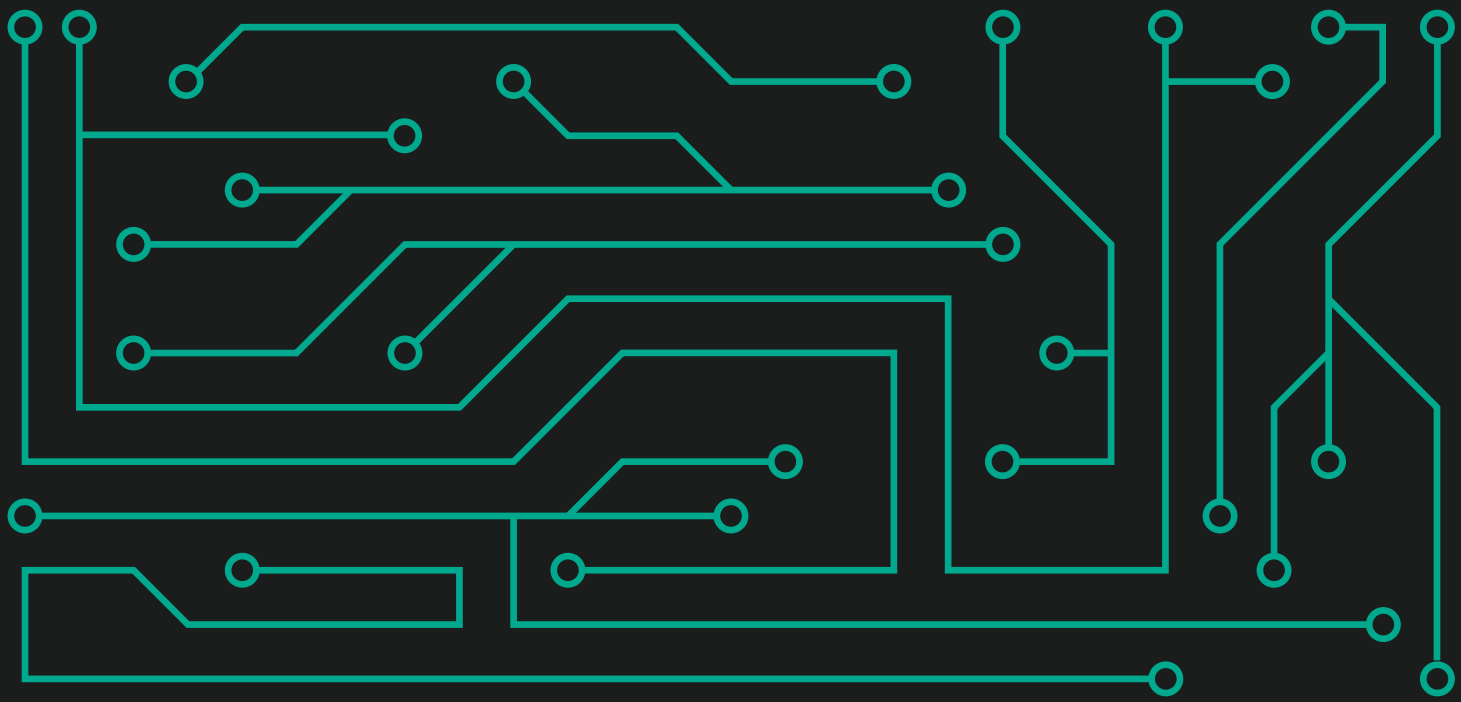
KASPERSKY lab

Kaspersky Security Bulletin 2018

STATISTICS



CONTENTS

All the statistics used in this report were obtained using Kaspersky Security Network (KSN), a distributed antivirus network that works with various anti-malware protection components. The data was collected from KSN users who agreed to provide it. Millions of Kaspersky Lab product users from 213 countries and territories worldwide participate in this global exchange of information about malicious activity. All the statistics were collected from November 2017 to October 2018.

THE YEAR IN FIGURES

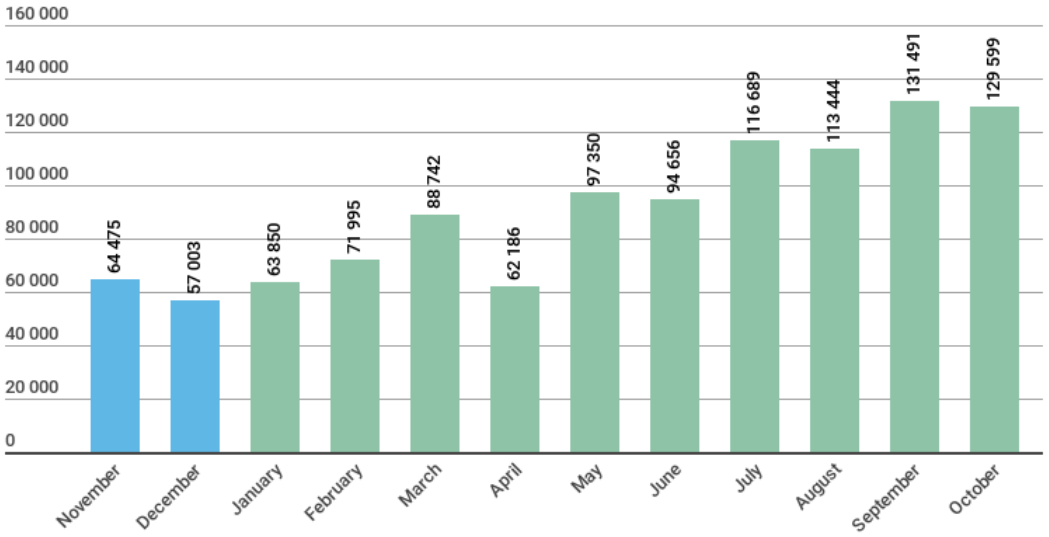
- **30.01%** of user computers were subjected to at least one Malware-class web attack over the year.
- Kaspersky Lab solutions repelled **1 876 998 691** attacks launched from online resources located all over the world.
- **554 159 621** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **21 643 946** unique malicious objects.
- **765 538** computers of unique users were targeted by encryptors.
- **5 638 828** computers of unique users were targeted by miners.
- Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **830 135** devices.

BANKING MALWARE

These statistics include not only banking malware but also malicious programs for ATMs and POS terminals. Mobile financial threats can be found in the yearly mobile report.

The number of users attacked by banking malware

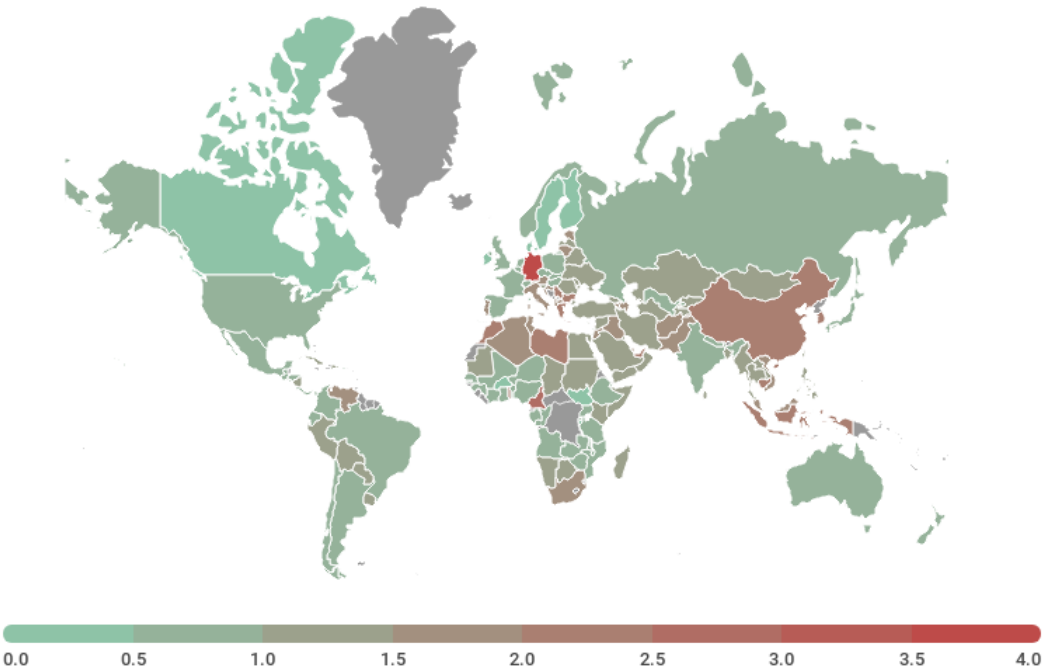
In 2018, Kaspersky Lab solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **830 135** users.



Number of unique users attacked by banking malware, November 2017 – October 2018

Geography of attacks

To evaluate and compare the risk of being infected by banking Trojans and ATM/POS malware worldwide, we calculated the share of users of Kaspersky Lab products in each country that faced this threat during the reporting period out of all users of our products in that country.



Geography of banking malware attacks, November 2017 – October 2018

TOP 10 countries by percentage of attacked users

	Country*	%**
1	Germany	4.0
2	Cameroon	2.6
3	South Korea	2.4
4	Republic of Maldives	2.4
5	Togo	2.3
6	Indonesia	2.2
7	Lebanon	2.2
8	UAE	2.1
9	Greece	2.1
10	China	2.0

** We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 10,000).*

*** Unique users attacked by banking malware in the country as a percentage of all users of Kaspersky Lab's products in that country.*

TOP 10 banking malware families

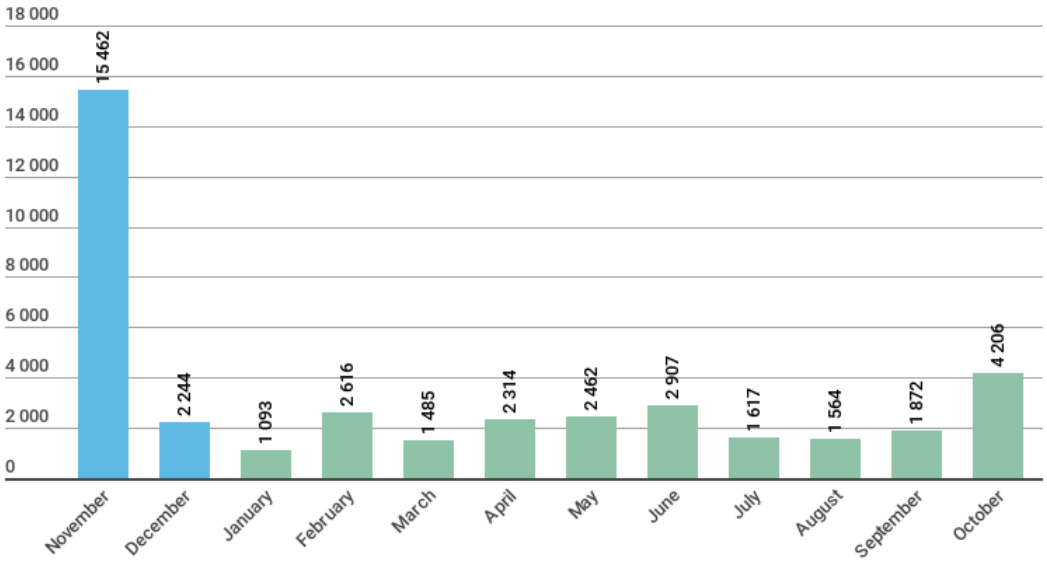
The table below shows the 10 malware families most commonly used in 2018 to attack banking users.

	Name	%*
1	Trojan.Win32. Zbot	26.3
2	Trojan.Win32. Nymaim	19.8
3	Backdoor.Win32. SpyEye	14.7
4	Backdoor.Win32. Caphaw	5.2
5	Trojan-Banker.Win32.RTM	5.2
6	Backdoor.Win32. Emotet	4.9
7	Trojan.Win32. Neurevt	3.9
8	Trojan-Banker.Win32.Tinba	1.9
9	Trojan.Win32. Gozi	1.8
10	Trojan-Banker.Win32.Trickster	1.5

** Unique users attacked by the given malware as a percentage of all users that were attacked by banking threats.*

CRYPTO-RANSOMWARE

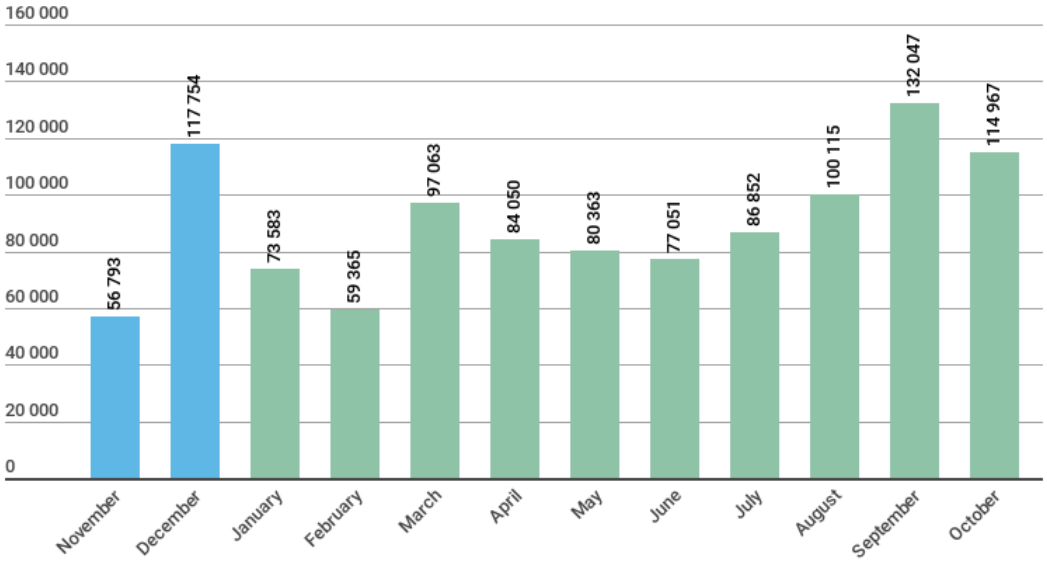
During the year, we detected **39 842** modifications of encryptors and discovered **11** new families. Note that we didn't create a new family for every new malware we found. Most threats of this type are assigned with generic verdicts that we use when detecting new and unknown samples.



Number of new crypto-ransomware modifications, November 2017 – October 2018

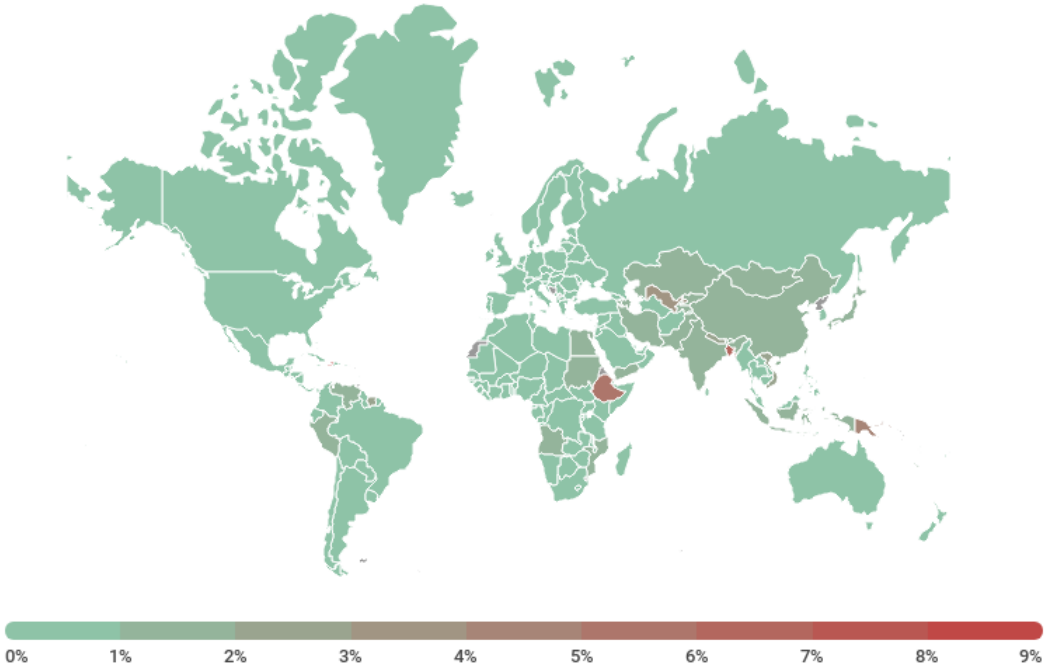
The number of users attacked by encryptors

During the reporting period, **765 538** unique KSN users were attacked by encryptors, including more than 220 thousand corporate users and more than 27 thousand SMB users.



Number of users attacked by crypto-ransomware, November 2017 – October 2018

Geography of attacks



Geography of crypto-ransomware attacks, November 2017 – October 2018

TOP 10 countries attacked by encryptors

	Country*	%**
1	Bangladesh	6.65
2	Ethiopia	5.25
3	Uzbekistan	3.50
4	Nepal	2.79
5	Vietnam	2.12
6	Indonesia	1.95
7	India	1.87

	Country*	%**
8	Angola	1.84
9	Pakistan	1.78
10	China	1.72

** We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 50,000).*

*** Unique users whose computers have been targeted by crypto-ransomware as a percentage of all unique users of Kaspersky Lab products in the country.*

TOP 10 most widespread encryptor families

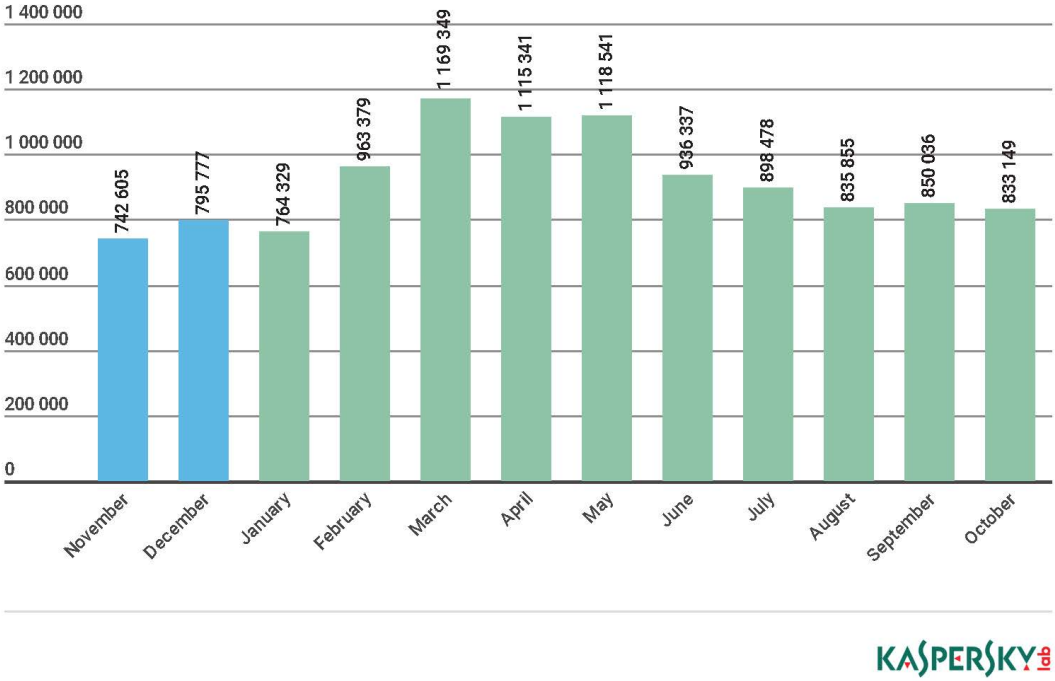
	Name	Verdict	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	29.32
2	(generic verdict)	Trojan-Ransom.Win32.Phny	11.43
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	6.67
4	Cryakl	Trojan-Ransom.Win32.Cryakl	4.59
5	PolyRansom/VirLock	Virus.Win32.PolyRansom	2.86
6	(generic verdict)	Trojan-Ransom.Win32.Gen	2.40
7	Shade	Trojan-Ransom.Win32.Shade	2.29
8	Cerber	Trojan-Ransom.Win32.Zerber	2.20
9	Purgen/GlobeImposter	Trojan-Ransom.Win32.Purgen	1.82
10	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	1.72

** Unique users whose computers have been targeted by a specific crypto-ransomware family as a percentage of all users of Kaspersky Lab products attacked by crypto-ransomware*

MINERS

The number of users attacked by miners

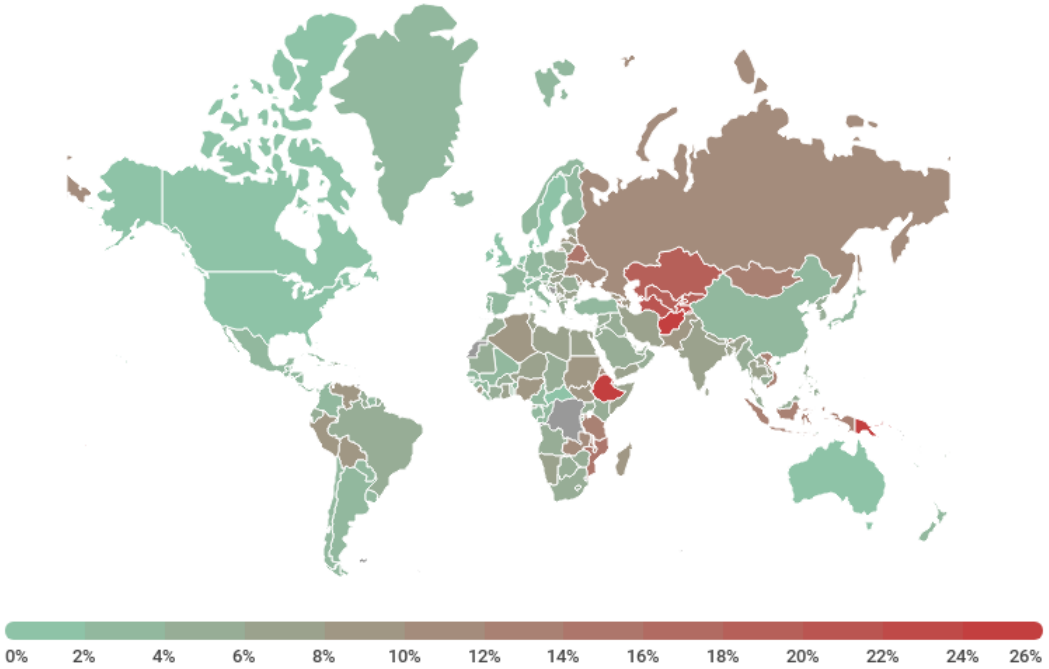
During the reporting period, **5 638 828** unique KSN users were attacked by miners. In the total volume of detections, the share of miners was 8.50%; for Risktool it was 16.88%.



