



POSITIVE TECHNOLOGIES

Cybersecurity threatscape

Q2 2018









Contents

Symbols used.....	2
Trends and forecasts.....	3
Statistics.....	4
Attack number.....	7
Attack methods.....	8
Malware use.....	8
Social engineering.....	9
Hacking.....	10
Credential compromise.....	11
Web attacks.....	12
DDoS.....	13
Victim categories.....	14
Government.....	14
Healthcare.....	15
Cryptocurrency exchanges.....	16
Retail.....	17
Individuals.....	18
What companies can do to stay safe.....	20
How vendors can secure their products.....	21
How users can avoid falling victim.....	21









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

Victim categories

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



Trends and forecasts

In this quarter's report, Positive Technologies experts share information on the most important IT security threats. This information is drawn from our own expertise, outcomes of numerous investigations, and data from authoritative sources.

Summarizing our findings from the second quarter of 2018, we note the following trends:

- The number of unique cyberincidents continued to grow, exceeding the equivalent year-ago period (Q2 2017) by 47 percent.
- Most cases involved targeted attacks on companies and their clients, as well as cryptocurrency exchanges. Attackers were quite resourceful. Not only did they use malware, but they also sought to exploit zero-day vulnerabilities, used social engineering to steal administrator passwords, and accessed partner companies in order to reach their ultimate targets.
- May and June were marked by a large number of attacks (twice as many as in the first quarter) on cryptocurrency platforms, in which hackers made off with more than \$100 million.
- Data theft continued to account for an increasing share of total attacks. In most cases, attackers sought personal data, credentials, and credit cards. To get this data, they compromised online platforms, including e-commerce websites, online ticketing systems, and hotel booking sites.
- Individuals suffered from malicious software, which was most often installed due to inattentiveness or lack of awareness. However, new methods also came into play, as some new store-bought smartphones came with malware out of the box.

We forecast an increase in the share of attacks aimed at data theft. Many companies fail to properly secure information, especially medical and personal data, making easy pickings even for low-skilled hackers, who perform more and more attacks every day. The information is then sold on the darkweb and used for further attacks.



Statistics

In the second quarter of 2018, we saw a growing number of attacks aimed at obtaining data. Information was the objective in 40 percent of cases, barely edging out financial profit, which was responsible for 39 percent. In our report "The criminal cyberservices market,"¹ we analyzed supply and demand on the darkweb, where sellers offer stolen personal information, credentials, and credit cards. The majority of supply on the darkweb (59% of offers) consists of user credentials for accessing various sites and services, including banks. These credentials are sold individually for up to \$10, or sold for hundreds of dollars when bundled with credentials for millions of other accounts. As a result, individuals or companies victimized by data theft can expect to be targeted soon after in follow-on attacks that attempt to make use of stolen credentials.

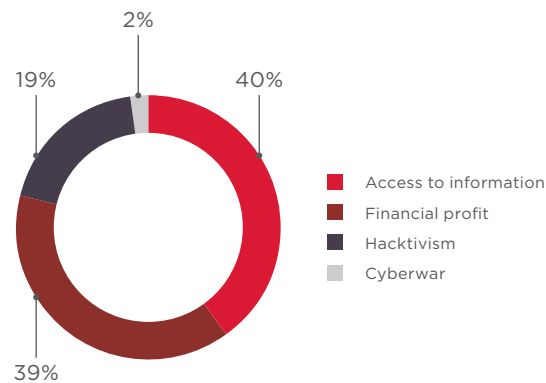


Figure 1. Attackers' motives

We took a look at which information attracted hackers the most in Q2 2018. At the top of the list are personal data (30%) and account credentials (22%), such as for online banking. Credit and debit card information (15%) was obtained most often by using spyware or via compromised websites.

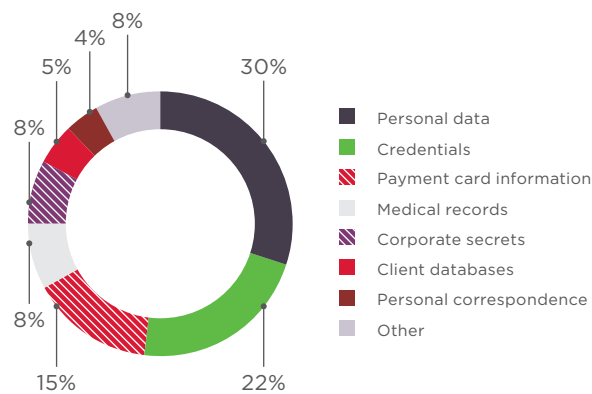


Figure 2. Types of stolen data

In Q2 2018, we saw a large number of targeted attacks against companies and organizations. Targeted attacks accounted for 54 percent of the total, outnumbering mass campaigns. Later in this report, we will more closely consider attacks against government and healthcare, since these two sectors are especially popular with hackers, as well as attacks on cryptocurrency exchanges, retailers, and individuals.

¹ [ptsecurity.com/ru-ru/research/analitics/darkweb-2018/](https://www.ptsecurity.com/ru-ru/research/analitics/darkweb-2018/)



Large-scale cyberattacks affecting more than one industry (most often, malware outbreaks) have been placed in the "Multiple industries" category.

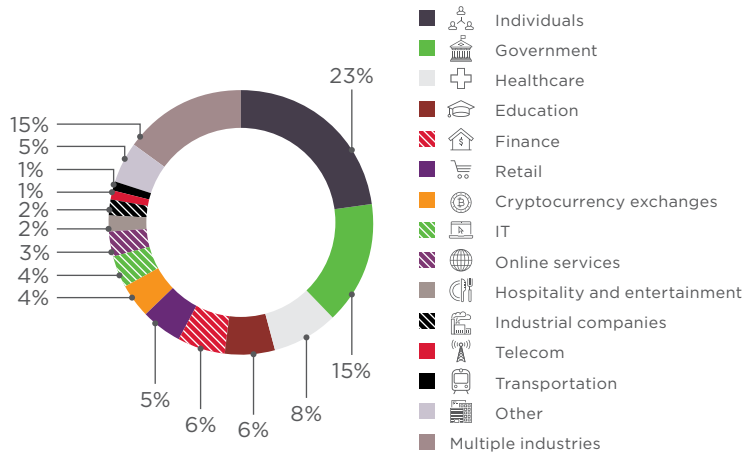


Figure 3. Victim categories

In Q2 2018, 44 percent of attacks were directed at infrastructure. Attacks on web resources increased compared to Q2 2017, growing from 23 to 32 percent of the total. In comparison to the prior quarter, attacks on IoT devices also grew, which can be explained by the appearance of new botnets, including PyRoMineloT, Muhstik, and Wicked Mirai.

