

A person wearing a grey hoodie is shown from the chest up, facing forward. The image is heavily stylized with a dark, textured overlay that resembles a cityscape or a digital environment. The background is a bright, cloudy sky. The overall aesthetic is gritty and futuristic.

POSITIVE TECHNOLOGIES

Cybersecurity threatscape

Q4 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
Web attacks.....	11
Credential compromise.....	12
DDoS.....	13
Victim categories	14
Government	14
Healthcare.....	16
Finance.....	17
IT	18
Individuals.....	19
What companies can do to stay safe.....	20
How vendors can secure their products.....	21
How users can avoid falling victim	22



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 fourth quarter of 2018, we note the following trends:

- The number of unique cyberincidents grew by 11 percent compared to Q4 2017, and by 7 percent compared to Q3 2018.
- As in previous quarters, nearly one in three leaks involved users' personal data. Reports of such leaks may become more prevalent in 2019. Our experts anticipate that introduction of the General Data Protection Regulation (GDPR), which sets rules for protection of personal data regarding EU citizens, may contribute to this trend.¹ Inspired by news of the first fines and notices (such as one for EUR 20 million²), companies will tend to inform clients of cyberattacks instead of staying silent as in the past.
- Attackers are actively embedding malicious scripts in the code of vulnerable web resources, siphoning off credit and debit card information from payment pages. This technique particularly threatens government sites responsible for handling municipal payments, since they are poorly protected.
- Weakness of the network perimeter was demonstrated in a relatively simple brute-force attack, in which remote access to a computer was established via RDP. This particular hacker struck dozens of companies in a wide range of industries. So it is fair to say that many companies fail to take administration and monitoring of their network perimeter seriously.
- Another problematic issue involves publication of articles by security researchers about zero-day vulnerabilities. Although information becomes public only after patches have been released, users often do not install these patches right away. Meanwhile, attackers quickly move to take advantage with the help of published information and, in some cases, even ready-made exploits.

¹ ec.europa.eu/info/law/law-topic/data-protection_en

² theinquirer.net/inquirer/news/3063193/ico-slaps-aggregateiq-with-first-official-gdpr-notice



Statistics

In Q4 2018, 48 percent of attacks were intended to obtain data. In half of them, attackers used malware. The share of incidents aimed at direct financial profit grew by 6 percent quarter-over-quarter. Compared to 2017, data theft has become more common than theft of funds from bank accounts and the like. Unfortunately, many worry only about keeping their bank balances intact. Yet personal data, credentials, card numbers, and medical information can provide criminals with a wealth of information, sometimes at the expense of these very same users.

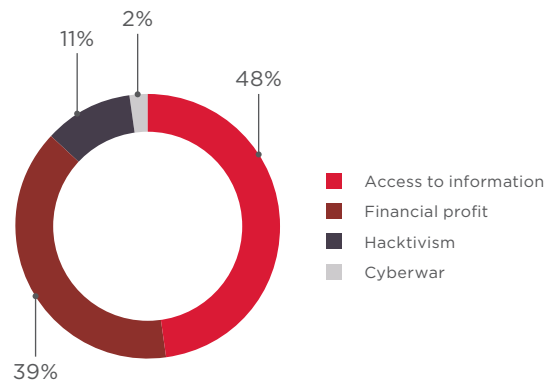


Figure 1. Attackers' motives

In Q4 2018, attackers targeted credentials (usernames and passwords) in 28 percent of attacks. These credentials were used for different services and systems, including corporate email. Note that in most cases, attackers do not have to use special software to obtain this information. People continue to use their birthdays, dog names, and other public information for their security questions. Personal data was stolen in 27 percent of cases, while payment card information was stolen in 16 percent. Towards year's end, attackers intensified their efforts to plant malicious scripts on websites to steal user-entered information.

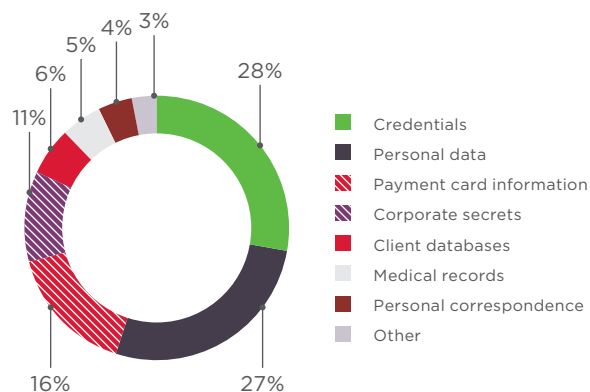


Figure 2. Types of stolen data

In Q4 2018, the percentage of targeted attacks continued growing, reaching 62 percent. Attackers are increasingly turning to individualized approaches against corporate targets, while home users are being hit by mass malware infections. In this report, we will focus on the most popular targets of cybercriminals: individual users, government, healthcare, finance, and IT.

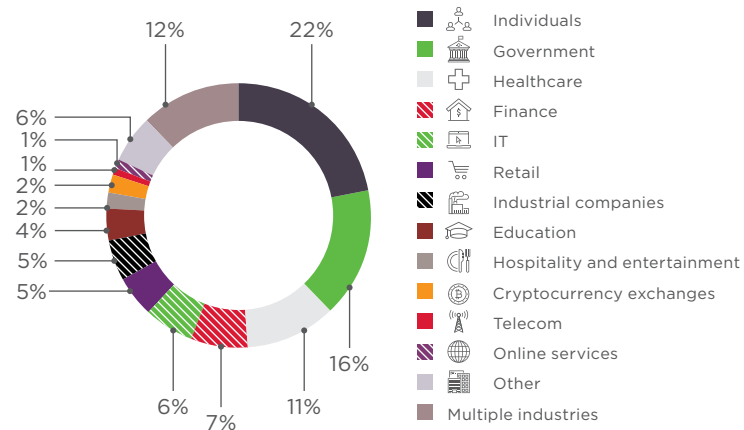


Figure 3. Victim categories

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

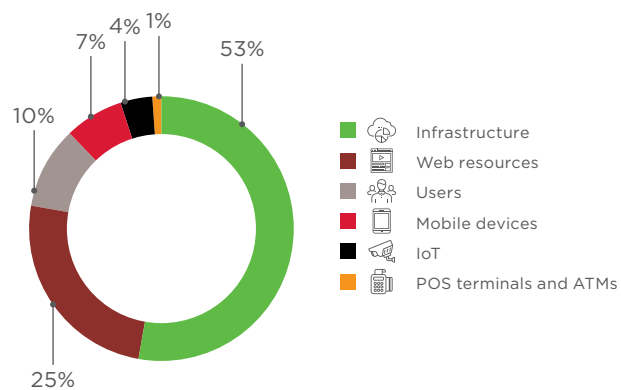


Figure 4. Attack targets

Attacks on infrastructure increased year-over-year from 46 percent (Q4 2017) to 53 percent (Q4 2018). Attacks on web resources grew slightly to 25 percent, while attacks on users and mobile devices declined to 10 percent and 7 percent of the total respectively.