Number of users attacked by miners,
November 2017 – October 2018

The most active miner this year was Trojan.JS.Miner.m; its accounted for almost 22% of the total number of users attacked by miners. It was followed by members of the Trojan.Win32.Miner family: Miner.gen (9.44%), Miner.ays (5.30%) and Miner.bbb (2.71%).

Geography of attacks



Geography of miners attacks, November 2017 – October 2018

VULNERABLE APPLICATIONS USED IN CYBERATTACKS

2018 will be remembered for the large number of targeted attacks using exploits for zero-day vulnerabilities. Notable incidents included:

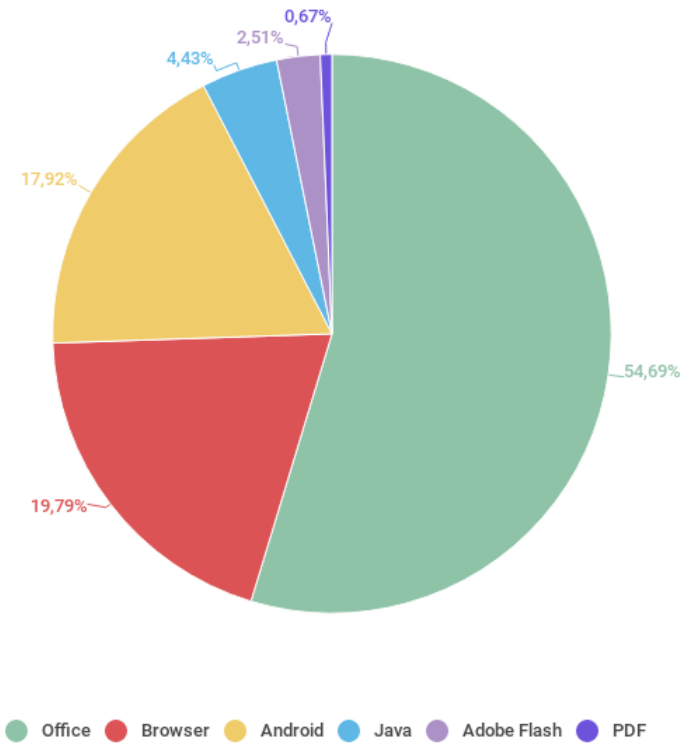
- The exploiting of vulnerabilities in Adobe Flash at the end of its lifecycle (CVE-2018-4878, CVE-2018-5002);
- The first case in a long time of Acrobat Reader vulnerability CVE-2018-4990 being exploited;
- Vulnerabilities in VBScript – one of the Windows script engines used, among others, in Internet Explorer (CVE-2018-8174, CVE-2018-8373);
- Several vulnerabilities in the win32k.sys driver that were used by cybercriminals both to escalate privileges in the Windows system and (together with other vulnerabilities) to bypass a sandbox (CVE-2018-8120, CVE-2018-8453, CVE-2018-8589).

As in the previous year, the share of users attacked by exploits for vulnerabilities in Adobe Flash Player and Internet Explorer has decreased, even though some new zero-day publicly exploited vulnerabilities have been found in both products. For example, the CVE-2018-4878 vulnerability in Adobe Flash Player, the proof-of-concept for which was released publicly by a researcher, was included in many popular exploit kits less than two months after the patch was released. Despite this, the share of these platforms in our statistics has more than halved.

The share of the exploits for Android fell to 18% (-9 p.p. compared to the previous year), which leads to the conclusion that the safety of this OS is increasing. This may be partly down to a more aggressive policy of updating devices to the latest version of the system. For example, according to our data up to October 2018, Android 8.0+ Oreo was installed on 22% of Android devices. By way of comparison, in October 2017, Android 7.0+ Nougat, the latest version of Android at that time, was used by just 16% of Android users.

At the same time, there was a significant increase in the number of users attacked by Microsoft Office exploits – four times more compared to the average for 2017. This led to an increase in the share of Microsoft Office exploits in our statistics, from 17.63% to an incredible 55%. The reason for this growth was the mass spam mailings that spread documents with exploits for vulnerabilities CVE-2017-11882 and CVE-2018-0802. Exploits for these vulnerabilities have gained popularity among cybercriminals due to their stability and ease of use – all that's required to create an exploit is to modify the exploit builder script published on a public resource. A significant role was played by the ability to implement obfuscation to avoid detection as well as wide coverage of various versions of Microsoft Office – without the patch, all versions of the office suite released over the past 18 years are vulnerable.

Exploits for the other popular vulnerabilities (CVE-2017-8570, CVE-2018-4878, CVE-2018-8174) that were distributed with MS Office documents, also played a role in increasing the share of this application in our statistics.



Distribution of exploits used in cyberattacks, by type of application attacked, November 2017 – October 2018

Vulnerable applications are ranked based on Kaspersky Lab product reports of blocked exploits used by cybercriminals both in web-borne attacks and in compromised local applications, including those on users' mobile devices.

In 2018, there were no such incidents like Shadow Brokers group's release of the Lost In Translation archive, which contains a large number of network exploits. However, the number of malicious files using exploits from this archive, as well as the number of attempts to attack using them, continued to grow: during the year, our intrusion detection component blocked 10 times more attempted attacks using the network exploit EternalBlue.

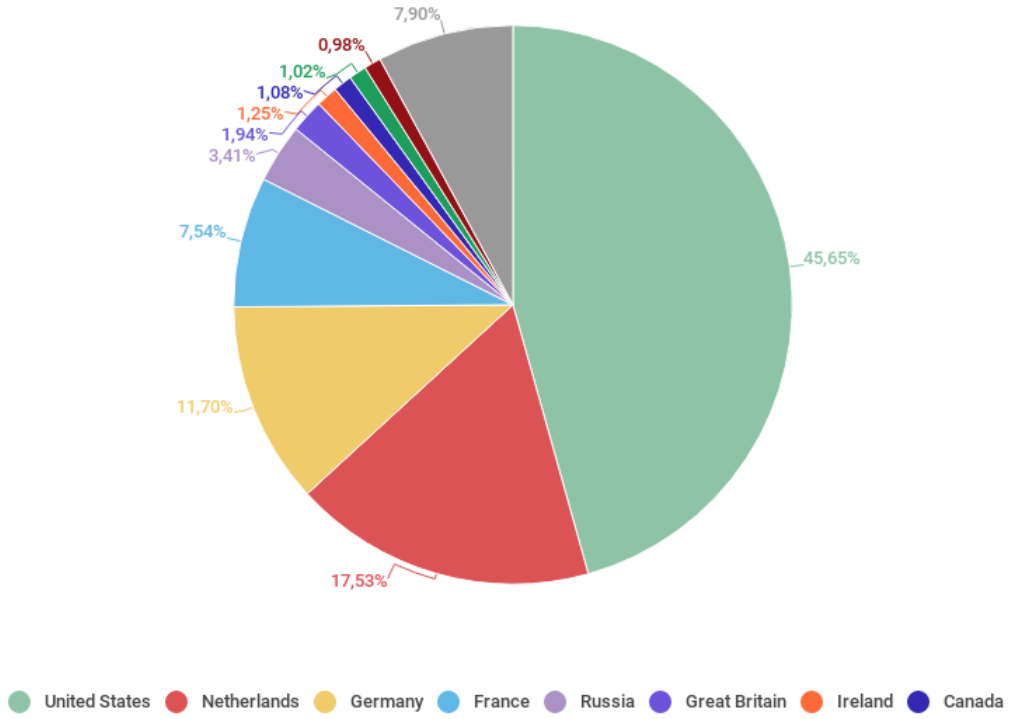
WEB-BASED ATTACKS

The statistics in this section were derived from web antivirus components that protect users from attempts to download malicious objects from a malicious/infected website. Malicious websites are deliberately created by malicious users; infected sites include those with user-contributed content (such as forums), as well as compromised legitimate resources.

Countries that are sources of web-based attacks

The following statistics are based on the physical location of the online resources used in attacks and blocked by our antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host could be the source of one or more web attacks. In order to determine the geographical source of web-based attacks, domain names are matched against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In 2018, Kaspersky Lab solutions blocked **1 876 998 691** attacks launched from web resources located in various countries around the world. **92.1%** of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries.



Distribution of web attack sources by country, November 2017 – October 2018

Compared to last year's results, the distribution of web attack sources has not changed much. The United States (45.65%) is still in first place, followed by the Netherlands (17.53%) and Germany (11.70%). Finland, Ukraine and China left the TOP 10; their places were taken by Ireland (1.25%), Luxembourg (1.02%) and Singapore (0.98%).

Countries where users face the greatest risk of online infection

In order to assess the countries in which users most often face cyberthreats, we calculated how often Kaspersky Lab users encountered detection verdicts on their machines in each country. The resulting data characterizes the risk of infection that computers are exposed to in different countries across the globe, providing an indicator of the aggressiveness of the environment facing computers in different parts of the world.

This rating only includes attacks by malicious programs that fall under the Malware class. The rating does not include web antivirus module detections of potentially dangerous or unwanted programs such as RiskTool or Adware.

Note that during the year, adware programs and their components were detected on 53% of user computers on which the web antivirus was triggered.

The TOP 20 countries where users face the greatest risk of online infection

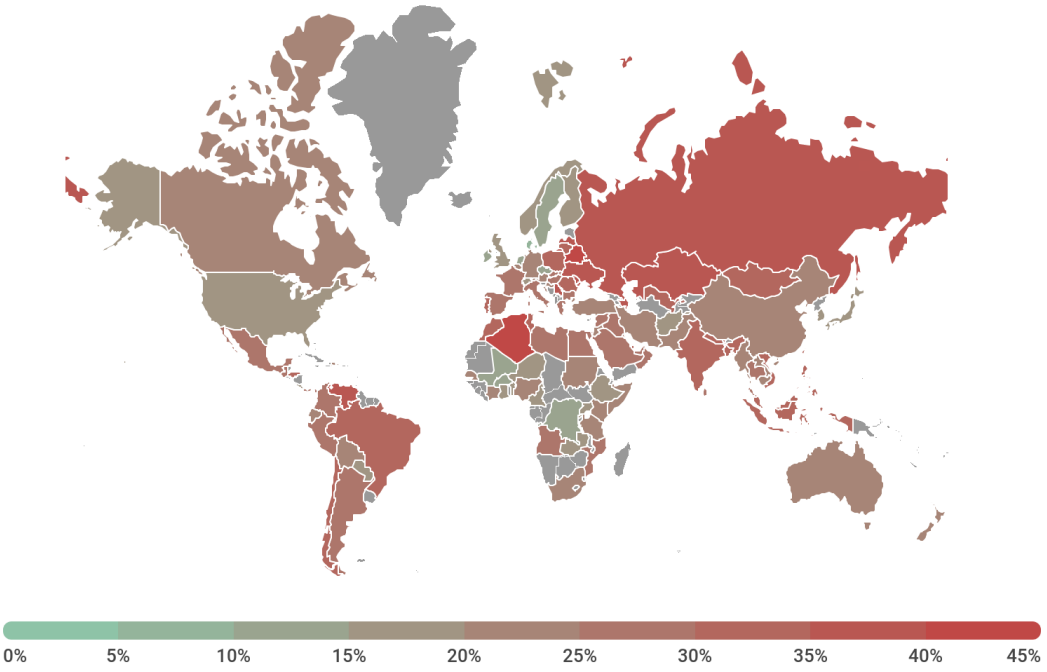
	Country*	%**
1	Algeria	43.31
2	Belarus	43.0
3	Venezuela	39.48
4	Kazakhstan	37.76
5	Moldova	37.39
6	Azerbaijan	36.82
7	Russia	36.22
8	Ukraine	35.52
9	Latvia	34.63
10	Serbia	34.62
11	Vietnam	34.45
12	Qatar	34.37
13	Tunisia	34.35
14	Indonesia	33.69
15	Romania	33.09
16	Mongolia	32.88
17	Philippines	32.81

	Country*	%**
18	Morocco	32.7
19	Brazil	31.0
20	Nepal	31.90

** We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 50,000).*

*** Unique users whose computers have been targeted by Malware-class web attacks as a percentage of all unique users of certain Kaspersky Lab products in the country*

On average, during the year a Malware-class attack was detected at least once on 30.01% of computers around the world.



Geography of malicious web attacks, November 2017 – October 2018

TOP 20 verdicts detected online

Throughout 2018, Kaspersky Lab's web antivirus detected 21 643 946 unique malicious objects (scripts, exploits, executable files, etc.) and **554 159 621** unique URLs that were blocked by web antivirus components. We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2018.

	Verdict	%*
1	Malicious URL	89.50
2	Trojan.Script.Generic	6.19
3	Trojan.Script.Miner.gen	1.95
4	Trojan.Script.Agent.gen	0.38
5	Trojan.JS.Miner.m	0.27
6	Trojan-Clicker.HTML.Iframe.dg	0.26
7	Trojan.JS.Agent.eak	0.13
8	Trojan.JS.Miner.d	0.12
9	Hoax.HTML.FraudLoad.m	0.08
10	Trojan.Win32.Miner.ays	0.06
11	Trojan-Dropper.VBS.Agent.bp	0.05
12	Trojan-Downloader.Script.Generic	0.05
13	Trojan.Win64.Shelma.a	0.04
14	Packed.Multi.MultiPacked.gen	0.04
15	Trojan.JS.Miner.x	0.04
16	Trojan.JS.Miner.y	0.04
17	Hoax.Script.Generic	0.03

	Verdict	%*
18	DangerousObject.Multi.Generic	0.03
19	Trojan.Script.Iframer	0.03
20	Trojan.JS.Agent.ecp	0.02

** The share of all malware web attacks detected on the computers of unique users.*

This year's TOP 20 includes many web miners; the Trojan.JS.Miner family boasted the biggest representation – four places out of 20. At the same time, web exploits, which were collected under the Exploit.Script.Generic verdict and which occupied 10th place last year, left the TOP 20 this time round.

LOCAL THREATS

Local infection statistics for user computers are a very important indicator: they reflect threats that have penetrated computer systems by infecting files or removable media, or initially got on the computer in an encrypted format (for example, programs integrated in complex installers, encrypted files, etc.). In addition, these statistics include objects detected on user computers after the first scan of the system by Kaspersky Lab's file antivirus.

This section contains an analysis of the statistical data obtained based on antivirus scans of files on the hard drive at the moment they are created or accessed, and the results of scanning various removable data storages.

TOP 20 malicious objects detected on user computers

For this rating, we identified the 20 most frequently detected threats on user computers in 2018. This rating does not include the Adware and Riskware classes of program.

	Verdict	%*
1	DangerousObject.Multi.Generic	32.15
2	Trojan.Script.Generic	14.46
3	Trojan.Multi.GenAutorunReg.a	5.76
4	Trojan.WinLNK.Agent.gen	4.56
5	Trojan.WinLNK.Starter.gen	3.47
6	HackTool.Win32.KMSAuto.c	3.14
7	HackTool.Win64.HackKMS.b	2.69
8	Trojan.Win32.Generic	2.56
9	Trojan.Script.Miner.gen	2.44
10	Trojan.Win32.AutoRun.gen	2.43
11	Trojan-Downloader.Script.Generic	2.33
12	Virus.Win32.Sality.gen	2.30
13	HackTool.Win32.KMSAuto.m	2.05

	Verdict	%*
14	Trojan.AndroidOS.Boogr.gsh	1.96
15	Trojan.Win32.Agentb.bqyr	1.48
16	Trojan.Win32.Miner.gen	1.41
17	Trojan.Multi.GenAutorunBITS.a	1.28
18	Trojan.Multi.Babits.genw	1.19
19	Virus.Win32.Nimnul.a	1.18
20	HackTool.MSIL.KMSAuto.ba	1.13

** The share of individual users on whose computers the file antivirus detected these programs as a percentage of all individual users of Kaspersky Lab products on whose computers any malicious program was detected.*

Traditionally, first place in our TOP 20 went to DangerousObject.Multi.Generic (32.15%), the verdict we use for malware detected using cloud-based technologies. Cloud technologies work when the antivirus databases lack the data to detect a piece of malware, but the cloud of the antivirus company already contains information about the object. This is basically how the latest malicious programs are detected.

Various variations of WinLNK malware are still being spread: Trojan.WinLNK.Agent.gen (4.56%) is in fourth place, followed immediately by Trojan.WinLNK.Starter.gen (3.47%). This malware can change the settings of the victim's browser or be used to download other malware.

Trojan.AndroidOS.Boogr.gsh (1.96%) takes 14th place; this threat is detected using machine learning technologies for Android OS malware detection.

Trojan.Multi.GenAutorunBITS.a (1.28%) and Trojan.Multi.Babits.genw (1.19%) occupy 17th and 18th places respectively. These malicious programs, like many others, use the Background Intelligent Transfer Service component to gain a foothold in the system.

Countries where users face the highest risk of local infection

For each country, we calculated the number of file antivirus detections users faced during the year. The data includes malicious programs located on user computers or on removable media connected to computers, such as flash drives, camera and phone memory cards, or external hard drives. This statistic reflects the level of infected personal computers in different countries around the world.