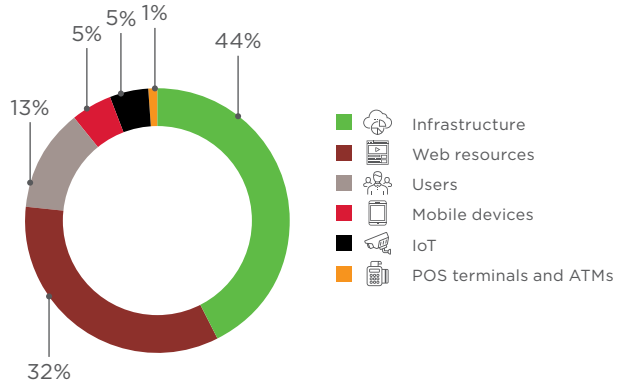


Figure 4. Attack targets

Malware attacks decreased to 49 percent, compared to 63 percent in Q1. However, credential compromises jumped by 12 percent during the same period. We will take a closer look at each attack method and indicate which targets and industries were most affected.

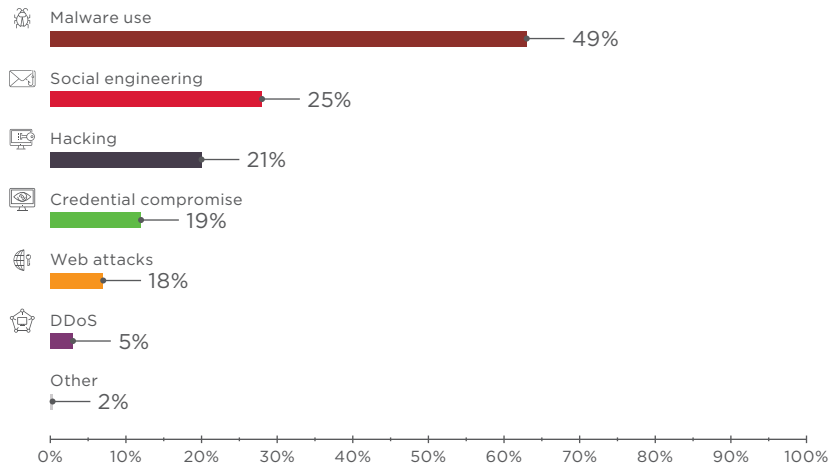
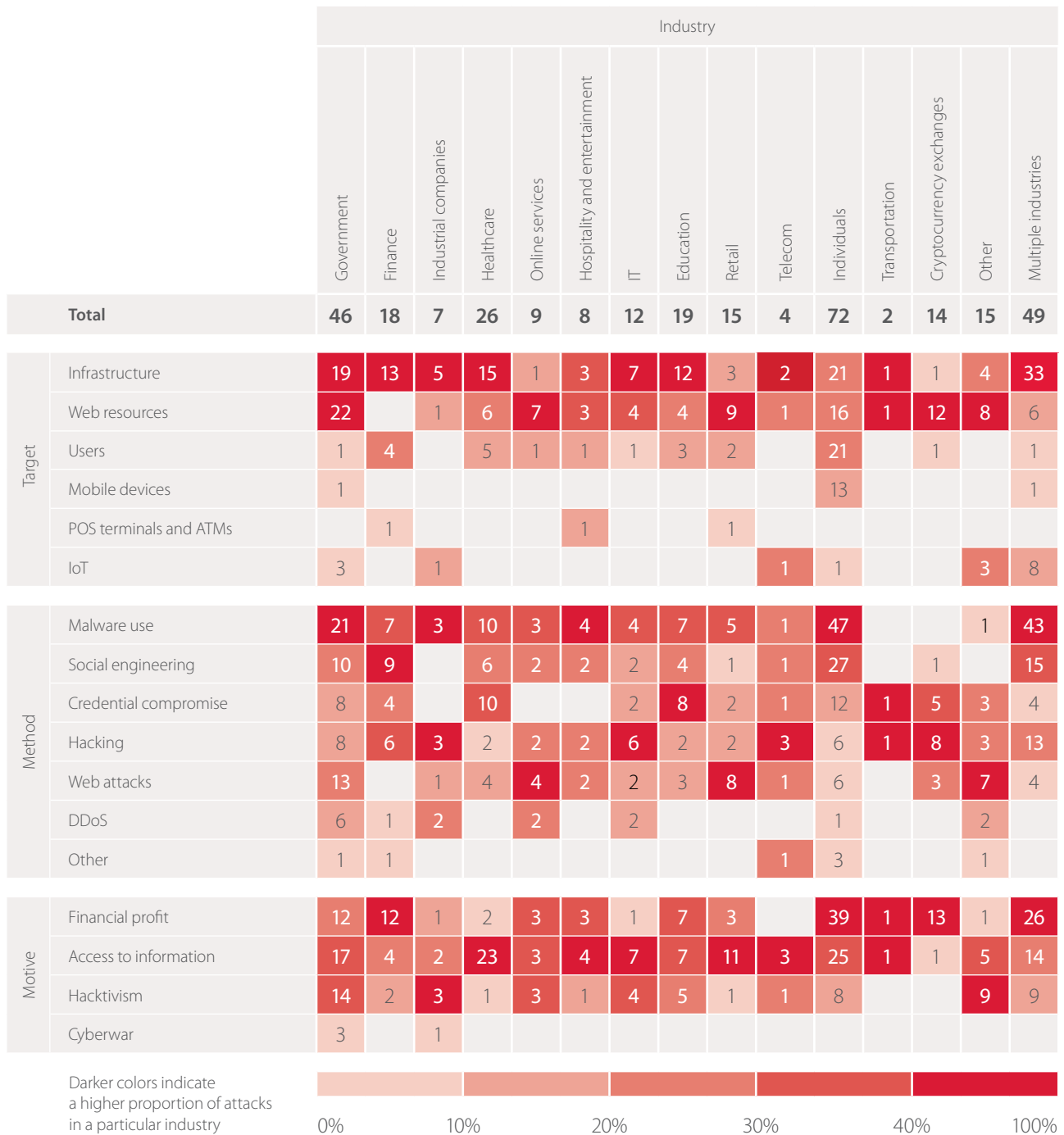


Figure 5. Attack methods



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





Attack number

The number of unique cyberincidents in Q2 2018 increased by 47 percent year-over-year.

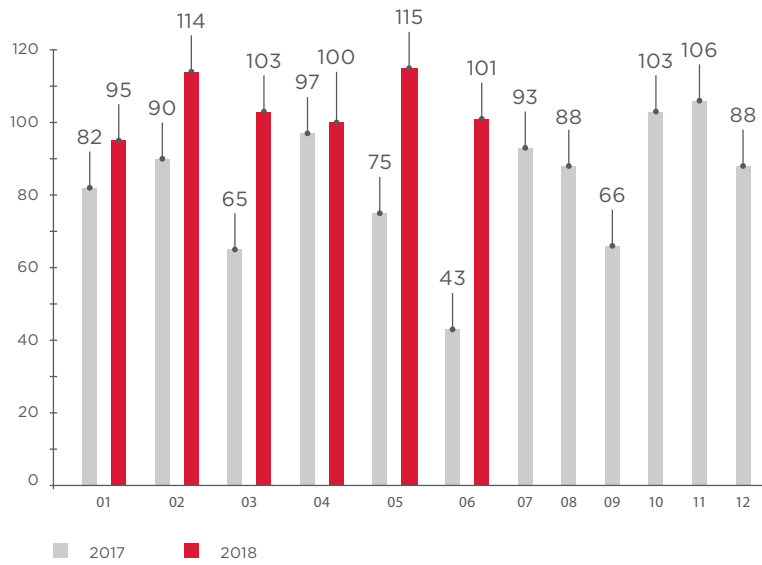


Figure 6. Number of incidents per month in 2017 and 2018 (1 = January, 12 = December)

