

CYBERSECURITY THREATSCAPE

Q4 2017









CONTENTS







Symbols used.....	3
Executive summary.....	4
Incident trends.....	6
Attack methods.....	7
Use of malware	7
Social engineering.....	9
Software vulnerabilities exploitation.....	10
Web vulnerabilities exploitation	12
Compromise of credentials.....	13
DDoS.....	14
Attack targets.....	16
Infrastructure	16
Web resources	18
Users	19
Mobile devices	20
POS terminals and ATMs	21
IoT.....	22
The big picture.....	24

SYMBOLS USED















Attack targets

-  Infrastructure
-  Web resources
-  Users
-  POS terminals and ATMs
-  Mobile devices
-  IoT

Attack methods

-  Use of malware
-  Compromise of credentials
-  Social engineering
-  Software vulnerabilities exploitation
-  Web vulnerabilities exploitation
-  DDoS

Victim categories

-  Finance
-  Government
-  Healthcare
-  Education
-  Military
-  Industrial companies
-  Online services
-  Entertainment
-  Transportation
-  IT
-  Retail
-  Individuals
-  Telecom
-  Other

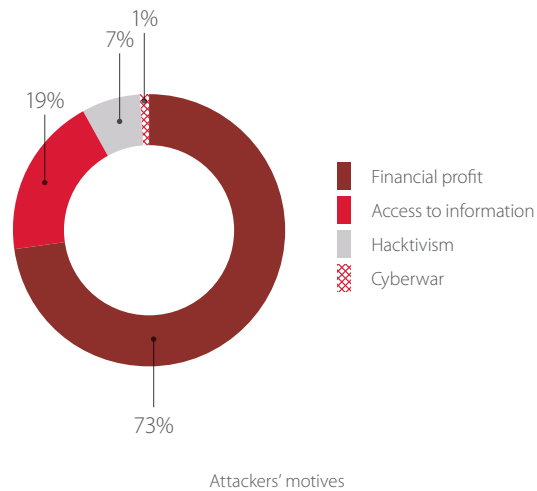
Positive Technologies regularly presents information on the most important and emerging IT security threats. In keeping with similar reports from previous quarters, this report covers incidents in the fourth quarter of 2017. Information is drawn from our own expertise, outcomes of numerous investigations, and data from authoritative sources.

EXECUTIVE SUMMARY

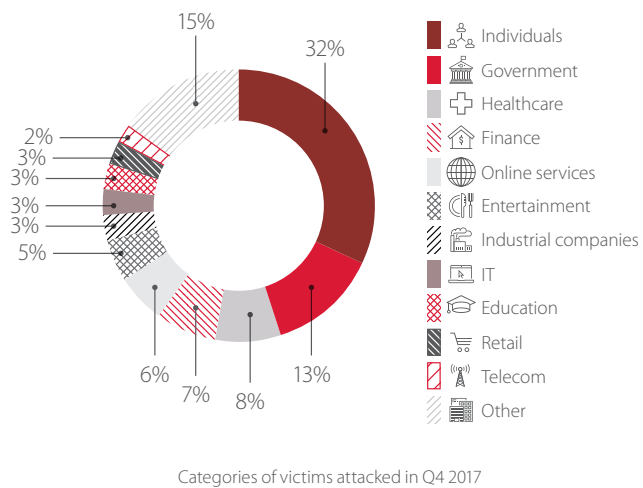
73 percent of attacks were aimed at direct financial gain. The fourth quarter also saw an uptick in hacktivism (typically intended to protest government actions): 7 percent compared to 3 percent in Q3. The share of attacks aiming to acquire data fell from 25 percent in Q3 to 19 percent in Q4.

In Q4, mass attacks again have taken a significant lead (58%).

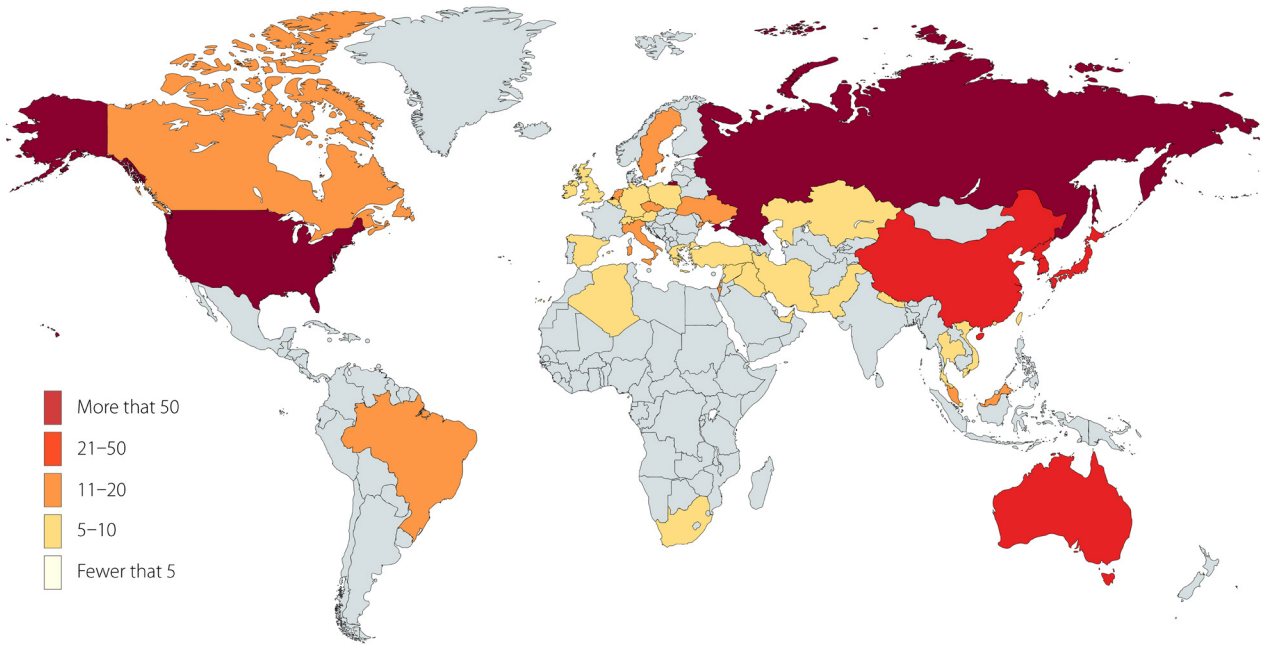
Government, healthcare, and finance are still under threat, attracting 13, 8, and 9 percent of the total, respectively. But most other cyberattacks targeted individuals (32%).



As mentioned, Q4 saw numerous mass attacks, most of them affecting two, three, ten, or more countries simultaneously. The U.S., Russia, Australia, South Korea, Japan, and China lead the list of countries by number of unique cyberincidents.



Mass attacks affecting hundreds or thousands of companies in diverse industries have been categorized for statistical purposes as targeting Other, which is why such a large number of incidents fall under this category.