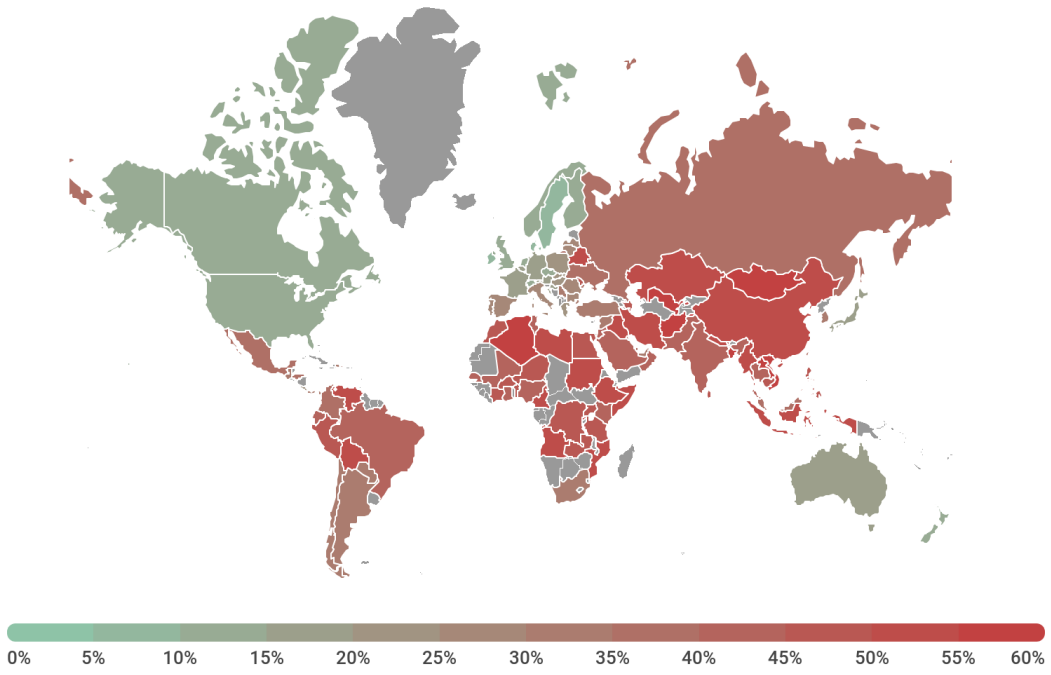
TOP 20 countries with the highest risk of local infection

	Country*	%**
1	Vietnam	62.29
2	Afghanistan	61.93
3	Uzbekistan	60.22
4	Laos	58.94
5	Mongolia	58.35
6	Algeria	58.13
7	Bangladesh	56.58
8	Rwanda	54.88
9	Syria	54.76
10	Myanmar	54.03
11	Sudan	53.77
12	Ethiopia	53.69
13	Iraq	53.5
14	Mozambique	53.31
15	Kazakhstan	53.15
16	Nepal	53.14
17	Belarus	52.38

	Country*	%**
18	Lebanon	51.92
19	Venezuela	51.18
20	China	51.17

** When calculating, we excluded countries where there are fewer than 50,000 Kaspersky Lab users.*

*** The percentage of unique users in the country with computers that blocked Malware-class local threats as a percentage of certain unique users of Kaspersky Lab products.*



Geography of local malware attacks, November 2017 – October 2018

In 2018, at least one malicious program was found on an average of 35.06% of computers, hard drives or removable media belonging to KSN users.

KASPERSKY lab

Kaspersky Security Bulletin 2018

TOP SECURITY STORIES 2018

David Emm, Victor Chebyshev

CONTENTS

INTRODUCTION

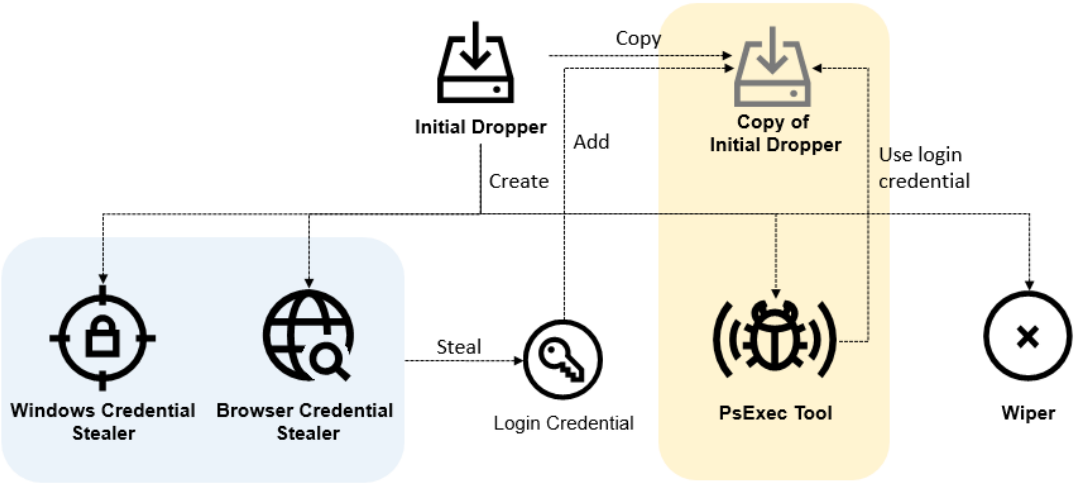
The internet is now woven into the fabric of our lives. Many people routinely bank, shop and socialize online and the internet is the lifeblood of commercial organizations. The dependence on technology of governments, businesses and consumers provides a broad attack surface for attackers with all kinds of motives – financial theft, theft of data, disruption, damage, reputational damage or simply 'for the lulz'. The result is a threat landscape that ranges from highly sophisticated targeted attacks to opportunistic cybercrime. All too often, both rely on manipulating human psychology as a way of compromising entire systems or individual computers. Increasingly, the devices targeted also include those that we don't consider to be computers – from children's toys to security cameras. Here is our annual round-up of major incidents and key trends from 2018.

TARGETED ATTACK CAMPAIGNS

At this year's Security Analyst Summit we reported on Slingshot – a sophisticated cyber-espionage platform that has been used to target victims in the Middle East and Africa since 2012. We discovered this threat – which rivals Regin and ProjectSauron in its complexity – during an incident investigation. Slingshot uses an unusual (and, as far as we know, unique) attack vector: many of the victims were attacked by means of compromised MikroTik routers. The exact method for compromising the routers is not clear, but the attackers have found a way to add a malicious DLL to the device: this DLL is a downloader for other malicious files that are then stored on the router. When a system administrator logs in to configure the router, the router's management software downloads and runs a malicious module on the administrator's computer. Slingshot loads a number of modules on a compromised computer, but the two most notable are Cahnadr and GollumApp – which are, respectively, kernel mode and user mode modules. Together, they provide the functionality to maintain persistence, manage the file system, exfiltrate data and communicate with the C2 (command-and-control) server. The samples we looked at were marked as 'version 6.x', suggesting that the threat has existed for a considerable length of time. The time, skill and cost involved in creating Slingshot indicates that the group behind it is likely to be highly organized and professional, and probably state sponsored.

Soon after the start of the Winter Olympics in Pyeongchang, we began receiving reports of malware attacks on infrastructure related to the games. OlympicDestroyer shut down display monitors, killed Wi-Fi and took down the Olympics website – preventing visitors from printing tickets. The attack also affected other organizations in the region – for example, ski gates and ski lifts were disabled at several South Korean ski resorts. OlympicDestroyer is a network worm, the main aim of which is to wipe files from remote network shares of its victims. In the days that followed the attack, research teams and media companies around the world variously attributed the attack to Russia, China and North Korea – based on a number of features previously attributed to cyber-espionage and sabotage groups allegedly based in those countries or working for the governments of those countries. Our own researchers were also trying to understand which group was behind the attack. At one stage during our research, we discovered something that seemed to indicate that the Lazarus group was behind the attack. We found a unique trace left by the attackers that exactly matched a previously known Lazarus malware component. However, the lack of obvious motive and inconsistencies with known Lazarus TTPs (tactics, techniques and procedures) that we found

during our on-site investigation at a compromised facility in South Korea led us to look again at this artefact. When we did so, we discovered that the set of features didn't match the code – it had been forged to perfectly match the fingerprint used by Lazarus. So we concluded that the 'fingerprint' was a very sophisticated false flag, intentionally placed inside the malware in order to give threat hunters the impression that they had found a 'smoking gun' and diverting them from a more accurate attribution.

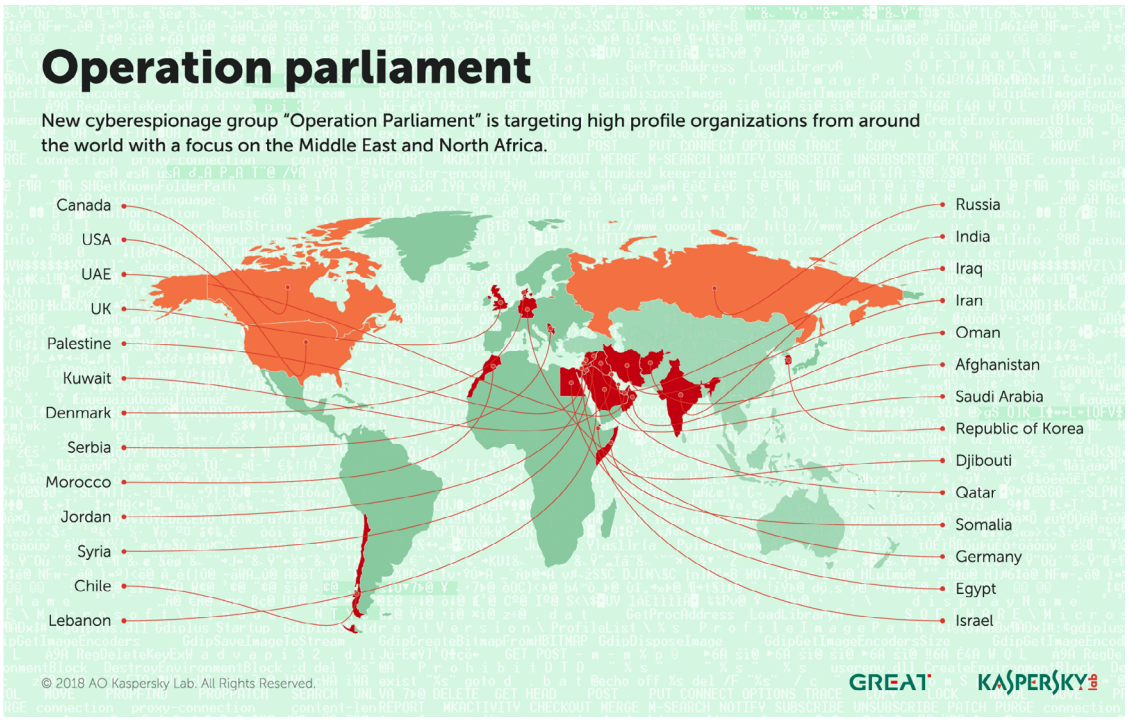


OlympicDestroyer component relations

We continued to track this APT group's activities and noticed in June that they had started a new campaign with a different geographical distribution and using new themes. Our telemetry, and the characteristics of the spear-phishing documents we analysed, indicated that the attacker behind OlympicDestroyer was targeting financial and biotechnology-related organizations based in Europe – specifically, Russia, the Netherlands, Germany, Switzerland and Ukraine. The earlier OlympicDestroyer attacks – designed to destroy and paralyze the infrastructure of the Winter Olympic Games and related supply chains, partners and venues – were preceded by a reconnaissance operation. This suggested to us that the new activities were part of another reconnaissance stage that would be followed by a wave of destructive attacks with new motives. The variety of financial and non-financial targets could indicate that the same malware was being used by several groups with different interests. This could also be the result of cyberattack

outsourcing, which is not uncommon among nation-state threat actors. However, it's also possible that the financial targets are another false-flag operation by a threat actor that has already shown that they excel at this.

In April, we reported the workings of Operation Parliament, a cyber-espionage campaign aimed at high-profile legislative, executive and judicial organizations around the world – with its main focus in the Middle East and North Africa region, especially Palestine. The attacks, which started early in 2017, targeted parliaments, senates, top state offices and officials, political science scholars, military and intelligence agencies, ministries, media outlets, research centers, election commissions, Olympic organizations, large trading companies and others. The targeting of victims was unlike that of previous campaigns in the region (Gaza Cybergang or Desert Falcons) and points to an elaborate information-gathering exercise that was carried out prior to the attacks (physical and/or digital). The attackers have been particularly careful to verify victim devices before proceeding with the infection, safeguarding their C2 servers. The attacks slowed down after the start of 2018, probably because the attackers achieved their objectives.



We have continued to track the activities of Crouching Yeti (aka Energetic Bear), an APT group that has been active since at least 2010, mainly targeting energy and industrial companies. The group targets organizations around the world, but with a particular focus on Europe, the US and Turkey – the latter being a new addition to the group's interests during 2016-17. The group's main tactics include sending phishing emails with malicious documents and infecting servers for different purposes, including hosting tools and logs and watering-hole attacks. Crouching Yeti's activities against US targets have been publicly discussed by US-CERT and the UK National Cyber Security Centre (NCSC). In April, Kaspersky Lab ICS CERT provided information on identified servers infected and used by Crouching Yeti and presented the findings of an analysis of several web servers compromised by the group during 2016 and early 2017. You can read the full report here, but below is a summary of our findings.

1. With rare exceptions, the group's members get by with publicly available tools. The use of publicly available utilities by the group to conduct its attacks renders the task of attack attribution without any additional group 'markers' very difficult.
2. Potentially, any vulnerable server on the internet is of interest to the attackers when they want to establish a foothold in order to develop further attacks against target facilities.
3. In most cases that we have observed, the group performed tasks related to searching for vulnerabilities, gaining persistence on various hosts, and stealing authentication data.
4. The diversity of victims may indicate the diversity of the attackers' interests.
5. It can be assumed with some degree of certainty that the group operates in the interests of or takes orders from customers that are external to it, performing initial data collection, the theft of authentication data and gaining persistence on resources that are suitable for the attack's further development.

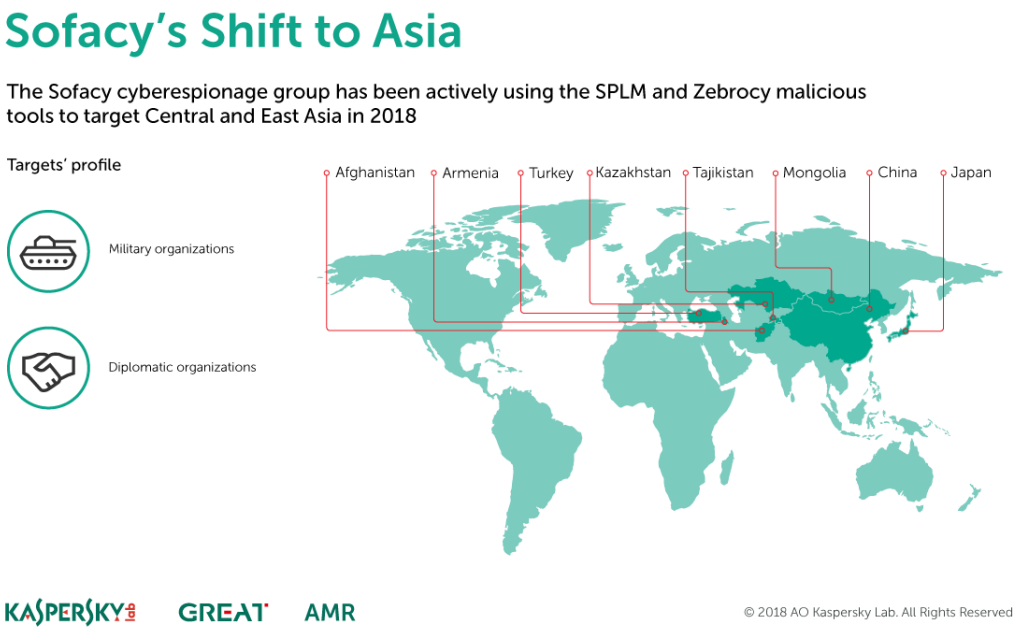
In May, researchers from Cisco Talos published the results of their research into VPNFilter, malware used to infect different brands of router – mainly in Ukraine, although affecting routers in 54 countries in total. You can read their analysis here and here. Initially, they believed that the malware had infected around 500,000 routers – Linksys, MikroTik, Netgear and TP-Link networking equipment in the small office/home office (SOHO) sector, and QNAP network-attached storage (NAS) devices. However, it later became clear that the list of infected routers was much longer – 75 in total, including ASUS, D-Link, Huawei,

Ubiquiti, UPVEL and ZTE. The malware is capable of bricking the infected device, executing shell commands for further manipulation, creating a TOR configuration for anonymous access to the device or configuring the router's proxy port and proxy URL to manipulate browsing sessions. However, it also spreads into networks supported by the device, thereby extending the scope of the attack. Researchers from our Global Research and Analysis Team (GReAT) took a detailed look at the C2 mechanism used by VPNFilter. One of the interesting questions is who is behind this malware. Cisco Talos indicated that a state-sponsored or state affiliated threat actor is responsible. In its affidavit for sink-holing the C2, the FBI suggests that Sofacy (aka APT28, Pawn Storm, Sednit, STRONTIUM, and Tsar Team) is the culprit. There is some code overlap with the BlackEnergy malware used in previous attacks in Ukraine (the FBI's affidavit makes it clear that they see BlackEnergy (aka Sandworm) as a sub-group of Sofacy).

Sofacy is a highly active and prolific cyber-espionage group that Kaspersky Lab has been tracking for many years. In February, we published an overview of Sofacy activities in 2017, revealing a gradual move away from NATO-related targets at the start of 2017, towards targets in the Middle East, Central Asia and beyond. Sofacy uses spear-phishing and watering-hole attacks to steal information, including account credentials, sensitive communications and documents. This threat actor also makes use of zero-day vulnerabilities to deploy its malware.

Sofacy deploys different tools for different target profiles. Early in 2017 the group's Dealer's Choice campaign was used to target military and diplomatic organizations (mainly in NATO countries and Ukraine). Later in the year, the group used other tools from its arsenal, Zebrocy and SPLM, to target a broader range of organizations, including science and engineering centers and press services, with more of a focus on Central Asia and the Far East. Like other sophisticated threat actors, Sofacy continually develops new tools, maintains a high level of operational security and focuses on making its malware hard to detect. Once any signs of activity by an advanced threat actor such as Sofacy have been found in a network, it's important to review logins and unusual administrator access on systems, thoroughly scan and sandbox incoming attachments, and maintain two-factor authentication for services such as email and VPN access. The use of APT intelligence reports, threat hunting tools such as YARA and advanced detection solutions such as KATA (Kaspersky Anti Targeted Attack Platform) will help you to understand their targeting and provide powerful ways of detecting their activities.

Our research shows that Sofacy is not the only threat actor operating in the Far East and this sometimes results in a target overlap between very different threat actors. We have seen cases where the Sofacy Zebrocy malware has competed for access to victims' computers with the Russian-speaking Mosquito Turla clusters; and where its SPLM backdoor has competed with the traditional Turla and Chinese-speaking Danti attacks. The shared targets included government administration, technology, science and military-related organizations in or from Central Asia. The most intriguing overlap is probably that between Sofacy and the English-speaking threat actor behind the Lamberts family. The connection was discovered after researchers detected the presence of Sofacy on a server that threat intelligence had previously identified as compromised by Grey Lambert malware. The server belongs to a Chinese conglomerate that designs and manufactures aerospace and air defense technologies. However, in this case the original SPLM delivery vector remains unknown. This raises a number of hypothetical possibilities, including the fact that Sofacy could be using a new, and as yet undetected, exploit or a new strain of its backdoor, or that Sofacy somehow managed to harness Grey Lambert's communication channels to download its malware. It could even be a false flag, planted during the previous Lambert infection. We think that the most likely answer is that an unknown new PowerShell script or legitimate but vulnerable web app was exploited to load and execute the SPLM code.



In June, we reported an ongoing campaign targeting a national data centre in Central Asia. The choice of target was especially significant – it means that the attackers were able to gain access to a wide range of government resources in one fell swoop. We think they did this by inserting malicious scripts into the country's official websites in order to conduct watering-hole attacks. We attribute this campaign to the Chinese-speaking threat actor, LuckyMouse (aka EmissaryPanda and APT27) because of the tools and tactics used in the campaign, because the C2 domain – 'update.iaacstudio[.]com' – was previously used by this group and because they have previously targeted government organizations, including Central Asian ones. The initial infection vector used in the attack against the data center is unclear. Even where we observed LuckyMouse using weaponized documents with CVE-2017-118822 (Microsoft Office Equation Editor, widely used by Chinese-speaking actors since December 2017), we couldn't prove that they were related to this particular attack. It's possible that the attackers used a watering hole to infect data center employees.

We reported another LuckyMouse campaign in September. Since March, we had found several infections where a previously unknown Trojan was injected into the 'lsass.exe' system process memory. These implants were injected by the digitally signed 32- and 64-bit network filtering driver NDISProxy. Interestingly, this driver is signed with a digital certificate that belongs to the Chinese company LeagSoft, a developer of information security software based in Shenzhen, Guangdong. We informed the company about the issue via CN-CERT. This campaign targeted Central Asian government organizations and we believe the attack was linked to a high-level meeting in the region. The choice of the Earthworm tunneler used in the attack is typical for Chinese-speaking actors. Also, one of the commands used by the attackers ('-s rssocks -d 103.75.190[.]28 -e 443') creates a tunnel to a previously known LuckyMouse C2 server. The choice of victims in this campaign also aligns with the previous interests shown by this threat actor. We did not see any indications of spear-phishing or watering-hole activity: and we think that the attackers spread their infectors through networks that were already compromised.

