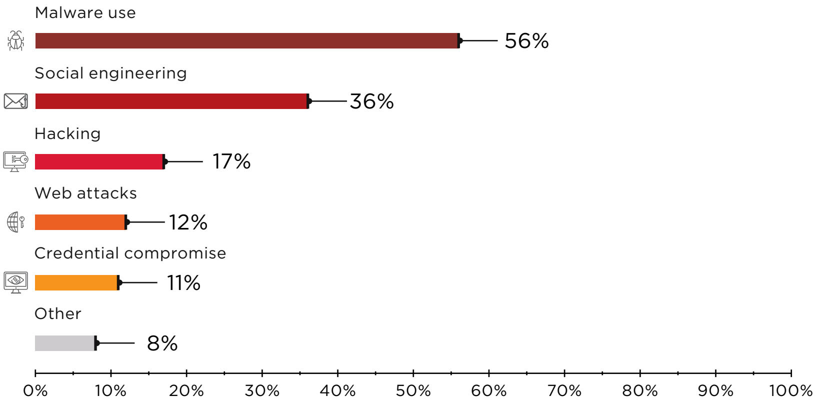


Figure 5. Attack methods

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

		Industry												
		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Science and education	Retail	Individuals	Blockchain	Other	Multiple industries
	Total	**45**	**17**	**28**	**28**	**16**	**16**	**11**	**17**	**10**	**74**	**10**	**5**	**70**
Target	Infrastructure	29	14	27	17	7	7	10	10	2	17	6	2	53
	Web resources	13	2		8	9	3	1	5	5	8	2	3	5
	Users	2	1	1	3		1		2	1	28	2		4
	Mobile devices	1									18			4
	POS terminals and ATMs						5			2				
	IoT										3			4
Method	Malware use	20	11	22	13	2	10	6	5	5	40	3	1	56
	Social engineering	10	10	20	9			1	4	2	42	3		25
	Credential compromise		1		7	4	3	5	5		5	2	2	5
	Hacking	7	2	6	2	3	2	2	4		5	5	1	20
	Web attacks	13				5	1	2	2	6	3		2	7
	Other	10	2			4		2	1		4			5
Motive	Financial profit	8	4	3	9		3	3	5	2	33	4	2	29
	Access to information	18	10	24	19	9	12	7	8	7	33	6	2	32
	Hacktivism	18	3			7	1	1	4	1	8		1	9
	Cyberwar	1		1										

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

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

Attack number

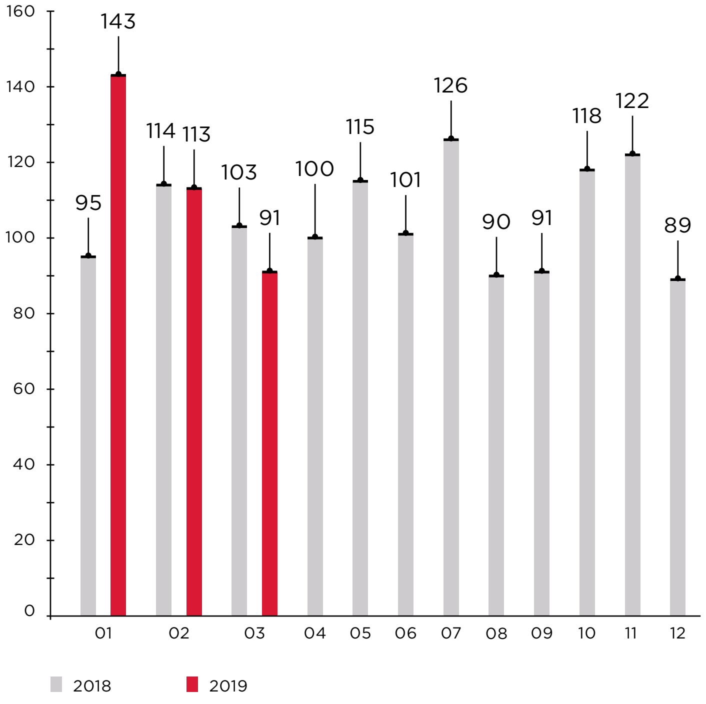


Figure 6. Number of incidents per month in 2018 and 2019 (1 = January, 12 = December)

