CYBERSECURITY THREATSCAPE 2017

TRENDS AND FORECASTS

POSITIVE TECHNOLOGIES

CONTENTS

TRENDS IN 2017

Each quarter in 2017, we shared data about the latest information security threats and trends, shedding light on new attack techniques and offering guidance for protection. In this report, we will take a look back at last year. Cybercriminals changed their tactics and many threats evolved to be more industry-specific. These and other changes are considered in the conclusion, which outlines what we expect to see in 2018.

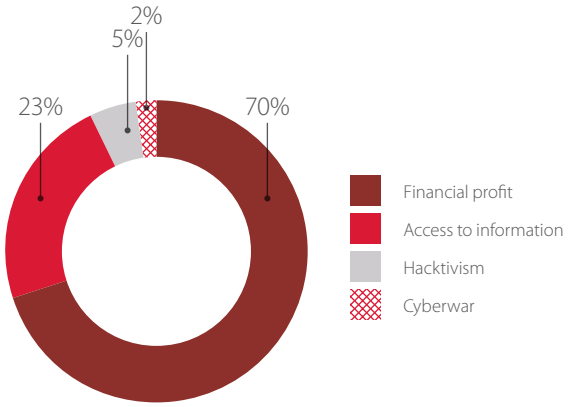
Key findings:

+ Trojan encryptionware was the biggest trend of 2017. Ransom was not the only goal of such malware—some Trojans encrypted victims' hard drives and threw away the key, causing enormous damage to corporate infrastructures.
+ The Ransomware as a Service model caught on, due to which the same Trojans were reused by different groups. The barrier to entry for cybercriminals fell dramatically: now anyone can buy malware, with no technical skills required.
+ As the number of malicious campaigns grows, so does the number of victimized individuals. This trend, too, is likely related to the popularity of Ransomware as a Service: novice cybercriminals in search of quick profit buy Trojans and use them against individual users.
+ Meanwhile, malware targeting industrial companies is no mere sideshow. This malware is uniquely well adapted to industrial infrastructure, which makes these threats extremely difficult to detect.
+ Malware aimed at POS terminals and ATMs is also on the rise. Despite the difficulty of placing malware on bank equipment, it was used in every eighth attack against banks.
+ In the world of data theft, healthcare and payment cards were the most popular. Personal data is still a major interest for criminals, although it fetches a lower price on the darknet than before.
+ The cryptocurrency boom and plethora of initial coin offerings (ICOs) attracted the attention of criminals, who attacked cryptocurrency exchanges, wallets, and ICOs.
+ Overall, attacks are tending to involve more stages and participants. This can be confirmed by the popularity of supply-chain attacks and drive-by attacks.
+ Botnets continued to spread thanks to new IoT devices. As a result, the strength of DDoS attacks has increased. Attackers continued to invent new Trojans and modify old ones to exploit numerous vulnerabilities in smart devices.
+ Major political events have inspired hackers to perform illegal acts. Attacks have become a political instrument and effective tool for shaping public opinion.

OVERVIEW OF ATTACKS

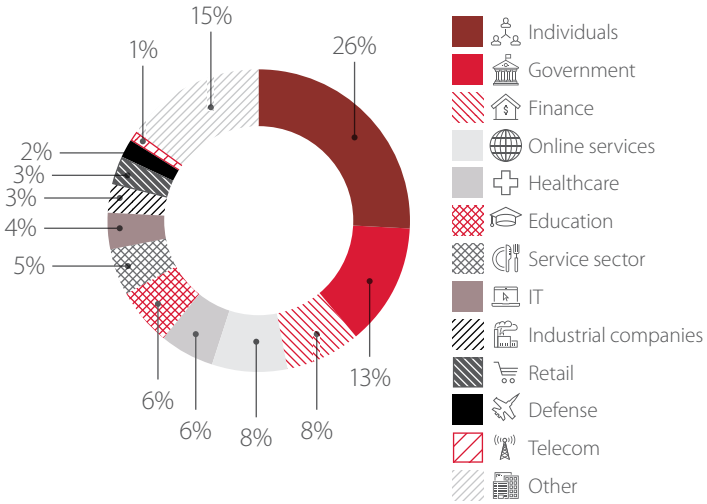
The majority of attacks (70%) were performed for direct financial gain, such as draining the victim's bank account. One quarter (23%) were intended to steal data.

Mass and targeted attacks were roughly balanced during the first six months of 2017. But by the end of the year, mass attacks took a significant lead (57%).



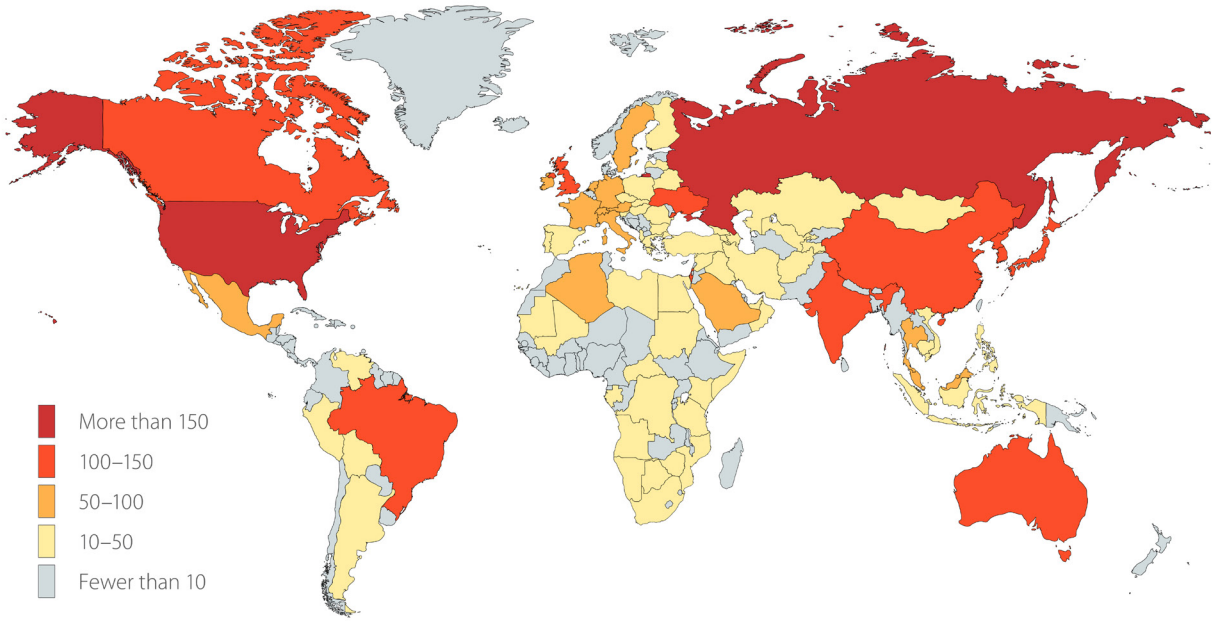
Attackers' motives

Individuals are the most common targets for attackers: a quarter of attacks were aimed at them (26%). Other major targets included governments (13%), banks and online services (8% each). Mass attacks affecting hundreds or thousands of companies in diverse industries have been categorized for statistical purposes as targeting "Other," which is why such a large number of incidents fall under this category (15%).



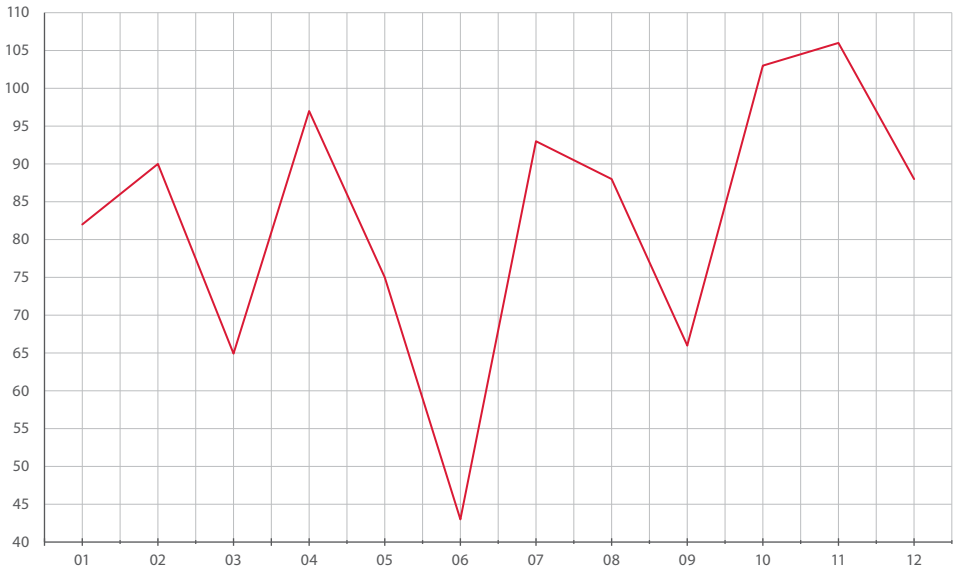
Categories of victims attacked in 2017

Cybercriminals know no borders: more and more attacks are affecting two, three, ten, or even more countries simultaneously. However, U.S. and Russia were absolute leaders in terms of the number of cyberincidents during 2017. This might be partly caused by the fact that the media paid close attention to these countries. In fact, dozens of countries all over the world experienced attacks, particularly the United Kingdom, Australia, Canada, India, Japan, Ukraine, Israel, and China.