Lazarus is a well-established threat actor that has conducted cyber-espionage and cybersabotage campaigns since at least 2009. In recent years, the group has launched campaigns against financial organizations around the globe. In August we reported that the group had successfully compromised several banks and infiltrated a number of global crypto-currency exchanges and fintech companies.

While assisting with an incident response operation, we learned that the victim had been infected with the help of a Trojanized crypto-currency trading application that had been recommended to the company over email. An unsuspecting employee had downloaded a third-party application from a legitimate looking website, infecting their computer with malware known as Fallchill, an old tool that Lazarus has recently started using again. It seems as though Lazarus has found an elaborate way to create a legitimate looking site and inject a malicious payload into a 'legitimate looking' software update mechanism – in this case, creating a fake supply chain rather than compromising a real one. At any rate, the success of the Lazarus group in compromising supply chains suggests that it will continue to exploit this method of attack. The attackers went the extra mile and developed malware for non-Windows platforms – they included a Mac OS version and the website suggests that a Linux version is coming soon. This is probably the first time that we've seen this APT group using malware for Mac OS. It looks as though, in the chase after advanced targets, software developers from supply chains and some high-profile targets, threat actors are forced to develop Mac OS malware tools. The fact that the Lazarus group has expanded its list of targeted operating systems should be a wake-up call for users of non-Windows platforms. You can read our report on Operation AppleJeus here.

Turla (aka Venomous Bear, Waterbug, and Uroboros) is best known for what was, at the time, an ultra-complex Snake rootkit focused on NATO-related targets. However, this threat actor's activity is much broader. In October, we reported on the Turla group's recent activities, revealing an interesting mix of old code, new code, and new speculations as to where they will strike next and what they will shed. Much of our 2018 research focused on the group's KopiLuwak JavaScript backdoor, new variants of the Carbon framework and Meterpreter delivery techniques. Other interesting aspects were the changing Mosquito delivery techniques, customized PoshSec-Mod open-source PowerShell use and borrowed injector code. We tied some of this activity together with infrastructure and data points from WhiteBear and Mosquito infrastructure and activity in 2017 and 2018. One interesting aspect of our research was the lack of ongoing targeting overlap with other APT activity. Turla was absent from the milestone DNC hack event – where Sofacy and CozyDuke were both present – but the group was quietly active around the globe on other projects. This provides some insight into the ongoing motivations and ambitions of the group. It is interesting that data related to these organizations has not been weaponized and found online while

this Turla activity quietly carries on. Both Mosquito and Carbon projects focus mainly on diplomatic and foreign affairs targets, while WhiteAtlas and WhiteBear activity stretched across the globe to include organizations related to foreign affairs, but not all targeting has consistently followed this profile: the group also targeted scientific and technical centres, along with organizations outside the political arena. The group's KopiLuwak activity does not necessarily focus on diplomatic and foreign affairs. Instead, 2018 activity targeted government-related scientific and energy research organizations and a government-related communications organization in Afghanistan. This highly selective but wider targeting set will probably continue into 2019.

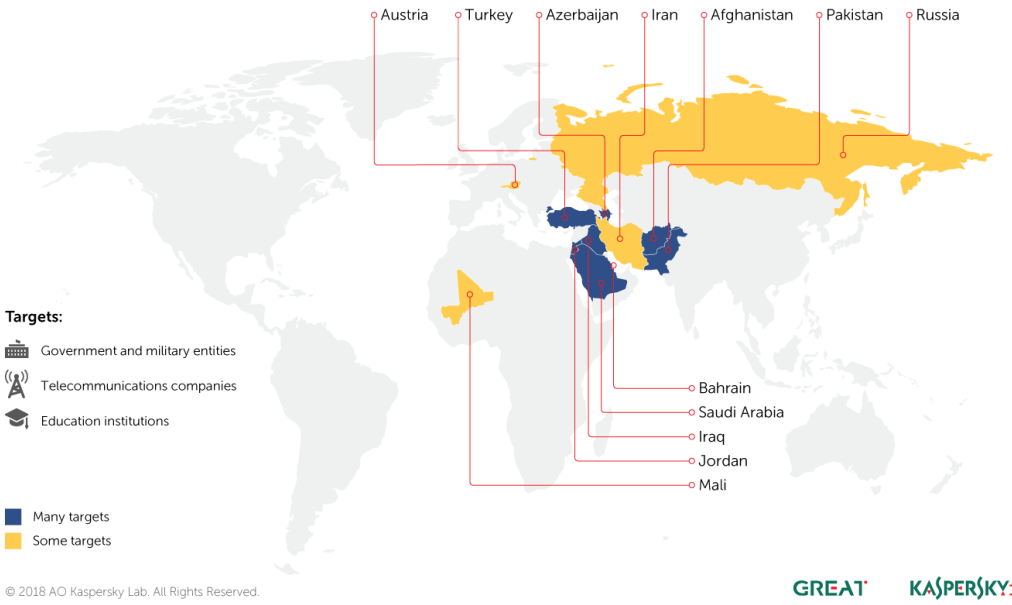
In October, we reported the recent activity of the MuddyWater APT group. Our past telemetry indicates that this relatively new threat actor, which surfaced in 2017, has focused mainly on government targets in Iraq and Saudi Arabia. However, the group behind MuddyWater has been known to target other countries in the Middle East, Europe and the US. We recently noticed a large number of spear-phishing documents that appear to be targeting government bodies, military entities, telcos and educational institutions in Jordan, Turkey, Azerbaijan and Pakistan, in addition to the continuous targeting of Iraq and Saudi Arabia. Other victims were detected in Mali, Austria, Russia, Iran and Bahrain. These new documents have appeared throughout 2018 and the activity escalated from May onwards. The new spear-phishing documents rely on social engineering to persuade the victims to enable macros. The attackers rely on a range of compromised hosts to deliver their attacks. In the advanced stages of our research, we were able not only to observe additional files and tools from the group's arsenal but also some OPSEC mistakes made by the attackers. In order to protect against malware attacks, we would recommend the following measures:

- Educate general staff so that they are able to identify malicious behaviour such as phishing links.
- Educate information security staff to ensure that they have full configuration, investigative and hunting abilities.
- Use a proven corporate-grade security solution in combination with anti-targeted attack solutions capable of detecting attacks by analyzing network anomalies.
- Provide security staff with access to the latest threat intelligence data, which will arm them with helpful tools for targeted attack prevention and discovery, such as IoCs (indicators of compromise) and YARA rules.
- Establish enterprise-grade patch management processes.

High-profile organizations should adopt elevated levels of cybersecurity, since attacks against them are inevitable and are unlikely to ever cease.

Muddy Water – global attack geography 2018

Countries targeted by the Muddy Water spear-phishing campaign in 2018, according to Kaspersky Lab detection data



DustSquad is another threat actor that has targeted organizations in Central Asia. Kaspersky Lab has been monitoring this Russian language cyber-espionage group for the last two years, providing private intelligence reports to our customers on four of their campaigns involving custom Android and Windows malware. Recently, we described a malicious program called Octopus, used by DustSquad to target diplomatic bodies in the region – the name was originally coined by ESET in 2017, after the 0ct0pus3.php script used by the actor on their old C2 servers. Using the Kaspersky Attribution Engine, based on similarity algorithms, we discovered that Octopus is related to DustSquad. In our telemetry, we tracked this campaign back to 2014 in the former Soviet republics of Central Asia (still mostly Russian-speaking) and in Afghanistan. In April, we discovered a new Octopus sample masquerading as Telegram Messenger with a Russian interface. We were unable to find legitimate software that this malware is impersonating – in fact, we don't believe it exists. However, the attackers used the potential Telegram

ban in Kazakhstan to push its dropper as alternative communication software for the political opposition. By subscribing to our APT intelligence reports, you can get access to our investigations and discoveries as they happen, including comprehensive technical data.

In October, we published our analysis of Dark Pulsar. Our investigation started in March 2017, when the Shadow Brokers published stolen data that included two frameworks – DanderSpritz and FuzzBunch. DanderSpritz contains various types of plugin designed to analyze victims, exploit vulnerabilities, schedule tasks, etc. The DanderSpritz framework is designed to examine already controlled machines and gather intelligence. Together, they provide a very powerful platform for cyber-espionage. The leak didn't include the Dark Pulsar backdoor itself: rather, it contained an administrative module for controlling the backdoor. However, by creating special signatures based on some magic constants in the administrative module, we were able to catch the implant itself. This implant gives the attackers remote control over compromised devices. We found 50 victims, all located in Russia, Iran and Egypt, but we believe there were probably many more. For one thing, the DanderSpritz interface is able to manage a large number of victims at the same time. In addition, the attackers often delete their malware once the campaign has ended. We think that the campaign stopped following the 'Lost in Translation' leak by the Shadow Brokers in April 2017. You can find our suggested mitigation strategies for complex threats such as Dark Pulsar here.

MOBILE APT CAMPAIGNS

The mobile APT threats segment saw three significant events: the detection of the Zoopark, BusyGasper and Skygofree cyber-espionage campaigns.

Technically, all three are well-designed and similar in their primary purpose – spying on selected victims. Their main aim is to steal all available personal data from a mobile device: interception of calls, messages, geolocation, etc. There is even a function for eavesdropping via the microphone – the smartphone is used as a 'bug' that doesn't even need to be hidden from an unsuspecting target.

The cybercriminals paid particular attention to the theft of messages from popular instant messaging services, which have now largely replaced standard means of communication. In several cases, the attackers used exploits that were capable of escalating the Trojans' local privileges on a device, opening up virtually unlimited access to remote monitoring, and often device management.

Keylogger functionality was also implemented in two of the three malicious programs, with the cybercriminals recording every keystroke on a device's keyboard. It's noteworthy that in order to intercept clicks the attackers didn't even require elevated privileges.

Geographically, victims were recorded in a variety of countries: Skygofree targeted users in Italy, BusyGasper attacked individual Russian users, and Zoopark operated in the Middle East.

It's also worth noting that there's an increasingly prominent trend of criminals involved in espionage showing a preference for mobile platforms, because they offer a lot more personal data.

EXPLOITS

Exploiting vulnerabilities in software and hardware remains an important means of compromising devices of all kinds.

Early this year, two severe vulnerabilities affecting Intel CPUs were reported. Dubbed Meltdown and Spectre respectively, they both allow an attacker to read memory from any process and from its own process respectively. The vulnerabilities have been around since at least 2011. Meltdown (CVE-2017-5754) affects Intel CPUs and allows an attacker to read data from any process on the host system. While code execution is required, this can be obtained in various ways – for example, through a software bug or by visiting a malicious website that loads JavaScript code that executes the Meltdown attack. This means that all the data residing in memory (passwords, encryption keys, PINs, etc.) could be read if the vulnerability is exploited properly. Vendors were quick to publish patches for the most popular operating systems. The Microsoft update, released on January 3, was not compatible with all antivirus programs – possibly resulting in a BSoD (Blue Screen of Death) on incompatible systems. So updates could only be installed if an antivirus product had first set a specific registry key, to indicate that there were no compatibility problems. Spectre (CVE-2017-5753 and CVE-2017-5715) is slightly different. Unlike Meltdown, this attack also works on other architectures (such as AMD and ARM). Also, Spectre is only able to read the memory space of the exploited process, and not that of any process. More importantly, aside from some countermeasures in some browsers, no universal solution is readily available for Spectre. It became clear in the weeks following the reports of the vulnerabilities that they are not easily fixable. Most of the released patches have reduced the attack surface, mitigating against known ways of exploiting the vulnerabilities, but they don't eradicate the danger completely. Since the problem is fundamental to the working of the vulnerable CPUs, it was clear that vendors would probably have to grapple with new exploits for years to come. In fact, it didn't take years. In July, Intel paid out a $100,000 bug bounty for new processor vulnerabilities related to Spectre variant one (CVE-2017-5753). Spectre 1.1 (CVE-2018-3693) can be used to create speculative buffer overflows. Spectre 1.2 allows an attacker to overwrite read-only data and code pointers to breach sandboxes on CPUs that don't enforce read-write protections. These new vulnerabilities were uncovered by MIT researcher Vladimir Kiriansky and independent researcher Carl Waldspurger.

On April 18, someone uploaded an interesting exploit to VirusTotal. This was detected by several security vendors, including Kaspersky Lab – using our generic heuristic logic for some older Microsoft Word documents. It turned out to be a new zero-day vulnerability for Internet Explorer (CVE-2018-8174) – patched by Microsoft on May 8, 2018. Following processing of the sample in our sandbox system, we noticed that it successfully exploited a fully patched version of Microsoft Word. This led us to carry out a deeper analysis of the vulnerability. The infection chain consists of the following steps. The victim receives a malicious Microsoft Word document. After opening it, the second stage of the exploit is downloaded – an HTML page containing VBScript code. This triggers a UAF (Use After Free) vulnerability and executes shellcode. Despite the initial attack vector being a Word document, the vulnerability is actually in VBScript. This is the first time we have seen a URL Moniker used to load an IE exploit in Word, but we believe that this technique will be heavily abused by attackers in the future, since it allows them to force victims to load IE, ignoring the default browser settings. It's likely that exploit kit authors will start abusing it in both drive-by attacks (through the browser) and spear-phishing campaigns (through a document). To protect against this technique, we would recommend applying the latest security updates and using a security solution with behavior detection capabilities.

In August, our AEP (Automatic Exploit Prevention) technology detected a new kind of cyberattack that tried to use a zero-day vulnerability in the Windows driver file, 'win32k.sys'. We informed Microsoft about the issue and on October 9 Microsoft disclosed the vulnerability (CVE-2018-8453) and published an update. This is a very dangerous vulnerability, giving attackers control over a compromised computer. The vulnerability was used in a highly targeted attack campaign on organizations in the Middle East – we found fewer than a dozen victims. We believe that these attacks were carried out by the FruityArmor threat actor.

In late October we reported another vulnerability to Microsoft, this time a zero-day elevation of privilege vulnerability in 'win32k.sys' – which can be used by an attacker to obtain the privileges necessary for persistence on a victim's system. This vulnerability has also been exploited in a very limited number of attacks on organizations in the Middle East. Microsoft published an update for this vulnerability (CVE-2018-8589) on November 13. This threat was also detected by means of our proactive technologies – the advanced sandboxing and anti-malware engine for the Kaspersky Anti Targeted Attack Platform and our AEP technology.

BROWSER EXTENSIONS – EXTENDING THE REACH OF CYBERCRIMINALS

Browser extensions can make our lives easier, hiding obtrusive advertising, translating text, helping us choose the goods we want in online stores and more. Unfortunately, there are also less desirable extensions that are used to bombard us with advertising or collect information about our activities. There are also extensions designed to steal money. Earlier this year, one of these caught our eye because it communicated with a suspicious domain. The malicious extension, named *Desbloquear Conteúdo* ('Unblock Content' in Portuguese), targeted customers of Brazilian online banking services, harvesting logins and passwords in order to obtain access to victims' bank accounts.

In September, hackers published the private messages from at least 81,000 Facebook accounts, claiming that this was just a small fraction of a much larger haul comprising 120 million accounts. In a Dark Web advert, the attackers offered the messages for 10 cents per account. The attack was investigated by the BBC Russian Service and cybersecurity company Digital Shadows. They found that of 81,000 accounts, most were from Ukraine and Russia, although accounts from other countries were also among them, including the UK, the US and Brazil. Facebook suggested that the messages were stolen using a malicious browser extension.

Malicious extensions are quite rare, but we need to take them seriously because of the potential damage they can cause. You should only install verified extensions with large numbers of installations and reviews in the Chrome Web Store or other official service. Even so, in spite of the protection measures implemented by the owners of such services, malicious extensions can still end up being published there. So it's a good idea to use an internet security product that gives you a warning if an extension acts suspiciously.

THE WORLD CUP OF FRAUD

Social engineering remains an important tool in the arsenal of cyberattackers of all kinds. Fraudsters are always on the lookout for opportunities to make money off the back of major sporting events; and the FIFA World Cup is no different. Long before the event kicked off, cybercriminals had started to create phishing websites and send messages exploiting World Cup themes. These phishing messages included notifications of a fake lottery win, or a message offering tickets to one of the matches. Fraudsters often go to great lengths to mimic legitimate partner sites, creating well-designed pages and even including SSL certificates for added credibility. The criminals also extract data by mimicking official FIFA notifications: the victim receives a message telling them that the security system has been updated and all personal data must be re-entered to avoid lockout. These messages contain a link to a fake page where the scammers harvest the victim's personal information.

You can find our report on the ways cybercriminals have exploited the World Cup in order to make money here. We also provided tips on how to avoid phishing scams – advice that holds true for any phishing scams, not just for those related to the World Cup.

In the run up to the tournament, we also analyzed wireless access points in the 11 cities hosting FIFA World Cup matches – nearly 32,000 Wi-Fi hotspots in total. While checking encryption and authentication algorithms, we counted the number of WPA2 and open networks, as well as their share among all the access points. More than a fifth of Wi-Fi hotspots were using unreliable networks. This meant that criminals simply needed to be located near an access point to intercept traffic and get their hands on people's data. Around three quarters of all access points used WPA/WPA2 encryption, considered to be one of the most secure. The level of protection mostly depends on the settings, such as the strength of the password set by the hotspot owner. A complicated encryption key can take years to successfully hack. However, even reliable networks, like WPA2, cannot be automatically considered totally secure. They are still susceptible to brute-force, dictionary and key reinstallation attacks, for which there are a large number of tutorials and open source tools available online. Any attempt to intercept traffic from WPA Wi-Fi in public access points can also be made by penetrating the gap between the access point and the device at the beginning of the session.

You can read our report here, together with our recommendations on the safe use of Wi-Fi hotspots, advice that is valid wherever you may be – not just at the World Cup.

FINANCIAL FRAUD ON AN INDUSTRIAL SCALE

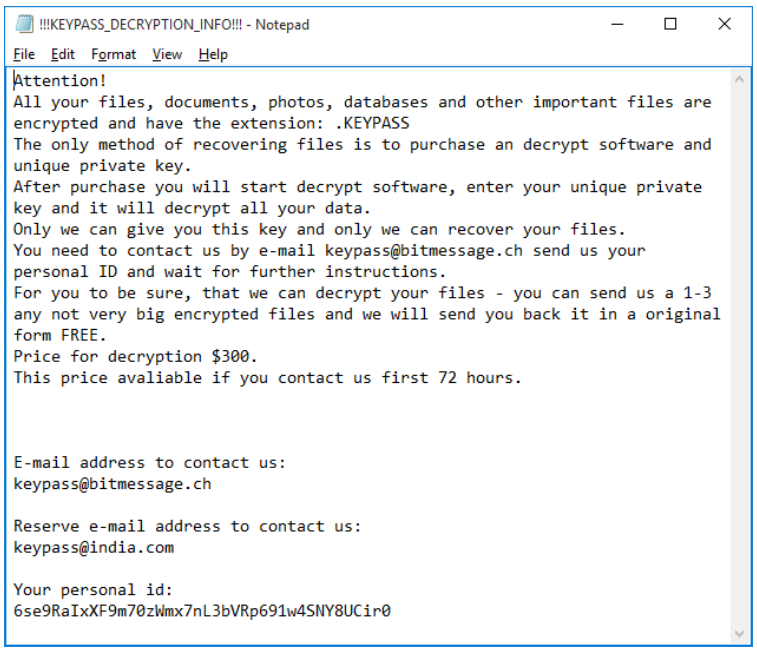
In August, Kaspersky Lab ICS CERT reported a phishing campaign designed to steal money from enterprises – primarily manufacturing companies. The attackers used standard phishing techniques to trick their victims into clicking on infected attachments, using emails disguised as commercial offers and other financial documents. The criminals used legitimate remote administration applications – either TeamViewer or RMS (Remote Manipulator System). These programs were employed to gain access to the device, scan for information on current purchases and details of financial and accounting software used by the victims. The attackers then used different ploys to steal company money – for example, by replacing the banking details in transactions. By the time we published our report, on August 1, we had seen infections on around 800 computers, spread across at least 400 organizations in a wide array of industries – including manufacturing, oil and gas, metallurgy, engineering, energy, construction, mining and logistics. The campaign has been ongoing since October 2017.

Our research highlights that, even when threat actors use simple techniques and known malware, they can successfully attack industrial companies by using social engineering tricks and hiding their code in target systems – using legitimate remote administration software to evade detection by antivirus solutions.

You can find out more about how attackers use remote administration tools to compromise their targets here, and an overview of attacks on ICS systems in the first half of 2018 here.

