Cybersecurity Threatscape

2019

ptsecurity.com

Contents

Symbols used

Attack targets

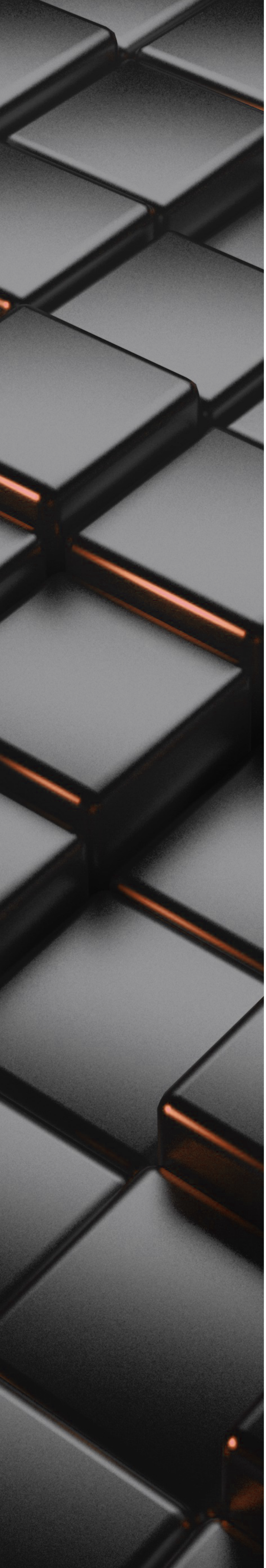
- Computers, servers, and network equipment
- Web resources
- Humans
- POS terminals and ATMs
- Mobile devices
- IoT

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

- The number of unique attacks increased every quarter, and at year-end it was 19 percent higher than the total for 2018.
- Top target sectors were government, industry, healthcare, science and education, and finance. These industries received the brunt (54%) of all attacks against organizations.
- Industrial companies accounted for 10 percent of attack targets, compared to 4 percent in 2018. Attacks on them tend to involve malware (in 90% of cases).
- Targeted attacks prevailed over mass attacks. The percentage of targeted attacks was 60 percent, which is 5 percentage points more than in 2018. One of the reasons is an increase in APT attacks. Throughout the year, we noted high activity by 27 APT groups.
- Information is still highly valuable in the cybercriminal community. 60 percent of campaigns against organizations and 57 percent of campaigns against individuals were aimed at obtaining data. Attackers were especially interested in personal data, credentials, and payment card numbers.
- The total number of malware infections in 2019 was 38 percent higher than in 2018. Malware campaigns were so successful because both the malware itself and the methods for its delivery have evolved.
- Ransomware is one of the biggest threats to companies worldwide. It was responsible for 31 percent of all malware infections among organizations. The average ransom paid in 2019 was hundreds of thousands of dollars. Ransomware operators threaten to make stolen data public unless the victim pays a ransom.
- Throughout the year, we saw regular attacks with MageCart JavaScript sniffers. These attacks were so widespread because of supply chain compromises of developers of website software.

Cyberattacks are rapidly increasing

In 2019, we recorded over 1,500 attacks, 19 percent more than in the previous year. In 81 percent of cases, the victims were organizations. The top five target sectors in 2019 were government, industry, healthcare, science and education, and finance.

