Kaspersky Security Bulletin '19

kaspersky

Contents

Kaspersky Security Bulletin ‘19

APT review

kaspersky

Contents

What the world’s threat actors got up to in 2019

What were the most interesting developments in terms of APT activity during the year and what can we learn from them?

This is not an easy question to answer, because researchers have only partial visibility and it´s impossible to fully understand the motivation for some attacks or the developments behind them. However, let´s try to approach the problem from different angles in order to get a better understanding of what happened with the benefit of hindsight and perspective.

Compromising supply chains

Targeting supply chains has proved very successful for attackers in recent years – high-profile examples include ShadowPad, ExPetr and the backdooring of CCleaner. In our threat predictions for 2019, we flagged this as a likely continuing attack vector. We didn’t have to wait very long to see this prediction come true.

In January, we discovered a sophisticated supply-chain attack involving a popular consumer hardware vendor, the mechanism used to deliver BIOS, UEFI and software updates to vendor’s laptops and desktops. The attackers behind Operation ShadowHammer added a backdoor to the utility and then distributed it to users through official channels. The goal of the attack was to target with precision an unknown pool of users, identified by their network adapter MAC addresses. The attackers hardcoded a list of MAC addresses into the Trojanized samples, representing the true targets of this massive operation. We were able to extract over 600 unique MAC addresses from more than 200 samples discovered in this attack, although it’s possible that other samples exist that target different MAC addresses. You can read our reports on ShadowHammer here and here.

Disinformation

Q3 was interesting for APT developments in the Middle East, especially considering the multiple leaks of alleged Iranian activity that were published within just a few weeks of each other. Even more interesting is the possibility that one of the leaks may have been part of a disinformation campaign carried out with the help of the Sofacy/Hades actor.

In March, someone going by the handle Dookhtegan or Lab_dookhtegan started posting messages on Twitter using the hashtag #apt34. They shared several files via Telegram that supposedly belonged to the OilRig threat actor. These included logins and passwords of several alleged hacking victims, tools, details of infrastructure potentially related to different intrusions, the résumés of the alleged attackers and a list of web shells – apparently relating to the period 2014-18. The targeting and TTPs are consistent with the OilRig threat actor, but it was impossible to confirm the origins of the tools included in the dump. If the data in the dump is accurate, it would also show the global reach of the OilRig group, which most researchers had thought operates primarily in the Middle East.

On April 22, an entity going by the alias Bl4ck_B0X created a Telegram channel named GreenLeakers. The purpose of the channel, as stated by its creator, was to publish information about the members of the MuddyWater APT group, "along with information about their mother and spouse and etc." for free. In addition to this free information, the Bl4ck_B0X actor(s) also hinted that they would put up for sale "highly confidential" information related to MuddyWater. On April 27, three screenshots were posted in the GreenLeakers Telegram channel containing alleged screenshots from a MuddyWater C2 server. On May 1, the channel was closed to the public and its status was changed to private. This was before Bl4ck_B0X had the chance to publish the promised information on the MuddyWater group. The reason for the closure is still unclear.

Finally, a website named Hidden Reality published leaks allegedly related to an entity named the Iranian RANA institute. It was the third leak in two months disclosing details of alleged Iranian threat actors and groups. Interestingly, this leak differed from the others by employing a website that allowed anyone to browse the leaked documents. It also relied on Telegram and Twitter profiles to post messages related to Iranian CNO capabilities. The Hidden Reality website contains internal documents, chat messages and other data related to the RANA institute's CNO (computer network operations) capabilities, as well as information about victims. Previous leaks had focused more on tools, source code and individual actor profiles.

Close analysis of the materials, the infrastructure and the dedicated website used by the leakers provided clues that lead us to believe that Sofacy/Hades may be connected to these leaks.

Lost in Translation and Dark Universe

The well-known Shadow Brokers leak, Lost in Translation, included an interesting Python script – sigs.py – that contained lots of functions to check if a system had already been compromised by another threat actor. Each check is implemented as a function that looks for a unique signature in the system – for example, a file with a unique name or registry path. Although some checks are empty, sigs.py lists 44 entries, many of them related to unknown APTs that have not yet been publicly described.

In 2019, we identified the APT described as the 27th function of the sigs.py file, which we call DarkUniverse. We assess with medium confidence that DarkUniverse is connected with the ItaDuke set of activities due to unique code overlaps.

The main component is a rather simple DLL with only one exported function that implements persistence, malware integrity, communication with the C2 and control over other modules. We found about 20 victims in Western Asia and Northeastern Africa, including medical institutions, atomic energy bodies, military organizations and telecommunications companies.

Mobile attacks

Mobile implants are now a standard part of the toolset of many APT groups; and we have seen ample evidence of this during 2019.

In May, the FT reported that hackers had exploited a zero-day vulnerability in WhatsApp, enabling them to eavesdrop on users, read their encrypted chats, turn on the microphone and camera and install spyware that allows even further surveillance. To exploit the vulnerability, the attacker simply needed to call the victim via WhatsApp. This specially crafted call triggered a buffer overflow in WhatsApp, allowing the attacker to take control of the application and execute arbitrary code in it. The hackers apparently used this, not only to snoop on people's chats and calls, but also to exploit previously unknown vulnerabilities in the operating system, which allowed them to install applications on the device. WhatsApp quickly released a patch for the exploit – and that seemed to be that. However, in October, the company filed a lawsuit accusing Israel-based NSO Group of having created the exploit. WhatsApp claims that the technology sold by NSO was used to target the mobile phones of more than 1,400 of its customers in 20 different countries, including human rights activists, journalists and others. NSO denies the allegations.

In July, we published a private report about the latest versions of FinSpy for Android and iOS, developed in mid-2018. The developers of FinSpy sell the software to government and law enforcement organizations all over the world, who use it to collect a variety of private user information on various platforms. The mobile implants are similar for iOS and Android. They are capable of collecting personal information such as contacts, messages, emails, calendars, GPS location, photos, files in memory, phone call recordings and data from the most popular messengers. The Android implant includes functionality to gain root privileges on an unrooted device by abusing known vulnerabilities. It seems that the iOS solution does not provide infection exploits for its customers, but is fine-tuned to clean traces of publicly available jailbreaking tools: this suggests that physical access to the victim's device is required in cases where devices are not already jailbroken. The latest version includes multiple features that we have not observed before. During our recent research, we detected up-to-date versions of these implants in the wild in almost 20 countries, but the size of the customer base would suggest that the real number of victims could be much higher.

In August, Google's Project Zero team published an extensive analysis of at least 14 iOS zero-days found in the wild and used in five exploitation chains to escalate privileges by an unknown threat actor. According to Google, the attackers used a number of 'water-holed' websites to deliver the exploits – possibly from as long as three years ago. While the blog contained no details about the compromised sites, or whether they were still active, Google claimed the websites had received "thousands of visitors per week". The lack of victim discrimination points to a relatively non-targeted attack. However, the not-so-high estimate of the number of visitors to the water-holed sites, and the capabilities needed to deliver and install this malware, and keep the exploitation chains up-to-date for more than two years, shows a high level of resources and dedication.

In September, Zerodium, a zero-day brokerage firm, indicated that a zero-day for Android was now worth more than one for iOS – the company is now willing to pay $2.5 million for a zero-click Android zero-day with persistence. This is a significant increase on the company's previous payout ceiling of $2 million for remote iOS jailbreaks. By contrast, Zerodium has also reduced payouts for Apple one-click exploits. On the same day, someone found a high-severity zero-day in the v412 (Video4Linux) driver, the Android media driver. This vulnerability, which could enable privilege escalation, was not included in Google's September security update. A few days later, an Android flaw was identified that left more than a billion Samsung, Huawei, LG and Sony smartphones vulnerable to an attack that would allow an attacker to gain full access to emails on a compromised device using an SMS message. Whatever the relative value of Android and iOS exploits, it's clear that mobile exploits are a valuable commodity.

Established threat actors continue to revamp their tools

While investigating some malicious activity in Central Asia, we identified a new backdoor, named Tunnus, which we attribute to Turla. This is.NET-based malware with the ability to run commands or perform file actions on an infected system and send the results to its C2. So far, the threat actor has built its C2 infrastructure with vulnerable WordPress installations.

This year, Turla also wrapped its notorious JavaScript KopiLuwak malware in a dropper called Topinambour, a new.NET file that the threat actor is using to distribute and drop KopiLuwak through infected installation packages for legitimate software programs such as VPNs. The malware is almost completely 'fileless': the final stage of infection, an encrypted Trojan for remote administration, is embedded into the computer's registry for the malware to access when ready. The group uses two KopiLuwak analogues – the.NET RocketMan Trojan and the PowerShell MiamiBeach Trojan – for cyber-espionage; we believe Turla deploys these versions where their targets are protected with security software capable of detecting KopiLuwak.

We also observed a new COMpfun-related targeted campaign using new malware. The Kaspersky Threat Attribution Engine shows strong code similarities between the new family and the old COMpfun. Moreover, the attackers use the original COMpfun as a downloader in one of the spreading mechanisms. We named the newly identified modules Reductor after a.pdb path left in some of the samples. We believe the same COMPfun authors, who we tentatively associate with Turla based on victimology, developed this malware. One striking aspect of Reductor is that the threat actors put a lot of effort into manipulating installed digital root certificates and marking outbound TLS traffic with unique host-related identifiers. The malware adds embedded root certificates to the target host and allows operators to add additional ones remotely through a named pipe. The authors don't touch the network packets at all. Instead, they analyze Firefox source and Chrome binary code to patch the corresponding system pseudo-random number generation (PRNG) functions in the process's memory. Browsers use PRNG to generate the 'client random' sequence during the very beginning of the TLS handshake. Reductor adds the victims' unique encrypted hardware- and software-based identifiers to this 'client random' field.

Zebrocy has continued adding new tools to its arsenal using various kinds of programming languages. We found Zebrocy deploying a compiled Python script, which we call PythocyDbg, within a Southeast Asian foreign affairs organization. This module primarily provides for the stealthy collection of network proxy and communications debug capabilities. In early 2019, Zebrocy shifted its development efforts with the use of Nimrod/Nim, a programming language with syntax resembling both Pascal and Python that can be compiled down to JavaScript or C targets. Both the Nim downloaders that the group mainly uses for spear phishing, and other Nim backdoor code, are currently being produced by Zebrocy and delivered alongside updated compiled AutoIT scripts, Go, and Delphi modules. In September, Zebrocy spear-phished multiple NATO and alliance partners throughout Europe, attempting to gain access to email communications, credentials and sensitive documents. This campaign is similar to past Zebrocy activity, with target-relevant content used within emails, and ZIP attachments containing harmless documents alongside executables with altered icons and identical filenames. The group also makes use of remote Word templates pulling contents from the legitimate Dropbox file-sharing site. In this campaign, Zebrocy targeted defense and diplomatic targets located throughout Europe and Asia with its Go backdoor and Nimcy variants.

In June, we came across an unusual set of samples used to target diplomatic, government and military organizations in countries in South and Southeast Asia that we attribute to Platinum – one of the most technologically advanced APT actors. In this campaign, the attackers used an elaborate, previously unseen steganographic technique to conceal communication. A couple of years ago, we predicted that more and more APT and malware developers would use steganography, and this campaign provides proof. Interestingly, the attackers decided to implement the utilities they need as one huge set – an example of the framework-based architecture that is becoming more and more popular. Later in the year, we discovered Platinum using a new backdoor, which we call Titanium, in a new campaign. Interestingly, we found certain similarities between this malware and a toolset that we called ProjectC. We detected ProjectC in 2016 being used as a toolset for lateral movement and we attributed it with low confidence to CloudComputating. Our new findings lead us to believe that the CloudComputating set of activities can be attributed to Platinum and that ProjectC was one of its toolsets.

One of the key findings of our 2018 report on Operation AppleJeus was the ability of the Lazarus group to target Mac OS. Since then, Lazarus has expanded its operations for this platform. This year, we discovered a new operation, active for at least a year, which utilizes PowerShell to control Windows systems and Mac OS malware to target Apple customers. Lazarus also targeted a mobile gaming company in South Korea that we believe was aimed at stealing application source code. It's clear that Lazarus keeps updating its tools very quickly.

In Q3, we tracked new activity by BlueNoroff, a sub-group of Lazarus. In particular, we identified a bank in Myanmar that this threat actor compromised. We promptly contacted the bank, to share the IoCs we had found. Our collaboration allowed us to obtain valuable information on how the attackers move laterally to access high-value hosts, such as those owned by the bank's system engineers interacting with SWIFT. They use a public login credential dumper and homemade PowerShell scripts for lateral movement. BlueNoroff also employs new malware with an uncommon structure, probably to slow down analysis. Depending on the command line parameters, this malware can run as a passive backdoor, an active backdoor or a tunneling tool; we believe the group runs this tool in different modes depending on the situation. Moreover, we found another type of PowerShell script used by this threat actor when it attacked a target in Turkey. This PowerShell script has similar functionality to those used previously, but BlueNoroff keeps changing it to evade detection.

Andariel, another sub-group of Lazarus, has traditionally focused on geo-political espionage and financial intelligence in South Korea. We observed new efforts by this actor to build a new C2 infrastructure targeting vulnerable Weblogic servers, in this case exploiting CVE-2017-10271. Following a successful breach, the attackers implanted malware signed with a legitimate signature belonging to a South Korean security software vendor. The malware is a brand new type of backdoor, called ApolloZeus, which is started by a shellcode wrapper with complex configuration data. This backdoor uses a relatively large shellcode in order to make analysis difficult. In addition, it implements a set of features to execute the final payload discreetly. The discovery of this malware allowed us to find several related samples, as well as documents used by the attackers to distribute it, providing us with a better understanding of the campaign.

