



POSITIVE TECHNOLOGIES

# **Cybersecurity threatscape 2018**







Trends and forecasts

## Contents








Symbols used .....	2
Trends.....	3
Overall statistics.....	4
Victim categories.....	7
Government .....	8
Healthcare.....	9
Finance.....	10
Education .....	11
IT .....	12
Retail.....	13
Industrial companies.....	14
Hospitality and entertainment.....	15
Individuals.....	16
Attack methods .....	17
Malware use.....	17
Social engineering .....	18
Hacking.....	18
Web attacks .....	19
Credential compromise.....	19
DDoS.....	20
Forecasts.....	20

## 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
-  DDoS
-  Abuse of legitimate software

### Victim categories

-  Finance
-  Government
-  Healthcare
-  Education
-  Industrial companies
-  Online services
-  Hospitality and entertainment
-  Transportation
-  IT
-  Retail
-  Cryptocurrency exchanges
-  Telecom
-  Other

## Trends

In this report, Positive Technologies experts share information on the most important IT security threats. This review will briefly summarize the outcomes of 2018 and expectations for 2019.

### Key trends of 2018:

- Most cases involved targeted attacks, with their share growing throughout the year and reaching 62 percent in Q4.
- The number of attacks aimed at data theft keeps growing. Attacker interest was focused on personal data (30%), credentials (24%), and payment card information (14%).
- In 2018, healthcare institutions in the U.S. and Europe were at the center of attention from hackers, receiving more attacks than even banks and finance. In addition to stealing medical information, hackers also demanded ransom for restoring the operability of computer systems. Hospitals were ready to pay hackers, patient lives being at stake.
- Malware was used in 56 percent of attacks. Malicious software is becoming more and more available, which reduces the barrier to entry for cybercriminals.
- In 2018, attackers mostly used spyware and remote administration malware to collect sensitive information or gain a foothold on systems during targeted attacks.
- The number of cyberincidents with miners decreased, as cryptocurrencies fell in price and mining became more difficult. The share of miners diminished from 23 percent in Q1 to only 9 percent in Q4 2018.
- Criminals are increasingly turning to complex multistage techniques, including infrastructure hacks of partner companies, infecting resources of well-known software developers, and combining several methods in a single attack.
- Hackers increasingly use social engineering in attacks against organizations and individuals. Various communications methods are leveraged, including email, chat clients, phone calls, SMS messages, and even postal mail.
- DDoS attacks are becoming more powerful. 2018 was marked by the two biggest DDoS attacks in history, reaching 1.35 and 1.7 terabits per second. Hackers used memcached servers to amplify the attacks.
- Boundaries between cybercrime and other criminal activity are rapidly blurring. A lot of attacks involve theft of data, not theft of funds. Hacking computer systems may be only a first step in a major fraud scheme or tool in a cyberwar. Stolen data can be used both against individuals (for example by taking out loans in someone else's name, receiving free medical care, or obtaining expensive medications) and against organizations and even governments (such as by stealing other people's technologies and inventions).

## Overall statistics

The majority of attacks in 2018 were aimed at direct financial profit or obtaining sensitive information. However, attacks aimed at data theft often have financial implications: data can be used for stealing money, blackmailing, and can even be sold on the darkweb.

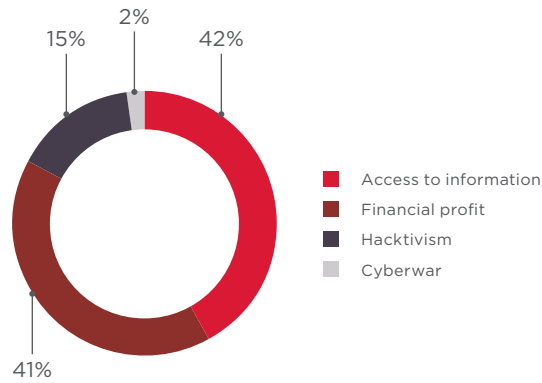


Figure 1. Attackers' motives

Unlike 2017, most attacks were targeted (55%), with their share growing gradually from quarter to quarter.

Since we count only unique cases, one attack refers to an entire malicious campaign (not an individual incident). A campaign may include multiple similar incidents, such as millions of infections by a particular piece of ransomware—and all of them will be counted as one massive attack.

Almost a quarter of attacks (23%) hit individuals. As for organizations, government institutions suffered in 19 percent of cases, whereas healthcare and financial institutions were targeted in 11 and 10 percent of cases, respectively. Large-scale cyberattacks affecting more than one industry have been placed in the "Multiple industries" category.

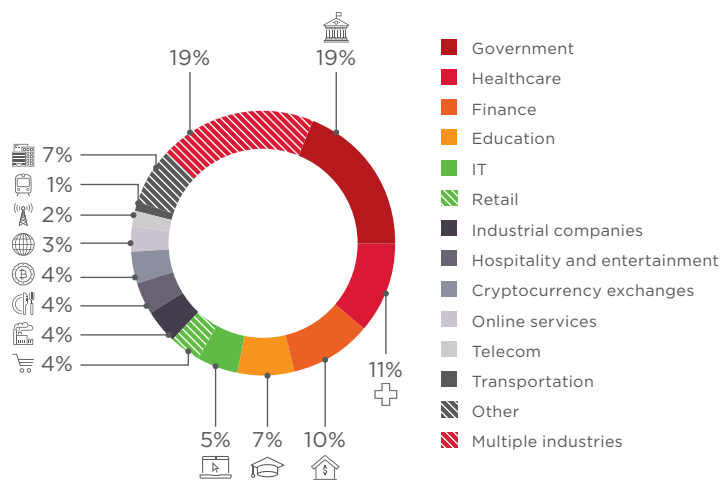


Figure 2. Victim categories among organizations

In 2018, the number of unique incidents grew by 27 percent compared to the previous year. No significant declines in hacker activity were seen during the year. Attacker activity was at its peak in February, May, July, and at the end of the year, which can be linked to major sports competitions (Winter Olympic Games and FIFA World Cup), as well as the winter holiday season, when both individuals and companies tend to be more active financially.

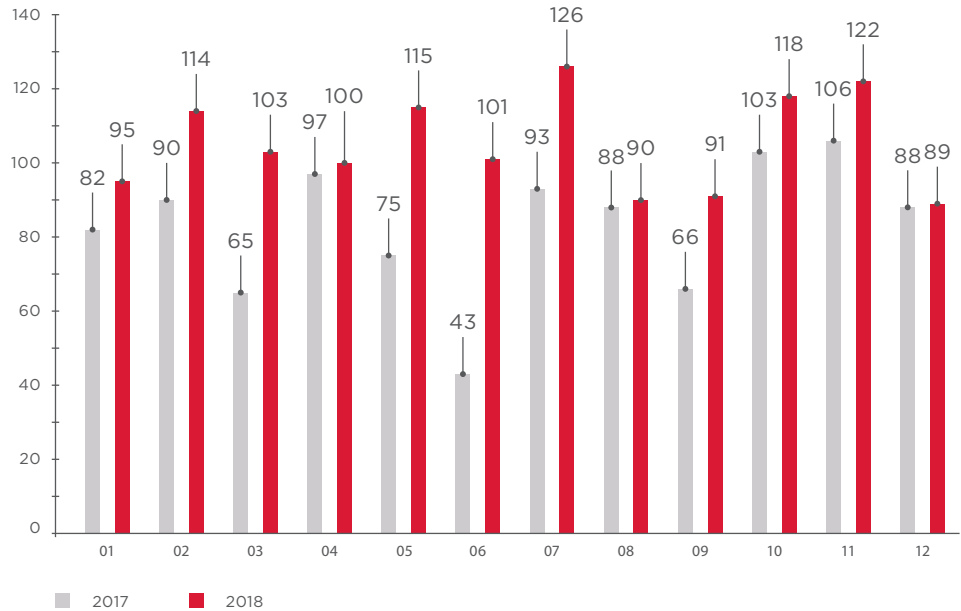


Figure 3. Number of incidents per month in 2017 and 2018 (1 = January, 12 = December)

The percentage of targets changed only minimally compared to 2017. In most cases, attackers hit corporate infrastructure (49%) and websites (26%). The share of attacks on POS terminals and ATMs decreased from 3 to 1 percent.