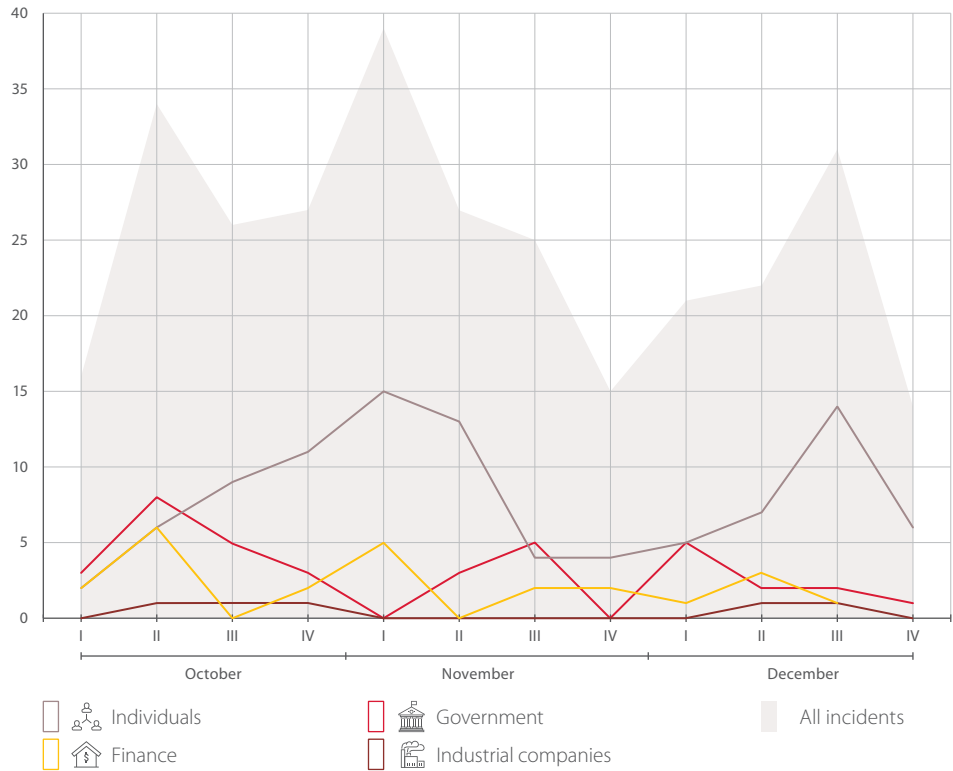


Cyberattack geography, Q4 2017

		Industry										
		Finance	Government	Healthcare	Education	Industrial companies	Online services	Entertainment	Individuals	Retail	IT	Other
Target	Infrastructure	12	22	7	9	5	4	9	29	2	8	31
	Web resources	3	12	1	1		15	5	19	1	5	6
	Users	4		10	4		3	2	22	1		6
	POS terminals and ATMs	3							1	2		1
	Mobile devices	2	2						23			1
	IoT		1						3		1	2
Method	Use of malware	17	11	5	6	2		4	51		3	23
	Compromise of credentials		2	6	1		3	1	8	1	2	5
	DDoS	2	8				4					2
	Social engineering	3	2	5	2	3	2	1	13			3
	Software vulnerabilities exploitation	1	7		3		3		10	2	2	5
	Web vulnerabilities exploitation		3	1	1		8	4	7	1	3	2
	Other	1	4	1	1		2	6	7	2	4	7
Motive	Financial profit	24	16	10	8	2	20	7	84	5	11	30
	Access to information		11	8	5	1	1	5	12	1	3	11
	Hacktivism		8		1	1	1	4				5
	Cyberwar		2			1						1

Classification of cyberincidents by motive, method, target, and industry

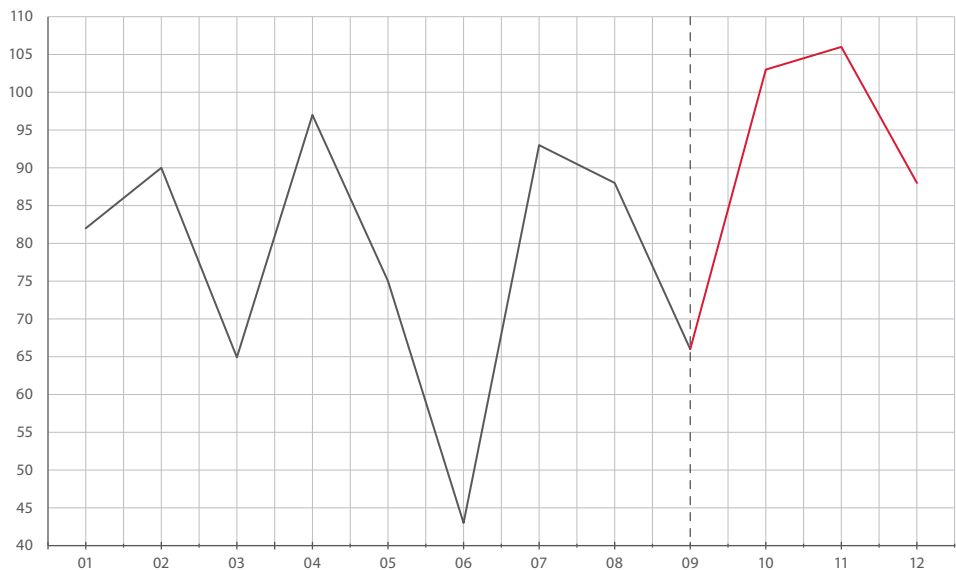
INCIDENT TRENDS



Number of incidents in Q4 2017

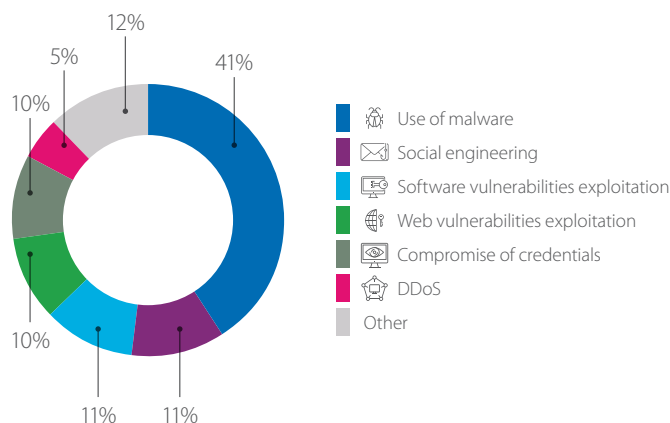
Q4 had more unique incidents than previous quarters. Early November and late December show an increase in the number of attacks on individuals. These peaks correlate with the holiday shopping season, when customers are inclined to buy online without necessarily checking the reputation of the merchants they visit.

Growth in cyberattacks in October and November was followed by a slight drop in December. However, information about cyberincidents often becomes known well after the fact—companies that fell victim during Q4 may still be investigating before they decide to go public, or perhaps they do not even know they were successfully attacked and will only find indicators of compromise much later.



Number of incidents in 2017 (01 = January, 12 = December)

ATTACK METHODS



Cyberincidents, by attack method used

USE OF MALWARE

41%

Most affected:
worldwide

Most frequently attacked targets:

62%	21%	3%

Most severe damage:

42%	14%	8%

Infected: > 23 million devices

Bitcoin cooled in the second half of December, though investors did not seem to be put off by the cryptocurrency's volatility. Neither were hackers: the number of people trying to profit from cryptocurrency via fraud is still growing. Hackers have created malware to secretly mine cryptocurrency on a victim's computer or mobile device, funneling the proceeds to the hacker's wallets. One such example is a Chrome extension that loads the Coinhive miner into the victim's browser.¹ This miner is in active development² and now can run in a hidden window, under the Windows taskbar and behind the clock, with moderate CPU usage for additional stealth.

With security awareness improving among users, hackers are having to invent new ways of distributing malware. For example, to distribute Emotet banking malware, hackers leveraged users' trust in information security websites and redirected their victims via a McAfee domain (cp.mcafee.com) to another website, which downloaded a malicious Microsoft Word document to the user's computer.³

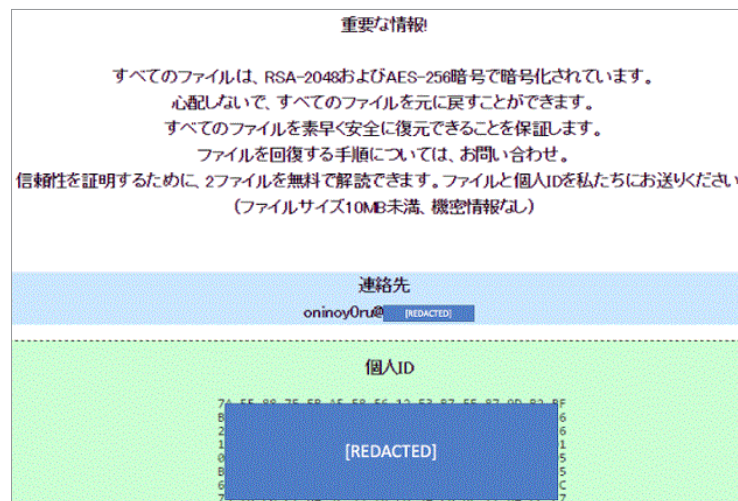
¹ bleepingcomputer.com/news/security/chrome-extension-uses-your-gmail-to-register-domains-names-and-injects-coinhive/

² blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/

³ twitter.com/benkow/status/930148339034869764

While investigating attacks against banks in Eastern Europe, our experts noticed one more unusual vector for malware attacks.⁴ Attackers advertised online to hire so-called mules, who then ordered debit cards from a targeted bank. The attackers compromised the bank's internal infrastructure to increase the overdraft limit of the cards received by the mules and to gain privileged access to bank ATMs. Hackers then commanded the mules to withdraw cash from ATMs at a specified time. As soon as cash was withdrawn, the attackers ran a file called dropper.exe on the ATM. This malware corrupted the master boot record of the ATM operating system, making the OS unbootable, and then deleted itself and restarted the system. These actions were intended to eliminate potential evidence and prevent investigators from reconstructing the sequence of events.

Another new trend in ransomware is its use to mask the real motives of attackers. In late October, researchers told about a campaign against Japanese companies:⁵ attackers sent phishing emails containing malicious documents, which, when opened, installed the Ammy Admin remote administration tool on the computer. Now equipped with remote access, the criminals compromised critical assets of the target company. As soon as attackers completed their malicious activities, they ran ONI and MBR-ONI malware that encrypted the disk and displayed a ransom note. The difference between these two malicious programs is that MBR-ONI was generally detected on Active Directory servers or other critical systems, and was not intended to decrypt data. On the contrary, its purpose was to erase traces of data theft. Incidentally, MBR-ONI is a modification of legitimate DiskCryptor encryption software.