In October, we reported a campaign that began when we stumbled upon a sample that uses interesting decoy documents and images containing a contact list of North Korean overseas residents. Almost all of the decoys contain content regarding the national holiday of the Korean Peninsula and the national day of North Korea. The lure content was also related to diplomatic issues or business relationships. Alongside the additional data from our telemetry, we believe that this campaign is aimed at targets with a relationship with North Korea, such as business people, diplomatic entities and human rights organizations. The actor behind this campaign used high-profile spear phishing and multi-stage infection in order to implant tailored Ghost RAT malware that can fully control the victim. We believe that the threat actor behind this campaign, which has been ongoing for more than three years, speaks Korean; and we believe that the DarkHotel APT group is behind it.

The Lamberts is a family of sophisticated attack tools used by one or multiple threat actors. The arsenal includes network-driven backdoors, several generations of modular backdoors, harvesting tools and wipers for carrying out destructive attacks. We created a colour scheme to distinguish the various tools and implants used against different victims around the world. More information about the Lamberts arsenal is available in our 'Unraveling the Lamberts Toolkit' report, available to our APT Intel customers. This year, we added several new colours to the Lamberts palette. The Silver Lambert, which appears to be the successor of Gray Lambert, is a full-fledged backdoor, implementing some specific NOBUS and OPSEC concepts such as protection from C2 sink-holing by checking the server SSL certificate hash, self-uninstall for orphaned instances (i.e. where the C2 is unavailable) and low level file-wiping functionality. We observed victims of Silver Lambert in China, in the Aeronautics sector. Violet Lambert, a modular backdoor that appears to have been developed and deployed in 2018, is designed to run on various versions of Windows – including Windows XP, as well as Vista and later versions of Windows. We observed victims of Violet Lambert in the Middle East. We also found other new Lamberts implants on computers belonging to a critical infrastructure victim in the Middle East. The first two we dubbed Cyan Lambert (including Light and Pro versions). The third, which we called Magenta Lambert, reuses older Lamberts code and has multiple similarities with the Green, Black and White Lamberts. This malware listens on the network, waiting for a magic ping, and then executes a very well-hidden payload that we have been unable to decrypt. All the infected computers went offline shortly after our discovery.

Early in the year, we monitored a campaign by the LuckyMouse threat actor that had been targeting Vietnamese government and diplomatic entities abroad since at least April 2018. We believe that this activity, which we call SpoiledLegacy, is the successor to the IronTiger campaign because of the similar tools and techniques it uses. The SpoiledLegacy operators use penetration-testing frameworks such as Cobalt Strike and Metasploit. While we believe that they exploit network service vulnerabilities as their main initial infection vector, we have also observed executables prepared for use in spear-phishing messages containing decoy documents, showing the operator's flexibility. Besides pen-testing frameworks, the operators use the NetBot downloader and Earthworm SOCKS tunneler. The attackers also include HTran TCP proxy source code into the malware, to redirect traffic. Some NetBot configuration data contains LAN IPs, indicating that it downloads the next stage from another infected host in the local network. Based on our telemetry, we believe that internal database servers are among the targets, as in a previous LuckyMouse Mongolian campaign. As the last stage, the attackers use different in-memory 32- and 64-bit Trojans injected into system process memory. Interestingly, all the tools in the infection chain dynamically obfuscate Win32 API calls using leaked HackingTeam code. From the start of 2019, we observed a spike in LuckyMouse activity, both in Central Asia and in the Middle East. For these new campaigns, the attackers seem to focus on telecommunications operators, universities and governments. The infection vectors are direct compromise, spear phishing and, possibly, watering holes. Despite different open-source publications discussing this actor's TTPs during the last year, LuckyMouse hasn't changed any of them. The threat actor still relies on its own tools to get a foothold in the victim's network, which in the new campaigns consists of using HTTPBrowser as a first stager, followed by the Soldier Trojan as a second stage implant. The group made a change to its infrastructure, as it seems to rely uniquely on IPv4 addresses instead of domain names for its C2s, which we see as an attempt to limit correlation.

The HoneyMyte APT has been active for several years. The group has adopted different techniques to perform its attacks over the past couple of years, and has targeted governments in Myanmar, Mongolia, Ethiopia, Vietnam and Bangladesh, along with remote foreign embassies located in Pakistan, South Korea, the US, the UK, Belgium, Nepal, Australia and Singapore. This year, the group has targeted government organizations related to natural resource management in Myanmar and a major continental African organization, suggesting that one of the main motivations of HoneyMyte is gathering geopolitical and economic intelligence. While the group targeted a military organization in Bangladesh, it's possible that the individual targets were related to geo-political activity in the region.

The Icefog threat actor, which we have been tracking since 2011, has consistently targeted government institutions, military contractors, maritime and shipbuilding organizations, telecom operators, satellite operators, industrial and high technology companies, and mass media located mainly in Korea, Japan and Central Asia. Following our original report on Icefog in 2013, the group's operational tempo slowed and we detected a very low number of active infections. We observed a slight increase in 2016; then, beginning in 2018, Icefog began conducting large waves of attacks against government institutions and military contractors in Central Asia, which are strategically important to China's Belt and Road Initiative. In the latest wave of attacks, the infection began with a spear-phishing email containing a malicious document that exploits a known vulnerability and ultimately deploys a payload. From 2018 to the beginning of 2019, the final payload was the typical Icefog backdoor. Since May 2019, the actors appear to have switched and are now using Poison Ivy as their main backdoor. The Poison Ivy payload is dropped as a malicious DLL and is loaded using a signed legitimate program, using a technique called load order hijacking. This technique is very common with many actors and it was also used in previous Icefog campaigns. During our investigation, we were also able to detect artefacts used in the actor's lateral movement. We observed the use of a public TCP scanner downloaded from GitHub, a Mimikatz variant to dump credentials from system memory, a customized keylogger to steal sensitive information, and a newer version of another backdoor named Quarian. The Quarian backdoor was used to create tunnels inside the victim infrastructure in an attempt to avoid network detections. The functionality of Quarian includes the ability to manipulate the remote file system, get information about the victim, steal saved passwords, download or upload arbitrary files, create tunnels using port forwarding, execute arbitrary commands, and start a reverse shell.

Evolution of the 'newcomers'

We first discussed ShaggyPanther, a previously unseen malware and intrusion set targeting Taiwan and Malaysia, in a private report in January 2018. Related activities date back to more than a decade ago, with similar code maintaining compilation timestamps from 2004. Since then, ShaggyPanther activity has been detected in several more locations: most recently in Indonesia in July, and – somewhat surprisingly – in Syria in March. The newer 2018 and 2019 backdoor code maintains a new layer of obfuscation and no longer maintains clear-text C2 strings. Since our original release, we have identified an initial server-side infection vector from this actor, using SinoChopper/ChinaChopper, a commonly used web shell shared by multiple Chinese-speaking actors. SinoChopper not only performs host identification and backdoor delivery but also email archive theft and additional activity. Although not all incidents can be traced back to server-side exploitation, we did detect a couple of cases and obtained information about their staged install process. In 2019, we observed ShaggyPanther targeting Windows servers.

In April, we published our report on TajMahal, a previously unknown APT framework that has been active for the last five years. This is a highly sophisticated spyware framework that includes backdoors, loaders, orchestrators, C2 communicators, audio recorders, keyloggers, screen and webcam grabbers, documents, and cryptography key stealers; and even its own file indexer for the victim's computer.

We discovered up to 80 malicious modules stored in its encrypted Virtual File System – one of the highest numbers of plugins we have ever seen in an APT toolset. The malware features its own indexer, emergency C2s, the ability to steal specific files from external drives when they become available again, and much more. There are two different packages, self-named Tokyo and Yokohama and the targeted computers we found include both packages. We think the attackers used Tokyo as the first stage infection, deploying the fully functional Yokohama package on interesting victims, and then leaving Tokyo in place for backup purposes. Our telemetry revealed just a single victim, a diplomatic body from a country in Central Asia. This begs the question, why go to all that trouble for just one victim? We think there may be other victims that we haven't found yet. This theory is supported by the fact that we couldn't see how one of the files in the VFS was used by the malware, opening the door to the possibility of additional versions of the malware that have yet to be detected.

In February, our AEP (Automatic Exploit Prevention) systems detected an attempt to exploit a vulnerability in Windows – the fourth consecutive exploited Local Privilege Escalation vulnerability in Windows that we had discovered in the preceding months. Further analysis led us to uncover a zero-day vulnerability in win32k.sys. Microsoft patched this vulnerability, CVE-2019-0797, on March 12, crediting Kaspersky researchers Vasiliy Berdnikov and Boris Larin with the discovery. We think that several threat actors, including FruityArmor and SandCat, used this exploit. FruityArmor had used zero-days before, while SandCat is a new APT actor that we discovered not long before. Interestingly, FrutiyArmor and SandCat seem to follow parallel paths, both having the same exploits available at the same time. This seems to point to a third party providing both groups with such artefacts.

During February 2019, we observed a highly targeted attack in the southern part of Russia using a previously unknown malware that we call Cloudmid. This spy program spread via email and masqueraded as the VPN client of a well-known Russian security company that, among other things, provides solutions to protect networks. So far, we have been unable to relate this activity to any known actor. The malware itself is a simplistic document stealer. However, given its victimology and the targeted nature of the attack, we considered it relevant enough to monitor, even though we were unable to attribute this set of activities to any known actor. The low OPSEC and simplistic malware involved in this operation does not seem to point to an advanced threat actor.

In February, we identified a campaign targeting military organizations in India that we were unable to attribute to any known threat actor. The attackers rely on watering holes and spear phishing to infect their victims. Specifically, they were able to compromise the Centre for Land Warfare Studies (CLAWS) website, using it to host a malicious document used to distribute a variant of the Netwire RAT. We also found evidence of a compromised welfare club for military personnel distributing the same malware during the same period.

In Q3, we observed a campaign utilizing a piece of malware referred to by FireEye as DADJOKE. This malware was first used in the wild in January 2019 and subsequently underwent constant development. We have only seen this malware used in a small number of active campaigns since January, all targeting government, military and diplomatic entities in the Southeast Asia region. The latest campaign, conducted in August, seems to have targeted only a select few individuals working for a military organization.

Privacy matters

On January 17, security researcher Troy Hunt reported a leak of more than 773 million email and 21 million unique password records. The data, dubbed Collection #1, were originally shared on the popular cloud service MEGA. Collection #1 is just a small part of a bigger leak of about 1 TB of data, split into seven parts and distributed through a data-trading forum. The full package is a collection of credentials leaked from different sources during the past few years, the most recent being from 2017, so we were unable to identify any more recent data in this 'new' leak. It turned out that Collection #1 was just part of a larger dump of leaked credentials comprising 2.2 billion stolen account records. The new data dump, dubbed Collection #2-5, was discovered by researchers at the Hasso Plattner Institute in Potsdam.

In February, further data dumps occurred. Details of 617 million accounts, stolen from 16 hacked companies, were put up for sale on Dream Market, accessible via the Tor network. The hacked companies include Dubsmash, MyFitnessPal, Armor Games and CoffeeMeetsBagel. Subsequently, data from a further eight hacked companies was posted to the same market place. Then in March, the hacker behind the earlier data dumps posted stolen data from a further six companies.

Stolen credentials, along with other personal information harvested from data leaks, is valuable not only to cybercriminals but also to targeted attackers, including those wishing to track the activities of dissidents and activists in various parts of the world.

We've become used to a steady stream of reports in the news about leaks of email addresses and passwords. The theft of such 'traditional' forms of authentication is bad enough, but the effects of using alternative methods of authentication can be much more serious. In August, two Israeli researchers discovered fingerprints, facial recognition data and other personal information from the Suprema Biostar 2 biometric access control system in a publicly accessible database. The exposure of biometric data is of particular concern. A compromised password can be changed, but a biometric characteristic is for life.

Moreover, the more widespread use of smart devices in new areas of our lives opens up a bigger pool of data for attackers. Consider, for example, the potential impact of smart speakers for listening in on unguarded conversations in the home. Social media giants are sitting on a growing pile of personal information – information that would prove very valuable to criminals and APT threat actors alike.

Final thoughts

We will continue to track all the APT activity we can find and will regularly highlight the more interesting findings, but if you want to know more, please reach out to us at intelreports@kaspersky.com.

Kaspersky Security Bulletin ‘19

Statistics

kaspersky

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 product users from 203 countries and territories worldwide participate in this global exchange of information about malicious activity. All the statistics were collected from November 2018 to October 2019.

The year in figures

- **19.8%** of user computers were subjected to at least one Malware-class web attack over the year.
- Kaspersky solutions repelled **975 491 360** attacks launched from online resources located all over the world.
- **273 782 113** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky's web antivirus detected **24 610 126** unique malicious objects.
- **755 485** computers of unique users were targeted by encryptors.
- **2 259 038** computers of unique users were targeted by miners.
- Kaspersky solutions blocked attempts to launch malware capable of stealing money via online banking on **766 728** devices.

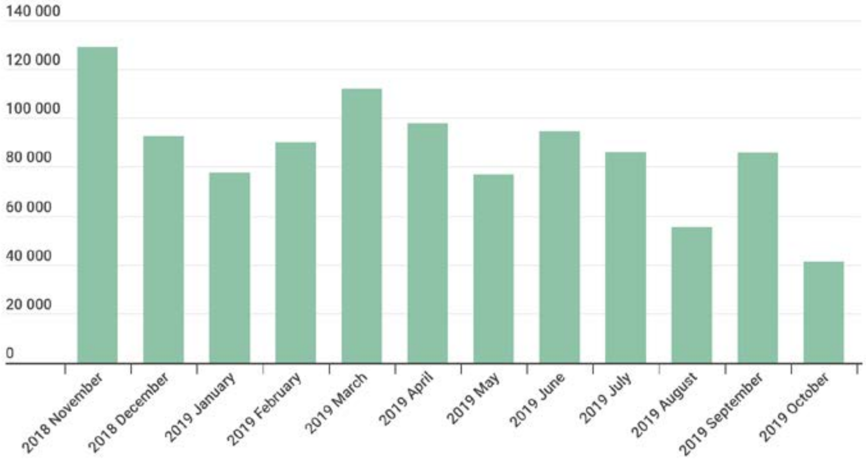
Mobile threats will be presented in the yearly report "Mobile malware evolution 2019".