The list of most common attack methods has been stable for the last year. In Q4 2018, the percentage of attacks involving malware dipped insignificantly (55% vs. 56% in Q3). Social engineering fell by 6 percent. Attacks leveraging vulnerabilities in web applications grew by 3 percent (to 20%) and brute-force attacks grew by 4 percent (to 17%). We will take a closer look at each attack method and indicate which targets and industries were most affected.

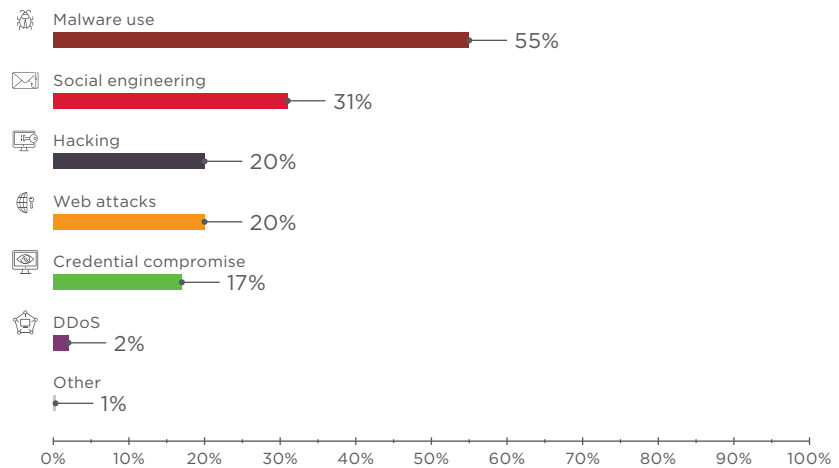


Figure 5. Attack methods

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

		Industry													
		Government	Finance	Industrial companies	Healthcare	Online services	Hospitality and entertainment	IT	Education	Retail	Telecom	Individuals	Cryptocurrency exchanges	Other	Multiple industries
Total		53	23	15	35	2	8	20	13	16	2	73	7	22	40
Target	Infrastructure	35	18	13	23		1	9	8	3	2	25	2	13	23
	Web resources	13	3	2	6	2	5	9	1	12		10	5	7	6
	Users	5			5		1	2	4	1		14		2	
	Mobile devices											22			
	POS terminals and ATMs		2				1								
	IoT				1							2			11
Method	Malware use	29	14	12	15		4	7	5	6		53	1	6	30
	Social engineering	19	12	5	7		1	1	8	1		34	1	5	8
	Credential compromise	11	4	1	13		2	2	2	2		8		7	5
	Hacking	8	10	1	5			6		2	2	4	6	5	18
	Web attacks	11	2	3	4	2	5	5	1	10		8	1	7	6
	DDoS	1						4							2
	Other											2			1
Motive	Financial profit	8	11		7		4	5	6	5	1	46	7	10	19
	Access to information	37	12	14	26	2	3	6	6	10	1	21		8	13
	Hactivism	6			2		1	9	1	1		5		4	7
	Cyberwar	2		1								1			1
Darker colors indicate a higher proportion of attacks in a particular industry															
		0%	10%				20%			30%			40%		100%



Attack number

The number of unique cyberincidents in Q4 2018 grew by 11 percent compared to the previous year (Q4 2017) and by 7 percent compared to the prior quarter (Q3 2018).

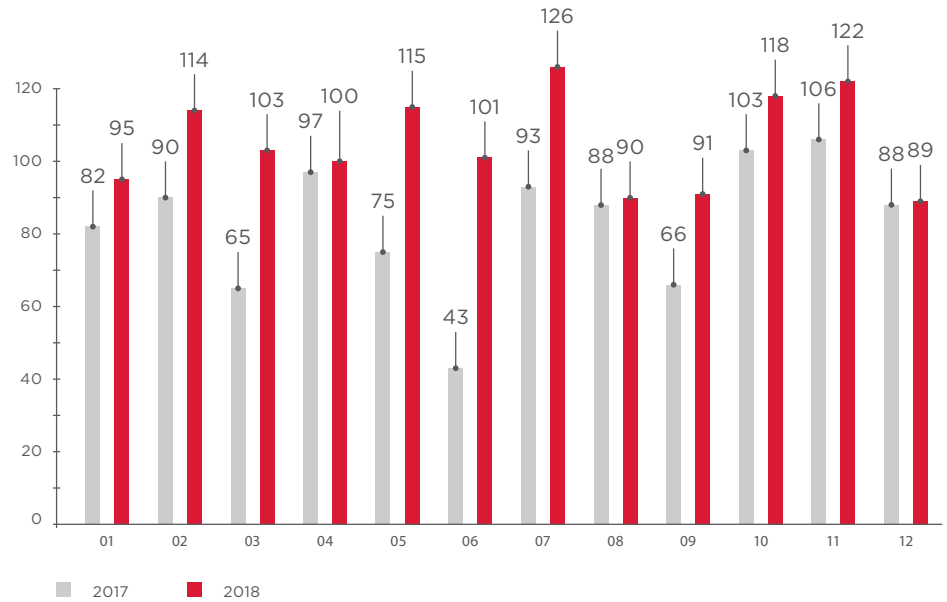


Figure 6. Number of incidents per month in 2017 and 2018 (1 = January, 12 = December)