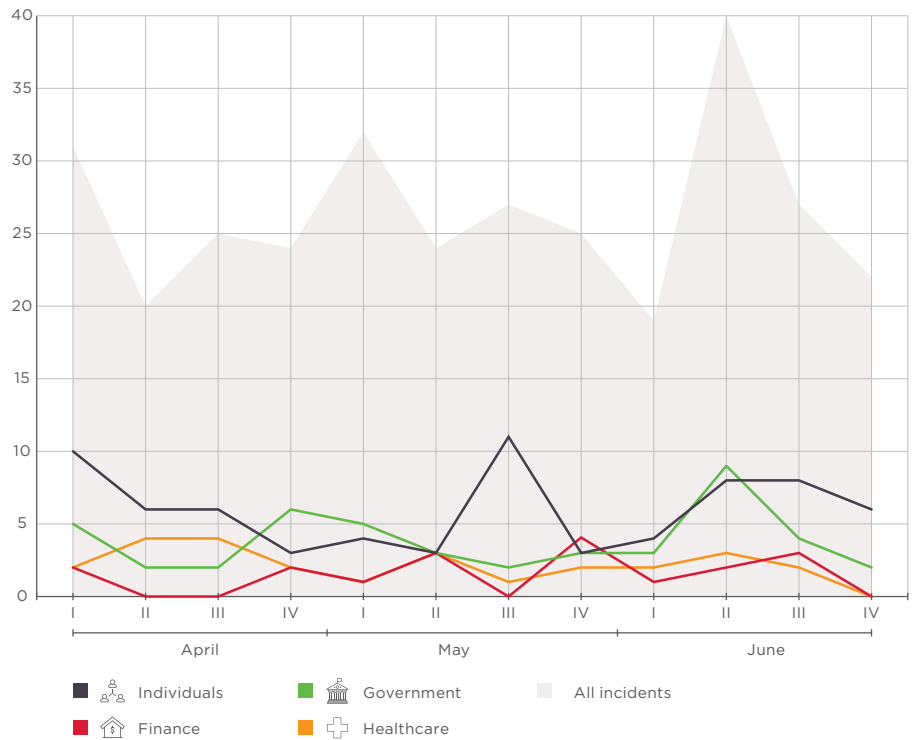


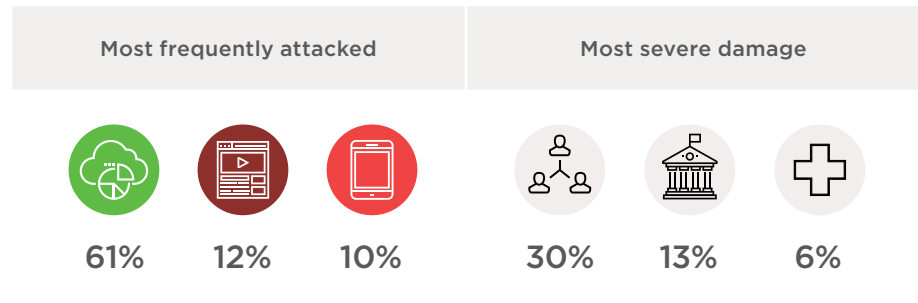
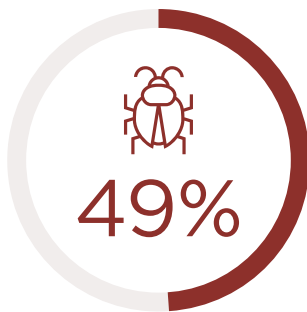
Figure 7. Number of incidents in Q2 2018 (by week)



Attack methods

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

Malware use



As mentioned, cybercriminals continue to harvest data from victims' PCs. They commonly use spyware (26%) or remote administration malware (22%) for the purpose. The number of cyberincidents with ransomware and miners decreased in Q2 compared to Q1. Attackers still find plenty of ways to incorporate leaked NSA exploits into their own malware. In one example, PyRoMine mining malware used the EternalRomance exploit (MS17-010) to steal computing power and create a hidden administrator account with remote desktop capabilities, setting the stage for subsequent attacks.

The three most common infection methods in Q2 2018 were:

- Compromising servers and workstations by accessing a targeted system using vulnerabilities, social engineering techniques, or bruteforced passwords (29%)
- Planting malicious software on victims' devices via infected websites (29%)
- Sending malicious attachments, or links to infected sites, by email (23%)

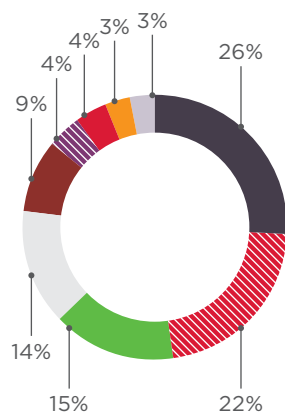
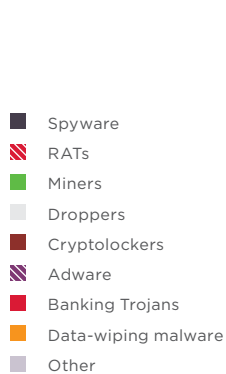


Figure 8. Malware types

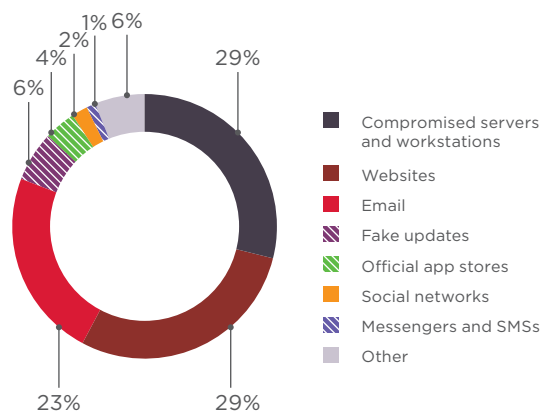


Figure 9. Malware distribution methods

Malicious emails remain the most common method for penetrating a target as part of an advanced persistent threat (APT). In Q2 2018, Positive Technologies Expert Security Center (PT ESC) experts detected a number of attempts to infect victims by means of malware-laden Microsoft Word documents.

To make an email look credible, attackers may forge sender addresses.

PT ESC experts also detected a phishing attack against a major IT company involving PlugX. The PlugX RAT (Remote Access Trojan) has been used by attackers for years against various companies for espionage purposes.