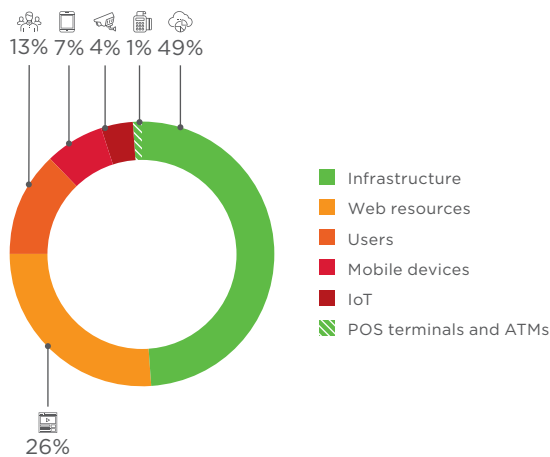


Figure 4. Attack targets

Attacks are becoming more and more sophisticated, and often consist of several stages with different methods used. Malware was used in more than half of attacks. Every third attack involved social engineering. Statistics are given at the end of the report.

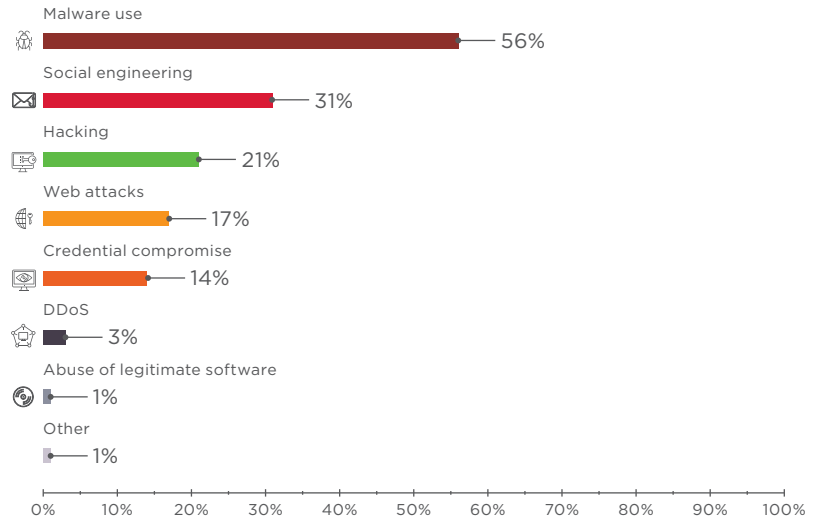


Figure 5. Attack methods

Figure 6. Per-industry classification of cyberincidents by motive, method, and target

		Industry														
		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Education	Retail	Telecom	Individuals	Transportation	Cryptocurrency exchanges	Other	Multiple industries
<b>Total</b>		<b>186</b>	<b>92</b>	<b>40</b>	<b>109</b>	<b>32</b>	<b>40</b>	<b>52</b>	<b>65</b>	<b>43</b>	<b>19</b>	<b>290</b>	<b>14</b>	<b>37</b>	<b>63</b>	<b>182</b>
Target	Infrastructure	108	64	31	72	3	14	21	38	8	11	89	6	6	32	110
	Web resources	57	7	6	18	25	14	24	14	27	6	52	5	27	21	27
	Users	16	12	1	18	4	5	7	12	6	1	66	2	4	6	7
	Mobile devices	1	2	-	-	-	-	-	-	-	-	75	1	-	1	3
	POS terminals and ATMs	-	6	-	-	-	6	-	-	2	-	2	-	-	-	-
	IoT	4	1	2	1	-	1	-	1	-	1	6	-	-	3	35
Method	Malware use	100	53	26	44	10	18	16	20	17	5	212	6	3	18	159
	Social engineering	60	45	9	27	5	7	5	25	4	3	124	1	6	18	47
	Credential compromise	26	10	1	37	2	3	5	17	5	3	33	3	7	12	15
	Hacking	34	33	10	16	8	9	15	9	6	8	22	2	23	16	56
	Web attacks	36	5	8	13	15	10	16	8	23	6	29	3	6	17	16
	Abuse of legitimate software	3	-	1	-	-	-	1	-	-	2	3	-	-	1	3
	DDoS	16	3	3	-	2	-	10	3	-	2	1	-	-	2	2
	Other	1	1	-	-	-	1	-	-	1	-	5	-	-	2	2
Motive	Financial profit	33	60	9	23	4	18	13	18	9	2	180	6	34	20	91
	Access to information	95	28	21	80	20	20	21	32	31	14	87	6	2	25	54
	Hactivism	44	4	6	6	8	2	18	15	3	3	19	2	1	17	36
	Cyberwar	14	-	4	-	-	-	-	-	-	-	4	-	-	1	1

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



## VICTIM CATEGORIES

This section analyzes the threats encountered by each of the most-attacked industries in 2018.