© Positive Technologies

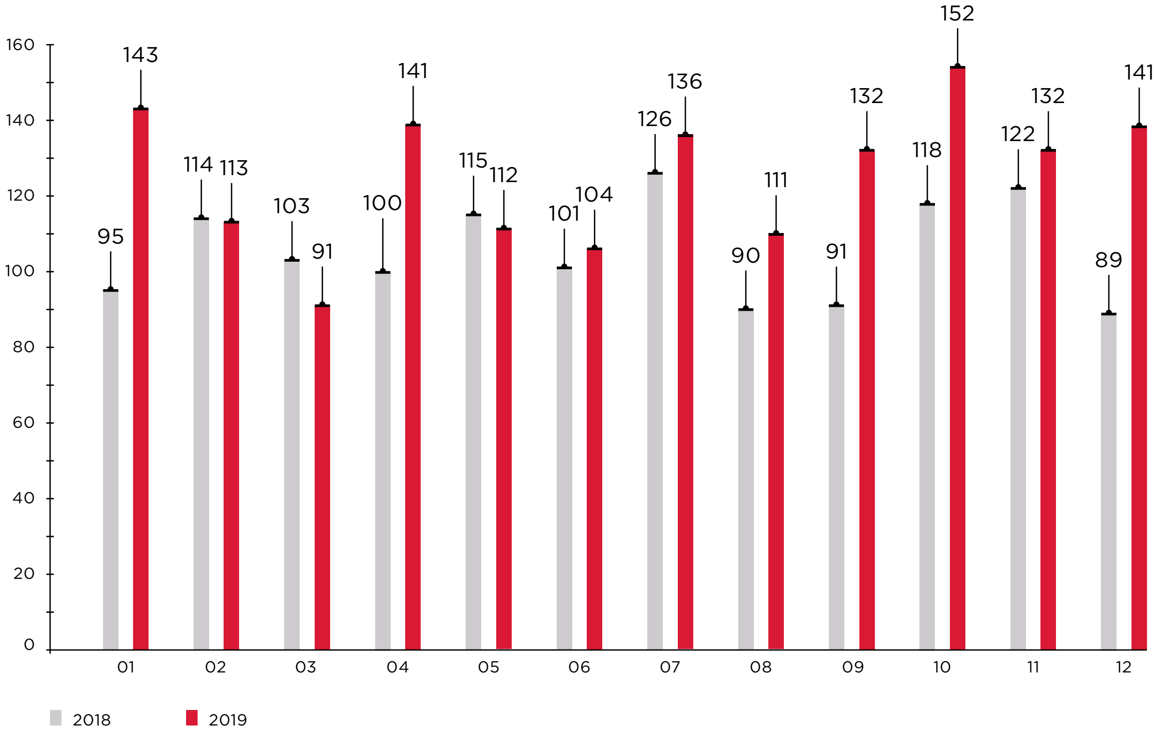


Figure 1. Number of attacks per month in 2018 and 2019

© Positive Technologies

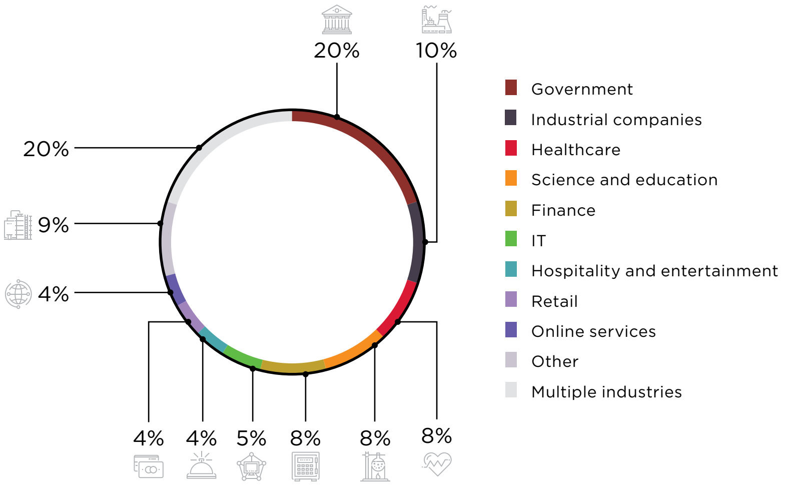


Figure 2. Victim categories among organizations

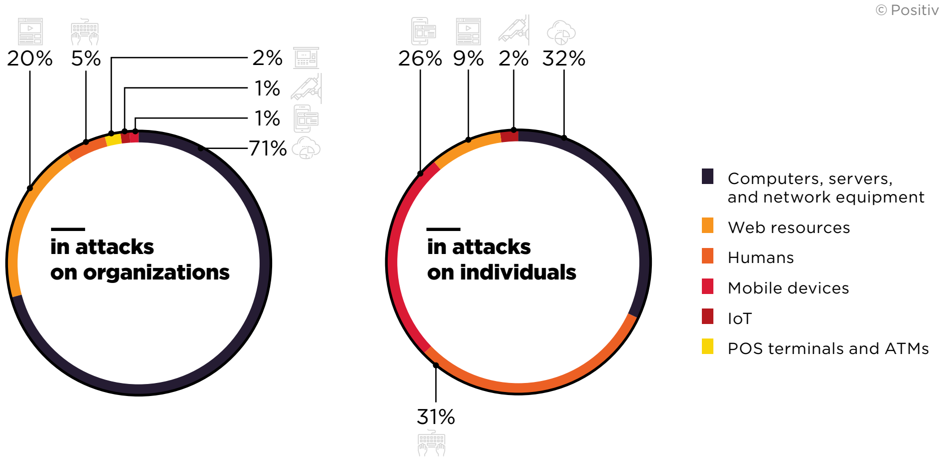


Figure 3. Attack targets

Targeted attacks take the lead

The percentage of targeted attacks increased by 5 percentage points compared to 2018, now standing at 60 percent. Every quarter, we saw more and more targeted attacks. In Q1, 47 percent of attacks were targeted. At year-end, this figure had grown to 67 percent.

© Positive Technologies

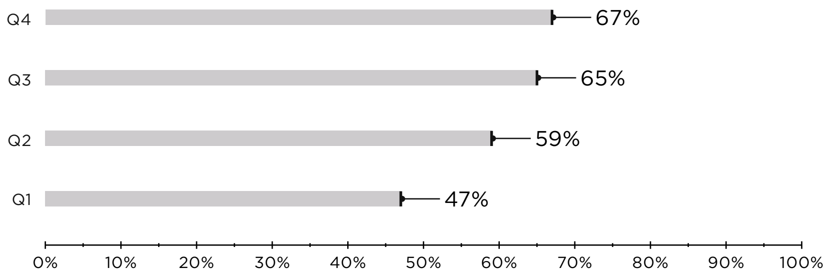
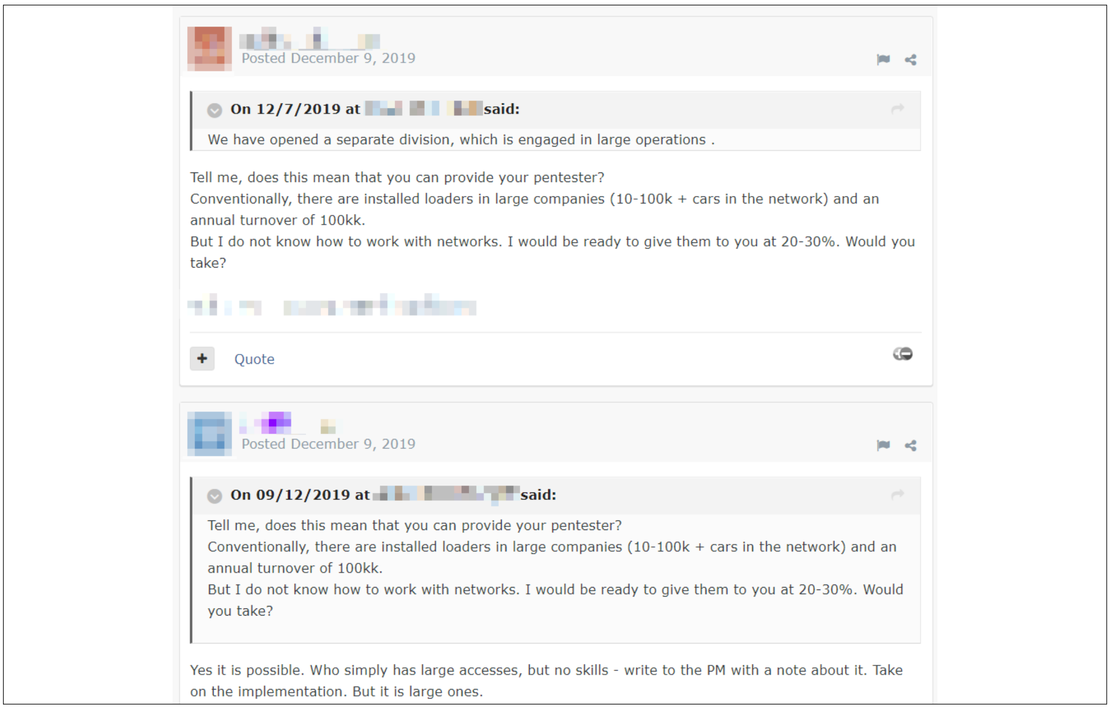


Figure 4. Percentage of targeted attacks

The increase in targeted attacks is due to several reasons. First, attackers prefer not to spend their time on mass campaigns which do not guarantee huge earnings. The current trend in the black-hat community is specialization and cooperation. When attackers join efforts, they can take on the security systems of large companies and share the profits.



[redacted]
Posted December 9, 2019

On 12/7/2019 at [redacted] said:

We have opened a separate division, which is engaged in large operations .

Tell me, does this mean that you can provide your pentester?
Conventionally, there are installed loaders in large companies (10-100k + cars in the network) and an annual turnover of 100kk.
But I do not know how to work with networks. I would be ready to give them to you at 20-30%. Would you take?

[redacted]

[redacted]
Posted December 9, 2019

On 09/12/2019 at [redacted] said:

Tell me, does this mean that you can provide your pentester?
Conventionally, there are installed loaders in large companies (10-100k + cars in the network) and an annual turnover of 100kk.
But I do not know how to work with networks. I would be ready to give them to you at 20-30%. Would you take?

Yes it is possible. Who simply has large accesses, but no skills - write to the PM with a note about it. Take on the implementation. But it is large ones.

Figure 5. A message on the darkweb from a hacker looking for accomplices

Second, every year we see new groups of attackers specializing in advanced persistent threat (APT) attacks. During the year, the Positive Technologies Expert Security Center (PT ESC) tracked APT attacks by 27 groups, ranging from well-known ones such as Cobalt, Silence, and APT28, to relatively little-known newcomers. In 2019, PT ESC experts had the first opportunity for detailed review and analysis of the Calypso APT group, which attacked government entities in Brazil, India, Kazakhstan, Russia, Thailand, and Turkey.

Information is worth its weight in gold

In 2019, the percentage of attacks aiming to steal information from organizations was 60 percent. There were significant changes in attacker motivations in attacks on individuals: data theft was the goal of 57 percent of attacks. By contrast, in 2018, that number was only 30 percent. In 2019, data theft was the primary driver both in attacks on organizations and in attacks against individuals.

