Cybersecurity threatscape

Q3 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

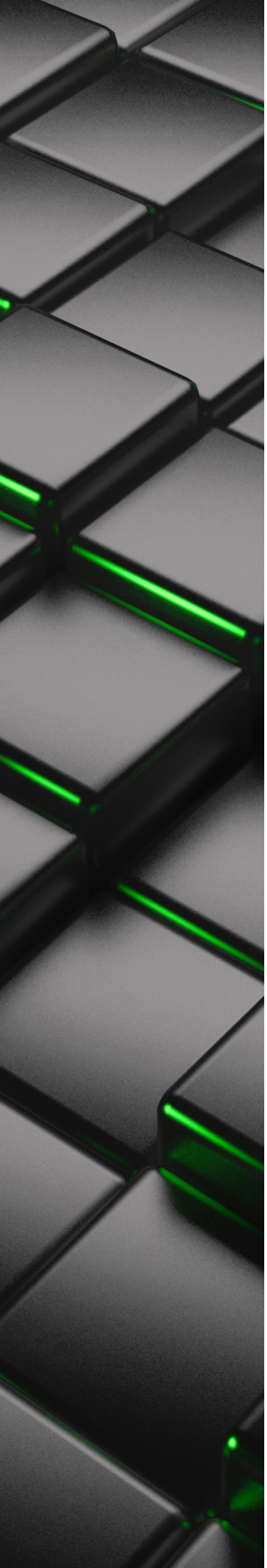

Retail


Individuals


Telecom


Blockchain


Other



Executive summary

Highlights of Q3 2019 include:

- Unique cyberincidents are growing, with a six-percent increase in their number compared to the previous quarter.
- Targeted attacks continue to predominate over mass ones: 65 percent of the total in Q3 versus 59 percent in Q2. Organizations around the world are at risk of APT attacks. Top targets of APT groups include governments, industrial companies, the financial sector, and science and education.
- TA505, an APT group, has expanded its reach to new countries and sectors.
- By a two-to-one ratio, data theft is a more common motivation for attackers than direct financial gain.
- Personal data accounted for one quarter of all data stolen from organizations. From individuals, data thieves most frequently made off with usernames and passwords (which comprised 47% of data stolen from individuals).
- Malware infections are on the rise. Three quarters of attacks on organizations, and nearly two thirds of attacks on individuals, involved malware infections.
- Spyware was responsible for one in three malware infections among both organizations and individuals. Just as ransomware accounts for a high percentage of infections of organizations (27%), adware hits individuals particularly hard (21%).
- In 81 percent of cases, malware infections of corporate infrastructure started with a phishing message. For individuals, the most frequent attack vector included visiting a malicious website: 35 percent of malware infections in Q3 took place in this way.

Statistics

In Q3, data theft was the motivation for 61 percent of attacks on organizations and 64 percent of attacks on individuals (compared to 58% and 55%, respectively, in Q2). Direct financial gain, at 31 percent, was equally popular as motivation for attacks against both organizations and individuals. Attackers seeking direct financial gain from organizations generally use ransomware to demand a ransom for decrypting the victim's data. Against individuals, such direct gain tends to involve intrusive advertising and mobile apps with subscriptions to paid services.

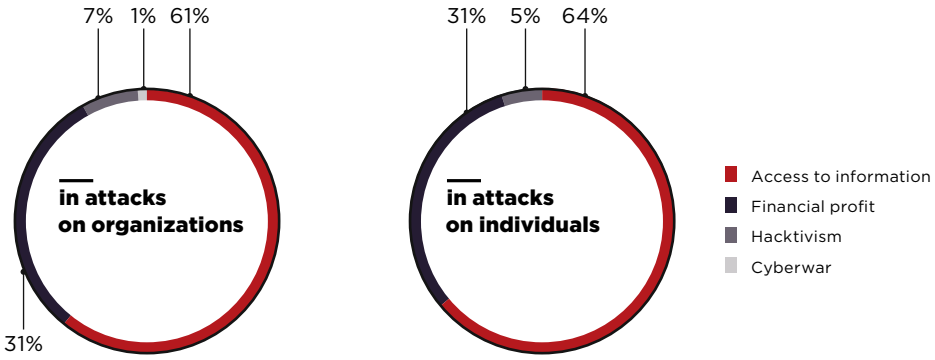


Figure 1. Attackers' motives

Breaches of personal data remain a major concern. In Q3, personal data accounted for one fourth of all data stolen from organizations. The General Data Protection Regulation (GDPR) took force in 2018. This September, reports appeared of a EUR 645,000 fine for a Polish shopping site after a breach of personal data for over 2 million site visitors in the previous year.

One out of five (19%) of attacks in Q3 targeted individuals. Almost half (47%) of data stolen from individuals consisted of credentials. Users may fall victim to clever phishing attacks designed to trick them into revealing usernames and passwords. For example, over 200 clients of Halyk Bank in Kazakhstan failed to notice a slight discrepancy in the online address of the bank. As a result, they entered their credentials on a fraudulent site designed to imitate the real one.

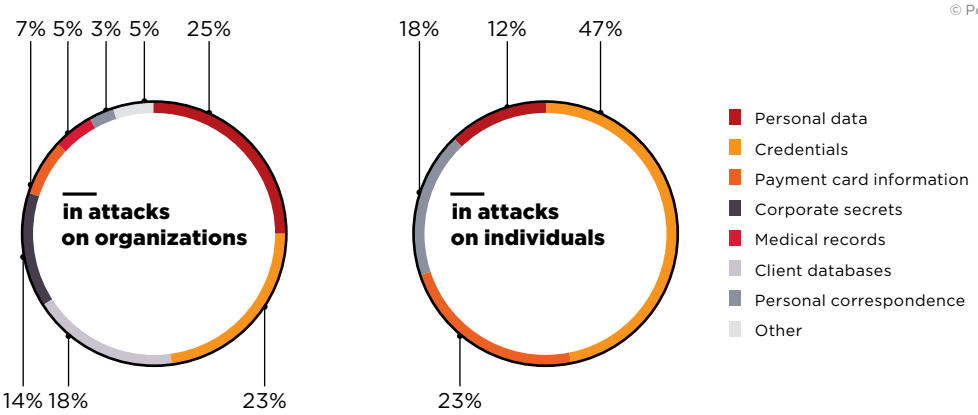


Figure 2. Types of data stolen

The high proportion of targeted attacks is a trend we have noticed accelerating in 2019. From 47 percent in the first quarter, they rose to 59 percent in the second quarter and now 65 percent in the third quarter. We associate this trend with increased activity by APT groups. In Q3, the PT Expert Security Center (PT ESC) detected attacks by APT groups including TA505, RTM, Cobalt, Bronze Union, APT-C-35, KONNI, and Gamaredon.

Attackers continue to be interested in government targets. Such targets accounted for 23 percent of attacks, representing an increase of 4 percentage points over Q2. Attackers also pursue targets relating to industrial companies, finance, and education and science. We will detail some of these attacks later in this report.

