POSITIVE TECHNOLOGIES

Cybersecurity threatscape

Q3 2018

Contents

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

Positive Technologies keeps monitoring the most important IT security threats. Although Q3 is considered vacation time, hackers do not take a break and keep inventing new cyberattacks.

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

- The number of unique cyberincidents exceeded the equivalent year-ago period (Q3 2017) by 24 percent.
- The number of attacks aimed at stealing information also continued to grow, almost reaching 50 percent of the total number of cybercrimes. Personal data, credentials, and credit card information remain the three favorite targets of attackers.
- The use of social engineering drastically increased over Q3. In vast majority of cases, hackers attacked individuals, reaching them via phone calls, SMSs, email, and even through ordinary post.
- Cases of malware infection also became quite widespread. Unlike cryptolockers that became less popular in Q3, the number of cases involving malware infection increased up to 20 percent (12% in Q1 and 9% in Q2). This is probably linked to the GandCrab operators' aggressive policy: discovered in early 2018, this ransomware evolved to the fifth version by September. Infection by miners keeps decreasing, which is apparently related to the drop in exchange rate of several cryptocurrencies.
- Attacks against financial institutions became more popular compared to Q2. This is mostly linked to a surge in phishing attacks performed by Cobalt group. In total, financial institutions lost $18 million to attacks in Q3 2018.

Q4 will be a time to take stock. We predict the growing number of phishing attacks against employees dealing with annual accounts and budget planning. These attacks will likely target government and financial institutions. As we approach the New Year, people will buy a lot of stuff online. We expect more cases of malware infection via websites and more thefts of credit card information. Despite an increasing number of attacks against cryptocurrency exchanges in Q3, we expect that they will become less widespread in Q4 as bitcoins are falling in price.

Statistics

The most common motive behind cyberattacks in Q3 2018 was data theft. Cases of data theft grew by 5 percent as compared to the previous quarter and by 20 percent as compared to Q3 2017; however, hackers were less driven by profit (only 33% compared to 53% at the beginning of 2018). Stealing money in cyberspace is becoming increasingly difficult; it is much easier to steal commercial secrets, private data, personal correspondence, photographs, or video recordings and demand enormous ransom for non-disclosure of information, or simply sell these data on the dark web.

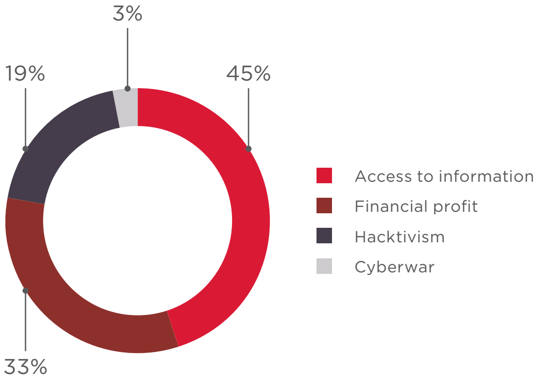


Figure 1. Attackers' motives

Personal data, credentials, and credit card information continue to tempt criminals, accounting for more than a half of all the compromised information. A lot of incidents involving personal data theft can be explained by poor digital literacy of victims. People very often provide personal data for a small compensation in online services or publish them in social media, without understanding how precious this information could be for attackers.

Every fifth data theft involved stealing account credentials. Oftentimes, attackers steal passwords used for online services and web applications in order to gain access to other systems where a more precious information is processed, for example medical data. Credential stuffing attacks are much effective than simple bruteforcing, as people often use the same credentials for accessing various systems.

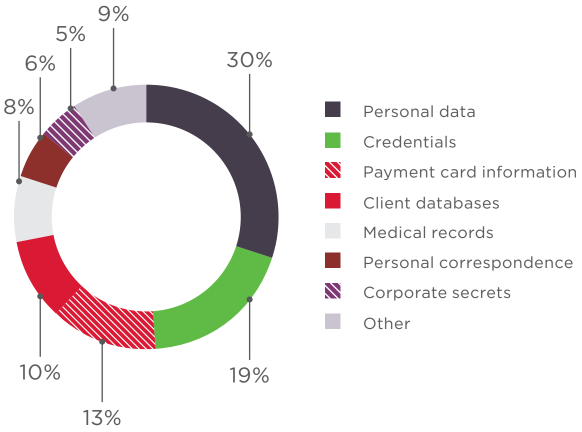


Figure 2. Types of stolen data

As in the previous quarter, targeted attacks prevailed over mass attacks in Q3 accounting for 55 percent of the total number of incidents. Targeted attacks were mainly aimed at government institutions. We saw a growing number of attacks against financial institutions (9% compared to 6% in Q2). Medical and education institutions also remained a popular hacking target. Every fifth attack was aimed at individuals. Later in this report, we will more closely consider these categories of attacks. Large-scale cyberattacks affecting more than one industry (most often, malware outbreaks) have been placed in the "Multiple industries" category.

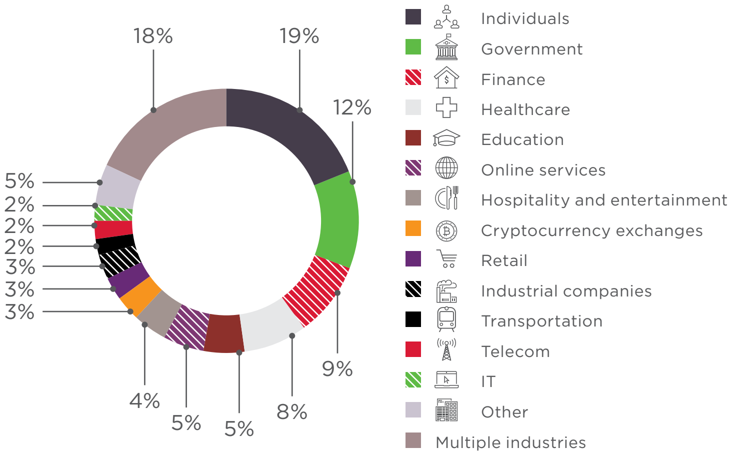


Figure 3. Victim categories

The percentage did not significantly change in comparison with Q2. However, it is worth mentioning a small decrease in the number of attacks compromising websites and an increase in attacks against users.

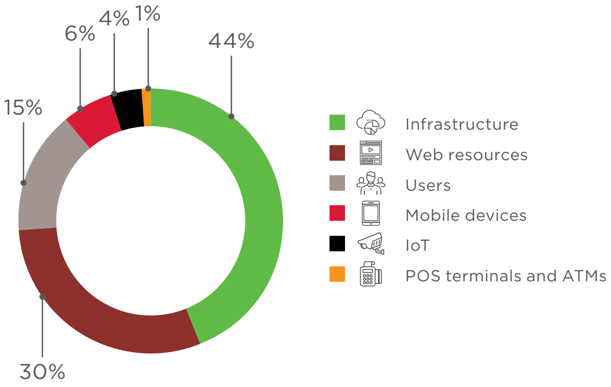


Figure 4. Attack targets

Q3 2018 saw a growing number of social engineering and malware attacks. Quite often attackers used these two methods simultaneously. Incidents involving hacking (exploitation of vulnerabilities without using social engineering and malicious software) increased as compared to Q2, reaching 23 percent. In 3 percent of cases attacks were conducted through abusing legitimate software. In July, PT ESC experts investigated cases in which attackers used publicly available utilities, such as PortScan, GsecDump, and Mimikatz in addition to their proper tools.