© Positive Technologies

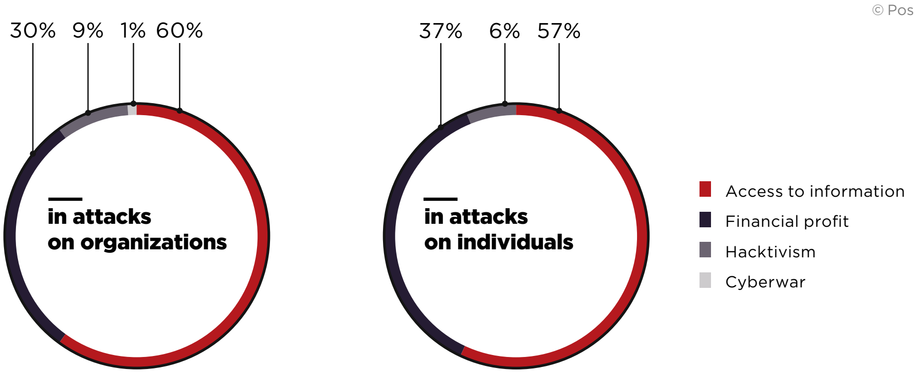


Figure 6. Attackers' motives

In attacks on organizations, hackers were mostly interested in personal data. A large portion of information stolen in cyberattacks was credentials (22% for organizations and 40% for individuals). Usernames and passwords are the keys to opening systems. So malefactors tried them on as many locks as they could. During the year, we saw a number of attacks in which compromised databases of credentials from one company were used to access systems of another company. This type of attack is called credential stuffing. In 2019, some of the victims included State Farm, an American financial group; the Dunkin' Donuts coffee shop chain; and Japanese online stores UNIQLO and GU. We believe that one of the reasons for successful credential stuffing could be the Collection #1 database published in early 2019. The database contained over a billion unique username/password pairs.

© Positive Technologies

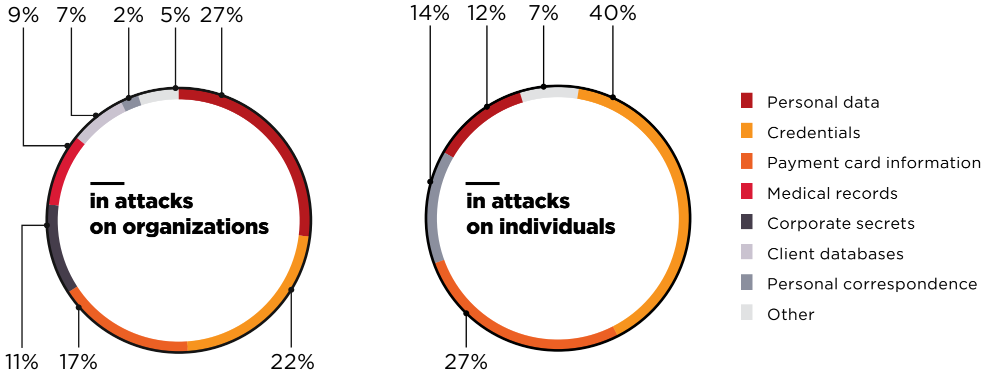


Figure 7. Types of data stolen

Malware develops by leaps and bounds

In 2019, malware infection increased by 38 percent compared to 2018. In 41 percent of cases, malware infection was combined with social engineering.

Malware campaigns were so successful because both malware itself and the methods for its delivery have evolved. First, in 2019 attackers were clever in hiding their malware. For instance, they could hide malware in files with whitelisted extensions to prevent detection by antivirus software. For stealth, they took advantage of legitimate processes and embedded mechanisms; signed malware with legitimate certificates; and actively used fileless infection techniques. In September 2019, Trend Micro released a report stating that fileless attacks in the first half of 2019 increased by 265 percent compared to the first half of 2018. At the end of 2019, Bitdefender described a new technique for infecting computers with miners, ransomware, and spyware by means of RDP. Second, attackers boosted their malware with new exploits, including exploits for vulnerabilities in popular software. For instance, the vulnerability in WinRAR, which was much spoken about in 2019 and affected half a billion users, was used both for infecting computers with JNEC.a ransomware and as part of complex targeted attacks. And finally, attackers tried to make their malware multifunctional, to improve the chances of profit from infection. For instance, a new rootkit called Scranos steals credentials and payment information, installs adware, and subscribes the victim to YouTube channels.

© Positive Technologies

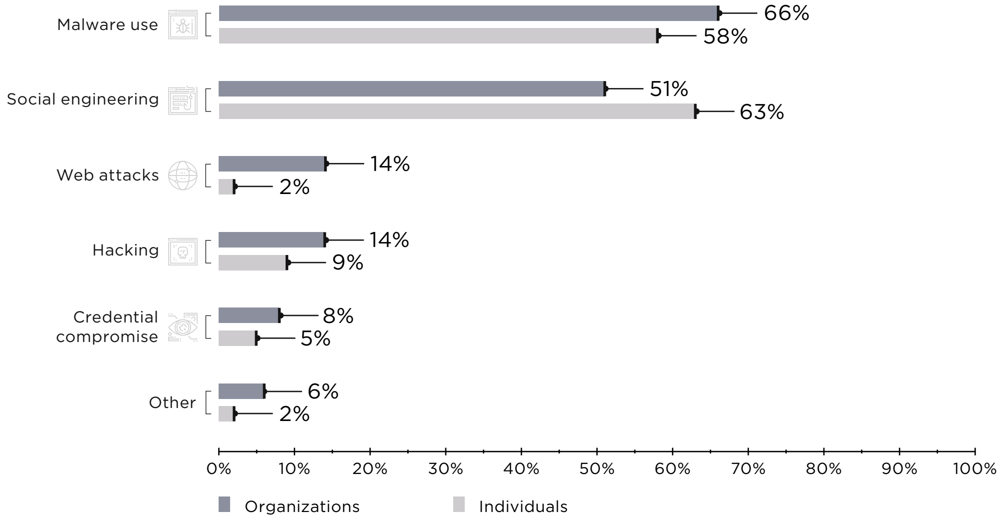


Figure 8. Attack methods

© Positive Technologies

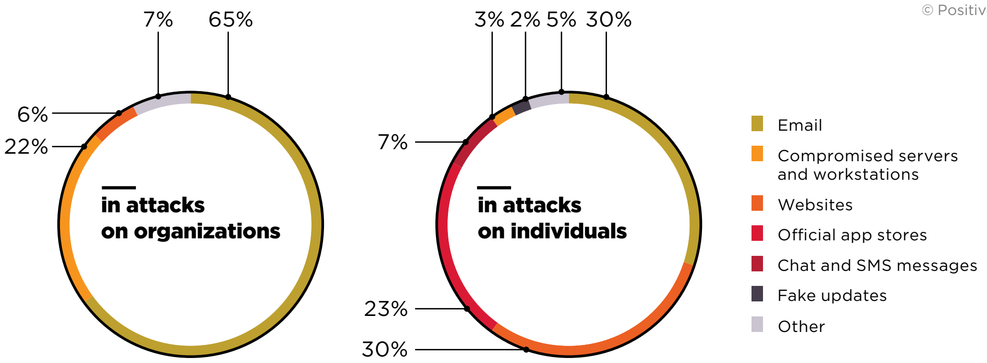
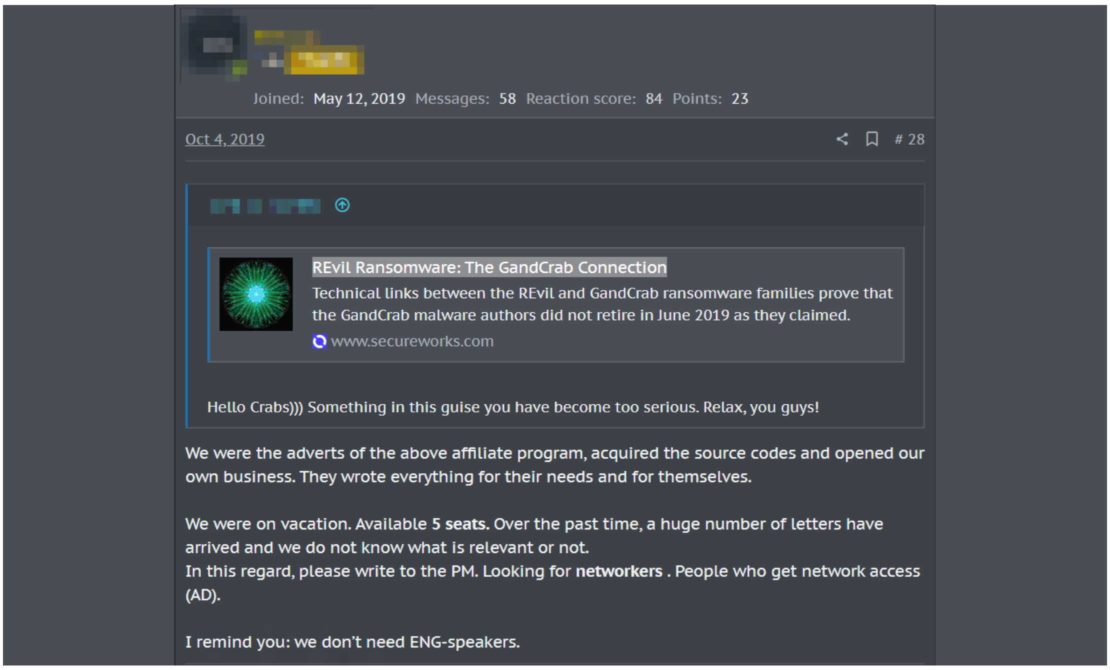