Geographical spread of cyberattacks in 2017

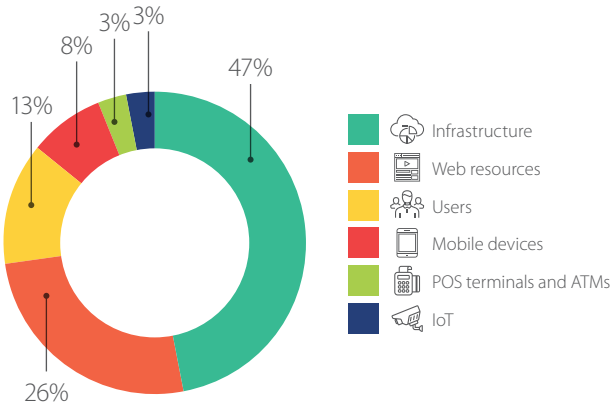
In 2017, we detected 13 percent more unique incidents than in 2016. As in the previous year, the fourth quarter of 2017 was the busiest one for attackers. The smallest number of attacks occurred in the second quarter. During the last two years, we have seen a consistent decline in hacker activity in May–June followed by an upsurge towards year's end.



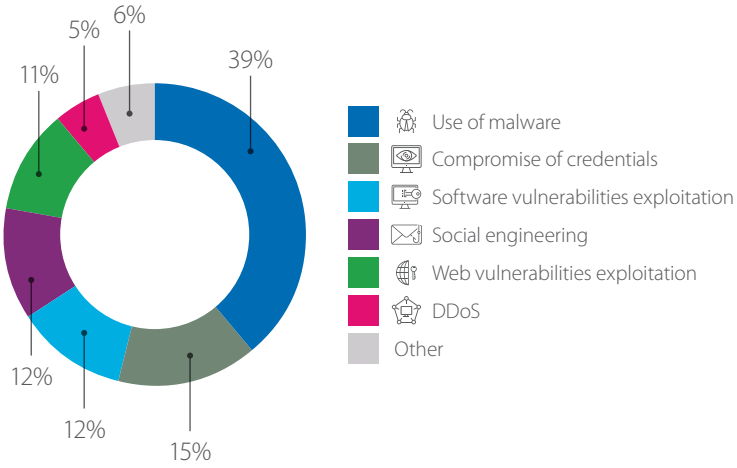
Numbers of monthly cyberattacks in 2017 (1 = January, 12 = December)

Attacks were generally aimed at company infrastructure and web resources (47% and 26%, respectively). There was also an increase in attacks against ATMs and POS terminals, which occurred seven times more often in 2017 than they did in 2016.

Only unique incidents were counted in our statistics. An incident includes all infections involving a particular Trojan and its variations. The most common attack method (39%) was use of malware. Detailed statistics on different attack methods are presented later in this report.



Attack targets



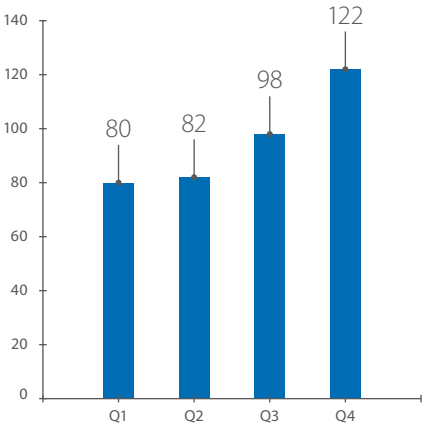
Attack methods

		Industry											
		Finance	Government	Healthcare	Education	Industrial companies	Online services	Service sector	Individuals	Retail	IT	Telecom	Other
Target	Infrastructure	32	73	34	33	23	15	22	89	6	20	3	112
	Web resources	25	45	6	10	1	54	16	47	14	12	2	23
	Users	8	8	21	15	5	5	4	46	1	2	1	13
	POS terminals and ATMs	12						7	1	6	1		2
	Mobile devices		3					3	70		1	1	3
	IoT		5				1	1	5		2	2	13
Methods	Use of malware	40	39	16	16	12	4	17	136	8	15	1	78
	Compromise of credentials	2	20	13	14	4	16	14	35	4	4	1	21
	DDoS	7	19	1			10	2		2	4	1	4
	Social engineering	12	9	12	9	8	2	2	38	2	2	1	21
	Exploitation of software vulnerabilities	8	20	8	9	2	13	3	20	3	5	2	26
	Exploitation of web vulnerabilities	9	19	7	8	1	27	9	12	5	3	1	7
	Other	2	8	4	2	2	3	6	14	3	5	2	9
Motives	Financial profit	74	59	42	47	16	64	37	202	20	32	7	93
	Access to information	6	45	17	10	7	7	11	49	7	6	2	59
	Hacktivism		23	2	1	2	4	5	2				9
	Cyberwar		7			4			2				5

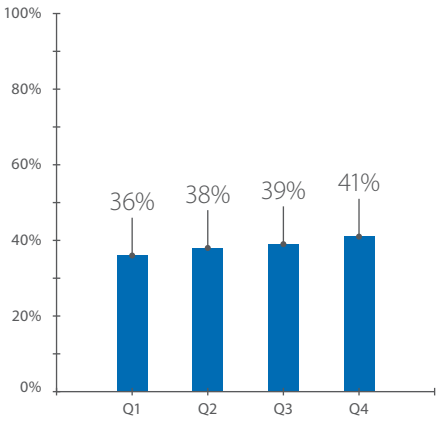
Classification of cyberincidents by motive, method, and target

USE OF MALWARE

Damage from malware attacks in 2017:
over $500 million



Number of malware-related attacks



Percentage of malware-related attacks

During the first six months of 2017, ransomware Trojans were particularly "popular." Along with the WannaCry and NotPetya epidemics, other ransomware campaigns such as Jaff and SOREBRECT struck networks.

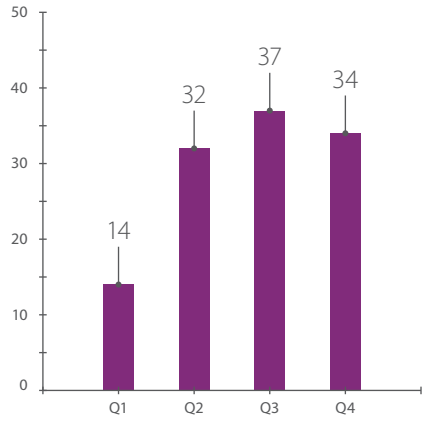
During the year, we saw a rise in the popularity of Ransomware as a Service. In this business model, malware creators do not organize attacks themselves. Instead, they sell Trojans to criminal groups, often for mass attacks. With this division of labor, malware developers receive payment for a Trojan and start developing the next one. Meanwhile, other criminals are already busy implementing attacks with the first Trojan. This has reduced the barrier to entry for cybercrime, since malware is available to anyone willing to pay.

Toward the end of the year, we noted the increasing use of malware to destroy evidence and hide the true motives of attackers. By destroying data permanently, this malware makes it difficult for investigators to reconstruct the chain of events and pinpoint how the attackers gained access to a system.

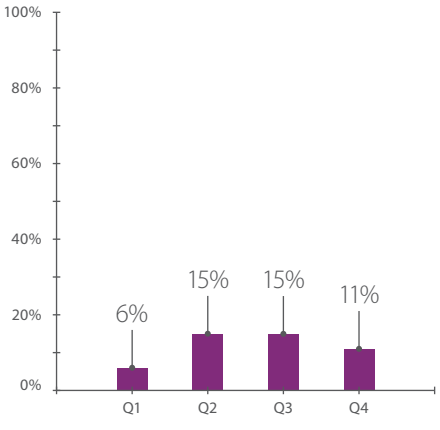
In the second half of 2017, as bitcoins soared in price, cryptocurrency mining became an attractive option for attackers. The CPU capacity of unsuspecting users could be used to mine cryptocurrency for attackers' benefit. A wave of mining attacks hit computers, servers, and mobile devices.

SOCIAL ENGINEERING

Damage from social engineering attacks in 2017:
over $250 million



Number of social engineering attacks



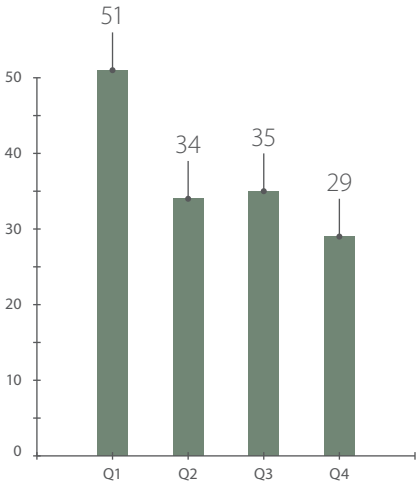
Percentage of social engineering attacks

In 2017, malefactors continued to refine their social engineering techniques. Phishing sites and emails were the most common avenues for targeted attacks against companies. To make phishing emails look more believable, attackers forged sender addresses, registered domains resembling trusted ones, and even hacked partner companies in order to masquerade as them in correspondence with the target while bypassing spam filters.