Social engineering

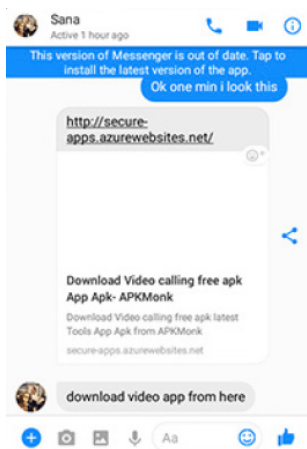
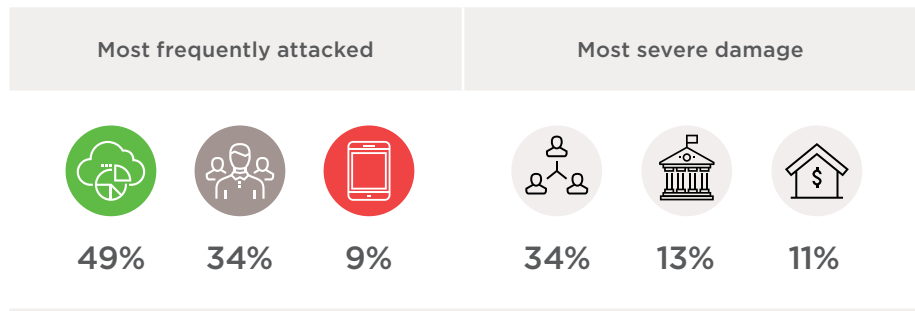


Figure 10. Phishing on Facebook

Cybercriminals keep inventing new methods and refining old ones to manipulate users, infect targeted systems with malicious software, steal money, and access confidential information. In May, Lookout reported² on attacks against government officials, diplomats, military figures, and other high-profile individuals in Pakistan, Afghanistan, India, and the UAE. Important information was stolen from their smartphones, including images, audio files, and text messages. To infect their victims, attackers initiated a conversation on Facebook and sent a phishing link, such as to a "video." In reality, opening the link would trigger installation of malicious software on the victim's smartphone from a third-party app store.

Also in May, Radware detected a malicious campaign on Facebook.³ Infected Facebook accounts pushed out phishing links to potential victims. On the linked page, which was made to resemble YouTube, victims were prompted to install a Google Chrome extension. The malicious extensions masqueraded as legitimate in the official Chrome Web Store. They turned infected computers into botnet "zombies," stole Facebook and Instagram credentials, and distributed malware to the victim's friends. Computing power of the infected devices was used for cryptocurrency mining.

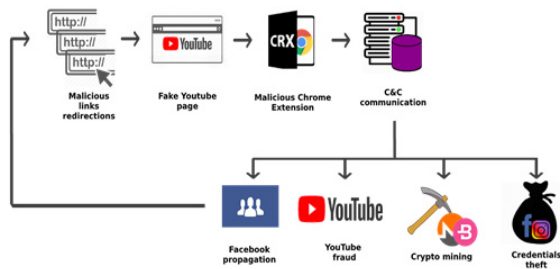


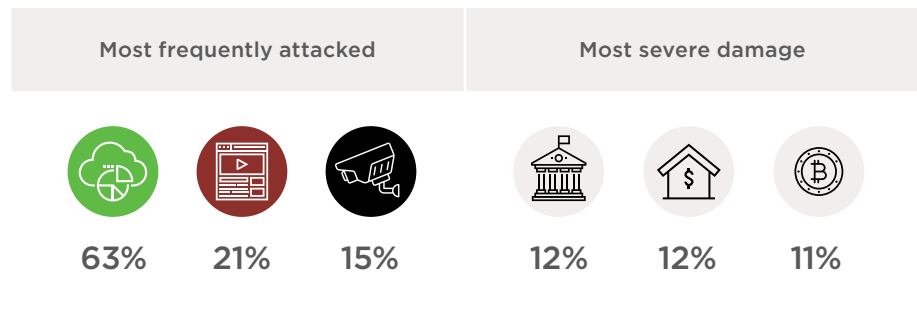
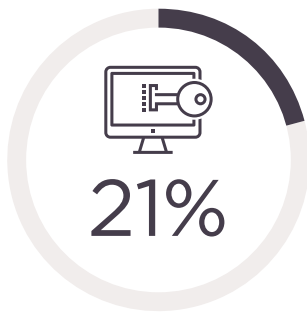
Figure 11. Scheme of a phishing attack via Facebook

2 info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

3 blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/



Hacking



Most attacks are carefully planned well in advance. The first step often consists of hacking—that is, exploiting vulnerabilities in software and hardware, or otherwise taking advantage of deficient protection mechanisms and security flaws.

But it is not always feasible to send malware by email to the target. Case in point: IoT botnets. A vulnerability in DrayTek (Taiwan) routers allowed attackers to gain administrator rights and change DNS settings, thereby redirecting all user traffic to an unknown server.⁴ Fortunately, the manufacturer acknowledged the vulnerability and quickly patched the issue in a security update.

Vulnerabilities in public DNS servers allow conducting phishing attacks against website users. In April, attackers compromised several DNS servers to redirect the users of the MyEtherWallet cryptocurrency wallet to a phishing website.⁵ In most cases browsers notify about SSL certificate mismatches, but these warnings often go ignored by users. As a result, the hackers made off with an estimated \$160,000.

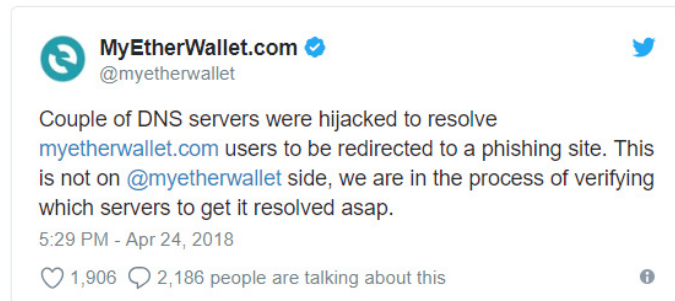


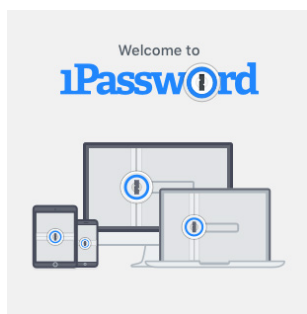
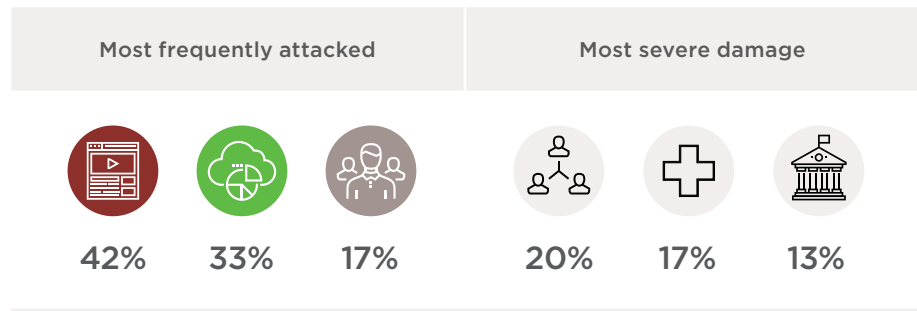
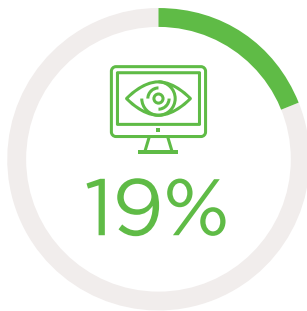
Figure 12. Notice regarding the MyEtherWallet.com attack

4 draytek.com/en/about/news/2018/notification-of-urgent-security-updates-to-draytek-router

5 www.bleepingcomputer.com/news/security/hacker-hijacks-dns-server-of-myetherwallet-to-steal-160-000/?utm_campaign=Security%2BNewsletter&utm_source=Security_Newsletter_co_85



Credential compromise



Users can choose from a number of password managers for creating, storing, and entering passwords. But by the same token, an attacker who obtains access to a victim's password manager is nearly unstoppable. Taylor, an ICO startup, lost more than \$1.47 million in one such incident in May 2018.⁶ According to the startup, cybercriminals compromised an employee's device and accessed 1Password files, including ICO-related passwords. The next step was to transfer all the cryptocurrency to the attackers' account.