Ransom note on computers infected by ONI

Advice for companies

- + Keep software up to date.
- + Use effective antivirus protection on all devices.
- + Monitor the network perimeter for unsafe resources.
- + Make regular backups. Store backups on dedicated servers that are isolated from production systems.
- + Increase user/employee awareness regarding information security.

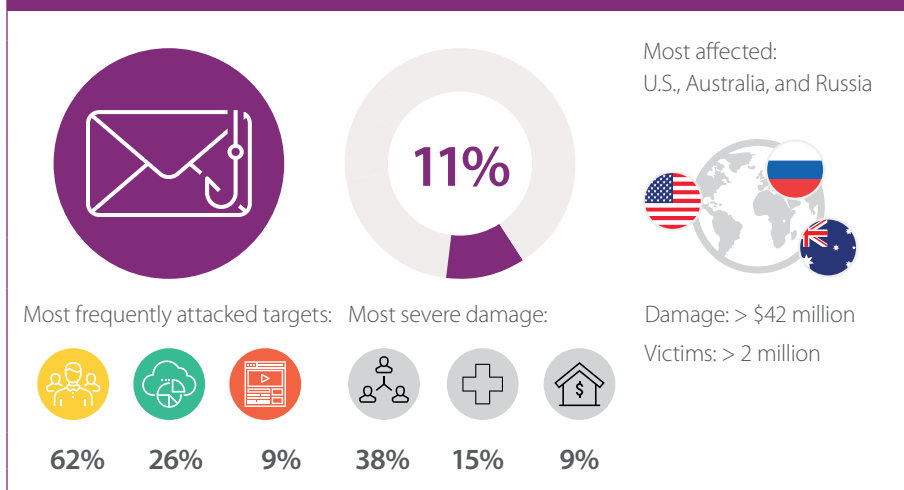
Tips for users

- + Install software updates as soon as they are released.
- + Use effective antivirus protection on all devices.
- + For important files stored on a hard disk, keep backups on removable drives, external hard disks, or in the cloud.
- + Do not open unknown suspicious links, especially if a browser displays a warning.
- + Do not click links in pop-up ads, even if you are familiar with the company or product being advertised.
- + Scan all email attachments with antivirus software.
- + Do not download files from suspicious websites or unknown sources.

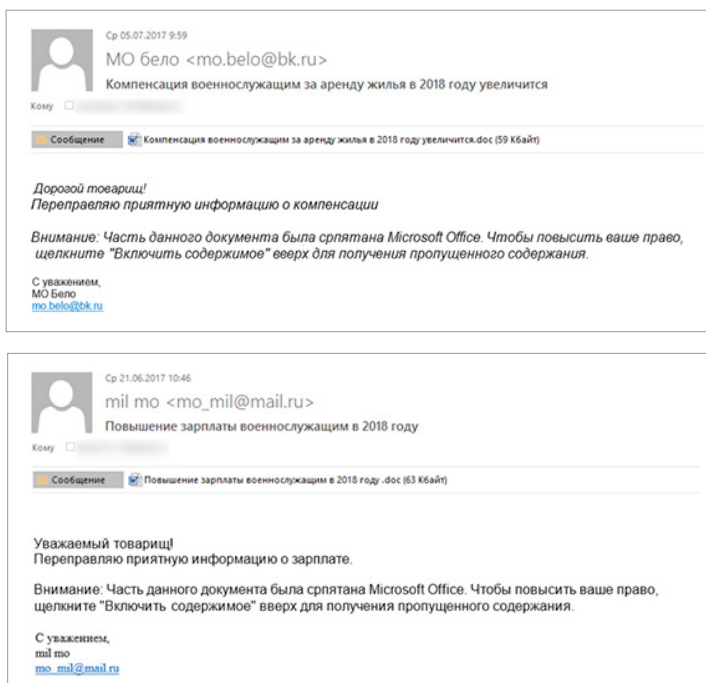
4 trustwave.com/Resources/SpiderLabs-Blog/Post-Soviet-Bank-Heists---A-Hybrid-Cybercrime-Study/

5 cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan

SOCIAL ENGINEERING



In April 2017, the Positive Technologies Expert Security Center (PT ESC) detected attacks by a group of hackers against defense contractors in Russia and former Soviet countries. This campaign (which we dubbed SongXY) involved distribution of CMstar and Lurid malware by means of targeted phishing emails. The "bait" in these messages was news of defense and political interest, with recipients including both companies and individuals. In mid-September, we saw a change in the attackers' tactics: some documents contained a link to an image, instead of a malicious payload. When the user opened a document containing this link, a request for the image was sent to the attackers' server, and the server received the IP address and Microsoft Office version of the user's system. This use of images enabled collecting statistics about the delivered emails, while the software version data allowed selecting a suitable exploit for subsequent attacks.



Examples of phishing emails sent by SongXY, supposedly informing of increased salaries and housing allowances for military personnel

The priority task of the SongXY campaign was spying; by installing such malware as Pilot RAT, Lurid, Gh0st, and RAT mini, attackers could secretly track users and remotely control the infected system. Investigation by PT ESC revealed that at least 17 companies in Japan, Mongolia, Belarus, Russia, U.S., Tajikistan, Uzbekistan, Kyrgyzstan, Kazakhstan, and Ukraine fell victim to SongXY. PT ESC immediately informed these companies about the compromise.

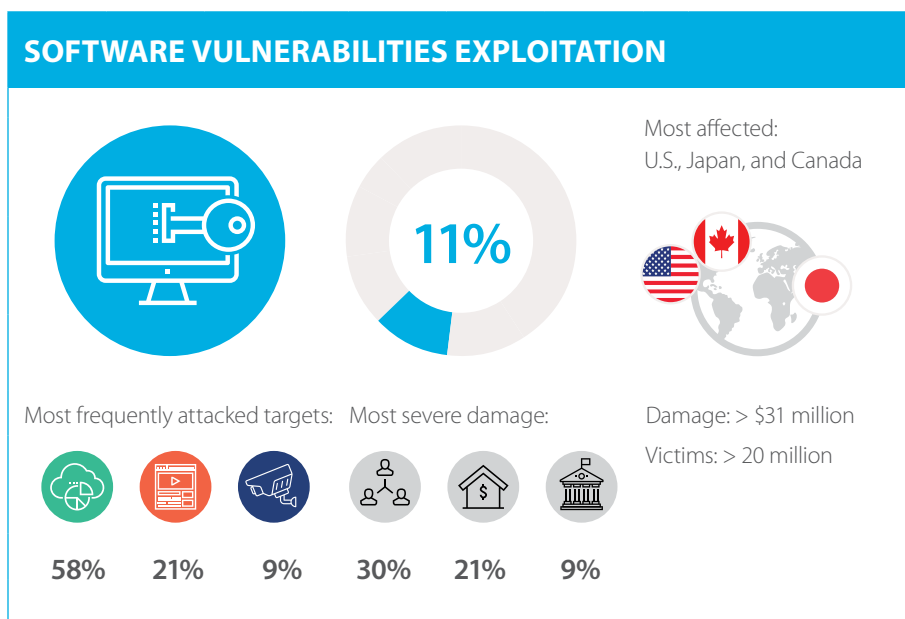
Last fall, PT ESC detected over 20 phishing attacks against banks in Russia, Kazakhstan, and Belarus by the Cobalt and Silence APT groups. Both groups used the supply-chain attack method: they compromised the IT infrastructure of a contractor in order to impersonate it in phishing emails to the company's partner (the real target), or registered phishing domains that resemble the names of trusted sites (for example, Cobalt used such domains as [visa-pay.com](#), [swift-alliance.com](#), [cards-cbr.ru](#), and [billing-cbr.ru](#) in their mailings). This approach evades spam filters and makes the messages appear trustworthy.

Advice for companies

- + Train employees and users on information security basics.
- + Use antivirus software that allows users to send suspicious files for verification before opening an attachment.
- + Use SIEM solutions for timely detection of attacks.