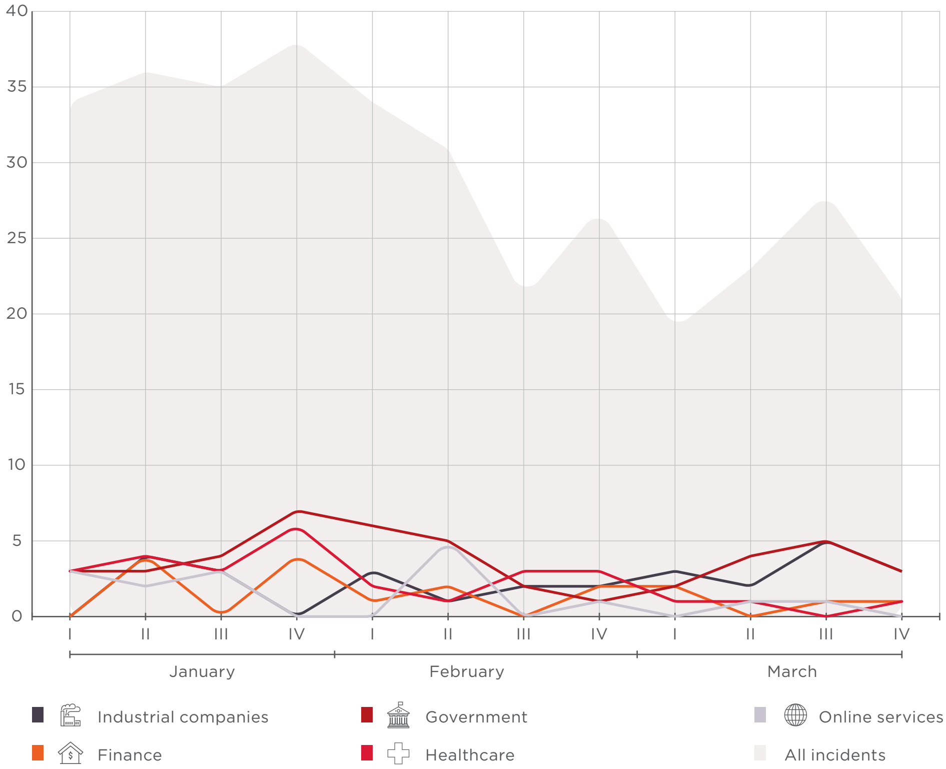


Figure 7. Number of incidents in Q1 2019 (by week)

Attack methods

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

Malware use

Since the beginning of 2019, we have been observing infections by multifunctional Trojans—modular malware capable of combining different types of functions. For example, the DanaBot Trojan has remote-control components, may function as a banking Trojan, and can also steal passwords of a number of applications.

56%

Most severe damage

21%

11%

10%

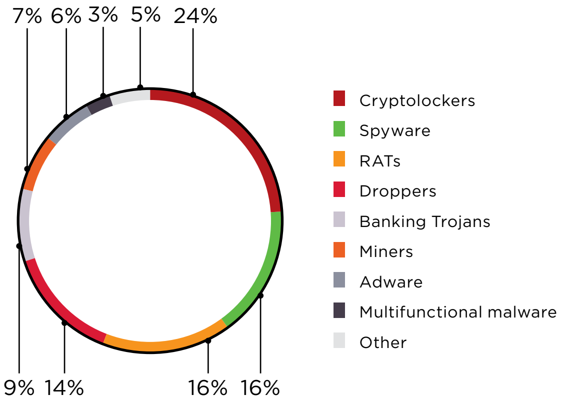


Figure 8. Malware types

Phishing remains an effective way of delivering malware. But email is far from the only channel of malware distribution. For example, users frequently download files from torrent trackers, on which the risk of malware infection grows exponentially. Under the guise of a movie, attackers distributed malware used for spoofing addresses of bitcoin and Ethereum wallets when the information is copied from the clipboard. Users also often download programs from official app stores. Programs with annoying advertising turn out to be the most common source of malware infection.[1, 2] Unfortunately, more dangerous malware can also be encountered on these stores, such as the MobSTSPY and Exodus spyware Trojans, as well as the Anubis and Gustuff banking Trojans. The last one is sold on the darknet under the malware-as-a-service model for $800 per month.

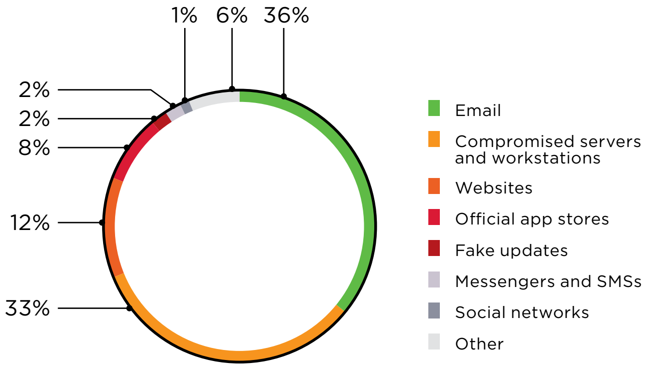


Figure 9. Malware distribution methods

[1] blog.trendmicro.com/trendlabs-security-intelligence/adware-disguised-as-game-tv-remote-control-apps-infect-9-million-google-play-users/

[2] research.checkpoint.com/simbad-a-rogue-adware-campaign-on-google-play/

Hidden mining is becoming less popular. In early 2018, the share of mining attacks reached 23 percent, but declined to 9 percent in Q4. In Q1 2019, cryptojacking accounted for only 7 percent of attacks. As mining becomes less profitable, cybercriminals are forced to upgrade miners by extending their capabilities to those of multifunctional Trojans. For example, a new Trojan dubbed CookieMiner not only installs a hidden miner on a victim's computer, but also steals credentials and payment card information.