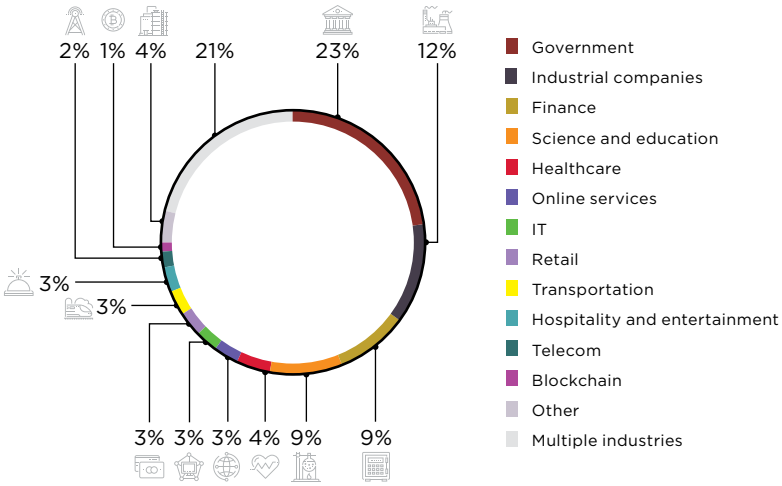


Figure 3. Victim categories among organizations

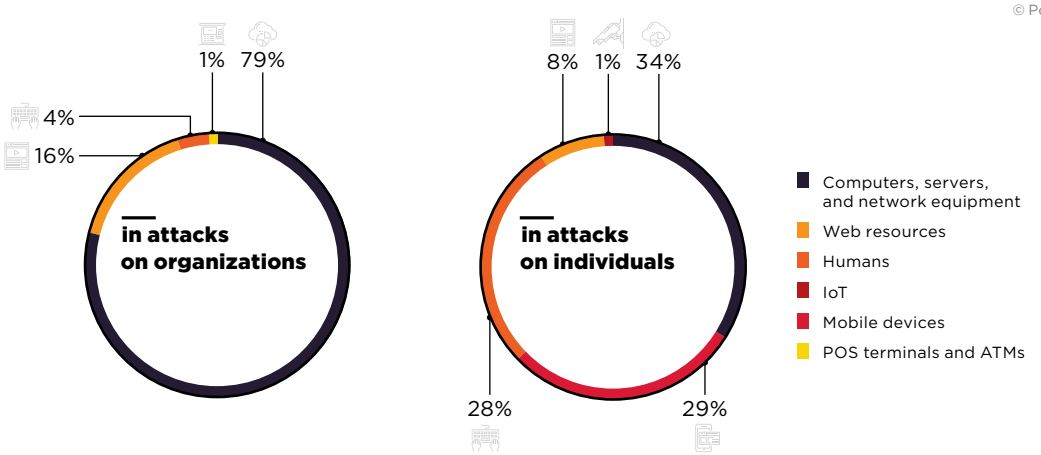


Figure 4. Attack targets

As before, the most common cyberattack method is malware infection combined with social engineering. In Q3, three quarters (74%) of attacks on organizations involved infection with malware, representing an increase of 13 percentage points over Q2.

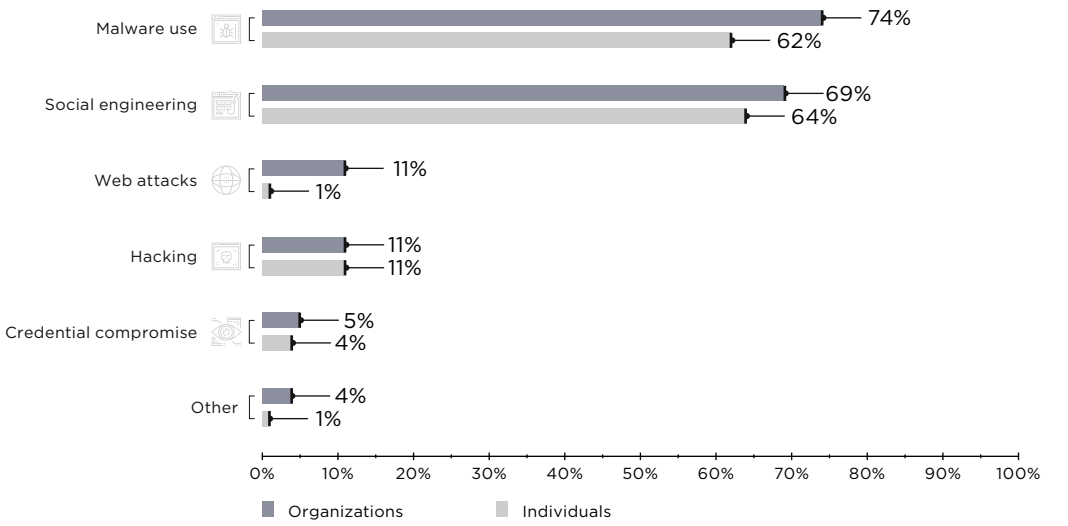


Figure 5. Attack methods

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	Telecom	Transportation	Blockchain	Other	Multiple industries	Individuals
	Total	**69**	**28**	**37**	**11**	**10**	**8**	**10**	**29**	**8**	**7**	**8**	**4**	**12**	**65**	**73**
Target	Computers, servers, and network equipment	52	23	34	8	3	3	8	27	6	7	5	2	7	56	25
	Web resources	14	2	1	1	7	4	2	1	2		2	2	4	6	6
	Humans	3	1	2	2				1			1		1	3	20
	Mobile devices															21
	POS terminals and ATMs		2				1									
	IoT															1
Method	Malware use	52	24	34	7	1	4	5	24	3	4	6		6	56	45
	Social engineering	49	24	35	8	1	4	5	23	3	4	7		6	42	47
	Credential compromise	3	1			1	2	1			1	1	1	1	3	3
	Hacking	7	1	2				3	3	1	1		3	1	12	8
	Web attacks	11	1	2		6	2	1		4			1	3	4	1
	Other	2	1	1	2	2					2			2	1	1
Motive	Access to information	46	27	33	5	7	7	7	9	4	5	8	1	10	28	46
	Financial profit	11	1	4	5			1	20	3			3	1	36	23
	Hacktivism	9			1	3	1	2		1	2			1	1	4
	Cyberwar	3														

Darker colors indicate a greater proportion of attacks within a particular industry

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

Attack number

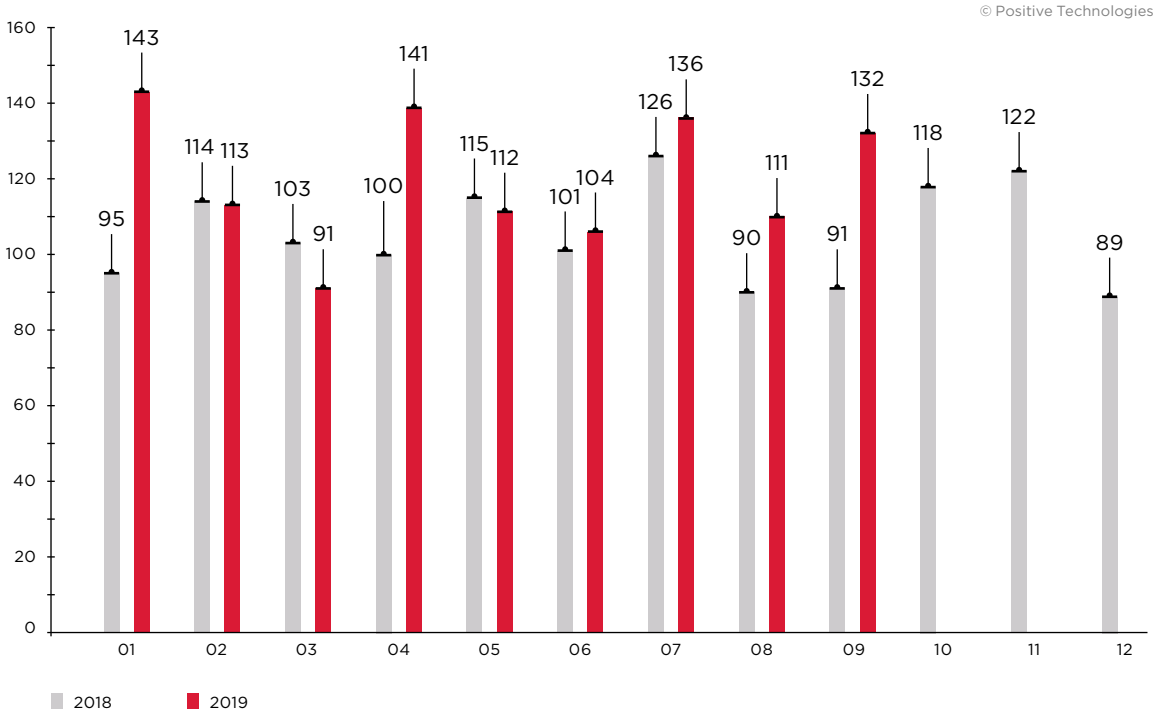


Figure 6. Number of incidents per month in 2018 and 2019 (1 = January, 12 = December)