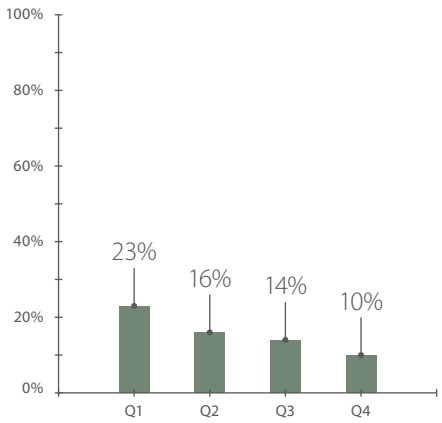
Many attacks were aimed at common users. The objective of these attacks was credit card numbers, online banking credentials, and credentials for email and other online services. Criminals forged websites, sent malware via email, used SMS messages containing a link to a phishing site, or simply called victims under false pretenses to obtain this information over the phone.

COMPROMISE OF CREDENTIALS

Damage resulting from compromised credentials in 2017: **over $100 million**



Number of attacks performed by compromising credentials



Percentage of attacks performed by compromising credentials

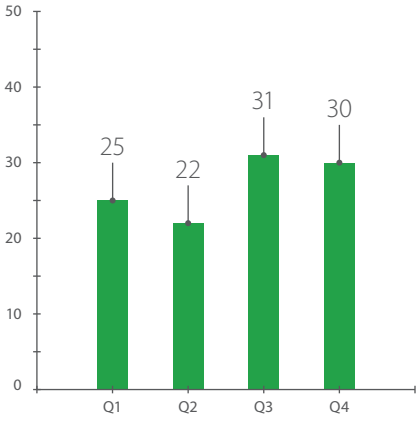
As 2017 showed, a weak password policy makes it easy work for attackers to guess passwords. Just one successfully guessed (bruteforced) password is enough to penetrate corporate systems. Worse still, passwords are often stored without encryption. In this case, if attackers hack a database, they can obtain all passwords in plaintext right away, without having to spend time reversing hash functions.

As cryptocurrency mania caught on, investors were busy setting up wallets and transferring money to them—as hackers bruteforced credentials and stole the proceeds.

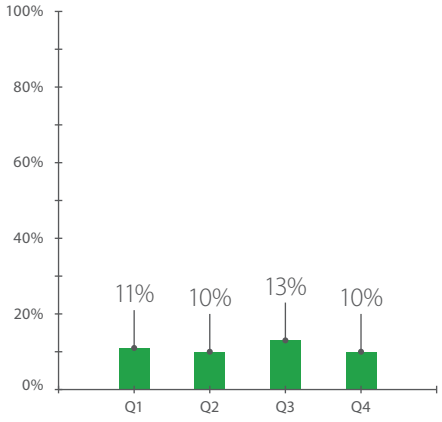
Compromise of IoT credentials led to millions of routers, IP cameras, vacuum cleaners, and other devices joining botnets for mining cryptocurrency, tracking user location, performing DDoS attacks, and other malicious activity.

EXPLOITATION OF WEB VULNERABILITIES

Damage caused by exploitation of web vulnerabilities in 2017: **over $390 million**



Number of attacks that used web vulnerabilities



Percentage of attacks that used web vulnerabilities

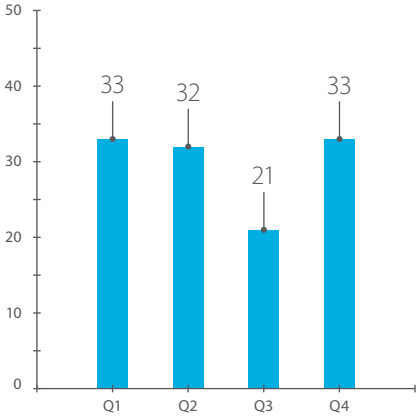
ICOs were among the most popular targets in 2017. Insufficient protection of web resources cost millions of dollars for ICO organizers. For example, in an attack against CoinDash, criminals made off with $9 million in investments.

Government websites became a favorite target for hacktivists. Ministries, departments, and state-owned companies are seen as the face of the government by the media, both domestically and internationally. This is why hacktivists often choose government websites for defacement and publish their own materials on them.

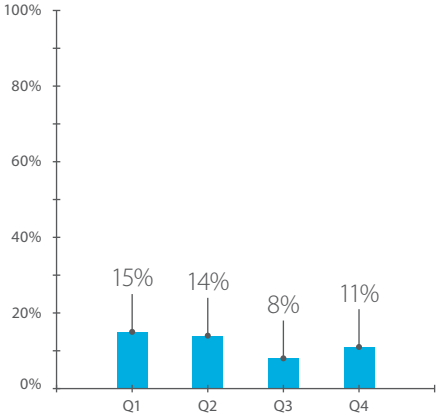
Attackers now use vulnerable websites for hosting malicious software and performing drive-by attacks. With search engine optimization (SEO) techniques, these same attackers raise the position of these sites in search results, attracting more visitors. Their techniques include adding specific keywords to hidden pages and using a SEO botnet to pump up traffic. The SEO-ified website is used to host malware as a go-between in attacks, making the site's owner an unwitting accomplice to cybercrime. This could ruin the reputation of such sites and their owners, lead to blocking of the sites, and result in seizure of server equipment by law enforcement as part of a criminal investigation. The moral is: any website may be attacked by cybercriminals, even if it is not their actual target.

EXPLOITATION OF SOFTWARE VULNERABILITIES

Damage from attacks involving software vulnerabilities in 2017: **over $280 million**



Number of attacks that used software vulnerabilities



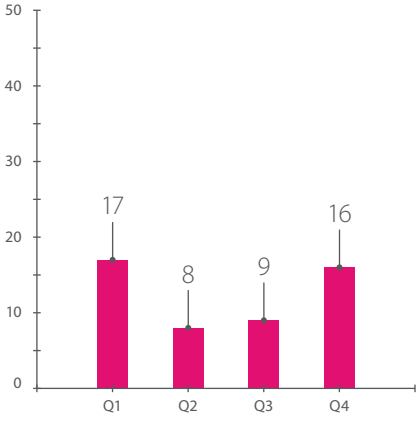
Percentage of attacks that used software

During penetration testing, Positive Technologies specialists regularly discover systems that are lacking necessary security updates or running out-of-date software versions. This means that an attacker can use known vulnerabilities in obsolete versions of software to perform an attack. Another option is to buy a ready-made exploit on the darknet, which will save time and get the job done, whether it be accessing a server database or something else.

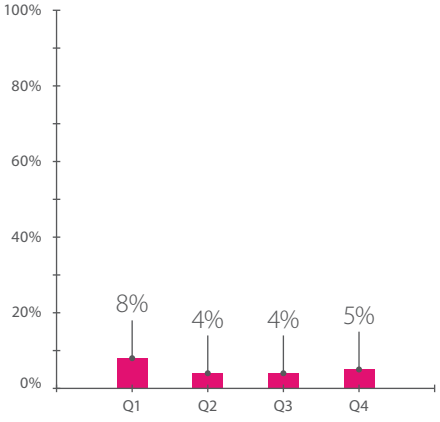
In the case of advanced persistent threats (APTs), attackers often use zero-day vulnerabilities so that their actions remain unnoticed for a long time. For example, a zero-day vulnerability in Apache Struts, CVE-2017-5638, brought cybercriminals around $100,000. This vulnerability allows executing arbitrary commands on a web server, so attackers installed backdoors, bots for DDoS attacks, ransomware, and software for cryptocurrency mining.