Ransomware Trojans, on the contrary, are picking up steam: their share of infections has risen from 9 percent in Q4 2018 to 24 percent in Q1 2019. However, attackers are now earning less money from "traditional" ransomware. This is probably due to the educational efforts of cybersecurity experts urging users not to pay a ransom for file recovery. Be that as it might, attackers keep inventing new ways to manipulate users. CryptoMix hackers promised to donate ransom payments to a children's charity. Another malicious attack hit users who for whatever reason were not able to pay ransom in bitcoins. A new version of ransomware offers PayPal as a payment option. If users choose to pay using PayPal, they are taken to a fake PayPal page. All credentials and payment information entered on the fake page are then stolen by attackers, who can withdraw money from victims' accounts or sell this data on the darkweb.

36%

Most severe damage

33%

16%

8%

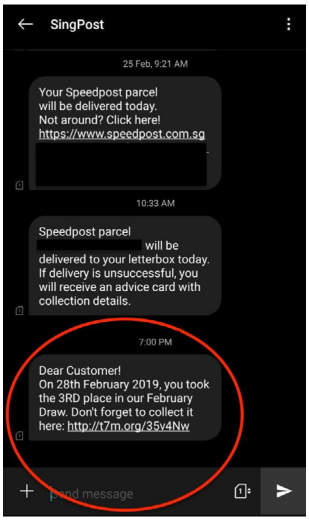
Social engineering

Social engineering remains a common method of malware distribution. In March, the Positive Technologies Expert Security Center (PT ESC) detected a mass email campaign distributing a text document regarding upcoming presidential elections in Ukraine. The document contained a macro which decoded a PowerShell Empire script hidden in metadata. The script was used to download malware to the victim's computer.

Besides political events, industry conferences also serve as a subject of phishing emails sent by attackers. Our experts discovered an invitation for a scientific conference that contained an exploit for vulnerability CVE-2018-0802 and remote control malware.

Another phishing trick is to ask victims to verify their account. Hackers sent messages to the owners of popular Instagram profiles prompting them to enter personal data and credentials in fake forms, putting all the submitted data into the hands of the hackers. In yet another example, clients of TD Bank received emails with the subject line "Confirm account status" pretending to come from the bank. The emails contained the TrickBot banking Trojan. In both cases, the malicious messages were sent from email addresses that closely resembled genuine addresses of the companies.

Savvy Internet users know that one or more scrambled letters in an address can be a warning sign indicating a phishing attack. But what if the domain matches the legitimate one? Is it absolutely safe to open attachments from such messages? As practice shows, this is not the case. In brand impersonation attacks, attackers often use compromised resources or vulnerabilities in mail services to send malicious emails while posing as genuine companies. In one case, hackers used an insecure SMTP server configuration to distribute malware and impersonate DHL in a phishing campaign. Messages were sent from support@dhl.com, which caused recipients to let their guard down.



SingPost

25 Feb, 9:21 AM

Your Speedpost parcel
will be delivered today.
Not around? Click here!
https://www.speedpost.com.sg
[redacted]

10:33 AM

Speedpost parcel
[redacted] will be
delivered to your letterbox today.
If delivery is unsuccessful, you
will receive an advice card with
collection details.

7:00 PM

Dear Customer!
On 28th February 2019, you took
the 3RD place in our February
Draw. Don't forget to collect it
here: http://t7m.org/35v4Nw

Figure 10. SMS message
with malicious link

In another sophisticated phishing attack, hackers used the SingPost name. The attackers sent a malicious link to users' phones in messages allegedly coming from the logistics services provider. Hackers managed to send messages grouped in the same conversation history as SingPost's actual ones, which made users less vigilant, just like in the case of DHL.