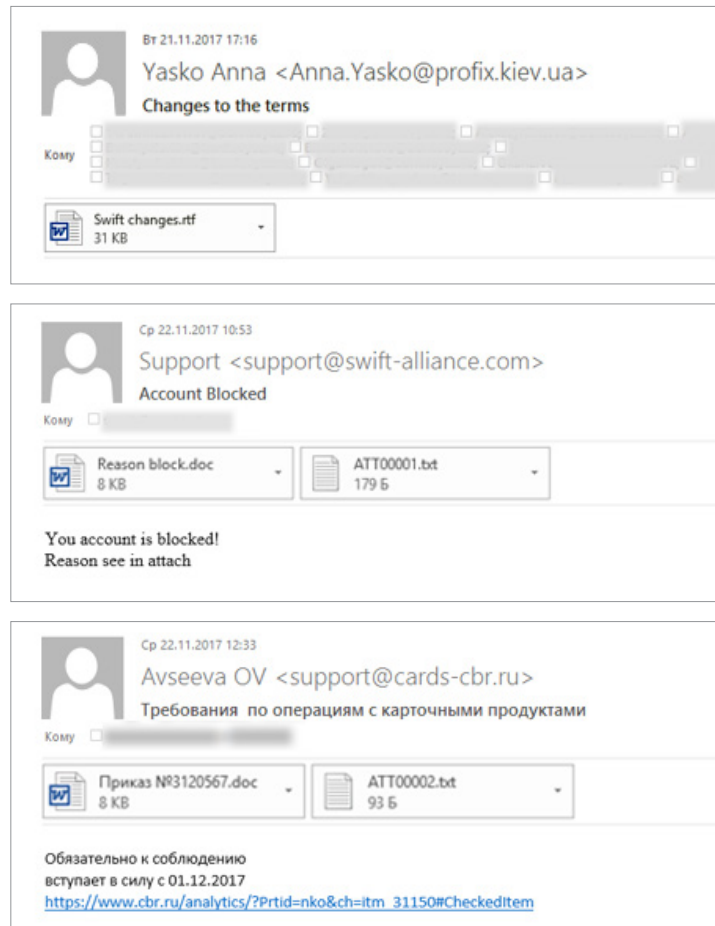
Tips for users

- + Use effective antivirus protection on all devices.
- + Do not open unknown suspicious links, especially if a browser displays a warning.
- + Beware of sites with invalid certificates. Remember that data entered on such sites can be intercepted.
- + Be extremely careful when entering passwords on websites and making online payments.
- + Scan all email attachments with antivirus software.



As soon as a white paper detailing a newly found vulnerability is published on the Internet, hackers race to put the vulnerability to use. What is more, some researchers are in such a hurry to share their discovery that they barely wait until the vendor has issued the relevant patch.

In late November, PT ESC learned that the Cobalt group had started to use a new Microsoft Office vulnerability ([CVE-2017-11882](#)) in their attacks on banks. Microsoft informed of the vulnerability on November 14, indicating that merely changing settings would not be enough to temporarily address the vulnerability—users must either disable Equation Editor in Microsoft Office or install the latest security update. This vulnerability was found by Embedi, so as soon as Microsoft released an update, Embedi researchers shared their proof of concept on [github.com](#), confirming the possibility of remote code execution without user interaction required. Later, even more instructions for how to exploit the vulnerability were published. Most likely, attackers made use of these public materials to generate malicious RTF files, which then were sent to banks in phishing emails. Attackers acted faster than companies installed updates; therefore, a significant number of financial institutions in Russia and Ukraine were affected by this incident.



Examples of phishing emails from the Cobalt group, typically claiming to inform of changes in banking industry rules and regulations

One interesting event, however, was neither an attack nor incident, and therefore not included in our statistics. Estonia is a world leader in digitalization of government functions and transactions. The national ID card includes a computer chip functioning as a citizen's signature. Even elections in Estonia have been held online since 2007. However, functioning of e-government relies on good security. That is why Estonian authorities in October had to recall 760,000 digital certificates when a vulnerability was reported in the trusted platform module (TPM) used to create RSA encryption keys (including for the chips used in Estonian ID cards).⁶ This proactive security measure is a positive example of prioritizing prevention above the short-term cost of reissuing certificates and updating government systems.

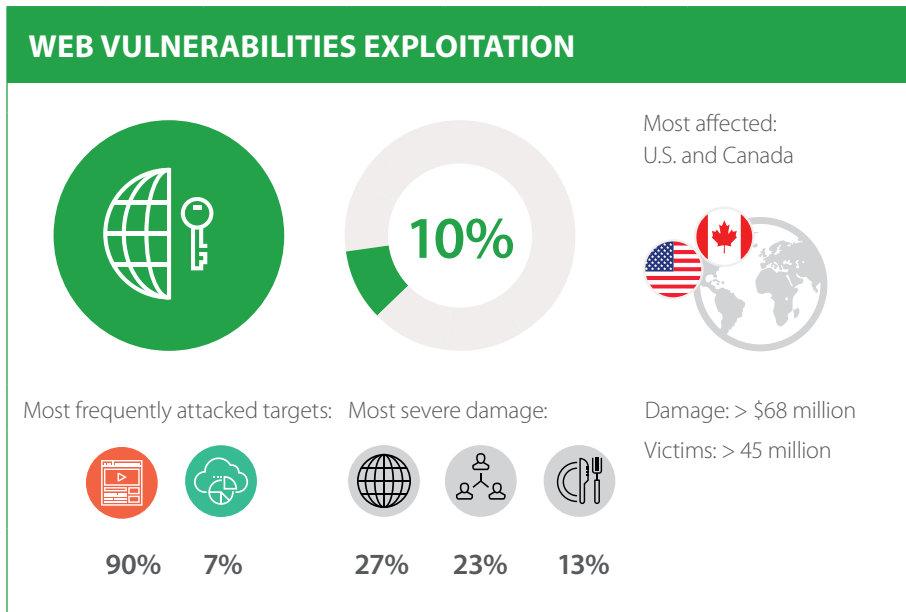
Advice for companies

- + Implement centralized management for timely installation of updates and patches.
- + Use automated tools to assess security and identify vulnerabilities in software.
- + Deploy a web application firewall for proactive protection.
- + Use effective antivirus protection on all devices.
- + Minimize the privileges of users and services as much as possible.

Tips for users

- + Keep software up to date.
- + Use effective antivirus protection on all devices.
- + Use accounts without administrator privileges for everyday work.
- + Do not open unknown suspicious links, especially if a browser displays a warning.
- + Scan all email attachments with antivirus software.
- + Do not download files from suspicious websites or unknown sources.

⁶ estonianworld.com/technology/possible-security-risk-affects-750000-estonian-id-cards/



Web application vulnerabilities generally are used in one of three different attack scenarios: an attack directly on a website (for example, to alter wallet information for an ICO); an attack to gain access to a company's network via its web applications; or an attack that lurks on a vulnerable website, such as to host malware and attack website users.

One out of every four web applications is vulnerable⁷ to SQL Injection, a critical flaw that allows attackers to obtain information about users. This type of attack happened to Hetzner Online GmbH,⁸ an Internet hosting company and data center operator. SQL Injection attacks against the company's database resulted in access to client data (including names, addresses, and phone numbers), domain names, FTP passwords, and payment information (except for credit cards).

Government websites are often hijacked for protest or propaganda purposes. For example, one group of cybercriminals spent months hacking hundreds of police and school websites⁹ to post pro-Islamic messages.



School website defacement

Another hacker group—Anonymous—targeted neo-Nazi websites and attacked 12 of them in November as part of the #OpDomesticTerrorism campaign.¹⁰

⁷ [ptsecurity.com/upload/corporate/ww-en/analytcs/Web-Application-Vulnerability-2016-eng.pdf](https://www.ptsecurity.com/upload/corporate/ww-en/analytcs/Web-Application-Vulnerability-2016-eng.pdf)

⁸ [hetzner.co.za/news/konsoleh-database-compromise/](https://www.hetzner.co.za/news/konsoleh-database-compromise/)

⁹ [ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210](https://www.ibtimes.co.uk/pro-isis-hackers-hijack-800-us-schools-sites-saddam-hussein-photo-i-love-islamic-state-message-1646210)

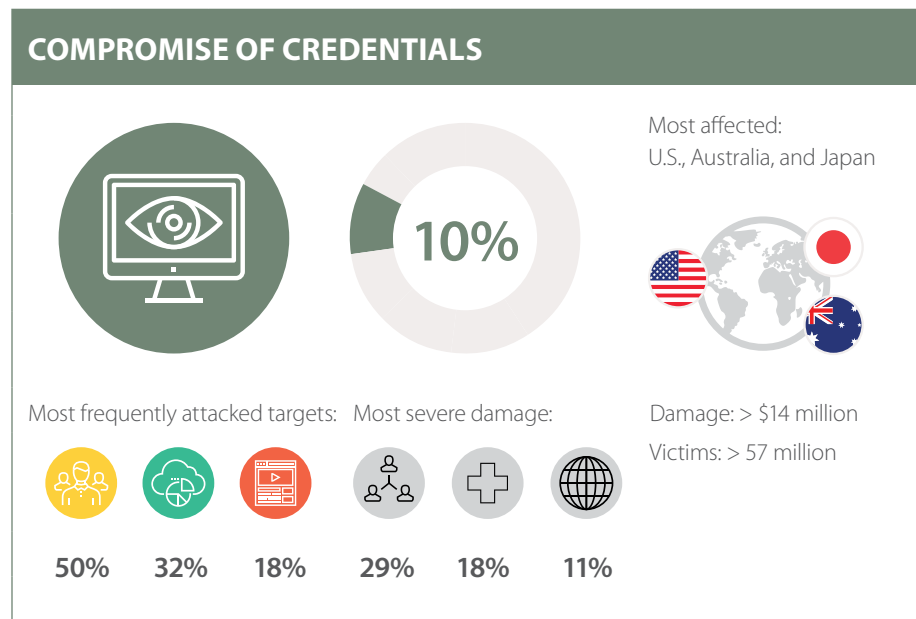
¹⁰ [ibtimes.co.uk/opdomesticterrorism-anonymous-hackers-take-down-over-dozen-neo-nazi-sites-new-wave-attacks-1647385](https://www.ibtimes.co.uk/opdomesticterrorism-anonymous-hackers-take-down-over-dozen-neo-nazi-sites-new-wave-attacks-1647385)



Defacement of a neo-Nazi website

Advice for companies

- + Perform regular analysis of web application security, including source code audits.
- + Deploy a web application firewall for proactive protection.
- + Practice a secure development lifecycle for web applications.
- + Use up-to-date versions of web servers and database systems. Avoid vulnerable versions of libraries or frameworks.