Figure 9. Malware distribution methods

Ransomware on the move

In attacks on organizations, 31 percent of malware infections were associated with ransomware. Over the year, dozens of cities, schools, universities, medical institutions, industrial facilities, and IT companies fell victim to such attacks. Main infection vectors were phishing emails, exploitation of vulnerabilities in software, and RDP attacks. Infection of government institutions peaked in the first half of 2019. In the second half of the year, we saw a spike in ransomware attacks on IT companies and educational institutions. Many victims opted to pay a ransom, which averaged several hundred thousand dollars. In the fall, the FBI released a statement providing security recommendations and urging victims not to pay up.

In the first half of 2019, the operators of GandCrab ransomware were some of the most active. However, at the end of spring 2019 they stated they were done with cybercrime. In April, there were first reports of attacks with new ransomware called Sodinokibi (aka REvil). Technical analysis of Sodinokibi revealed numerous similarities with GandCrab. In the fall, the anonymous malefactors behind Sodinokibi attacks posted on a darkweb forum that they had purchased GandCrab source code, adapted it to their needs, and were preparing new attacks.



Joined: May 12, 2019 Messages: 58 Reaction score: 84 Points: 23

Oct 4, 2019 # 28

REvil Ransomware: The GandCrab Connection
Technical links between the REvil and GandCrab ransomware families prove that the GandCrab malware authors did not retire in June 2019 as they claimed.
www.secureworks.com

Hello Crabs))) Something in this guise you have become too serious. Relax, you guys!

We were the adverts of the above affiliate program, acquired the source codes and opened our own business. They wrote everything for their needs and for themselves.

We were on vacation. Available **5 seats**. Over the past time, a huge number of letters have arrived and we do not know what is relevant or not.
In this regard, please write to the PM. Looking for **networkers** . People who get network access (AD).

I remind you: we don't need ENG-speakers.

Figure 10. Connection between GandCrab and Sodinokibi

Starting in November, ransomware operators started threatening victims with disclosure of the data they had copied before encrypting. As of the end of 2019, such attacks were carried out by hackers operating Maze and the aforementioned Sodinokibi. The potential connection between Sodinokibi and the infamous GandCrab, whose previous owners claim they had made $2 billion in ransom, gives reason to expect a new wave of ransomware attacks in 2020, and that the trend of disclosing the data of victims who refuse to pay up will continue.

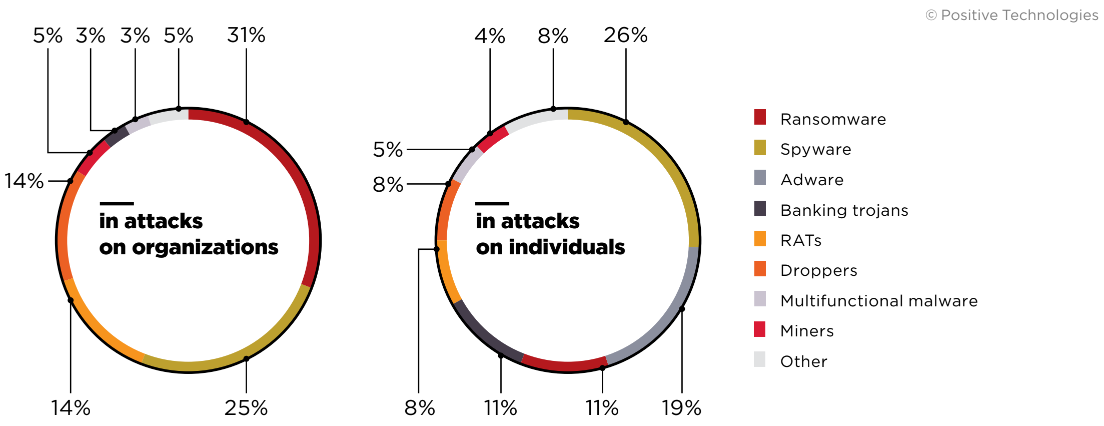


Figure 11. Types of malware

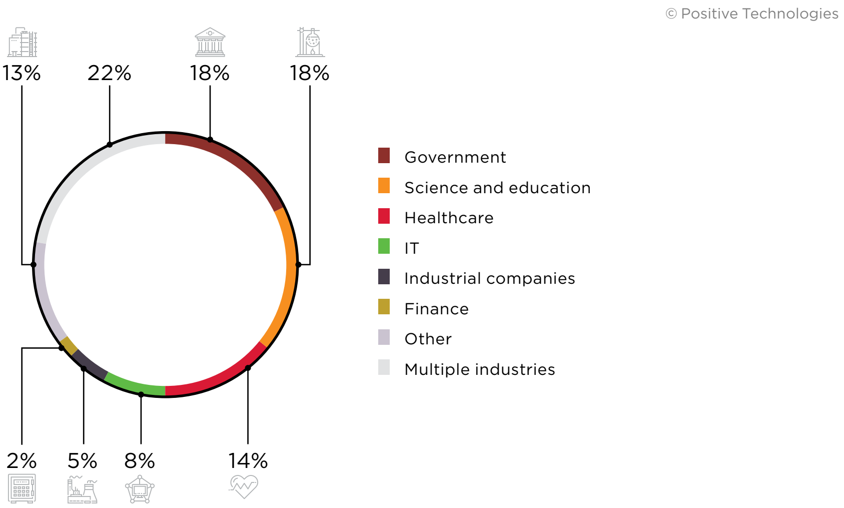


Figure 12. Ransomware victim categories among organizations

Dangerous vulnerabilities

We will now discuss some software vulnerabilities discovered in 2019 that caught the attention of the global information security community due to critical risk and the large number of potential victims. A vulnerability is especially dangerous if an exploit for it has been developed and published.

"Hack the Internet" button

- ID: CVE-2019-19781
- Publication date: December 2019
- Vulnerable software: Citrix Application Delivery Controller (NetScaler ADC) and Citrix Gateway (NetScaler Gateway)
- Severity level: Critical
- Exploit: Available

This vulnerability involves potential remote code execution without authorization. It allows an external attacker to not only access published applications, but also attack other resources of a company's internal network from a Citrix server. According to our data, about 80,000 companies were at risk as of 2019. We believe that in 2020 hackers may actively exploit this vulnerability against companies that have not implemented the protection measures recommended by Citrix.

Next day, NextCry

- ID: CVE-2019-11043
- Publication date: October 2019
- Vulnerable software: PHP-FPM
- Severity level: Critical
- Exploit: Available

A vulnerability in PHP 7 allows an attacker who is not logged in to execute arbitrary code. The threat affects nginx servers with FPM (a package for handling PHP scripts) enabled. This vulnerability caused infection of NextCloud cloud storage users with NextCry ransomware.