Hacking

Attackers exploit known and zero-day vulnerabilities in software for various purposes. For example, ready-made exploits are often used to deliver hidden miners to devices. In Q1 2019, hackers used security flaws in the clusters with outdated Elasticsearch versions (CVE-2014-3120, CVE-2015-1427) and exploited vulnerabilities CVE-2019-6340 in the Drupal CMS and CVE-2019-5736 in Docker containers. Attackers also seek escalation of privileges on a system, since administrator rights give them a free hand to conduct malicious actions. For example, a zero-day vulnerability in the WordPress Easy WP SMTP plugin allowed attackers to create administrator accounts, modify SMTP options, and redirect traffic. The flaw may be used to conduct brand impersonation attacks against companies whose sites have been compromised. We have already looked into an example of such an attack in the section on social engineering. In another privilege escalation attack, hackers exploited two zero-day vulnerabilities at the same time—one in Google Chrome and the other in Windows 7. Google experts discovered the attacks in late February.

Also in February, cybersecurity experts discovered vulnerabilities in WinRAR that had existed in the program for around 19 years. Such flaws offer hackers new opportunities for infecting victims with malware. In the first month since the vulnerability was disclosed, experts have identified about a hundred exploits for the detected vulnerability. WinRAR is an ubiquitous compression tool used by millions of people as well as major companies, making the vulnerability immensely attractive for hackers. According to experts, the vulnerability threatens 500 million users worldwide. The developers have already fixed the bugs and released a new version of the software, but the threat remains relevant as WinRAR does not have an automatic update mechanism.

17%

Most severe damage

🏛	12%
🏭	10%
₿	8%

Web attacks

The beginning of the year was marked by mass attacks by the MageCart group famous for so-called web skimmers—scripts used to steal payment card information from websites. We already discussed these attacks in the Q4 2018 report. In January 2019, experts noted a new surge of MageCart attacks. The attackers infected 277 e-commerce websites. They managed to extend their reach by using supply chain attacks, in which a company is compromised in order to attack another one. MageCart hackers injected skimming code into a JavaScript library used by Adverline, an online advertising company. As a result, websites of the companies that published advertisements via Adverline were in turn infected. The Media Trust experts registered a similar but larger attack. They discovered a malicious campaign compromising tens of adtech vendors and threatening 49 high-profile websites.

When compromising websites, attackers are motivated by more than just data theft. A website attack can be an effective way to draw attention to a problem. Attackers often hit government websites following significant events that have caused public outcry. After a terrorist attack in Pulwama on February 14, hundreds of Pakistani websites were hacked.

12%

Most severe damage

🏛	31%
🛒	14%
🌐	12%

Sometimes hackers strive to draw public attention to security problems. The website of Dublin's tram system operator, Luas, was hacked because the website owners did not reply to a message sent by an anonymous hacker pointing out security flaws. Developer neglect of security issues likely contributed to an XSS attack targeting users of VK, the popular Russian social network, in February 2019.

XSS attacks also threaten users of WordPress websites. A vulnerability in the Abandoned Cart plugin allows attackers to create a backdoor, specifically, an account with administrator rights. According to experts, the flaw has already been exploited by attackers at least 5,000 times. A vulnerability in the Social Warfare plugin allows redirecting users to attacker-controlled websites. And our company's research shows that XSS attacks are still among the most common risks threatening web application users.

Credential compromise

11%

One source of hacker income is selling credentials on the darkweb. The more usernames and passwords hackers steal, the more money they get, which inspires them to conduct mass bruteforcing attacks. Experts observe a growing number of attacks aimed at bruteforcing credentials for Office 365 and G Suite. Attackers are taking advantage of vulnerabilities in outdated versions of the IMAP protocol to significantly increase the speed of password bruteforcing.

Traces of credential compromise were also found in an attack against Citrix that resulted in theft of trade secrets. Experts believe that attackers could have used so-called "password spraying" for the attack. This method involves trying the same password or handful of passwords for a whole list of usernames. Unlike traditional bruteforcing, this technique avoids the automatic lockouts that would otherwise occur after numerous failed login attempts.

Most severe damage

18%

13%

13%

In March 2019, the W3C and FIDO Alliance adopted the WebAuthn passwordless login standard. It is hoped that the new technology will make bruteforcing and password spraying a thing of the past. However, implementation of the standard will take some time.