DDOS ATTACKS

Damage caused by DDoS attacks: no estimate provided



Number of DDoS attacks



Percentage of DDoS attacks

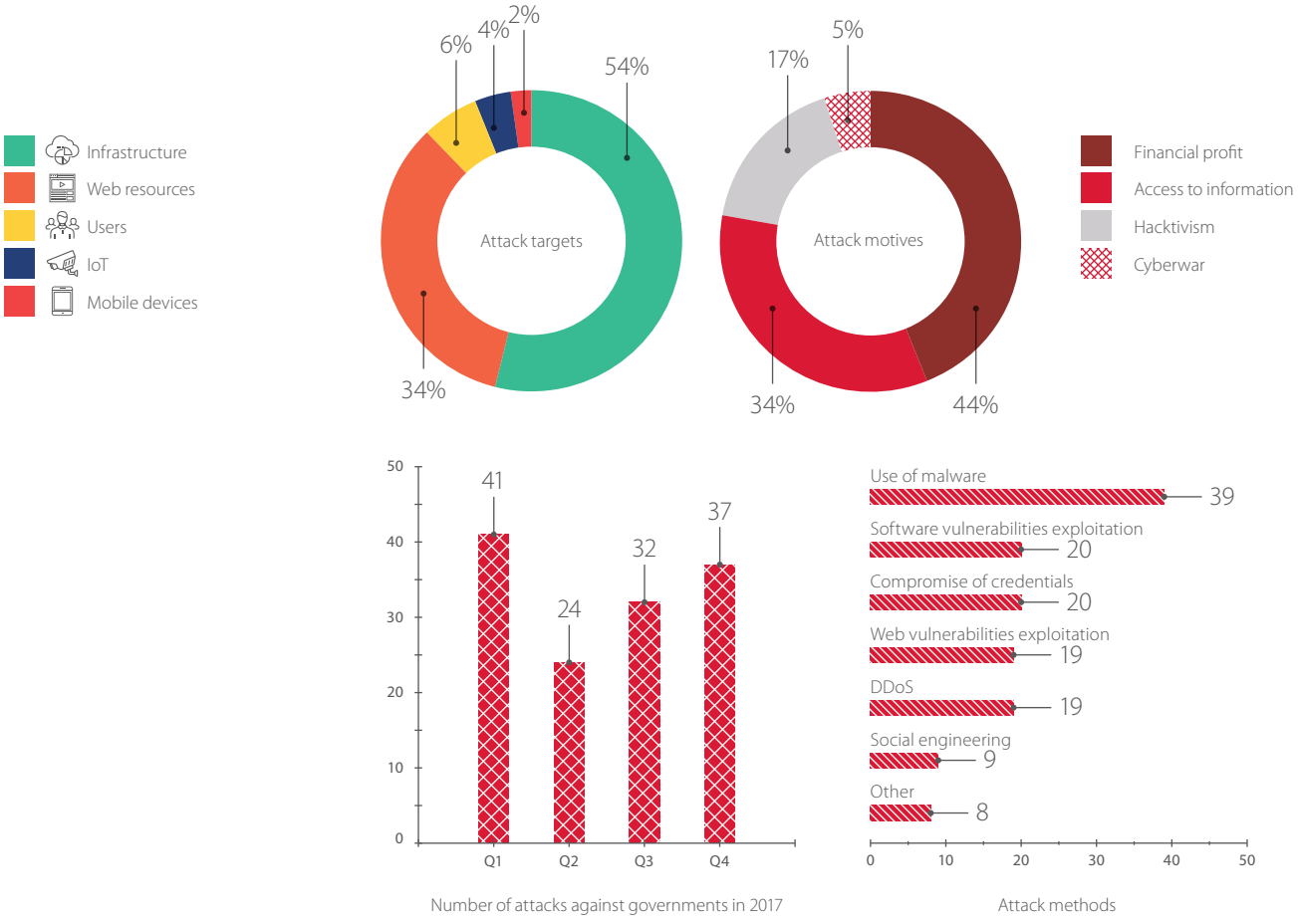
Temporary lack of access to a website may seem minor at first. But in fact, DDoS attacks can cause companies to lose large amounts of money, not to mention client loyalty. When clients are unable to move money or pay via online banking for hours at a time, they begin to doubt the reliability of the bank and sometimes incur financial losses of their own, due to the inability to pay bills, for example.

Main victims of DDoS attacks in 2017 were governments (usually because of hacktivists), online services (for example, cryptocurrency markets and ICO platforms), and financial organizations. Note that we counted only unique DDoS campaigns. When multiple companies became victims of a single botnet attack, this mass attack was considered as one incident.

ATTACKS BY INDUSTRY

This section analyzes the threats encountered by each of the most-attacked industries in 2017.

Government



Number of attacks against governments in 2017

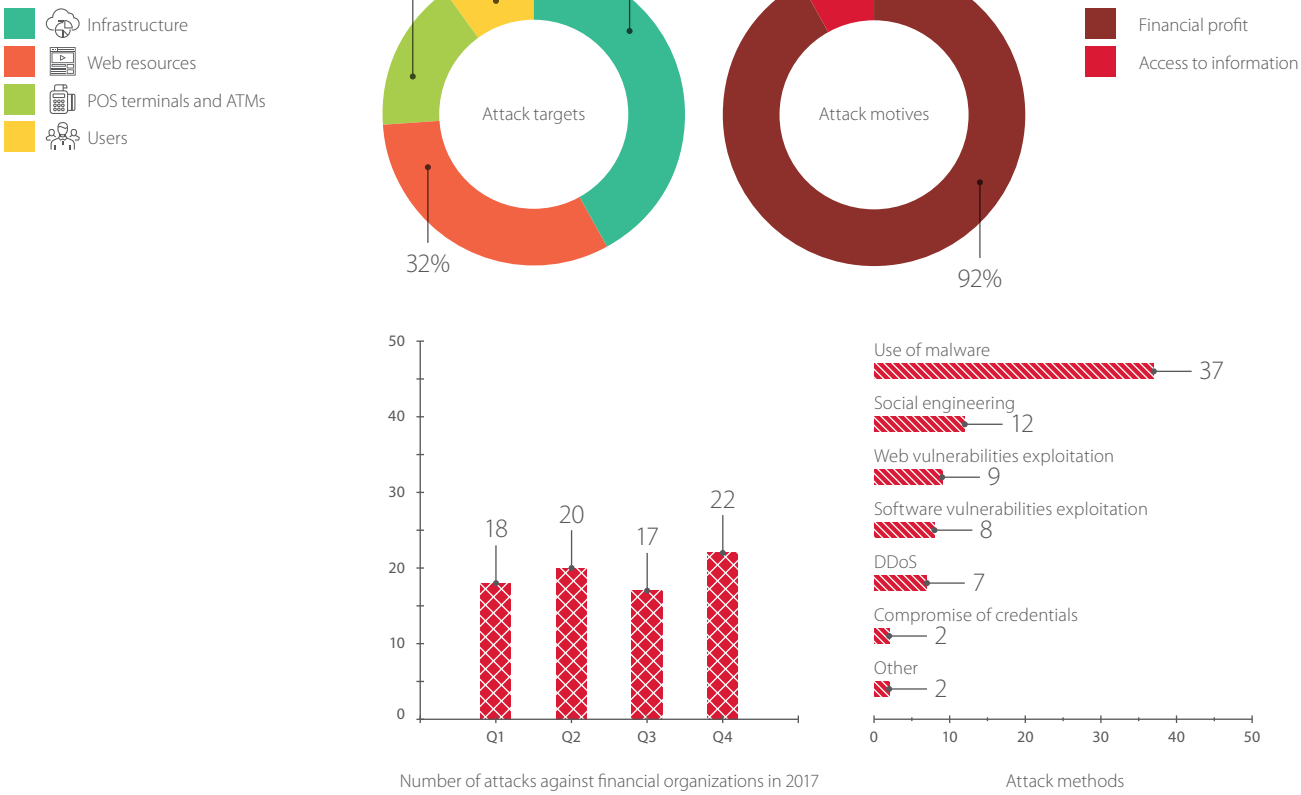
Attack methods

Governments were on the receiving end of 13 percent of all attacks. Attacks against governments are often attributed to hacker groups (such as OilRig, Turla, and Lazarus). Because attribution is difficult and multiple names may refer to the same group of hackers, different security researchers sometimes may refer to a single group by multiple names. As a result, it is difficult to estimate the total number of active hacker groups. Our estimates indicate that at least 70 such groups were operating in 2017.

Several attacks with malware targeted the cell phones of government employees. Since they often checked work email accounts on their phones, the attackers obtained access to confidential information.

About one third (34%) of attacks on government were aimed at data theft. In these cases, attackers try to obtain access to internal resources of the victim's organization. Once the attackers have server access, they can do anything they want: the cautious may bide their time for a future attack, while the bold might disable server equipment and destroy databases.