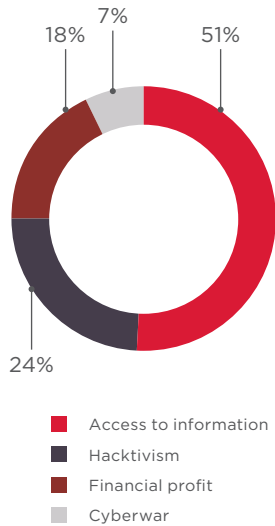


Figure 7. Attack motives

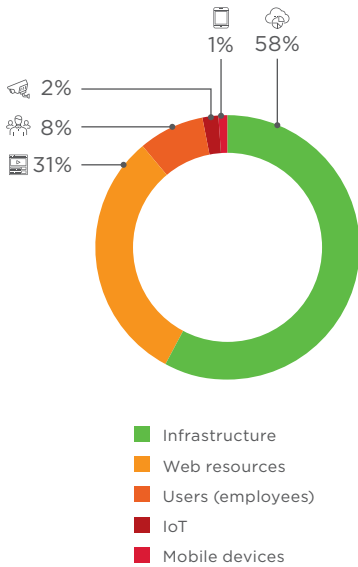


Figure 8. Attack targets

## Government

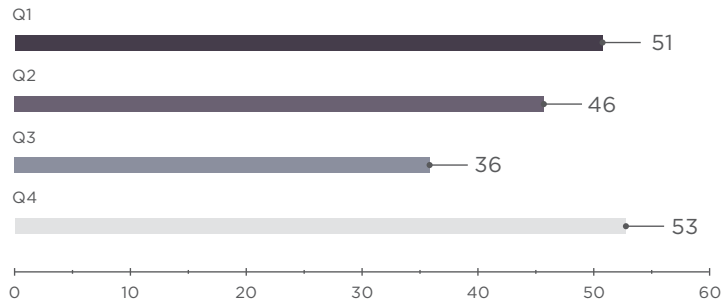


Figure 9. Number of attacks against government

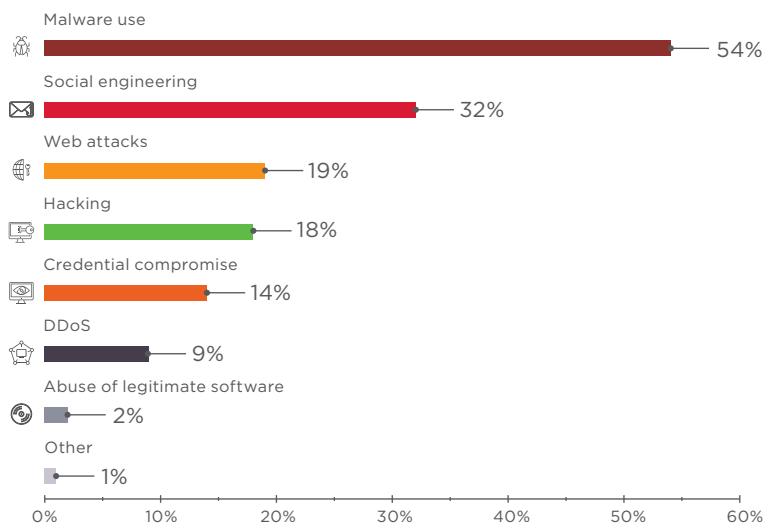


Figure 10. Government: attack methods used in 2018

Attacks were mostly driven by theft of sensitive information, which accounted for 51 percent of cases. Government websites are often targeted as a way to draw public attention: hacktivist attacks accounted for approximately a quarter of all incidents.

In most cases, hackers attacked government infrastructure and infected computers with spyware and remote administration malware. Over 20 ransomware campaigns against government institutions were recorded in 2018.

Attackers made extensive use of social engineering to penetrate internal networks: malware was distributed via official app stores, sent by email, and even delivered on CDs by ordinary post. In Q1, Positive Technologies Expert Security Center (PT ESC) experts discovered phishing emails distributing an updated version of SANNY spyware and the Fucobha Trojan. The end of the year was marked by attacks by the Treasure Hunters, Danti APT, and SongXY groups, which sent malicious documents to government institutions in Russia and the CIS.

## Healthcare

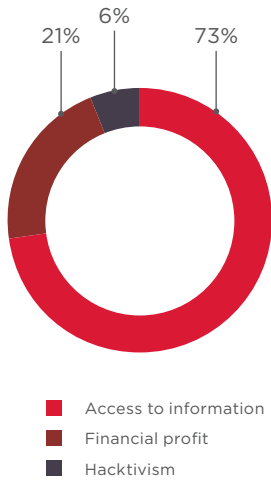


Figure 11. Attack motives

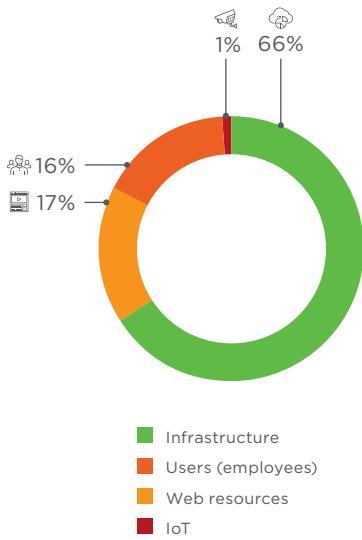


Figure 12. Attack targets

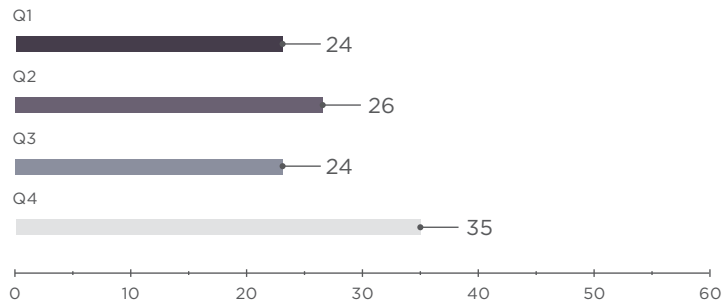


Figure 13. Number of attacks against healthcare

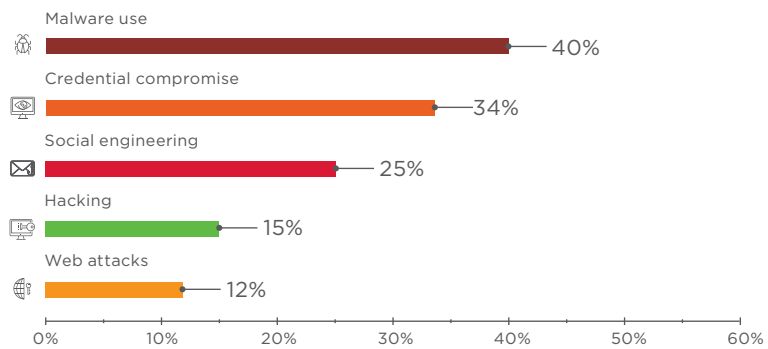


Figure 14. Healthcare: attack methods used in 2018

In 2018, hackers showed increased interest in healthcare institutions. The number of attacks against healthcare was even higher than that against the financial sector. Attackers got hold of personal data and medical information of more than 6 million people.

Hackers hunt for data but also for quick profits, knowing that uninterrupted system operation is key when patients' lives are at stake. Attackers penetrated the infrastructure of medical institutions, encrypted data, and then demanded a ransom for restoring the systems. One case in point: Hancock Regional Hospital in the U.S. paid hackers \$55,000 to regain use of its computer systems.

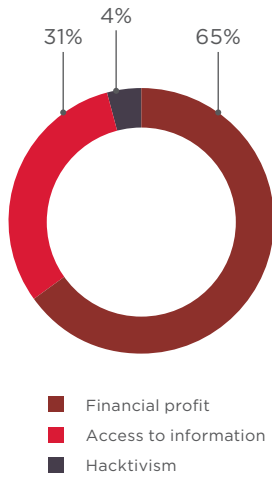


Figure 15. Attack motives

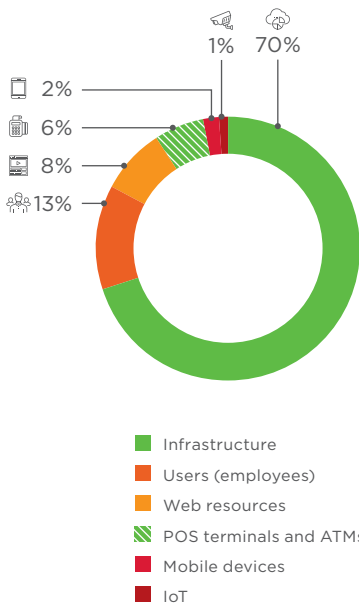


Figure 16. Attack targets

## Finance

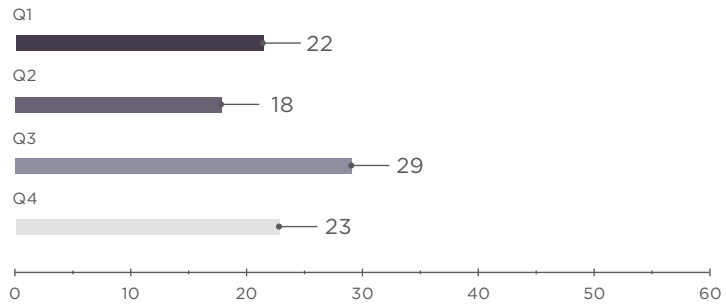


Figure 17. Number of attacks against financial institutions

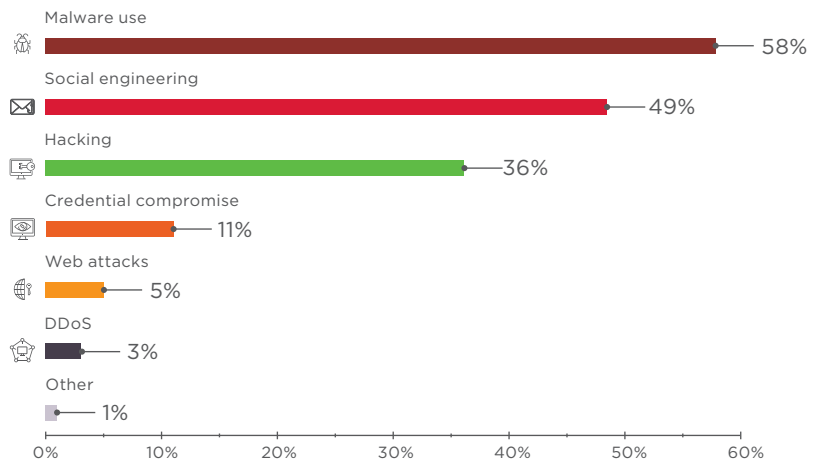


Figure 18. Finance: attack methods used in 2018

In most attacks against financial institutions, hackers were driven by direct financial profit (65% of incidents). All the same, stealing payment card information, personal data, and account credentials also accounted for a large share of incidents. Criminals can use this data to steal money from people's accounts or sell it on the darkweb.