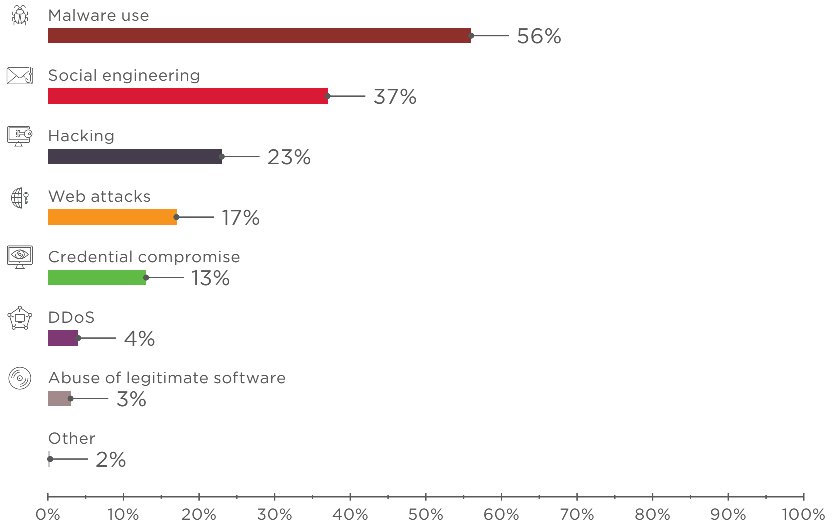


Figure 5. Attack methods

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	Transportation	Cryptocurrency exchanges	Other	Multiple industries
	Total	36	29	9	24	16	14	5	17	8	7	58	6	9	14	55
Target	Infrastructure	24	21	6	15	1	5	2	9	1	3	12	3	2	6	25
	Web resources	10		2	3	14	6	3	6	6	4	12	2	6	5	12
	Users	2	4		6	1	1		2	1		20		1	2	6
	Mobile devices		1									13	1		1	2
	POS terminals and ATMs		2				2									
	IoT		1	1								1				10
Method	Malware use	21	21	5	8	6	5		3	3	2	39	4	1	5	49
	Social engineering	13	15	2	11	1	2		7	1		35		2	7	19
	Credential compromise	4	1		11	1		1	5	1	1	7	1		2	5
	Hacking	9	10	3	3	6	5	1	3	1	1	4		6	5	15
	Web attacks	7	1	3	2	7	3	2	2	4	5	6	2	1	1	6
	Abuse of legitimate software	2		1				1			1	1				3
	DDoS	3	1	1				2	3		1					
	Other	1					1			1		2			1	1
Motive	Financial profit	4	23	3	6		4		2			27	1	7	6	20
	Access to information	16	4	3	16	12	10	3	8	7	6	23	3	1	6	19
	Hacktivism	11	2	2	2	4		2	7	1	1	6	2	1	2	16
	Cyberwar	5		1								2				

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

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

Attack number

In July, we observed the highest number of attacks since the beginning of 2018. Over 40 percent of all the unique attacks registered in Q3 were performed in July. This can be explained by the FIFA World Cup held in Russia from June 14 to July 15. During this period, our experts counteracted about 38,000 attempts to disrupt the Transport Directorate services.

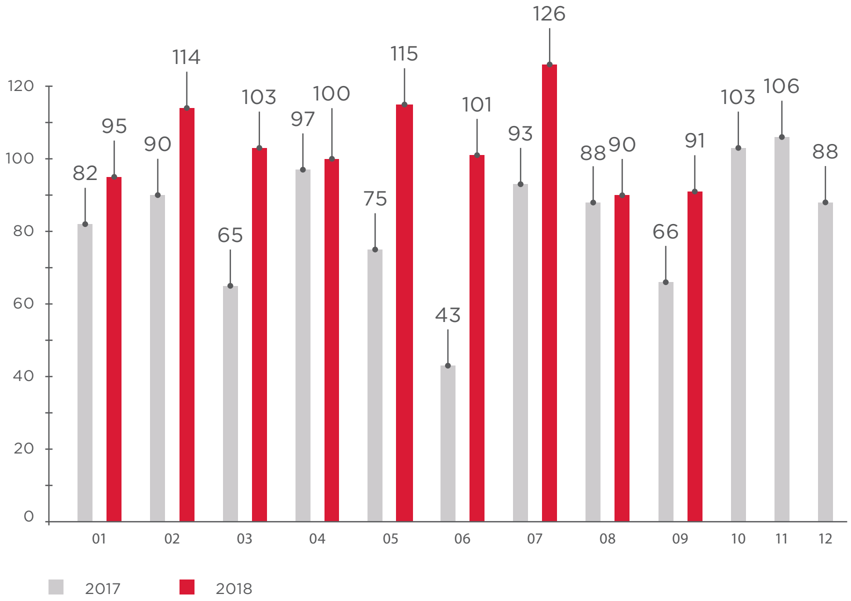


Figure 6. Number of incidents per month in 2017 and 2018 (1 = January, 12 = December)

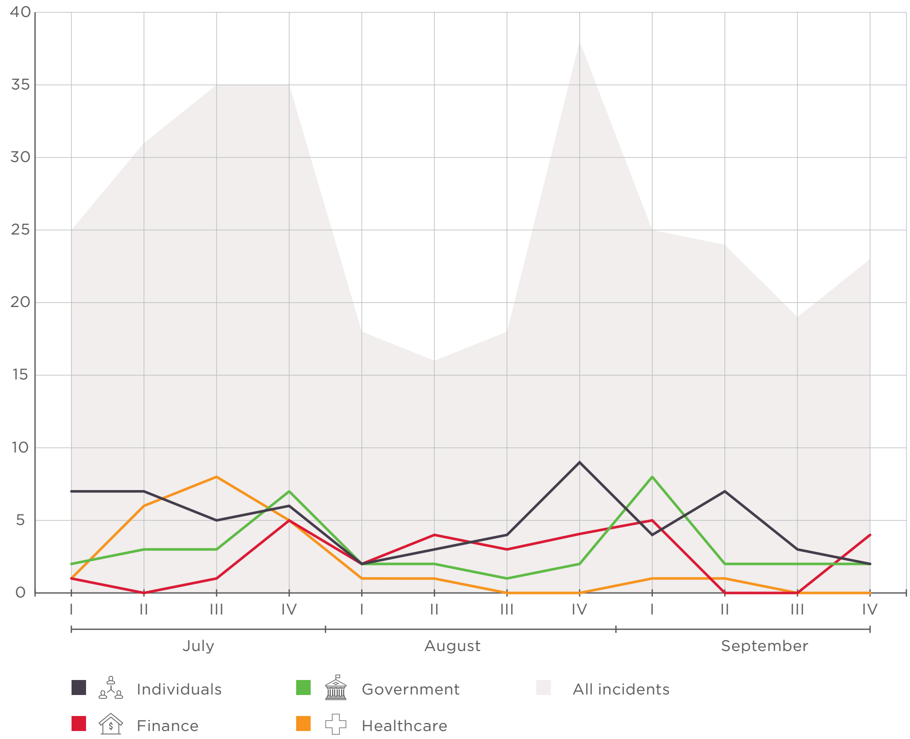
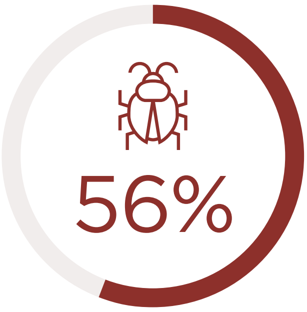