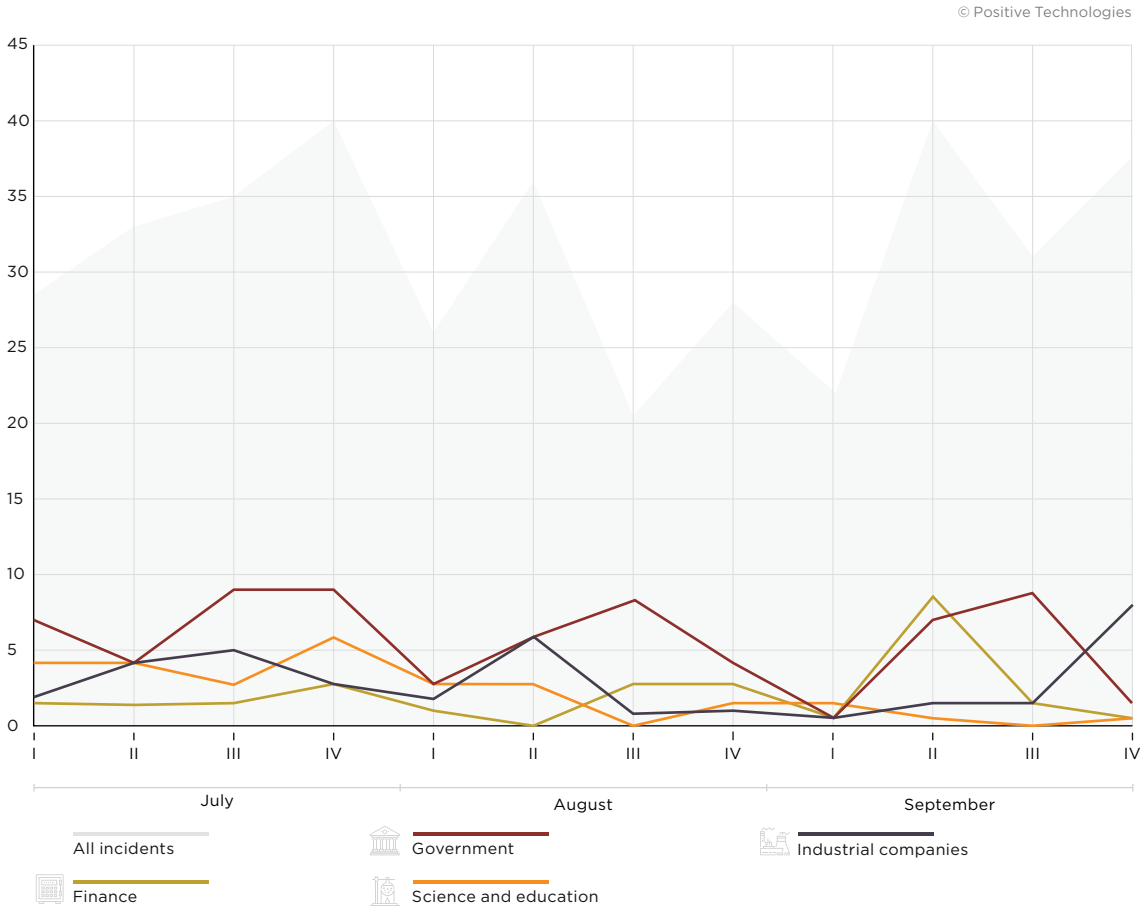


Figure 7. Number of incidents in Q3 2019 (by week)

Attack methods

Here we will describe the attack methods used by criminals, based on some of the highest-profile cyberincidents in Q3 2019.

Malware use

During the third quarter, the PT ESC regularly recorded attacks by APT group TA505. The group's arsenal includes Dridex (a banking trojan), Cryptomix (ransomware signed with certificates issued to dummy legal entities), ServHelper and FlawedAmmyy (remote administration trojans), and Upxxec (a plugin able to detect and disable a large range of antivirus software). The attackers made active use of phishing to send messages to organizations around the world related to finance, industry, government, science, and transportation. Some of their campaigns are analyzed in more detail in individual sections of this report.

In Q3, our experts also detected new activity by Bronze Union (also known as LuckyMouse or APT27), which uses ZxShell malware for remote access. The malware components had been digitally signed with compromised certificates belonging to various companies. Once installed, ZxShell is difficult to detect with normal antivirus techniques: the attackers place a special rootkit on infected systems to swap out the installation paths to malware modules with the paths to legitimate utilities upon access.

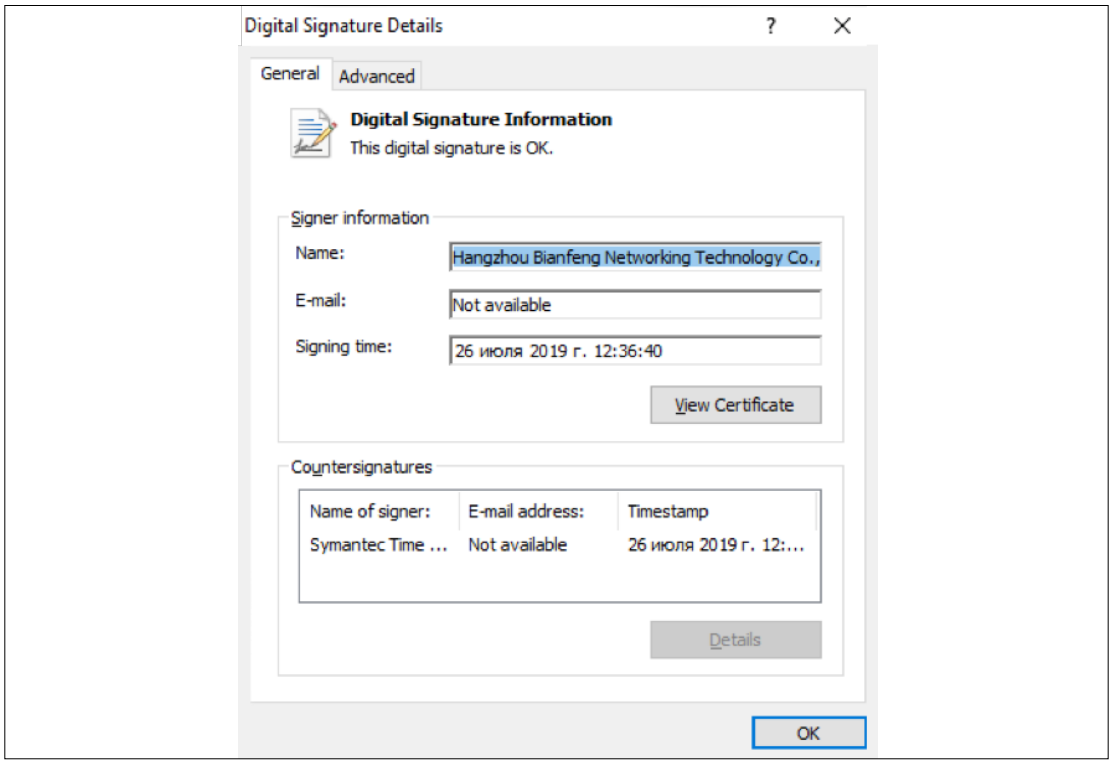


Figure 8. ZxShell installer signed with a compromised certificate

The operators of the Sodinokibi ransomware, which we already covered in the second quarter, continue to act aggressively. A breach of cloud provider PerCSoft resulted in encryption of data belonging to the company's client base of approximately 400 dental clinics. In August, over 20 Texas communities fell victim to this ransomware. The attackers constantly invent new methods for placing Sodinokibi on victim computers.

In the third quarter, mining software fell to 3 percent of attacks on organizations and just 2 percent of attacks on individuals. In our view, this is because attackers are gradually switching to malware with multifunction capabilities. One example is the Clipsa trojan, which can stealthily mine cryptocurrency, steal passwords, tamper with addresses of cryptocurrency wallets, and launch brute-force attacks against WordPress sites.

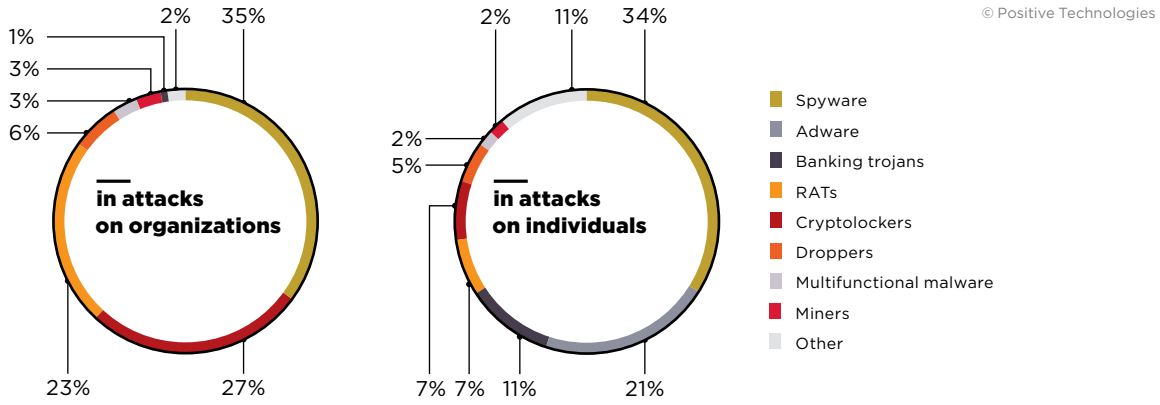


Figure 9. Types of malware

In late August, Emotet (one of the largest botnets in the world) resumed activity after a lull of several months. The botnet's operators offer malware as a service (MaaS): by providing access to Emotet-infected computers, they enable other cybercriminals to infect victims with additional malware. Since September, they have been sending out malicious mailings disguised as invoices, financial documents, and even a free version of the new book by Edward Snowden. The attachments to these messages infect the victim with the Emotet trojan. With it, the botnet operators can place yet more malware on compromised devices, such as the Trickbot trojan or Ryuk ransomware, which are frequently found together on infected machines.