The beginning of 2018 saw a surge of *jackpotting* attacks in the U.S., with criminals installing Ploutus-D malware on ATMs to empty them of cash. Interestingly, the fraudsters used medical endoscopes to emulate physical authentication without access to the ATM's safe.

The second half of 2018 was marked by attacks from known APT groups. PT ESC experts recorded 23 attacks by the Cobalt group. The criminals created new malware and distributed it in emails seemingly originating from trusted financial institutions.

In addition, the experts discovered a new group attacking the finance sector. The mal-factors sent malicious documents with macros that downloaded utilities providing remote access to infected computers. Phishing messages were sent from a compromised mailbox of an employee of a major financial company. In another case, they were disguised as coming from a government cybersecurity authority. A modified script earlier used by Treasure Hunters was uncovered in the documents. However, further analysis of traffic and the utilities used by the attackers indicated the emergence of a new criminal group.

## Education

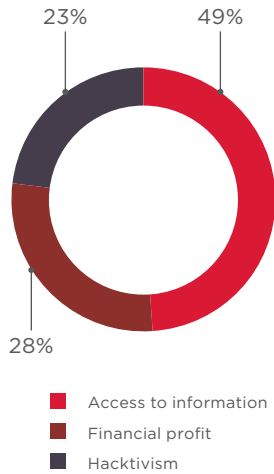


Figure 19. Attack motives

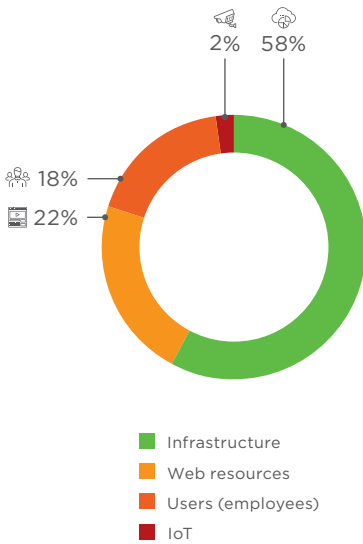


Figure 20. Attack targets

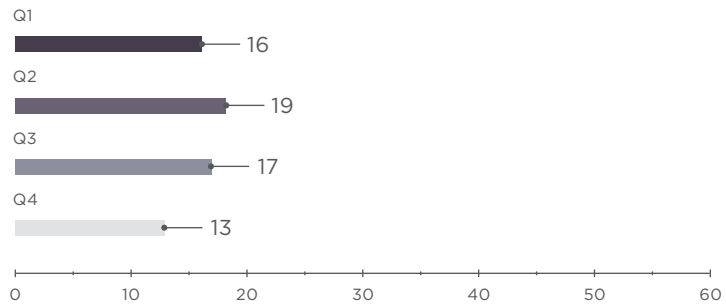


Figure 21. Number of attacks against educational institutions

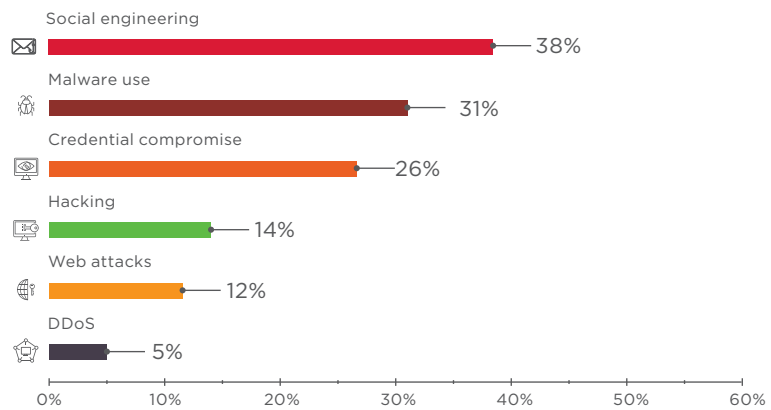


Figure 22. Education: attack methods used in 2018

By and large, criminals stole personal data of employees and students, as well as credentials used for email, bank accounts, and other services. At several educational institutions, attackers accessed bank accounts and payment documents, stealing over \$2 million in total. Every sixth attack involved ransomware. Hackers either demanded a ransom to restore data or simply wanted to paralyze the computer systems of educational institutions. Q2, which marks the end of the academic year, saw an increasing number of attacks aimed at changing grades in virtual student records.

Attempting to steal intellectual property, such as scientific work and unpublished research, hackers attacked scientific institutes. This information is often sought by government-sponsored hacker groups. Several such attacks were attributed to hackers in Iran and North Korea. Malefactors also cash in by publishing stolen research on attacker-controlled websites that users must pay to access.