Siphoning cryptocurrency is a major interest for hackers. Late October saw attacks on the ethOS operating system installed on Ethereum mining equipment.¹¹ Attackers scanned the Internet to look for mining equipment supporting SSH connections with the default username and password combinations (ethos:live and root:live). If successful, the attackers logged in to direct the proceeds of mining to the attackers' wallet. According to Bitdefender, the attackers' wallet shows only 10 transactions, with a total value of around USD \$600.

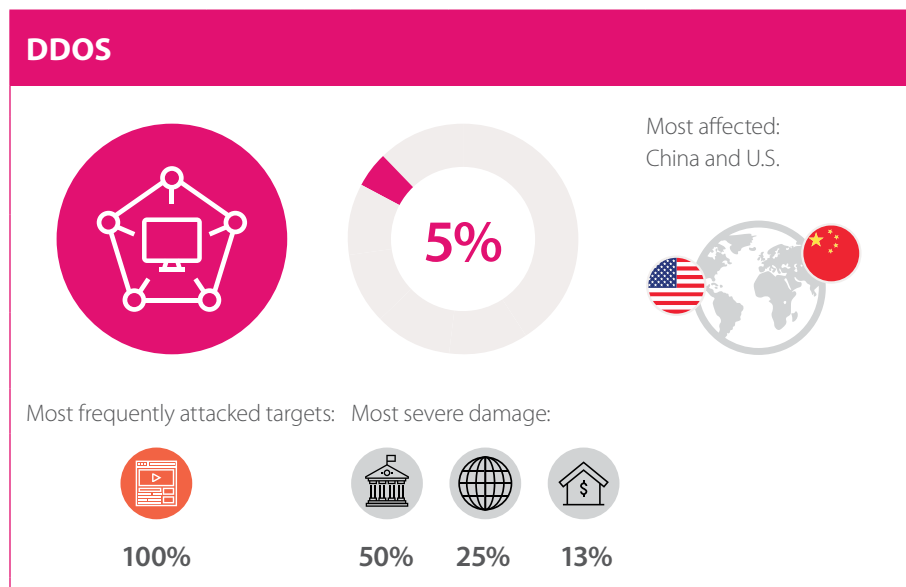
Advice for companies

- + Enforce a password policy with strict length and complexity requirements.
- + Do not reuse the same accounts and passwords for different sites or services.
- + Do not store user passwords in cleartext. Do not encrypt passwords using reversible encryption algorithms.
- + Require that passwords be changed at least once every 90 days.
- + Use two-factor authentication where possible (for example, to protect privileged accounts).
- + Ensure that user accounts of former employees are deleted or blocked in a timely manner.

¹¹ labs.bitdefender.com/2017/11/ethereum-os-miners-targeted-by-ssh-based-hijacker/

Tips for users

- + Use complex passwords consisting of at least eight letters, numbers, and symbols. Use a password manager to create and store passwords.
- + Do not use the same password for different systems (including sites and email).
- + Change all passwords at least once every six months, or even better, every two to three months.
- + Use two-factor authentication where possible, such as to protect email accounts.



Government websites are the most popular targets of DDoS attacks, drawing the brunt of public discontent. In October 2017, Catalonia held a referendum in which over 90 percent of voters opted for independence, but Spanish authorities ruled the process illegal. The central government's response drew public ire, which spilled over into a series of DDoS attacks by Anonymous¹² hacktivists against the websites of the Autonomous Community of Madrid, Constitutional Court of Spain, Ministries of Economy and Justice, and many more.

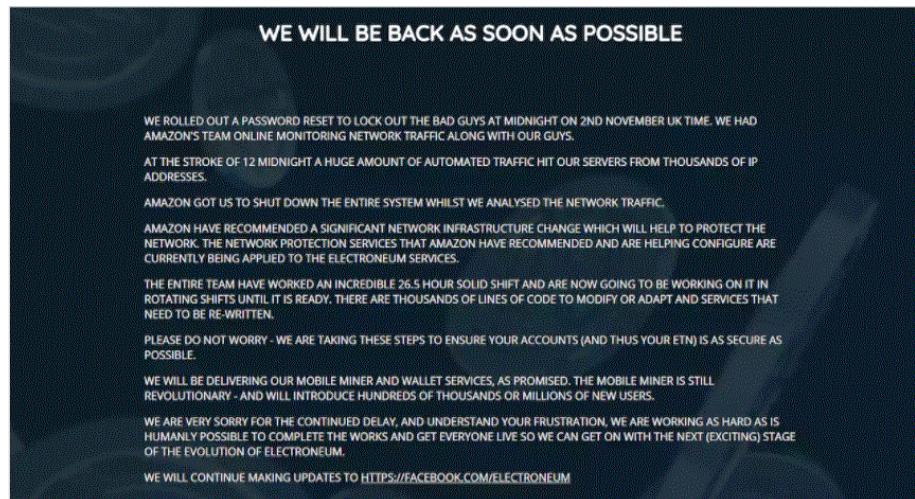


DDoS attacks against Spanish government websites

DDoS attacks pose a particular threat to cryptocurrency exchanges and ICOs, which draw ever-greater sums but still give short shrift to security. Electroneum,¹³ a UK cryptocurrency startup that crowdfunded USD 40 million in an ICO, fell victim to a DDoS attack, which disabled both the website and access to investors' accounts. Electroneum blocked accounts to avoid any losses for clients during the attack.

¹² politica.elpais.com/politica/2017/10/21/actualidad/1508574710_898791.html

¹³ telegraph.co.uk/technology/2017/11/06/british-cryptocurrencyelectroneum-hit-cyber-attack-raising-30m/



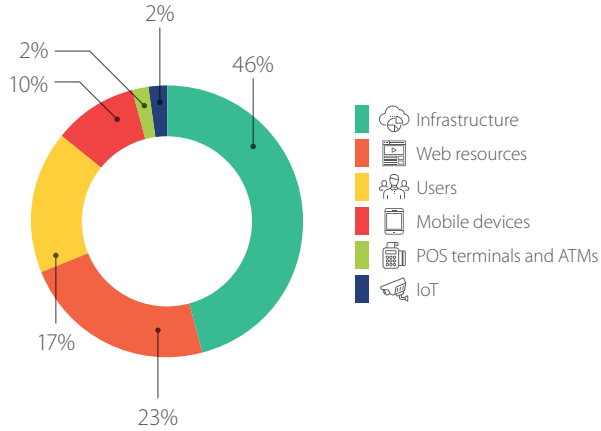
DDoS on Electroneum's ICO

Advice for companies

- + Configure servers and network devices to withstand common attacks (for example, TCP and UDP flooding, or high numbers of database requests).
- + Monitor requests per second for sudden jumps in activity.
- + Use an anti-DDoS service.
- + If holding an ICO, hire specialists to check the integrity of smart contracts and ensure cybersecurity (see ico.positive.com).

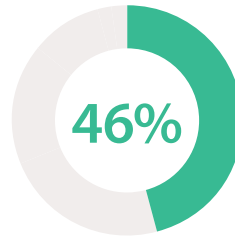
ATTACK TARGETS

Based on the statistics throughout the year, we see that attack targets remain stable overall.