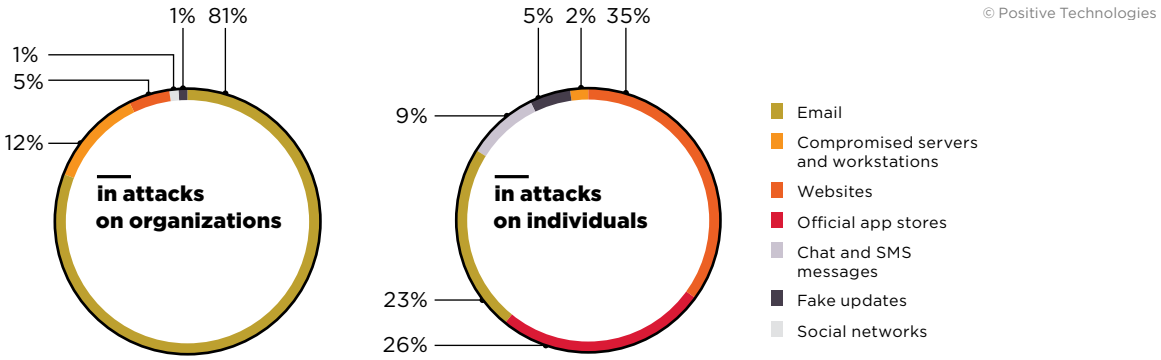


Figure 10. Malware distribution methods

Social engineering

For attackers, social engineering is a perennial favorite. This method figured in 69 percent of attacks on organizations in the third quarter, compared to 37 percent in the second quarter. Cybercriminals continue to rack up huge amounts by forging messages or employing business email compromise (BEC) to send phishing messages. They present themselves as belonging to a trusted company (such as a vendor) and send an invoice with their own bank account number. In the state of North Carolina, Cabarrus County received an email stating that the account number of the county's construction contractor had changed. Not realizing that the message was a fake, the county transferred $2.5 million to

an account belonging to cybercriminals instead of the contractor. A similar attack hit Toyota Boshoku Corporation, which lost a whopping $37.5 million. According to the U.S.-based Internet Crime Complaint Center (IC3), worldwide losses from BEC fraud in the last three years top $26 billion.

A malicious link, even if sent from a trusted address, can be blocked by email security gateways. But cybercriminals keep finding ways to evade anti-phishing systems. In Q3, attackers sent messages to bank employees with a link to a compromised SharePoint site. There the attackers had posted a document with another link, which led victims to a fake page asking for their username and password. If the phishing link had been included directly in the email message, anti-phishing systems might have blocked it. But SharePoint links had been whitelisted and therefore were not blocked.

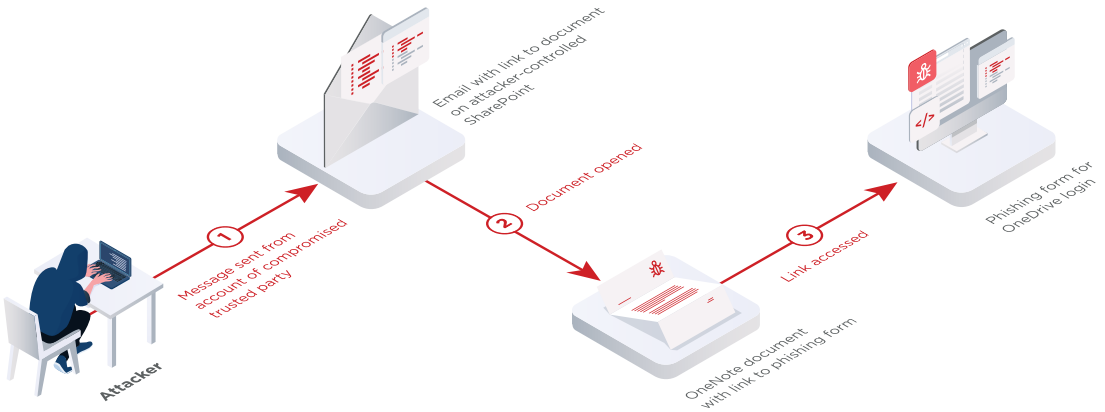


Figure 11. Phishing attack involving compromised SharePoint resources

Hacking

As we regularly remind readers, it is critical to keep software up to date. When a software vulnerability becomes known to the public, the first to get attacked are the organizations and individuals who have failed to install the relevant updates quickly. In one example in Q3, the eGobbler criminal group responsible for inserting malicious ads into web pages continued to exploit vulnerability CVE-2019-5840, affecting the Chrome browser for iOS, which had been patched back in June. But soon after the browser update was released, eGobbler found a new vulnerability, this time in the WebKit engine. The vulnerability allows displaying pop-up ads every time the keyboard is used for site navigation. The vulnerability has been fixed in iOS 13 and Safari 13.0.1.

Last quarter, we mentioned critical RDS vulnerability CVE-2019-0708, better known as BlueKeep. In August, Microsoft fixed another two vulnerabilities in RDS. These new critical vulnerabilities CVE-2019-1181 and CVE-2019-1182 resemble BlueKeep but affect more recent versions of Windows, including server versions.

Web attacks

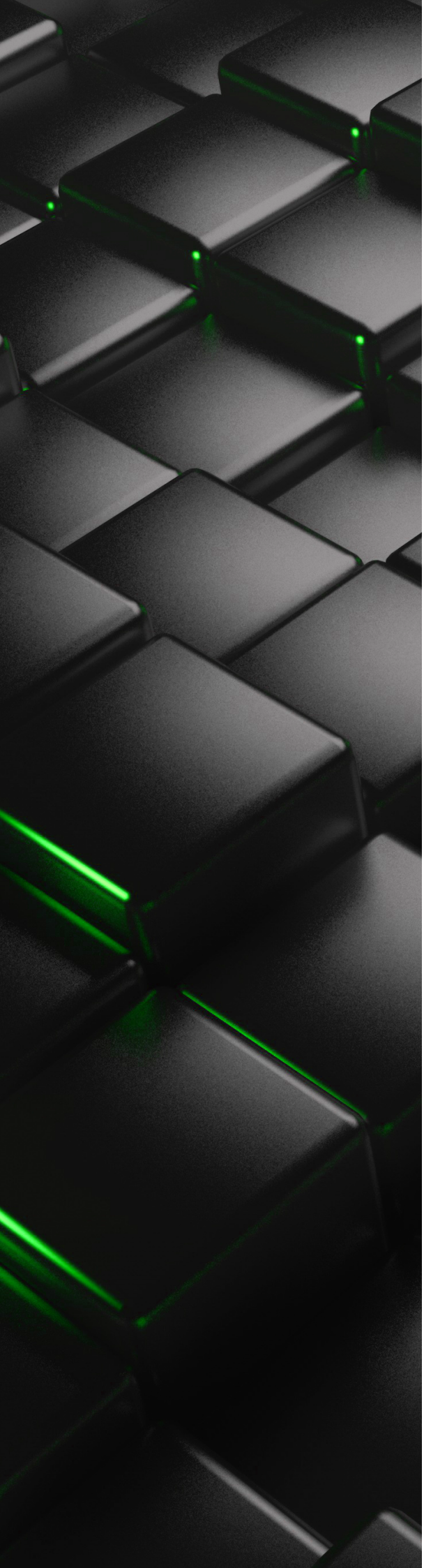
In late September, an exploit became public for a zero-day vulnerability in the vBulletin forum engine. News spread quickly of Remote Code Execution vulnerability CVE-2019-16759, exploitation of which does not require logging in to a vulnerable forum. Some security experts state that they had knowledge of the vulnerability years prior. At the end of September, the issue with vBulletin enabled attackers to breach the Comodo forums. Reports indicate that data for over 170,000 users is being sold on the darkweb.

For users who make online purchases, MageCart JavaScript sniffers remain a hazard. These sniffers are small scripts that attackers use to infect sites with online payment functionality. In Q3 2019, Trend Micro researchers discovered malicious scripts on the sites of two major hotel chains. The attacks affected guests who paid for their stays via mobile devices. Experts established that the hotels had fallen victim to a supply chain attack. MageCart sniffers were placed on the site by means of an infected JavaScript library. This library was used by the company responsible for developing both of the hotel sites.

But web security is an issue for more than just online services and Internet stores. A file upload vulnerability in property management software SuperINN Plus enabled attackers to hack the application by uploading a web shell (a PHP script that, when run on a server, enables remote command execution). In addition, the attackers were able to perform SQL injection. They obtained the encrypted card numbers, personal data, and contact details for over 43,000 people. The attackers are believed to have succeeded in obtaining the decryption key. This incident underscores the need to regularly audit the security of web applications. Arbitrary File Upload is a widespread critical vulnerability, which in 2018 our experts found in one out of every four web applications tested.