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

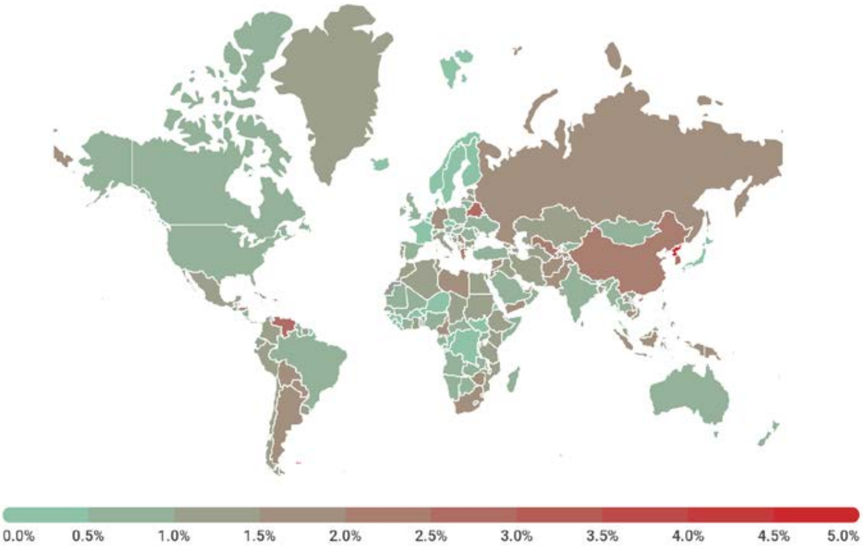
During the reporting period, Kaspersky solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **766 728** users.



Number of unique users attacked by banking malware, November 2018 – October 2019

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 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 2018 – October 2019

TOP 10 countries by percentage of attacked users

	Country*	%**
1	Belarus	2.8
2	Republic of Korea	2.6
3	Venezuela	2.6
4	China	2.4
5	Greece	2.1
6	Maldives	2.0
7	Uzbekistan	2.0
8	Cameroon	1.9
9	Serbia	1.9
10	Afghanistan	1.8

* We excluded those countries where the number of Kaspersky 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's products in that country.

TOP 10 banking malware families

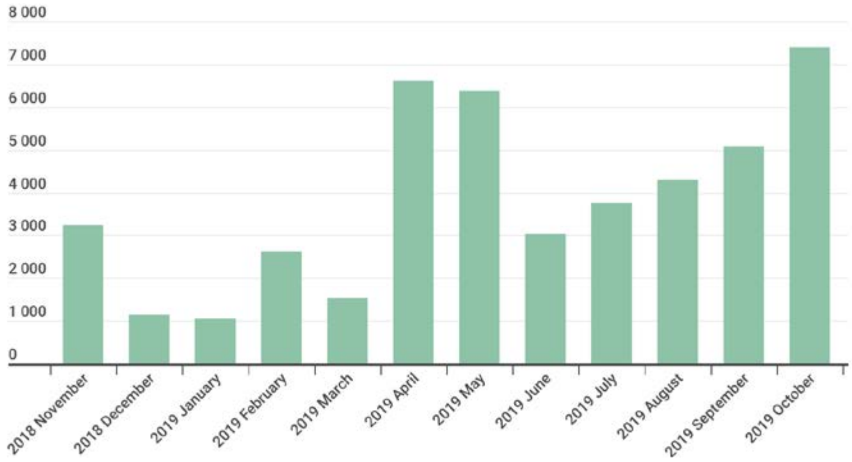
The table below shows the 10 malware families most commonly used to attack banking users during the reporting period.

	Name	%*
1	Trojan.Win32.Zbot	23.10
2	Trojan-Banker.Win32.RTM	21.60
3	Backdoor.Win32.Emotet	12.30
4	Backdoor.Win32.SpyEye	7.10
5	Trojan.Win32.Nymaim	5.80
6	Trojan-Banker.Win32.Trickster	4.80
7	Trojan-Banker.Win32.Ramnit	4.40
8	Trojan.Win32. Neurevt	3.10
9	Trojan-Banker.Win32.CliptoShuffler	1.90
10	Trojan-Banker.Win32.Danabot	1.30

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

Crypto-ransomware

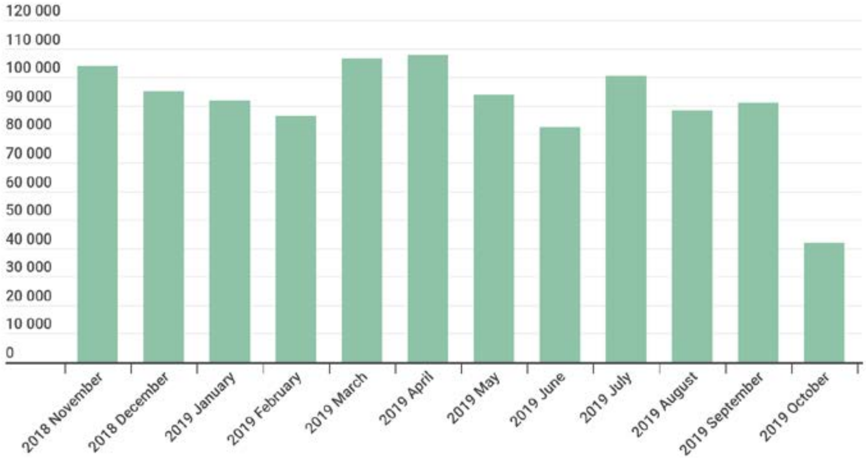
During the year, we detected **46 156** modifications of encryptors and discovered **22** new families. Note that we didn't create a new family for every new malware we found. Most threats of this type are assigned with generic verdicts that we use when detecting new and unknown samples.



Number of new crypto-ransomware modifications, November 2018 – October 2019

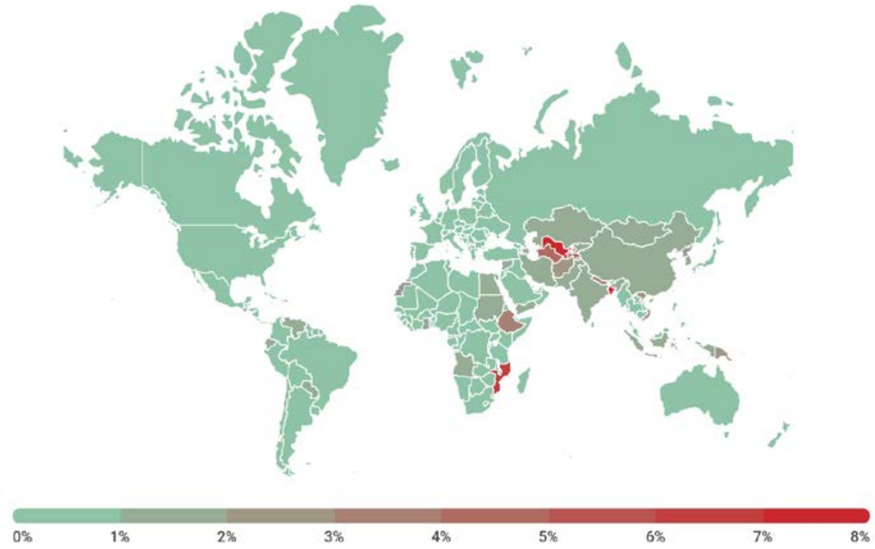
The number of users attacked by encryptors

During the reporting period, **755 485** unique KSN users were attacked by encryptors, including 209 679 corporate users (excluding SMB) and 22 440 SMB users.



Number of users attacked by crypto-ransomware, November 2018 – October 2019

Geography of attacks



Geography of crypto-ransomware attacks, November 2018 – October 2019

TOP 10 countries attacked by encryptors

	Country*	%**
1	Bangladesh	13.78
2	Uzbekistan	7.20
3	Mozambique	6.08
4	Turkmenistan	4.23
5	Ethiopia	3.97
6	Nepal	3.86
7	Afghanistan	2.45
8	Vietnam	2.34
9	China	1.94
10	India	1.91

* We excluded those countries where the number of Kaspersky 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 products in the country.

TOP 10 most widespread encryptor families

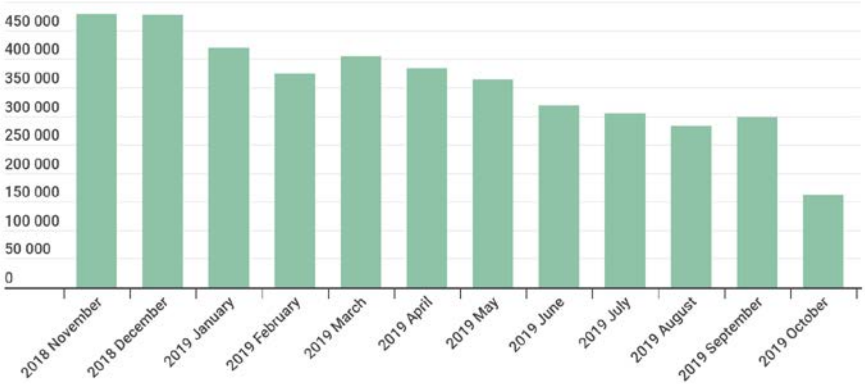
	Name	Verdict	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	23.56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	16.81
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12.17
4	(generic verdict)	Trojan-Ransom.Win32.Gen	6.26
5	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5.08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	4.65
7	Shade	Trojan-Ransom.Win32.Shade	2.66
8	PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2.43
9	(generic verdict)	Trojan-Ransom.Win32.Crypren	2.28
10	Stop	Trojan-Ransom.Win32.Stop	1.94

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

Miners

The number of users attacked by miners

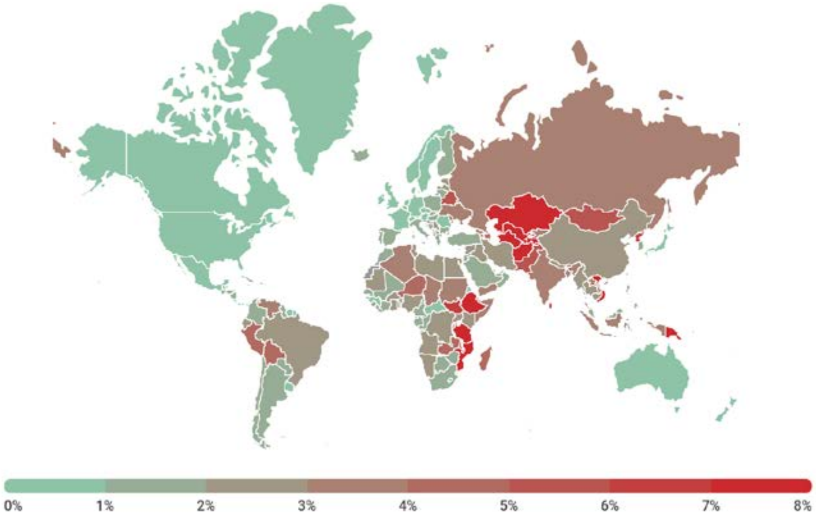
During the reporting period, **2 259 038** unique KSN users were attacked by miners. In the total volume of detections, the share of miners was 3.64%; for Risktool it was 6.94%.



Number of users attacked by crypto-ransomware, November 2018 – October 2098

During the reporting period, the most active miner was Trojan.Win32.Miner.bbb; its accounted for 13.45% of the total number of users attacked by miners. It was followed by Trojan.Win32.Miner.ays (11.35%), Trojan.JS.Miner.m (11.12%) and Trojan.Win32.Miner.gen (9.32%).

Geography of attacks



Geography of miners attacks, November 2018 – October 2019

Vulnerable applications used in cyberattacks

This reporting period will stick in our memory for a great number of targeted attacks based on zero-day exploits. During 2019, Kaspersky experts made the following discoveries:

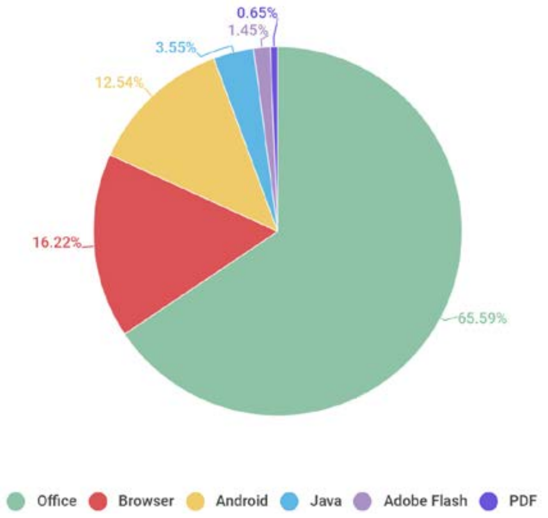
- The vulnerability CVE-2018-8611 patched in the December collection of fixes was used by FruityArmor and SandCat hacker groups, and possibly others. By the time an exploit was detected for this vulnerability, FruityArmor was already quite a famous hacker group with a history of using zero-day exploits, while SandCat, on the contrary, was relatively new on the scene. The detected vulnerability proved a very serious one, as it allowed to obtain system privileges and execute kernel-level code in all Windows versions, including the then most current Windows 10 RS4. In addition, it resided in the Kernel Transaction Manager driver, enabling the exploit to bypass web browser sandboxes.
- The vulnerability CVE-2019-0797 was detected in February and patched in the March collection of fixes. Same as the previous one — CVE-2018-8611 — the new vulnerability could potentially be used by different hacker groups, including FruityArmor and SandCat. It became the fourth actively exploited zero-day vulnerability detected by Kaspersky during the first six months of the year. Same as the ones detected earlier, it was used to obtain elevated privileges in Windows, but unlike CVE-2018-8611, the vulnerable component was the win32k.sys diver in charge of graphics and interface.
- In March, the actively exploited vulnerability CVE-2019-0859 was discovered, which allowed to elevate Windows user rights through yet another win32k.sys driver error. Its rather peculiar payload, provided together with shellcode, may indicate that the exploit was used by one of the cybercriminal groups targeting the financial sector.
- The vulnerability CVE-2019-13720 was discovered in late August in the aftermath of a series of attacks on fresh versions of Google Chrome. After we alerted Google about this actively exploited vulnerability, the company updated its Chrome browser to version 78.0.3904.87. We tagged these attacks Operation WizardOpium, for even though the code was somewhat similar, we were unable to get clear connections with other groups.