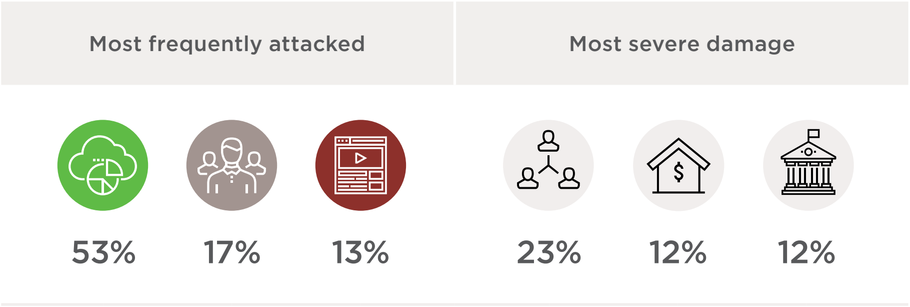
Figure 7. Number of incidents in Q3 2018 (by week)

Attack methods

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

Malware use





Malware use remained the most widespread method of attacks in Q3. The number of incidents involving malware increased up to 56 percent in Q3 as opposed to 49 percent in Q2. Infections by cryptolockers also increased from 9 to 20 percent, outrunning spyware attacks. Ransomware attacks hit government and education institutions, medical centers, industrial companies, and individuals. Thus, the GandCrab ransomware discovered in early 2018 evolved to the fifth version by September. Illicit cryptocurrency mining, on the contrary, decreased, with only 8 percent of cases in Q3, compared to 15 and 23 percent in Q2 and Q1, respectively. It is quite difficult to discover a hidden miner, whereas illicit file encryption is normally detected on the first day of the incident. Users are simply not aware of helping attackers earn money by illicit cryptocurrency mining.

The decreasing number of cases involving illicit cryptocurrency mining can be explained by the fact that attackers themselves are losing interest in this business. Cryptocurrency mining is becoming more and more difficult (due to the increase in the hashrate). In addition, the exchange rate of several cryptocurrencies has been falling since the early 2018. All these reasons make illicit mining unprofitable. At the same time, a first-ever prison sentence in cryptojacking case was issued in July 2018.[1] A Japanese man was sentenced for a year in prison for illicit cryptocurrency mining despite making only $45.

Cases involving infection via official app stores grew from 4 percent in Q2 to 9 percent in Q3 2018. In August, Doctor Web experts detected[2] over 100 fraudulent Android applications on Google Play. These applications subscribe users to paid services and spread advertisement. In late September, ESET found[3] a banking Trojan, an even more dangerous malware. The banker was introduced into QRecorder—an application used to record phone calls—and allowed attackers to steal victims' credentials and credit card information. By using this data, hackers stole over €78,000 from the victims' accounts.

[1] zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive/
[2] news.drweb.com/show/?i=12797&lng=en
[3] lukasstefanko.com/2018/09/banking-trojan-found-on-google-play-stole-10000-euros-from-victims.html

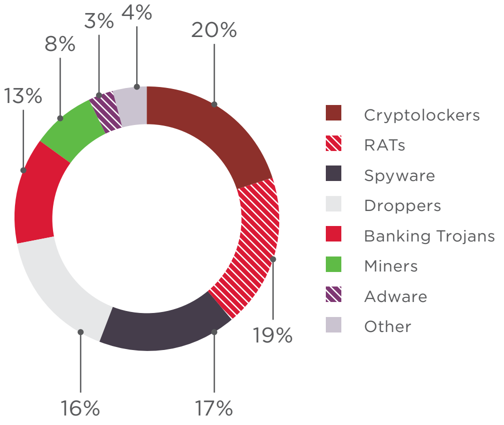


Figure 8. Malware types

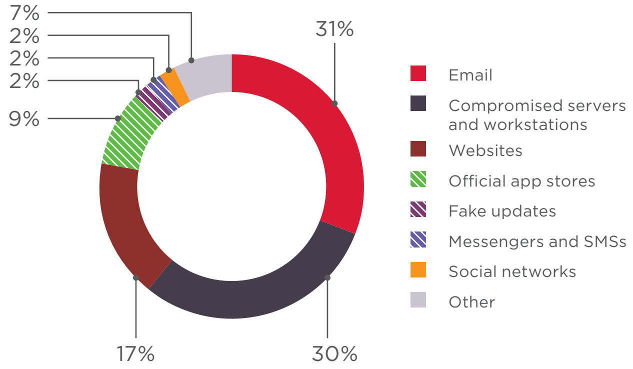
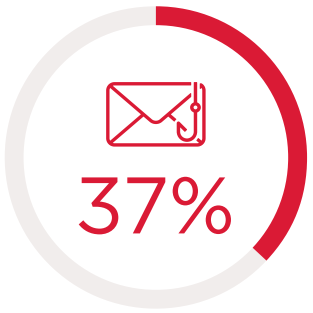
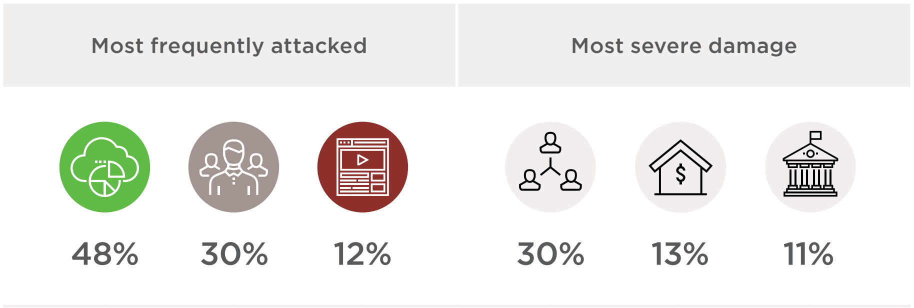


Figure 9. Malware distribution methods

In 31 percent of cases malware was spread by email. This is the easiest and therefore the most popular method of delivering malware to a victim's computer. In September, PT ESC experts discovered a new surge in continuous APT attacks. By using the CMstar downloader, hackers exploited the vulnerability CVE-2017-11882.

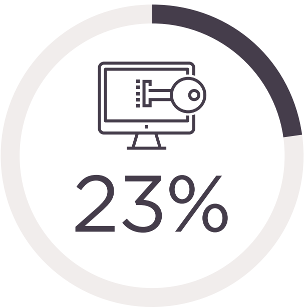
Social engineering





At a time of permanent cyberwar between criminals and information security experts, hackers aspire to not only upgrade their technical skills, but also get a deeper knowledge of human psychology. Q3 2018 saw a significant increase in cases of deceiving people in order to gain profit. Thus, a 20-year-old U.S. student performed numerous SIM hijacking attacks. The student convinced mobile providers of having lost his mobile phone and thus got hold of the SIM cards belonging to the people he chose as victims. He then got access to various services, including cryptocurrency wallets. The criminal hijacked more than 40 phone numbers and stole several million U.S. dollars in cryptocurrency.

Hacking



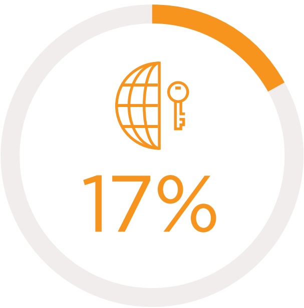
Most frequently attacked			Most severe damage		
49%	39%	11%	14%	13%	8%

To conduct attacks, hackers use business logic errors in applications, flaws in security mechanisms, and known vulnerabilities in non-updated software. Attackers use the found vulnerabilities to get profit, a process we call hacking.

IoT vulnerabilities allow attackers to create botnets in order to conduct powerful DDoS attacks. Routers remain a popular hacking target. eSentire Threat Intelligence experts detected[4] an attempt to exploit the vulnerability CVE-2018-10562 in Dasan and D-Link devices. Recently, attackers started using vulnerable routers as a point of entry to mine cryptocurrency in users' browsers. For this end, in Q3 they exploited[5] a zero-day vulnerability in hundreds of thousands of MikroTik devices. The manufacturer released a patch the next day after the vulnerability was detected; however, a lot of router owners still have not updated their firmware.