Victim categories

Government

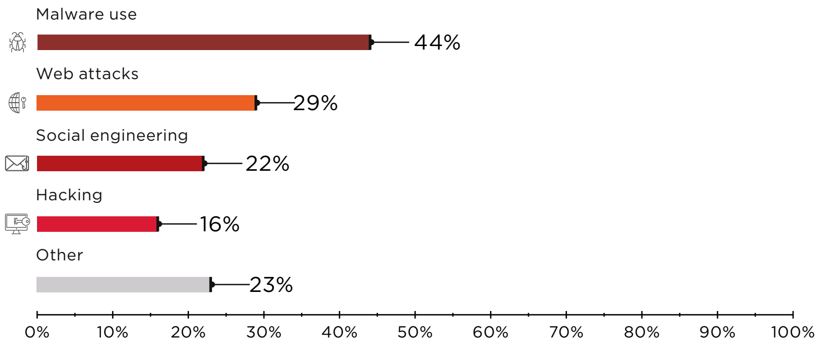


Figure 11. Government: attack methods used in Q1 2019

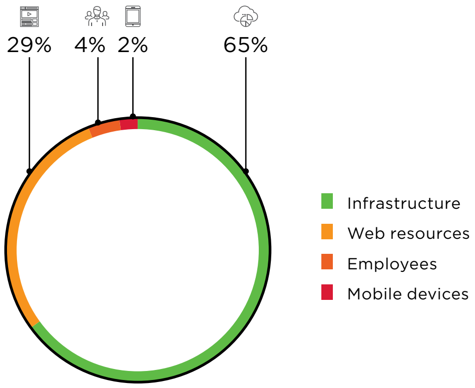


Figure 12. Attack targets

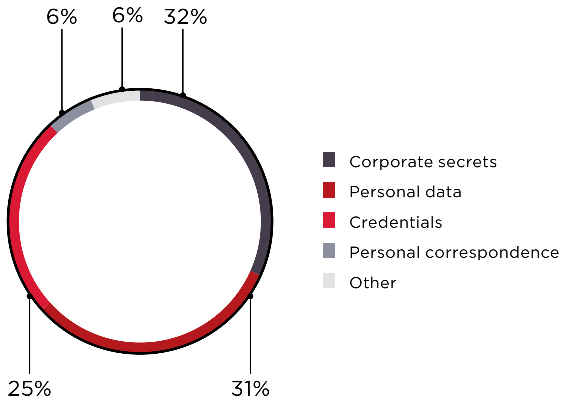


Figure 13. Data stolen

The beginning of the year offered unpleasant surprises for government institutions in many countries. A complex but well-planned cyberespionage campaign, DNSpionage, started at the end of last year and went on the march in January and February 2019. Cybercriminals stole credentials for email accounts and other government resources. This classic supply chain attack managed to compromise the accounts of two major DNS providers. However, the attackers' ultimate targets were government institutions in the Middle East. After gaining access to providers' servers, hackers performed a DNS hijacking attack, altering DNS records and redirecting all mail and VPN traffic to an attacker-controlled server. The campaign reached such a scale that the U.S. Department of Homeland Security had to issue an emergency directive outlining security measures to be taken by all federal agencies.

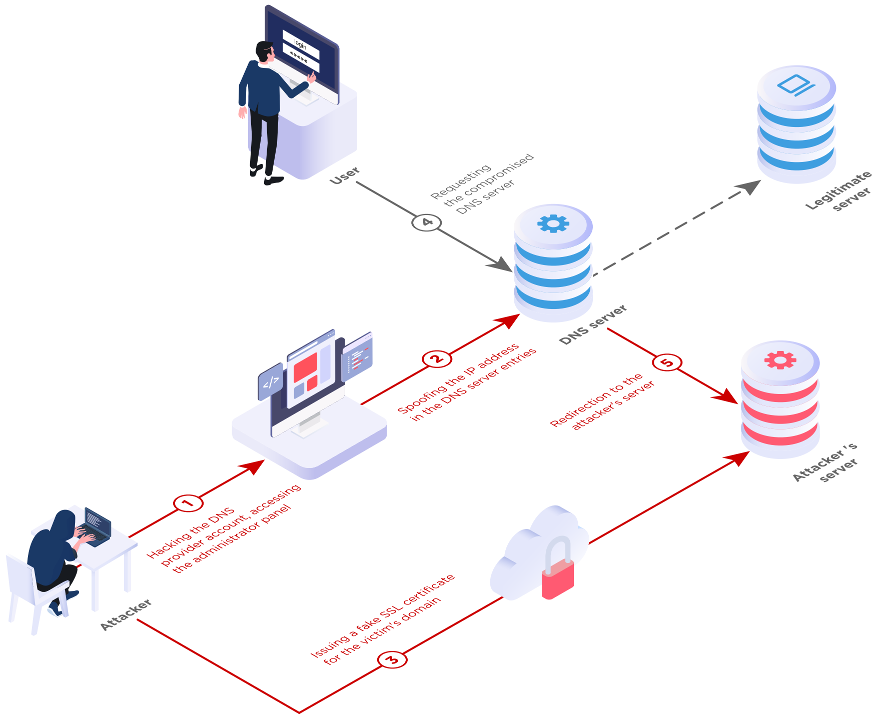

User
4
Requesting the compromised DNS server
Legitimate server
DNS server
2
Spoofing the IP address in the DNS server entries
5
Redirection to the attacker's server
Attacker's server
1
Hacking the DNS provider account, accessing the administrator panel
Attacker
3
Issuing a fake SSL certificate for the victim's domain

Figure 14. DNS hijacking attack scheme

Early January was also marked by the resurgence of the DarkHydrus APT group. The group targets government institutions, mainly in the Middle East, and distributes an updated version of the RogueRobin Trojan (developed by the group itself). The updated malware version can communicate with the C2 server via the Google Drive API.