Compared to last year, the total number of actively used zero-day exploits we detected together with other industry peers in 2019 increased.

During the reporting period, we registered a drop in the number of exploits for Adobe Flash Player, which will cease to be supported by the end of next year. The share of web browser exploits has slightly shrunk, too, despite the arrival of some new publicly exploited zero-day vulnerabilities. The same is true for Android, the share of exploits for which has dropped to 12%. The share of PDF exploits, on the contrary, has somewhat grown.

During the previous reporting period, we observed a rapid growth in the number of users attacked by Microsoft Office exploits, and by Q4 2018 exploits for this application package were leading by the number of attacks. In the current period of report, Microsoft Office remains in the lead among the most attacked applications, but unlike previous years, this year the cybercriminals' arsenal has not suffered any major changes: CVE-2017-11882, CVE-2018-0802, CVE-2017-8570, and CVE-2017-0199 are still the most used exploits. Even though the exploit lineup is basically the same, the attackers keep finding new methods to obfuscate documents and avoid static detection techniques, but this topic deserves a separate Securelist review.

The rating list of vulnerable applications is based on verdicts returned by Kaspersky products for the blocked exploits used by cybercriminals, both in network attacks and vulnerable local applications, including those run on mobile devices.



Malicious exploits broken down by type of target applications, November 2018 — November 2019

During this reporting period, network attacks continued to be one of the most common types of attacks. It is safe to say that the year 2019 will be remembered for discovery of multiple vulnerabilities in the remote desktop subsystem in different versions of Windows OS. These received the general designations of BlueKeep and DejaBlue. At present we observe no widespread exploiting of these vulnerabilities, which may be down to the complexity of the process. Same as in previous years, the network attacks list is topped by various exploits for the SMB protocol, known as EternalBlue, EternalRomance, etc. It also should not go unmentioned that a large share of malicious network traffic comes from password mining queries targeting popular network services and servers like Remote Desktop Protocol and Microsoft SQL Server, respectively.

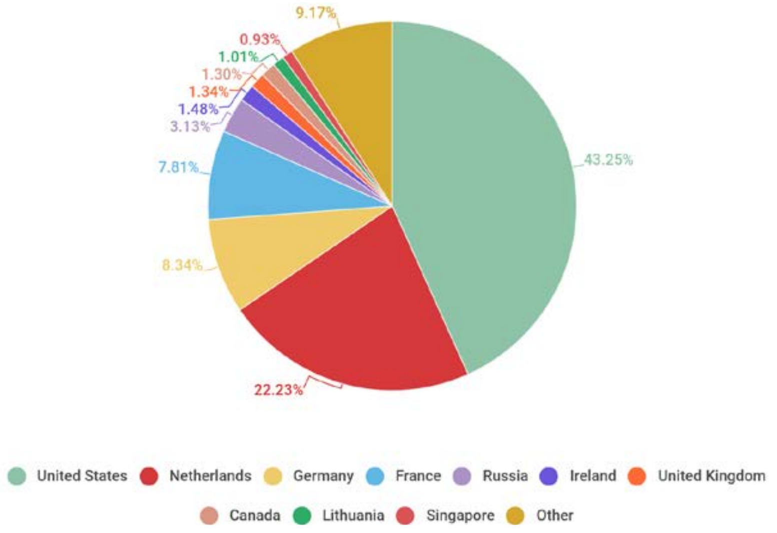
Web-based attacks

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.

During the reporting period, Kaspersky solutions blocked **975 491 360** attacks launched from web resources located in various countries and territories around the world. **90.83%** 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 2018 – October 2019

Compared to last year's results, the distribution of web attack sources has not changed much. The United States (43.25%) is in first place, followed by the Netherlands (22.23%) and Germany (8.34%).

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 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 reporting period, adware programs and their components were detected on 78% of user computers on which the web antivirus was triggered.

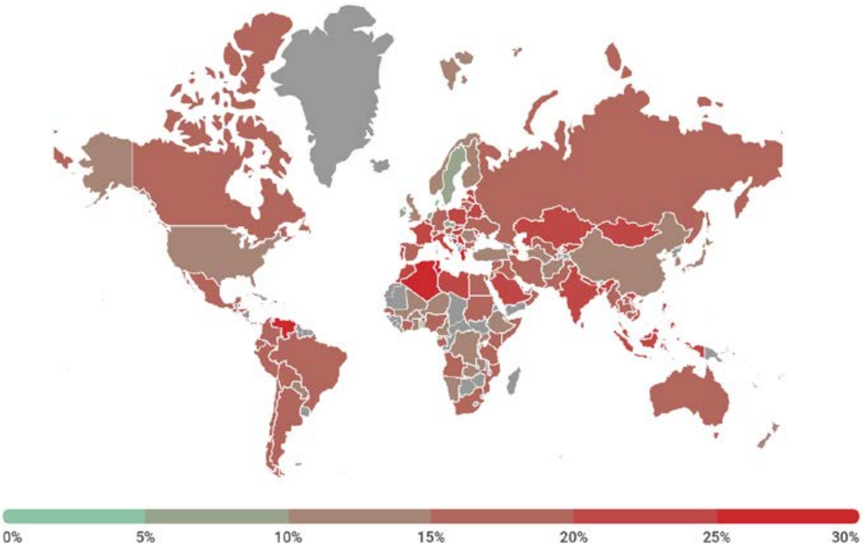
The TOP 20 countries where users face the greatest risk of online infection

	Country*	%**
1	Algeria	33.02
2	Venezuela	30.25
3	Tunisia	29.50
4	Greece	26.07
5	Serbia	25.80
6	Bangladesh	24.95
7	Moldova	24.78
8	Azerbaijan	24.74
9	Belarus	24.52
10	Poland	24.13
11	Mongolia	24.05
12	Philippines	23.89
13	Morocco	23.87
14	Latvia	23.22
15	Qatar	22.94
16	Vietnam	22.57
17	Taiwan, province of China	22.13
18	France	21.99
19	Portugal	21.97
20	Italy	21.96

On average, during the reporting period a Malware-class attack was detected at least once on 19.8% of computers around the world.

* We excluded those countries where the number of Kaspersky 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 products in the country



Geography of malicious web attacks, November 2018 – October 2019

TOP 20 verdicts detected online

During the reporting period, Kaspersky's web antivirus detected **24 610 126** unique malicious objects (scripts, exploits, executable files, etc.) and **273 782 113** unique URLs that were blocked by web antivirus components. We identified the 20 malicious programs most actively involved in online attacks launched against computers.

	Verdict	%*
1	Malicious URL	85.40
2	Trojan.Script.Generic	5.89
3	Trojan.Script.Miner.gen	3.89
4	Trojan-Clicker.HTML.Iframe.dg	0.65
5	Trojan.BAT.Miner.gen	0.26
6	Trojan-Downloader.JS.Inor.a	0.22
7	Trojan.PDF.Badur.gen	0.21
8	DangerousObject.Multi.Generic	0.21
9	Trojan-Downloader.Script.Generic	0.17
10	Trojan-PSW.Script.Generic	0.15
11	Trojan.Script.Agent.gen	0.15
12	Hoax.HTML.FraudLoad.m	0.13
13	Exploit.Script.Generic	0.08
14	Trojan.Script.Agent.bg	0.07
15	Trojan.Multi.Preqw.gen	0.06
16	Exploit.MSOffice.CVE-2017-11882.gen	0.06
17	Trojan-Downloader.JS.SLoad.gen	0.05
18	Hoax.Script.Loss.gen	0.05
19	Trojan.JS.Miner.m	0.05
20	Trojan-Downloader.VBS.SLoad.gen	0.04

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

Though several detections related to web-miners still can be seen in this top, number of mining Javascripts downloads and attempts to connect web-mining related esources dropped down significantly in comparison to 2018. This affects overall number of web-detections and Malicious URLs blocks particularly.

Malicious URL (85.40%) in the first place is the verdict identifying links from our black list (links to web pages containing redirects to exploits, sites with exploits and other malicious programs, botnet control centers, extortion websites, etc.).

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'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 during the reporting period. This rating does not include the Adware and Riskware classes of program.

	Verdict	%*
1	DangerousObject.Multi.Generic	26.43
2	Trojan.Multi.BroSubsc.gen	9.48
3	Trojan.Script.Generic	6.19
4	Trojan.Multi.GenAutorunReg.a	5.94
5	HackTool.Win64.HackKMS.b	4.40
6	HackTool.MSIL.KMSAuto.by	3.69
7	HackTool.Win32.KMSAuto.bu	3.54
8	Trojan.WinLNK.Agent.gen	3.45
9	HackTool.MSIL.KMSAuto.a	3.43
10	Trojan.WinLNK.Starter.gen	3.42
11	HackTool.MSIL.KMSAuto.dh	2.83
12	HackTool.Win32.KMSAuto.c	2.75
13	HackTool.MSIL.KMSAuto.di	2.65
14	Trojan.Win32.Generic	2.53
15	HackTool.Win32.KMSAuto.cb	2.50
16	HackTool.Win64.HackKMS.c	2.47
17	HackTool.MSIL.KMSAuto.bx	2.18
18	Trojan.Win32.AutoRun.gen	1.93
19	Virus.Win32.Sality.gen	1.90
20	HackTool.Win32.KMSAuto.m	1.90

The entities in our TOP 20 are quite the same as in the previous year, though their order slightly differs.

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

On the 1st place is DangerousObject.Multi.Generic (26.43%) verdict, which is used for malware detected with the help of cloud technologies. Cloud technologies work when the antivirus databases do not yet contain either signatures or heuristics to detect a malicious program but the company's cloud antivirus database already has information about the object. In fact, this is how the very latest malware is detected.

The second place in the top is taken by relatively new threat, that appears to be widely spread – Trojan.Multi.BroSubsc.gen (9.48%). Malware of this family is installed on browsers deceptively after the user visits fraudulent or advertising resources. This malware displays advertising messages even if a browser is inactive.

It is also noticeable, that rather old family Virus.Win32.Sality.gen still persists and it is the only Virus threat that keeps appearing in the TOP 20.

Overall, we have noticed that local Miners became less popular, and has left the top of local threats.

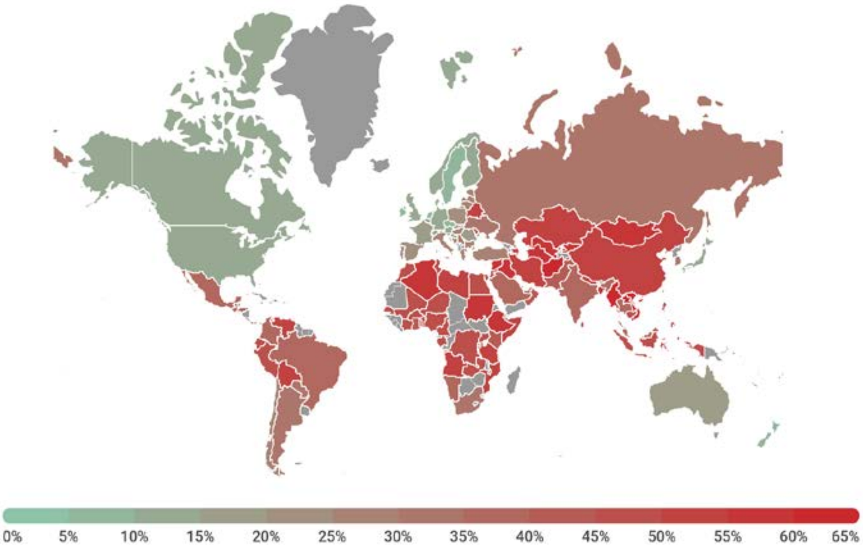
Countries where users face the highest risk of local infection

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	Afghanistan	65.55
2	Vietnam	61.84
3	Lao people's democratic republic	61.95
4	Myanmar	60.80
5	Bangladesh	59.51
6	Mongolia	59.41
7	Uzbekistan	58.06
8	Turkmenistan	57.57
9	Algeria	57.50
10	Iraq	57.33
11	Syriac	57.04
12	Sudan	55.41
13	Kyrgyzstan	55.15
14	Ethiopia	55.08

	Country*	%**
15	Bolivia	54.85
16	China	54.64
17	Nepal	54.57
18	Mozambique	54.52
19	Libya	54.36
20	Rwanda	54.14



Geography of local malware attacks, November 2018 – October 2019

In 2018, at least one malicious program was found on an average of 34.05% of computers, hard drives or removable media belonging to KSN users.

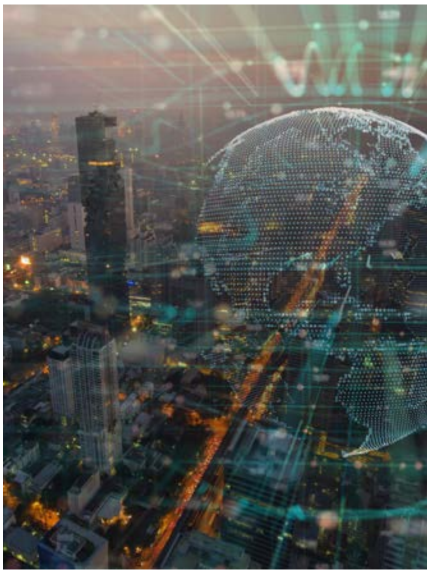
* When calculating, we excluded countries where there are fewer than 50,000 Kaspersky users.