BlueKeep

- ID: CVE-2019-0708 (BlueKeep)
- Publication date: May 2019
- Vulnerable software: Microsoft Windows Remote Desktop Services
- Severity level: Critical
- Exploits: Multiple, including a Metasploit module

A vulnerability in implementation of the RDP protocol in some versions of Windows allows an unauthorized attacker to execute arbitrary code and spread malware. Windows Server 2008, Windows 7, Windows 2003, and Windows XP are at serious risk. This vulnerability had the potential to cause malware outbreaks on the scale of WannaCry, NotPetya, and Bad Rabbit, but this was avoided. Throughout the year, cybersecurity specialists saw regular attempts to exploit BlueKeep. However, in 2019 there were no consequences from this critical vulnerability, other than unsanctioned installation of miners.

After BlueKeep, specialists spotted two more similar RDP vulnerabilities (CVE-2019-1181 and CVE-2019-1182), with patches released in August. As with CVE-2019-0708, these vulnerabilities are wormable: they allow propagating malware with no user interaction required. Unlike BlueKeep, the vulnerabilities affected recent Windows versions, up to and including Windows 10.

Keep your finger on the Pulse

- ID: CVE-2019-11510
- Publication date: April 2019
- Vulnerable software: Pulse Secure Pulse Connect Secure (PCS)
- Severity level: Critical
- Exploit: Available

A popular VPN solution by Pulse Secure contained a vulnerability that allowed an unauthorized user to read arbitrary files, including sensitive configuration information, by sending specially crafted HTTP requests to the server. According to FBI reports, in August 2019 hackers used this vulnerability to get inside the networks of a municipal institution and a financial institution in the U.S. The same vulnerability was likely used to hack the corporate infrastructure of Travelex and infect it with Sodinokibi. In August 2019, this vulnerability, along with another dangerous vulnerability (CVE-2018-13379) in Fortinet, was exploited by APT5 (Manganese) in a campaign against telecom and technology companies.

MageCart outbreak

Every quarter, we wrote about major MageCart attacks. These are attacks in which online payment pages are injected with JavaScript sniffers that steal payment information. The name also refers to the groups behind these attacks. The first attacks of this type were seen nine years ago, but in 2019 we saw a real upsurge. Victims included online shops selling consumer goods and food, hospitality and entertainment companies, educational establishments, and the media. Mass distribution of JavaScript sniffers is the result of supply chain attacks. Throughout the year, malicious scripts reached victims' sites via third-party software intended to optimize or enhance functionality, such as advertisement platforms, content management systems, and web analytics services. In the first half of 2019, attackers searched for vulnerable Amazon S3 buckets. When attackers obtained access, they injected sniffers into JavaScript files already stored there. That campaign affected 17,000 sites. In the second half of 2019, attackers injected a sniffer into the JavaScript library supplied by e-commerce platform Volusion. According to RiskIQ, in 2019 the infrastructure of attackers behind the MageCart attacks had around 600 domains. Average dwell time on victim sites is 22 days.

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

		Sector														
		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Science and education	Retail	Telecom	Transportation	Blockchain	Other	Multiple industries	Individuals
	Total	**241**	**92**	**125**	**93**	**47**	**51**	**63**	**93**	**49**	**15**	**17**	**23**	**59**	**248**	**292**
Target	Computers, servers, and network equipment	169	82	118	54	15	18	51	72	17	13	11	14	41	195	92
	Web resources	54	5	4	22	31	14	11	17	27	2	5	6	15	27	25
	Humans	15	2	3	17	1	1	1	4	1		1	3	3	12	91
	Mobile devices	3													5	77
	POS terminals and ATMs		3				18			4						
	IoT														9	7
Method	Malware use	154	78	112	47	5	31	34	62	19	8	11	4	37	202	169
	Social engineering	130	74	105	47	2	9	20	55	15	6	11	4	30	107	184
	Credential compromise	10	2	3	15	7	9	11	9	3	2	1	3	6	19	16
	Hacking	25	5	10	4	5	4	13	9	2	1	1	14	3	73	25
	Web attacks	45	1	5	3	23	8	9	9	27	3	2	2	10	25	5
	Other	24	6	4	2	11		7	2		4		2	5	11	7
Motive	Access to information	143	61	110	57	29	42	37	40	37	11	10	9	26	118	167
	Financial profit	51	28	12	35	3	7	21	45	9		5	13	21	111	109
	Hacktivism	39	3	2	1	15	2	5	8	3	4	2	1	10	19	16
	Cyberwar	8		1										2		

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

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

Attack methods

Below are the most common attack methods used by criminals in 2019.