IT

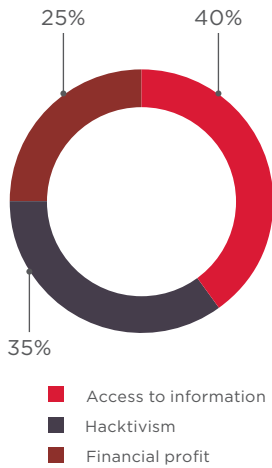


Figure 23. Attack motives

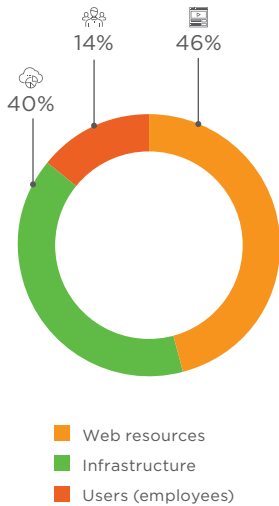


Figure 24. Attack targets

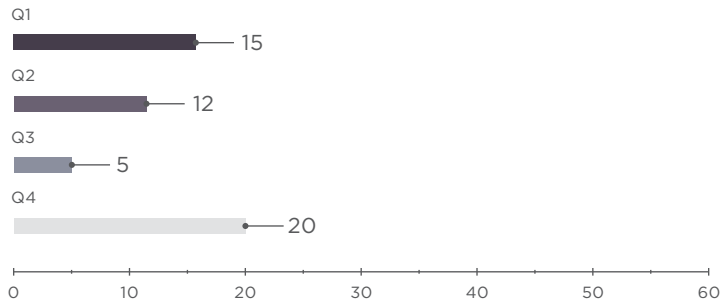


Figure 25. Number of attacks against IT companies

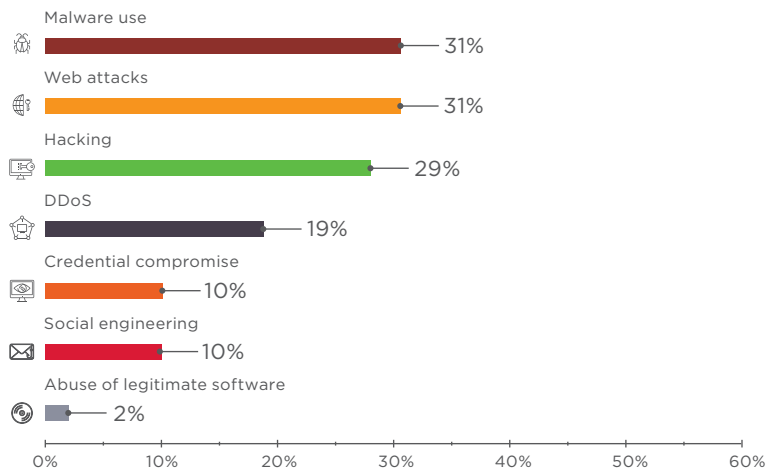


Figure 26. IT: attack methods used in 2018

Hackers attacked websites and infrastructure of IT companies. Oftentimes, such hacks are just intermediate links in more complex attacks. The servers of IT companies may store confidential client information. In the case of service providers, these systems hold data belonging to other companies, including those companies' websites. Hackers also seek to gain access to corporate email accounts in order to use them for phishing attacks. Websites of prominent software developers have become a convenient platform for distributing malware under the guise of official updates.

In Q2, PT ESC experts detected a phishing attack aimed at a major IT company: the PlugX Trojan was distributed via corporate email. The Trojan has been used by attackers for years as spyware.

IT companies were the second-most common target of DDoS attacks, after government institutions. Hackers disrupted the operations of internet service providers and game companies, which are particularly sensitive to downtime and equipment disruption.

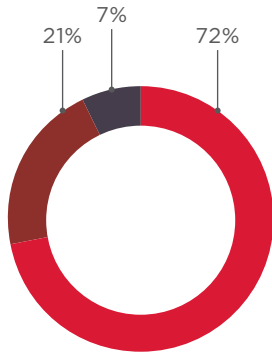


Figure 27. Attack motives

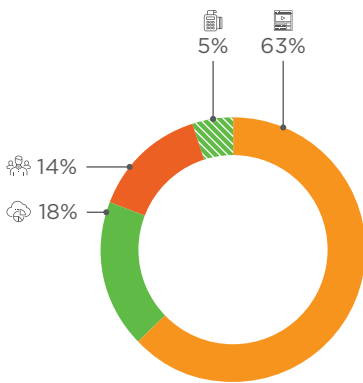


Figure 28. Attack targets

## Retail

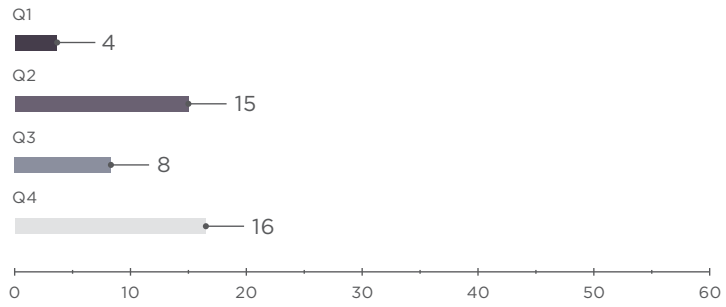


Figure 29. Number of attacks against retail

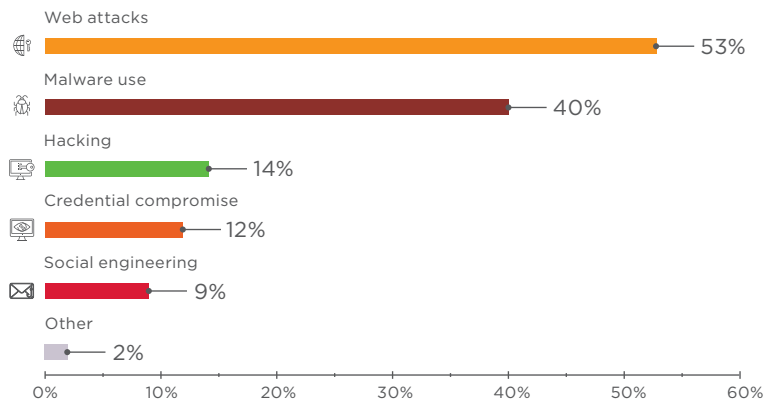


Figure 30. Retail: attack methods used in 2018

Online stores were a favorite target of attacks aimed at data theft. In 70 percent of cases, payment card information was stolen. The second part of the year was marked by attacks conducted by the Magecart group. Hackers injected malicious scripts into web applications in order to collect payment information and contact data entered by users. The number of attacks against POS terminals decreased by two thirds compared to 2017. However, POS terminals were still hit hard in one of the biggest retail attacks. Hackers installed malware on POS terminals located in Saks Fifth Avenue and Lord & Taylor stores and stole data for more than 5 million cards.

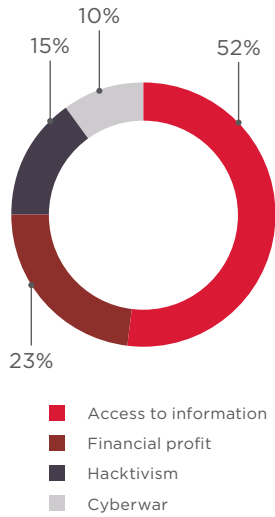


Figure 31. Attack motives

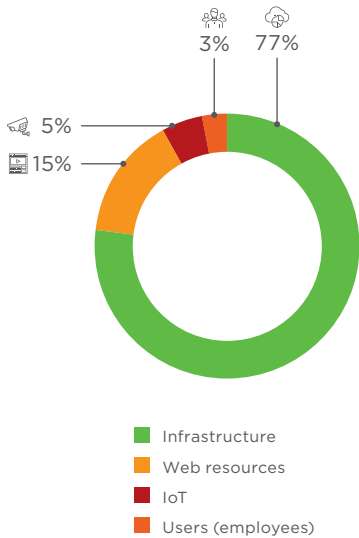


Figure 32. Attack targets

## Industrial companies

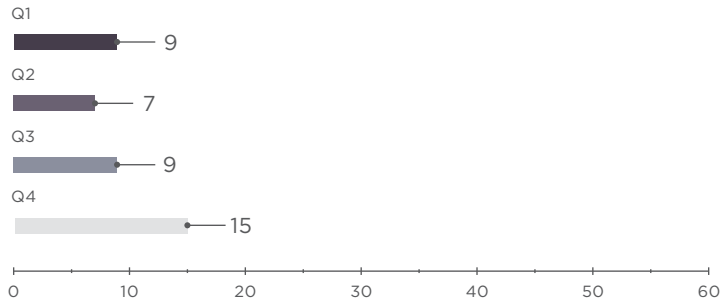


Figure 33. Number of attacks against industrial companies

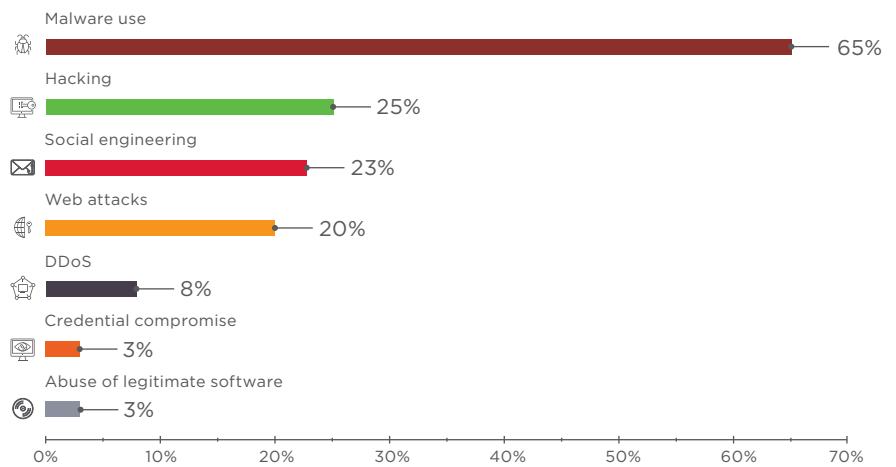


Figure 34. Industrial companies: attack methods used in 2018

The industrial sector escaped catastrophic incidents in 2018, but there were some very close calls indeed. In August, a cyberattack hit a [petrochemical plant](#) in Saudi Arabia. The attack was designed to do more than just shut down the facility. It was meant to trigger an explosion, leading to an environmental disaster and loss of life. Hackers gained a foothold on the company's computer network and stayed there for an extended period. Only coding errors in the hackers' malware prevented them from accomplishing their goal.