Finance



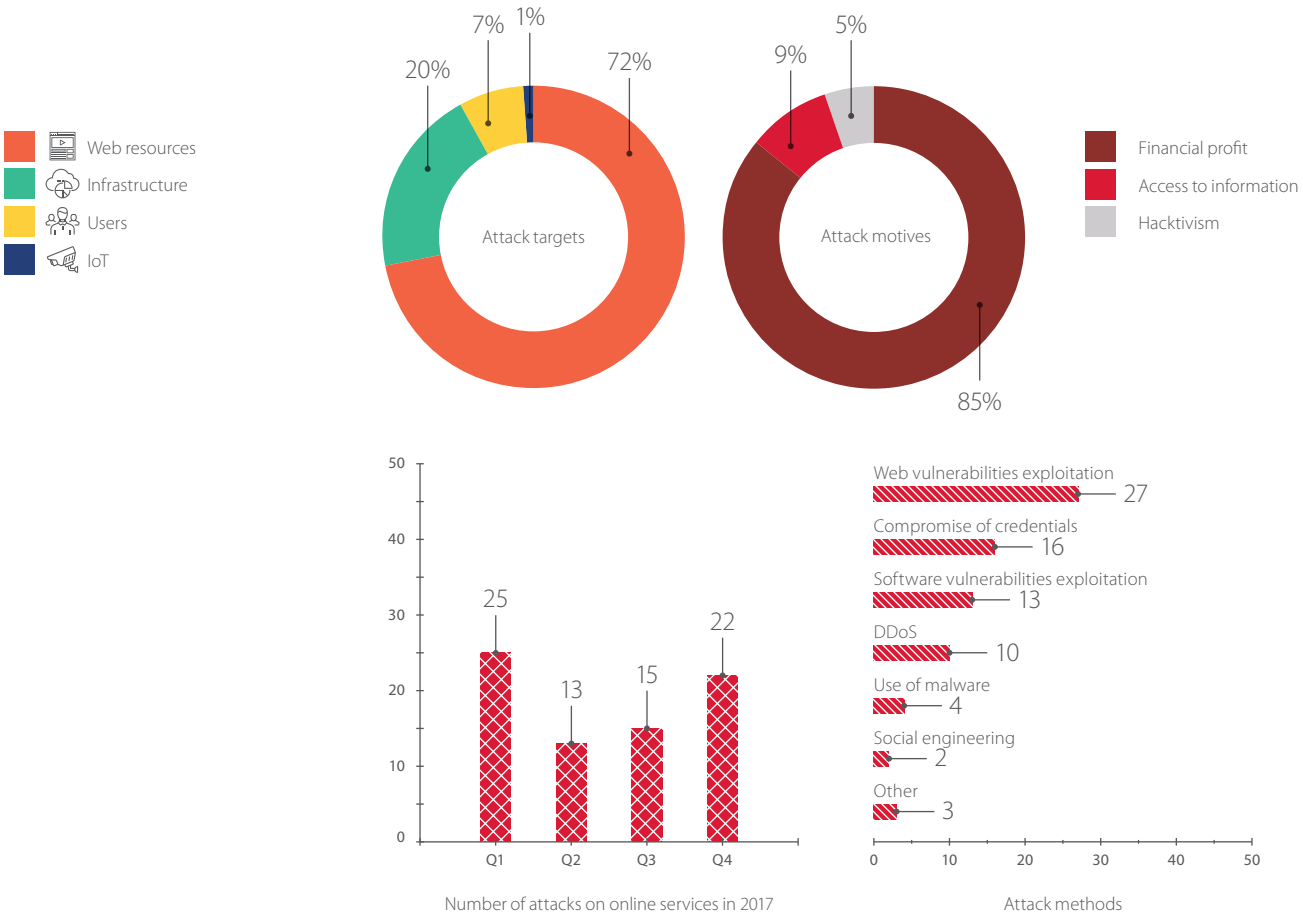
Number of attacks against financial organizations in 2017

Attack methods

Attackers are attracted to the financial industry. Around half of attacks on banks in 2017 involved malware. Many of the targets were POS terminals and ATMs. Compared to 2016, there was a significant increase in this category of attacks. Attackers used malicious software either to take over ATMs for "jackpotting," or to compromise a bank's internal systems.

One case in point is the Cobalt group, which we have been monitoring for the second year in a row. These hackers usually target a bank's local area network. Their modus operandi is to send phishing emails to bank employees. To bypass spam filters and make messages more convincing to recipients, the Cobalt group has registered domains resembling trusted ones (for example, visa-pay.com, swift-alliance.com, cards-cbr.ru, and billing-cbr.ru) and compromised legitimate business partners (such as hardware vendors or insurance companies) in order to send malware-laden messages masked as coming from trusted partner companies. Having penetrated the LAN of one certain bank, the attackers investigated the network to find the computers of employees responsible for ATMs. Via these computers, the attackers installed malicious software on the ATMs and obtained remote control over them. Then, at a fixed time (generally at night), so-called money mules went to the ATMs to withdraw money.

Online services



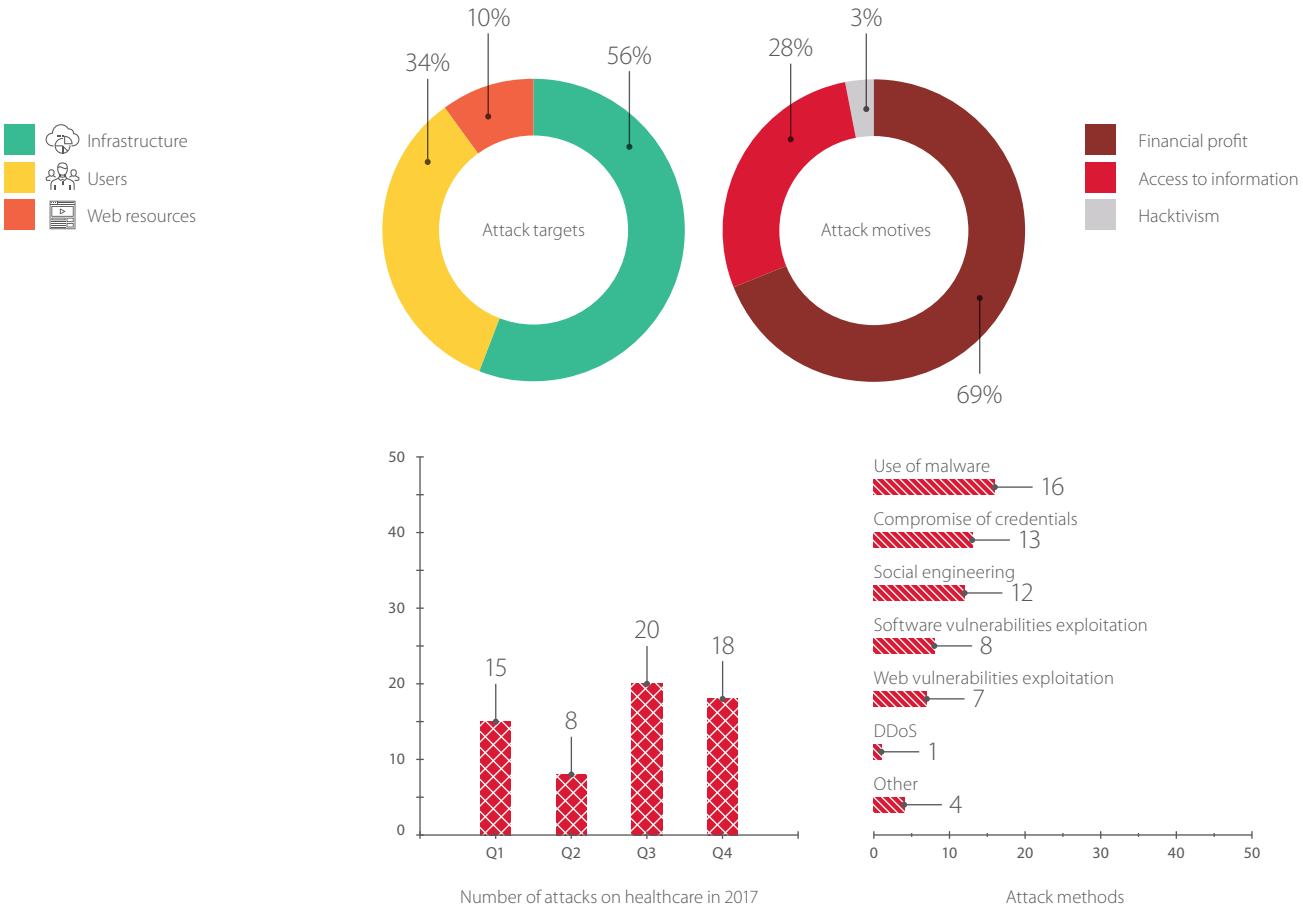
Number of attacks on online services in 2017

Attack methods

Investment inflows to ICOs exceeded $5 billion in 2017. The most profitable ventures raised $883.4 million (EOS), $257 million (Filecoin), and $232 million (Tezos). But ICOs brought in more than just big money. Hackers, too, discovered ways to profit to the tune of around $300 million in 2017, which is equivalent to around 7 percent of all ICO proceeds during that period.

The most common method was not overly complicated: attackers altered the address of the organizer's wallet given on an ICO website so that unsuspecting investors, after reading the altered website, would send their funds to the attacker's wallet instead. To hack ICO websites, attackers used vulnerabilities in web applications or targeted the organizers (for example, by accessing organizers' email accounts and then resetting passwords for the ICO domain or web host). Other techniques included phishing against investors (creating fake sites or sending messages about a supposed change in contact information and wallet of the organizer) and finding errors in smart contract code.