RANSOMWARE – STILL A THREAT

The fall in the number of ransomware attacks in the last year or so has been well-documented. Nevertheless, this type of malware remains a significant problem and we continue to see the development of new ransomware families. Early in August, our anti-ransomware module started detecting the KeyPass Trojan. In just two days, we found this malware in more than 20 countries – Brazil and Vietnam were hardest hit, but we also found victims in Europe, Africa and the Far East. KeyPass encrypts all files, regardless of extension, on local drives and network shares that are accessible from the infected computer. It ignores some files, located in directories that are hardcoded in the malware. Encrypted files are given the additional extension 'KEYPASS' and ransom notes, called '!!!KEYPASS_DECRYPTION_INFO!!!.txt', are saved in each directory containing encrypted files. The creators of this Trojan implemented a very simplistic scheme. The malware uses the symmetric algorithm AES-256 in CFB mode with zero IV and the same 32-byte key for all files. The Trojan encrypts a maximum of 0x500000 bytes (~5 MB) of data at the start of each file. Shortly after launch, the malware connects to its C2 server and obtains the encryption key and infection ID for the current victim. The data is transferred over plain HTTP in the form of JSON. If the C2 is unavailable – for example, if the infected computer is not connected to the internet, or the server is down – the malware uses a hardcoded key and ID. As a result, in the case of offline encryption, the decryption of the victim's files is trivial.



Probably the most interesting feature of the KeyPass Trojan is the ability to take 'manual control'. The Trojan contains a form that is hidden by default, but which can be shown after pressing a special button on the keyboard. This form allows the criminals to customize the encryption process by changing such parameters as the encryption key, the name of the ransom note, the text of the ransom, the victim ID, the extension of encrypted files and the list of directories to be excluded from encryption. This capability suggests that the criminals behind the Trojan might intend to use it in manual attacks.

However, it's not only new ransomware families that are causing problems. One and a half years after the WannaCry epidemic, it continues to top the list of the most widespread cryptor families – so far, we have seen 74,621 unique attacks worldwide. These attacks accounted for 28.72% of all those targeted with cryptors in Q3 2018. This percentage has risen by two-thirds during the last year. This is especially alarming considering that a patch for the EternalBlue exploit used by WannaCry existed even before the initial epidemic in May 2017.

ASACUB AND BANKING TROJANS

2018 showed the most impressive figures in terms of the number of attacks involving mobile banking Trojans. At the beginning of the year, this type of threat seemed to have leveled off both in number of unique samples detected and number of users attacked.

However, in the second quarter there was a dramatic change for the worse: record-breaking numbers of detected mobile banking Trojans and attacked users. The root cause of this significant upturn is unclear, though the main culprits were the creators of Asacub and Hqwar. An interesting feature of Asacub is its longevity: according to our data, the group behind it has been operating for more than three years.

Asacub evolved from an SMS Trojan, which from the very outset possessed techniques for preventing deletion and intercepting incoming calls and SMSs. The creators subsequently complicated the program logic and started the mass distribution of the malware. The chosen vector was the same as that at the very beginning – social engineering via SMS. However, this time the valid phone numbers were sourced from popular bulletin boards, with owners often expecting messages from unfamiliar subscribers.

The propagation technique then snowballed when the devices that the Trojan had infected started spreading the infection – Asacub self-proliferated to the victim's entire contact list.

SMART DOESN'T MEAN SECURE

These days we're surrounded by smart devices. This includes everyday household objects such as TVs, smart meters, thermostats, baby monitors and children's toys. But it also includes cars, medical devices, CCTV cameras and parking meters. We're even seeing the emergence of smart cities. However, this offers a greater attack surface to anyone looking to take advantage of security weaknesses – for whatever purpose. Securing traditional computers is difficult. But things are more problematic with the internet of things (IoT), where lack of standardization leaves developers to ignore security, or consider it as an afterthought. There are plenty of examples to illustrate this.

In February, we explored the possibility that a smart hub might be vulnerable to attack. A smart hub lets you control the operation of other smart devices in the home, receiving information and issuing commands. Smart hubs might be controlled through a touch screen, or through a mobile app or web interface. If it's vulnerable, it would potentially provide a single point of failure. While the smart hub our researchers investigated didn't contain significant vulnerabilities, there were logical mistakes that were enough to allow our researchers to obtain remote access.

Researchers at Kaspersky Lab ICS CERT checked a popular smart camera to see how well protected it is from hackers. Smart cameras are now part of everyday life. Many now connect to the cloud, allowing someone to monitor what's happening at a remote location – to check on pets, for security surveillance, etc. The model our researchers investigated is marketed as an all-purpose tool – suitable for use as a baby monitor, or as part of a security system. The camera is able to see in the dark, follow a moving object, stream footage to a smartphone or tablet and play back sound through a built-in speaker. Unfortunately, the camera turned out to have 13 vulnerabilities – almost as many as it has features – that could allow an attacker to change the administrator password, execute arbitrary code on the device, build a botnet of compromised cameras or stop it functioning completely.

Potential problems are not limited to consumer devices. Early this year, Ido Naor, a researcher from our Global Research and Analysis Team and Amihai Neiderman from Azimuth Security, discovered a vulnerability in an automation device for a gas station. This device was directly connected to the internet and was responsible for managing every component of the station, including fuel dispensers and payment terminals. Even more alarming, the web interface for the

device was accessible with default credentials. Further investigation revealed that it was possible to shut down all fueling systems, cause a fuel leakage, change the price, circumvent the payment terminal (in order to steal money), capture vehicle license plates and driver identities, execute code on the controller unit and even move freely across the gas station network.

Technology is driving improvements in healthcare. It has the power to transform the quality and reduce the cost of health and care services. It can also give patients and citizens more control over their care, empower carers and support the development of new medicines and treatments. However, new healthcare technologies and mobile working practices are producing more data than ever before, at the same time providing more opportunities for data to be lost or stolen. We've highlighted the issues several times over the last few years (you can read about it here, here and here). We continue to track the activities of cybercriminals, looking at how they penetrate medical networks, how they find data on publicly available medical resources and how they exfiltrate it. In September, we examined healthcare security. More than 60% of medical organizations had some kind of malware on their computers. In addition, attacks continue to grow in the pharmaceutical industry. It's vital that medical facilities remove all nodes that process personal medical data, update software and remove applications that are no longer needed, and do not connect expensive medical equipment to the main LAN. You can find our detailed advice here.

This year, we also investigated smart devices for animals – specifically, trackers to monitor the location of pets. These gadgets are able to access the pet owner's home network and phone, and their pet's location. We wanted to find out how secure they are. Our researchers looked at several popular trackers for potential vulnerabilities. Four of the trackers we looked at use Bluetooth LE technology to communicate with the owner's smartphone. But only one does so correctly. The others can receive and execute commands from anyone. They can also be disabled, or hidden from the owner – all that's needed is proximity to the tracker. Only one of the tested Android apps verifies the certificate of its server, without relying solely on the system. As a result, they are vulnerable to man-in-the-middle (MitM) attacks—intruders can intercept transmitted data by 'persuading' victims to install their certificate.

Some of our researchers also looked at human wearable devices – specifically, smart watches and fitness trackers. We were interested in a scenario where a spying app installed on a smartphone could send data from the built-in motion sensors (accelerometer and gyroscope) to a remote server and use the data to piece together the wearer's actions – walking, sitting, typing, etc. We started with an Android-based smartphone, created a simple app to process and transmit the data and then looked at what we could get from this data. Not only was it possible to work out that the wearer is sitting or walking, but also figure out if they are out for a stroll or changing subway trains, because the accelerometer patterns differ slightly – this is how fitness trackers distinguish between walking and cycling. It is also easy to see when someone is typing. However, finding out what they are typing would be hard and would require repeated text entry. Our researchers were able to recover a computer password with 96 per cent accuracy and a PIN code entered at an ATM with 87 per cent accuracy. However, it would be much harder to obtain other information – for example, a credit card number or CVC code – because of the lack of predictability about when the victim would type such information. In reality, the difficulty involved in obtaining such information means that an attacker would have to have a strong motive for targeting someone specific. Of course, there are situations where this might be worthwhile for attackers.

There has been a growth in car sharing services in recent years. Such services clearly provide flexibility for people wanting to get around major cities. However, it raises the question of security – how safe is the personal information of people using the services? In July, we tested 13 apps, to see if their developers have considered security. The results of our tests were not encouraging. It's clear that app developers don't fully understand the current threats to mobile platforms – this is true for both the design stage and when creating the infrastructure. A good first step would be to expand the functionality for notifying customers of suspicious activities – only one service currently sends notifications to customers about attempts to log in to their account from a different device. The majority of the apps we analyzed are poorly designed from a security standpoint and need to be improved. Moreover, many of the programs are not just very similar to each other but are actually based on the same code. You can read our report here, including advice for customers of car sharing services and recommendations for developers of car sharing apps.

The use of smart devices is increasing. Some forecasts suggest that by 2020 the number of smart devices will exceed the world's population several times over. Yet manufacturers still don't prioritize security: there are no reminders to change the default password during initial setup or notifications about the release of new firmware versions. And the updating process itself can be complex for the average consumer. This makes IoT devices a prime target for cybercriminals. Easier to infect than PCs, they often play an important role in the home infrastructure: some manage internet traffic, others shoot video footage and still others control domestic devices – for example, air conditioning. Malware for smart devices is increasing not only in quantity, but also quality. More and more exploits are being weaponized by cybercriminals, and infected devices are used to launch DDoS attacks, to steal personal data and to mine crypto-currency. In September, we published a report on IoT threats, and this year we have started to include data on IoT attacks in our quarterly and end-of-year statistics reports.

It's vital that vendors improve their security approach, ensuring that security is considered when products are being designed. Governments in some countries, in an effort to encourage security by design in manufacturers of smart devices, are introducing guidelines. In October, the UK government launched its code of practice for consumer IoT security. The German government recently published its suggestions for minimum standards for broadband routers.

It's also important that consumers consider security before buying any connected device.

- Consider if you really need the device. If you do, check the functions available and disable any that you don't need to reduce your attack surface.
- Look online for information about any vulnerabilities that have been reported.
- Check to see if it's possible to update the firmware on the device.
- Always change the default password and replace it with a unique, complex password.
- Don't share serial numbers, IP addresses and other sensitive data relating to the device online.

You can use the free Kaspersky IoT Scanner to check your Wi-Fi network and tell you if the devices connected to it are safe.

OUR DATA IN THEIR HANDS

Personal information is a valuable commodity. This is evident from the steady stream of data breaches reported in the news – these include Under Armour, FIFA, Adidas, Ticketmaster, T-Mobile, Reddit, British Airways and Cathay Pacific.

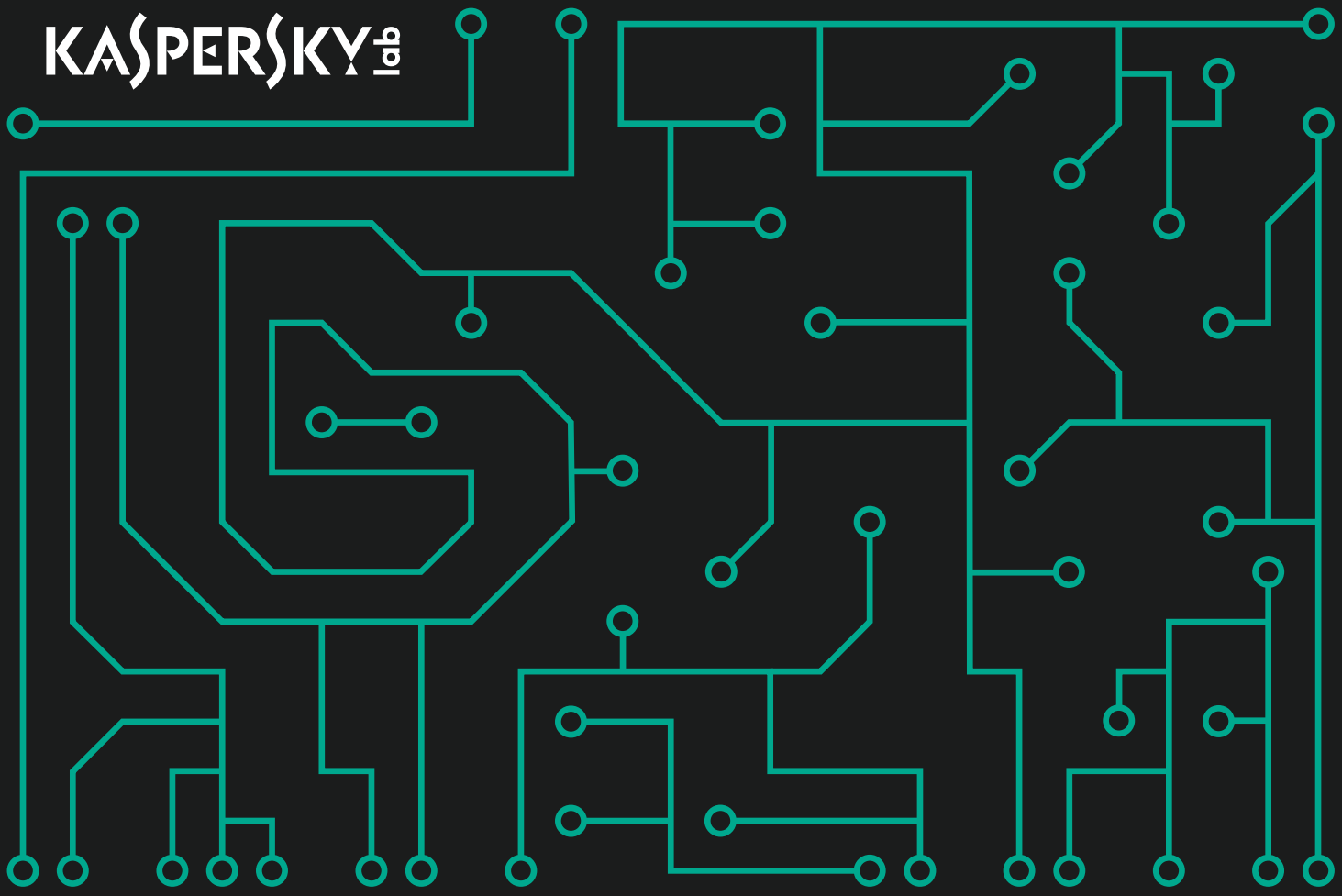
The scandal involving the use, by Cambridge Analytica, of Facebook data is a reminder that personal information is not just valuable to cybercriminals. In many cases, personal data is the price people pay to obtain a product or service – 'free' browsers, 'free' email accounts, 'free' social network accounts, etc. But not always. Increasingly, we're surrounded by smart devices that are capable of gathering details on the minutiae of our lives. Earlier this year, one journalist turned her apartment into a smart home in order to measure how much data was being collected by the firms that made the devices. Since we generally pay for such devices, the harvesting of data can hardly be seen as the price we pay for the benefits they bring in these cases.

Some data breaches have resulted in fines for the companies affected (the UK Information Commissioner's Office fined Equifax and Facebook, for example). However, so far fines levied have been for breaches that occurred before the EU General Data Protection Regulation (GDPR) came into force in May. The penalties for any serious breaches that occur in the future are likely to be much higher.

There's no such thing as 100% security, of course. But any organization that holds personal data has a duty of care to secure it effectively. And where a breach results in the theft of personal information, companies should alert their customers in a timely manner, enabling them to take steps to limit the potential damage that can occur.

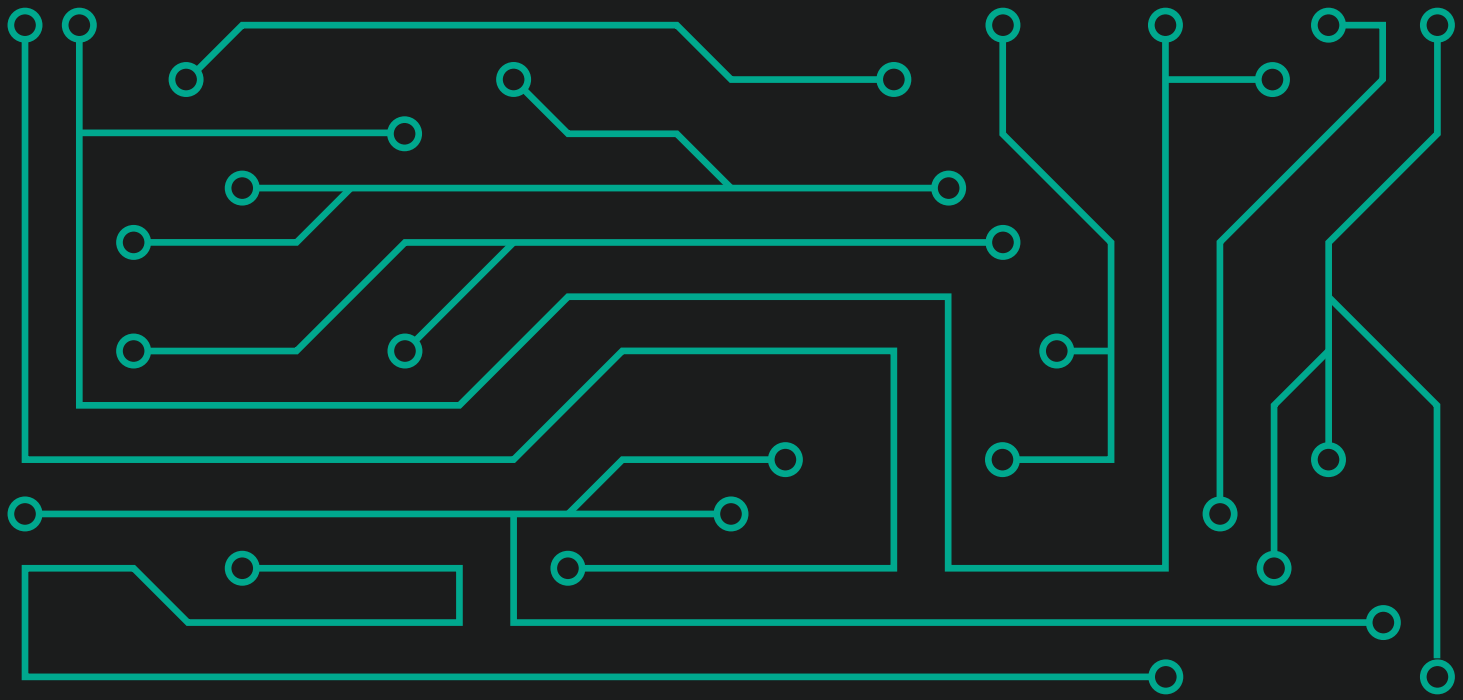
While there's nothing that we, as individuals, can do to prevent the theft of our personal information from an online provider, it's important that we take steps to secure our online accounts and to minimize the impact of any breach – in particular, by using unique passwords for each site, and by using two-factor authentication.

KASPERSKY lab



Kaspersky Security Bulletin 2018

STORY OF THE YEAR: MINERS



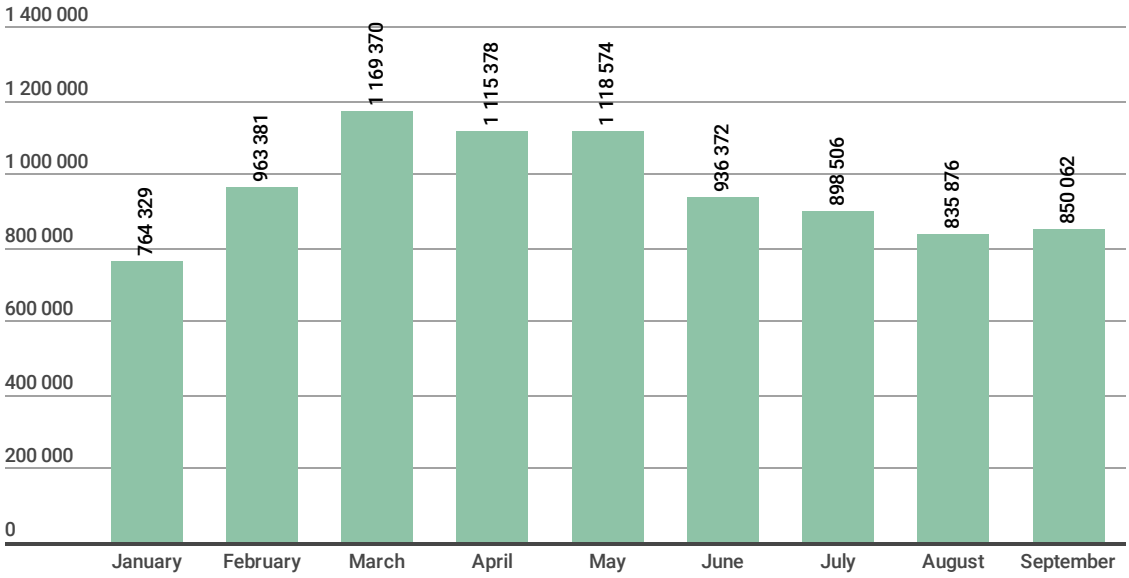
CONTENTS

Cryptocurrency miners that infect the computers of unsuspecting users essentially operate according to the same business model as ransomware programs: the victim's computing power is harnessed to enrich the cybercriminals. Only in the case of miners, it might be quite a while before the user notices that 70–80% of their CPU or graphics card power is being used to generate virtual coins. Encrypted documents and ransomware messages are far harder to miss.