Errors in the software code can be extremely detrimental. Cryptocurrency platforms are especially attractive for attackers, as they have numerous logic errors, for example in transaction mechanisms. In July, Livecoin crypto exchange lost more than $1.8 million because of a Monero code vulnerability. In September, hackers exploited the vulnerability CVE-2018-17144 in a Bitcoin protocol. The vulnerability was found in a little-known pigeoncoin cryptocurrency that was not timely patched by its developers. The hackers made off with $15,000 in cryptocurrency.

Web attacks



Most frequently attacked			Most severe damage		
73%	15%	12%	13%	13%	12%

Attacks against web applications not only allow hackers to gain control over the apps and penetrate a company's internal network, but can also be used for political purposes. Websites remain a favorite target of hacktivists, allowing to quickly communicate ideas to millions of people. In July, hackers hit the website of the Taiwan's Democratic Progressive Party leaving political messages on the compromised pages.[6]

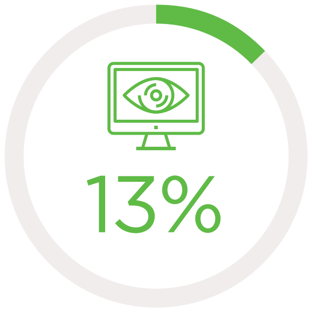
Hackers usually exploit vulnerabilities in applications to use them as a platform for spreading malicious software. In July, hackers replaced[7] the links on the VSDC Video Editor website. After following the modified links, a spyware was installed into victims' computers

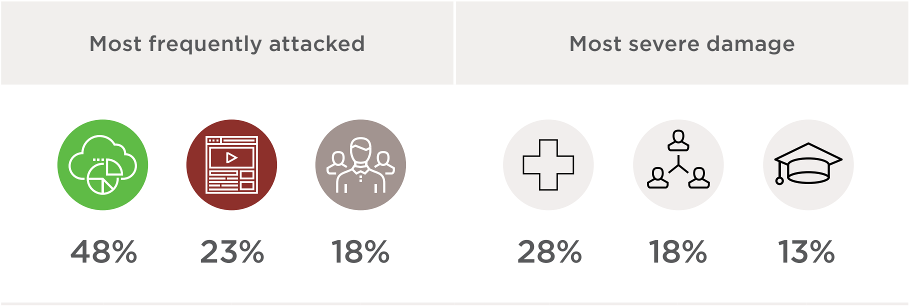
[4] esentire.com/news-and-events/security-advisories/increase-in-attacks-on-gpon-routers/
[5] trustwave.com/en-us/resources/blogs/spiderlabs-blog/mass-mikrotik-router-infection-first-we-cryptojack-brazil-then-we-take-the-world/
[6] taiwannews.com.tw/en/news/3473203
[7] videosoftdev.com/news/attacks-successfully-stopped

collecting data and sending them to the hacker's server. People in more than 30 countries suffered from the incident.

Web application code errors may lead to major data leaks due to insufficient user authorization. An error[8] on the website of Telefónica, a telecommunication provider, led to the disclosure of personal and financial information of the Movistar TV customers. The company faces a fine of 2–4 percent of the annual turnover for the GDPR violation. A similar fine threatens Facebook for compromising tens of millions of user accounts because of a coding error.[9]

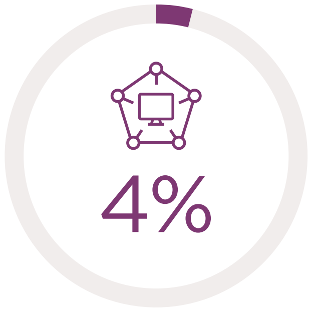
Credential compromise

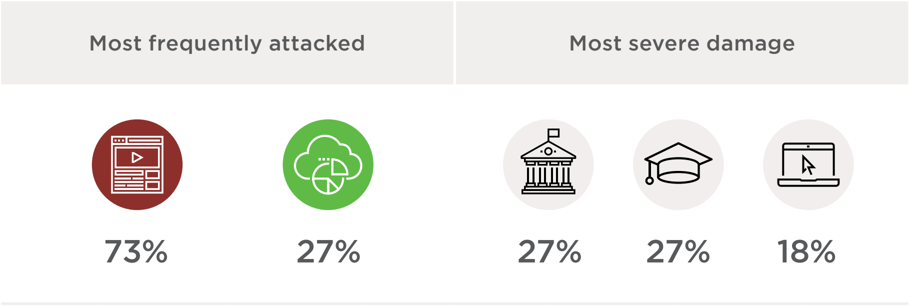




In Q3 2018, we observed a small decrease in the number of attacks aimed at bruteforcing credentials. In early July, weak passwords and the absence of two-factor authentication allowed attackers to steal personal data of 21 million Timehop users.[10] Users are well aware of the requirements for strong passwords. Unfortunately, even people working in the IT industry can fall victim to credentials bruteforcing. Thus, hackers gained access to a developer's npm account, which allowed them to inject malware directly into the JavaScript library code.[11] In September, the developers of AdGuard, a famous ad blocking software, reset passwords to all user accounts because of a bruteforce attack.[12]

DDoS





The beginning of the school year was marked by a surge in DDoS attacks against education institutions. Thus, the University of Edinburgh website was hit on September 12 and was unavailable for more than 24 hours.[13]

It is no secret that unscrupulous entrepreneurs hire hackers to disrupt competitors' infrastructure or to disable their websites. In July, two major game developers, Blizzard Entertainment and Ubisoft, were hit within days of each other with DDoS attacks. The attacks were probably initiated by competitors or disgruntled gamers, unhappy with the companies' policy.

[8] facua.org/es/noticia.php?Id=13025
[9] newsroom.fb.com/news/2018/09/security-update/
[10] timehop.com/security
[11] bleepingcomputer.com/news/security/compromised-javascript-package-caught-stealing-npm-credentials/
[12] adguard.com/en/blog/adguard-security-notice/
[13] edinburghnews.scotsman.com/our-region/edinburgh/edinburgh-university-hit-by-crippling-cyber-attack-1-4798612

Another popular reason for DDoS attacks is hacktivism. Thus, politically motivated hacktivists disabled the website of the Swedish Social Democratic Party,[14] shut down for almost 24 hours the website of Bryan Caforio, a Californian candidate for U.S. Congress,[15] hit a Dutch government website,[16] and attempted cyberattack on the website of South Africa Department of Labor.[17]

Victim categories

Here we will analyze the most important attacks against particular sectors in Q3 2018.