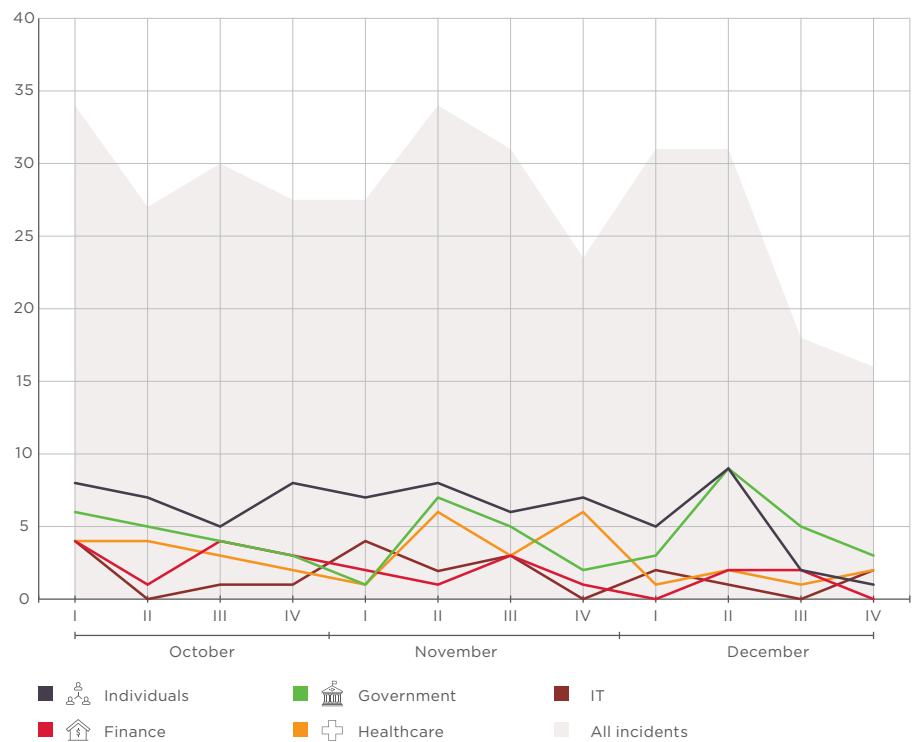


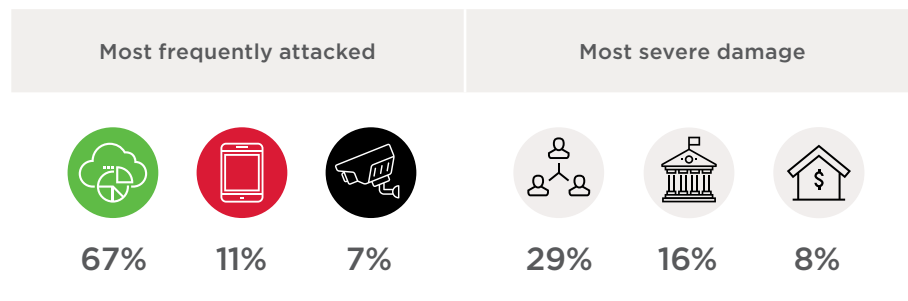
Figure 7. Number of incidents in Q4 2018 (by week)



Attack methods

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

Malware use



Attackers continue to use spyware (29% of cases) and remote administration malware (25%) to collect information from victims' computers and smartphones. The Q3 jump in ransomware infections petered out in Q4, returning to just 9 percent of all infections.

In 39 percent of cases, infection was preceded by compromise of servers and workstations. JungleSec ransomware³ infected computers via Intelligent Platform Management Interface (IPMI) consoles that were left unprotected, such as with default credentials. Malicious email attachments were used in 29 percent of malware attacks. In 16 percent of cases, malware struck during a visit to an infected site.

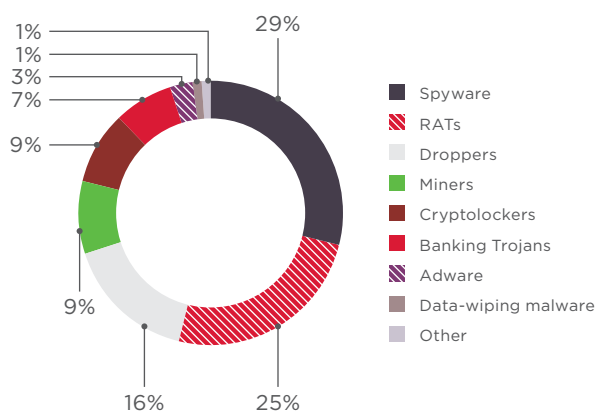


Figure 8. Malware types

Security experts regularly uncover malware in official mobile app stores. In one example, the public learned in November of fake cryptocurrency wallets on Google Play.⁴ But this was not the only case of malware spreading with the help of trusted names. In October, the Python Package Index (PyPI) was found to contain 12 modified libraries with deceptive look-alike names intended to resemble legitimate libraries (such as diango, djago, or dajngo instead of Django).⁵ In 2017, the Slovak National Security Office had already found malicious libraries hosted on the same repository. However, the situation seems unchanged and security checks to prevent uploading of malicious packages were not performed.

³ bleepingcomputer.com/news/security/junglesec-ransomware-infected-victims-through-ipmi-remote-consoles/

⁴ lukasstefanko.com/2018/11/fake-cryptocurrency-wallets-found-on-play-store.html

⁵ zdnet.com/article/twelve-malicious-python-libraries-found-and-removed-from-pypi/

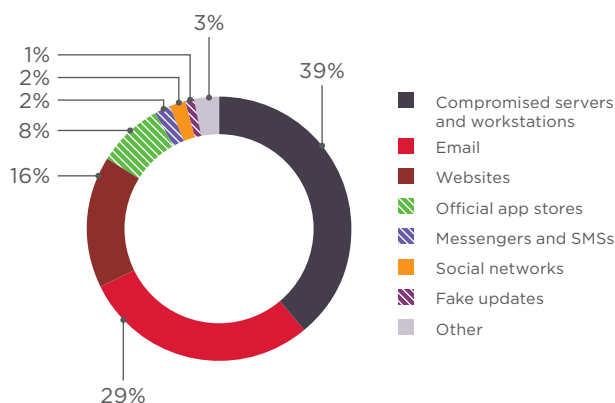
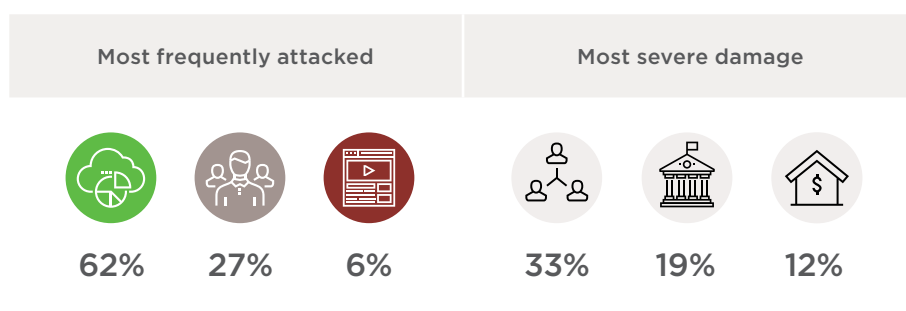


Figure 9. Malware distribution methods

Social engineering



Social engineering featured in nearly one in three attacks in Q4. Criminals routinely operate finely honed phishing schemes against company employees in targeted attacks.

In November, the Positive Technologies Expert Security Center (PT ESC) discovered an email attachment in Publisher format. The payload enabled attackers to capture images from webcams, record audio on command, and when a Skype window was available, run PowerShell scripts, take screenshots, and copy files from media devices. To run the payload, the victim needed to enable a Microsoft Publisher script after opening the document. Victims were enticed to open the document by a blurry image containing an official-looking seal, presumably to inspire trust and urgent need to know by running the script. In reality, the file contained embedded JavaScript code, which decoded a PDF and EXE from Base64 and ran them.

Meanwhile, the victim would see just the decoy document on screen. Treasure Hunter remote administration malware would invisibly install itself on the computer, collecting and sending information about the system as well as receiving commands from a remote server.

Marketing emails often contain buttons that invite the user to visit a website. But before clicking a button, it is important to check the identity of the message sender and the destination of the link. In November, Spotify customers fell victim to a phishing campaign.⁶ Attackers tricked users into visiting a counterfeit site and entering their credentials.