** 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 products.

Story of the Year 2019

Cities Under Ransomware Siege

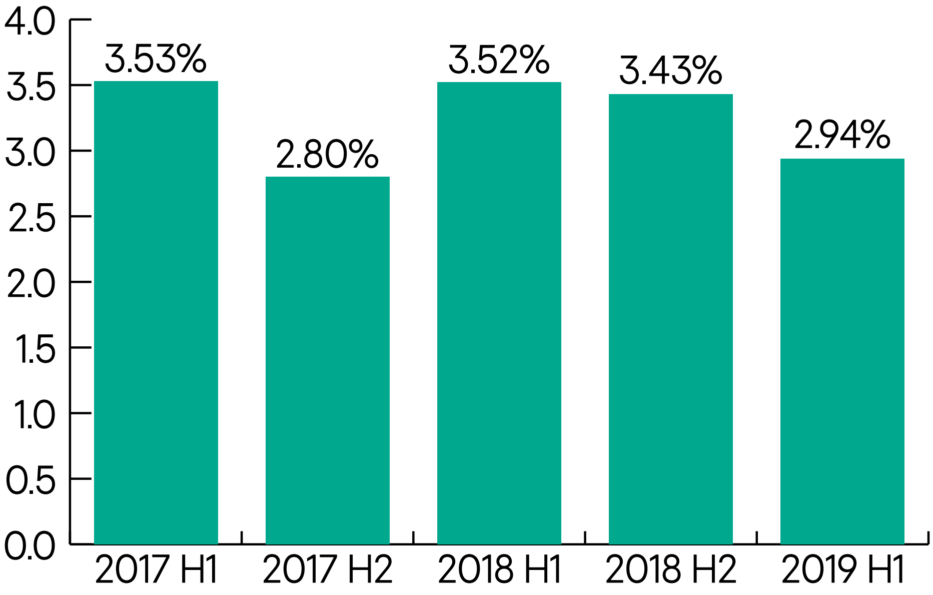
kaspersky



STORY OF THE YEAR 2019: CITIES UNDER RANSOMWARE SIEGE

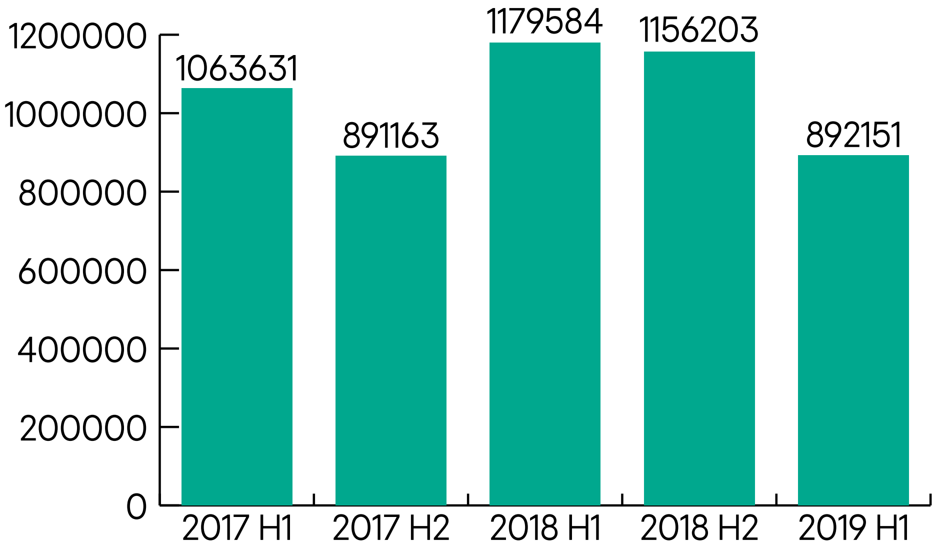
Ransomware has been targeting the private sector for years now.

Overall awareness of the need for security measures is growing, and cybercriminals are increasing the precision of their targeting to locate victims with security breaches in their defense systems. Looking back at the past three years, **the share of users targeted with ransomware in the overall number of malware detections has risen from 2.8% to 3.5%**. While this might seem like a modest amount, ransomware is capable of causing extensive damage in the affected systems and networks, which means this threat should never be overlooked. The proportion of ransomware targets among all users attacked with malware has been fluctuating, yet appears to be decreasing, with the figure for H1 2019 showing 2.94% compared to 3.53% two years ago.



Share of users attacked with ransomware from all users attacked with malware.

The overall number of users attacked annually has changed. **Kaspersky experts usually observe from around 900,000 to almost 1.2 million users targeted by ransomware every six months.**



Number of users attacked with ransomware H1 2017-H1 2019

Despite there being many extremely sophisticated cryptor samples, the mechanism behind how they operate is painstakingly simple: they turn the files on victims' computers into encrypted data and demand a ransom for the decryption keys. These keys are created by threat actors to decipher the files and transform them back into the original data. Without a key, it is impossible to operate the infected device. The malware may be distributed by the creators of the threat, sold to other actors or to the creators' partner networks – 'outsourced' distributors that share the profit from successful ransomware attacks with the technology holders.

2019 has seen this plague actively shifting towards a new target – municipalities. Arguably, the most prominent and widely discussed incident was that in Baltimore, which suffered from a large-scale ransomware campaign that knocked out a number of city services and required tens of millions of dollars to restore the city's IT networks.

Based on publicly available statistics and announcements monitored by Kaspersky experts, 2019 has seen at least 174 municipal organizations targeted by ransomware. This is an approximately 60% increase from the number of cities and towns that reported falling victim to attacks a year earlier. Whereas not everyone has confirmed the amount of extorted funds and whether a ransom was paid or not, the average demand for ransom ranged from $5,000 to $5,000,000, and on average was equal to around $1,032,460. The numbers, however, varied greatly, as the funds extorted from small town school districts, for example, were sometimes 20 times smaller than those extorted from city halls in big municipalities.

However, the actual damage caused by attacks, according to estimates by independent analysts, often differs from the sum that the criminals request. First of all, some municipal institutions and vendors are insured against cyber-incidents, which compensates the costs one way or another. Secondly, the attacks can often be neutralized by timely incident response. Last but not the least, not all cities pay the ransom: in the Baltimore encryption case, where officials refused to pay the ransom, the city ended up spending $18 million to restore its IT infrastructure. While this sum might seem way more than the initial $114,000 requested by the criminals, paying the ransom is a short-term solution that encourages threat actors to continue their malicious practices. You need to keep in mind that once a city's IT infrastructure has been compromised, it requires an audit and a thorough incident investigation to prevent similar incidents from occurring again, plus the additional cost of implementing robust security solutions.

Attack scenarios vary. For instance, an attack may be the result of unprotected remote access. In general, however, there are two entry points through which a municipality can be attacked: **social engineering and a breach in un-updated software**. A vivid illustration of the latter problem has been observed quarterly by Kaspersky experts: the all-time leader of almost all rankings of ransomware most frequently blocked on user devices is WannaCry. Even though Microsoft released a patch for its Windows operating system that closed the relevant vulnerability months before the attacks started, WannaCry still affected hundreds of thousands of devices around the globe. And what's more striking is the fact that it still lives and prospers. The latest statistics gathered by Kaspersky in Q3 2019 demonstrated that two and a half years after the WannaCry epidemic ended, a fifth of all users targeted by cryptors were attacked by WannaCry. What's more, the statistics from 2017 to mid-2019 show that WannaCry is consistently one of the most popular malware samples, accounting for 27% of all users attacked by ransomware in that time period.

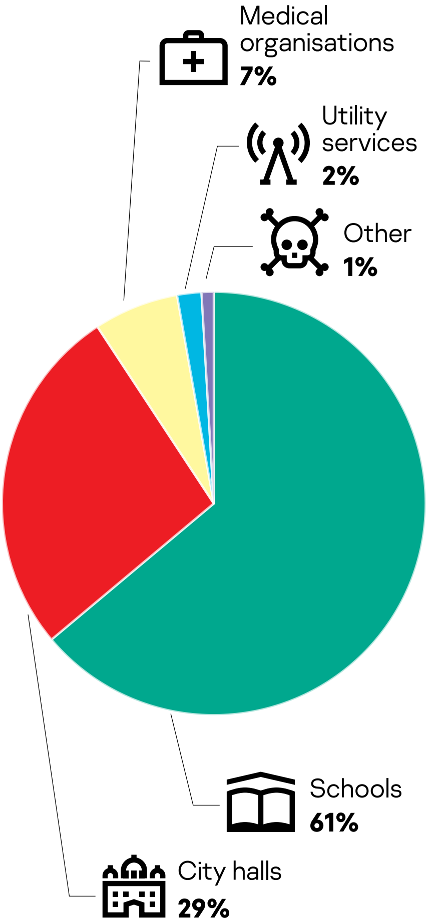
An alternative scenario involves criminals exploiting human factors: this is arguably the most underestimated attack vector, as training of employees in security hygiene is nowhere near as universal as it should be. Many industries lose a tremendous amount of money due to employee errors (in some industries this is the case for half of all incidents), phishing and spam messages containing installers for dangerous malware are still circulating around the web and reaching victims. Sometimes those victims may be managing the company's accounts and finances and not even suspect that opening a scammer email and downloading what appears to be a PDF file on their computers can result in a network being compromised.

Among the many types of municipal organizations attacked throughout 2019, some attracted more attacks than others.

Ransomware attack on cities in 2019:

174 municipalities attacked:

Targeted Systems



$15,663,200 – Sum of publicly announced ransoms

$5,000 to $5.3 million – Range of ransom demands

$1,032,460 – Average ransom demand

The most targeted entities were undoubtedly **educational organisations**, such as school districts, accounting for approximately 61% of all attacks: 2019 saw operations against more than 105 school districts, with a whopping 530 schools targeted. This sector has been hit hard, yet demonstrated a resilience: while some colleges had to cancel classes, many educational institutions adopted a position of continuing studies despite a lack of technical support, claiming that computers have only recently become part of the educational process, and that staff are perfectly capable of teaching pupils without them.

City halls and municipal centers, meanwhile, accounted for around 29% of cases. Threat actors are often aiming at the heart of processes that, if stopped, will result in an extremely problematic interruption of vital processes for the vast majority of citizens and local organizations. Unfortunately, such institutions are still often equipped with weak infrastructure and unreliable security solutions, as the workflow (especially in small, quiet towns or villages without advanced infrastructure) does not require high computing capacities. As a consequence, the locals often don't bother updating old computers because they appear to still be functioning well.. This might be related to a common mistake, whereby security updates are associated with design changes or technical developments introduced in the software, while their most vital function is in fact closing breaches found by white- or black-hat hackers and security researchers.

Another popular target was **hospitals**, accounting for 7% of all attacks. While some black-hat hackers and cybercriminal groups claim to have a code of conduct, in most cases attackers are motivated purely by the prospect of financial gain and go for vital services that cannot tolerate long periods of disruption, such as medical centers.

Furthermore, around 2% of all institutions subjected to an attack were **municipal utility services** or their subcontractors. The reason for this might be that such service providers are often used as an entry point to a whole network of devices and organizations, as they are responsible for communications in terms of billing for multiple locations and households. In the scenario where threat actors successfully attack the service provider, they might also compromise every locality that particular vendor or institution services. In addition, the disruption of utility services may result in disruption to vital regular operations, such as providing online payment services for residents of the town or city to pay their monthly bills – this adds to the pressure the victims' experience and pushes them towards a short-term, yet seemingly effective solution – paying the ransom.

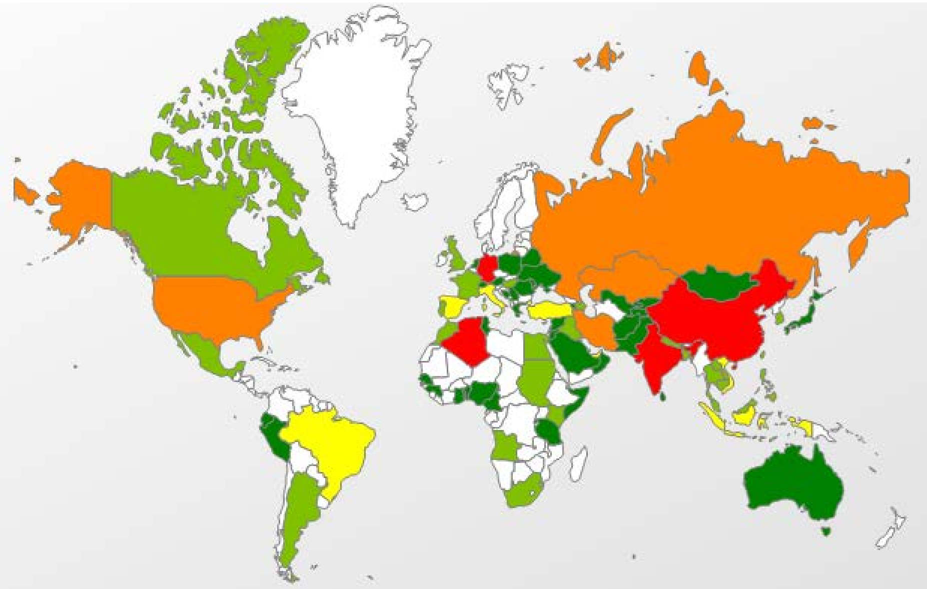
Let's take a closer look at the malware that has been actively used in attacks on municipalities.

THE BESIEGERS

Ryuk

While not all organizations disclose technical details about the ransomware that hits them, Ryuk ransomware (Detection name: Trojan-Ransom.Win32.Hermez) has been cited as a reason for incidents in municipalities noticeavly often. It is known to be notorious for attacking large organizations and governmental and municipal networks. This malware first appeared in the second half of 2018 and has been mutating and actively propagating throughout 2019.