Healthcare

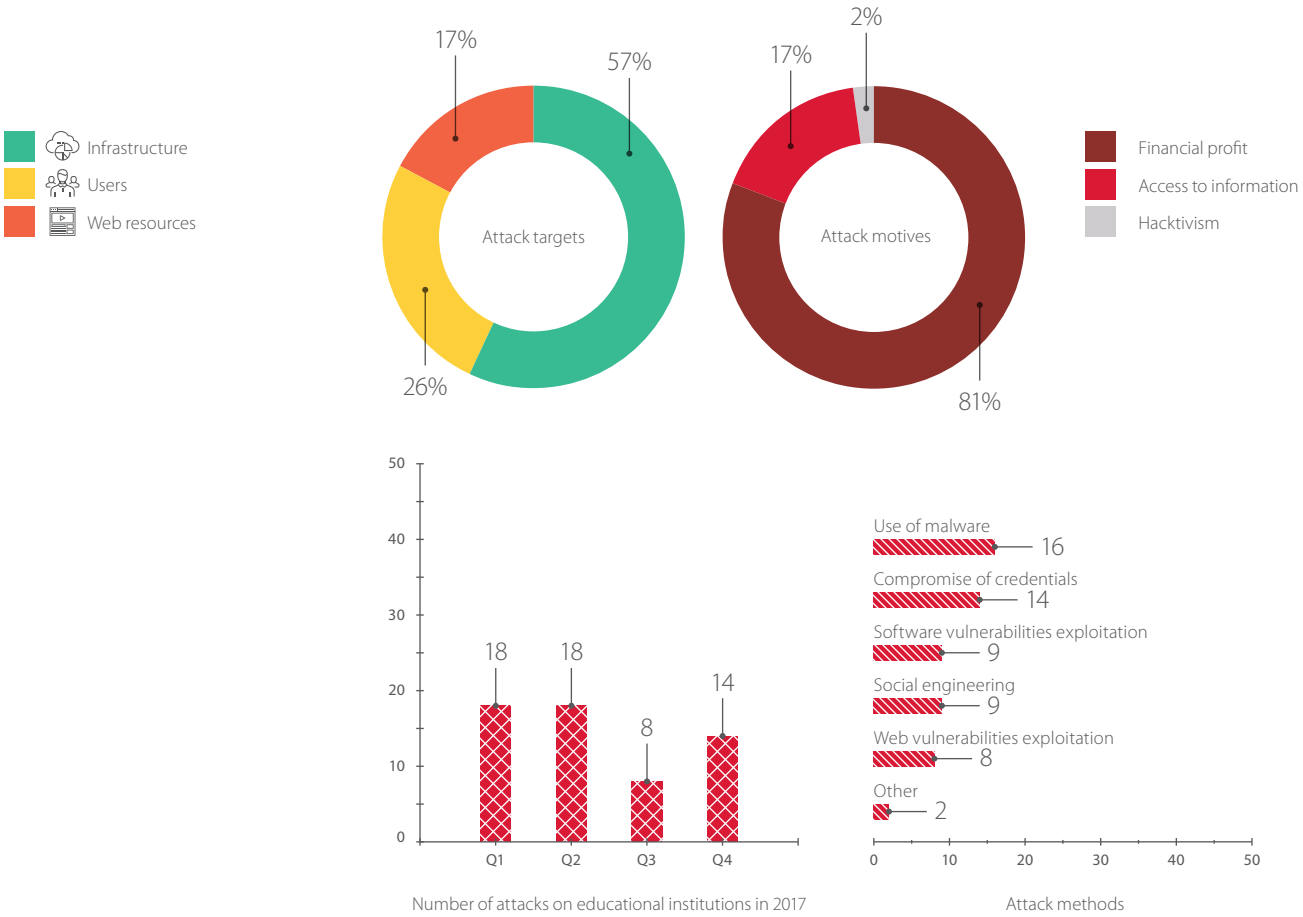


Number of attacks on healthcare in 2017

Attack methods

Medical records for more than two million people were stolen in 2017 as a result of attacks on healthcare institutions. This data is in demand on the black market, with a price that is 10–15 times higher than for passport data. In half of cases (56%), attackers penetrated an organization's internal network (for example, by sending phishing emails to employees or bruteforcing passwords) and accessed servers and databases.

Education



Number of attacks on educational institutions in 2017

Attack methods

Educational institutions are often targeted by their own students. This applies equally to universities (where serious programming skills can be expected) and to ordinary grade schools.

Students find malicious software on the Internet and use it to hack school computers to change their grades.

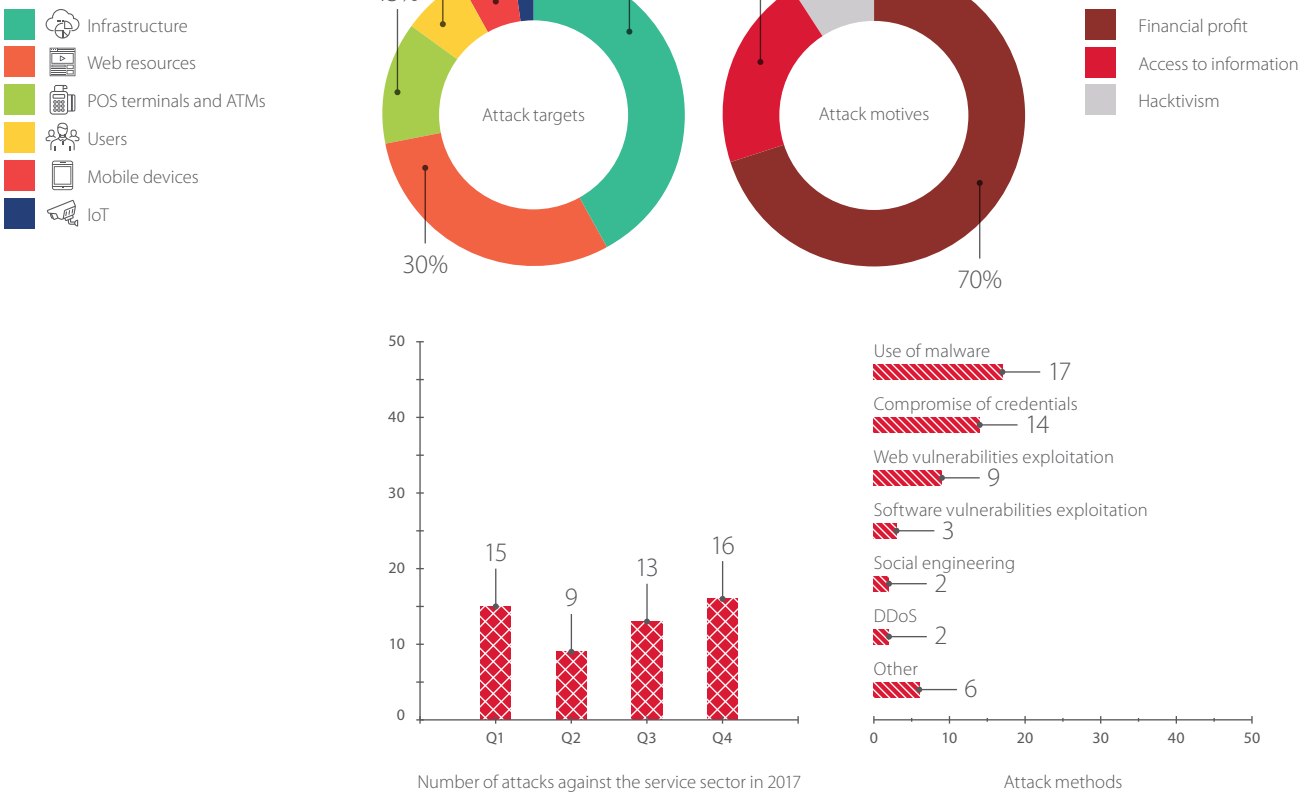
These students usually do not think about the consequences of their actions and are quickly caught by law enforcement.

However, not only students threaten educational institutions.

Another popular motive for attacks on educational institutions is obtaining personal data about students and their parents, which usually includes their residence address as well as parents' email addresses and places of work. This data can be used in targeted attacks on the company at which the parents work.

Cybercriminals usually profited by either demanding a ransom (for example, for decrypting data) or by selling their hacking services (for example, for changing student grades).