Government

Damage over
$35,000

Victims over
272,000

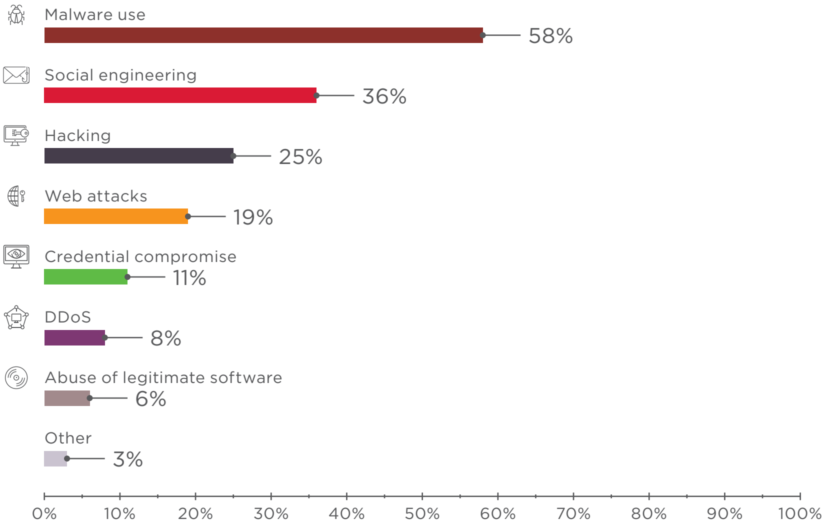
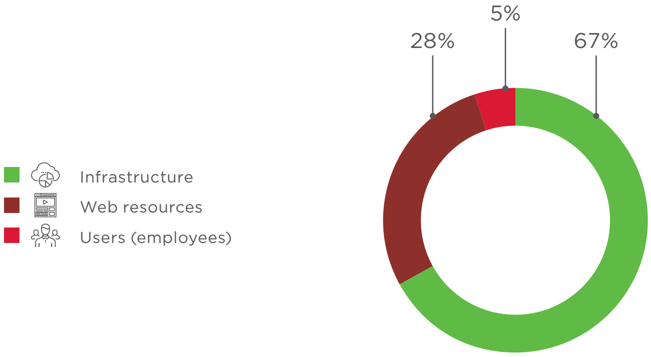


Figure 10. Government: attack methods used in Q3 2018



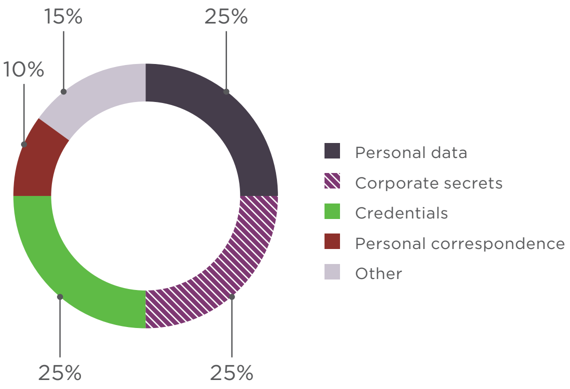
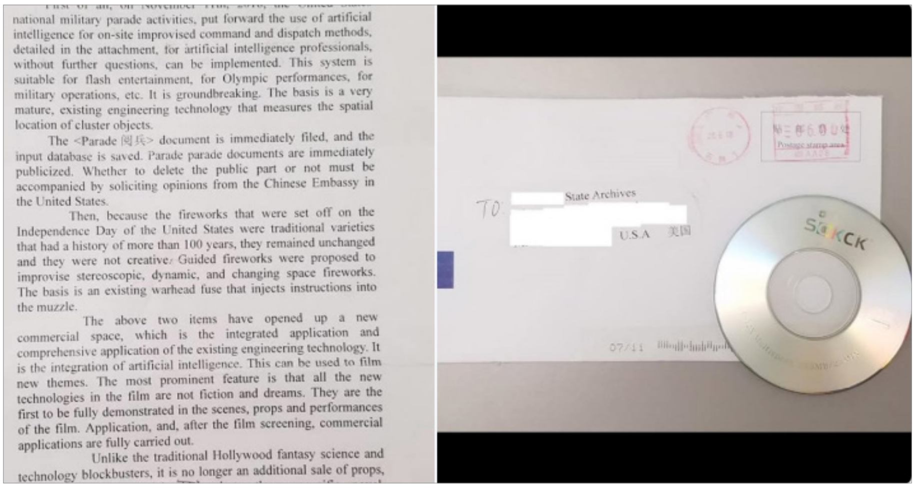


Figure 11. Attack targets

Figure 12. Data stolen

In order to get hold of secret government data, hackers keep searching for new ways of penetrating government information systems. In one such case, the attackers found an unusual way to deliver malware to the U.S. government agencies, playing up curiosity of potential victims. Employees received letters via mail that included malware-laden compact discs.[18]

[14] https://www.thelocal.se/20180822/swedens-social-democrats-website-hacked
[15] thehill.com/policy/cybersecurity/407608-california-democrat-hit-with-ddos-attacks-during-failed-primary-bid
[16] nltimes.nl/2018/08/01/ddos-attack-leaves-digid-site-unreachable
[17] mybroadband.co.za/news/security/274161-hackers-did-not-compromise-our-servers-department-of-labour.html
[18] krebsonsecurity.com/2018/07/state-govts-warned-of-malware-laden-cd-sent-via-snail-mail-from-china/



national military parade activities, put forward the use of artificial intelligence for on-site improvised command and dispatch methods, detailed in the attachment, for artificial intelligence professionals, without further questions, can be implemented. This system is suitable for flash entertainment, for Olympic performances, for military operations, etc. It is groundbreaking. The basis is a very mature, existing engineering technology that measures the spatial location of cluster objects.

The <Parade 阅兵> document is immediately filed, and the input database is saved. Parade parade documents are immediately publicized. Whether to delete the public part or not must be accompanied by soliciting opinions from the Chinese Embassy in the United States.

Then, because the fireworks that were set off on the Independence Day of the United States were traditional varieties that had a history of more than 100 years, they remained unchanged and they were not creative. Guided fireworks were proposed to improvise stereoscopic, dynamic, and changing space fireworks. The basis is an existing warhead fuse that injects instructions into the muzzle.

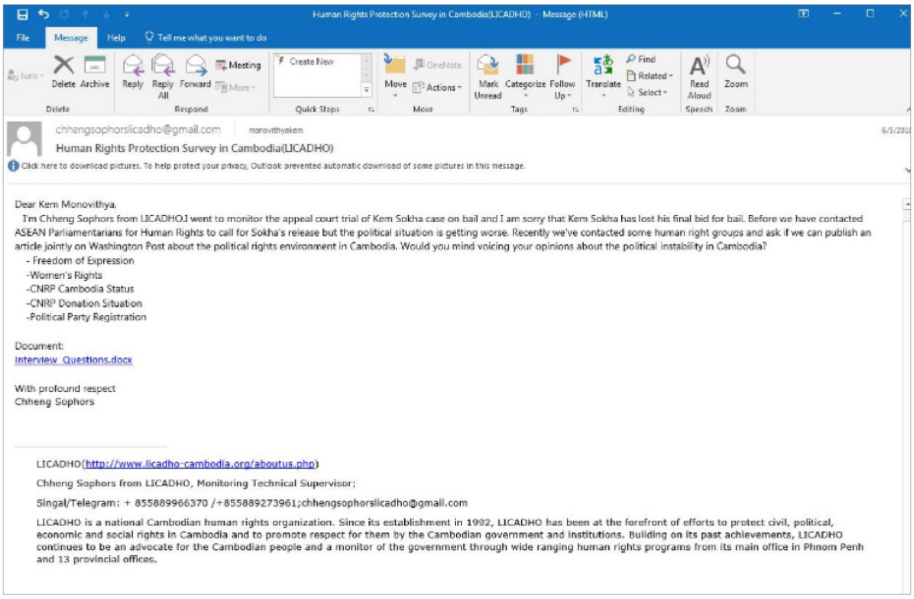
The above two items have opened up a new commercial space, which is the integrated application and comprehensive application of the existing engineering technology. It is the integration of artificial intelligence. This can be used to film new themes. The most prominent feature is that all the new technologies in the film are not fiction and dreams. They are the first to be fully demonstrated in the scenes, props and performances of the film. Application, and, after the film screening, commercial applications are fully carried out.