Malware use

© Positive Technologies

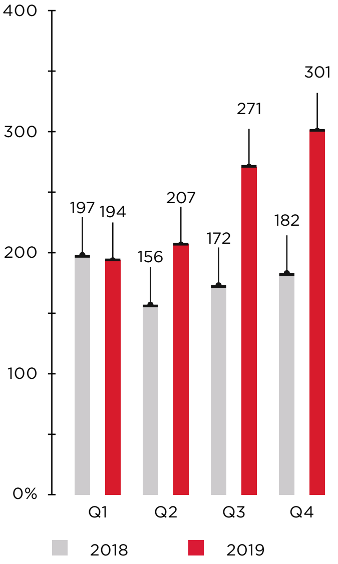


Figure 13. Number of attacks

© Positive Technologies

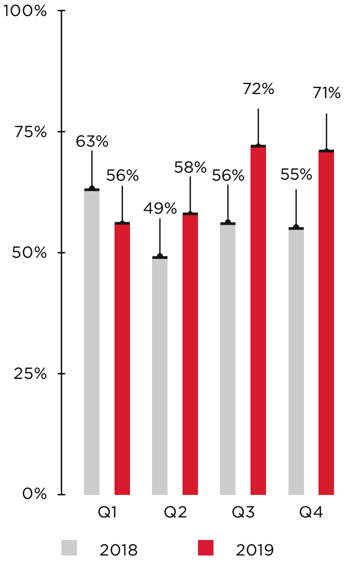


Figure 14. Percentage of attacks

Social engineering

© Positive Technologies

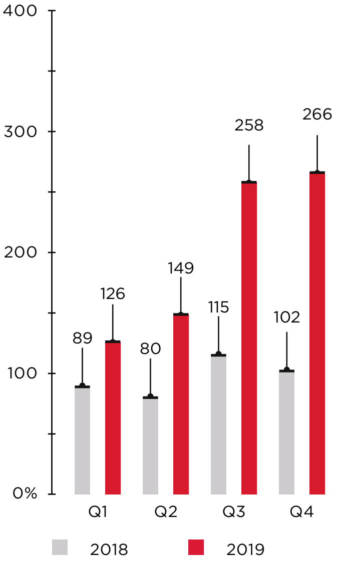


Figure 15. Number of attacks

© Positive Technologies

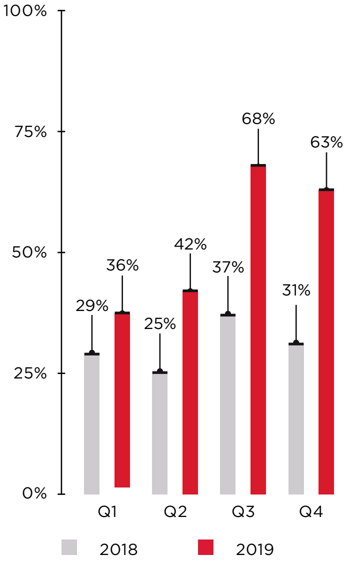


Figure 16. Percentage of attacks

Web attacks

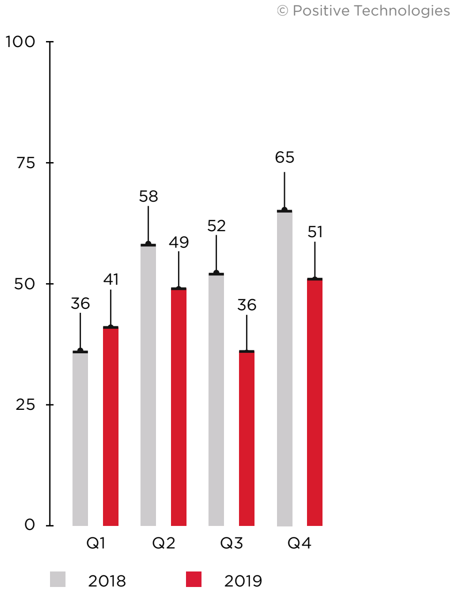


Figure 17. Number of attacks

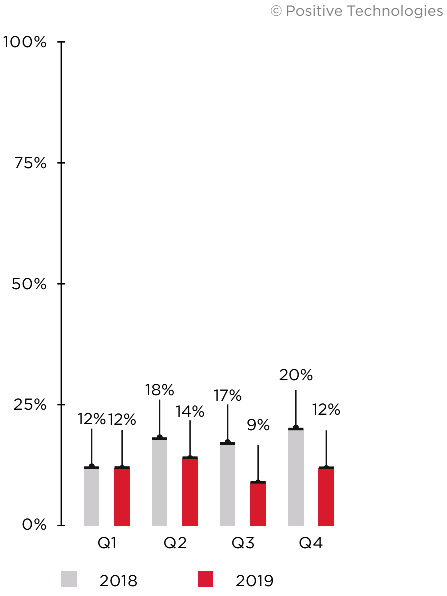


Figure 18. Percentage of attacks

Hacking

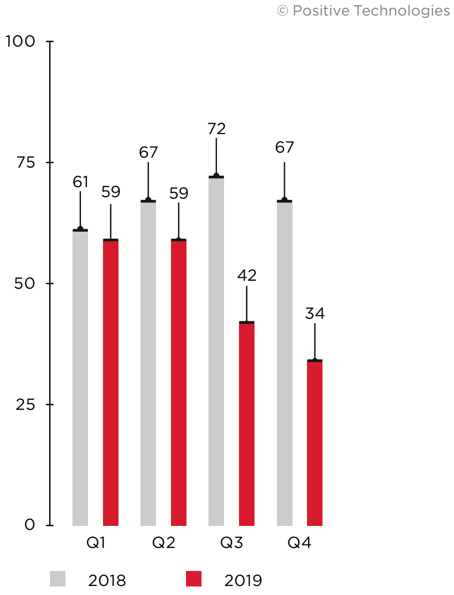


Figure 19. Number of attacks

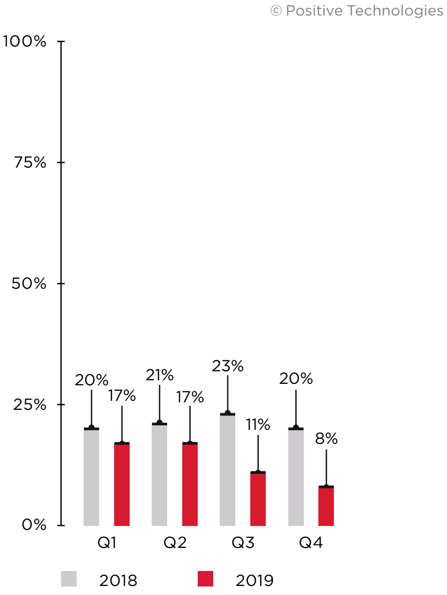


Figure 20. Percentage of attacks

Credential compromise

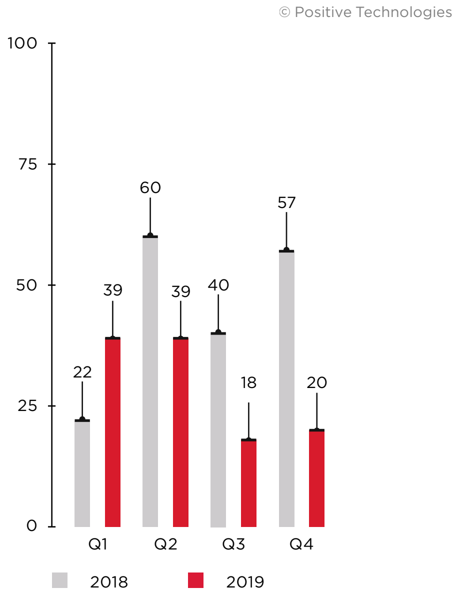


Figure 21. Number of attacks

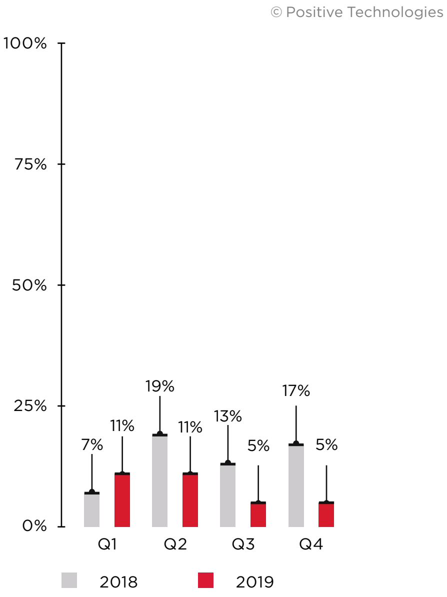


Figure 22. Percentage of attacks

Victim categories: government

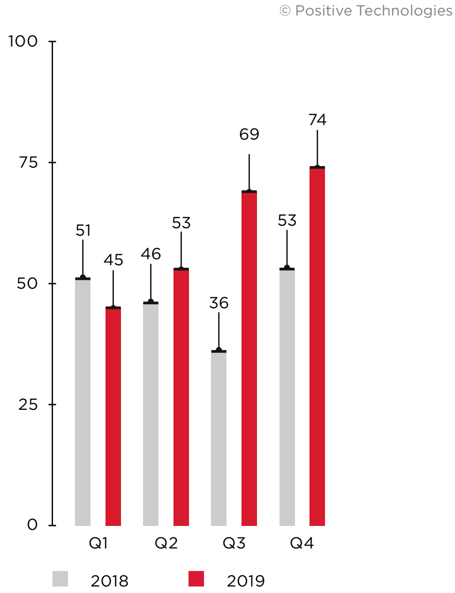


Figure 23. Number of attacks against government

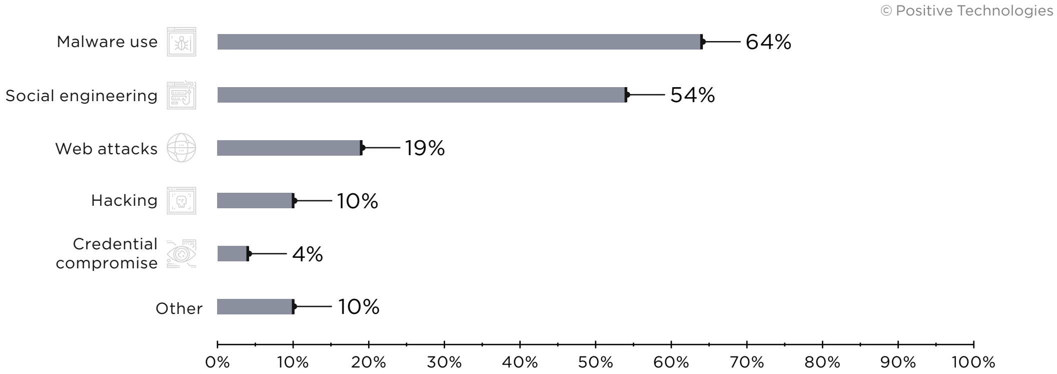


Figure 24. Government: attack methods

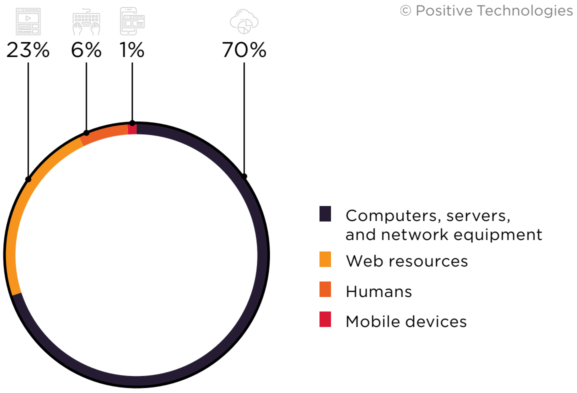