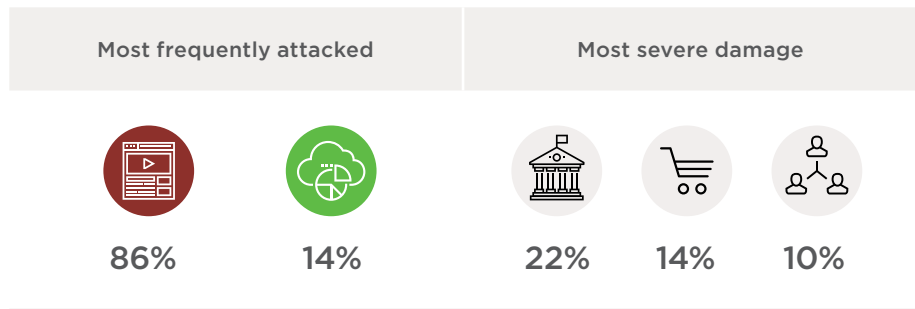
Users of the WordPress CMS platform who insufficiently protected their credentials (in particular, by not using two-factor authentication) fell victim to mass attacks.⁷ Hackers obtained administrative access to the websites and installed the Jetpack plug-in to redirect users to phishing sites. As a result, companies relying on WordPress-powered sites unwittingly participated in attacks against their clients.

⁶ medium.com/smarttaylor/this-is-a-dark-day-for-taylor-ded587463da7

⁷ wordfence.com/blog/2018/05/wordpress-com-jetpack-infection/



Web attacks



Cybercriminals eagerly extort and shake down site owners for profit, such as by threatening to steal client databases or shut down the website entirely. In May, one attacker offered to sell information to Ticketfly, a ticket seller, about vulnerabilities in the company's website.⁸ Ticketfly refused, after which the attacker defaced the main page of the website and published links to the client database.

Hacktivists also conduct defacement attacks against government websites. Recent victims include the Ministry of Defense and the Supreme Court of India⁹ and Bologna municipality in Italy.¹⁰

In April, a Pakistani hacker attacked the web resources of Thai Airways, including the official website, mail server, payment system, and booking system. The attacker altered several pages and accessed clients' personal data.



Figure 13. Message about hacking of the Indian Ministry of Defense website



Figure 14. Defacement of the Bologna municipality website

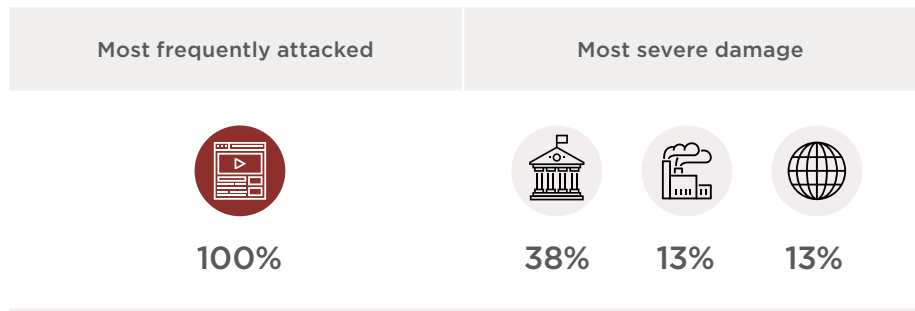
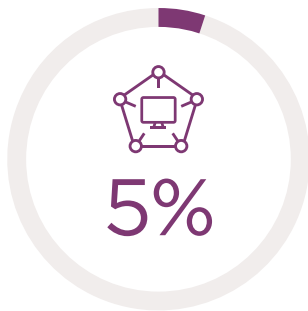
8 twitter.com/ticketfly/status/1002144038319882240

9 bankinfosecurity.asia/supreme-court-website-defaced-a-10867

10 bologna.repubblica.it/cronaca/2018/04/26/news/bologna_il_sito_del_comune_sotto_attacco_informatico-194878573/?refresh_ce



DDoS



DDoS is a weapon of choice for business rivals, disgruntled clients, and hackers. These attacks mostly hit government institutions. High-profile political events are a major driver of interest. In one example, the website of a Mexican opposition political party was attacked during the final TV debate of the presidential campaign.¹¹

Cybercriminals also perform DDoS attacks for profit. They take websites offline and demand that the victim pay up in order for the attack to stop. PT ESC experts investigated one such incident in June, when attackers performed several short DDoS attacks (each less than 2 minutes in duration) on a company website to demonstrate their abilities. They threatened to continue the attack if the company refused to pay a ransom. The criminals used Wreckuests, a freely distributed utility for performing DDoS attacks with HTTP flooding. Wreckuests generated a large number of GET requests with random parameters via a network of proxy servers, which overwhelmed the technical capacity of the website and caused denial of service.

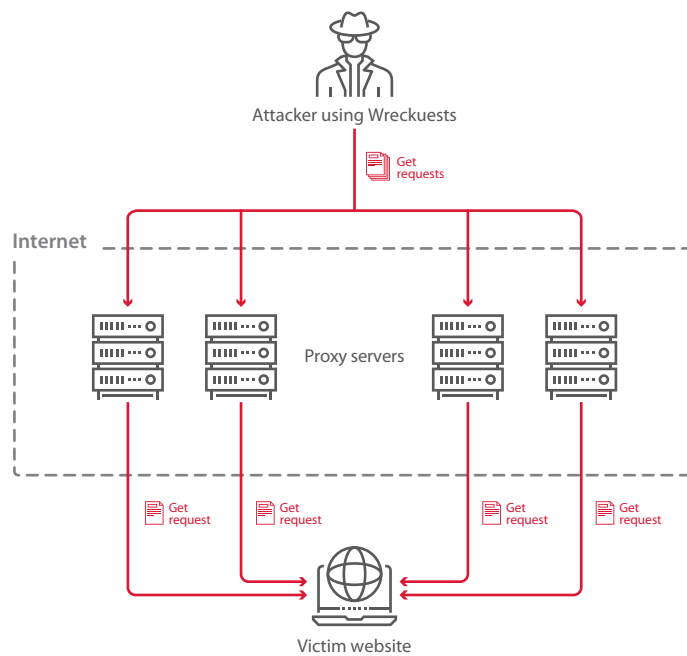


Figure 15. Illustration of DDoS attack with Wreckuests

¹¹ [reuters.com/article/uk-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerve-idUKKBN1J93C0](https://www.reuters.com/article/uk-mexico-election-cyber/cyber-attack-on-mexico-campaign-site-triggers-election-nerve-idUKKBN1J93C0)



Victim categories

Here we will analyze the most important attacks against particular sectors in Q2 2018.