Cyberincidents, by attack target

INFRASTRUCTURE



Most affected: U.S., Russia, South Korea, and Italy



Most common attack methods:

Most severe damage:

Damage: > \$143 million



55%



14%



7%



22%



17%



9%

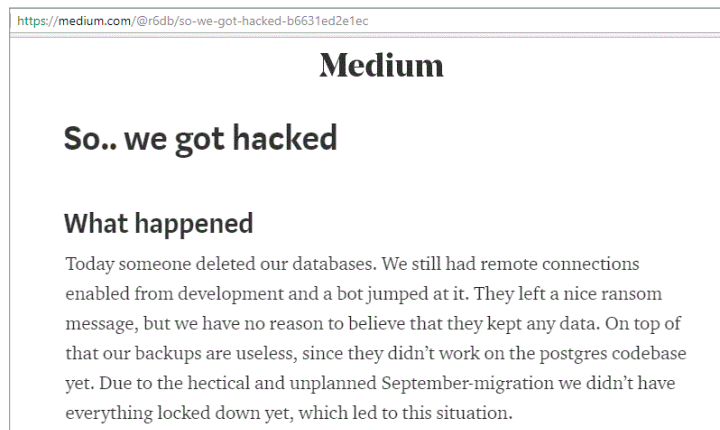
Almost every company has business systems and components whose compromise would be disastrous. For banks, the most critical and protected system is SWIFT messaging for interbank transfers. In October, attackers injected malware into the infrastructure and SWIFT terminal¹⁴ of Far Eastern International Bank, a major Taiwanese bank, and withdraw nearly USD 60 million from customer accounts to Sri Lanka, Cambodia, and the U.S. However, a prompt response succeeded in returning almost all the stolen funds. Later that month, NIC Asia Bank¹⁵ in Nepal suffered an attack, and although the attackers initiated transfers of USD 4 million via SWIFT, timely measures helped to recover USD 3.9 million.

Time is valuable for cybercriminals, who try to automate attacks as much as possible. They use bots to search for open ports on the Internet, bruteforce credentials of web-accessible devices, and identify websites running vulnerable content management systems. Most commonly, attackers target unprotected databases (found online with the help of scripts), then delete the database contents and demand a ransom for recovery.

¹⁴ taipeitimes.com/News/front/archives/2017/10/08/2003679926

¹⁵ bankinfosecurity.com/report-attackers-hacked-nepalese-banks-swift-server-a-10437

This fall, the forgetfulness of R6DB engineers resulted in loss of the gaming service's data.¹⁶ They failed to disable remote connections to a server, due to which a bot accessed the server, wiped the PostgreSQL database, and left a ransom message.



Attack on the R6DB gaming service

The march of technology has changed all areas of life, including education. Now there is no point to hiding a report card from one's parents, since they can check grades online at any time. But human nature remains unchanged and some young people have hacked school computers to change their grades. In the U.S.,¹⁷ one student bought a keystroke logger to obtain a teacher's password, changing an F to an A. Another incident occurred in Russia:¹⁸ a school student in Siberia used malware to escalate privileges in the electronic gradebook and obtain administrator rights in order to "improve" his grades. Criminal proceedings against the student started in November, with possible harsh punishment to follow.

In a discouraging trend, hackers are becoming younger. It used to be that attacks were the work of experienced programmers. But minors are becoming increasingly involved in crime, as well as receiving the punishment. The Internet is full of ads promising easy money. Teenagers fall for the bait and act as accomplices to fraud, most often by working as a money mule for moving stolen funds. Experienced cybercriminals and attack masterminds keep their hands clean by offloading the risk to others. Motivated by greed and possibly unaware of the criminality of what they are doing, these young bit players follow orders and become the main suspects when law enforcement arrives. Unfortunately, as cybercrime thrives, the situation with minors will likely continue to worsen.

Advice for companies

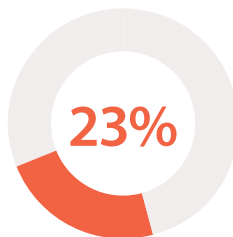
- + Enforce a strict password policy, especially for privileged accounts.
- + Encrypt and restrict access to sensitive data.
- + Minimize privileges of users and services.
- + Implement effective traffic filtering to minimize the network service interfaces accessible to external attackers.
- + Use SIEM systems for prompt detection of attacks.
- + Use a web application firewall.
- + Perform regular penetration testing to proactively identify new attack vectors and evaluate the effectiveness of protection measures.

¹⁶ medium.com/@r6db/so-we-got-hacked-b6631ed2e1ec

¹⁷ kansascity.com/news/local/article178522396.html

¹⁸ ehackingnews.com/2017/12/student-from-russian-city-vuktyl-hacked.html

WEB RESOURCES



Most affected:
U.S., Czech Republic,
and Canada



Most common attack methods:

Most severe damage:

Damage: > \$73 million



40%



24%



10%



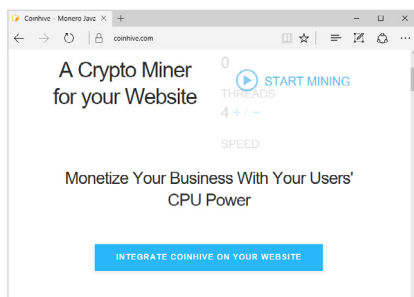
31%



24%



18%



Service for embedding a crypto miner
in web applications

When it comes to earning money from site visitors, mining cryptocurrency (by running computations on visitors' machines) may soon eclipse contextual advertising. In October, Coinhive, a service that enables website owners to earn money by embedding mining scripts on their website, fell victim to cybercriminals.¹⁹ Coinhive's DNS settings were manipulated to redirect requests for mining-related JavaScript code to the attackers' server. So instead of accruing to the website owners, cryptocurrency was mined for the benefit of the hackers instead.

Another attack scenario is to inject a mining script into the code of a compromised website. In October, visitors to the official D-Link website²⁰ who tried to download a patch to fix WPA2 vulnerabilities found themselves to be mining Monero cryptocurrency on behalf of unknown hackers.

In 2017, the hottest targets for attackers were cryptocurrency exchanges and services. In one Q4 2017 attack, hackers compromised the payment system of NiceHash,²¹ a service for buying and selling cryptocurrency mining capacity, and made off with 4,700 BTC (approximately USD 62 million) from user wallets.

↑ **Official press release statement by NiceHash** self.NiceHash
657 Submitted 12 days ago by Andrej_ID niceHASH - announcement
↓

Unfortunately, there has been a security breach involving NiceHash website. We are currently investigating the nature of the incident and, as a result, we are stopping all operations for the next 24 hours.

Importantly, our payment system was compromised and the contents of the NiceHash Bitcoin wallet have been stolen. We are working to verify the precise number of BTC taken.

Clearly, this is a matter of deep concern and we are working hard to rectify the matter in the coming days. In addition to undertaking our own investigation, the incident has been reported to the relevant authorities and law enforcement and we are co-operating with them as a matter of urgency.

Statement from NiceHash regarding theft of bitcoins

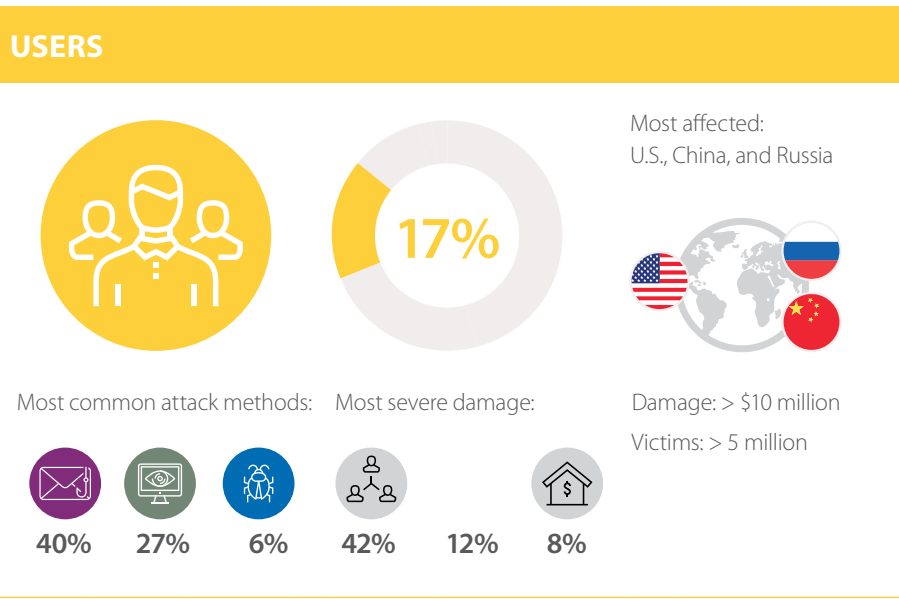
Advice for companies

- + Deploy a web application firewall for proactive protection.
- + Perform regular analysis of web application security, including source code audits.
- + Enforce a strict password policy, especially for privileged accounts.
- + Keep software up to date.
- + Practice a secure development lifecycle for web applications.
- + If holding an ICO, hire specialists to check the integrity of smart contracts and ensure cybersecurity (see ico.positive.com).