Credential compromise

No company is immune to compromised credentials. In so-called credential stuffing attacks, criminals try to obtain access to a system by re-using usernames and passwords already stolen in previous attacks or acquired elsewhere (such on the darkweb). In Q3 2019, credential stuffing struck Transport for London, which is responsible for managing the city's transportation network. The website for its Oyster system was temporarily closed due to the attack. Another victim was State Farm, a financial services and insurance company. Overall, research from Akamai indicates that from November 2017 through April 2019, 6.1 percent of credential stuffing attacks were directed at the financial sector.



Victim categories

In this section, we will go into detail on attacks affecting particular industries of interest in Q3 2019.

Government

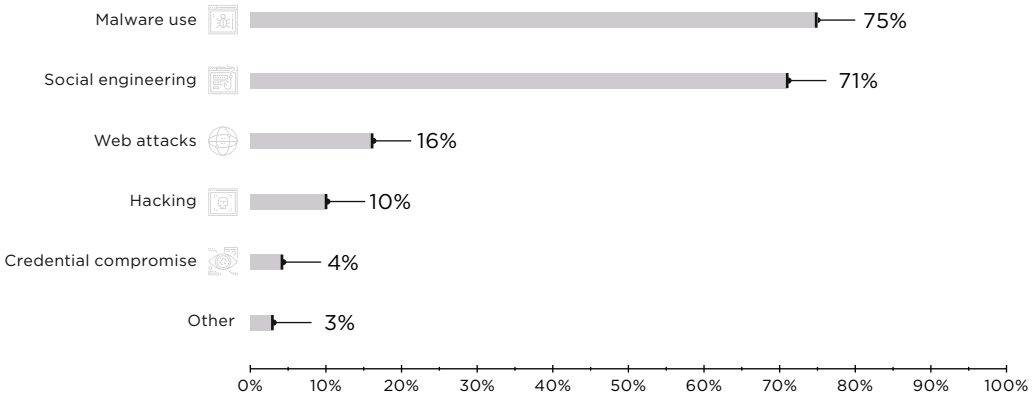


Figure 12. Government: attack methods used in Q3 2019

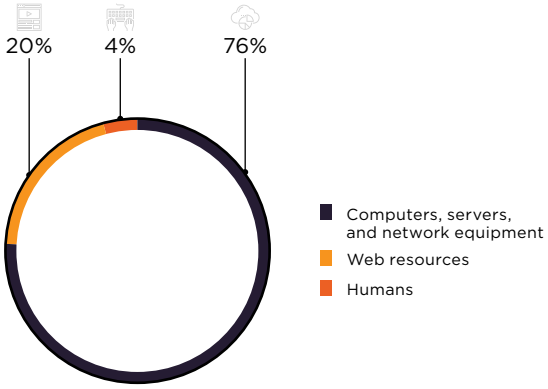


Figure 13. Attack targets

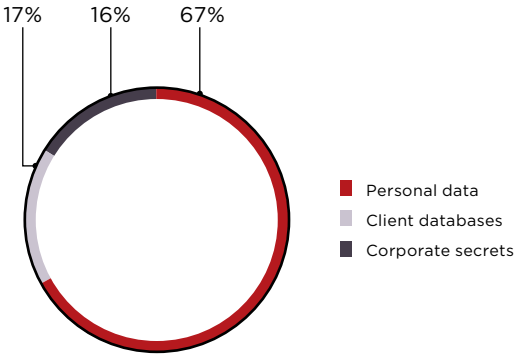


Figure 14. Data stolen

Hackers eagerly eye government targets. Ministries and departments, agencies, and city governments are at constant risk of sophisticated targeted attacks. We have noted that some criminal groups seeking to steal money do so by attacking governments. In Q3 2019, the PT ESC detected phishing mailings by TA505 to governmental entities in South Korea, China, Canada, and the United Kingdom.

The RTM group has also turned its gaze to government. In Q3, PT ESC experts detected phishing messages sent to governmental organizations in Russia and Belarus.

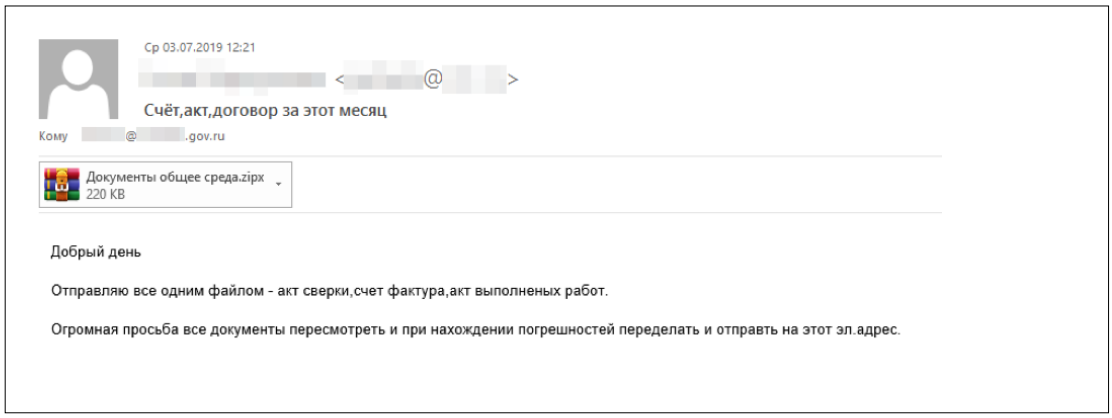


Figure 15. Phishing message from the RTM group to a Russian governmental organization

PT ESC has also noted attacks on government entities by the Gamaredon group. The attackers are interested only in entities related to the Ukrainian government: their C2 servers filter by geographic region. In their attacks, the group uses a chain of scripts that download the Ultra VNC remote control utility to the victim's computer.

Figure 16. Phishing message from the Gamaredon group supposedly from the OSCE

In addition in Q3, the PT ESC recorded attacks by APT-C-35 (also known as Donot). The group sent phishing mailings containing an Office document linking to an RTF file, which contained an exploit for vulnerability CVE-2018-0802 in Microsoft Office Equation Editor. yty malicious modules were installed on compromised computers.

Ransomware operators also have governments in their sights. They hope to receive large payouts for restoring encrypted files. And their appetites are constantly increasing. Besides Sodinokibi attacks on governments in Texas, mentioned already in the report, another wave of attacks by Ryuk ransomware hit throughout the U.S. La Porte County in Indiana paid ransom of $130,000 to cybercriminals. In New Bedford, Massachusetts, attackers demanded ransom of $5.3 million, but failed to receive it.

In 2018, we wrote about attacks on Click2Gov, an Internet portal used in many American cities to pay for municipal services. A second wave of attacks was seen in Q3 2019. The victims in August were eight cities, six of which had already fallen victim to previous attacks on Click2Gov.