Service sector



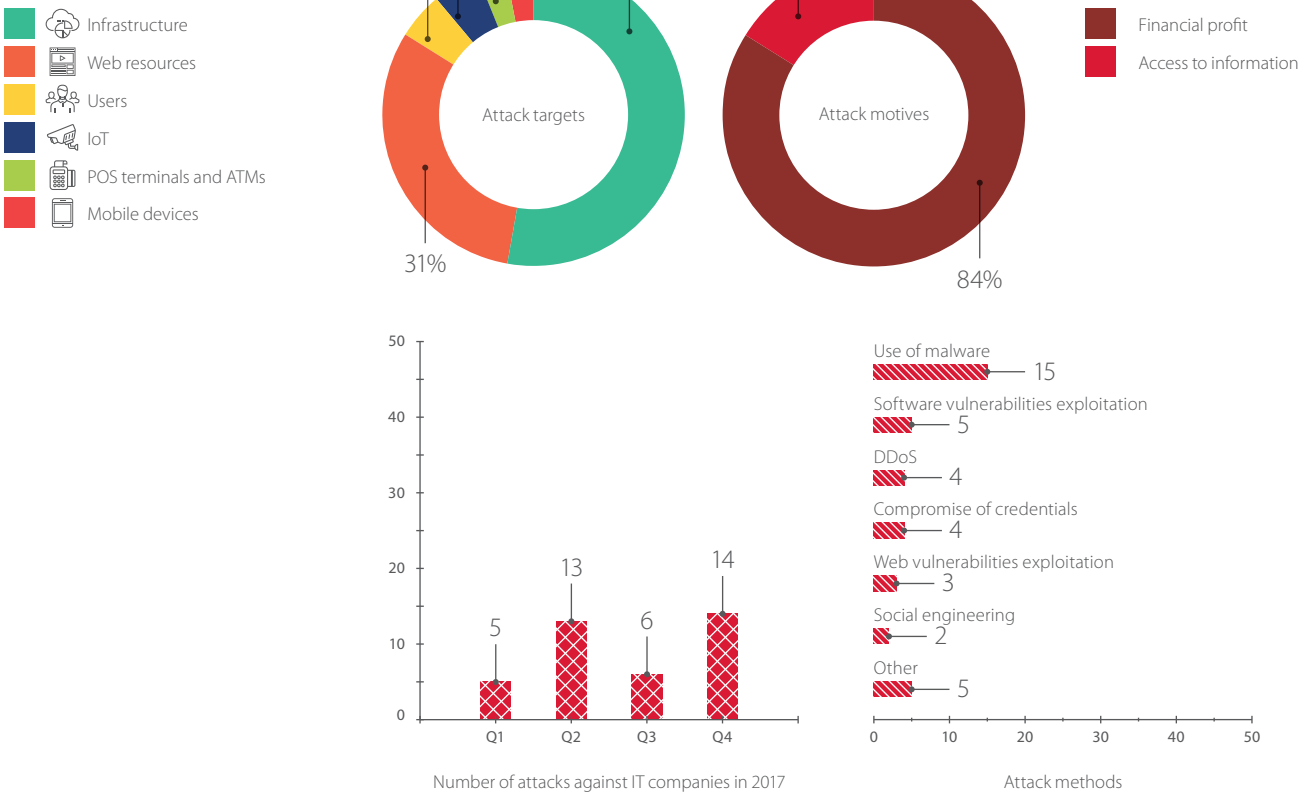
Number of attacks against the service sector in 2017

Attack methods

In a large number of incidents against the service sector, malware was installed on POS terminals to steal payment card information. Customers of fast food restaurants and hotels were targeted most often.

When attackers steal money or obtain personal data, this is bad for customers, of course. But this also incurs long-term reputational risks for the hacked company.

IT



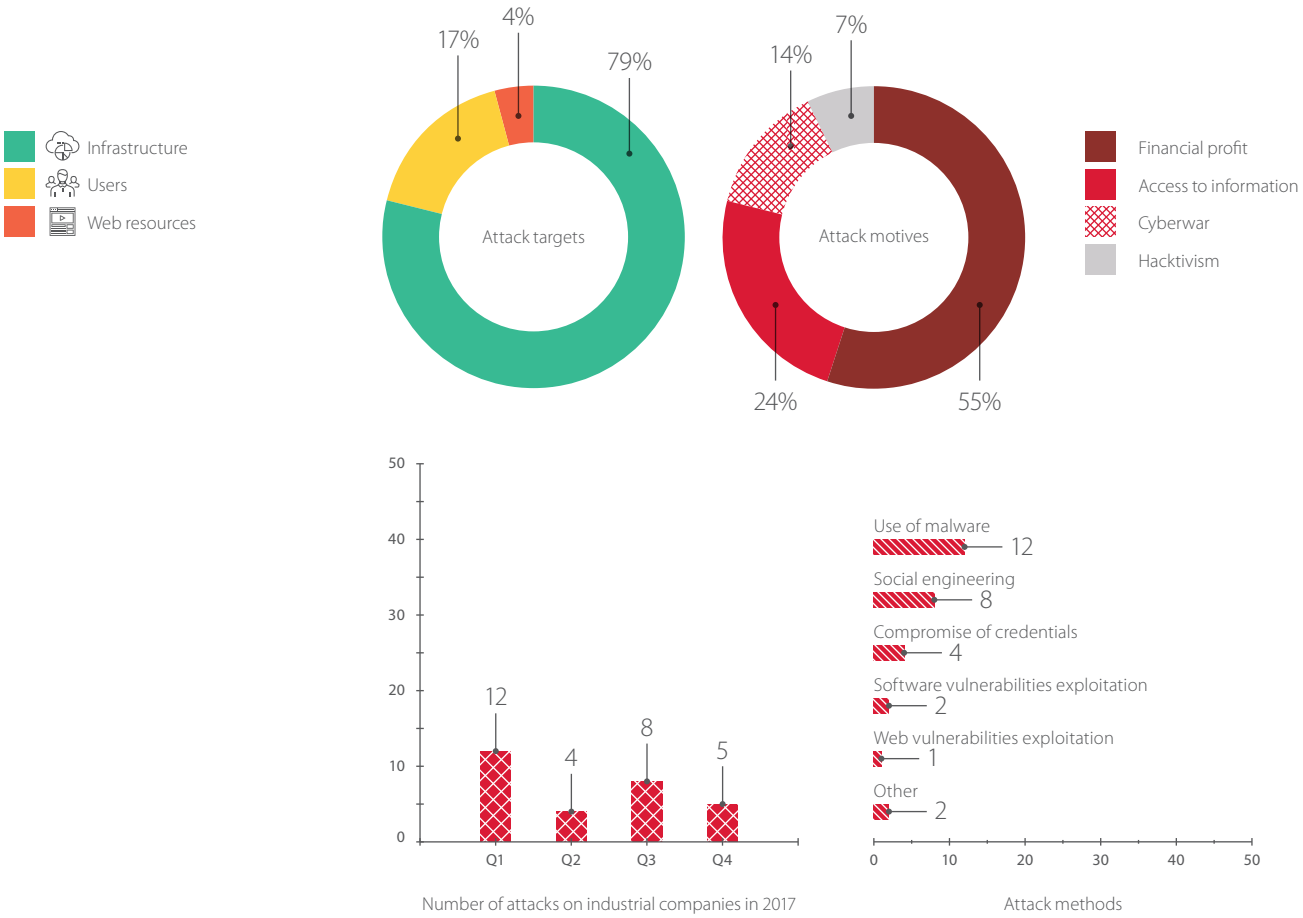
Number of attacks against IT companies in 2017

Attack methods

Attacks on IT companies were consistent with those observed in other industries. Cybercriminals brazenly targeted information security companies multiple times in 2017. They abused visitor trust in these companies' websites to spread malicious software. Any company, regardless of industry, may be used by attackers as part of a targeted attack. This method, called a supply-chain attack, involves first compromising one company to then attack the actual target (for example, a partner of the first company).

This method is often used to send phishing emails, because they appear to come from a trusted partner and therefore evade spam filters.