Figure 25. Attack targets

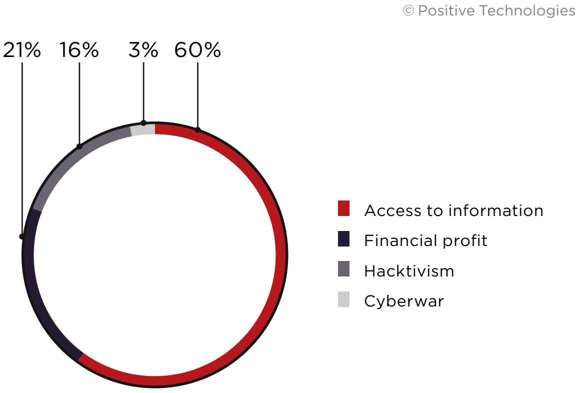


Figure 26. Attack motives

Victim categories: industrial companies

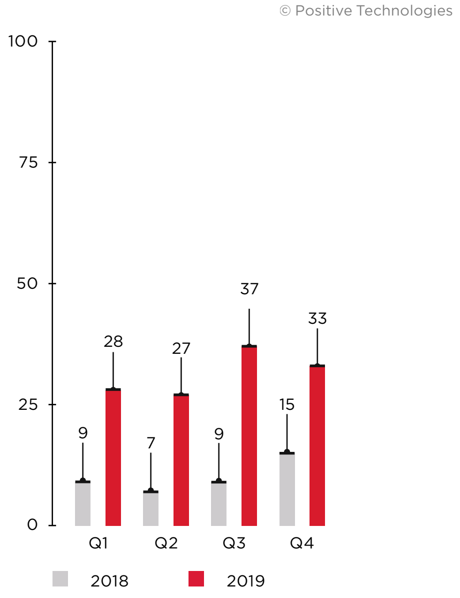


Figure 27. Number of attacks against industrial companies

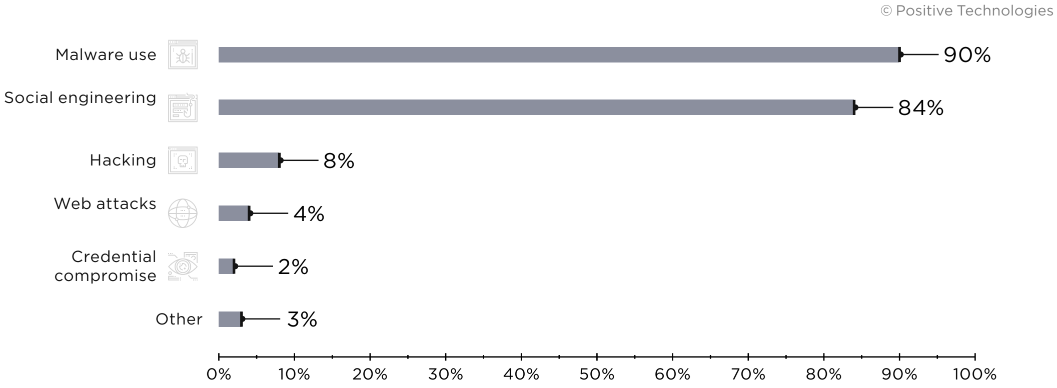


Figure 28. Industrial companies: attack methods

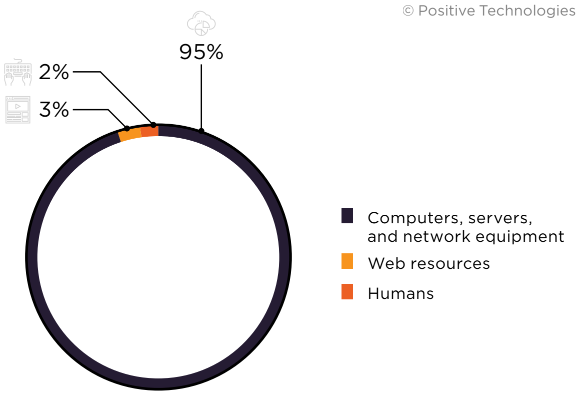


Figure 29. Attack targets

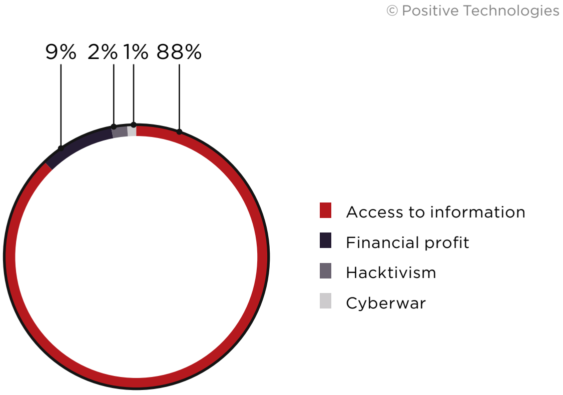


Figure 30. Attack motives

Victim categories: financial institutions

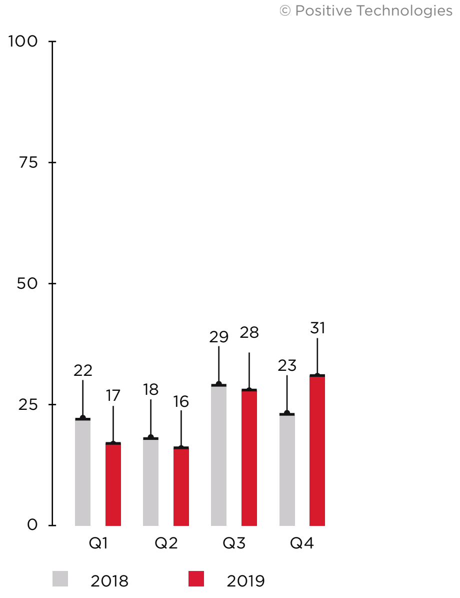


Figure 31. Number of attacks against financial institutions

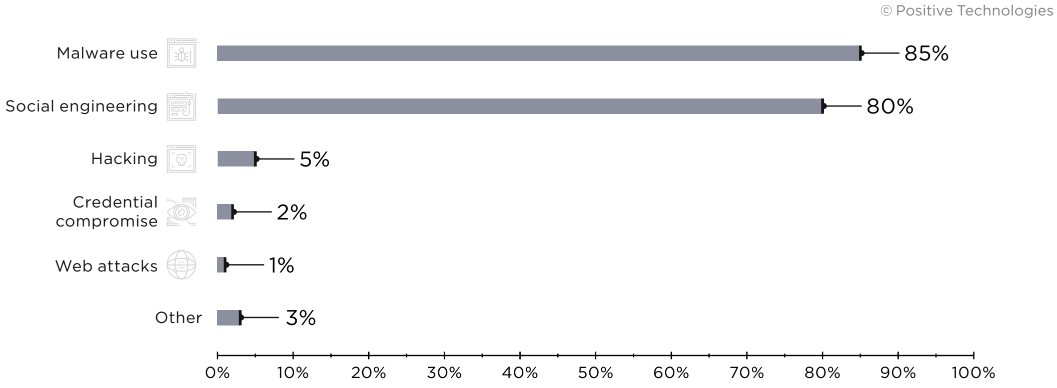


Figure 32. Finance: attack methods

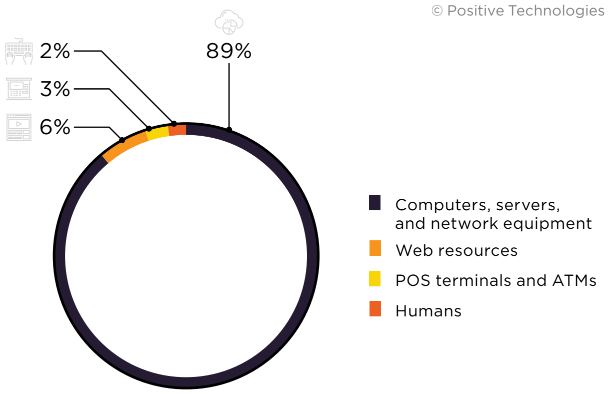


Figure 33. Attack targets

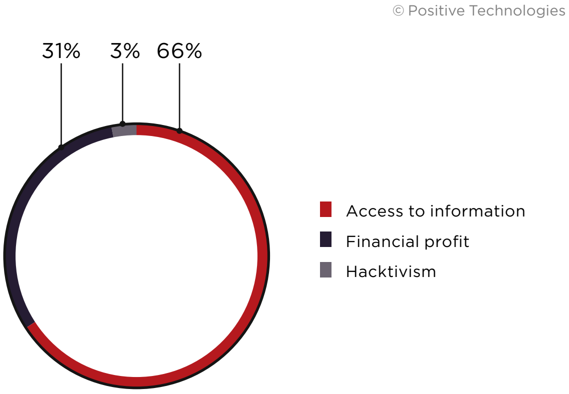


Figure 34. Attack motives

Victim categories: IT

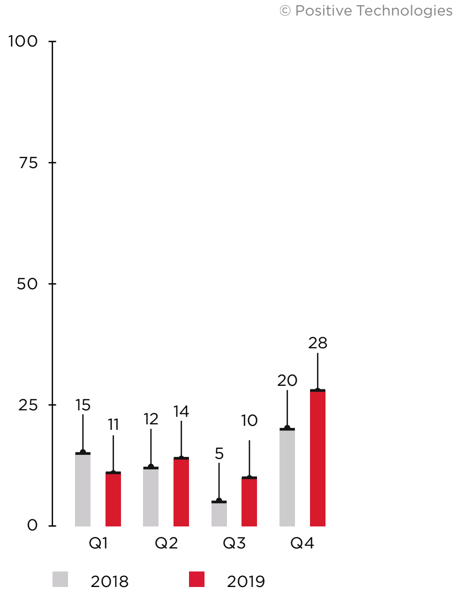


Figure 35. Number of attacks against IT companies

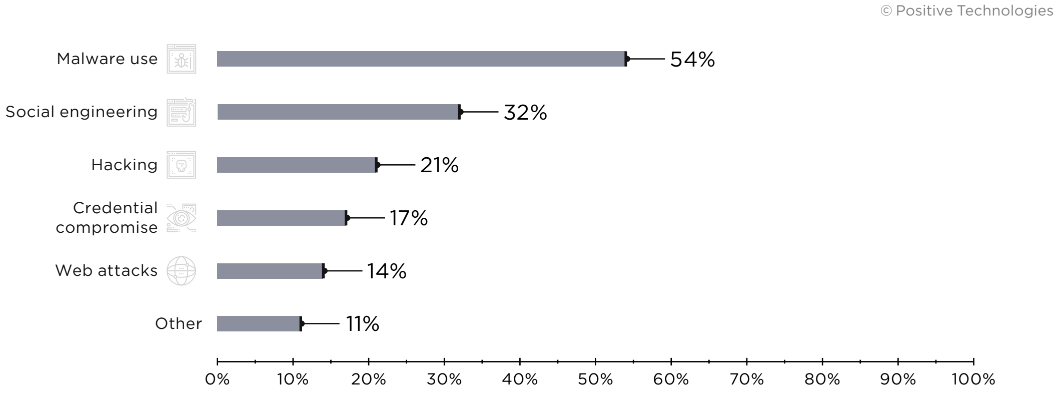


Figure 36. IT: attack methods

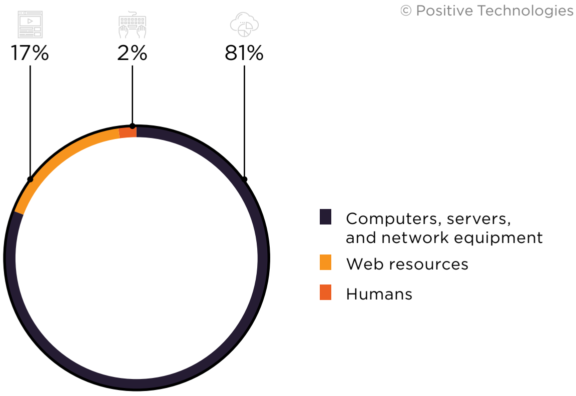


Figure 37. Attack targets

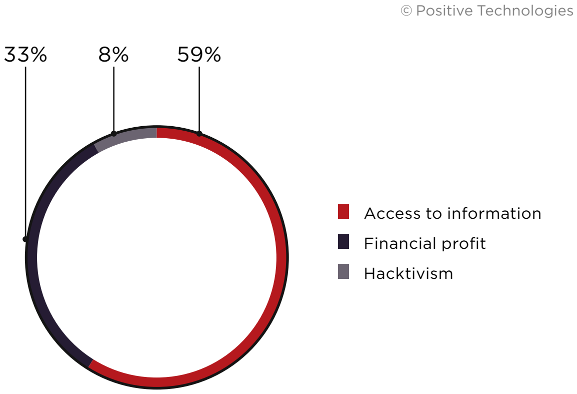