As before, attackers keep hitting high-traffic government websites and infecting them with malware. In one such case, hackers posted links to malicious Word documents with the Godzilla loader on the website of the Bangladesh embassy in Cairo.

A Pakistani government site was infected by malware. The website in question allows users to apply for a Pakistani passport and track the status of their application. The Scanbox JavaScript framework collected all the data submitted by visitors and sent it to criminals.

Q1 2019 also saw a number of ransomware attacks on government institutions. In most cases, the encrypted files were recovered from backups. However, officials in Jackson County, Georgia, paid $400,000 to restore IT infrastructure.

Healthcare

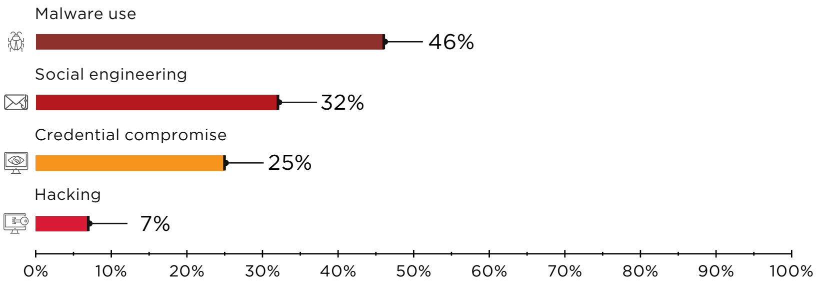


Figure 15. Healthcare: attack methods used in Q1 2019

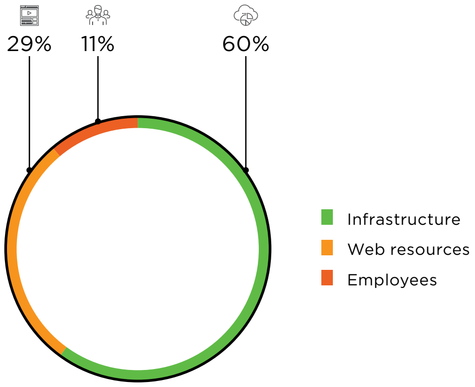


Figure 16. Attack targets

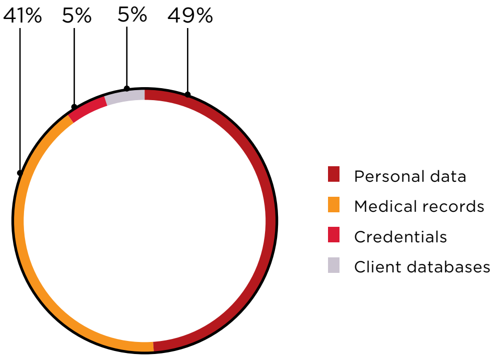


Figure 17. Data stolen

Healthcare attacks mostly involved malware infection and theft of employee credentials, which remain the two most common attack methods against medical institutions. For example, email accounts of Verity Medical Foundation employees were hacked three times within several months.

Healthcare is a favorite target of ransomware attacks for several reasons. Medical institutions often do not have an adequate information security budget. Weak protection makes hospitals easy prey for hackers. Moreover, healthcare facilities store and process huge amounts of personal data, including patients' diagnoses. Hospitals risk substantial fines for losing these databases, which forces them to pay ransoms more willingly than other businesses. Columbia Surgical Specialists preferred not to risk patients' data and paid $15,000 for file recovery.