Unlike the traditional Hollywood fantasy science and technology blockbusters, it is no longer an additional sale of props,

Figure 13. Malware-laden CD sent to a U.S. government agency

Hackers take an increasing interest in government institutions in the run-up to important political events. Thus, in the run-up to the Swedish elections, hacktivists spread nationalist slogans and deceptive information in Twitter via botnets.[19]

Oftentimes, hackers use their skills to cyberspy government agencies. TEMP.Periscope, a Chinese espionage group previously known for its attacks against maritime entities, sent[20] a phishing message to the Deputy Director General of an opposition party in the run-up to the general elections in Cambodia. The message purported to come from LICADHO, a non-governmental organization promoting human rights. A malicious attachment in the message contained a downloader that installed spyware on the victim's computer.



chhengsophorslicadho@gmail.com monovithyakem 6/5/201

Human Rights Protection Survey in Cambodia(LICADHO)

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Kem Monovithya,

I'm Chheng Sophors from LICADHO.I went to monitor the appeal court trial of Kem Sokha case on bail and I am sorry that Kem Sokha has lost his final bid for bail. Before we have contacted ASEAN Parliamentarians for Human Rights to call for Sokha's release but the political situation is getting worse. Recently we've contacted some human right groups and ask if we can publish an article jointly on Washington Post about the political rights environment in Cambodia. Would you mind voicing your opinions about the political instability in Cambodia?

- Freedom of Expression
-Women's Rights
-CNRP Cambodia Status
-CNRP Donation Situation
-Political Party Registration

Document:
Interview_Questions.docx

With profound respect
Chheng Sophors

LICADHO(http://www.licadho-cambodia.org/aboutus.php)

Chheng Sophors from LICADHO, Monitoring Technical Supervisor;

Singal/Telegram: + 855889966370 /+855889273961;chhengsophorslicadho@gmail.com

LICADHO is a national Cambodian human rights organization. Since its establishment in 1992, LICADHO has been at the forefront of efforts to protect civil, political, economic and social rights in Cambodia and to promote respect for them by the Cambodian government and institutions. Building on its past achievements, LICADHO continues to be an advocate for the Cambodian people and a monitor of the government through wide ranging human rights programs from its main office in Phnom Penh and 13 provincial offices.

Figure 14. Phishing email with malicious attachment

[19] bloomberg.com/news/articles/2018-08-30/sweden-sees-increase-in-cyber-attacks-seeking-to-disrupt-vote?cmpId=flipboard

[20] fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

Finance

Damage approximately $18 million

Victims over 350 million

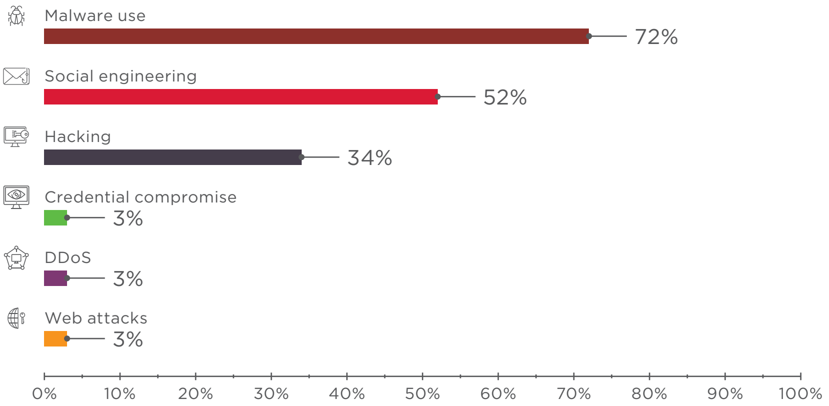
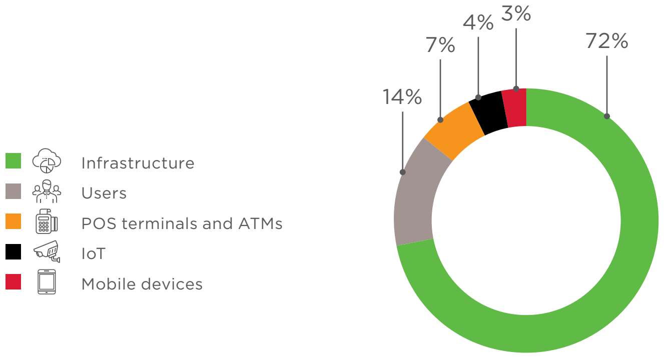


Figure 15. Finance: attack methods used in Q3 2018



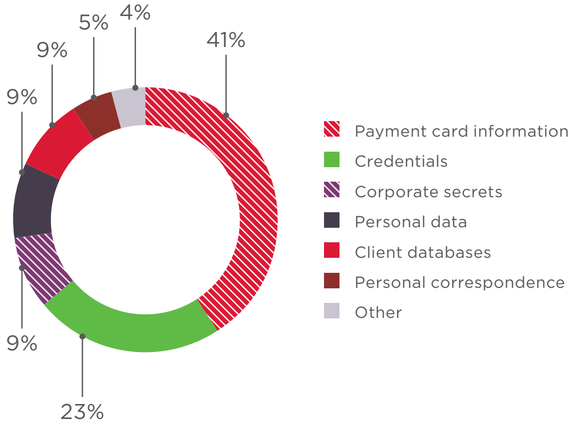


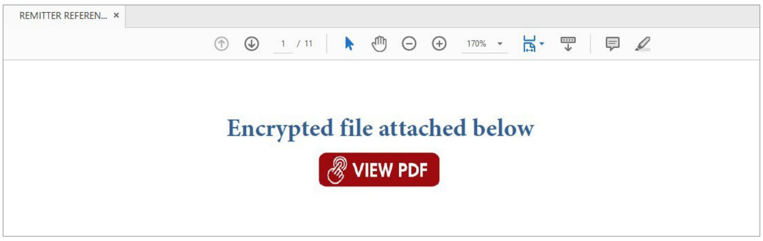
Figure 16. Attack targets

Figure 17. Data stolen

Q3 was marked by attacks against financial institutions performed by the APT groups. Thus, MoneyTaker attack[21] against network infrastructure of PIR Bank (Russia) resulted in the theft of over 58 million rubles (about $850,000). Another major attack hit[22] Cosmos Bank (India) resulting in the damage worth approximately $13 million. The crime was allegedly performed[23] by the North Korean hacking group APT38. In Q3 2018, we observed an increasing number of attacks against banks performed by Cobalt group. PT ESC experts registered 12 such attacks from July to September. In July, the attackers generally used JavaScript backdoor; since August, however, they started spreading CobInt malware. In August and early September, phishing messages were sent from fake domain addresses that were supposed to belong to the Interkassa payment system, the European Central Bank, BBVA Compass Bancshares, Unibank, Alfa-Bank, and Raiffeisenbank.