Figure 38. Attack motives

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 malicious activity, prevent infrastructure hacking, detect attackers' presence, and enable prompt measures to neutralize threats.
- Automated tools for analyzing security and identifying software 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 meet the strict password policy requirements.

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 (SDL).
- 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

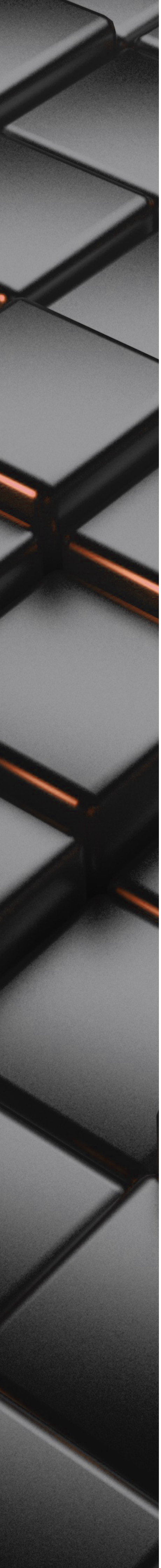
- Back up critical files. In addition to storing them on your hard drive, keep a copy on a USB drive, external disk, or a backup service in the cloud.
- Use an account without administrator privileges for everyday tasks.
- Use two-factor authentication where possible, such as for email accounts.

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 this research

In this annual 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. For instance, 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 bruteforcing 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.

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