In Q2, security experts detected [VPNFilter](#) malware, which had infected more than 500,000 routers. The malware was designed to intercept and spoof traffic being routed through a device. The attackers seemed to have a particular interest in SCADA systems: code analysis revealed scanning of traffic for certain data used in industrial control systems.

The sector also suffered heavily as hackers stole confidential technical information, such as documents pertaining to nuclear energy and ship construction projects. They also got hold of other valuable information that could be sold to criminal groups. Among other data, documents showing the planned locations of video cameras in prisons were stolen from the servers of an [engineering company](#).

Throughout the year, PT ESC experts observed attacks by the SongXY group targeting government and defense-related organizations. The group uses spyware to track user activities and control infected computers.

## Hospitality and entertainment

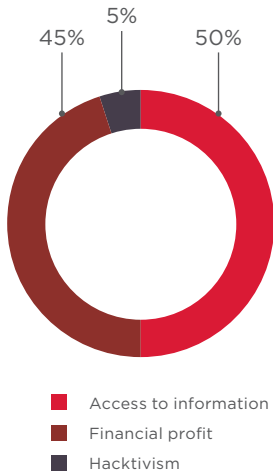


Figure 35. Attack motives

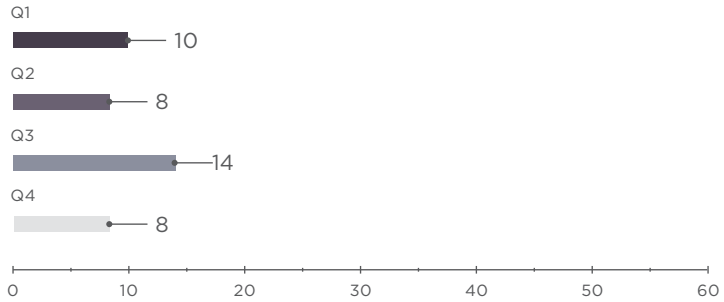


Figure 37. Number of attacks against hospitality and entertainment

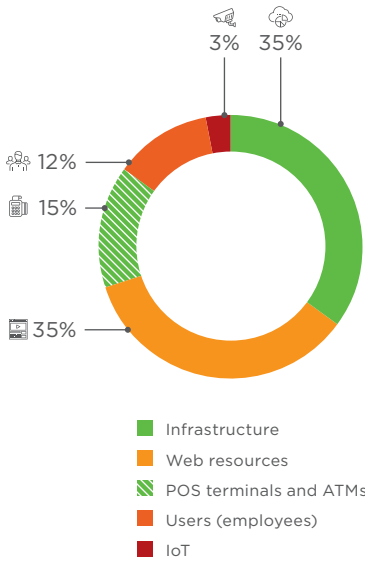


Figure 36. Attack targets

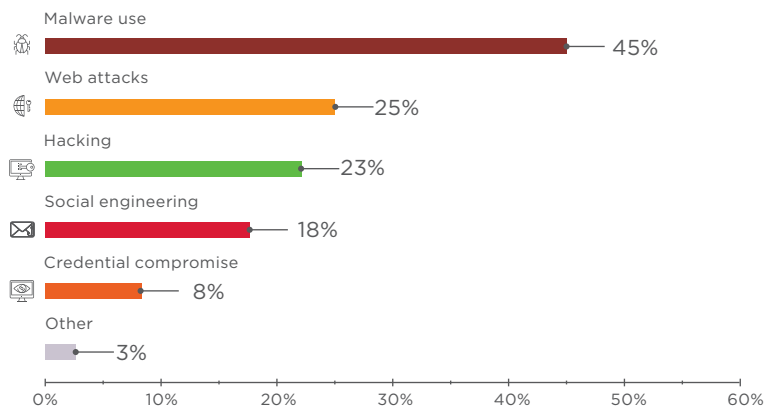


Figure 38. Hospitality and entertainment: attack methods used in 2018

In this sector, attacks were mainly aimed at stealing client data, especially payment card information. Many incidents involved installing malware on POS terminals.

A massive data leak happened in 2018 as a result of a cyberattack on the Marriott hotel chain. Hackers stole personal information for 383 million guests, including passport and payment card information. Marriott stock fell 6 percent in one day and kept falling for another two weeks.