Government



Damage over \$150,000

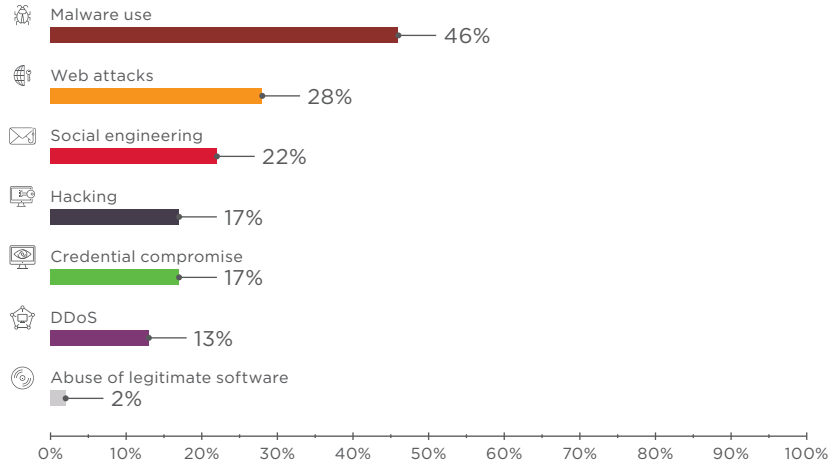


Figure 16. Government: attack methods used

- Web resources
- Infrastructure
- IoT
- Users (employees)
- Mobile devices

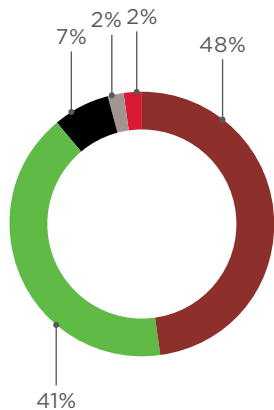


Figure 17. Attack targets

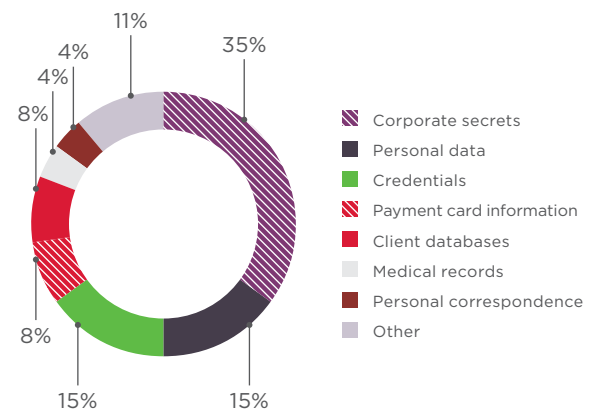


Figure 18. Data stolen



Figure 19. Phishing Facebook account with link to malicious Dardesh instant messenger

Governments remain a favorite target for criminals. In particular, state-owned companies are a ripe source of commercial secrets. In the outgoing quarter, we detected an increase in attacks against employees and spying on them. For example, the APT-C23¹² and ViperRAT¹³ groups distributed malicious software with the help of social engineering and the official Google Play store.

The APT-C23 attackers used social media accounts to pose as young women and persuade victims to download the infected Dardesh instant messenger from Google Play. Dardesh then downloaded the second component of the malware, disguised as a configuration program. As a result, the attackers could secretly spy on victims, record audio, and copy data.

12 blog.lookout.com/desert-scorpion-google-play
 13 blog.lookout.com/viperratt-google-play



Victims over 1 million

Healthcare

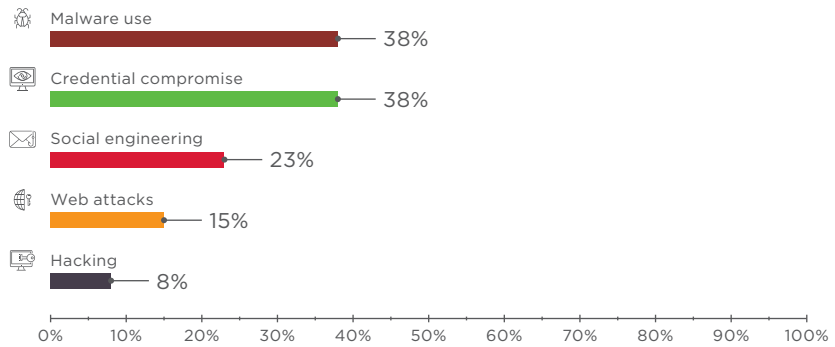


Figure 20. Healthcare: attacks methods used

- Infrastructure
- Web resources
- Users (employees)

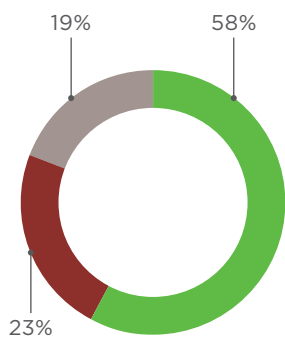


Figure 21. Attack targets

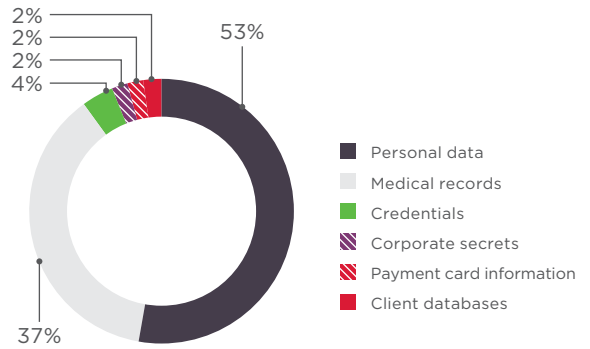


Figure 22. Data stolen

Healthcare institutions process huge amounts of data. Perhaps unsurprisingly, information security often takes a back seat to patient care and other considerations. As a result, 88 percent of attacks performed against health facilities in Q2 2018 involved data theft. In addition to personal information and run-of-the-mill medical records, hackers are also starting to show interest in new kinds of information, such as the results of genetic tests. In April, hackers attacked Sangamo Therapeutics, a company focused on decoding the human genome and treating genetic diseases.¹⁴ They hacked an email account of a top executive and therefore had the ability to compromise the company's internal resources.

Another burning issue is digital interruption to healthcare operations. Hackers don't hesitate to hold the data of medical institutions hostage. SamSam ransomware has been hitting government-owned and private healthcare providers for three years.¹⁵ SamSam brings healthcare to a halt by encrypting all data on a hospital's servers and then demanding a ransom for the decryption key. Restoring data from backups takes time, all while patient lives are at stake. This is one reason why hospitals often give in to ransom demands, even if they have working backups.