Cryptominers usually find their way onto user computers and corporate machines along with adware, hacked games, and other pirated content. What's more, the present "entry threshold" — that is, the actual process of creating a miner — is rather low: cybercriminals are assisted by ready-to-use affiliate programs, open mining pools, and miner builders. If that weren't enough, there is another way to steal computing resources through a webpage-embedded mining script that starts when the user opens the site in a browser. A separate category of cybercriminals are those who target not private computers, but the servers of large companies, for which the infection process is considerably more resource-intense.

TRENDS

2018 began with a rise in the number of miner-related attacks. However, after a drop in the value of the main cryptocurrencies, which lasted from January to February, infection activity noticeably declined. General interest in cryptocurrencies also waned. Yet the graph clearly shows that while the number of cryptominer attacks decreased, the threat is still current. As for how the November collapse in the Bitcoin exchange rate will affect the number of infections, time will tell.



Number of unique users attacked by miners in Q1–Q3 2018

Hidden mining software was very popular among botnet owners, as confirmed by our statistics on files downloaded by zombie networks: Q1 2018 saw a boom in cryptominers, and the share of this malware in the first half of the year was 4.6% of the total number of files downloaded by botnets. For comparison, in Q2 2017 this figure was 2.9%. It follows from the data that cybercriminals have come to view botnets as a means of spreading software for mining cryptocurrencies.

	H2 2017		H1 2018	
1	Lethic	17.0%	njRAT	5.2%
2	Neutrino.POS	4.6%	Lethic	5.0%
3	njRAT	3.7%	Khalesi	4.9%

4	Emotet	3.5%	Miners	4.6%
5	Miners	2.9%	Neutrino.POS	2.2%
6	Smoke	1.8%	Edur	1.3%
7	Cutwail	0.7%	PassView	1.3%
8	Ransomware	0.7%	Jimmy	1.1%
9	SpyEye	0.5%	Gandcrab	1.1%
10	Snojan	0.3%	Cutwail	1.1%

Most downloaded threats, H2 2017–H1 2018

Still on the topic of botnets, it is impossible not to mention that in Q3 2018 we registered a decline in the number of DDoS attacks, the most likely reason being, according to our experts, the "reprofiling" of botnets from DDoS attacks to cryptocurrency mining. This was induced not only by the high popularity of cryptocurrencies, but also the high competition in the "DDoS market", which made the attacks less expensive for clients, but not for the botnetters themselves, who still have to cope with more than a few less-than-legal "organizational issues."

Mining differs favorably for cybercriminals in that, if executed properly, it can be impossible for the owner of an infected machine to detect, and thus the chances of encountering the cyberpolice are far lower. And the reprofiling of existing server capacity completely hides its owner from the eyes of the law. Evidence suggests that the owners of many well-known botnets have switched their attack vector toward mining. For example, the DDoS activity of the Yoyo botnet dropped dramatically, although there is no data about it being dismantled.

Moreover, mining has started to command as much (or more) attention as ransomware: this year we encountered several examples of reprofiled malware with added functionality for cryptocurrency mining. And the techniques used by the creators of miners have become more sophisticated.

For instance, an interesting miner implementation, which we dubbed PowerGhost, caught our eye in July this year. The malware can stealthily establish itself in the system and spread inside large corporate networks, infecting workstations and servers alike. To go unnoticed by users and security solutions for as long as possible,

the miner employs various fileless techniques. Infection occurs remotely using exploits or remote management tools (Windows Management Instrumentation), and involves running a single-line powershell script that downloads the main body of the malware and immediately starts it without writing to the hard drive.

Another example of reprofiling is the ransomware Trojan Trojan-Ransom.Win32.Rakhni, the first samples of which were detected by Kaspersky Lab back in 2013. Its mining functions are a 2018 innovation. At the same time, their activation depends on whether the folder %AppData%\Bitcoin is present on the infected machine. If it exists, the loader downloads the ransomware. If there is no such folder and, in addition, the computer has more than two logical processors, a miner is downloaded. To keep the malware hidden in the system, the developers made it look like an Adobe product. This can be seen by the icon and the name of the executable file, as well as the fake digital signature, which uses Adobe Systems Incorporated as the company name.

Another piece of malware that has learned how to seed computers with mining utilities is the previously adware-only PBot. The malware spreads through affiliate sites that inject scripts into their pages for redirecting users to sponsored links. The standard distribution scheme looks as follows:

1. The user visits one of the sites in the affiliate network.
2. Clicking anywhere on the page causes a new browser window to appear, where an intermediate link opens.
3. The link directs the user to the PBot download page, which is tasked with downloading and running the malware by deceptive means.

The most common coin among all illegally mined cryptocurrencies is Monero (xmr). This is due to its anonymous algorithm, relatively high market value, and ease of sale, since it is accepted by most major cryptocurrency exchanges. For botnets mining this coin illegally, it is important that CPU resources can be utilized. By some accounts, a total of $175 million has been mined illegally, representing around 5% of all Monero currently in circulation.

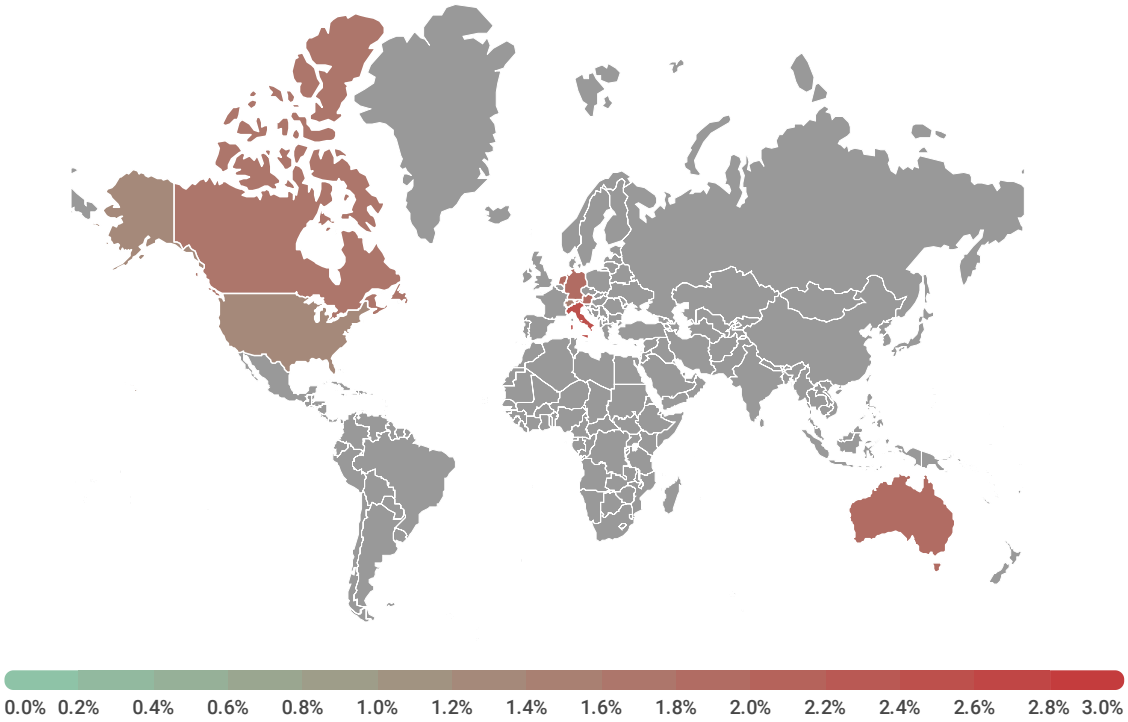
FACTORS AFFECTING THE DISTRIBUTION OF MINERS

The conclusion based on data we obtained from various sources is that legislative control over cryptocurrencies has little impact on the spread of hidden mining. For example, in Algeria and Vietnam cryptocurrencies are either prohibited or severely restricted under domestic law. Yet Vietnam is third in the ranking of leading countries by number of miner attacks, and Algeria is sixth. Meanwhile, Iran, which is presently drafting legislation to govern cryptocurrency and developing plans to issue its own "coins," is in seventh place.

Country	Cryptocurrency status	% of attacks
Kazakhstan	Not prohibited, Not legalized	16.75%
Vietnam	Issuance (mining) prohibited	13.00%
Indonesia	Recognized as an exchange commodity	12.87%
Ukraine	Circulation governed by law	11.19%
Russia	Legislation under consideration	10.71%
Algeria	Prohibited	9.03%
Iran	Legislation in preparation, creation of own cryptocurrency planned	7.21%
India	Ban under consideration, hearings in progress	7.20%
Thailand	Circulation governed by law	6.76%
Taiwan	Not prohibited	5.81%

Top 10 countries by share of miner attacks, January–October 2018 (includes only countries with more than 500,000 Kaspersky Lab clients)

At the other end of the scale, US users were the least affected by cryptominters (1.33% of the total number of attacks), followed by users in Switzerland (1.56%) and Britain (1.66%).



Map representing countries with the lowest share of miner attacks, January–October 2018 (includes only countries with more than 500,000 Kaspersky Lab clients)

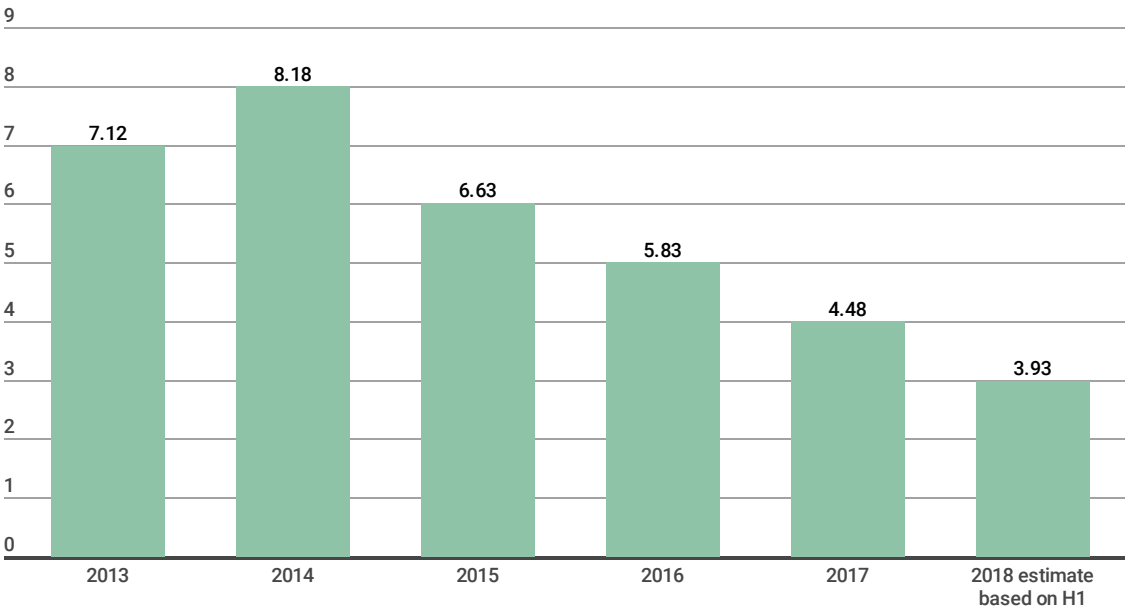
The prevalence of miners is not impacted by the cost of electricity, which varies greatly from country to country. Again, this factor is not a consideration for cybercriminals as they exploit third-party resources.

DISTRIBUTION METHODS

Looking at the distribution of pirated software in countries with the highest number of miner attacks, one sees a clear correlation: the more freely unlicensed software is distributed, the more miners there are. This is confirmed by our statistics, which indicates that miners most often land on victim computers together with pirated software.

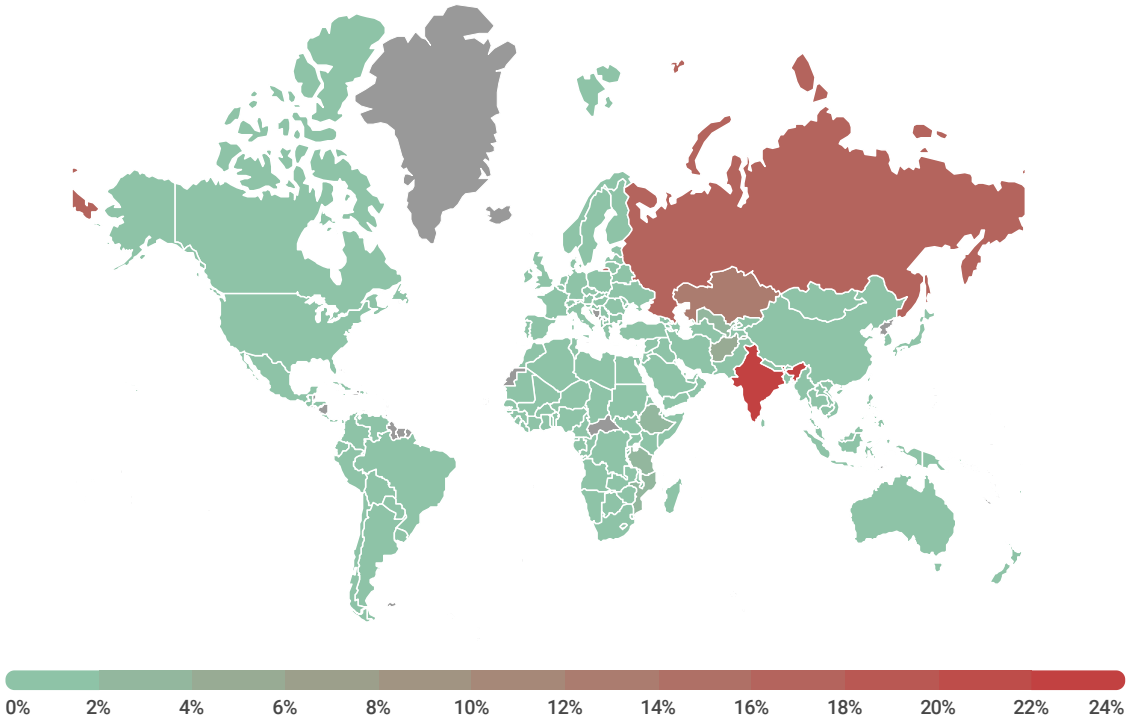
Another penetration vector for miners is adware installers distributed using social engineering. More sophisticated options (for example, propagation through vulnerabilities such as EternalBlue) are aimed at server capacities and are less frequently encountered.

And it should not be forgotten that USB drives have been used to distribute cryptocurrency mining software since at least 2015. The percentage of detections of the popular Bitcoin miner Trojan.Win64.Miner.all on removable devices is growing annually by about one-sixth. In 2018, one in ten users affected by malware transmitted through flash drives was the victim of this particular miner (roughly 9.22%; for comparison, in 2017 it was 6.7%, and in 2016 4.2%).



Millions of unique users found to have malware in the root directory, which is the main sign of infection via removable drives, 2013–2018. Source: KSN.

Trojan.Win32.Miner.ays/Trojan.Win.64.Miner.all was detected in India (23.7%), Russia (18.45%), and Kazakhstan (14.38%), but some cases were also logged in Asia, Africa, and Europe (Britain, Germany, the Netherlands, Switzerland, Spain, Belgium, Austria, Italy, Denmark, Sweden), as well as the US, Canada, and Japan.



Share of users impacted by Bitcoin miners on removable drives, 2018. Source: KSN (includes only countries with more than 10,000 Kaspersky Lab clients)

CONCLUSION

Summing up the past year, we can highlight the following bullet points:

1. Given the growing value and popularity of cryptocurrencies, cybercriminals are investing resources in the development of new mining technologies, which, according to our data, are gradually replacing ransomware Trojans.
2. Hidden mining activity declines when cryptocurrency prices fall.
3. The spread of hidden mining is not impacted by factors such as domestic legislative control or cost of electricity.
4. Miners often get on victims' computers during the download of unlicensed content or installation of pirated software. As a consequence, this type of threat is most prevalent in countries with poor regulation of the unlicensed software market, as well a low level of overall digital literacy among users.

KASPERSKY lab

Kaspersky Security Bulletin:

THREAT PREDICTIONS FOR 2019

Vicente Diaz

CONTENTS

There's nothing more difficult than predicting. So, instead of gazing into a crystal ball, the idea here is to make educated guesses based on what has happened recently and where we see a trend that might be exploited in the coming months. Asking the most intelligent people I know, and basing our scenario on APT attacks because they traditionally show the most innovation when it comes to breaking security, here are our main 'predictions' of what might happen in the next few months.

NO MORE BIG APTS

What? How is it possible that in a world where we discover more and more actors every day the first prediction seems to point in the opposite direction?

The reasoning behind this is that the security industry has consistently discovered highly sophisticated government-sponsored operations that took years of preparation. What seems to be a logical reaction to that situation from an attacker's perspective would be exploring new, even more sophisticated techniques that are much more difficult to discover and to attribute to specific actors.

Indeed, there are many different ways of doing this. The only requirement would be an understanding of the techniques used by the industry for attribution and for identifying similarities between different attacks and the artifacts used in them– something that doesn't seem to be a big secret. With sufficient resources, a simple solution for an attacker could be having different ongoing sets of activity that are very difficult to relate to the same actor or operation. Well-resourced attackers could start new innovative operations while keeping their old ones alive. Of course, there's still a good chance of the older operations being discovered, but discovering the new operations would pose a greater challenge.

Instead of creating more sophisticated campaigns, in some cases it appears to be more efficient for some very specific actors who have the capability to do so, to directly target infrastructure and companies where victims can be found, such as ISPs. Sometimes this can be accomplished through regulation, without the need for malware.

Some operations are simply externalized to different groups and companies that use different tools and techniques, making attribution extremely difficult. It's worth keeping in mind that in the case of government-sponsored operations this 'centrifugation' of resources and talent might affect the future of such campaigns.

Technical capabilities and tools are owned by the private industry in this scenario, and they are for sale for any customer that, in many cases, doesn´t fully understand the technical details and consequences behind them.

All this suggests that we're unlikely to discover new highly sophisticated operations – well-resourced attackers are more likely to simply shift to new paradigms.

NETWORKING HARDWARE AND IOT

It just seemed logical that at some point every actor would deploy capabilities and tools designed to target networking hardware. Campaigns like VPNFilter were a perfect example of how attackers have already started deploying their malware to create a multipurpose 'botnet'. In this particular case, even when the malware was extremely widespread, it took some time to detect the attack, which is worrisome considering what might happen in more targeted operations. Actually, this idea can go even further for well-resourced actors: why not directly target even more elemental infrastructure instead of just focusing on a target organization? We haven't reached that level of compromise (to our knowledge), but it was clear from past examples (like Regin) how tempting that level of control is for any attacker.

Vulnerabilities in networking hardware allow attackers to follow different directions. They might go for a massive botnet-style compromise and use that network in the future for different goals, or they might approach selected targets for more clandestine attacks. In this second group we might consider 'malware-less' attacks, where opening a VPN tunnel to mirror or redirect traffic might provide all the necessary information to an attacker.

All these networking elements might also be part of the mighty IoT, where botnets keep growing at an apparently unstoppable pace. These botnets could be incredibly powerful in the wrong hands when it comes to disrupting critical infrastructure, for instance. This can be abused by well-resourced actors, possibly using a cover group, or in some kind of terror attack.

One example of how these versatile botnets can be used, other than for disruptive attacks, is in short-range frequency hopping for malicious communications, avoiding monitoring tools by bypassing conventional exfiltration channels.

Even though this seems to be a recurrent warning year after year, we should never underestimate IoT botnets – they keep growing stronger.

PUBLIC RETALIATION

One of the biggest questions in terms of diplomacy and geopolitics was how to deal with an active cyberattack. The answer is not simple and depends heavily on how bad and blatant the attack was, among many other considerations. However, it seems that after hacks like that on the Democratic National Committee, things became more serious.