Industrial companies

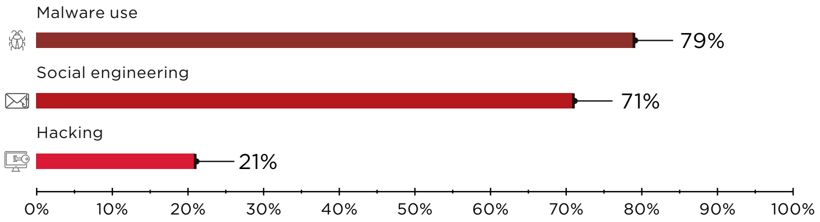


Figure 18. Industrial companies: attack methods used in Q1 2019

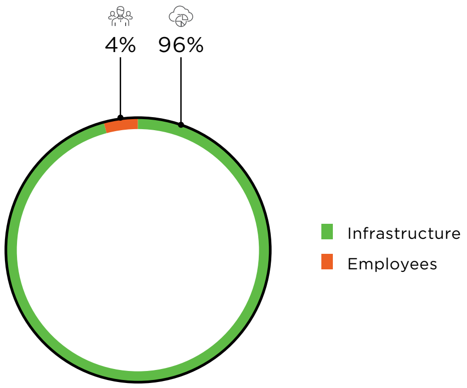


Figure 19. Attack targets

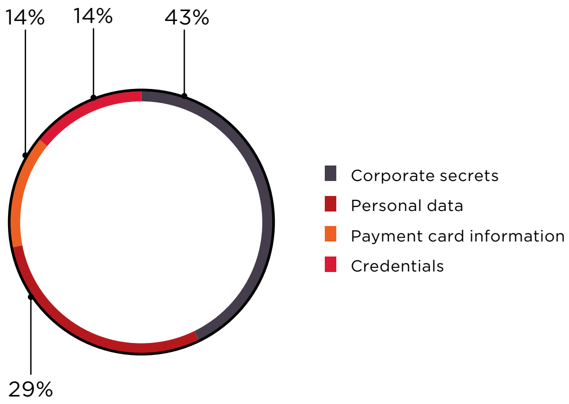


Figure 20. Data stolen

New LockerGoga ransomware is attacking major engineering and industrial companies. The virus gained public attention in January in an attack against Altran Technologies, a French engineering consulting firm. Just a month later, Norwegian aluminum company Norsk Hydro had to halt operations due to a similar cyberattack. The ransomware victims also included two American chemical companies. Security experts are actively studying the infamous malware and have already uncovered a coding error that could be used to stop the spread of the virus. However, victory is a long way off: to date, experts have identified 31 samples of this rapidly developing ransomware.

Financial institutions

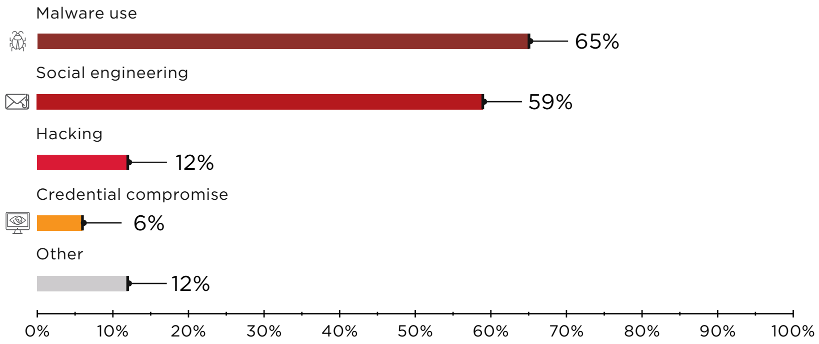


Figure 21. Financial institutions: attack methods used in Q1 2019

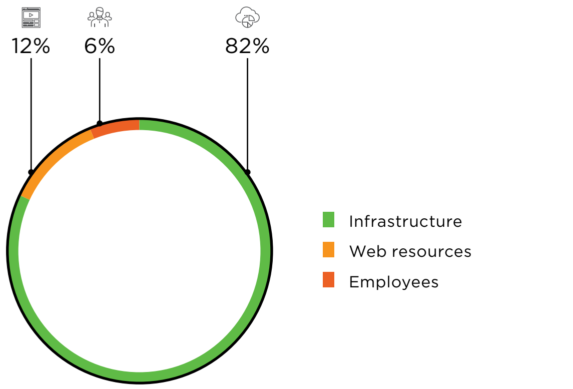


Figure 22. Attack targets

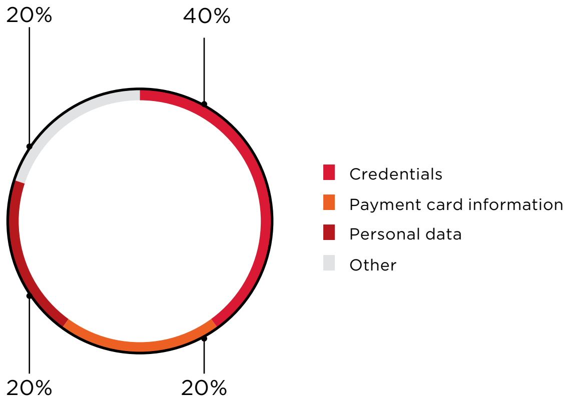


Figure 23. Data stolen

The Cobalt group did not give up ground either. In Q1 2019, hackers used the same technique they applied in late 2018. Just like before, attacks involved COM-DLL-Dropper loaded with an obfuscated JavaScript backdoor.

In February, PT ESC detected an attack that involved the use of Metasploit in conjunction with COM-DLL-Dropper. The Metasploit stager is loaded into the memory of an infected computer from an attacker-controlled server, providing remote access to the device and downloading the necessary Metasploit modules. A similar attack was conducted in last October and December by an unknown group—a fact we already covered in our previous report.