¹⁴ sec.gov/Archives/edgar/data/1001233/000119312518119788/d562135d8k.htm

¹⁵ healthitsecurity.com/news/samsam-ransomware-attackers-target-healthcare-providers



Cryptocurrency exchanges



Damage over \$100 million

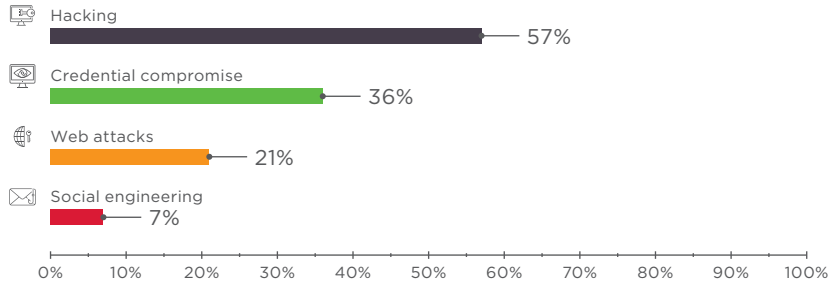


Figure 23. Cryptocurrency exchanges: attacks methods used in Q2 2018

- Web resources
- Infrastructure
- Users (employees)

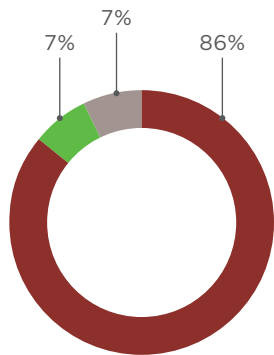


Figure 24. Attack targets



Figure 25. Data stolen



An unknown party accessing large amounts of hashpower is using "51% attacks" to perform "double spend" attacks on Exchanges. We have been advising all exchanges to increase their confirmations requirement and to review large deposits.



6:47 PM - 18 May 2018



\$XVG @vergecurrency is once again under attack, someone is 51%ing the chain and invalidating all legit blocks. All pools and miners suffer from this, the attacker is getting all blocks currently.

10:51 AM - 22 May 2018

Figure 26. Attacks on cryptocurrency networks

In Q2 2018 a number of so-called "51% attacks" targeted cryptocurrencies based on the proof of work (PoW) consensus mechanism. Attackers (in most cases, a group of them) obtain a majority of the computing power on the network, which is measured by the hash rate. An attacker with control of more than half of the network's hash rate can wreak havoc by rolling back or refusing to confirm transactions, or even double-spending (paying with the same coin multiple times).

Hackers stole tens of millions of dollars by attacking Verge,¹⁶ Monacoin,¹⁷ Bitcoin Gold,¹⁸ ZenCash,¹⁹ and Litecoin Cash.²⁰ Although criminals did not steal directly from users in these attacks, clients still lose out. The affected cryptocurrencies stand to lose credibility, risk bankruptcy, and have funds frozen. The value of client investments will suffer accordingly.

16 news.bitcoin.com/verge-struck-by-second-pow-attack-in-as-many-months/
 17 newsbtc.com/2018/05/22/japans-monacoin-network-still-suffering-selfless-mining-attack/
 18 forum.bitcoingold.org/t/double-spend-attacks-on-exchanges/1362
 19 bitcoinist.com/zencash-target-51-attack-loses-500k-double-spend-transactions/
 20 cryptocurrencynews.com/litecoin-cash-lcc-51-attack/



Victims over 48 million

Retail

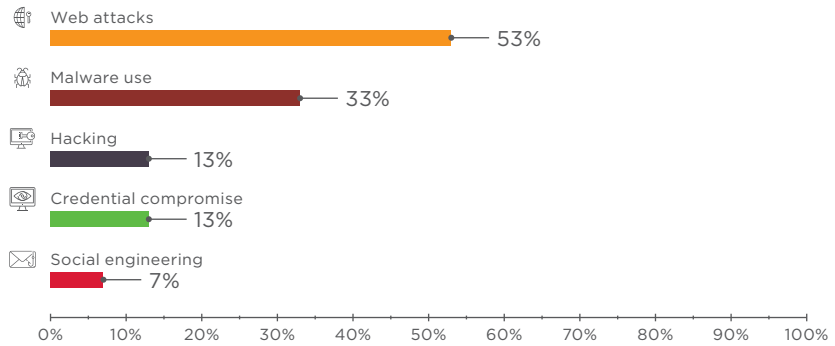


Figure 27. Retail: attack methods used in Q2 2018

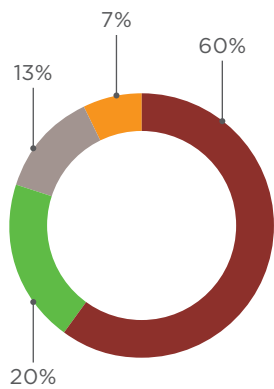
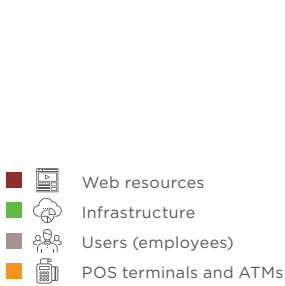


Figure 28. Attack targets

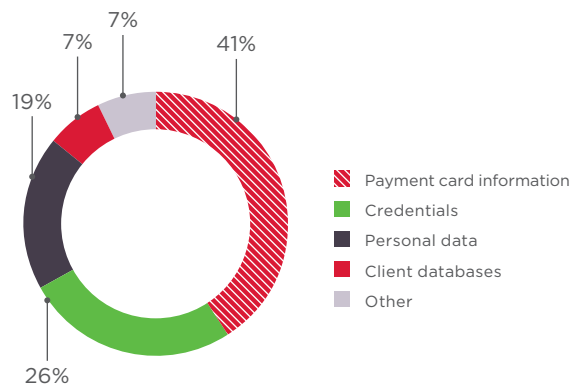


Figure 29. Data stolen

Customers are the main victims of attacks against retail and online stores. Some attacks remain unnoticed for several months, until "card dumps" are put up for sale on the darkweb.

In one such case, hackers stole information for more than 5 million credit cards from Saks Fifth Avenue and Lord & Taylor. The data was then offered to buyers online.²¹ Theft was made possible by malware placed on POS terminals in retail stores. Nothing about the payment process would have seemed out of place to customers and store staff.

More than half (60%) of retail attacks were aimed at websites. Online stores may be a company's primary or only source of business, making them extremely sensitive to any disruption. Ticketfly, a ticket seller, temporarily suspended operations because of defacement of the main page of the company's website. Another threat comes from web vulnerabilities, which may allow hackers to access personal data and payment information. For instance, the website for American bakery chain Panera Bread did not sufficiently protect user information.²² As a result, names, email addresses, physical addresses, dates of birth, and the last four numbers of credit cards for millions of users were available in plain text.

