POSITIVE TECHNOLOGIES

CYBERSECURITY THREATSCAPE

Q2 2017

CONTENTS

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
- Software development
- Retail
- Individuals
- Other

INTRODUCTION

While the security community was following the latest developments involving WannaCry and NotPetya cryptoware, attackers were not sitting idle. 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

Some 67 percent of attacks in the second quarter were intended to obtain direct financial profit (for example, by receiving ransoms for recovery of Trojan-encrypted user data) while another 29 percent had sensitive information as their goal.

More than half of attacks (55%) were non-targeted, and spread mainly via malware.

In Q2, attackers showed increased interest in individuals (more precisely, their money and personal data), which accounted for 24 percent of attacks.

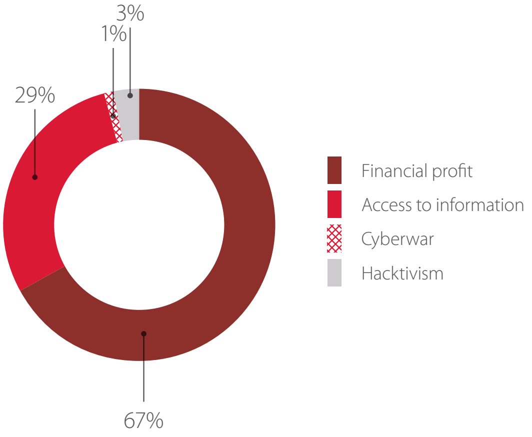


Figure 1. Attackers' motives

The U.S. and Russia remain the most frequent victims of cyberattacks. However, more than a quarter (28%) of attacks in Q2 2017 were performed en masse, with each such attack affecting systems in dozens of countries and hundreds (sometimes even thousands) of companies simultaneously. Most mass attacks included victims in diverse industries, so these have been categorized for statistical purposes as targeting Other, hence such a large number of incidents falling under this category.