Geography



TOP 10 countries

Countries	%*
Germany	8.60%
China	7.99%
Algeria	6.76%
India	5.84%
Russian Federation	5.22%
Iran	5.07%
United States	4.15%
Kazakhstan	3.38%
United Arab Emirates	3.23%
Brazil	3.07%

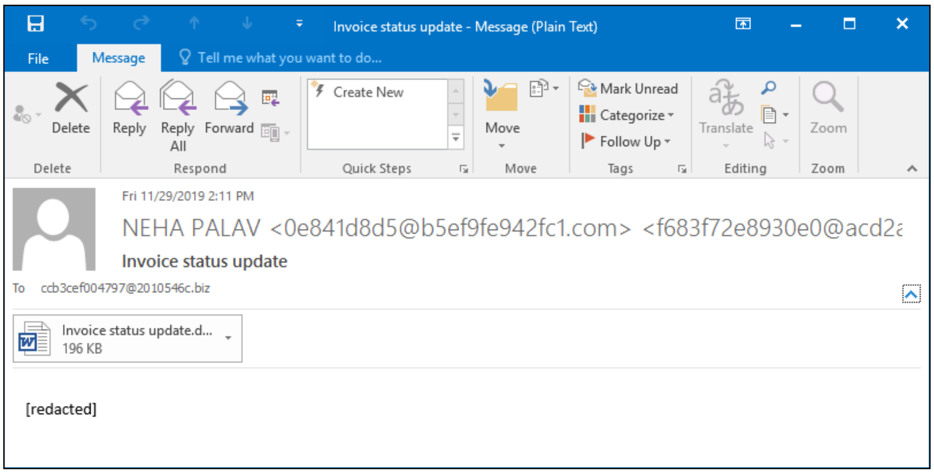
* Percentage of users attacked in each country by Ryuk, relative to all users attacked worldwide by this malware

Ryuk has been seen all over the world, although some countries have been affected more than others. According to Kaspersky Security Network statistics, in 8.6% of cases it attempted to attack German-based targets, followed by China (8%) and Algeria (6.8%).

Distribution

The threat actors behind Ryuk employ a multi-stage scheme to deliver this ransomware to their victims.

The initial stage involves infecting a large number of machines by the Emotet bot (Detection name: Trojan-Banker.Win32.Emotet). Typically this is achieved by sending out spam emails containing a document with a malicious macro that will download the bot if the victim allows the execution of macros.



Fri 11/29/2019 2:11 PM

NEHA PALAV <0e841d8d5@b5ef9fe942fc1.com> <f683f72e8930e0@acd2a

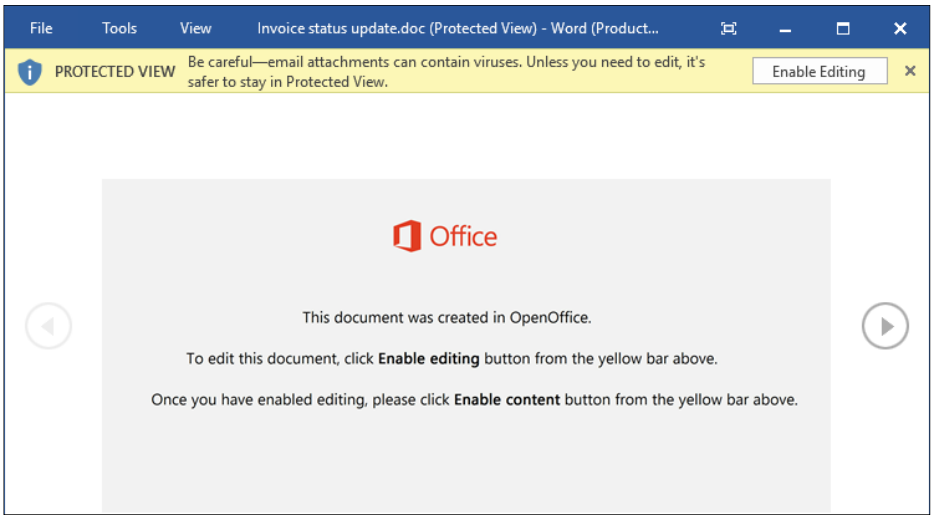
Invoice status update

To ccb3cef004797@2010546c.biz

Invoice status update.d...
196 KB

[redacted]

Spam message with a malicious document attached


File
Tools
View
Invoice status update.doc (Protected View) - Word (Product...
PROTECTED VIEW
Enable Editing
Office

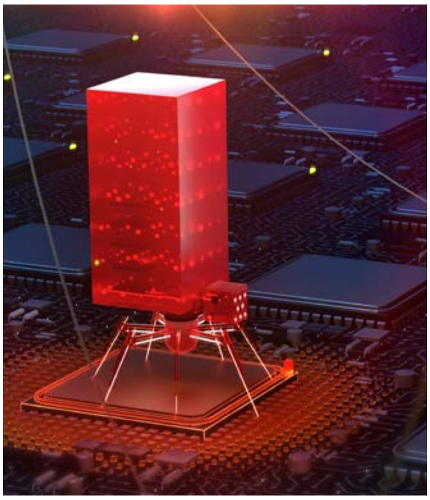
Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

This document was created in OpenOffice.

To edit this document, click **Enable editing** button from the yellow bar above.

Once you have enabled editing, please click **Enable content** button from the yellow bar above.

The malicious document



At the second stage of the infection, Emotet will receive a command from its servers to download and install another piece of malware – Trickbot (verdict: Trojan.Win32.Trickster) – into the compromised system. This piece of malware will allow the threat actors to carry out reconnaissance in the compromised network.

If the criminals find they have infiltrated a high-profile victim, for example, a large municipal network, or a corporation, they will likely continue to the third stage of the infection and deploy Ryuk ransomware to numerous nodes in the affected network.

Brief technical description

Ryuk has been evolving since its creation and there is a certain variation between the numerous samples existing ITW. Some of them are built as 32-bit binaries, others are 64-bit; some variants contain a hardcoded list of processes that will be targeted for code injections, other variants white-list several processes and will try to inject all others; the encryption scheme also sometimes differs from one sample to another.

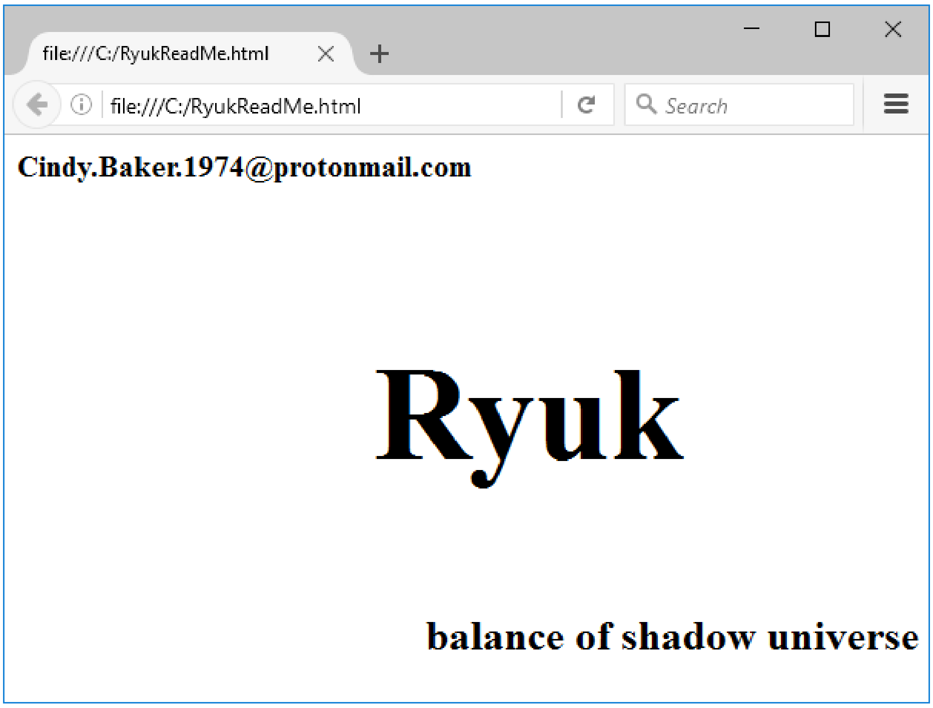
We will describe one of the recent modifications discovered in late October 2019 (MD5: fe8f2f9ad6789c6dba3d1aa2d3a8e404).

File encryption

This modification of Ryuk uses a hybrid encryption scheme employing the AES algorithm to encrypt the content of the victim's files, and the RSA algorithm to encrypt the AES keys. Ryuk uses the standard implementation of cryptographic routines provided by Microsoft CryptoAPI.

The Trojan sample contains the threat actor's embedded 2048-bit RSA key. The private counterpart is not exposed and may be used by the criminals for decryption if the ransom is paid. For each victim file Ryuk will generate a new unique 256-bit AES key that will be used to encrypt the file content. The AES keys are encrypted by RSA and saved at the end of the encrypted file.

Ryuk encrypts both local drives and network shares. Encrypted files will get an additional extension (.RYK), and a ransom note containing the email of the criminals will be saved nearby.



Cindy.Baker.1974@protonmail.com

Ryuk

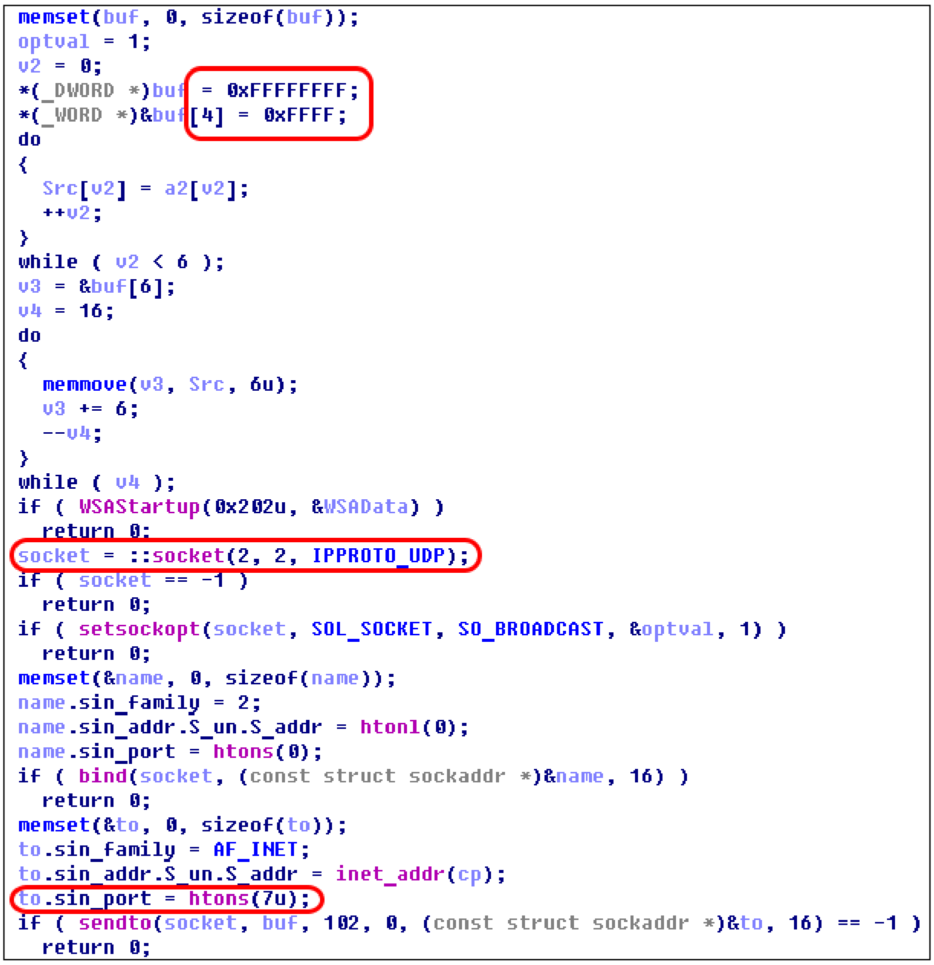
balance of shadow universe

Ransom note

Additional functionality

To cause more damage in the network, this Ryuk variant uses a trick that we haven't observed in other ransomware families before; the Trojan attempts to wake other machines that are in a sleeping state but have been configured to use Wake-on-LAN.