Industrial companies

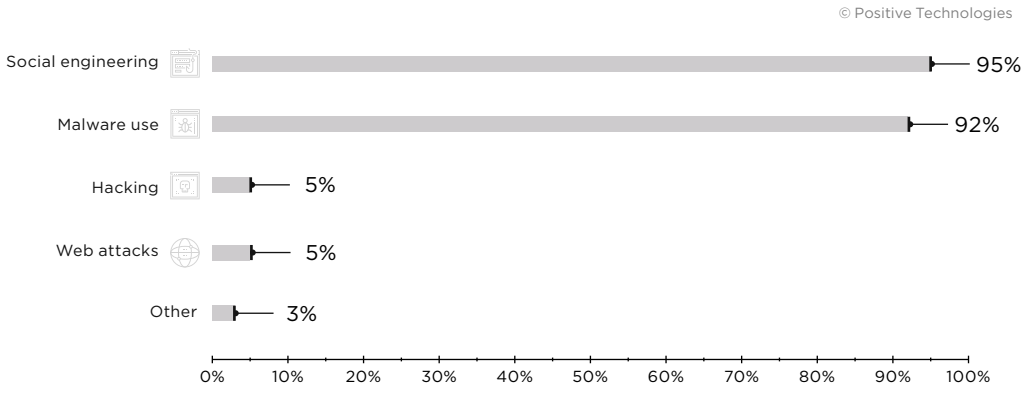


Figure 17. Industrial companies: attack methods used in Q3 2019

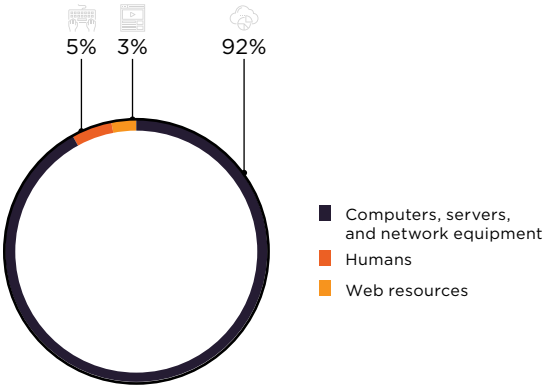


Figure 18. Attack targets

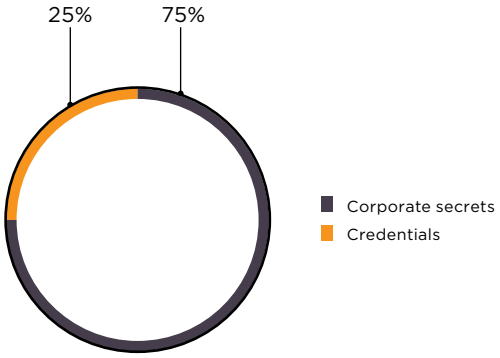


Figure 19. Data stolen

In Q3, PT ESC experts detected attacks by the TA505 APT group on American companies in the food industry, pharmaceutical companies, and medical equipment suppliers. The group also attacked industrial and energy-related companies in South Korea and Taiwan, as well as high-tech engineering companies in a number of European countries. The attackers sent phishing emails with Office documents that infected victim computers with FlawedAmmyy remote administration malware. In addition, in July our experts detected mailings to industrial companies in South Korea in which victims were infected with the ServHelper trojan. The malware was disguised by the attackers as ISO files. The PT ESC has identified two modifications of ServHelper: one can be used as a RAT, while the other acts as loader for the legitimate remote control software NetSupport Manager.

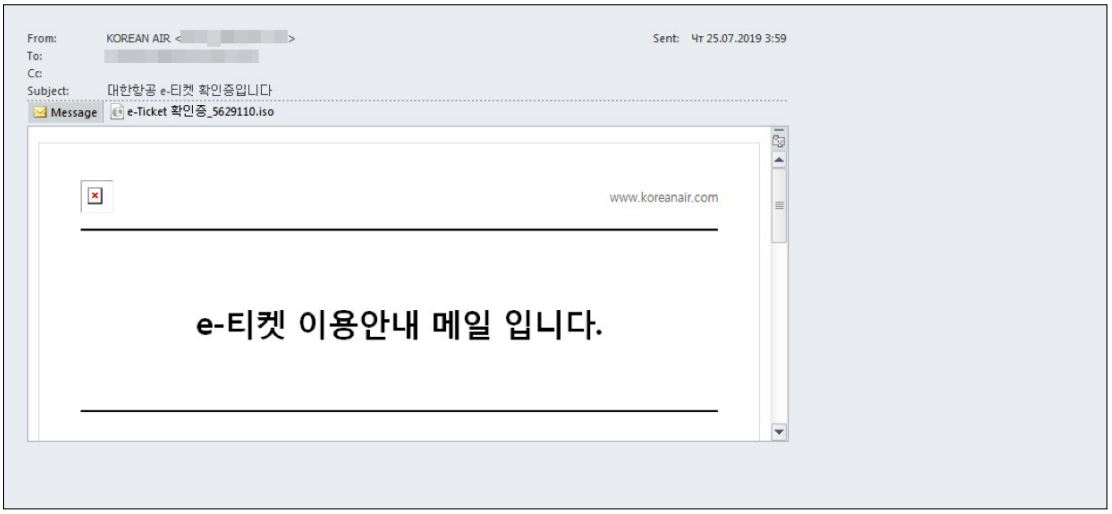


Figure 20. Phishing mesage sent by TA505 to a Korean industrial company

In August, reports appeared of an attack with LokiBot spyware on an American industrial company. The malware was delivered to the company's infrastructure in an email message supposedly from a partner company.

Restoring infrastructure at an industrial company after a targeted attack can take large investments of time and money. At the end of the quarter, major German military equipment manufacturer Rheinmetall announced that it had been hit by a cyberattack. This led to interruptions in business processes at the company's facilities in Brazil, Mexico, and the U.S. Downtime-related losses cost the company millions of euros per week. Rheinmetall estimated that restoring operations would take from two to four weeks.

In August, reports appeared of an attack with LokiBot spyware on an American industrial company. The malware was delivered to the company's infrastructure in an email message supposedly from a partner company.

Restoring infrastructure at an industrial company after a targeted attack can take large investments of time and money. At the end of the quarter, major German military equipment manufacturer Rheinmetall announced that it had been hit by a cyberattack. This led to interruptions in business processes at the company's facilities in Brazil, Mexico, and the U.S. Downtime-related losses cost the company millions of euros per week. Rheinmetall estimated that restoring operations would take from two to four weeks.

Financial institutions

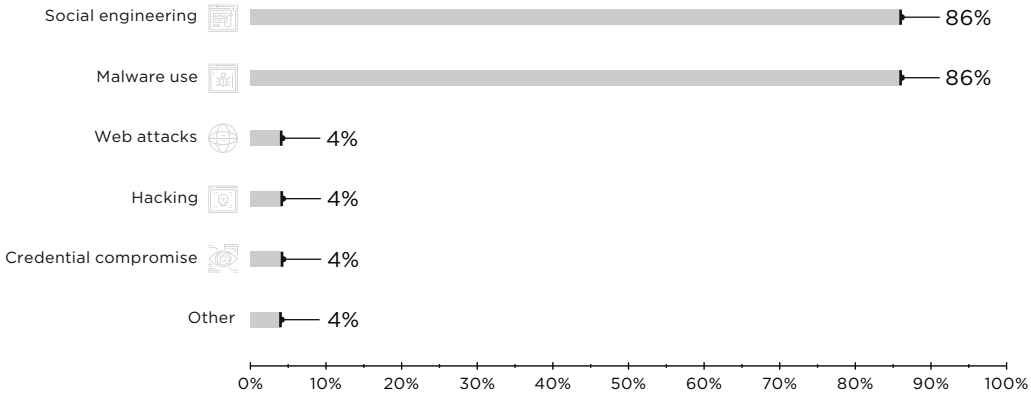


Figure 21. Financial institutions: attack methods used in Q3 2019

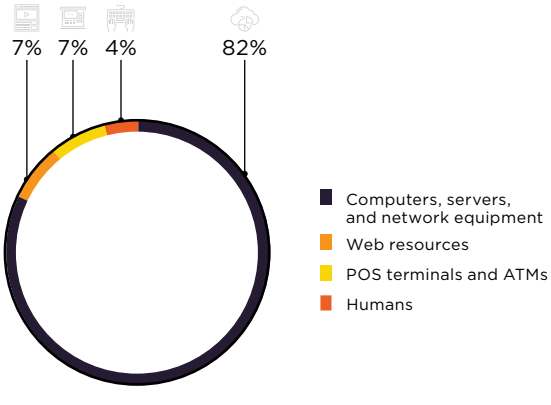


Figure 22. Attack targets

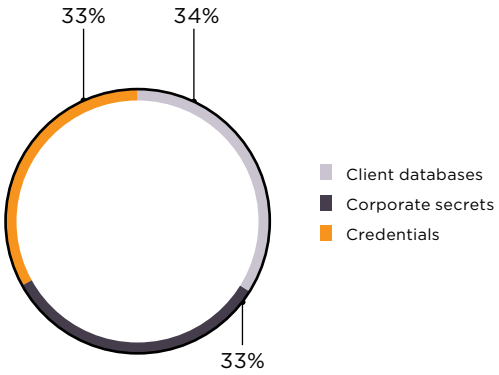


Figure 23. Data stolen

Cobalt, a financially driven APT group, remains active. Check Point announced attacks by Cobalt on banks in Kazakhstan in the third quarter. PT ESC experts detected phishing mailings to Russian and European banks. As spear phishing emails, they are carefully prepared and well composed. In July, the group sent messages from a hacked email address belonging to an employee of a Moscow airport.