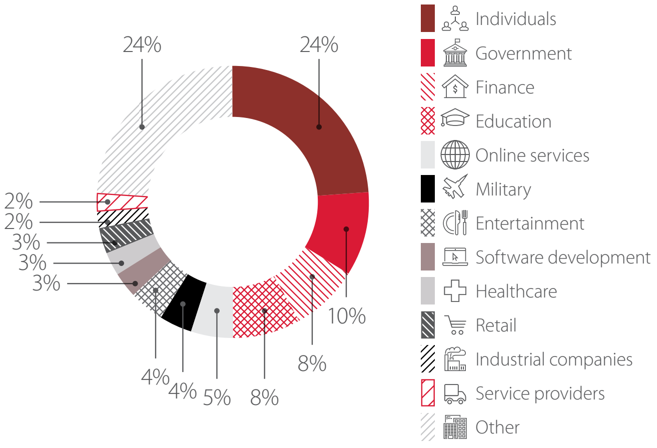


Figure 2. Categories of victims attacked in Q2 2017

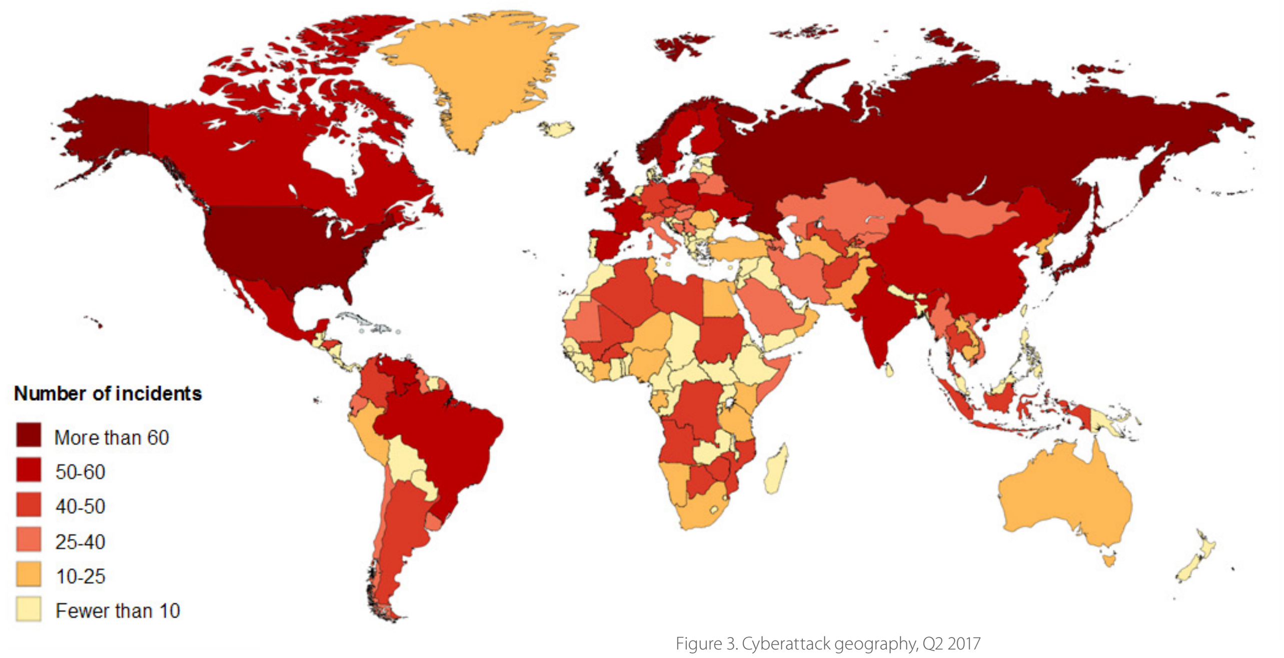


Figure 3. Cyberattack geography, Q2 2017

		Victim categories											
		Finance	Government	Healthcare	Education	Military	Industrial companies	Online services	Services	Individuals	Software development	Retail	Other
Targets	Infrastructure	5	13	4	10	7	4	2	2	8	4		27
	Web resources	9	7	1	5	1		9	2	7	2	4	3
	Users	1	1	3	3	1		1		28	1		1
	POS terminals and ATMs	3							2			3	
	Mobile devices		1			1			3	15	1		
	Network equipment and peripherals												1
	IoT												5
Methods	Use of malware	7	4	2	2	1	3		4	28	3	5	20
	Compromise of credentials	1	7	2	2	2		3	1	13	1	1	
	DDoS	2	3					1			1		1
	Social engineering	3	2		5	3			1	10	1		5
	Software vulnerabilities exploitation	2	5	2	3	2		2	1	3	2		9
	Web vulnerabilities exploitation	3	3	2	4			5	2	1		1	2
	Unknown				2	2	1	1		2			
Motives	Financial profit	16	9	8	14	1	3	10	7	37	8	5	23
	Access to information	2	12		4	7		2	2	18		1	13
	Hacktivism		3			2							1
	Cyberwar						1						

Classification of cyberincidents by motive, method, and target

INCIDENT TRENDS

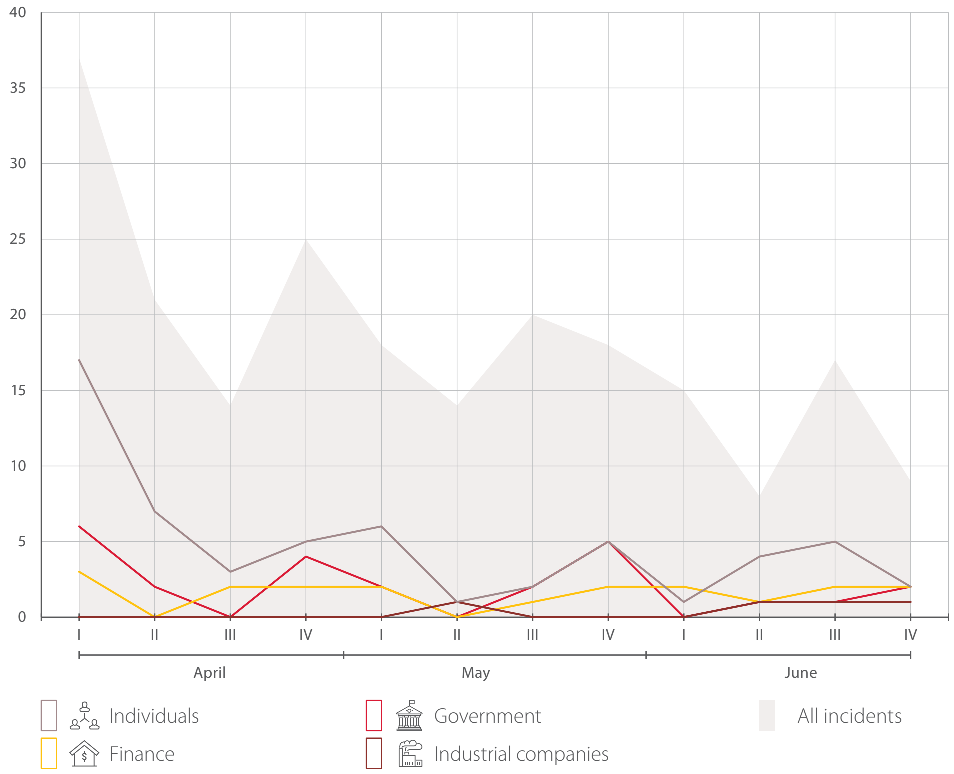


Figure 4. Number of incidents in Q2 2017

June saw a decrease in the number of unique incidents—it would seem that hackers prefer to take the summer off. At that time, the threatscape was dominated by large-scale campaigns aimed at many organizations at once. (These campaigns are treated as a single incident for analysis purposes.) Based on our 2016 observations, following a summer lull in June and July we expect that attackers will become more active in the fall (October and November), so we advise companies to keep their guard up.