Investigations into recent high-profile attacks, such as the Sony Entertainment Network hacks or the attack on the DNC, culminated in a list of suspects being indicted. That results not only in people facing trial but also a public show of who was behind the attack. This can be used to create a wave of opinion that might be part of an argument for more serious diplomatic consequences.

Actually we have seen Russia suffering such consequences as a result of their alleged interference in democratic processes. This might make others rethink future operations of this kind.

However, the fear of something like that happening, or the thought that it might already have happened, was the attackers' biggest achievement. They can now exploit such fear, uncertainty and doubt in different, more subtle ways – something we saw in notable operations, including that of the Shadowbrokers. We expect more to come.

What will we see in the future? The propaganda waters were probably just being tested by past operations. We believe this has just started and it will be abused in a variety of ways, for instance, in false flag incidents like we saw with Olympic Destroyer, where it's still not clear what the final objective was and how it might have played out.

EMERGENCE OF NEWCOMERS

Simplifying somewhat, the APT world seems to be breaking into two groups: the traditional well-resourced most advanced actors (that we predict will vanish) and a group of energetic newcomers who want to get in on the game.

The thing is that the entry barrier has never been so low, with hundreds of very effective tools, re-engineered leaked exploits and frameworks of all kinds publicly available for anyone to use. As an additional advantage, such tools make attribution nearly impossible and can be easily customized if necessary.

There are two regions in the world where such groups are becoming more prevalent: South East Asia and the Middle East. We have observed the rapid progression of groups suspected of being based in these regions, traditionally abusing social engineering for local targets, taking advantage of poorly protected victims and the lack of a security culture. However, as targets increase their defenses, attackers do the same with their offensive capabilities, allowing them to extend their operations to other regions as they improve the technical level of their tools. In this scenario of scripting-based tools we can also find emerging companies providing regional services who, despite OPSEC failures, keep improving their operations.

One interesting aspect worth considering from a more technical angle is how JavaScript post-exploitation tools might find a new lease of life in the short term, given the difficulty of limiting its functionality by an administrator (as opposed to PowerShell), its lack of system logs and its ability to run on older operating systems.

THE NEGATIVE RINGS

The year of Meltdown/Spectre/AMDFlaws and all the associated vulnerabilities (and those to come) made us rethink where the most dangerous malware actually lives. And even though we have seen almost nothing in the wild abusing vulnerabilities below Ring 0, the mere possibility is truly scary as it would be invisible to almost all the security mechanisms we have.

For instance, in the case of SMM there has at least been a publicly available PoC since 2015. SMM is a CPU feature that would effectively provide remote full access to a computer without even allowing Ring 0 processes to have access to its memory space. That makes us wonder whether the fact that we haven´t found any malware abusing this so far is simply because it is so difficult to detect. Abusing this feature seems to be too good an opportunity to ignore, so we are sure that several groups have been trying to exploit such mechanisms for years, maybe successfully.

We see a similar situation with virtualization/hypervisor malware, or with UEFI malware. We have seen PoCs for both, and HackingTeam even revealed a UEFI persistence module that's been available since at least 2014, but again no real ITW examples as yet.

Will we ever find these kinds of unicorns? Or haven't they been exploited yet? The latter possibility seems unlikely.

YOUR FAVORITE INFECTION VECTOR

In probably the least surprising prediction of this article we would like to say a few words about spear phishing. We believe that the most successful infection vector ever will become even more important in the nearest future. The key to its success remains its ability to spark the curiosity of the victim, and recent massive leaks of data from various social media platforms might help attackers improve this approach.

Data obtained from attacks on social media giants such as Facebook and Instagram, as well as LinkedIn and Twitter, is now available on the market for anyone to buy. In some cases, it is still unclear what kind of data was targeted by the attackers, but it might include private messages or even credentials. This is a treasure trove for social engineers, and could result in, for instance, some attacker using the stolen credentials of some close contact of yours to share something on social media that you already discussed privately, dramatically improving the chances of a successful attack.

This can be combined with traditional scouting techniques where attackers double-check the target to make sure the victim is the right one, minimizing the distribution of malware and its detection. In terms of attachments, it is fairly standard to make sure there is human interaction before firing off any malicious activity, thus avoiding automatic detection systems.

Indeed, there are several initiatives using machine learning to improve phishing's effectiveness. It's still unknown what the results would be in a real-life scenario, but what seems clear is that the combination of all these factors will keep spear phishing as a very effective infection vector, especially via social media in the months to come.

DESTRUCTIVE DESTROYER

Olympic destroyer was one of the most famous cases of potentially destructive malware during the past year, but many attackers are incorporating such capabilities in their campaigns on a regular basis. Destructive attacks have several advantages for attackers, especially in terms of creating a diversion and cleaning up any logs or evidence after the attack. Or simply as a nasty surprise for the victim.

Some of these destructive attacks have geostrategic objectives related to ongoing conflicts as we have seen in Ukraine, or with political interests like the attacks that affected several oil companies in Saudi Arabia. In some other cases they might be the result of hacktivism, or activity by a proxy group that's used by a more powerful entity that prefers to stay in the shadows.

Anyway, the key to all these attacks is that they are 'too good' not to use. In terms of retaliation for instance, governments might use them as a response ranged somewhere between a diplomatic answer and an act of war, and indeed some governments are experimenting with them. Most of these attacks are planned in advance, which involves an initial stage of reconnaissance and intrusion. We don´t know how many potential victims are already in this situation where everything is ready, just waiting for the trigger to be pulled, or what else the attackers have in their arsenal waiting for the order to attack.

ICS environments and critical infrastructure are especially vulnerable to such attacks, and even though industry and governments have put a lot of effort in over the last few years to improve the situation, things are far from ideal. That's why we believe that even though such attacks will never be widespread, in the next year we expect to see some occurring, especially in retaliation to political decisions.

ADVANCED SUPPLY CHAIN

This is one of the most worrisome vectors of attack, which has been successfully exploited over the last two years, and it has made everyone think about how many providers they have and how secure they are. Well, there is no easy answer to this kind of attack.

Even though this is a fantastic vector for targeting a whole industry (similar to watering hole attacks) or even a whole country (as seen with NotPetya), it's not that good when it comes to more targeted attacks as the risk of detection is higher. We have also seen more indiscriminate attempts like injecting malicious code in public repositories for common libraries. The latter technique might be useful in very carefully timed attacks when these libraries are used in a very particular project, with the subsequent removal of the malicious code from the repository. Now, can this kind of attack be used in a more targeted way? It appears to be difficult in the case of software because it will leave traces everywhere and the malware is likely to be distributed to several customers. It is more realistic in cases when the provider works exclusively for a specific customer.

What about hardware implants? Are they a real possibility? There has been some recent controversy about that. Even though we saw from Snowden's leaks how hardware can be manipulated on its way to the customer, this does not appear to be something that most actors can do other than the very powerful ones. And even they will be limited by several factors.

However, in cases where the buyer of a particular order is known, it might be more feasible for an actor to try and manipulate hardware at its origin rather than on its way to the customer.

It's difficult to imagine how all the technical controls in an industrial assembly line could be circumvented and how such manipulation could be carried out. We don´t want to discard this possibility, but it would probably entail the collaboration of the manufacturer.

All in all, supply chain attacks are an effective infection vector that we will continue to see. In terms of hardware implants we believe it is extremely unlikely to happen and if it does, we will probably never know....

AND MOBILE

This is in every year's predictions. Nothing groundbreaking is expected, but it's always interesting to think about the two speeds for this slow wave of infections. It goes without saying that all actors have mobile components in their campaigns; it makes no sense only going for PCs. The reality is that we can find many examples of artifacts for Android, but also a few improvements in terms of attacking iOS. Even though successful infections for iPhone requires concatenating several 0-days, it's always worth remembering that incredibly well-resourced actors can pay for such technology and use it in critical attacks. Some private companies claim they can access any iPhone that they physically possess. Other less affluent groups can find some creative ways to circumvent security on such devices using, for instance, rogue MDM servers and asking targets through social engineering to use them in their devices, providing the attackers with the ability to install malicious applications.

It will be interesting to see if the boot code for iOS leaked at the beginning of the year will provide any advantage to the attackers, or if they'll find new ways of exploiting it.

In any case, we don´t expect any big outbreak when it comes to mobile targeted malware, but we expect to see continuous activity by advanced attackers aimed at finding ways to access their targets' devices.

THE OTHER THINGS

What might attackers be thinking about in more futuristic terms? One of the ideas, especially in the military field, might be to stop using weak error-prone humans and replacing them with something more mechanical. With that in mind, and also thinking of the alleged GRU agents expelled from the Netherlands last April after trying to hack into the OPCW's Wi-Fi network as an example, what about using drones instead of human agents for short-range hacking?

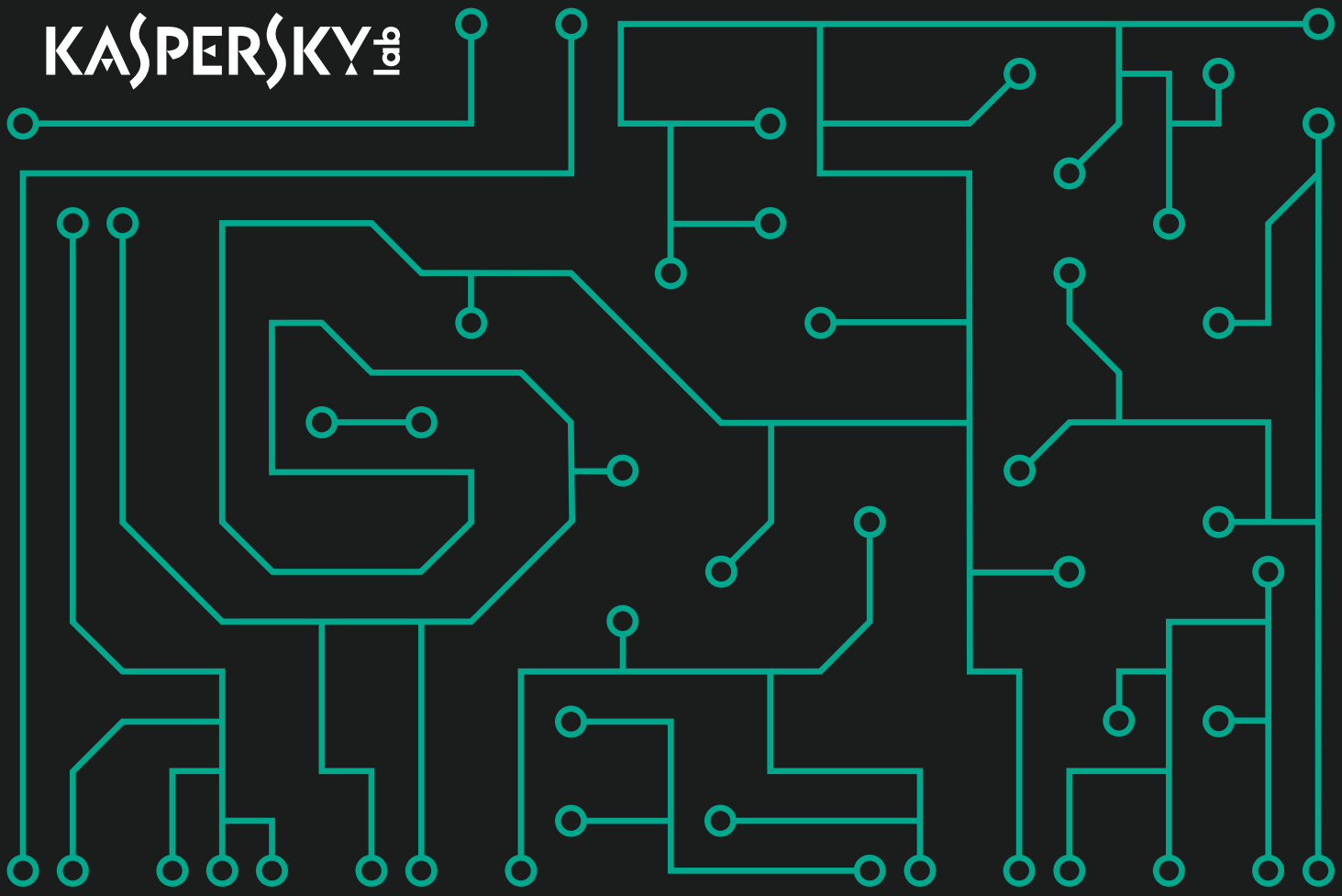
Or what about backdooring some of the hundreds of cryptocurrency projects for data gathering, or even financial gain?

Use of any digital good for money laundering? What about using in-game purchases and then selling such accounts later in the marketplace?

There are so many possibilities that predictions always fall short of reality. The complexity of the environment cannot be fully understood anymore, raising possibilities for specialist attacks in different areas. How can a stock exchange's internal inter-banking system be abused for fraud? I have no idea, I don´t even know if such a system exists. This is just one example of how open to the imagination the attackers behind these campaigns are.

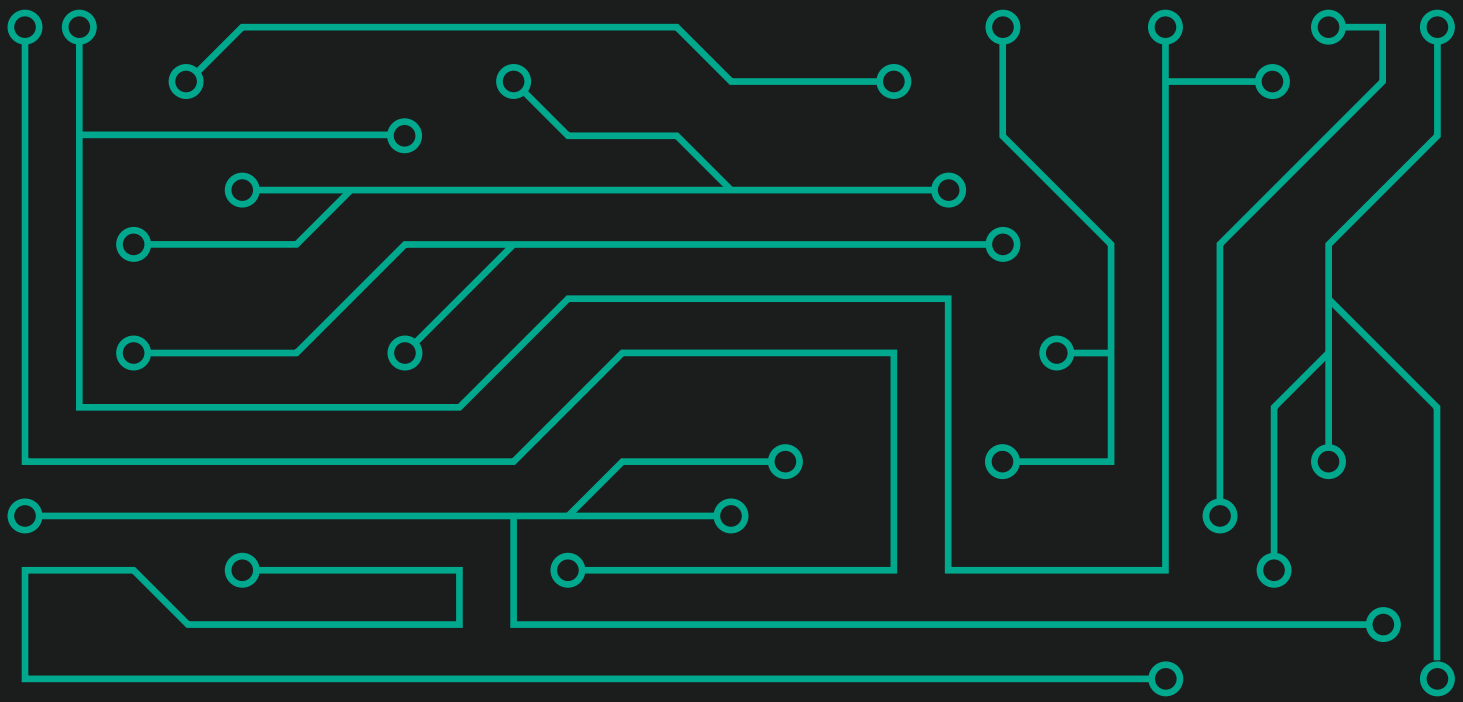
We are here to try and anticipate, to understand the attacks we don´t, and to prevent them from occurring in the future.

KASPERSKY lab



Cyberthreats to financial institutions 2019:

OVERVIEW AND PREDICTIONS



CONTENTS

INTRODUCTION – KEY EVENTS IN 2018

The past year has been extremely eventful in terms of the digital threats faced by financial institutions: cybercrime groups have used new infiltration techniques, and the geography of attacks has become more extensive.

Despite this, let's start the review with a positive trend: in 2018 police arrested a number of well-known cybercrime group members responsible for Carbanak/Cobalt and Fin7, among others. These groups have been involved in attacks on dozens, if not hundreds of companies and financial institutions around the world. Unfortunately, the arrest of group members including the leader of Carbanak, did not lead to a complete halt in activities – in fact, it seemingly started the process of splitting the groups into smaller cells.

The most active actor of 2018 was Lazarus. This group is gradually expanding its arsenal of tools and looking for new targets. The area of interest today includes banks, fin-tech companies, crypto-exchanges, PoS terminals, ATMs, and in terms of geography, we have recorded infection attempts in dozens of countries, most of which are located in Asia, Africa and Latin America.

At the end of last year, we noted that young fin-tech companies and crypto-exchanges are at a higher risk, due to the immaturity of their security systems. This certain type of companies was targeted most often. The most creative attack seen in 2018, from our point of view, was AppleJeus, which targeted cryptocurrency traders. In this case, criminals created special software that looked legitimate and carried out legitimate functions. However, the program also uploaded a malicious update that turned out to be a backdoor. This is a new type of attack, which infects its targets via the supply chain.

Continuing the topic of supply chain attacks, it is worth mentioning the MageCart group, which, by infecting website payment pages (including those of large companies such as British Airways) was able to access a huge amount of payment card data this year. This attack was even more effective because the criminals chose an interesting target – Magento, which is one of the most popular platforms for online stores. Using vulnerabilities in Magento, criminals were able to infect dozens of sites in a technique that is likely to be used by several other groups.

We should also note the development of ATM malware families. In 2018, Kaspersky Lab specialists discovered six new families, meaning that there are now more than 20 of this kind. Some ATM malware families have also evolved: for example, the Plotus malware from Latin America has been updated to a new version, Peralda, and has gained new functionality as a result. The greatest damage associated with attacks on ATMs was caused by infections from internal banking networks, such as FASTCash and ATMJackPot, which allowed attackers to reach thousands of ATMs.

2018 also saw attacks on organizations that use banking systems. Firstly, our machine learning-based behavioral analysis system detected several waves of malicious activity related to the spread of the Buhtrap banking Trojan this year, as attackers embedded their code in popular news sites and forums. Secondly, we detected attacks on the financial departments of industrial companies, where payments of hundreds of thousands of dollars would not cause much suspicion. Often in the final stages of attacks like this, attackers install remote administration tools on infected computers such as RMS, TeamViewer, and VNC.

Before giving our forecasts for 2019, let's see how accurate our forecasts for 2018 turned out to be...

- **Attacks made through the underlying blockchain technologies of financial systems implemented by the financial institutions themselves** – this did not happen in the financial field, but was seen in the online casino sector.
- **More supply chain attacks in the financial world** – yes
- **Attacks on mass media (in general, including Twitter accounts, Facebook pages, telegram channels and more) including hacks and manipulation for getting financial profit through stock/crypto exchange trade** – yes
- **ATM malware automation** – yes. For example, there are malicious programs that immediately give money to attackers.
- **More attacks on crypto exchange platforms** – yes
- **A spike in traditional card fraud due to the huge data breaches that happened in the previous year** – no
- **More nation-state sponsored attacks against financial organizations** – yes
- **The inclusion of fin-techs and mobile-only users in attacks: a fall in the number of traditional PC-oriented internet banking Trojans, with novice mobile banking users becoming the new prime target for criminals** – yes. In particular, some banking Trojans stopped attacking users of online banking on PCs, while the number of Trojans attacking users of mobile devices has more than doubled over the past year.

PREDICTIONS FOR 2019

- **The emergence of new groups due to the fragmentation of Cobalt/Carbnal and Fin7: new groups and new geography**

The arrest of leaders and separate members of major cybercrime groups has not stopped these groups from attacking financial institutions. Next year, we will most likely see the fragmentation of these groups and the creation of new ones by former members, which will lead to the intensification of attacks and the expansion of the geography of potential victims.