21 blog.gemalto.com/security/2018/04/03/saksfifthavenuedatabreach/

22 krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/



```

Secure | https://delivery.panerabread.com
{"accounts": [{"username": " ", "name": " ", "cardNumber": "*****6515"},
{"username": " ", "name": " ", "cardNumber": "*****5527"},
{"username": " ", "name": " ", "cardNumber": "*****7921"},
{"username": " @msn.com", "name": "F B", "cardNumber": "*****7188"},
{"username": " @yahoo.com", "name": "C", "cardNumber": "*****6128"},
{"username": " @aol.com", "name": " ", "cardNumber": "*****6061"},
{"username": " @yahoo.com", "name": " ", "cardNumber": "*****8950"},
{"username": "k", "name": " ", "cardNumber": "*****4412"},
{"username": "l", "name": " ", "cardNumber": "*****8386"},
{"username": " @aol.com", "name": " ", "cardNumber": "*****5384"},
{"username": " @optonline.net", "name": " ", "cardNumber": "*****5144"},
{"username": " @hotmail.com", "name": " ", "cardNumber": "*****7488"},
{"username": " ", "name": " ", "cardNumber": "*****6702"},
{"username": " ", "name": " ", "cardNumber": "*****7085"}, {"username": " @hotmail.com", "name": " ", "cardNumber": "*****4220"}, {"username": " ", "name": " ", "cardNumber": "*****9123"}, {"username": "art", "name": " ", "cardNumber": "*****8139"}, {"username": " ", "name": " ", "cardNumber": "*****0102"}, {"username": " ", "name": " ", "cardNumber": "*****6851"}, {"username": "k", "name": "Sandra", "cardNumber": "*****2654"}]}}

```

Figure 30. Poor security on Panerabread.com

Individuals



Damage over \$22 million
Victims over 765 million

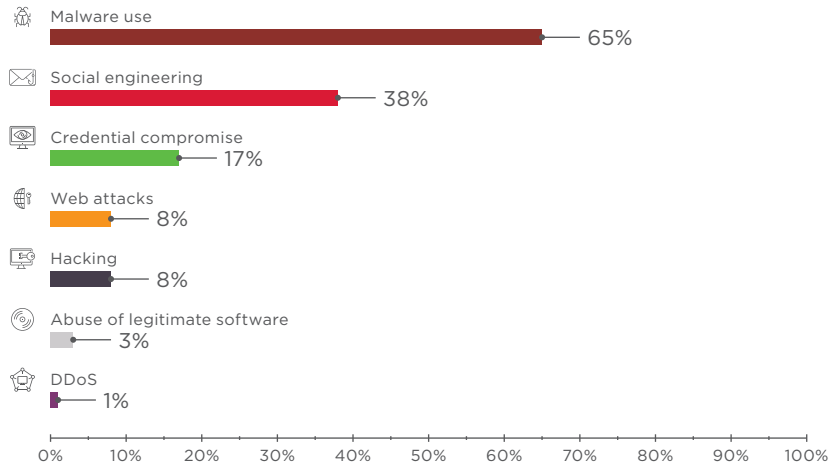


Figure 31. Individuals: attack methods used

- Infrastructure
- Users
- Web resources
- Mobile devices
- IoT

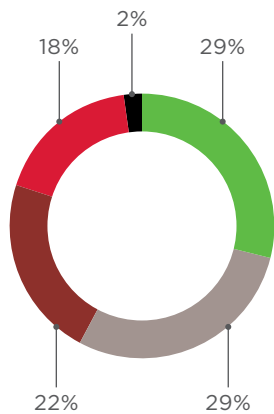


Figure 32. Attack targets

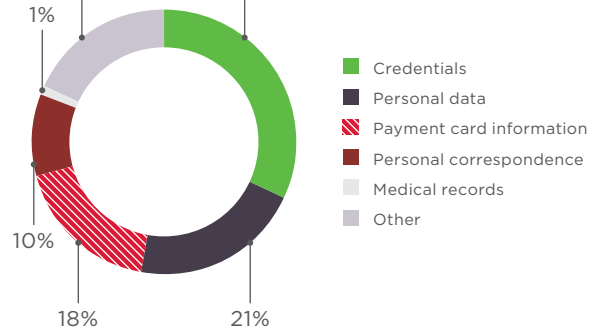


Figure 33. Data stolen

Every fourth attack is directed at individuals. These attacks are usually large-scale, making for a total of hundreds of millions of victims.



Malicious software may even come pre-installed on new smartphones bought in stores, particularly in the case of some Chinese brands. Avast researchers discovered Cosiloon malware installed at the firmware level on thousands of mobile phones.²³ The manufacturer installed dropper apps to covertly place adware. Since the payloads are downloaded from a command-and-control server, threats go beyond just annoying pop-ups. Spyware, ransomware, and any other type of malware could be placed on the devices via the same mechanism.

In early summer, security experts detected a malicious campaign directed at macOS users.²⁴ Messages on cryptocurrency-focused Slack and Discord channels urged users to run a particular command to resolve issues. But the command was actually malicious and allowed hackers to access the victim's system. The attackers could use this access for subsequent attacks, such as stealing cryptocurrency.

²³ blog.avast.com/android-devices-ship-with-pre-installed-malware

²⁴ objective-see.com/blog/blog_0x32.html



What companies can do to stay safe

What companies can do to stay safe:

- Centralized update management
- Antivirus protection on all systems and endpoints, preferably with support for on-demand scanning by users of suspicious attachments prior to opening them
- SIEM capabilities, for timely attack detection
- Automated software audit tools, to identify vulnerabilities
- Web application firewall, as a preventive measure for websites
- Anti-DDoS services

Protect your data:

- Encrypt all sensitive information. Do not store sensitive information where it can be publicly accessed.
- Perform regular backups and keep them on dedicated servers that are isolated from the network segments used for day-to-day operations.
- Minimize the privileges of users and services as much as possible.
- Do not allow reuse of identical username–password combinations for multiple systems.
- Use two-factor authentication where possible, especially for authenticating privileged accounts.

Do not allow weak passwords:

- Enforce a password policy with strict length and complexity requirements.
- Require password changes every 90 days.
- Replace all default passwords with stronger ones that are unique.

Monitor and stay current:

- Keep software up to date. Do not delay installing patches.
- Test and educate employees regarding information security.
- Monitor the network perimeter for any new insecure resources.
- 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.
- Track the number of incoming requests per second. Configure servers and network devices to resist typical attacks (including TCP/UDP flooding and database overloading).
- Filter traffic to minimize the number of network service interfaces accessible to external attackers.

Keep clients in mind:

- Improve security awareness among clients.
- Regularly remind clients how to stay safe online from the most common attacks.
- Urge clients to not enter their credentials on suspicious websites and to not give out such information by email or over the phone.
- Explain what clients should do if they suspect fraud.
- Inform of security-related events.



How vendors can secure their products

- All of the preceding recommendations for companies ("What companies can do to stay safe"), plus:
- Implement a secure development lifecycle (SSDL).
- Regularly audit the security of software and web applications, including source-code analysis.
- Keep web servers and database software up to date.
- Do not use libraries or frameworks with known vulnerabilities.

How users can avoid falling victim

Invest in security:

- Use only licensed software.
- Maintain effective antivirus protection on all devices.
- Keep software up to date. Do not delay installing patches.

Protect your data:

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

Do not use weak passwords:

- Set strong passwords at least eight characters long that include hard-to-guess combinations of letters, numbers, and special characters. Consider using a password manager to store, generate, and automatically enter all your passwords.
- Do not reuse 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.
- Beware of websites with invalid certificates. Remember that data entered on such websites can be intercepted.
- 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 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

© 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.