Industrial companies



Number of attacks on industrial companies in 2017

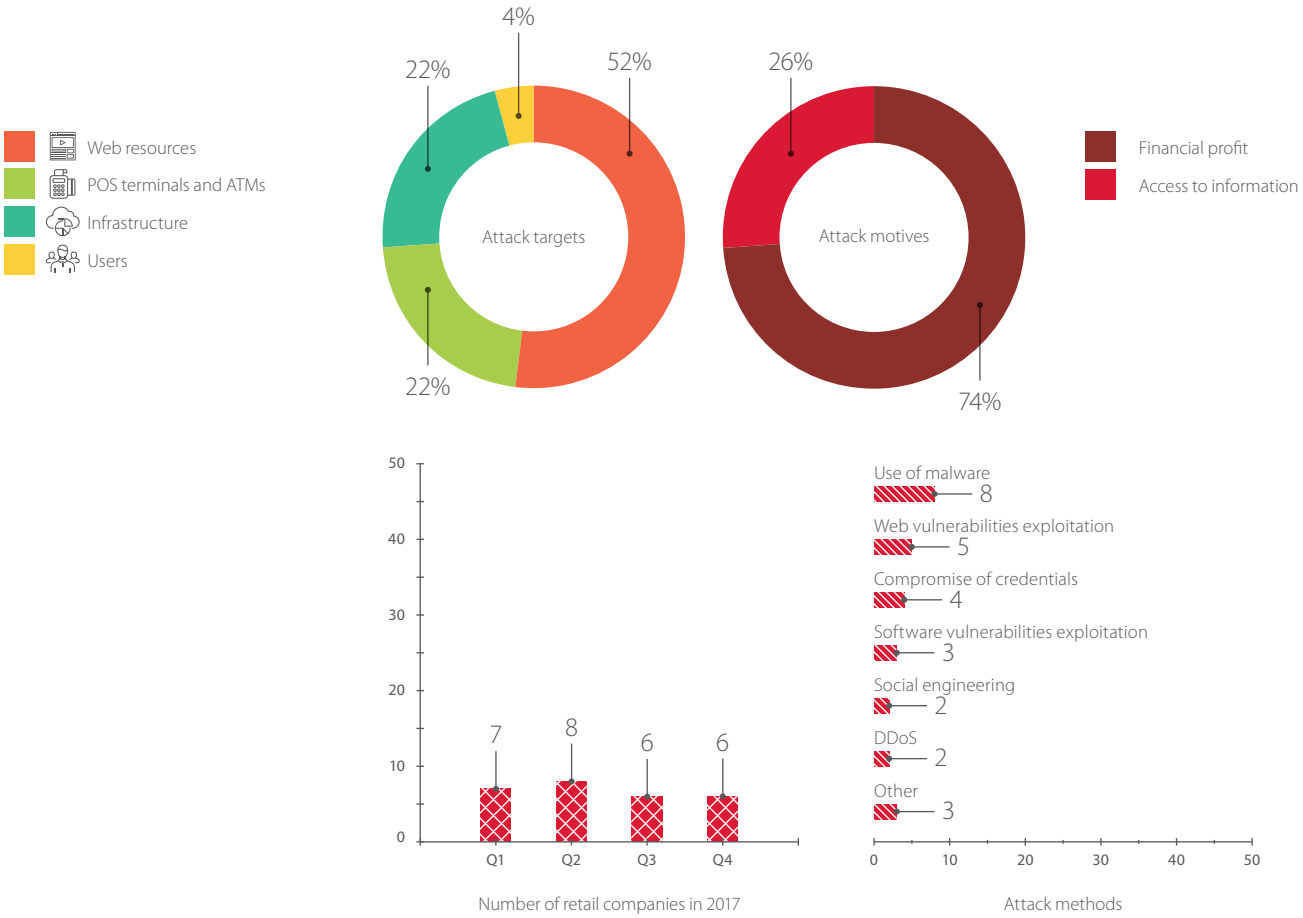
Attack methods

More than half of attacks on industrial companies were carefully planned by groups of hackers. Most often, attackers send phishing messages to employees. If these messages are opened, the attackers then penetrate the target's infrastructure and gain control over IT systems. If the attackers' goal is to collect information, they can lurk for years at a time and silently observe all goings-on at the target company.

We noticed that in 2017, malware aimed at industrial control systems (ICS) and other key systems became more advanced overall, and more alarmingly, better-customized to specific industry infrastructures.

Companies should be concerned: if industry fails to keep operating systems and software up to date, in addition to taking other necessary precautions, headline-grabbing targeted attacks are a distinct possibility.

Retail



Number of retail companies in 2017

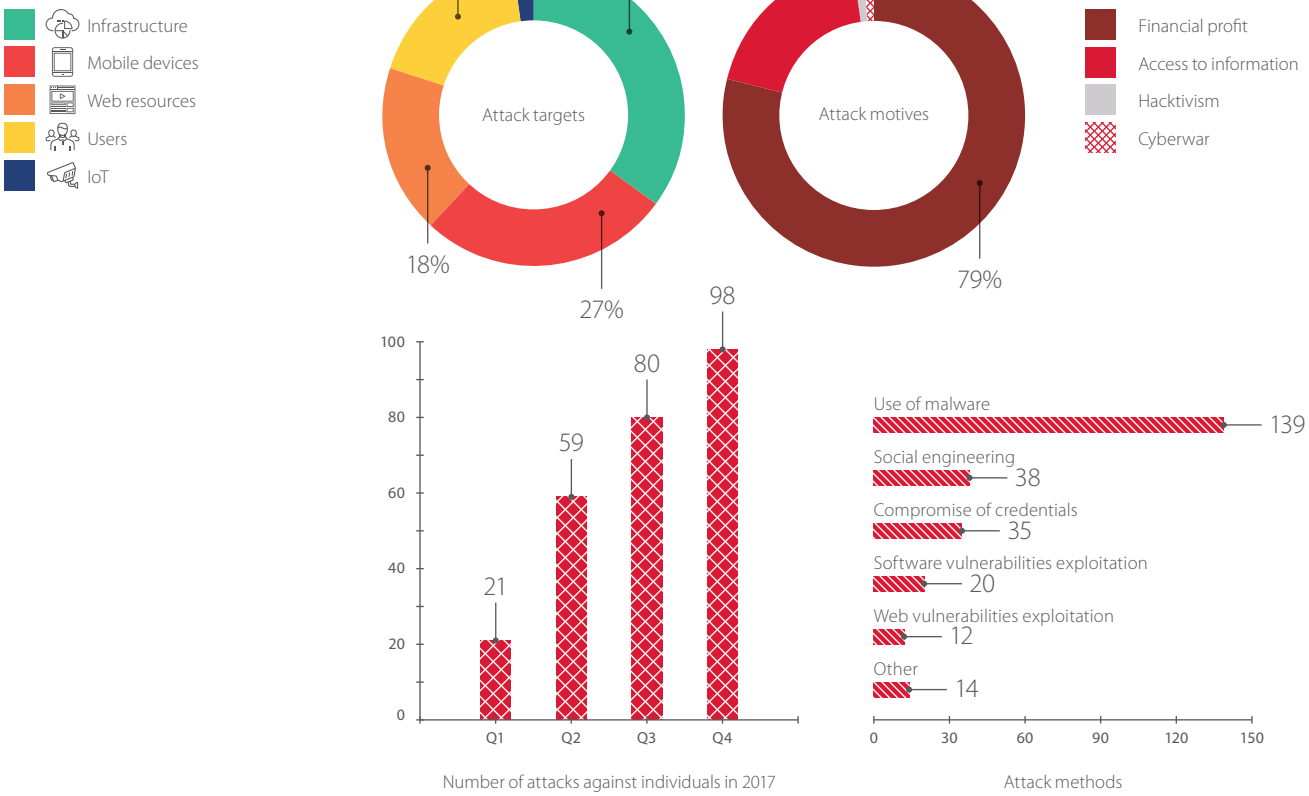
Attack methods

In 2017, half of cyberattacks (52%) in the retail sector were against web applications, primarily online stores. Attackers compromised client credentials, stole credit card information, and disrupted web applications.

Almost every fifth attack (19%) involved planting malware on POS terminals in retail stores, though installing a Trojan on such terminals is not a trivial task. Attackers have a limited window of opportunity for modifying POS firmware: during manufacturing, transportation, repair, or maintenance.

They can also intervene in the update process by compromising the manufacturer's update servers and replacing the original firmware with an altered version. These changes are invisible to store customers. The only difference is that all the information about the payment card ends up in the hands of the attacker, as well as the retailer.

Individuals



Number of attacks against individuals in 2017

Attack methods

Every fourth cyberattack in 2017 targeted ordinary people, and during the year we noticed a significant increase in this category of attacks.

Attackers preferred to use malware and social engineering. Computer literacy and security awareness among the public is growing, forcing attackers to come up with new attack scenarios.

When attacking individuals, cybercriminals were looking for financial gain (a ransom for unlocking data or returning a social network account) or attempting to steal information: credit card numbers or credentials for online services.

Due to the popularity of cryptocurrency, cybercriminals have attempted to monetize the computing power of victims' computers and cell phones. They have spread Trojans and created entire botnets for mining cryptocurrency. Another way is to create special scripts, which run on a website and make visitors' computers perform CPU-intensive mining of cryptocurrency. In this case, cryptocurrency is mined directly in the visitor's browser without installing any malware.

FORECASTS FOR 2018

We predict that many of last year's trends will continue to resonate this year:

+ Large-scale malicious attacks will evolve. They will likely aim at having a destructive impact on the infrastructure of a target company (or even an entire industry, by attacking several companies), as opposed to economic motivation alone. Malware is turning into a bona fide weapon with destructive capabilities.
+ Having proven itself against individuals, Ransomware as a Service will likely be directed against companies instead. As adolescents buy or download malicious software on the Internet and get caught by law enforcement, some will simply try to not get caught next time. More instructions and training materials will appear on the Internet about how to avoid going to jail.
+ Cyberattacks will become even more sophisticated and complex, due to the use of hacked web applications as attack tools and multistage campaigns that affect both a target company and its partners.
+ If operators of network-connected industrial equipment fail to keep operating systems and software up to date, in addition to taking other necessary measures, dramatic targeted attacks on ICS equipment are a distinct risk.
+ As long as banks use cards and card data to authenticate transactions, criminals will continue to profit from flaws in card handling, data storage, and transmission. Malicious software for POS terminals and ATMs will continue to evolve, driving protection to improve as well.
+ Attacks on ICOs will continue. However, if companies pay greater attention to security during the pre-ICO period such as by working with specialists in smart contracts and comprehensive infrastructure protection, the damage from cyberattacks will become significantly lower.
+ When it comes to earning money from website visitors, mining cryptocurrency may soon eclipse contextual advertising.
+ Several services already offer website owners the opportunity to make money by embedding mining scripts in their content. The number of willing owners will grow.
+ In 2017, the number of new botnets and number of devices in existing botnets increased. Soon we can expect new large-scale DDoS attacks, likely with use of known malware.
+ Countries that do not regulate cryptocurrency transactions may reconsider their approach. Without government oversight, cryptocurrency's anonymity may offer a golden opportunity for criminals interested in money laundering.

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.

© 2018 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.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com