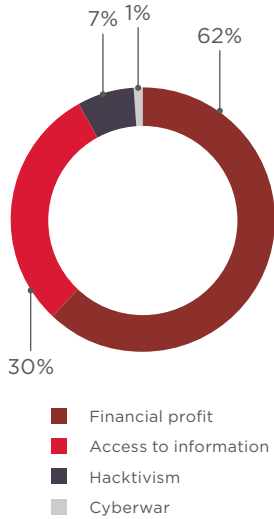


Figure 39. Attack motives

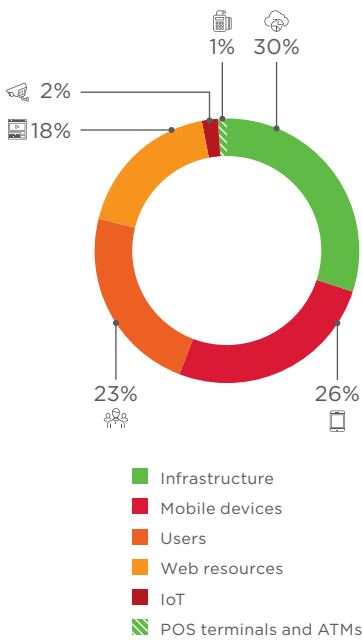


Figure 40. Attack targets

## Individuals

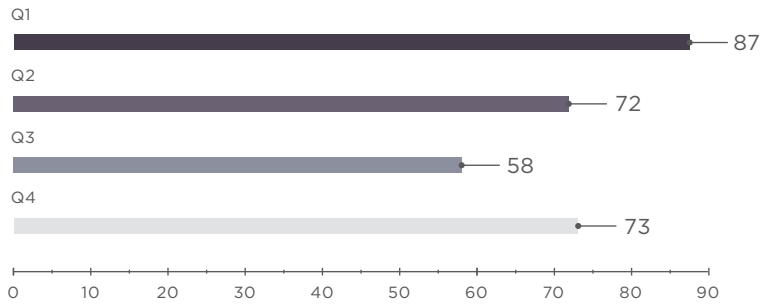


Figure 41. Number of attacks against individuals

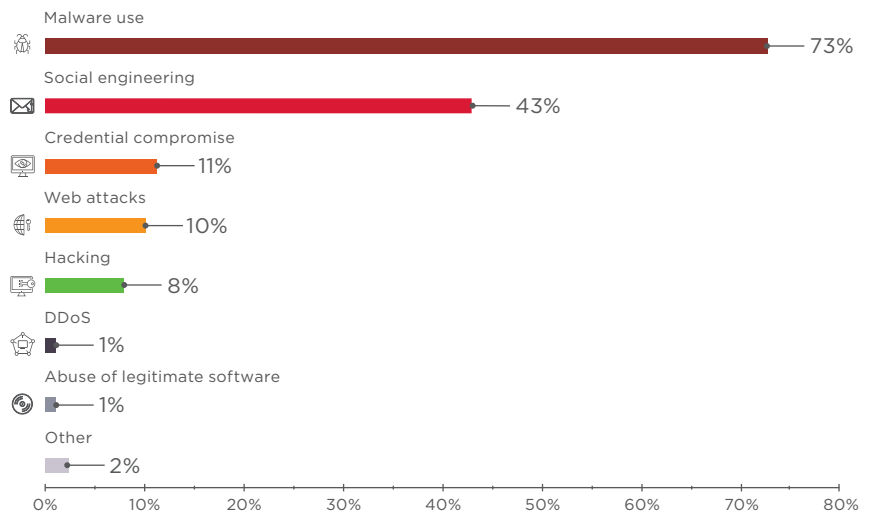


Figure 42. Individuals: attack methods used in 2018

Ordinary users were a favorite target of attackers. Hackers mainly used social engineering (43% of incidents) and malware (73% of incidents). In most cases, computers and mobile phones were infected with spyware (21% of incidents) that collected credentials for access to online banking personal accounts, cryptocurrency wallets, and other services. Malware was mainly distributed via official app stores, websites, and by email.

2017 saw a boom in cryptocurrency which subsided in 2018. As cryptocurrencies fell in price, the number of cyberincidents with miners diminished, and mining is no longer considered profitable by attackers. The share of mining among detected malware attacks against individuals fell from 27 percent in Q1 to 13 percent in Q4.

## Attack methods

Below are the most common attack methods used by criminals in 2018.

### Malware use

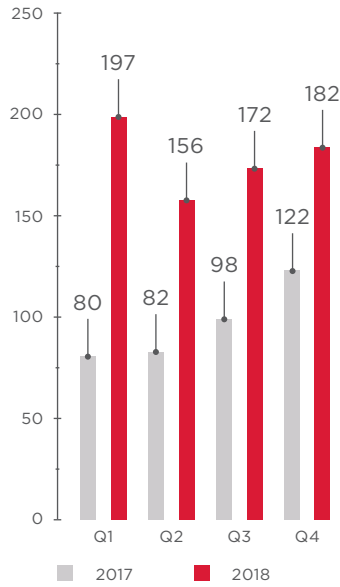



Figure 43. Number of malware-related attacks

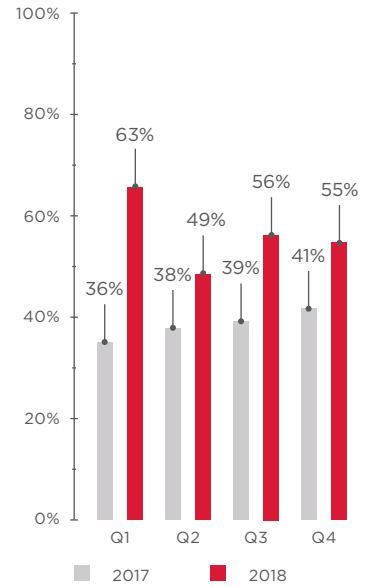


Figure 44. Percentage of malware-related attacks

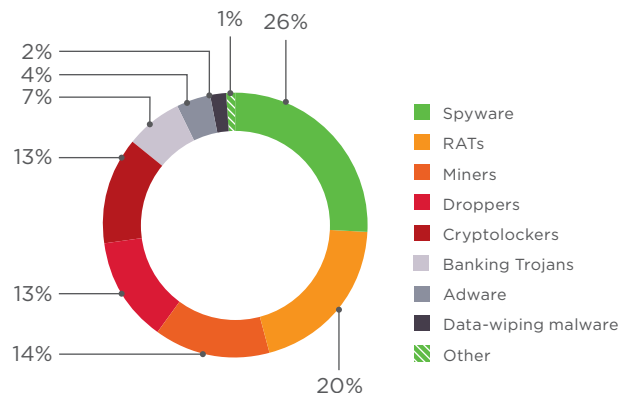


Figure 45. Types of malware

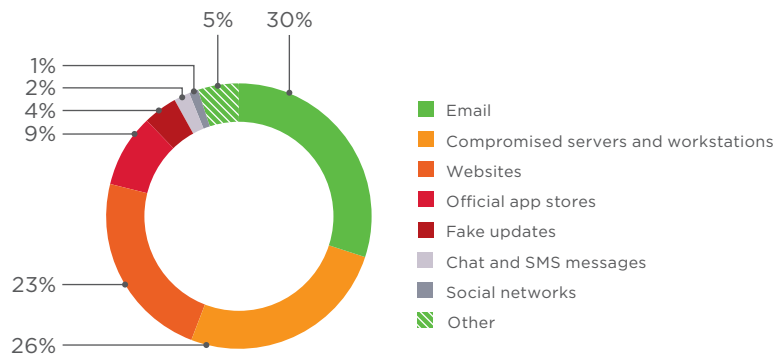


Figure 46. Malware distribution methods

## Social engineering

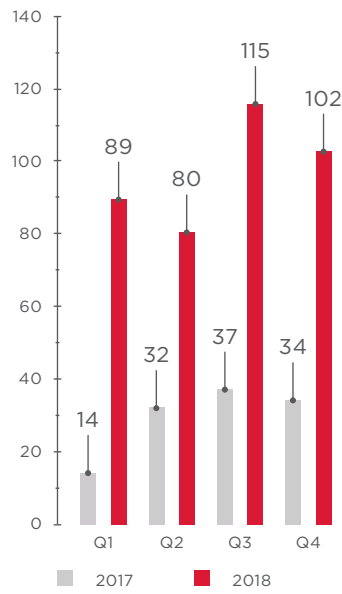


Figure 47. Number of social engineering attacks

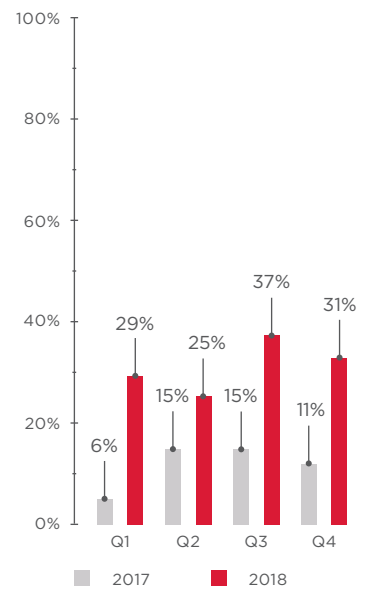


Figure 48. Percentage of social engineering attacks

## Hacking

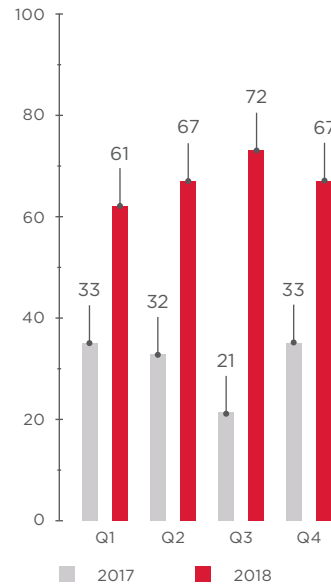


Figure 49. Number of attacks that used software vulnerabilities and security flaws