A bank cyberattack may lead to infrastructure downtime costing tens and sometimes hundreds of thousands of dollars. In February, Malta's Bank of Valletta shut down operations as the result of a cyberattack. Hackers tried to steal €13 million, but the attack was discovered and stopped just in time.

Online services

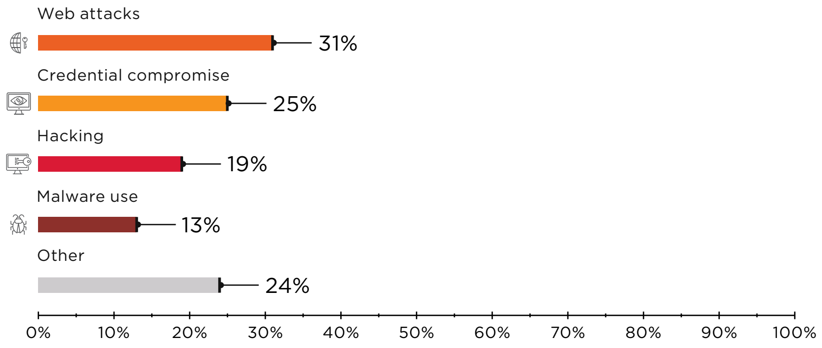


Figure 24. Online services: attack methods used in Q1 2019

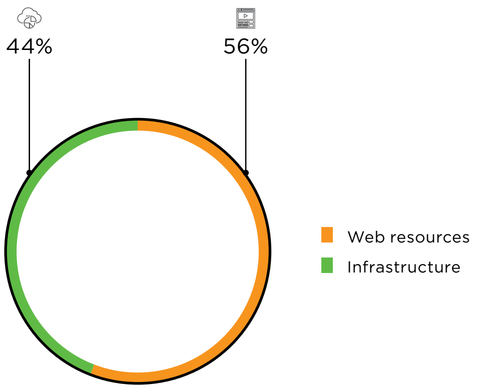


Figure 25. Attack targets

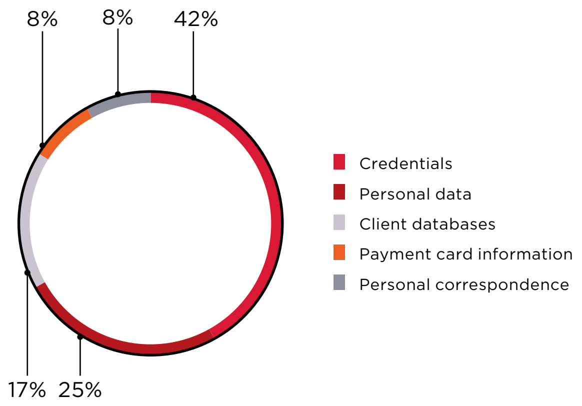


Figure 26. Data stolen

Active Internet users constantly interact with various online services by communicating on social networks, playing games, watching movies, buying tickets, and booking hotel rooms. However, these services also attract hacker attention, as they store huge amounts of data, including of a personal nature, that can bring large profits if sold.

Today, one of the most popular methods of hacking is credential stuffing, when hackers try to log in to a service with credentials used for other online services. In January, Reddit announced hacker attempts to obtain unauthorized access to users' accounts, and had to lock down the affected accounts. According to the Reddit owners, the attackers could have been trying to make use of large-scale password leaks. Video sharing platform DailyMotion also fell victim to a credential stuffing attack. But where do hackers get the databases of credentials needed to conduct such attacks? The darkweb is one such place. Data for 620 million accounts stolen from 16 hacked major websites, including popular online services, was put on sale on Dream Market, a darkweb marketplace.

However, attackers can have other objectives as well. VFEmail, an email provider, was completely destroyed in a cyberattack in February 2019. The attackers formatted all disks on every server, as a result of which even backups were lost. The attack can be explained by high competition on the market and the struggle for customers.

What companies can do to stay safe

Use proven security solutions:

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

- 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. Previously unnoticed attacks are detected. Monitoring shows 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 infrastructure, minimizes the risk of loss of critical data and disruption to business systems, and decreases the financial damage caused by attackers.

- Use 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.

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.

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).

How vendors can secure their products

- All of the measures for companies given above, plus:
- 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. For example, if an attack strikes network equipment, servers, or user workstations, the attack target is "infrastructure."
- **Attack motive** is the ultimate goal of cybercriminals. If an attack results in theft of payment card information, the motive is "access to information."
- **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 category** is the economic sector 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 was conducted in order to educate companies and individuals who care about information security on the most common 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

Cybersecurity_threatscape-2019-Q1_A4.ENG.0003.04