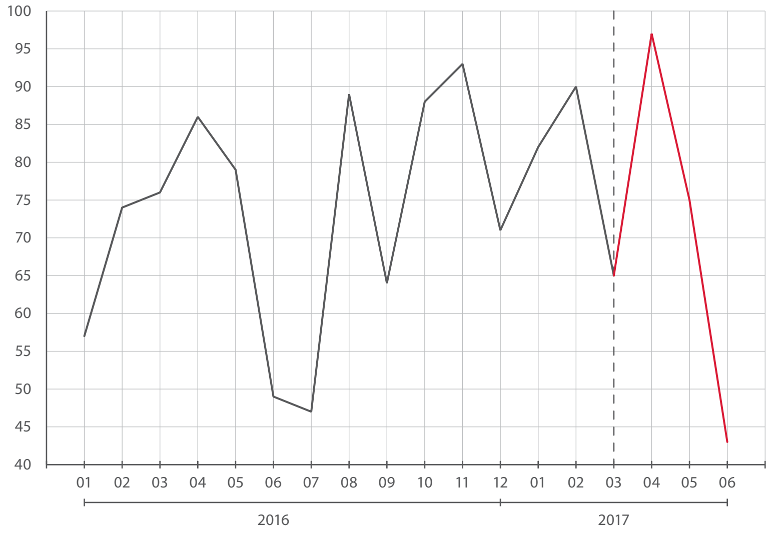


Figure 5. Number of incidents in 2016–2017

ATTACK METHODS

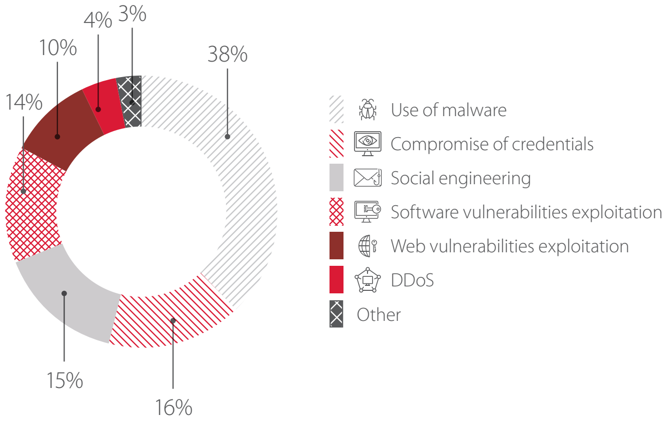
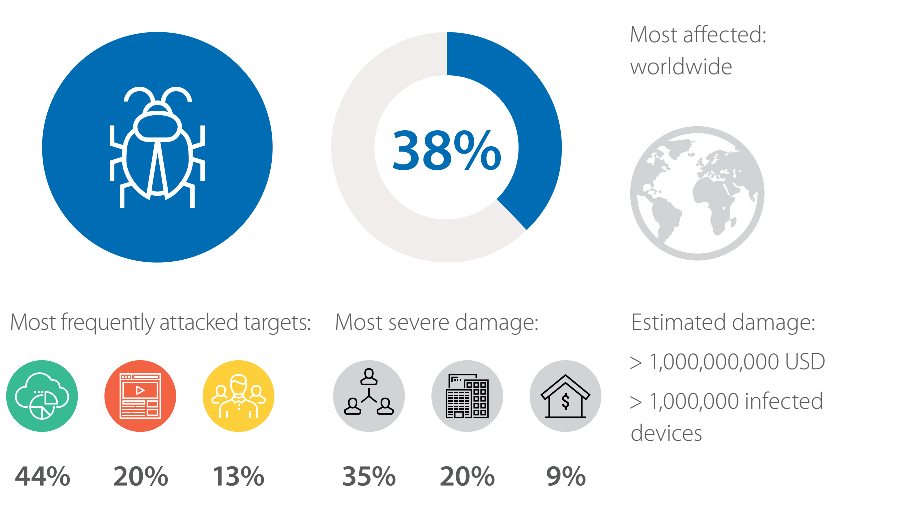


Figure 6. Cyberincidents, by attack method used

Only unique incidents are counted in our statistics. An incident includes all infections involving a particular Trojan or its strains. Overall, the number of malware-related attacks rose by 3 percent. Social engineering was used more frequently than in Q1, accounting for 15 percent of all attacks. Q2 saw a decreased number of DDoS attacks, but the appearance of new IoT botnets indicates a likely uptick in this category in Q3.

USE OF MALWARE



Ransomware, used by attackers to encrypt user data and demand payment for the decryption key, is far from new. Still, it was the most pressing topic for IT security experts in May and June 2017. Companies in at least 150 countries suffered substantial losses due to IT disruptions caused by ransomware.

The outbreak of WannaCry (WanaCypt0r, WCry)[1] proved that even savvy users who avoid suspicious messages and dubious links can still fall victim to ransomware. According to Intel,[2] the number of infected computers exceeded 530,000. Although the Bitcoin wallets of the WannaCry developers received only about 50 BTC (USD $128,000) from victims, the damage to companies exceeded $1 billion.

[1] blog.ptsecurity.com/2017/05/a-closer-look-at-cve-2017-0263.html
[2] intel.malwaretech.com/botnet/wcrypt/

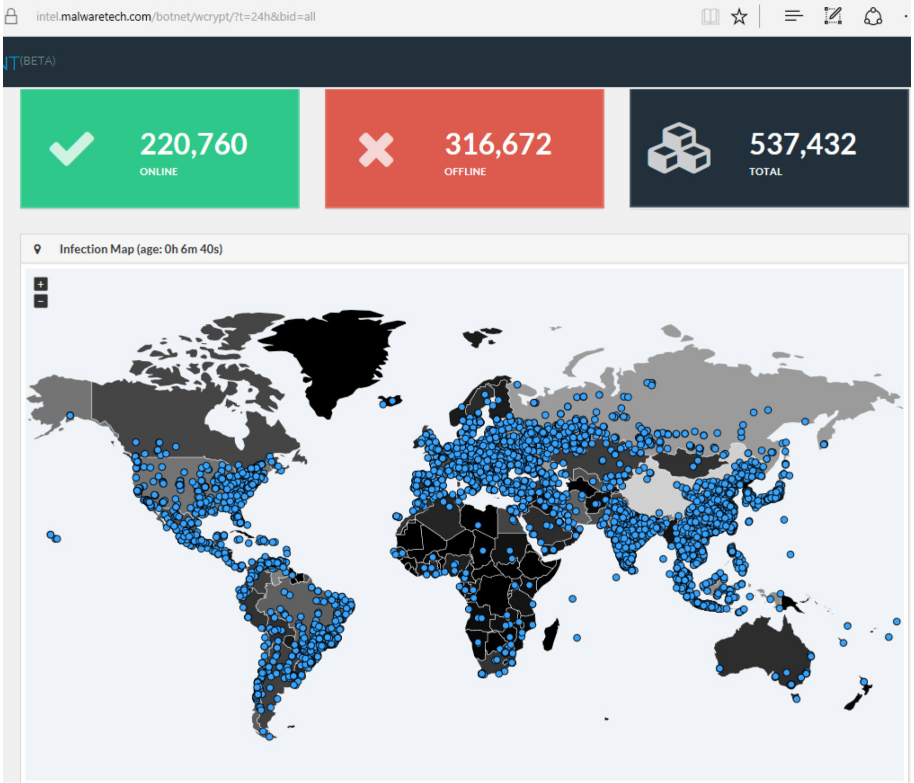

intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all
T (BETA)
220,760
ONLINE
316,672
OFFLINE
537,432
TOTAL
Infection Map (age: 0h 6m 40s)
+
−

Figure 7. WannaCry spread map

Late June saw another malware campaign, this time involving NotPetya cryptoware (also known as ExPetr, PetrWrap, Petya, or Petya.A).[3] Curiously, the attackers were not interested in financial profit. They did not attempt to send out recovery keys in return for ransom money. Instead, the malware was aimed at incapacitating systems, destroying files, and causing sabotage. However, thanks to mistakes made by the attackers in their implementation of an encryption algorithm, Positive Technologies experts were able to find a way to recover data in cases when NotPetya had administrator privileges while encrypting the entire hard drive.[4] More than 40 victims paid ransom, totaling around $10,000. NotPetya's initial infection vector[5] was aimed at Ukrainian organizations, taking advantage of a backdoor in M.E.Doc accounting software. The malware found its way into the victim's computer as part of official developer updates. Then it launched other malware on the now-infected system. Based on these facts, we can say that NotPetya was a well-planned and carefully implemented malware campaign that required compromising a software developer and its update servers, as well as obtaining access to source code.