Ryuk does this in order to maximize the attack surface: the files located on network shares hosted on sleeping PCs are unavailable for access, but if the Trojan manages to wake them, it will be able to encrypt those files as well. To achieve this, Ryuk retrieves the MAC addresses of the nearby machines from the local ARP cache of the infected system and sends broadcast UDP packets starting with the magic value {0xff, 0xff, 0xff, 0xff, 0xff, 0xff} to port 7 which will wake up the targeted computers.



```
memset(buf, 0, sizeof(buf));
optval = 1;
v2 = 0;
*(_DWORD *)buf = 0xFFFFFFFF;
*(_WORD *)&buf[4] = 0xFFFF;
do
{
  Src[v2] = a2[v2];
  ++v2;
}
while ( v2 < 6 );
v3 = &buf[6];
v4 = 16;
do
{
  memmove(v3, Src, 6u);
  v3 += 6;
  --v4;
}
while ( v4 );
if ( WSAStartup(0x202u, &WSAData) )
  return 0;
socket = ::socket(2, 2, IPPROTO_UDP);
if ( socket == -1 )
  return 0;
if ( setsockopt(socket, SOL_SOCKET, SO_BROADCAST, &optval, 1) )
  return 0;
memset(&name, 0, sizeof(name));
name.sin_family = 2;
name.sin_addr.S_un.S_addr = htonl(0);
name.sin_port = htons(0);
if ( bind(socket, (const struct sockaddr *)&name, 16) )
  return 0;
memset(&to, 0, sizeof(to));
to.sin_family = AF_INET;
to.sin_addr.S_un.S_addr = inet_addr(cp);
to.sin_port = htons(7u);
if ( sendto(socket, buf, 102, 0, (const struct sockaddr *)&to, 16) == -1 )
  return 0;
```

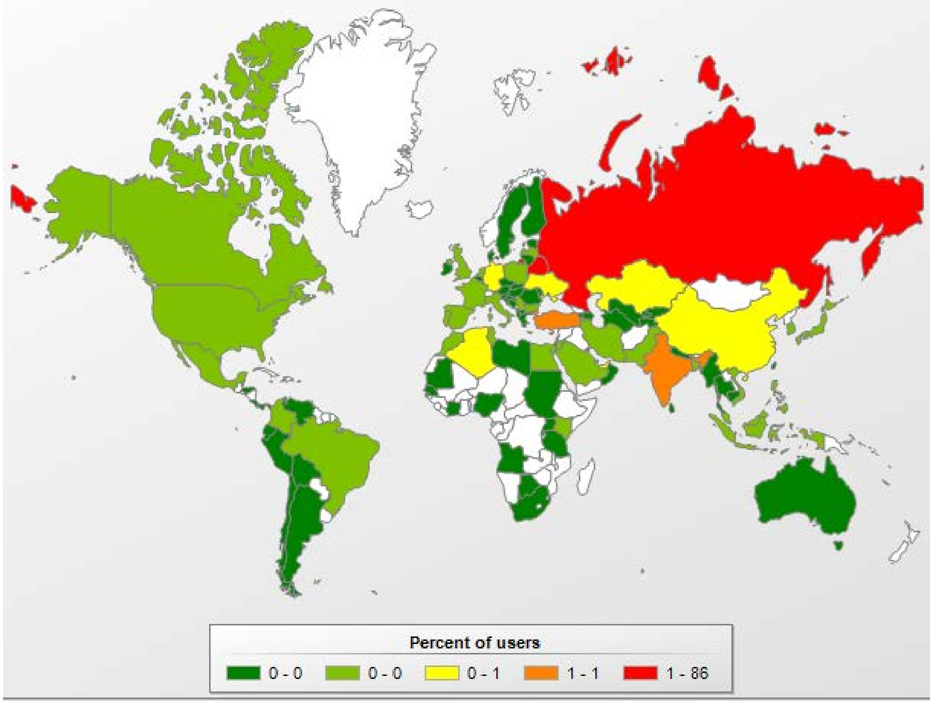
Fragment of the procedure implementing Wake-on-Lan packet broadcast

Other features of the Ryuk algorithm that are more conventional for ransomware families include: code injection into legitimate processes in order to avoid detection; attempting to terminate processes related to business applications to make the files used by these programs available for modification; attempting to stop various services related both to business applications and to security solutions.

Purga

This ransomware family appeared in the middle of 2016 and is still being actively developed and distributed around the world. It has been recorded targeting municipalities. One of the features of this malware is that it attacks regular users as well as large corporations and even governmental organizations. Our products detect this malware as Trojan-Ransom.Win32.Purga. The Trojan family is also known as Globe, Amnesia or Scarab ransomware.

Geography



TOP 10 countries

Countries	%*
Russian Federation	85.59%
Belarus	1.37%
Turkey	0.85%
India	0.80%
Kazakhstan	0.74%
Germany	0.62%
Ukraine	0.54%
China	0.46%
Algeria	0.40%
United Arab Emirates	0.40%

* Percentage of users attacked in each country by Purga, relative to all users attacked worldwide by this malware

Distribution

Throughout this family's existence, the criminals behind it have used various types of infection vectors. The main attack vectors are spam campaigns and RDP brute-force attacks.

According to our information, this is currently the most common attack scenario:

1. The criminals scan the network to find an open RDP port
2. They try to brute-force credentials to log in to the targeted machine
3. After a successful login, the criminals try to elevate privileges using various exploits
4. The criminals launch the ransomware

Brief technical description

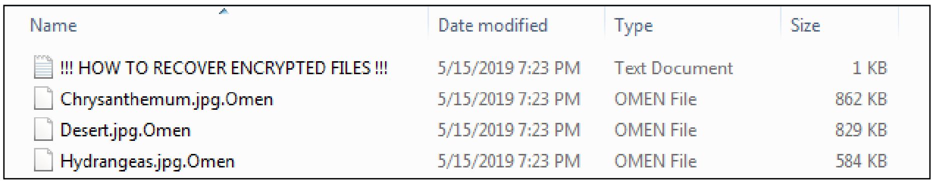
Purga ransomware is an example of very intensively developed ransomware. Over the last couple of years, the criminals have changed several encryption algorithms, key generation functions, cryptographically schemes and so on.

Here we will briefly describe the latest modification.

Naming scheme:

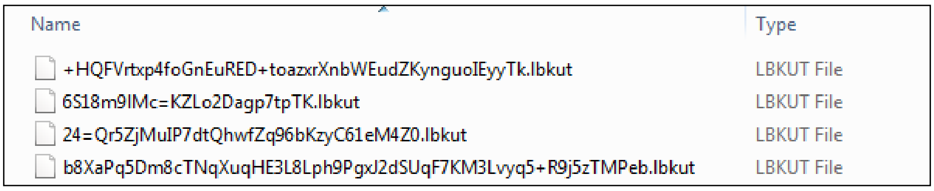
Each modification of Purga uses a different extension for each file and a different email address to contact. Despite using various extensions for the encrypted files, the Trojan uses only two naming schemes, which depend on its configuration:

1. <original file name>.<original extension>.<new extension>



Name	Date modified	Type	Size
!!! HOW TO RECOVER ENCRYPTED FILES !!!	5/15/2019 7:23 PM	Text Document	1 KB
Chrysanthemum.jpg.Omen	5/15/2019 7:23 PM	OMEN File	862 KB
Desert.jpg.Omen	5/15/2019 7:23 PM	OMEN File	829 KB
Hydrangeas.jpg.Omen	5/15/2019 7:23 PM	OMEN File	584 KB

2. <encrypted file name>.<new extension>



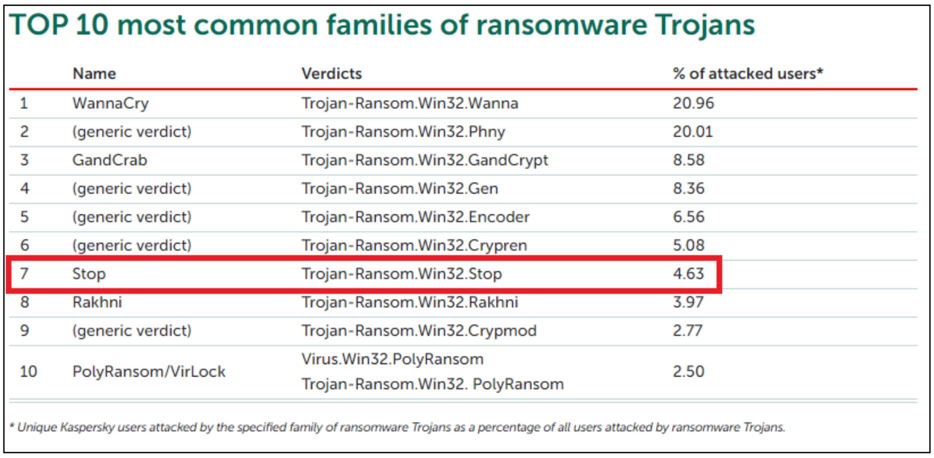
Name	Type
+HQFVrtxp4foGnEuRED+toazxrXnbWEudZKynguoIEyyTk.lbkut	LBKUT File
6S18m9IMc=KZLo2Dagp7tpTK.lbkut	LBKUT File
24=Qr5ZjMuIP7dtQhwfZq96bKzyC61eM4Z0.lbkut	LBKUT File
b8XaPq5Dm8cTNqXuqHE3L8Lph9PgxJ2dSUqF7KM3Lvyq5+R9j5zTMPeb.lbkut	LBKUT File

File encryption

During encryption the Trojan uses a standard scheme that combines symmetric and asymmetric algorithms. Each file is encrypted using a randomly generated symmetric key, then this symmetric key is encrypted with an asymmetric key and the result is stored in the file, in a specifically built structure.

Stop

The notorious Stop ransomware (also known as Djvu STOP) was first encountered at the end of the 2018. Our detection name for this family is Trojan-Ransom.Win32.Stop and, according to our statistics, in 2019 alone the various modifications of Stop ransomware attacked more than 20,000 victims around the world. Unsurprisingly, according to our KSN report for the third quarter of 2019, Stop ransomware finished seventh among the most common ransomware.

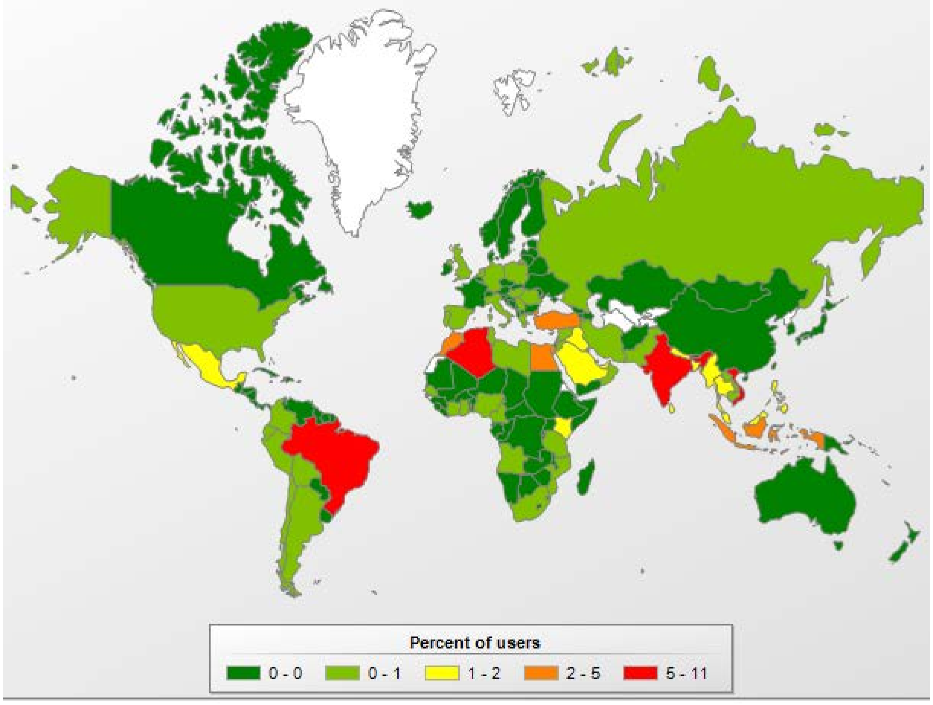


TOP 10 most common families of ransomware Trojans

	Name	Verdicts	% of attacked users*
1	WannaCry	Trojan-Ransom.Win32.Wanna	20.96
2	(generic verdict)	Trojan-Ransom.Win32.Phny	20.01
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	8.58
4	(generic verdict)	Trojan-Ransom.Win32.Gen	8.36
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	6.56
6	(generic verdict)	Trojan-Ransom.Win32.Crypren	5.08
7	Stop	Trojan-Ransom.Win32.Stop	4.63
8	Rakhni	Trojan-Ransom.Win32.Rakhni	3.97
9	(generic verdict)	Trojan-Ransom.Win32.Crypmod	2.77
10	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32. PolyRansom	2.50

** Unique Kaspersky users attacked by the specified family of ransomware Trojans as a percentage of all users attacked by ransomware Trojans.*

Geography



TOP 10 countries

Countries	%*
Vietnam	10.28%
India	10.10%
Brazil	7.90%
Algeria	5.31%
Egypt	4.89%
Indonesia	4.59%
Turkey	4.30%
Morocco	2.42%
Bangladesh	2.25%
Mexico	2.09%

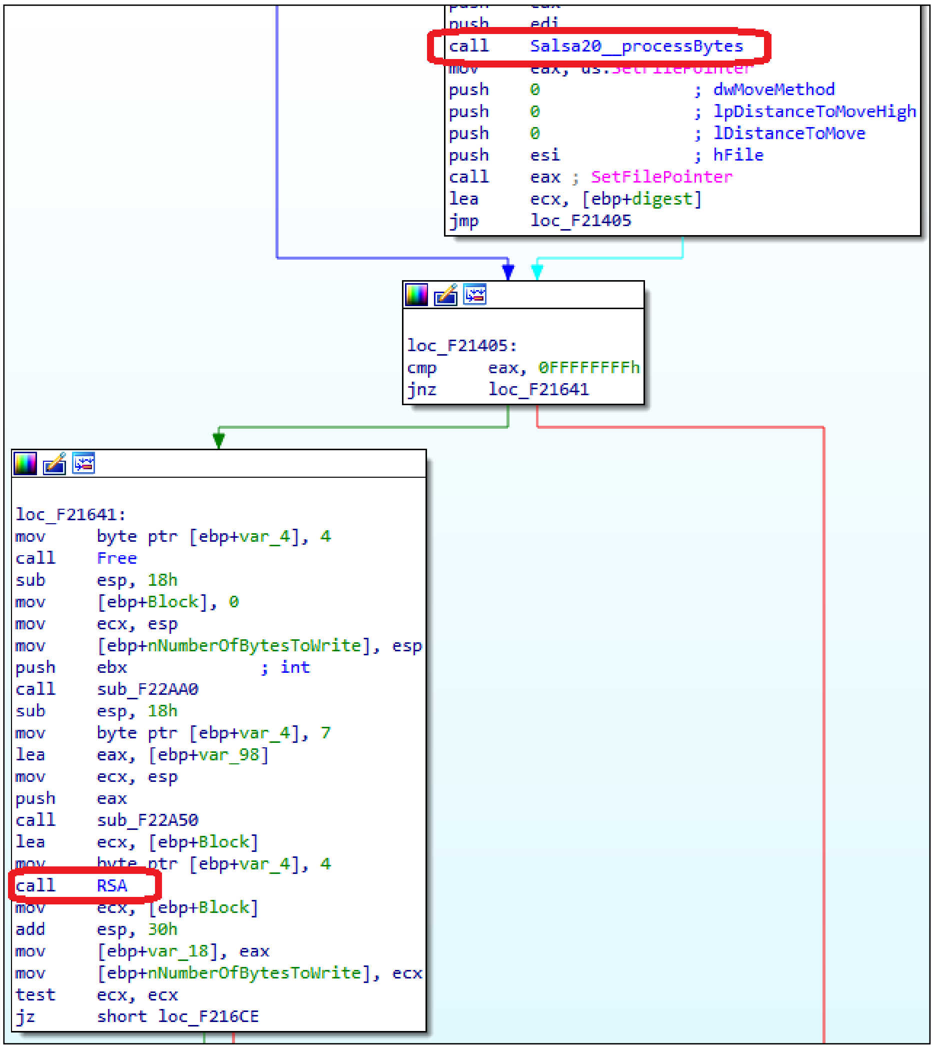
* Percentage of unique users attacked in each country by Stop, relative to all users attacked worldwide by this malware

Distribution

The authors chose to distribute their malware primarily through software installers. When users try to download specific software from an untrusted site or try to use software cracks, instead of the desired result their machines become infected by the ransomware.