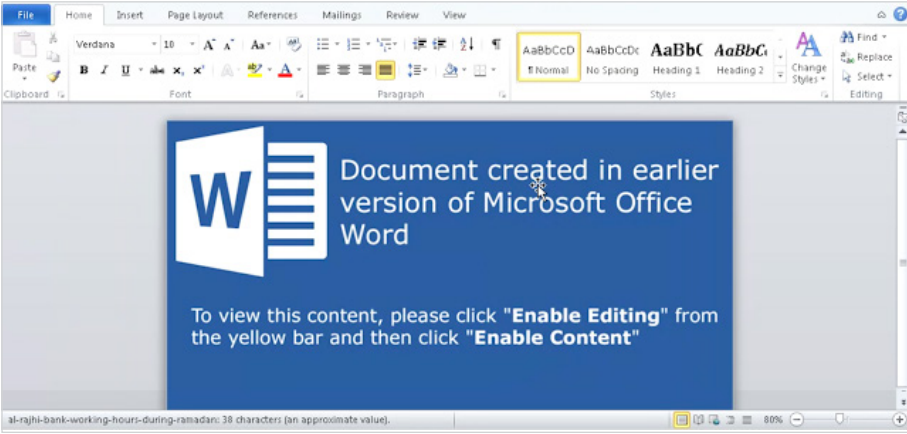
¹⁹ coinhive.com/blog/dns-breach

²⁰ seekurity.com/blog/general/d-link-middle-east-dlink-mea-website-is-secretly-mining-cryptocurrencies/

²¹ reddit.com/r/NiceHash/comments/7i0s6o/official_press_release_statement_by_nicehash/



Social engineering is the most common threat for most users. But attackers are having to think up new twists as the public becomes more security-savvy. For example, according to Cisco Talos researchers,²² attackers leveraged hacked websites to infect users with the Zeus Panda banking Trojan. This approach was unusual because the attackers used search engine optimization (SEO) to improve the position of the hacked websites in search results. Their methods included adding specific keywords to hidden pages and a SEO botnet to pump up traffic. As soon as a user opened a link to a website, a malicious script performed redirection via several other websites (thus improving their rating) and downloaded an infected Microsoft Word document to the victim's computer. If this document was opened, a macro installed the banking Trojan, capable of tracking all user activities.



Document that downloaded Zeus Panda to a victim's computer

Another popular type of attack on users consists of stealing their credentials, personal data, and credit card information. Sadly, most victims are not even aware that anything has happened. In October, the public learned of a massive data breach exposing details of more than 46 million people in Malaysia.²³ The stolen database, containing subscriber records from twelve mobile operators and the personal data of 80,000 healthcare consumers, was put up for sale on the dark web.

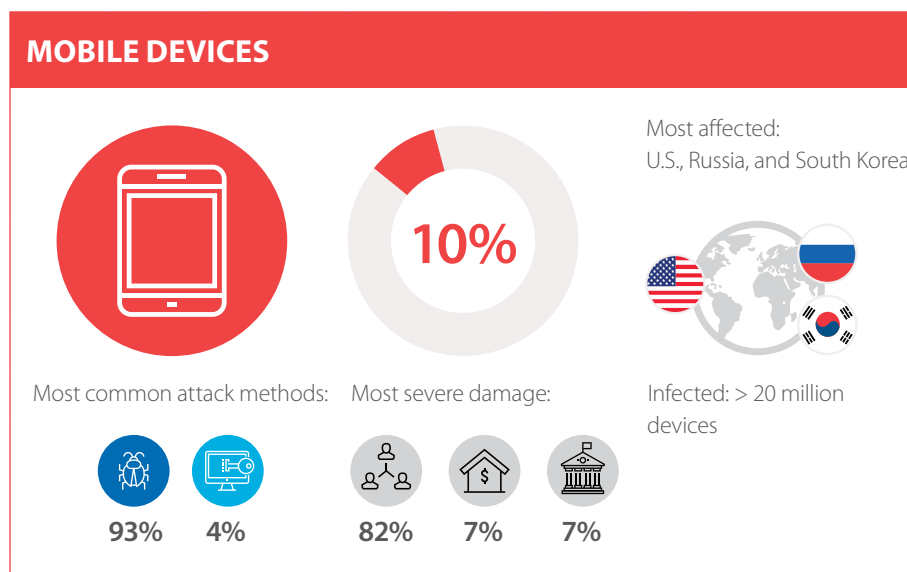
²² blog.talosintelligence.com/2017/11/zeus-panda-campaign.html
²³ bankinfosecurity.com/malaysia-stung-by-massive-data-breach-affecting-millions-a-10426

Advice for companies

- + Regularly remind customers about how to stay safe online. Provide advice for avoiding common hacker tricks. Warn clients against logging in on suspicious websites or giving out this information by email or over the phone. Instruct customers about what to do if they suspect fraud.
- + Send out-of-band notifications about security events (such as attempts to log in using the user's credentials and any online banking transactions).
- + Regularly assess web application protection, including source code audits, to detect and remediate vulnerabilities.

Tips for users

- + Use effective antivirus protection on all devices.
- + Keep software up to date.
- + Do not open unknown suspicious links, especially if a browser displays a warning.
- + Be careful on websites with invalid certificates (when a browser displays a warning) and remember that attackers can intercept any information on such sites.
- + Scan all email attachments with antivirus software.
- + Do not download files from suspicious websites or unknown sources.
- + Use complex passwords consisting of at least eight letters, numbers, and symbols. Use a password manager to create and store passwords.
- + Do not use the same password for different systems (including sites and email).
- + Change all passwords at least once every six months, or even better, every two to three months.



All attacks on mobile devices in our dataset in Q4 2017 involved malware. In most of these cases, malware made its way to the victim's phone through an official app store.

Nowadays, mobile malware tends to be multifunctional. As soon as a phone is infected, a variety of attack scenarios come into play. For example, after installing a certain skinning app for Minecraft from Google Play,²⁴ the victim's smartphone joins a botnet. Attackers used this botnet to earn money by displaying ads on infected smartphones, but could also use it for other purposes, such as DDoS attacks or renting out the botnet ("cybercrime as a service").

The LokiBot banking Trojan²⁵ can imitate the interface of a mobile bank, in order to steal credentials and access a victim's account, and also make an infected device send spam or open specific pages in a browser. If the user tries to stop LokiBot from gaining administrator rights, the Trojan acts as ransomware: it locks the screen, encrypts data, and demands a ransom payment.

²⁴ [symantec.com/connect/blogs/android-malware-google-play-adds-devices-botnet-and-performs-ddos-attacks](https://www.symantec.com/connect/blogs/android-malware-google-play-adds-devices-botnet-and-performs-ddos-attacks)

²⁵ [kaspersky.com/blog/lokibot-trojan/20030/](https://www.kaspersky.com/blog/lokibot-trojan/20030/)

Hidden cryptocurrency mining is a trend for smartphones, too. For instance, such mobile Trojans as ANDROIDOS_JSMINER, ANDROIDOS_CPUMINER, ANDROIDOS_KAGECOIN,²⁶ and their modifications use smartphone CPU capacity to mine such cryptocurrencies as Magicoin, Feathercoin, VertCoin, MyriadCoin, and Unitus. The malware was both spread through phishing SMS messages and disguised as legitimate apps on Google Play. Research found that attackers' profit was a meager USD 170.

Mining on 5 wallets , 1623 miners						
Name	Amount	Diff	Block	TTF***	Hash**	Profit*
Magicoin (m7m)	9.365 XMG	5.951	1 531 138	68 mins	6.2 Mh/s	1.12791
Feathercoin (neoscrypt)	40.01 FTC	31.559	1 938 557	3 weeks	60.8 kh/s	0.19824
VertCoin (lyra2z2)	60.03 VTC	70.983 k	813 053			0.00000
MyriadCoin (yescrypt)	250 XMY	0.204	2 224 463			0.00000
Unitus (yescrypt)	31.481 UBS	0.275	1 167 904			0.00000

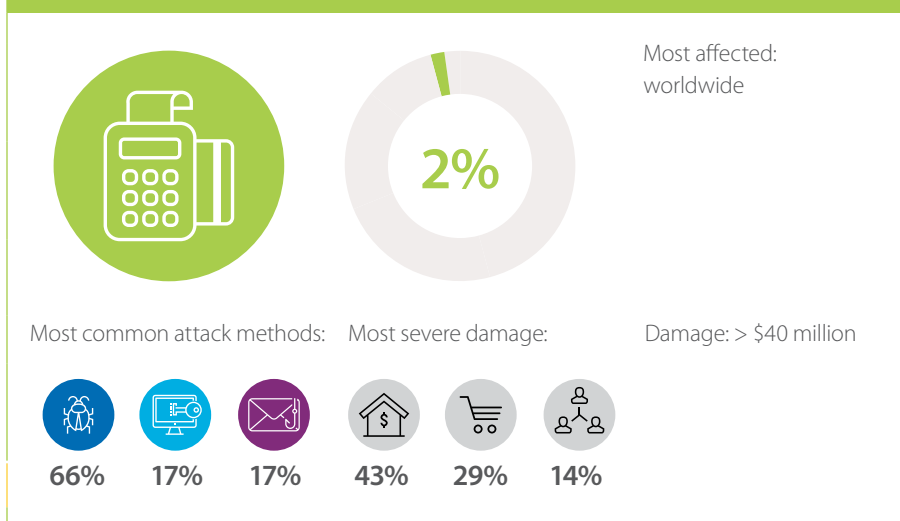
*** estimated average time to find a block at full pool speed
** approximate from the last 5 minutes submitted shares
* 24h estimation from network difficulty in mBTC/Mh/day (mBTC/Gh/day for sha256 and blake algos)