In addition, Q2 saw an increase in the popularity of other malware, such as Jaff ransomware,[6] which is spread via .pdf files attached to spam messages, and SOREBRECT,[7] which burrows into the Windows svchost.exe process by using the legitimate utility PsExec while destroying the malicious source file.

Simultaneous with the WannaCry outbreak, we witnessed incidents caused by other malware (Adylkuzz)[8] that exploited the same vulnerability (MS17-010).[9] Adylkuzz received less media buzz, however, because it did not demand any ransom. All the same, many computers were infected while most victims remained unaware. The initial infection vector—an Internet-accessible vulnerable host with out-of-date OS and software versions—was similar to that of WannaCry. Particularly interesting was the attackers' aim: to use the computing capacity of infected PCs to mine cryptocurrency. Analyzing transactions involving a known wallet of the

[3] www.ptsecurity.com/ww-en/about/news/283096/
[4] blog.ptsecurity.com/2017/07/recovering-data-from-disk-encrypted-by.html
[5] blog.talosintelligence.com/2017/07/the-medoc-connection.html
[6] isc.sans.edu/forums/diary/Jaff+ransomware+gets+a+makeover/22446/
[7] blog.trendmicro.com/trendlabs-security-intelligence/analyzing-fileless-code-injecting-sorebrect-ransomware/
[8] securingtomorrow.mcafee.com/mcafee-labs/adylkuzz-coinminer-spreading-like-wannacry/
[9] technet.microsoft.com/en-us/library/security/ms17-010.aspx

attacker, we found that the CPU capacity controlled by the attacker would be sufficient to generate currency worth about $2,000 per day.

"Ransomware as a service", which we mentioned in our Q1 report,[10] gained momentum in Q2. New rent-a-Trojan services are emerging. For example, distributors of Petya and Mischa malware take a cut of 25 to 85 percent from the ransoms paid to attackers,[11] while Karmen[12] is available on the black market for a mere $175.

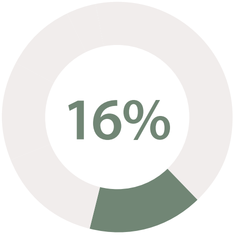
Advice for companies

- 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.

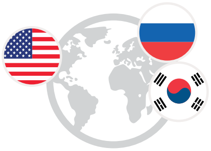
Tips for users

- 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 click links to unfamiliar or suspicious sites, especially when the browser warns that the connection is untrusted.
- Scan all email attachments with antivirus software.
- Do not download files from suspicious websites or unknown sources.

COMPROMISE OF CREDENTIALS



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



Most frequently attacked targets: 42% 36% 18%

Most severe damage: 39% 21% 9%

Estimated damage:

> 20,000,000 USD

> 1,500,000 victims

Compromising of user credentials is widespread both in targeted attacks against a company infrastructure and in various attacks against individuals. For instance, hackers may take control of social network or email accounts to send spam—or to impersonate the victim in social media posts.[13]

Ransomware goes hand in hand with cryptocurrency, because attackers prefer bitcoins for their ease and anonymity. So perhaps unsurprisingly, attacks against Bitcoin wallets have risen as well. For example, two large South Korean cryptocurrency exchanges fell victim to a massive compromise of user credentials. Attackers obtained access to the personal data of 31,800

[10] www.ptsecurity.com/upload/corporate/ww-en/analytics/Current-Cyberattacks-eng.pdf
[11] www.bleepingcomputer.com/news/security/petya-and-mischa-ransomware-affiliate-system-publicly-released/
[12] www.recordedfuture.com/karmen-ransomware-variant/
[13] news.softpedia.com/news/hacktivist-defaces-250-isis-twitter-accounts-with-adult-content-515153.shtml

Bithumb users[14] and obtained access to their accounts. Losses totaled approximately 1 billion won ($890,000). As part of an attack against Tapizon,[15] attackers gained access to four wallets and stole a total of 3,816 bitcoins ($5.3 million).

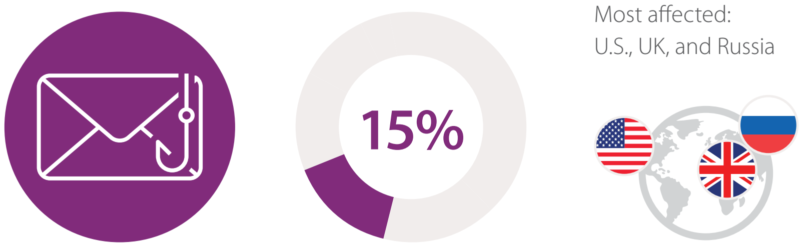
Advice for companies

- 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 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 re-use the same password for different accounts (such as 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.
- Use "cold wallets" not accessible via the Internet to store cryptocurrency. For example, paper or hardware wallets, or multi-signature or offline-signature wallets.

SOCIAL ENGINEERING



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

Most frequently attacked targets:

63% 37%

Most severe damage:

33% 17% 13%

Estimated damage:

> 50,000 USD

> 500,000 victims

Q2 2017 saw a rising number of social engineering attacks. For example, the Cobalt group—which we have been monitoring since 2016—continues to attack banks worldwide by using new techniques to penetrate target systems.[16] Their campaigns have substantially increased in scale.