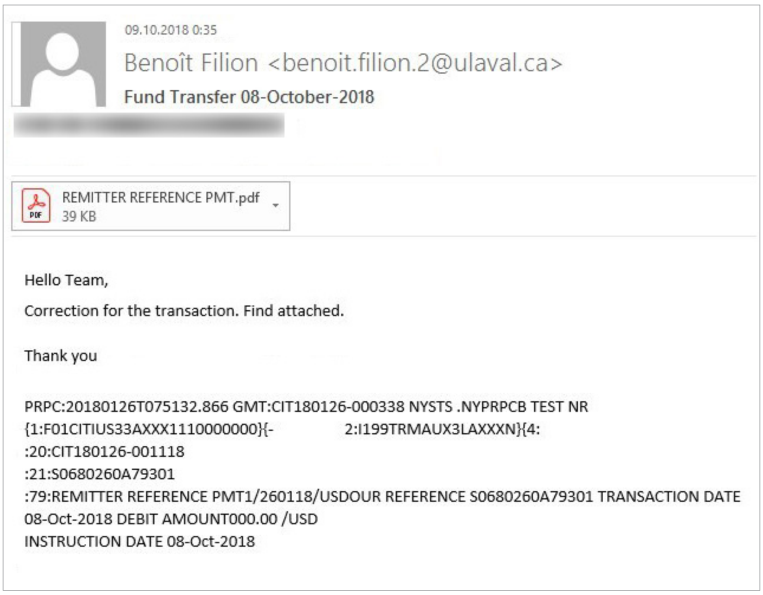
Cobalt group uses different methods to deliver malware. Thus, in early 2018, the criminals sent documents containing exploits. Since May, however, they switched to sending documents with obfuscated macros that made it difficult to detect attacks by antivirus solutions. Since September, the group started sending PDF files with malicious links, exploiting the Open redirect vulnerability.[24]

[21] bankingtech.com/2018/07/pir-bank-in-russia-victim-of-domestic-1m-hack/
[22] hindustantimes.com/india-news/15-000-transactions-in-7-hrs-cosmos-bank-s-server-hacked-rs-94-cr-moved-to-hong-kong/story-wazUXZs3LRhcbPLg7LYx5O.html
[23] content.fireeye.com/apt/rpt-apt38
[24] openbugbounty.org/reports/81002/



Encrypted file attached below

Figure 18. PDF file with a link to a malicious code



09.10.2018 0:35

Benoît Filion <benoit.filion.2@ulaval.ca>

Fund Transfer 08-October-2018

[redacted]

REMITTER REFERENCE PMT.pdf
39 KB

Hello Team,

Correction for the transaction. Find attached.

Thank you

```
PRPC:20180126T075132.866 GMT:CIT180126-000338 NYSTS .NYPRPCB TEST NR
{1:F01CITIUS33AXXX1110000000}{-            2:I199TRMAUX3LAXXXN}{4:
:20:CIT180126-001118
:21:S0680260A79301
:79:REMITTER REFERENCE PMT1/260118/USDOUR REFERENCE S0680260A79301 TRANSACTION DATE
08-Oct-2018 DEBIT AMOUNT000.00 /USD
INSTRUCTION DATE 08-Oct-2018
```

Figure 19. Phishing email with a malicious PDF file

Healthcare

Victims over
2 million

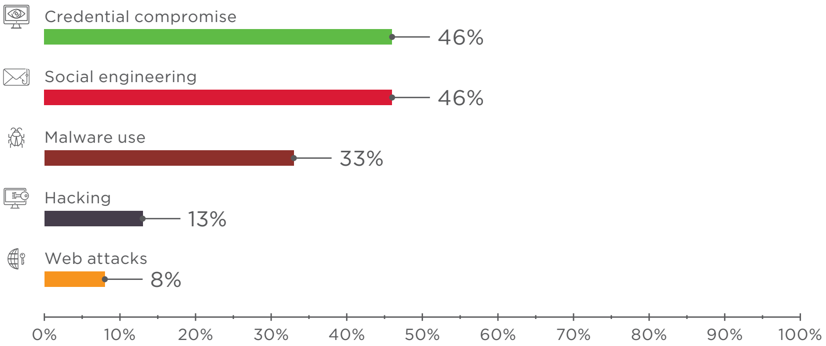
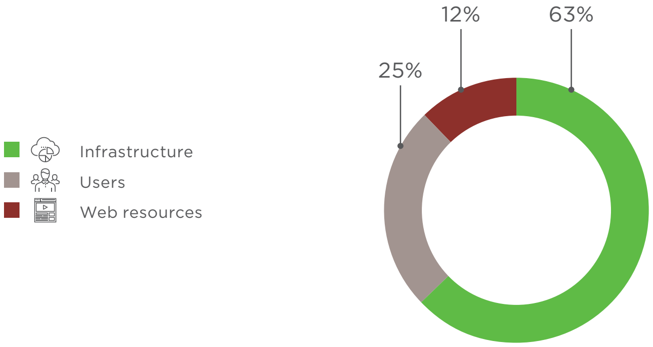


Figure 20. Healthcare: attack methods used in Q3 2018



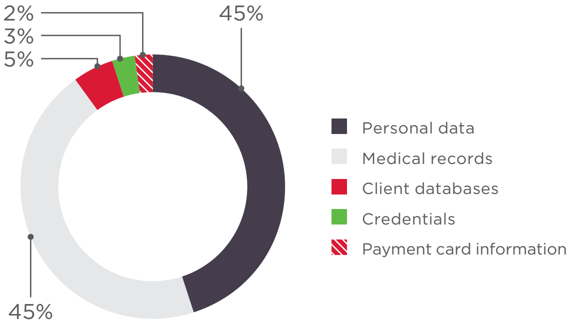


Figure 21. Attack targets

Figure 22. Data stolen

Healthcare institutions keep attracting criminals, as stolen medical data can bring huge profits, especially data of top-ranking government officials. An attack against SingHealth group in Singapore resulted in the theft of personal data of over 1.5 million people and medical data of about 160,000 patients, including the country's prime minister and other government officials.[25] Phishing attacks usually allow hackers to get hold of medical employees' credentials and to access closed databases. Thus, an attack against the Guardant Health medical center in California resulted in the leak of personal and medical data of over a thousand of clients.[26]

Despite the decrease in the number of attacks against medical institutions (33% as compared to 38% in Q2), several medical centers still got hit by attackers. Thus, hackers attacked medical institutions in the U.S., Canada, India, and Hong Kong, infecting computers with ransomware. In most cases, infection becomes possible when companies do not timely upgrade their software. Software upgrading can take a lot of time and effort, and any failure or error may put patient lives and health at risk. Thus, a vulnerability in the software of CarePartners, a Canadian healthcare company, allowed attackers to conduct a ransomware attack compromising medical and contact data of tens of thousands of clients.[27] The company now faces substantial fines.

Education

Victims over 42,000

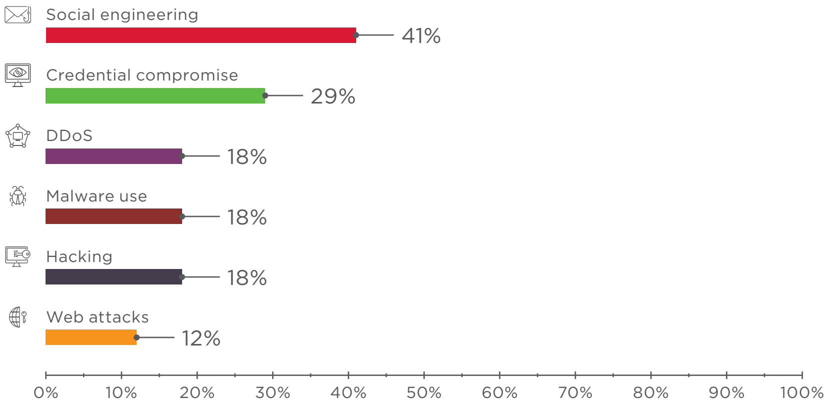
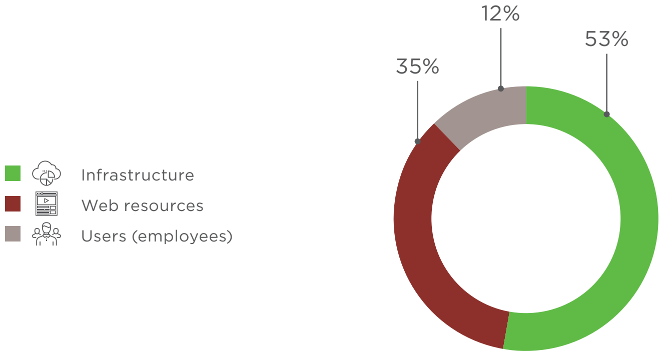