At the same time, local groups will expand their activities, increasing quality and scale. It is reasonable to assume that some members of the regional groups may contact former members of the Fin7 or Cobalt group to facilitate access to regional targets and gain new tools with which they can carry out attacks.

- **The first attacks through the theft and use of biometric data**

Biometric systems for user identification and authentication are being gradually implemented by various financial institutions, and several major leaks of biometric data have already occurred. These two facts lay the foundation for the first POC (proof-of-concept) attacks on financial services using leaked biometric data.

- **The emergence of new local groups attacking financial institutions in the Indo-Pakistan region, South-East Asia and Central Europe**

The activity of cybercriminals in these regions is constantly growing: the immaturity of protective solutions in the financial sector and the rapid spread of various electronic means of payment among the population and companies in these regions are contributing to this. Now, all the prerequisites exist for the emergence of a new center for financial threats in Asia, in addition to the three already in Latin America, Korean peninsula and the ex-USSR.

- **Continuation of the supply-chain attacks: attacks on small companies that provide their services to financial institutions around the world**

This trend will remain with us in 2019. Attacks on software providers have proven effective and allowed attackers to gain access to several major targets. Small companies (that supply specialized financial services for the larger players) will be jeopardized first, such as the suppliers of money transfer systems, banks and exchanges.

- **Traditional cybercrime will focus on the easiest targets and bypass anti-fraud solutions: replacement of PoS attacks with attacks on systems accepting online payments**

Next year, in terms of threats to ordinary users and stores, those who use cards without chips and do not use two-factor authorization of transactions will be the most at risk. The malicious community has focused on some simple goals that are easy to monetize. However, this does not mean that they do not use any complex techniques. For example, to bypass anti-fraud systems, they copy all computer and browser system settings. On the other hand, this cybercriminal behavior will mean that the number of attacks on PoS terminals will decrease, and they will move towards attacks on online payment platforms instead.

- **The cybersecurity systems of financial institutions will be bypassed using physical devices connected to the internal network**

Due to the lack of physical security and the lack of control over connected devices in many networks, cybercriminals will more actively exploit situations where a computer or mini-board can be installed, specifically configured to steal data from the network and transfer the information using 4G/LTE modems.

Attacks like this will provide cybergangs with an opportunity to access various data, including information about the customers of financial institutions, as well as the network infrastructure of financial institutions.

- **Attacks on mobile banking for business users**

Mobile applications for business are gaining popularity, which is likely to lead to the first attacks on their users. There are enough tools for this, and the possible losses that businesses incur are much higher than the losses incurred when individuals are attacked. The most likely attack vectors are attacks at the Web API level and through the supply chain.

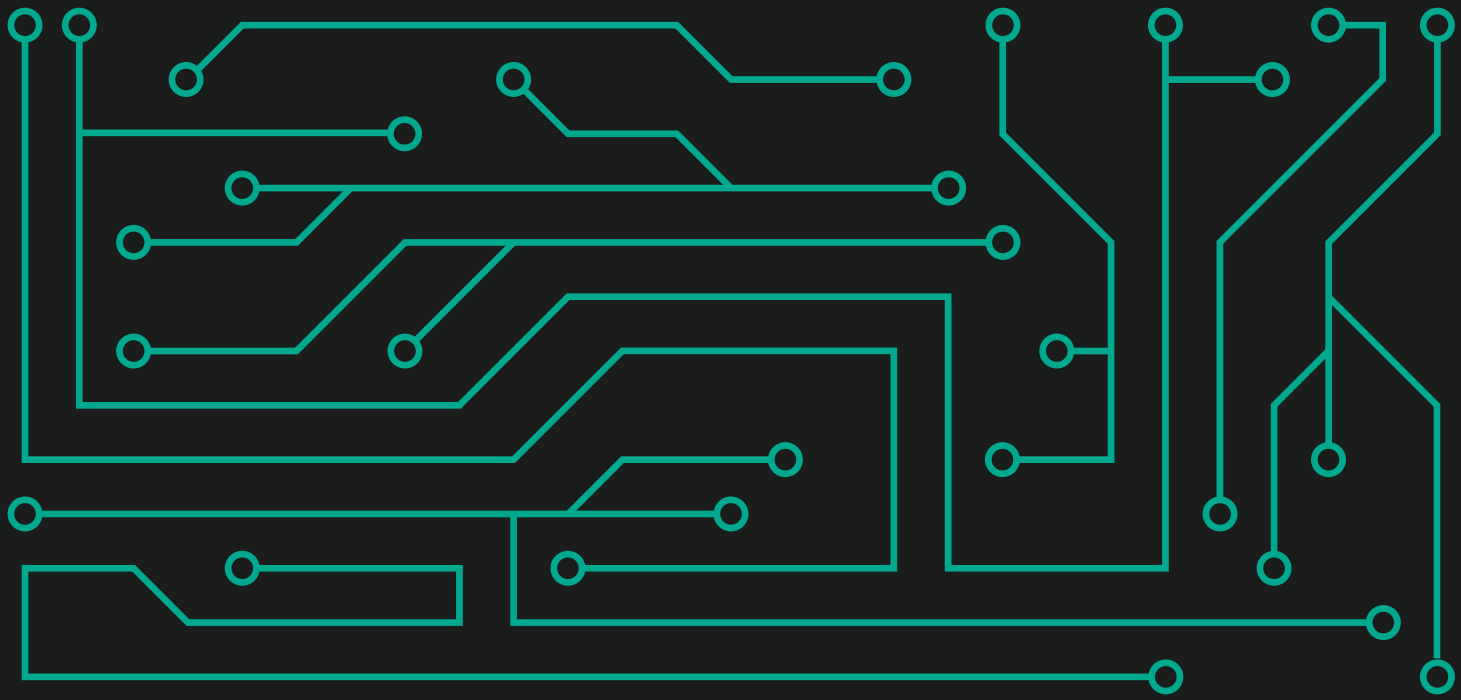
- **Advanced social engineering campaigns targeting operators, secretaries and other internal employees in charge of wires: result of data leaks**

Social engineering is particularly popular in some regions, for example Latin America. Cybercriminals keep targeting specific people in companies and financial institutions to make them wire big sums of money. Due to high amount of data leakages previous years this type of attacks becomes more effective, since criminals are able to use leaked internal information about targeted organization to make their messages look absolutely legit. Main idea remains the same: they make these targets believe that the financial request has come from business partners or directors. These techniques use zero malware, but demonstrate how targeted social engineering gets results and will become more powerful in 2019. This includes attacks like "simswap".

KASPERSKY lab

Kaspersky Security Bulletin:

THREAT PREDICTIONS FOR INDUSTRIAL SECURITY IN 2019



The past few years have been very intense and eventful when it comes to incidents affecting the information security of industrial systems. That includes new vulnerabilities, new threat vectors, accidental infections of industrial systems and detected targeted attacks. In response, last year we developed some Threat Predictions for Industrial Security in 2018, outlining the trends most likely to unfold in the year ahead.

The industrial cybersecurity threat landscape moves at a slower and more rigid pace than the information technology threat landscape in general. Attacks on ICS are still hard to monetize. Industrial organizations are still out of scope for the majority of cybercriminals. They are a relatively new target for adversaries who have already started attacking them. These are still applying existing tools and tactics to their attacks. That is why the majority of the industrial threat predictions from last year are still unfolding, although some of them have already come true.

Kaspersky Lab specialists have spent a few years investigating the cyberthreat landscape for industrial organizations and trying to bring their expertise and technology to OT environments. We are still on a long journey, with various to difficulties cope with and problems yet to solve. Constantly keeping in contact with many researchers in other security organizations and some ICS security pioneers from inside industrial companies; we have come to the conclusion that some of the difficulties we face are common to the industry. Solving some of those is mandatory to make the world more secure and safe.

So, although the fog of 2018's predictions and threat landscape has yet to clear, we decided to focus on the major problems likely to affect the work of professionals involved in industrial systems in 2019.

TOP FOUR CYBERSECURITY CHALLENGES FACING INDUSTRIAL ENTERPRISES IN 2019

1. The ever-increasing attack surface

The increasing amount of automation systems, the variety of automation tools, number of organizations and individuals with direct or remote access to automation systems, as well as the emergence of communication channels for monitoring and remote control between previously independent objects – all expand the opportunities for criminals to plan and execute their attacks.

2. Growing interest of cybercriminals and special services

A decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new targets, including those within industrial organizations.

At the same time, special services in many countries, as well as other organized groups – motivated by internal and external political interests – and financially-motivated groups, are actively engaged in the research and development of techniques to implement espionage and terrorist attacks aimed at industrial enterprises.

Taking into account the current geopolitical context, the development of industrial enterprises' automation systems, and the transition to new management processes and models of production and economic activity, this situation will continue to develop in the coming years, negatively affecting industrial organizations.

3. The underestimation of general threat levels

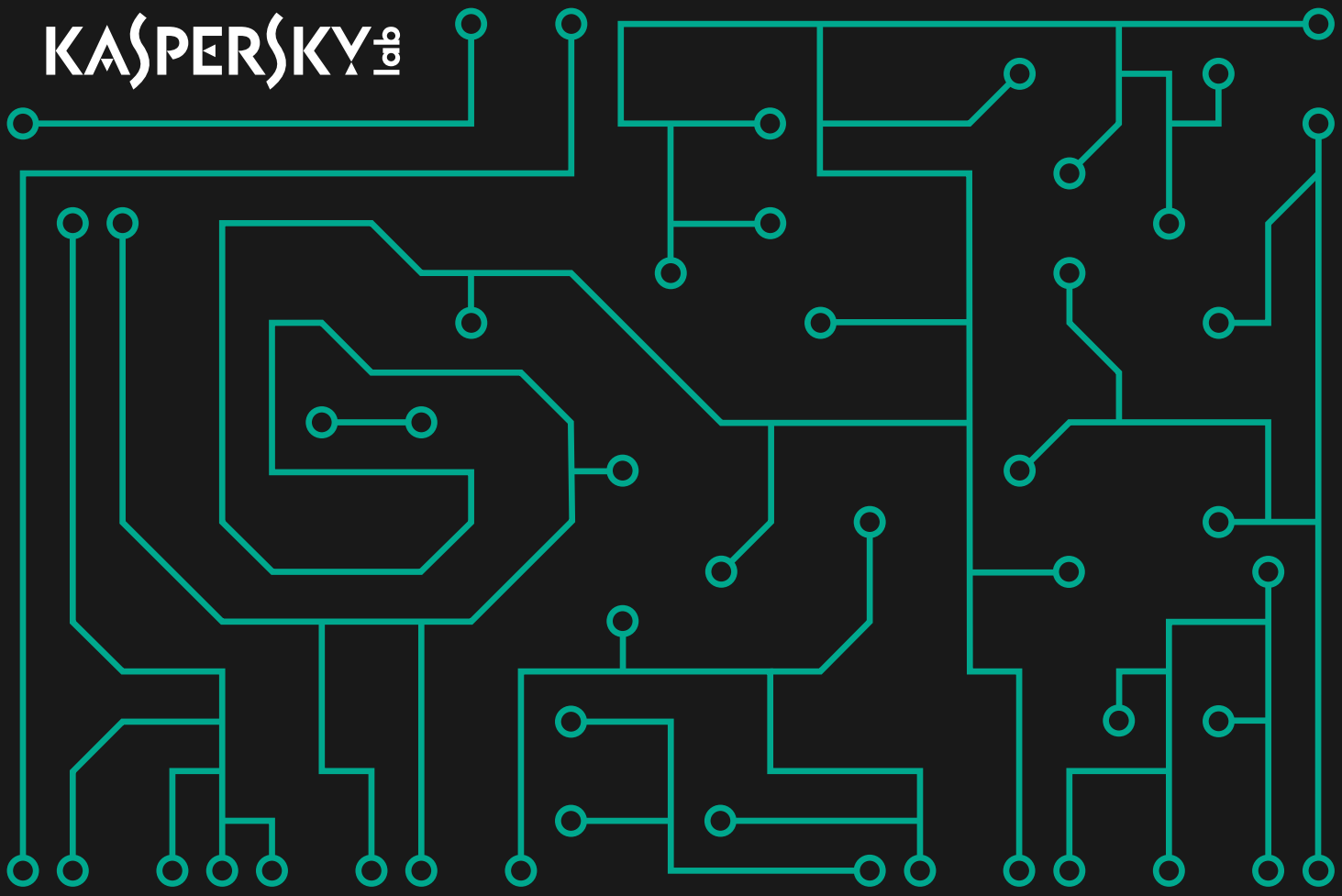
A lack of public access to information about information security issues within industrial enterprises, coupled with the relative rarity of targeted attacks on automation systems, an excessive belief in emergency protection systems and the denial of objective reality is having a negative effect on the assessment of threat levels by owners and operators of industrial enterprises and their personnel.

4. The misunderstanding of threat specifics and the suboptimal choice of protection options

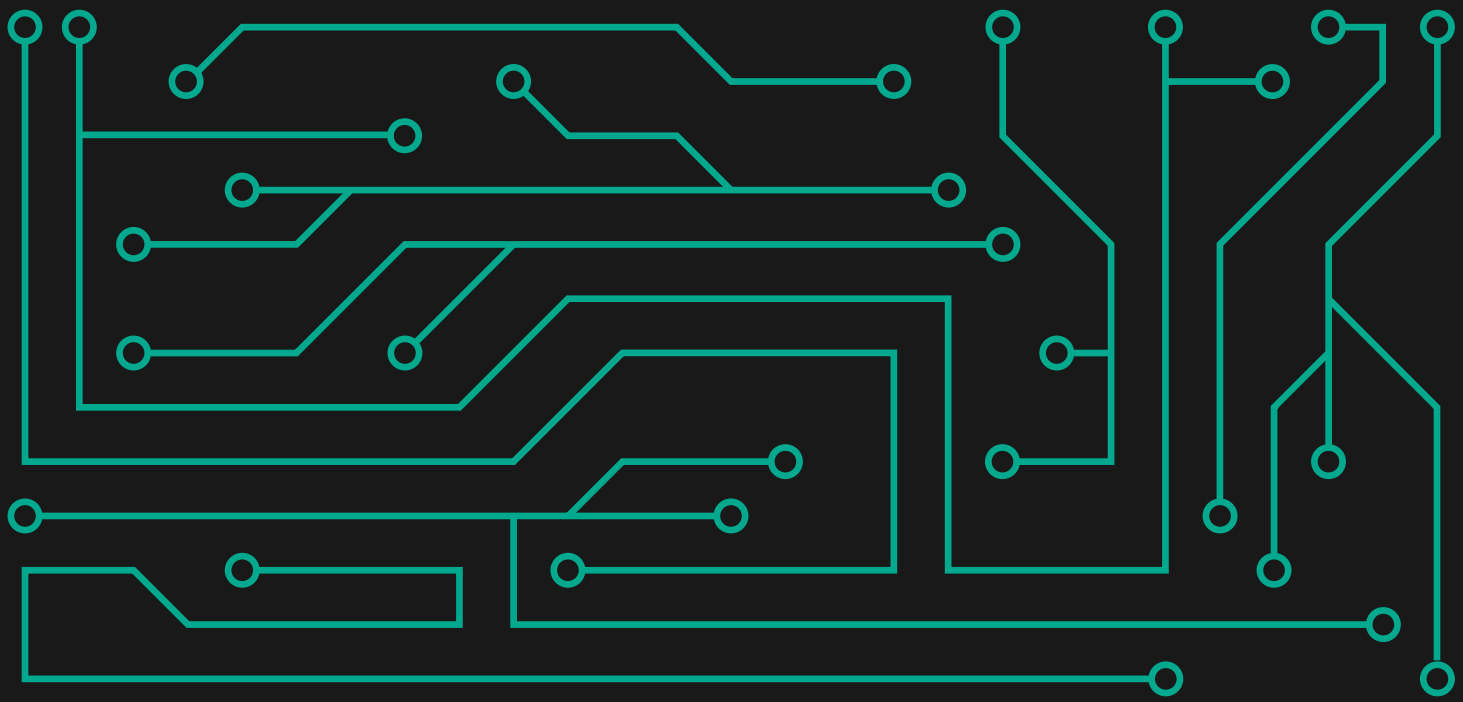
In the world of industrial cybersecurity, several high–profile incidents carried out with the help of targeted attacks against a very limited number of victims, created an information landscape that formed fully the idea of a potential threat – both among information security researchers and security developers, and among potential users of these tools.

However, the professional reporting of these incidents was often too difficult to understand by the majority of potential users, and was devoid of important OT details. The information field formed in these conditions, including the absence of a daily need to deflect the attacks aimed at automated control systems, gave developers a chance to create products that might protect better from the artificial scenarios thought up by researchers themselves, than from real world day-to-day threats. This could leave the automation systems of industrial enterprises vulnerable to real life attacks, including random ones and targeted attack campaigns organized by cyber criminals.

KASPERSKY lab



CRYPTOCURRENCY THREAT PREDICTIONS FOR 2019



CONTENTS

INTRODUCTION – KEY EVENTS IN 2018

2018 saw cryptocurrency become an established part of many people's lives, and a more attractive target for cybercriminals across the world. To some extent, the malicious mining of cryptocurrencies even prevailed over the main threat of the last few years: ransomware.
However, in the second half of 2018, the blockchain and cryptocurrency industry faced a major development: falling prices for cryptocurrencies. The impact was felt across the landscape, with rapid decline in public interest, the activity of the crypto community and traders, and in the related activity of cybercriminals.
While this will certainly affect our forecasts for 2019, let's see how the forecasts we made for this year worked out.

1. 'Ransomware attacks will force users to buy cryptocurrency'

This prediction turned out to be partially true. In 2018, we saw a decline in the popularity of encryptors, combined with a rise in the malicious use of cryptocurrency miners. It transpired that it is safer for attackers to perform discreet mining on infected devices than to demand a ransom and attract attention. However, it is too early to dismiss ransomware as a major threat; it is still an effective method of infection and monetization of both individuals and organizations – and cryptocurrencies remain a more easily anonymized form of ransom payment.

2. 'We will see targeted attacks with malicious miners'

This prediction did not come true. We observed mainly isolated incidents where miners were maliciously installed in an infected corporate network. There are several reasons for that:

1. Companies have learned to detect miners that are run on the computers of employees/administrators; both those installed by users themselves and by third parties without the knowledge of the user.

2. The attackers themselves do not appear to consider this a promising approach. Targeted and sophisticated attacks are more about gaining persistence in the network for the purpose of espionage or the theft of money or data. It is therefore better not to attract attention by crypto-mining.

3. 'The rise of miners will continue and involve new actors'

This prediction also turned out to be partially true: the malicious use of cryptocurrency miners actively increased during the first quarter of 2018, peaking in March. Over the following months there was a gradual decrease in activity due to the drop in price for cryptocurrencies.

4. 'There will be more web-mining'

Again, this prediction turned out to be partially true. The web mining of cryptocurrencies reached a peak in January 2018, after which it began to decline. Webmasters, hoping to use web mining as an alternative means of website monetization alongside advertising, did not usually notify users about any hidden mining taking place on their sites. This meant that web mining quickly became associated with malicious activity. After that, it was difficult to restore its reputation.

5. 'The fall of ICOs (Initial Coin Offering)'

Yes and no. On the one hand, collecting money with the help of ICOs continued: projects became larger and the fees did not fall. On the other hand, many projects that collected impressive amounts through ICOs in 2017 were not be able to create the promised product in time during 2018, which inevitably affected the exchange price of the sold tokens.

TOP THREE PREDICTIONS FOR 2019

1. Excessive expectations about the use of blockchain beyond the cryptocurrency sphere will disappear

In the end, we expect this trend to be driven by people rather than the technology's capability, as organizations and industries come to the conclusion that blockchain has a rather narrow scope of application, and most attempts to use in different ways are not justified. The reliable application of blockchain beyond cryptocurrency has been explored and experimented with for years, but there is little evidence of achievement. We expect 2019 to be the year people stop trying.

2. Cryptocurrencies as a means of payment will decline further

In 2017 a number of suppliers of goods and services announced that they would accept cryptocurrencies as a form of payment. However, in the face of huge commissions (an acute problem in December 2017), slow transfers, a large price for integration, and, most importantly, a small number of customers, its use as a method of payment declined steadily. In the end, the use of cryptocurrencies by a legitimate business simply does not make much sense.

3. There will be no return to 2017's sky-high exchange rates

Until January 2018, there were immense highs and lows in the price of Bitcoin. But we do not expect these to return as the value of cryptocurrencies levels out to reflect their popularity. We believe there is a finite audience for whom cryptocurrencies are of interest, and once that limit is reached the price will not rise further.