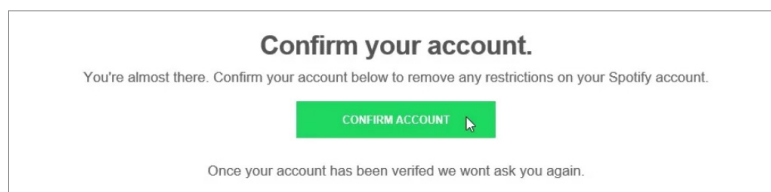


Figure 10. Text of phishing message

⁶ blog.appriver.com/spotify-phishing-campaign-making-rounds

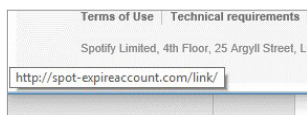


Figure 11. Destination of the message link

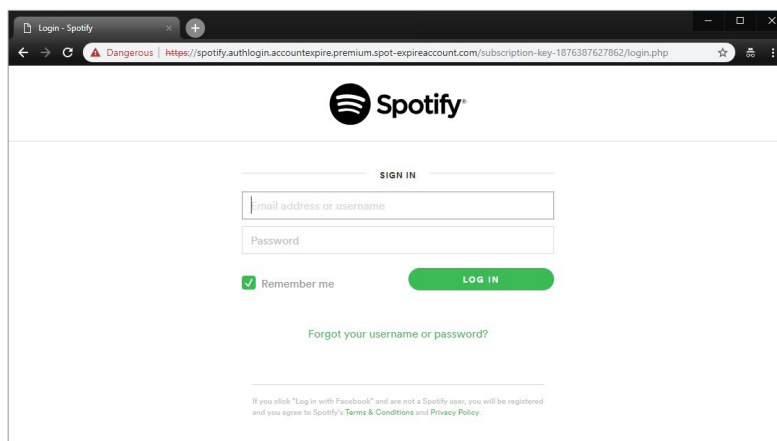
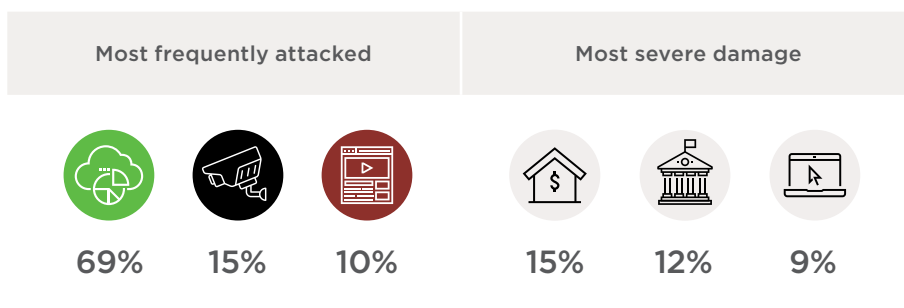
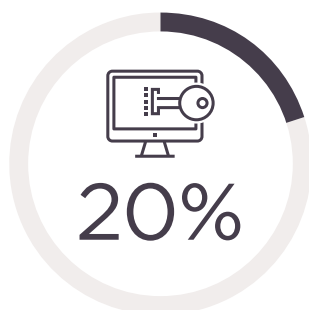


Figure 12. Linked phishing site

Hacking



For the purposes of this report, hacking refers to attacks that take advantage of vulnerabilities in software and services, weaknesses in protection mechanisms, and other shortcomings of targeted systems that do not involve social engineering or malware. This category does not include web attacks, which are counted separately. Hackers have put blockchain platforms in their crosshairs in the last few years. In the first two quarters of the year, we saw so-called 51% attacks, in which criminals obtain control over a majority of the hashrate (CPU power) of a cryptocurrency network, which enables them to double-spend. In one such incident with the Vertcoin cryptocurrency in November,⁷ attackers were able to double-spend coins 15 times to commit over \$100,000 of fraud.

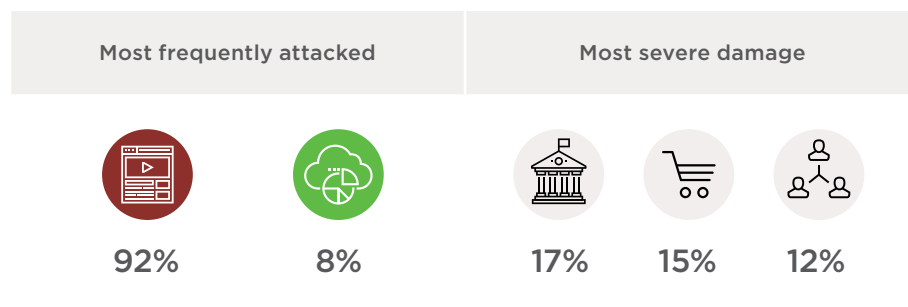
A vulnerability in the ThinkPHP framework, which allowed running arbitrary code on a server, threatened over 45,000 Chinese sites.⁸ A mere day after information about the vulnerability and a proof-of-concept were published, multiple hacker groups started probing sites to exploit the vulnerability.

⁷ medium.com/coinmonks/vertcoin-vtc-is-currently-being-51-attacked-53ab633c08a4

⁸ zdnet.com/article/chinese-websites-have-been-under-attack-for-a-week-via-a-new-php-framework-bug/



Web attacks



Q4 2018 was marked by a large number of cyberattacks involving injection of malicious scripts into the code of vulnerable sites. For instance, the MageCart group (which actually refers to seven different groups with a similar "signature")⁹ looks for vulnerable online stores and uses vulnerabilities in a CMS or plug-ins to inject malicious JavaScript code into payment pages. This was the approach used to steal user-entered information (such as payment card numbers, names, and addresses) from online stores belonging to OppoSuits,¹⁰ Infowars,¹¹ and Umbro Brasil.¹² Instead of taking money from the cards themselves, the criminals tend to sell this information on the darkweb.¹³

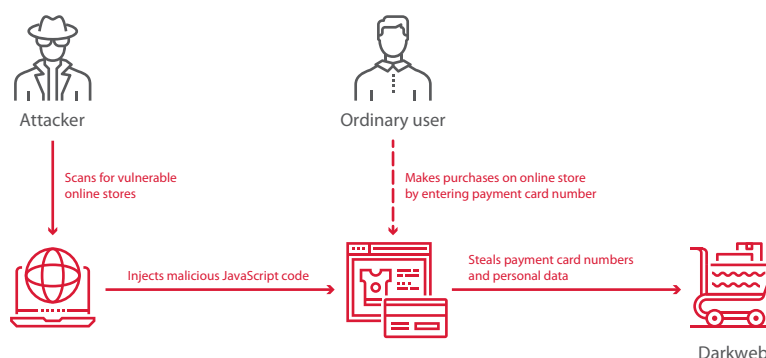


Figure 13. MageCart attack anatomy

In November, ESET reported on the OceanLotus group and its compromise of 21 sites for a watering hole attack.¹⁴ The attackers placed malware on sites ("watering holes") of likely interest to their target victims. These could be sites belonging to partner companies or vendors, public organizations, or even government institutions. Just by getting a victim to visit an infected site, an attacker gains access to information on the victim's computer, emails, and other important information such as account credentials. Among the sites compromised by OceanLotus were the Cambodian Ministries of Foreign Affairs and Defense, as well as a number of Vietnamese news sites.