Figure 23. Education: attack methods used in Q3 2018



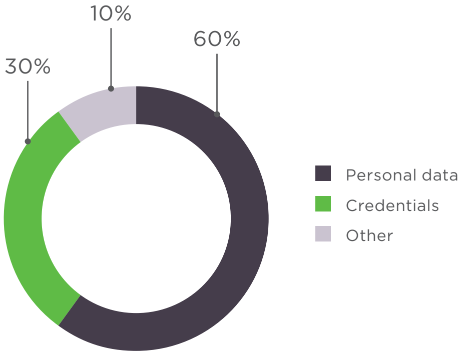


Figure 24. Attack targets

Figure 25. Data stolen

[25] moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack
[26] mddionline.com/guardant-exposed-cybersecurity-threat-phishing-scheme
[27] cbc.ca/news/technology/carepartners-data-breach-ransom-patients-medical-records-1.4749515

As mentioned, education institutions suffered from numerous attacks at the beginning of the school year. In late August, Cloquet schools (U.S.) were hit by a ransomware attack second time in the past three years.[28] Monroe County School District was also hit by a ransomware campaign.[29]

A large-scale campaign by Cobalt Dickens spread during summer vacation hit 76 universities in 14 countries all over the world.[30] The attackers sent phishing messages to the university employees with links to spoofed websites and login pages. By stealing the account credentials, hackers got access to intellectual property of education institutions.

Individuals

Damage approximately $28 million

Victims approximately 43 million

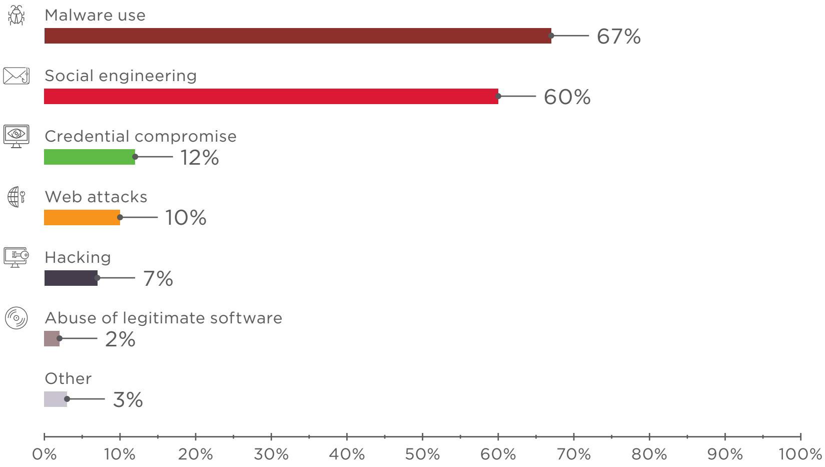
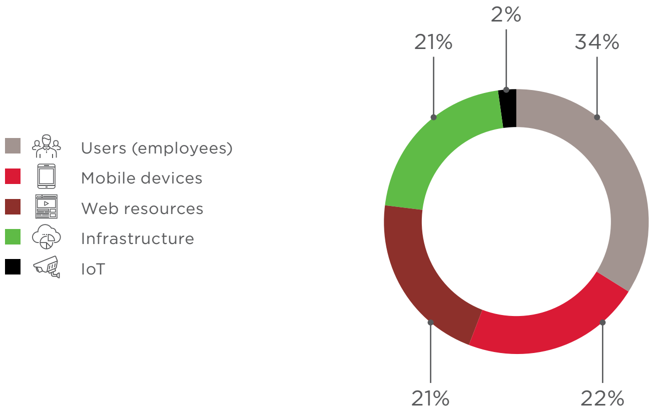


Figure 26. Individuals: attack methods used in Q3 2018



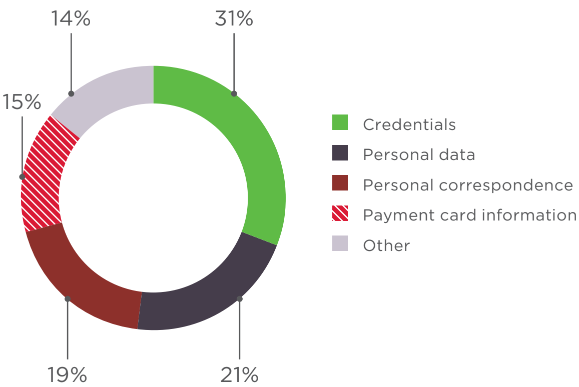


Figure 27. Attack targets

Figure 28. Data stolen

Q3 was marked by an increasing number of attacks involving social engineering (60% as opposed to 38% in Q2). By manipulating people's feelings, hackers hit individuals who are often not security-savvy. In August, an extortion email campaign took place with attackers claiming that the recipients' phones were hacked and that people were recorded over their webcam.[31]

[28] spamfighter.com/News-21734-Cloquet-School-District-Again-Targeted-by-a-Ransomware-Attack.htm
[29] scmagazine.com/home/news/new-gandcrab-variant-attacks-florida-school-district/
[30] secureworks.com/blog/back-to-school-cobalt-dickens-targets-universities
[31] twitter.com/secguru_otx/status/1028364785631617025

In addition to credit card information, hackers also steal private data, correspondence, and photographs, using this information to demand ransom. In Q3, criminals hacked numerous user accounts in messengers and social networks. In August and September, large-scale attacks targeted Instagram users.[32] Thousands of people lost their accounts, many of them having over 10,000 subscribers. The victims were often ready to pay a ransom to get their accounts back, as they had largely invested in promoting their accounts in the first place. If attackers fail to get ransom, they can try selling the accounts or using them to send spam messages.

What companies can do to stay safe

Use proven security solutions:

- Implement centralized management for timely installation of updates and patches.
- Use antivirus protection solutions with embedded isolated environment (sandbox) for dynamic file testing, capable to detect and block malicious files in corporate emails before the messages are opened by employees, and to eliminate other viruses. The most effective approach is to use antivirus software solutions developed by different manufacturers, capable to detect hidden malware and block viruses in data flows, including email, network, and web traffic, file storages, and web portals. The solution must not only check files in real time, but also automatically analyze files that have already been checked; this will allow detecting new threats when signature bases are updated.
- We also recommend using the SIEM solutions to timely detect and effectively respond to information security incidents. This will help identify suspicious activity, prevent infrastructure hacking, detect attackers' presence, and take prompt measures to neutralize the threats.
- Use automated software audit tools to identify vulnerabilities.
- Use web application firewalls as a preventive measure to protect websites.
- Implement systems allowing deep network traffic analysis in order to detect complex targeted attacks in real time and in backup copies. You will be able to detect attacks that have not been found earlier and to monitor network attacks in real time, including malware run and hacking tools, exploitation of software vulnerabilities, and attacks against the domain controller. This approach will allow you to quickly identify attackers' presence in the infrastructure, minimize the risk of losing critical data and disrupting business systems, and to decrease financial damage caused by attackers.
- Use 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 use identical username–password combinations for multiple systems.
- Use two-factor authentication where possible, especially for authenticating privileged accounts.

[32] mashable.com/2018/08/13/instagram-hack-locked-out-of-account/?europe=true#KzywbMs8rqq6

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:

- Use complex passwords consisting of at least eight letters, numbers, and symbols. Use a password manager to create and store 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