Figure 24. Malicious attachment from Cobalt phishing message

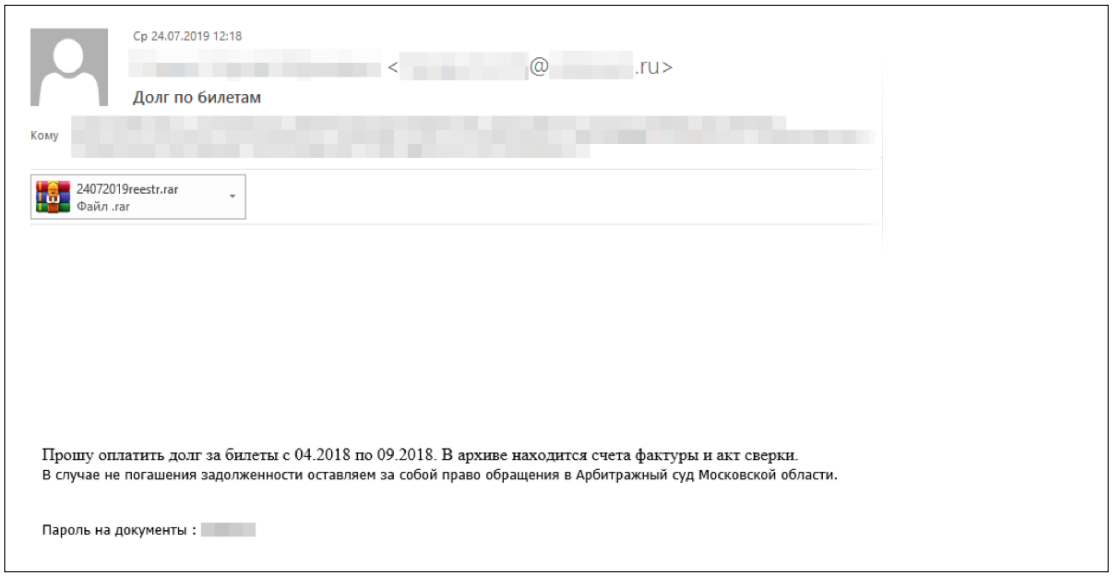


Figure 25. Phishing message, sent by the Cobalt group, supposedly from an airport employee claiming money owed for tickets

In the first half of September, the PT ESC noted phishing messages from TA505 to European and African banks. The group used Office documents with macros as their attachment of choice. These extract a DLL, save it, and run the new FlawedAmmyy loader.

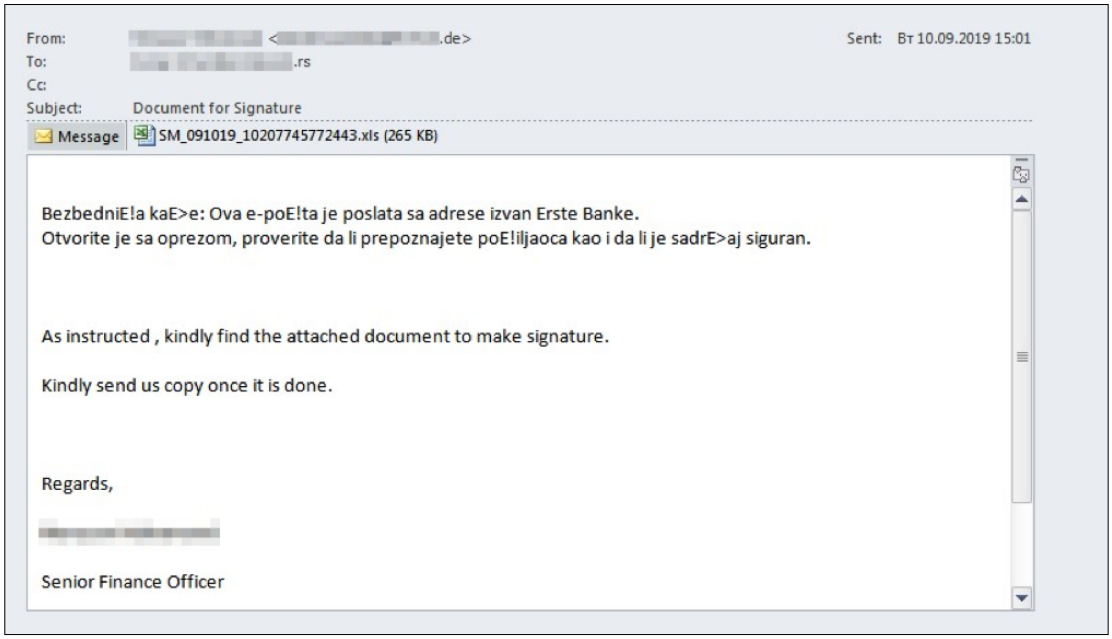


Figure 26. Phishing message from TA505 to a Serbian bank

Although the group concentrates on the industrial sector on particular, RTM regularly attempts to attack financial institutions. In Q3, the PT ESC detected phishing mailings from the group to banks in Russia and Belarus.

Science and education

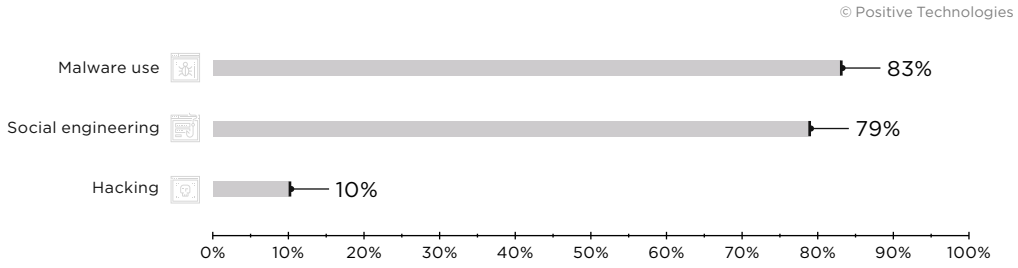


Figure 27. Science and education: attack methods used in Q3 2019

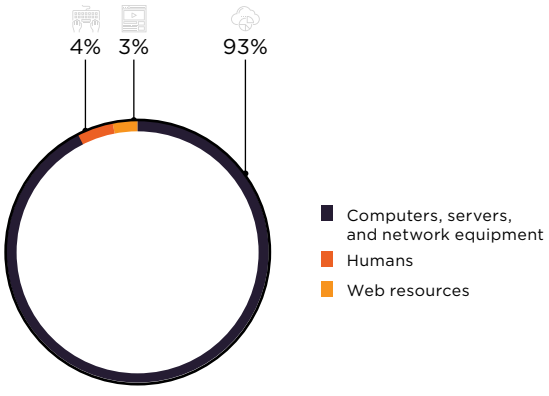


Figure 28. Attack targets

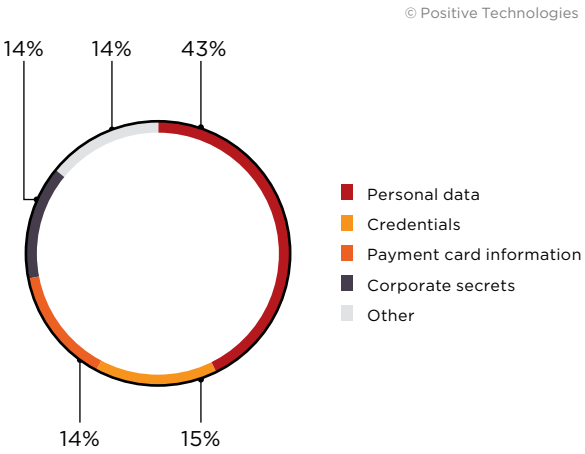


Figure 29. Data stolen

In Q3, the share of attacks targeting science and education grew to 9 percent, compared to 6 percent in the quarter prior. One possible reason is the start of the academic year. Schools are on the receiving end of numerous ransomware attacks. Cyberattacks on Louisiana schools led to declaration of a state of emergency.

The APT group Cobalt Dickens has resumed its hunt for intellectual property. Experts at Secureworks indicated that among the regular recipients of the group's phishing messages, there are 60 educational institutions. In these messages, the criminals lured victims to fake library websites, on which users were asked to log in. By entering their username and password on the page, users effectively handed their credentials over to attackers.

In summer 2019, Microsoft detected new malware, which was dubbed Nodersok. Most Nodersok infections (42%) are in the educational sector. Infections take place via malicious website advertising. Compromise begins with download of an HTA file. The result of this multistage attack is that the computer is infected with malware that turns it into a proxy server for forwarding malicious traffic.

What companies can do to stay safe

Use proven security solutions

- Centrally manage software 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. It should be able to check files both in real time and retrospectively, by automatically re-scanning files when signature databases are updated to detect previously unknown threats.
- 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.
- Deploy web application firewalls as a preventive measure.
- Detect sophisticated targeted attacks in real time and in saved traffic with deep traffic analysis. 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 attacker presence in the infrastructure, minimizes the risk of loss of critical data and disruption to business systems, and decreases the financial damage caused by 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.
- Use a different username and password for each site or service.
- 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 the security situation

- 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 taking necessary measures.
- 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).