Of course, not only organizations, but ordinary users are frequently tricked by attackers. As part of one phishing campaign, attackers used spam messages to lure users to fake PayPal pages.[17] On these pages, users were asked for their credit card numbers and other sensitive information. The cybercriminals could not spoof the PayPal URL, so attentive users were able to notice a dubious link. Meanwhile, less attentive users not only disclosed their banking information but also provided a selfie with their ID in hand.

[14] betanews.com/2017/07/05/bithumb-hacked/
[15] www.hackread.com/south-korean-bitcoin-exchange-yapizon-hacked/
[16] blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html
[17] phishme.com/smile-new-paypal-phish-victims-sending-selfie/

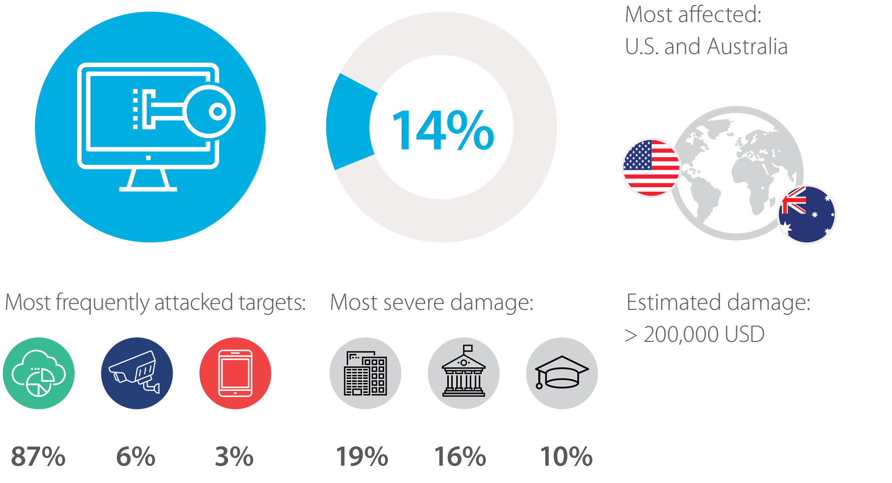
Advice for companies

- 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 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.
- Scan all email attachments with antivirus software.

SOFTWARE VULNERABILITIES EXPLOITATION



Most affected:
U.S. and Australia

Most frequently attacked targets:
87% 6% 3%

Most severe damage:
19% 16% 10%

Estimated damage:
> 200,000 USD

Although known software vulnerabilities offer plenty of opportunities for malware to perform dangerous actions on many devices, attackers keep exploiting previously unknown (zero-day) vulnerabilities.

The most popular vulnerabilities are found in Microsoft products—specifically, Microsoft Office. For instance, according to FireEye,[18] the APT28 and Turla groups used zero-day vulnerabilities in Microsoft Office to perform remote execution of arbitrary code as the initial vector for penetration of a target system. The attackers' exploit of the CVE-2017-0261 vulnerability[19] involved sending email messages with an attached Microsoft Word document that contained embedded malicious EPS content (Encapsulated PostScript is a graphics format supported by Microsoft Office). After this, using vulnerability CVE-2017-0263,[20] the attackers obtained administrator privileges and, therefore, full control of the system. This zero-day vulnerability in Windows (CVE-2017-0263) was first discovered by a Positive Technologies expert.[21]

As part of attacks against 120 Israel-based government and commercial organizations,[22] the OilRig APT group used another zero-day vulnerability in Microsoft Office—CVE-2017-0199. The exploit was spread mainly via .doc files. After a connection was established to the command server, an HTA file (disguised as an RTF file) was downloaded and run. (HTA is an HTML application that runs outside of a browser window.) Attackers could then plant various malware on the target system.

[18] www.fireeye.com/blog/threat-research/2017/05/eps-processing-zero-days.html
[19] cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0261
[20] cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0263
[21] www.securityfocus.com/bid/98258
[22] securityaffairs.co/wordpress/58464/hacking/oilrig-apt-target-israel.html

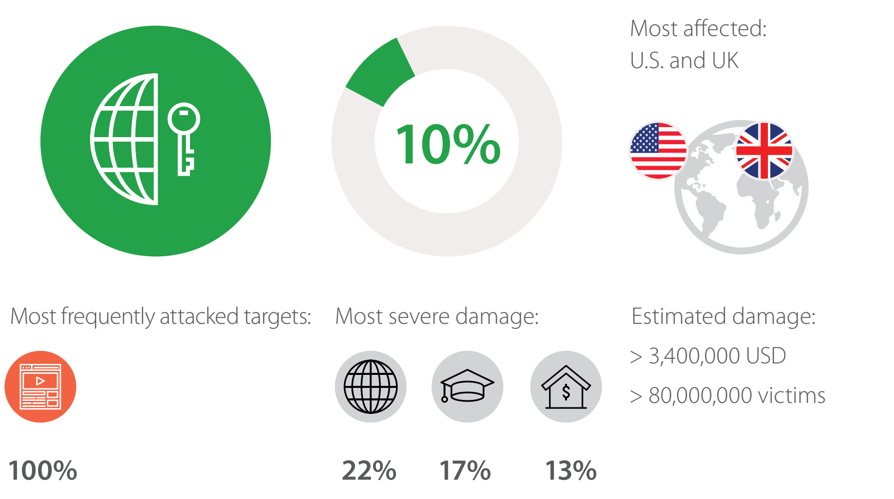
Advice for companies

- 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.[23]
- Use effective antivirus protection on all devices.

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 links to unfamiliar or suspicious sites, especially when the browser warns that the connection is untrusted.
- Scan all email attachments with antivirus software.
- Do not download files from suspicious websites or unknown sources.