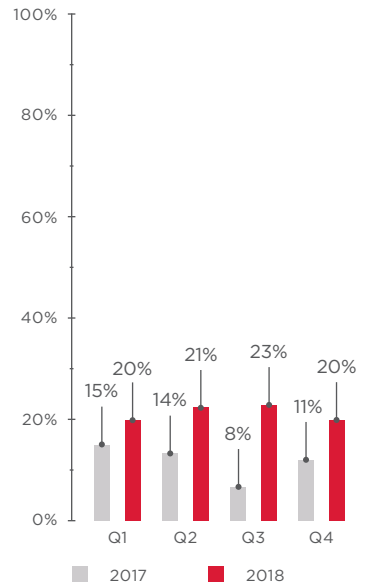


Figure 50. Percentage of attacks that used software vulnerabilities and security flaws

## Web attacks

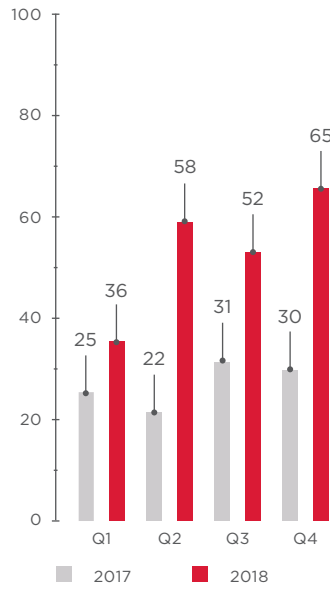



Figure 51. Number of attacks that used web vulnerabilities

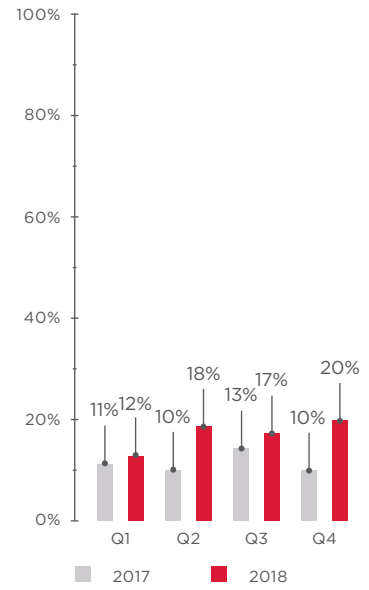


Figure 52. Percentage of attacks that used web vulnerabilities

## Credential compromise

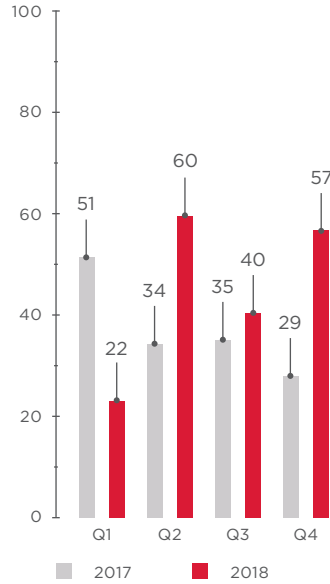



Figure 53. Number of brute-force attacks

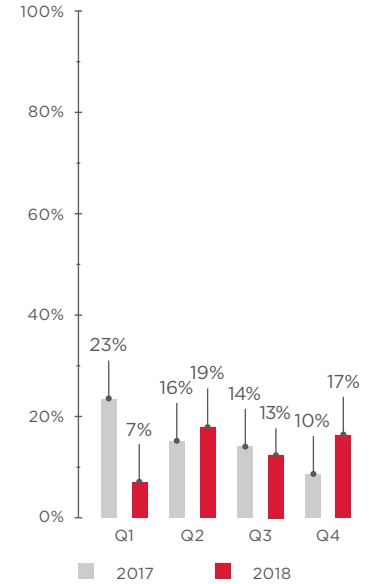


Figure 54. Percentage of brute-force attacks



2018 was marked by the two biggest DDoS attacks in history, reaching 1.35 and 1.7 terabits per second

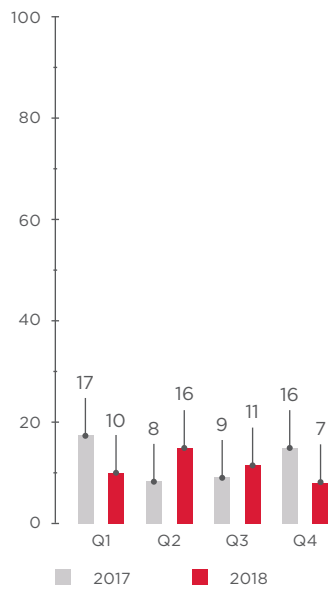


Figure 55. Number of DDoS attacks

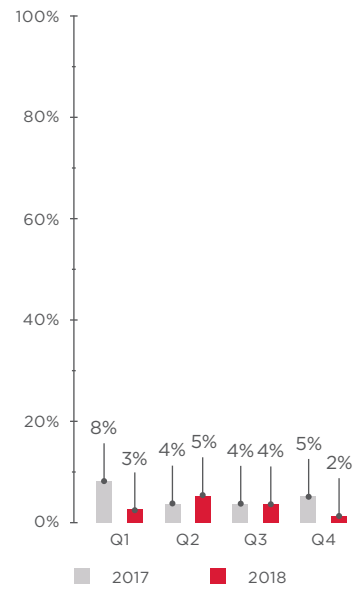


Figure 56. Percentage of DDoS attacks

## Forecasts

Forecasts for 2019:

- We believe data theft attacks will continue to resonate this year. Criminals will keep attacking weakly protected resources in order to steal personal, medical, and payment information. Businesses lacking security protection, such as service companies, educational institutions, healthcare, and retail, are especially at risk. Malware used to collect payment data from websites, POS terminals, and ATMs will continue to evolve.
- Criminals will look for new ways to distribute malware and refine the old ones. Social engineering will likely remain the main method of malware distribution. As people are becoming more aware of various fraudulent techniques, hackers will devise new sophisticated ways to deceive users. Multistage supply chain attacks will also remain popular.
- Ransomware will keep hitting the companies with the most to lose from downtime and data loss. As practice shows, some organizations have no action plans or backups in case of failures of critical systems. Instead, they prefer to pay up to restore normal operations.
- Cryptomining attacks have become much less profitable than in the past. If cryptocurrency prices continue to fall, the number of infections with mining malware will decline further.
- DDoS attacks will become more powerful, due to both growth in botnets and use of new techniques and exploits to amplify attacks. In addition, the marketplace for malware will make it possible even for low-skilled hackers to conduct attacks.
- Pro-government groups will continue to attack industrial enterprises. They will likely be less motivated by espionage than by the desire to disrupt operations, which may lead to injury or worse. In 2018 we already saw attempts to perform such attacks, but

they could well become a reality if companies do not take appropriate measures to improve their security.

- Cybercrimes will be increasingly intertwined with other criminal activities. Computer hacks, including personal data theft, will be incorporated in other types of criminality that are not usually associated with digital security.
- The darknet will continue to evolve. More and more groups will prefer to buy ready-made tools instead of investing in custom development. As a result, the same programs will be used by different cybercrime groups, which will significantly complicate attribution.
- Malware developers will benefit from selling more and more copies of the same utility, so they will likely target broad audiences of buyers. Priority will be given to extensible modular malware with flexible architectures that allow easily adding new functionality. It stands to reason that such versatile malware will be more popular with hackers than niche tools.
- In 2018, several companies were already fined for violating GDPR requirements, but regulators applied such measures only in extreme cases. Going forward, they will likely become stricter against organizations with negligent data handling practices.

---

## About Positive Technologies

[ptsecurity.com](https://ptsecurity.com)  
[info@ptsecurity.com](mailto:info@ptsecurity.com)

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](https://ptsecurity.com).

© 2019 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.