Help clients to stay safe

- 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

- All the measures described for organizations, 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

Do not skimp on 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

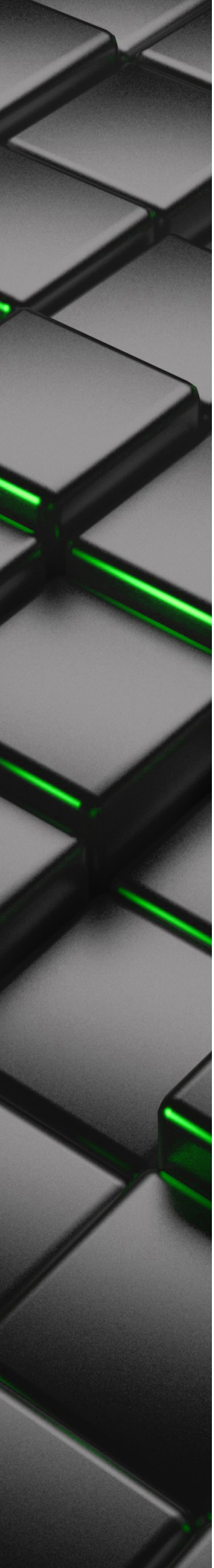
- Back up critical files. In addition to storing them on your hard drive, keep a copy on a USB drive, external disk, or a backup service in the cloud.
- Use an account without administrator privileges for everyday tasks.
- Use two-factor authentication where possible, such as for email accounts.

Do not use trivial 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 store passwords securely.
- Do not re-use passwords. Set a unique password for each site, email account, and system 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 mindful of sites with invalid certificates. Remember that data entered on such sites could be intercepted by criminals.
- 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.

For the purposes of this report, any particular mass incident (such as a virus attack in which criminals send phishing messages to a large number of targets) is counted as one unique security threat. Terms used in this report:

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

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

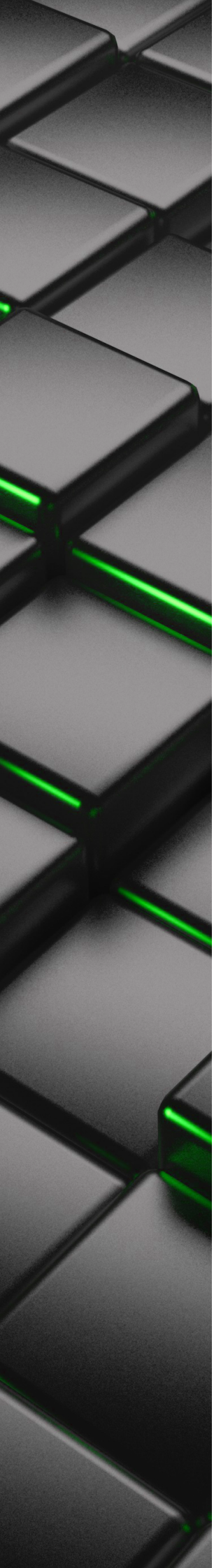
An **attack target** is the target of unauthorized actions by cybercriminals. In cases when social engineering is used to obtain information directly from an individual, client, or employee, the attack target is "Humans." On the other hand, when social engineering is part of an attempt to place malware on corporate infrastructure or on the computer of an individual, the attack target is "Computers, servers, and network equipment."

Attack motive is the overall 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. For instance, an attacker might perform reconnaissance, detect vulnerable network services available for connection, exploit vulnerabilities, and get access to resources or information. For the purposes of this report, such a 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 with respect to employer). 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, such as 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.

In our view, the majority of cyberattacks are not made public due to reputational risks. The result is that even organizations that investigate incidents and analyze activity by hacker groups are unable to perform a precise count. This research is conducted in order to draw the attention of companies and



ordinary individuals who care about the state of information security to the key motives and methods of cyberattacks, as well as to highlight the main trends in the changing cyberthreat landscape.

Group profiles

APT-C-35 (Donot, SectorE02), active since 2016, attacks organizations in South Asia: Pakistan, Bangladesh, Sri Lanka, Maldives, Myanmar, Nepal, and countries of the Shanghai Cooperation Organization. The attackers take the guise of governmental institutions, military entities, and telecom companies.

Bronze Union, also known as TG-3390, LuckyMouse, APT27, or Emissary Panda, has been involved in cyberespionage attacks since 2010. To gain a foothold on networks, the group often uses watering hole attacks: they target the websites frequented by targeted users and place malware on the websites in order to automatically infect visitors' computers. Currently the group targets governmental entities and companies involved in industry, military manufacturing, energy, aerospace, and other high-tech fields around the world.

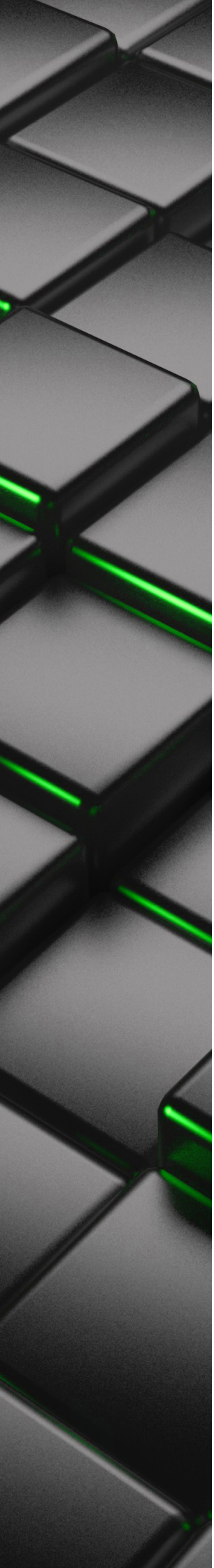
Cobalt has been known since 2016 for its attacks on financial institutions. The group started off by stealing from banks in CIS countries. Since 2017, it has expanded its range of targets to include banks in Eastern Europe and Southeast Asia. The group was named after Cobalt Strike, the penetration testing software used by the group to develop attacks within target networks. Its primary method of breaching corporate networks is phishing messages with malicious files in various formats: executable files, Office documents with macros or exploits, LNK files, and passworded archives containing executable files.

Cobalt Dickens first caught attention in 2017. In 2019, the group attacked at least 380 post-secondary educational institutions in over 30 countries in order to obtain intellectual property. University faculty and students received phishing messages claiming to come from libraries. The messages pointed to phishing pages, where users were prompted to enter their credentials, which were then used by the attackers to access research of interest.

eGobbler, known since early 2019, exploited Chrome vulnerability CVE-2019-5840 to show malicious advertising to users of iOS mobile devices. In the second half of 2019, the group increased its reach to all WebKit browsers, including desktop versions, running on Windows, Linux, and macOS. From August 1 to September 23, the group was able to show around 1.16 billion impressions to potential victims, in the hope of drawing them to fraudulent and phishing-related sites.

Gamaredon has been active since 2013. The attackers focus exclusively on Ukrainian governmental entities: their C2 servers perform filtering by geographic region. In their attacks, the group uses a chain of scripts to download the Ultra VNC remote management utility to the victim's computer. They use a self-developed framework named Pteranodon for full-fledged management of infected hosts. With it, the attackers can collect information about the system and users, steal passwords, run scripts and commands, and exfiltrate information to C2 servers.

KONNI has been active since at least 2014. The group's name comes from the malware named KONNI, which it used in its attacks. The malware can



steal files containing sensitive information, intercept and save passwords entered by users, take screenshots, and run commands on infected computers. The main objective of the group is espionage and access to data.

The history of **RTM** dates back to 2016. The group attempts to access corporate bank accounts and steal funds. They use phishing messages to obtain access to corporate networks. Since the very start, the group has used a consistent format in such messages. Positive Technologies data indicates that in 2018 alone, the group carried out 59 mailings, the recipients of which included financial institutions. In 2019, the group moved to use of the Bitcoin blockchain. Most targets are financial institutions, although cases have also included industry, government, and IT-related organizations. In addition, the group has used .bit domains for C2. The .bit zone is powered by the Namecoin blockchain, which acts as a censor-proof and confiscation-resistant alternative to traditional DNS registrars. Experts at the PT Expert Security Center were able to use the blockchain architecture to devise an algorithm for monitoring registration of new domains by RTM and changes in their IP addresses. This enabled warning financial institutions and the security community of new C2 servers in a matter of minutes (or sometimes even before) they entered use by the attackers.

TA505 has operated since 2014. The group's targets include major financial, manufacturing, transportation, and governmental organizations in Canada, South Korea, the United Kingdom, the United States, and dozens of other countries. Phishing messages are the group's main method for penetrating target networks. With each new wave of attacks, the group has made qualitative changes to its toolkit and advanced to more sophisticated techniques for maintaining stealth. Since 2014, the group's arsenal has included the Dridex banking trojan, Neutrino botnet, and several families of ransomware, including Locky, Jaf, and GlobeImposter. Since spring 2018 the group has used the FlawedAmmyy remote access trojan, and since late 2018, the new ServHelper backdoor.

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-Q3_A4.ENG.0003.02