WEB VULNERABILITIES EXPLOITATION



Most affected:
U.S. and UK

Most frequently attacked targets:
100%

Most severe damage:
22% 17% 13%

Estimated damage:
> 3,400,000 USD
> 80,000,000 victims

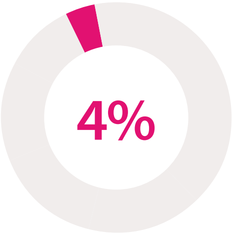
In Q2, insufficient protection of web resources resulted in leakage of confidential information belonging to more than 80 million users all over the world. The largest attack struck Edmodo, an American social network for education.[24] The attackers stole a database dump containing sensitive information on 77 million users, including their email addresses. The attack likely involved remote execution of arbitrary Python code. The stolen information was then made available on the black market for the low price of $1,000.

Advice for companies

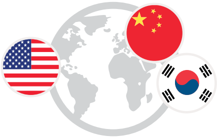
- Perform regular analysis of web application security, including source code audits.
- Deploy a web application firewall for proactive protection.[25]
- Practice a secure development lifecycle for web applications.
- Use up-to-date versions of web servers and database systems. Avoid vulnerable versions of libraries or frameworks.

[23] Lack of web application firewall is a vulnerability as per OWASP Top 10 2017.
[24] benhamouglobalventures.com/2017/06/07/deep-dive-into-the-edmodo-data-breach/
[25] Absence of a web application firewall is a vulnerability according to the updated list of Top 10 vulnerabilities from OWASP (2017).

DDOS



Most affected:
China, U.S., and South Korea



Most frequently attacked targets:

87% 13%

Most severe damage:

38% 25% 13%

Impact:
16 hours average downtime

In Q2 DDoS attacks accounted for only a small share of incidents. Researchers are detecting new botnets that consist of IoT devices, yet incidents involving high-load attacks are few and far between. This may mean that attackers are building up their botnets in preparation for massive future attacks. It may also be the case that companies victimized by DDoS attacks are reluctant to publicize this fact. For example, Skype was unavailable in Europe and part of the U.S. for two days. Although Microsoft did not discuss the cause, the service may have fallen victim to a DDoS attack. The CyberTeam group, which specializes in such attacks, claimed responsibility.[26]

Attackers continue to blackmail companies with DDoS threats. For example, several South Korean banks (KB Kookmin Bank, Shinhan Bank, Woori Bank, KEB Hana Bank, and NH Bank) were simultaneously hit by blackmailers,[27] who demanded the equivalent of around $315,000. However, as no bank downtime occurred, three possibilities remain: the threats were a mere bluff that the attackers did not have the resources to follow through with; the banks had high a level of security and repelled the attack, or they simply paid the amount demanded.

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.

[26] twitter.com/_CyberTeam_/status/876926485428305920
[27] www.scmagazineuk.com/hackers-threaten-south-korean-banks-with-ddos-attacks/article/671607/

ATTACK TARGETS

Corporate IT infrastructure and web resources are the most popular attack targets.

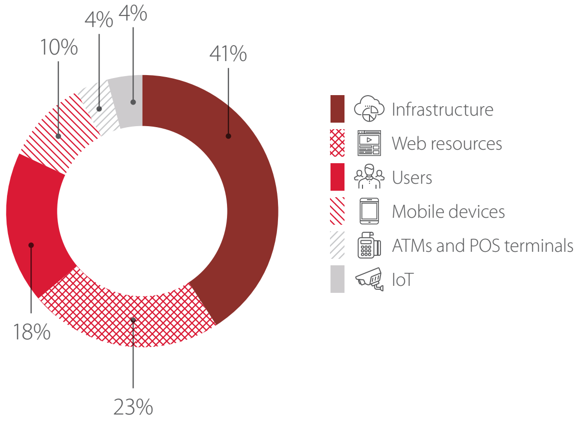
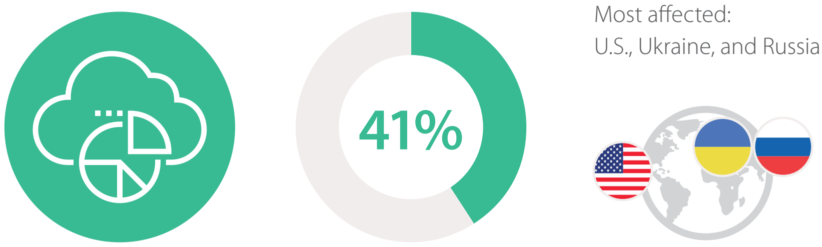


Figure 9. Cyberincidents, by attack target

Attacks against web resources fell in the second quarter (33% in Q1, 23% in Q2) while attacks against mobile devices increased (2% in Q1, 10% in Q2). In this report, we have introduced the IoT category, which primarily consists of routers, IP cameras, and DVRs.

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



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

Most common attack methods:

40% 31% 13%

Most severe damage:

27% 15% 12%

Estimated damage:
> 3,000,000 USD

In Q2, most incidents targeting IT infrastructure involved malware. However, other vectors were also used. For example, the APT10 group found an unconventional method for penetrating victims' corporate networks.[28] As part of targeted attacks, the intruders obtained access to networks of cloud service providers, after which they used the trust placed in those providers to penetrate the target company's corporate network. The attackers made use of PlugX malware and a new Trojan named RedLeaves.

The main objective of attacks on corporate infrastructure is data. But the situation with data theft may be stabilizing: an independent study by the Ponemon Institute with support from