⁹ riskiq.com/research/inside-magecart/

¹⁰ itwire.com/security/85506-clothing-company-opposuits-hit-by-magecart-attack.html

¹¹ zdnet.com/article/card-skimming-malware-removed-from-infowars-online-store/

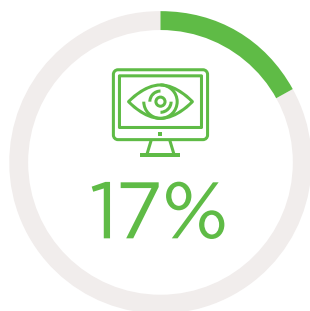
¹² blog.malwarebytes.com/threat-analysis/2018/11/web-skimmers-compete-umbro-brasil-hack/

¹³ ptsecurity.com/upload/corporate/ww-en/analytics/Darkweb-2018-eng.pdf

¹⁴ welivesecurity.com/2018/11/20/oceanlotus-new-watering-hole-attack-southeast-asia/



Credential compromise



Most frequently attacked



58%



21%



17%

Most severe damage



23%



19%



14%

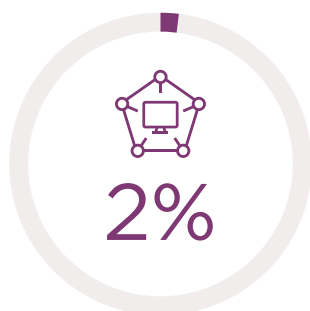
In practice, bruteforcing passwords is often how attackers get their foot in the door on target infrastructure. In one incident investigated by PT ESC in late 2018, an attacker compromised the victim's server by bruteforcing passwords for the RDP protocol and then started reconnaissance of the internal network. The attacker disabled servers by encrypting system files, and then demanded a ransom for decryption. Access to the victim's internal network was the result of three factors: use of dictionary passwords, absence of two-factor authentication, and insufficient protection of resources. The attacker in this particular incident was interested in short-term financial gain. But potential consequences could have included access to sensitive information, attacks on company partners, and other more sophisticated attacks. It was later established that the hacker had performed similar attacks on the network perimeter of approximately 30 companies in different industries. Around half of attacks were successful because the password for the OS administrator was extremely weak (along the lines of 123456, Pass123123, Qwerty12345, or 123qweASD), while RDP ports on computers and servers were open to Internet connections. Such attacks are within the capacity of any threat actor, even very low-skilled ones, making it important to monitor the security of the network perimeter and take an inventory of externally accessible resources.

Botnets can be used for more than just DDoS attacks. In December, Defiant researchers described an unusual botnet consisting of over 20,000 sites.¹⁵ Attackers used WordPress-powered websites for brute-force attacks on the administration panels of targeted sites, in order to perform new attacks from those in turn. Over 5 million such brute-force attempts were recorded in the space of one month.

¹⁵ wordfence.com/blog/2018/12/wordpress-botnet-attacking-wordpress/



DDoS



Most frequently attacked



72%



14%



14%

Most severe damage



57%



14%

The share of DDoS attacks changed little from quarter to quarter. A new DDoS botnet was discovered in October.¹⁶ DemonBot consists of vulnerable Hadoop servers with a misconfigured Yet Another Resource Negotiator (YARN) module. The vulnerability allows adding a new application to a cluster, upon which attackers install malware on servers to perform DDoS attacks (UDP/TCP flooding). Although the vulnerability has been known since 2016,¹⁷ IT specialists frequently underestimate the importance of security and fail to deploy infrastructure with secure configuration settings.

October also saw activity by hackers under the banner of Anonymous, this time targeting over 70 sites belonging to the government of Gabon.¹⁸

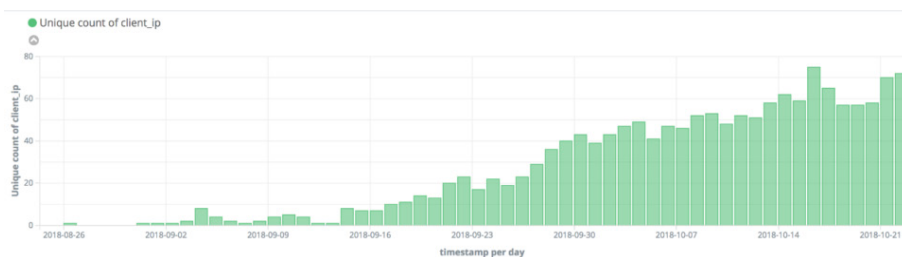


Figure 14. Number of attacked Hadoop servers

¹⁶ blog.radware.com/security/2018/10/new-demonbot-discovered/

¹⁷ archive.hack.lu/2016/Wavestone-Hack.lu-2016-Hadoop-safari-Hunting-for-vulnerabilities-v1.0.pdf

¹⁸ news24.com/Africa/News/gabon-official-websites-hacked-anonymous-group-20181029



Victim categories

In this section, industries of special interest in Q4 2018 will be considered in greater detail.

Government



Damage over
\$50,000

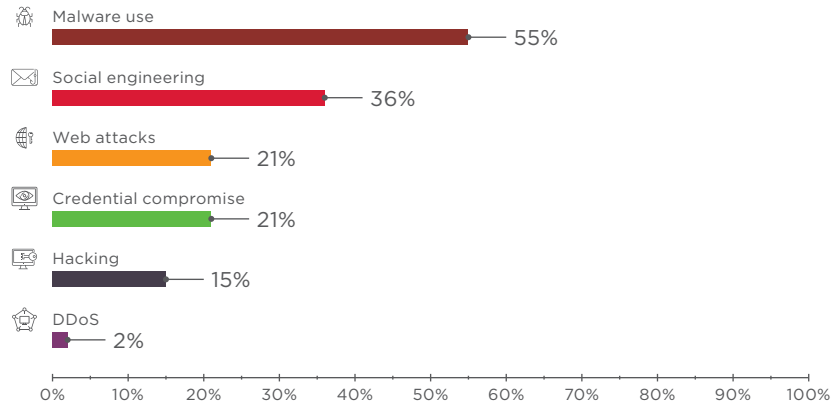


Figure 15. Government: attack methods used in Q4 2018

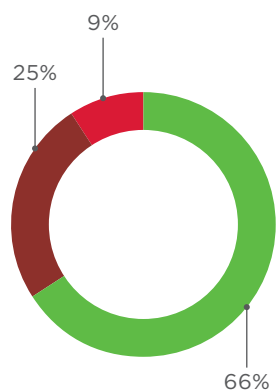
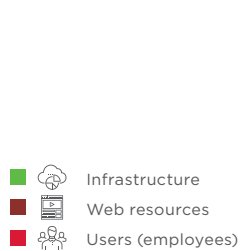