Attackers' profits from cryptocurrency mining on smartphones

Tips for users

- + Keep software up to date.
- + Do not open suspicious links, especially those received by SMS, MMS, email, or instant messenger.
- + Disable the option to download and install applications that come from unidentified developers or other untrusted sources.
- + Pay attention to the permissions requested by an application before installing it. If an application requests excessive privileges, installation may not be worth the risk of data theft.
- + Do not install unofficial firmware or root your device.
- + Do not activate autopay for your mobile phone account. It can be convenient for your phone account to be topped up when the balance dips below a certain amount. But if your phone is infected by malware that sends SMS messages to expensive premium-rate numbers, your entire bank account can be drained.
- + Use complex passwords consisting of at least eight letters, numbers, and symbols. Use a password manager to create and store passwords.
- + Do not use the same password for different systems (including sites and email).
- + Change all passwords at least once every six months, or even better, every two to three months.
- + Use two-factor authentication where possible, such as to protect email accounts.

POS TERMINALS AND ATMS



²⁶ blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

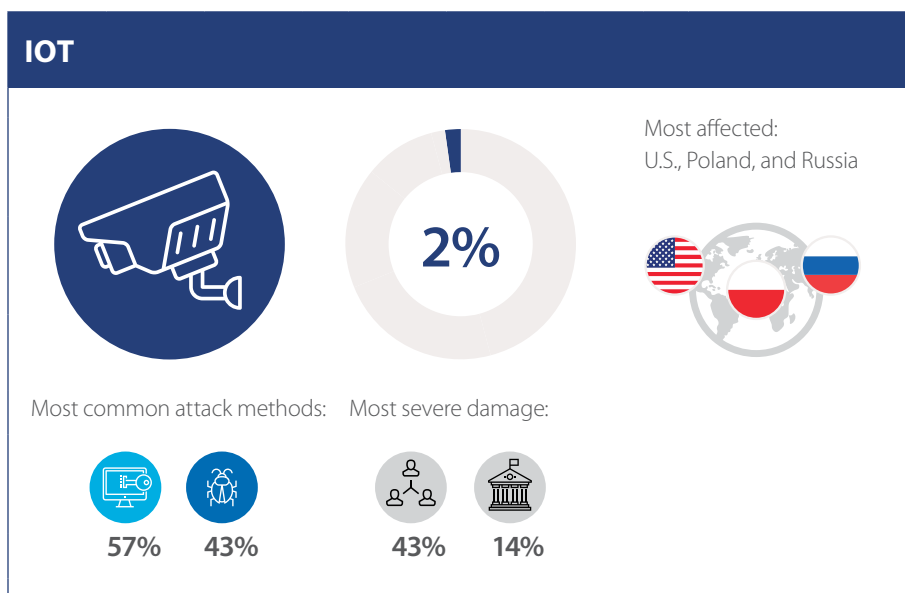
Q4 is the height of the retail season: Christmas and New Year sales attract shoppers eager for presents and discounts. Yet while everyone was preparing to celebrate the holidays, hackers were developing attacks on POS terminals and stealing credit card data. November marked the debut of GratefulPOS, a new variety of FrameworkPOS that shares some code fragments with TRINITY, BlackPOS, and BrickPOS.²⁷ The malware is installed on a POS terminal manually, most often from the intranet of a compromised company. After installation, GratefulPOS extracts payment card data from the device's RAM and sends it to a command-and-control server. The malware bypasses standard protections because it communicates with internal DNS servers instead of accessing the Internet directly.

E-commerce websites and POS terminals make an increasingly popular target for attackers. They are often poorly secured compared to online banks, making it a breeze to steal credit card information.

Vendor best practices

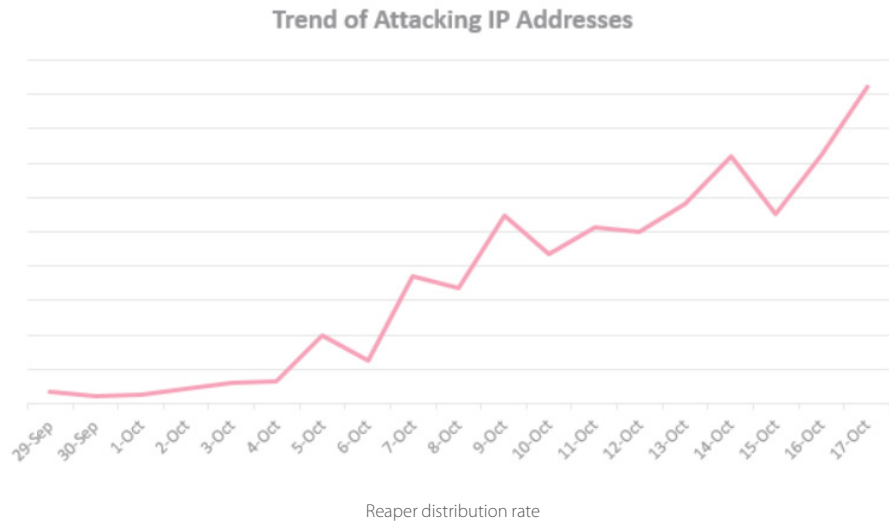
Organizations involved in development and maintenance of POS terminals, ATMs, and related software must take protective measures:

- + Use Application Control software on all ATMs.
- + Encrypt sensitive data between the device and the processing center.
- + Check integrity of incoming traffic from the processing center.
- + Ensure timely installation of updates.



IoT devices continue to join the ranks of botnet armies. In Q4, new Reaper malware became known to the public as it took over as many as 2 million devices²⁸ (including D-Link, Netgear, Linksys, AVTech, Vacron, JAWS, and GoAhead) at lightning speed. Infected devices, such as routers, video surveillance systems, IP cameras, and network drives, automatically spread the malware to other gadgets on their networks. Curiously, despite the ability of this malware to use infected devices as part of DDoS attacks, this functionality has not yet been used. In all likelihood, the botnet mastermind is waiting for the device army to grow further still. Most vendors of infected IoT devices have already issued security updates, but updating the devices is no easy task: a preset default password unknown to the user, or the absence of a usable interface, can make the process difficult.

²⁷ community.rsa.com/community/products/netwitness/blog/2017/12/08/gratefulpos-credit-card-stealing-malware-just-in-time-for-the-shopping-season
²⁸ research.checkpoint.com/new-iot-botnet-storm-coming/



Vendor best practices

- + Practice a secure development lifecycle.
- + Audit the security of IoT devices before releasing firmware.
- + Fix vulnerabilities, including those reported by users and security researchers, in a timely manner.

Advice for companies

- + Replace factory-default passwords with unique strong combinations of letters, numbers, and symbols.
- + Disconnect Internet-accessible IoT devices from critical network segments.
- + Install software updates as soon as they are released.

Tips for users

- + Change default passwords. Use complex passwords consisting of at least eight letters, numbers, and symbols.
- + Install software updates as soon as they are released.
- + Inform the vendor immediately upon finding a vulnerability.

THE BIG PICTURE

Summarizing our findings from the fourth quarter of 2017, we note the following trends:

- + Attackers are busy inventing new ways to distribute malware, including by making vulnerable websites part of their attacks.
- + To push phishing websites higher in search results, cybercriminals have started to make use of SEO in combination with special botnets. These botnets drive traffic to certain websites to improve their rating, or modify code so that a visitor is redirected to a series of websites, which increases the rating of these websites.
- + A new trend is to use ransomware not for financial profit, but to conceal the true motive of a cyberattack. The data encrypted in such attacks is usually unrecoverable.
- + Attacks on banks tend to target the SWIFT system as a way to get money out. But in most cases, banks are able to react before damage is done.
- + The face of fraud is becoming younger. More and more underage cybercriminals are getting caught by law enforcement. As cybercrime continues to thrive, the situation with youth is likely to worsen.
- + Cryptocurrency is booming: while investors pour their savings into volatile currencies, fraudsters try to mine at the expense of someone else. Users are gripped by attacks gobbling up the CPU capacity of computers, servers, and smartphones—in short, any device that can be used to mine cryptocurrency.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

© 2018 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.