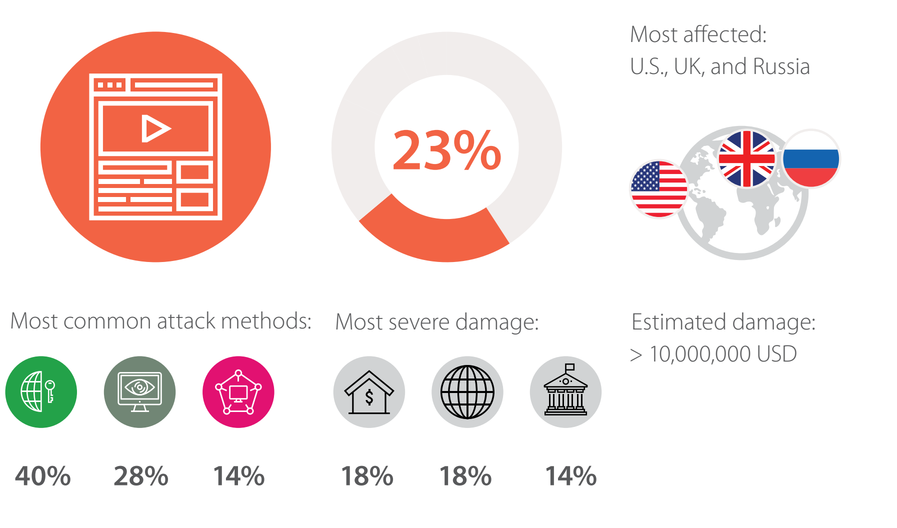
[28] baesystemsai.blogspot.ru/2017/04/apt10-operation-cloud-hopper_3.html

IBM showed that in 2017, average per-incident losses from data leaks decreased by 10 percent, to $3,620,000.[29]

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.

WEB RESOURCES



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

Most common attack methods:
40% 28% 14%

Most severe damage:
18% 18% 14%

Estimated damage:
> 10,000,000 USD

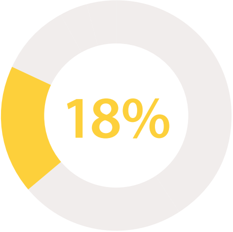
Access to sensitive information and penetration of internal corporate networks are typical outcomes of attacks against web resources. Yet in Q2 2017 we noticed a curious technique used by the Cobalt group[30] in its attacks on financial institutions. The attackers used arbitrary vulnerable sites to host malware. They placed malicious files on vulnerable websites, from which the files could be later downloaded to the victim's infrastructure. These sites served as an intermediate link in a targeted attack chain, while the sites' owners became unwitting accomplices to those attacks. 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.

Advice for companies

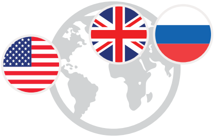
- Use a web application firewall for preventive protection.[31]
- Perform regular analysis of web application security, including source code audits.
- Enforce a strict password policy, especially for privileged accounts.
- Keep software up to date.
- Practice a secure development lifecycle for web applications.

[29] www.ibm.com/security/data-breach/
[30] blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html
[31] Lack of web application firewall is a vulnerability as per OWASP Top 10 2017.

USERS



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



Most common attack methods:

33% 30% 25%

Most severe damage:

70% 8% 8%

Estimated damage:
> 1,000,000 victims

Ordinary users often bear the brunt of cybercrime. Even if companies are the victims of first choice, users may still present a tempting target. Attackers may steal a company's database and demand a ransom from the company. But if the company refuses to pay, the attackers shift their attention to the clients whose data they obtained. This was the situation experienced by a Lithuanian plastic surgery clinic in May.[32] Tsar Team, a cybercriminal group, stole about 25,000 photos of over 1,500 of the clinic's clients. First the group demanded a ransom of 300 bitcoins (about $590,000), but the clinic refused to pay. So the criminals turned their sights to the patients, demanding from $61 to $2,200 from each.

Ordinary users are also the frequent victims of malware. Particularly curious is the motive of the attacker spreading RensenWare malware.[33] Instead of demanding bitcoins, the attacker asks the victim to score 200 million points in the game TH12: Undefined Fantastic Object. If the victim attempts to close the program, the key is destroyed and the user's data is lost forever.

Advice for companies

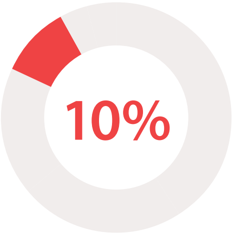
+ Regularly remind clients about how to stay safe online. Provide advice on avoiding common hacker tricks. Warn clients against logging in on suspicious websites or giving this information by email or over the phone. Explain to the clients what to do in case of suspected fraud.
+ Send out-of-band notifications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

[32] www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments
[33] www.bleepingcomputer.com/news/security/rensenware-will-only-decrypt-files-if-victim-scores-2-billion-in-th12-game/

MOBILE DEVICES



Most affected:
Russia, Austria, and UK

Most common attack methods:

76% 14% 5%

Most severe damage:

95% 5%

Q2 saw increased numbers of attacks against mobile devices due to expansion of malware campaigns.

Malware is often able to bypass the security checks of official stores (Apple App Store, Google Play) and get onto the victim's mobile device under the guise of a legitimate application. For example, Funny Videos 2017[34] and HappyTimes Videos, which were published on Google Play in April, contained a new version of BankBot malware.[35] The Trojan displayed a fake log-in window on top of the interface of a legitimate banking application, thus obtaining the user's mobile bank credentials.

All the same, files on the Internet remain the most popular way for a Trojan to make its way onto a victim's phone. Attackers often lure users into downloading malware by claiming to offer a torrent file or music. They may even convince the user that the phone is infected and antivirus "protection" is required. Malware distributors may spread download links via SMS or popular messengers (WhatsApp, Telegram, Viber) disguised as innocent advertising.

Attackers are taking advantage of the fact that mobile browsers do not fully display site URLs in the address bar. Cybercriminals register subdomains that resemble the names of trusted sites, causing a false sense of security in order to collect users' credentials. For example,[36] http://m.facebook.com----------------validate----step1.rickytaylk[dot]com/sign_in.html is actually hosted on rickytaylk.com—but based on the first part of the address (the only part visible in mobile browsers), users may think that they are on m.facebook.com.

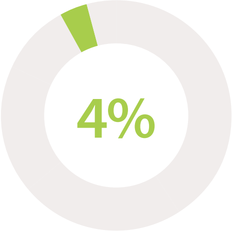
Tips for users

- 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.
- 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).