Figure 16. Attack targets

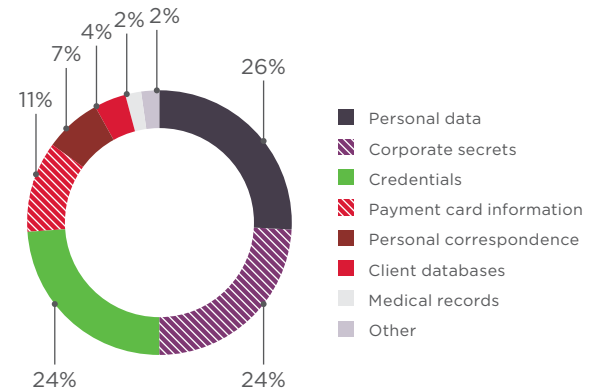


Figure 17. Data stolen

Governments are riding the digital wave and moving payments online. But ease and convenience come at the price of cybercrime-related risks. Click2Gov, responsible for accepting parking, utility, and other municipal payments in the U.S., was subjected to attacks from April 2017 to December 2018.¹⁹ A total of 20 such incidents, resulting in theft of information for at least 111,860 payment cards, occurred. It is thought that the attackers uploaded the SJavaWebManage JSP shell to web servers, using debug mode to obtain access to unencrypted payment card numbers. News of vulnerabilities in this payment service, as well as recommendations for addressing them, were made public in 2017. But judging by how attacks have continued for one and a half years, the organizations using this system have failed to keep up with security developments and take adequate protective measures.

¹⁹ geminiadvisory.io/hacked-click2gov-exposed-payment-data/

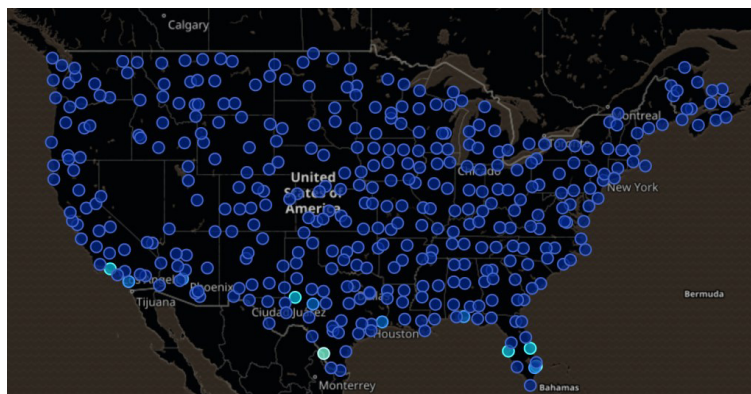


Figure 18. Locations of Click2Gov victims

In Q4 2018, PT ESC recorded activity by two groups, Danti APT and SongXY, against government organizations in Russia and the CIS. A malicious document from the Danti APT group, last active in 2016, surfaced in November. Notably, the functions of the malware had not changed in the last two years: the Trojan collected and sent information about infrastructure (CPU, memory, OS version, username, network information) to a server. Instead of vulnerability CVE-2015-2545,²⁰ this time the group exploited a different Microsoft Office vulnerability, CVE-2017-11882.²¹

Also in November, PT ESC experts identified a malicious document from the SongXY group. When last active in 2017 and early 2018, the group used Microsoft Office documents with macros. Now the group has changed the loader and moved to use the same exploit as Danti APT, CVE-2017-11882. The malware collected information from the infected computer and sent it to attackers.

²⁰ nvd.nist.gov/vuln/detail/CVE-2015-2545

²¹ nvd.nist.gov/vuln/detail/CVE-2017-11882



Victims over
3 million

Healthcare

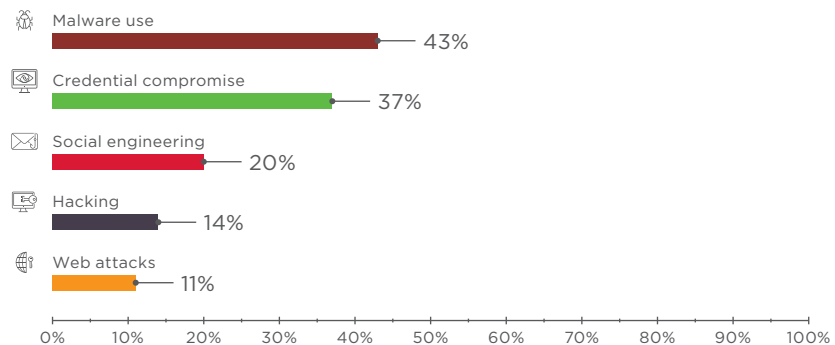


Figure 19. Healthcare: attack methods used in Q4 2018

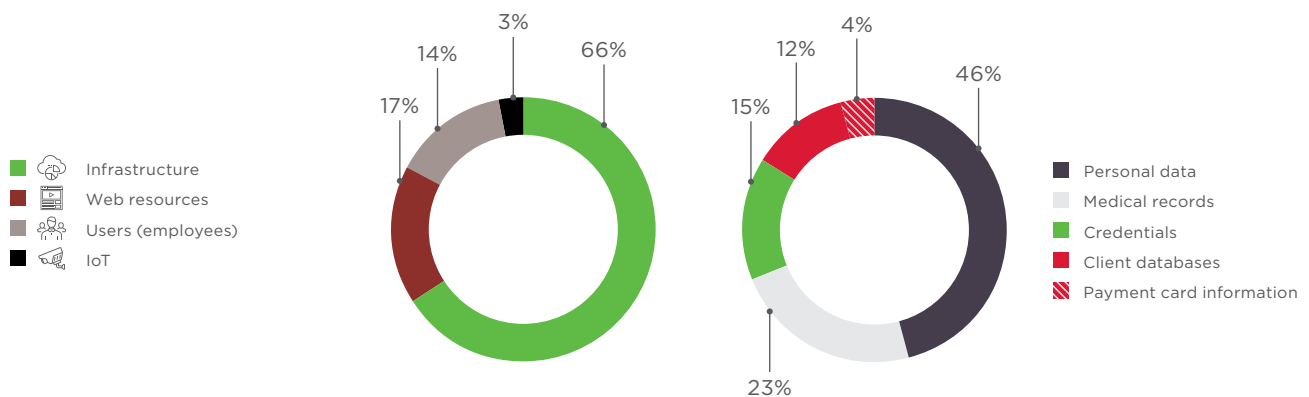


Figure 20. Attack targets

Figure 21. Data stolen

Malicious scripts on vulnerable sites have become a trend, and healthcare is no exception. One payment portal for medical services was attacked, likely resulting in attacker access to payment card data for 5,850 people who used the site between October 25 and November 8.²² Most likely, this information is already being sold on the darkweb.