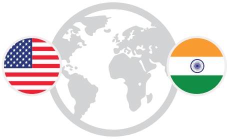
[34] www.clientsidedetection.com/banking_malware_in_google_play_targeting_many_new_apps.html
[35] twitter.com/SfyLabs/status/854055785156009984
[36] info.phishlabs.com/blog/the-mobile-phishing-threat-youll-see-very-soon-url-padding

- 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



Most affected:
U.S. and India



Most common attack methods:

🐞

100%

Most severe damage:

🏠$	🛒	🍴
38%	38%	24%

Estimated damage:
> 20,000,000 USD

Malware attacks against POS terminals and ATMs increased in the outgoing quarter. For the second time in three years, American retailer Kmart[37] fell victim to a malware infection of the company's POS terminals. Target, another American retail chain, experienced a similar attack back in 2013[38] that compromised information for around 40 million cards and forced the company to pay a total of $18 million in compensation to affected customers, payment of which ended only in May 2017.

Although attackers have come to prefer global targeted attacks against financial institutions, they are still inventing new methods and malware to steal money from ATMs. For instance, attackers in India emptied out ATMs in a matter of minutes by infecting them with a USB stick.[39] In spring of 2017, as stated by the FinCERT of Russia, financial organizations could experience a new attack with fileless banking malware, and Kaspersky Lab reported[40] on such attacks on ATMs.[41]

Vendor best practices

Organizations involved in development and maintenance of POS terminals and 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.

[37] krebsonsecurity.com/2017/05/credit-card-breach-at-kmart-stores-again/

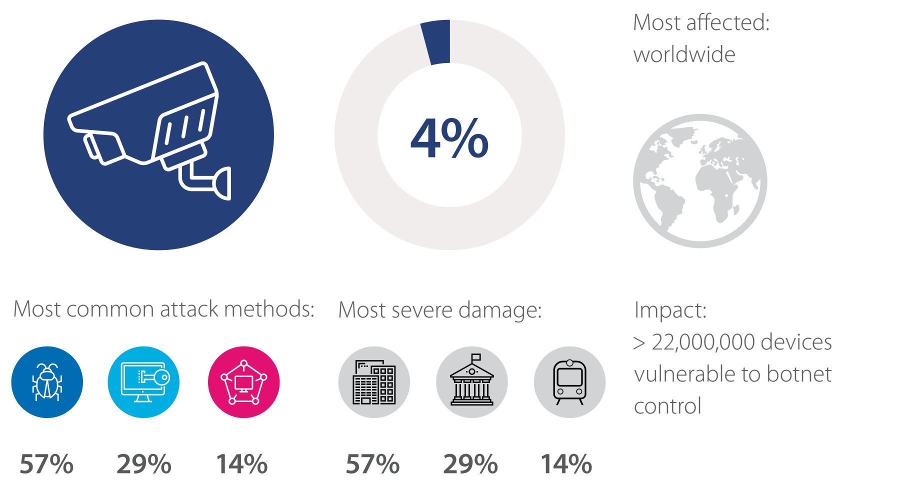
[38] www.pcworld.com/article/2087240/target-pointofsale-terminals-were-infected-with-malware.html

[39] economictimes.indiatimes.com/industry/banking/finance/banking/indian-banks-and-atms-had-a-narrow-escape-from-wannacry/articleshow/58689401.cms

[40] threatpost.com/fileless-banking-malware-attackers-break-in-cash-out-disappear/124711/

[41] Kaspersky Lab later confirmed that ATMs in Russia were not affected. Even so, the FinCERT of Russia informed financial organizations that they could suffer from such attacks in 2017.

IOT



Most affected:
worldwide

Most common attack methods:

57% 29% 14%

Most severe damage:

57% 29% 14%

Impact:
> 22,000,000 devices vulnerable to botnet control

Currently, there are over 6 billion Internet of Things devices worldwide,[42] the majority consisting of IP cameras, routers and other network devices, control and access management systems, and smart home components. Almost all IoT devices have numerous security flaws enabling attackers to obtain access to them via the Internet. Unfortunately, software developers have been rather slow to address these vulnerabilities. For example, security experts have identified several vulnerabilities in the firmware of IP cameras from a particular vendor.[43] These vulnerabilities can give attackers control over the device and access to the user's internal network. However, the vendor has not made any response to these vulnerability reports and has not offered any solution. In the meantime, a new botnet dubbed Persirai has emerged,[44] infecting 120,000 IP cameras with malware.

While IoT devices can be useful for attacking other targets as the "foot soldiers" in botnets and DDoS attacks, they can also be interesting targets in and of themselves. Attackers can virtually stalk victims (by hacking IP cameras) or simply make a nuisance for others. For instance, in April 2017 attackers in the U.S. triggered a city emergency alert system,[45] causing sirens to blare for an hour and a half in the middle of the night.

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.

[42] securelist.com/honeypots-and-the-internet-of-things/78751/

[43] images.news.f-secure.com/Web/FSecure/%7B43df9e0d-20a8-404a-86d0-70dcca00b6e5%7D_vulnerabilities-in-foscam-IP-cameras_report.pdf

[44] blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

[45] www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html

THE BIG PICTURE

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

- Non-targeted malicious campaigns may inflict harm equivalent to that of a targeted attack. With the growing momentum of "ransomware as a service" we may be on the verge of emergence of an entire ransomware market.
- The cryptocurrency boom has inspired attacks against Bitcoin wallets and exchanges.
- Researchers are finding new botnets of IoT devices, but to date there have been very few incidents with high-throughput attacks. This may be the quiet before the storm as adversaries bide their time and accumulate resources for large-scale DDoS attacks yet to come.
- Countries without dedicated cyberforces have come to understand the importance of digital security. For instance, Australia has officially announced the establishment of a military unit specialized in information warfare,[46] publishing a relevant job vacancy on a Department of Defence website.[47] "Cyber commands" are likely to emerge in other countries in the near future.

[46] www.abc.net.au/news/2017-06-30/cyber-warfare-unit-to-be-launched-by-australian-defence-forces/8665230

[47] www.defencejobs.gov.au/navy/jobs/ElectronicWarfare/

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.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com