Otherwise, attacks on healthcare organizations in Q4 offered little of interest. Cybercriminals continued compromising employee computers, by bruteforcing accounts and sending malicious email attachments, in order to access medical information and patient data.

²² bnd.com/news/local/article223273720.html



Damage over \$20 million
Victims over 1 million

Finance

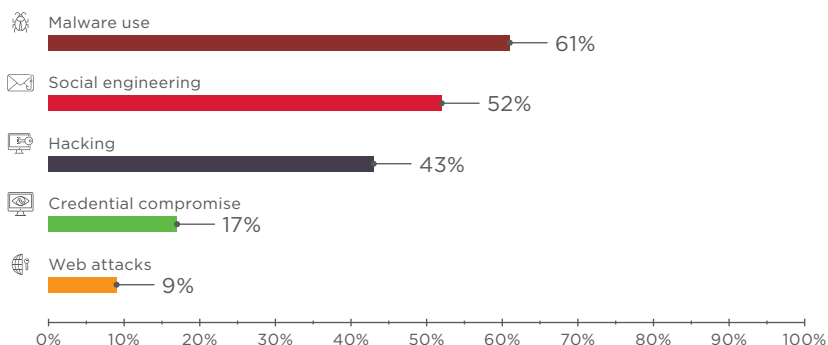


Figure 22. Finance: attack methods used in Q4 2018

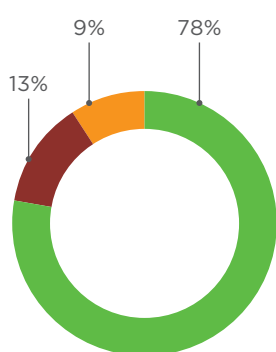


Figure 23. Attack targets

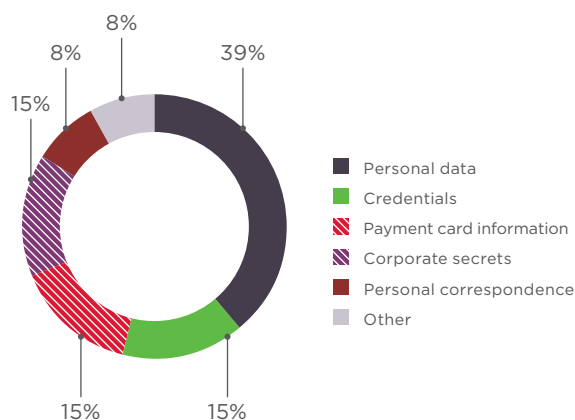


Figure 24. Data stolen

In Q4, PT ESC detected activity by three groups against financial institutions: Silence, Cobalt, and a new group targeting Russian banks. Silence performed two attacks in October and another in late December. In October, the group sent a malicious CHM file packed in an archive with a very low antivirus detection rate. The final loader in these attacks, "silence," collects information about the system (systeminfo and ipconfig) and sends it to a remote server, together with the hard disk serial number for uniqueness. In December, the group sent an RTF file with an OLE-embedded CHM file. The code of the final silence loader had been substantially revised.

Cobalt performed 11 attacks during Q4, some of which targeted banks outside the CIS. Two phishing attacks sought to imitate hacked banks Unistream and Kassa Nova, both in Kazakhstan. The other attacks were targeted at Russian banks. The group sent phishing messages on the same day that zero-day vulnerability CVE-2018-15982²³ was published (the group was similarly quick in 2017 when CVE-2017-11882 became public). But the criminals made a mistake: they did not place the payload in an archive and the shell commands (taken from an article about the vulnerability) to unpack the archive failed.

In addition, in October the experts at PT ESC discovered a new group attacking the finance sector. Masquerading as FinCERT of the Russian Central Bank, attackers sent malicious documents containing macros for downloading the Metasploit stager. This stager determined the system version (x86 or x64) and, based on the version, accessed one of two hard-coded URLs. Another payload, Meterpreter, was downloaded from these URLs into system memory, providing the attackers with remote access to the infected computer.

²³ cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15982



The secure TLS protocol was used for downloading Meterpreter, as well as for communicating with the command-and-control server and downloading additional modules.

In December, phishing messages were sent from the compromised account of an employee of investment company Alfa Capital. Analysis of the attachment uncovered a JavaScript script used by the Treasure Hunters group, but to which functionality for running the Metasploit stager had been added.

Despite the similarity of these two attacks with those performed by the Treasure Hunters group previously, analysis of traffic, as well as use of the Metasploit stager and Meterpreter, suggests the existence of a new cybercriminal group that is targeting financial institutions.

IT



Victims over
1 million

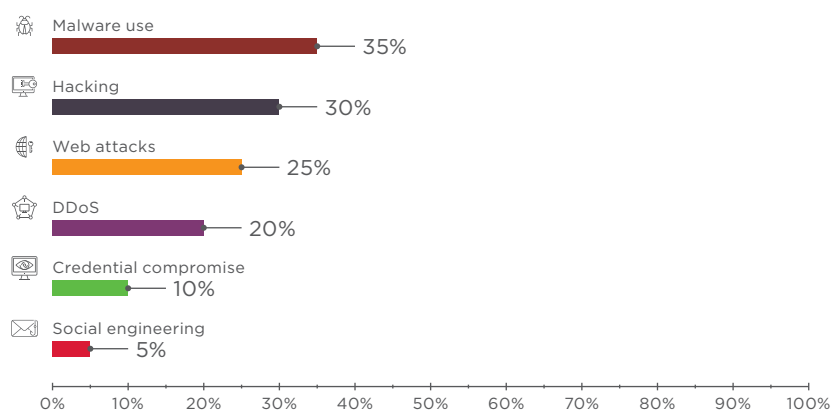


Figure 25. IT: attack methods used in Q4 2018

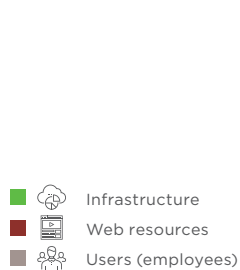


Figure 26. Attack targets

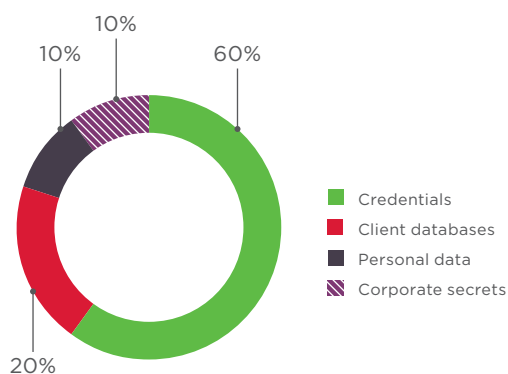


Figure 27. Data stolen

IT companies develop software, maintain infrastructure for companies, and provide cloud data storage services, making them an alluring target for cybercriminals. Attacks are tending to include a larger number of stages, and hacking related parties (such as the developer of software used by the target) may be one of these stages. What's more, cloud providers are ripe for ransom: they promise their clients secure storage of large amounts of data with no downtime or interruption, making them desperate to avoid loss of business. In late December, cloud hosting provider Dataresolution.net fell victim to Ryuk ransomware.²⁴ It is thought that the Lazarus group has been using this malware since late August 2018 in targeted attacks around the world.

²⁴ krebsonsecurity.com/2019/01/cloud-hosting-provider-dataresolution-net-battling-christmas-eve-ransomware-attack/



Damage over \$8 million
Victims over 30 million

Individuals

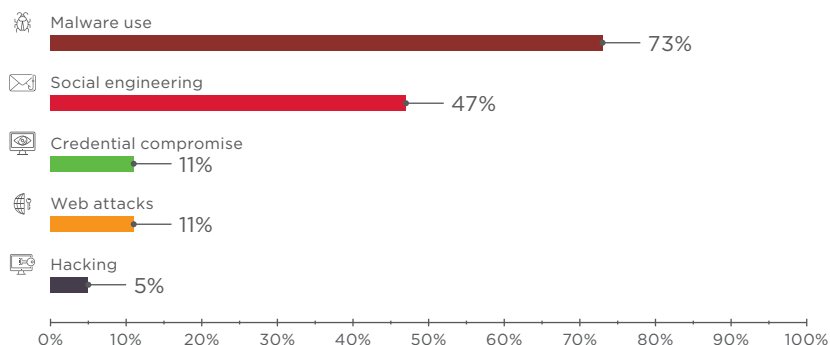


Figure 28. Individuals: attack methods used in Q4 2018

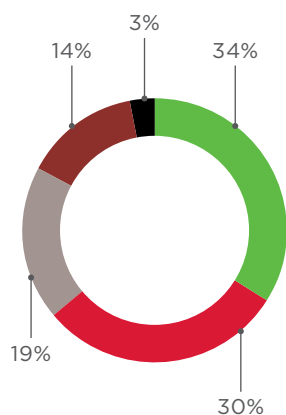


Figure 29. Attack targets

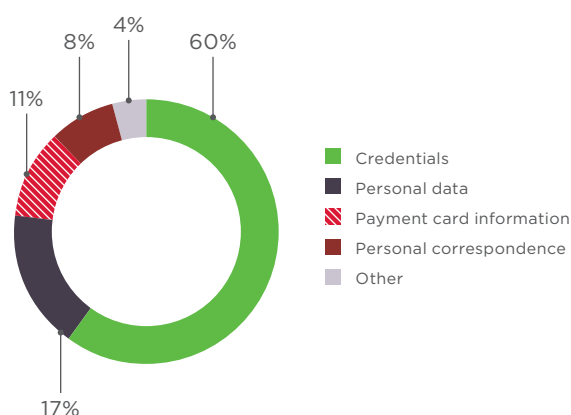


Figure 30. Data stolen

One third of attacks on individuals were intended for the purpose of data theft. Attacker interest was focused on credentials, which were the target in 60 percent of cases. In October, the Israel National Cyber Directorate described a new method used to hack WhatsApp accounts by means of voicemail.²⁵ An attacker adds the victim's phone number as a new account, after which a verification code is sent by WhatsApp via SMS. But if the user does not see these messages (such as when sleeping), after several failed attempts WhatsApp offers to provide the code by voice. If the victim is sleeping or away from the phone, the code is left on the victim's voicemail. And if the password for voicemail has not been changed, the attacker can enter the default password and hear the voice message, providing the code necessary to use the victim's WhatsApp account. These accounts can then be used for social engineering, such as to request money from the victim's friends or send links to phishing sites.

Malicious attachments target both corporate accounts and those of ordinary users. In November, discovery was made of a spam campaign targeted at macOS users of the Exodus cryptowallet: attackers distributed spyware in the guise of a wallet update.²⁶

25 scribd.com/document/390119600/Whatsapp-Israel-National-Cyber-Directorate

26 labsblog.f-secure.com/2018/11/02/spam-campaign-targets-exodus-mac-users/



What companies can do to stay safe

Use proven security solutions:

- Systems for centralized administration of updates and patches.
- Antivirus software with a sandbox for dynamically scanning files and the ability to detect and block threats such as malicious email attachments before they are opened by employees. Ideally, antivirus software should simultaneously support solutions from multiple vendors and have the ability to detect signs of hidden or obfuscated malware, as well as block malicious activity across diverse data streams: email, web traffic, network traffic, file storage, and web portals. It is crucial that antivirus software, besides scanning files in real time, automatically perform retrospective analysis of previously scanned files: newer detection signatures may reveal threats in files that had passed scanning in the past.
- Security information and event management (SIEM) solutions, for timely detection and rapid response to incidents. These capabilities allow detecting malicious activity, infrastructure hack attacks, and attacker presence in time to neutralize the threat.
- Automated tools for analyzing security and identifying software vulnerabilities.
- A web application firewall (WAF) as a preventive measure for protecting web resources.
- Systems for deep analysis of network traffic, to detect advanced persistent threats in real time and from saved traffic. This provides visibility into previously unnoticed hacks and indicates when a network attack is underway, such as use of malicious tools, exploitation of vulnerabilities, and attacks on domain controllers. By reducing the time that attackers are able to remain hidden, companies can minimize the risk of data loss, ensure uninterrupted operation, and reduce financial losses.
- Specialized anti-DDoS services.

Protect your data:

- Encrypt all sensitive information. Do not store sensitive information where it can be publicly accessed.
- Perform regular backups and keep them on dedicated servers that are isolated from the network segments used for day-to-day operations.
- Minimize the privileges of users and services as much as possible.
- 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.
- Make sure that insecure resources do not appear on the network perimeter. Regularly take an inventory of Internet-accessible resources, check their security, and remediate any vulnerabilities found. It is a good idea to monitor the news for any new vulnerabilities: this gives a head start in identifying affected resources and applying necessary patches.
- Filter traffic to minimize the number of network service interfaces accessible to an external attacker. Pay special attention to interfaces for remote management of servers and network equipment.
- Regularly perform penetration testing to identify new vectors for attacking internal infrastructure and evaluate the effectiveness of current measures.
- Regularly audit the security of web applications, including source-code analysis, to identify and eliminate vulnerabilities that put application systems and clients at risk of attack.
- Keep an eye on the number of requests per second received by resources. Configure servers and network devices to withstand typical attack scenarios (such as TCP/UDP flooding or high numbers of database requests).

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 measures for companies given above, 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:

- Use complex passwords consisting of at least eight hard-to-guess letters, numbers, and special characters. Consider using a password manager to create and securely store passwords.
- Set a different password for each site, email address, or other account that you use.
- Change all passwords at least once every six months, or even better, every two to three months.

Be vigilant:

- Scan all email attachments with antivirus software.
- Be careful when visiting sites with invalid certificates. Remember that information entered on these sites could be intercepted by attackers.
- 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

ptsecurity.com
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.

© 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.