Brief technical description

For file encryption, Stop ransomware uses a randomly generated Salsa20 key, which is then encrypted by a public RSA key.



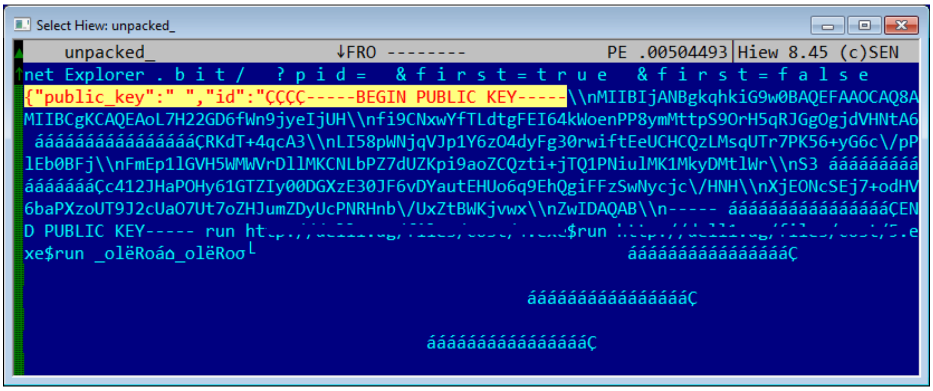
```
push    eax
push    edi
call    Salsa20__processBytes
mov     eax, ds:SetFilePointer
push    0                       ; dwMoveMethod
push    0                       ; lpDistanceToMoveHigh
push    0                       ; lDistanceToMove
push    esi                     ; hFile
call    eax ; SetFilePointer
lea     ecx, [ebp+digest]
jmp     loc_F21405
```

```
loc_F21405:
cmp     eax, 0FFFFFFFFh
jnz     loc_F21641
```

```
loc_F21641:
mov     byte ptr [ebp+var_4], 4
call    Free
sub     esp, 18h
mov     [ebp+Block], 0
mov     ecx, esp
mov     [ebp+nNumberOfBytesToWrite], esp
push    ebx                     ; int
call    sub_F22AA0
sub     esp, 18h
mov     byte ptr [ebp+var_4], 7
lea     eax, [ebp+var_98]
mov     ecx, esp
push    eax
call    sub_F22A50
lea     ecx, [ebp+Block]
mov     byte ptr [ebp+var_4], 4
call    RSA
mov     ecx, [ebp+Block]
add     esp, 30h
mov     [ebp+var_18], eax
mov     [ebp+nNumberOfBytesToWrite], ecx
test    ecx, ecx
jz      short loc_F216CE
```

Piece of code from the file encryption routine

Depending on the availability of the C&C server, Stop ransomware uses either an online or offline RSA key. The offline public RSA key can be found in the configuration of each malicious sample.



```
   unpacked_                         ↓FRO --------            PE .00504493|Hiew 8.45 (c)SEN
net Explorer . b i t /   ? p i d =   & f i r s t = t r u e   & f i r s t = f a l s e
{"public_key":" ","id":"ÇÇÇÇ-----BEGIN PUBLIC KEY-----\\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAoL7H22GD6fWn9jyeIjUH\\nfi9CNxwYfTLdtgFEI64kWoenPP8ymMttpS9OrH5qRJGgOgjdVHNtA6
 áááááááááááááááááÇRKdT+4qcA3\\nLI58pWNjqVJp1Y6zO4dyFg30rwiftEeUCHCQzLMsqUTr7PK56+yG6c\/pP
lEb0BFj\\nFmEp1lGVH5WMWVrDllMKCNLbPZ7dUZKpi9aoZCQzti+jTQ1PNiulMK1MkyDMtlWr\\nS3 áááááááááá
áááááááÇc412JHaPOHy61GTZIy00DGXzE30JF6vDYautEHUo6q9EhQgiFFzSwNycjc\/HNH\\nXjEONcSEj7+odHV
6baPXzoUT9J2cUaO7Ut7oZHJumZDyUcPNRHnb\/UxZtBWKjvwx\\nZwIDAQAB\\n----- áááááááááááááááááÇEN
D PUBLIC KEY----- run ht[redacted]$run [redacted]5.e
xe$run _olëRoáo_olëRoσ└                                   áááááááááááááááááÇ

                                                    áááááááááááááááááÇ

                                           áááááááááááááááááÇ
```

The dumped fragment of the malware

CONCLUSION AND RECOMMENDATIONS

2019 has been a year of ransomware attacks on municipalities, and this trend is likely to continue in 2020. There are various reasons why the number of attacks on municipalities is increasing.

First of all, the cybersecurity budgeting of municipalities is often more focused on insurance and emergency response than on proactive defense measures. This results in cases where the only possible solution is to pay the criminals and facilitate their activities.

Secondly, municipal services often have numerous networks that include multiple organizations, so hitting them causes disruption on many levels at the same time, bringing processes across entire districts to a halt.

What's more, the data stored in municipal networks is often vital for the functioning of everyday processes, as it directly concerns the welfare of citizens and local organizations. By striking such targets, cybercriminals are hitting a sensitive spot.

However, simple preventive measures can help combat the epidemic:

- It is essential to install all security updates as soon as they appear. Most cyberattacks exploit vulnerabilities that have already been reported and addressed, so installing the latest security updates lowers the chances of an attack.
- Protect remote access to corporate networks by VPN and use secure passwords for domain accounts.
- Always update your operating system to eliminate recent vulnerabilities and use a robust security solution with updated databases.
- Always have fresh back-up copies of your files so you can replace them in case they are lost (e.g. due to malware or a broken device) and store them not only on a physical medium but also in the cloud for greater reliability.
- Remember that ransomware is a criminal offence. You shouldn't pay a ransom. If you become a victim, report it to your local law enforcement agency. Try to find a decryptor on the internet first – some of them are available for free here: https://noransom.kaspersky.com

- Educating employees about cybersecurity hygiene is necessary to prevent attacks from happening in the first place. Kaspersky Interactive Protection Simulation Games offer a special scenario that focuses on threats relevant to local public administration.
- Use a security solution for organizations in order to protect business data from ransomware. Kaspersky Endpoint Security for Business has behavior detection, anomaly control and exploit prevention capabilities that detect known and unknown threats and prevent malicious activity. A preferred third-party security solution can also be enhanced with the free Kaspersky Anti-Ransomware Tool.

Kaspersky Security Bulletin

Advanced threat predictions for 2020

CONTENTS

ADVANCED THREAT PREDICTIONS FOR 2020

Nothing is more difficult than making predictions. Rather than trying to gaze into a crystal ball, we will be making educated guesses based on what has happened during the last 12 months, to see where we can see trends that might be exploited in the near future.

This is what we think might happen in the coming months, based on the knowledge of experts in this field and our observation of APT attacks – since APT threat actors have historically been the center of innovation.

The next level of false flag attacks

The use of false flags has become an important element in the playbook of several APT groups. In the past, this has generally involved trying to deflect attention away from those responsible for the attack – for instance, the usage of Russian words in Lazarus group malware, or Romanian words by WildNeutron. In one notable case – the Olympic Destroyer attack – the Hades APT group sought to go further than just clouding the waters of attribution by forging elements of the attack to make it seem like the work of a different threat actor. We believe that this will develop further, with threat actors seeking not only to avoid attribution but to actively lay the blame on someone else.

We should consider how actors continually use commodity malware, scripts, publicly available security tools or administrator software during their attacks and for lateral movement, making attribution increasingly difficult

For instance, this could include the usage of established backdoors by other unrelated APT actors, the theft and re-use of code (the recently published case of Turla reusing code from an unknown Iranian group, outlined by the UK NCSC and NSA comes to mind) or deliberately leaking source code so that other groups adopt it and muddy the waters further.

On top of all that, we should consider how actors continually use commodity malware, scripts, publicly available security tools or administrator software during their attacks and for lateral movement, making attribution increasingly difficult. Mixing a couple of false flags into this equation, where security researchers are hungry for any small clue, might be enough to divert authorship to someone else.

Ransomware is, unfortunately, the most effective tool for extracting a financial profit from the victims.

From ransomware to targeted ransomware

In the last two years we've seen a decline in numbers of all-purpose widespread ransomware attacks as cybercriminals have become more targeted in their use of this type of malware – focusing on organizations that are likely to make substantial payments in order to recover their data. We are calling this technique 'targeted ransomware'. Throughout the year, we recorded several cases where attackers used targeted ransomware, and we think that a likely future development will be more aggressive attempts to extort money. A potential twist might be that, instead of making files unrecoverable, threat actors will threaten to publish data that they have stolen from the victim company.

In addition to targeted ransomware, it is inevitable that the cybercriminals will also attempt to diversify their attacks to include other types of devices besides PCs or servers. For instance, ransomware in consumer products, such as smart TVs, smart watches, smart cars/houses/cities. As more devices become connected to the internet, cybercriminals will also be looking for ways to monetize their access to these devices. Ransomware is, unfortunately, the most effective tool for extracting a financial profit from the victims.

New online banking and payments attack vectors

A new potential attack vector for cybercriminals could open up with the new banking regulations that have recently come into full effect across the EU. The PSD2 (Payments Services Directive) lays down regulatory requirements for companies that provide payment services, including the use of personal data by new fintech companies that are not part of the established banking community. Security of online, including mobile, payments is a key aspect of the legislation. Nevertheless, as banks will be required to open their infrastructure and data to third parties who wish to provide services to bank customers, it is likely that attackers will seek to abuse these new mechanisms with new fraudulent schemes.

More infrastructure attacks and attacks against non-PC targets

Determined threat actors have, for some time, been extending their toolsets beyond Windows, and even beyond PC systems: VPNFilter and Slingshot, for example, targeted networking hardware. The benefit to an attacker, of course, is that once they have compromised such devices, it gives them flexibility. They could opt 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 our threat predictions for 2019, we considered the possibility of 'malware-less' attacks, where opening a VPN tunnel to mirror or redirect traffic might provide all the necessary information to an attacker. In June, it was revealed that hackers had infiltrated the networks of at least 10 cellular telcos around the world, and had remained hidden for years. In some cases, it seems they had been able to deploy their own VPN services on telco infrastructure. The convergence of real and cyber worlds brought about by the profusion of IoT devices offers growing opportunities for attackers; and it's evident that threat actors are aware of the potential. This year it was reported that unknown attackers stole 500MB of data from NASA's Jet Propulsion Laboratory using a Raspberry Pi. In December last year, the UK's Gatwick airport was brought to a standstill for fear of a possible collision after at least one drone was sighted above one of the runways. While it's unclear whether this was the result of a hobbyist drone owner or a determined DDoS attacker, the fact remains that part of the country's critical infrastructure was brought to a standstill because of the use of a drone. The number of such attacks will undoubtedly grow.

In recent years, we have seen a number of high-profile attacks on critical infrastructure facilities and these have typically been aligned to wider geo-political objectives. While most infections in industrial facilities continue to be from 'mainstream' malware, this fact itself highlights just how vulnerable these facilities can be. While targeted attacks on critical infrastructure facilities are unlikely ever to become a mainstream criminal activity, we do expect to see the number grow in the future. Geo-political conflicts are now played out in a world where the physical and cyber are increasingly converging; and, as we have observed before, such attacks offer governments a form of retaliation that lies between diplomacy and war.

“War is merely the continuation of politics by other means”

Increased attacks in regions that lie along the trade routes between Asia and Europe

Clausewitz’s dictum, “War is merely the continuation of politics by other means”, can be extended to include cyberconflict, with cyberattacks reflecting wider real-world tensions and conflicts. We have seen numerous examples. Consider, for example, accusations of Russian interference in US elections and fears about a possible reboot of this in the run-up to the 2020 elections. We’ve seen it in the ‘naming-and-shaming’ of alleged Chinese hackers in US indictments. The widespread use of mobile implants to surveil ‘persons of interest’ is another example.

There are several ways this could play out. They include a growth in political espionage as governments seek to secure their interests at home and abroad. This could mean monitoring the activities of ‘undesirable’ individuals or movements within the country, as well as those of potential opponents abroad. It is likely to extend also to technological espionage in situations of potential or real economic crisis and resulting instability. This could result in new attacks in regions that lie along trade routes between Asia and Europe, including Turkey, East and South Europe and East Africa.

It’s quite possible that we will see changes to legislation and policy, as governments look to define more clearly what is and what isn’t allowed. On the one hand, this could be used as a way to establish plausible deniability and thereby avoid sanctions if the finger of suspicion is pointed at one state by another. On the other hand, it could enable more aggressive use of technology, as several justice departments seem keen to open the door to different kinds of ‘lawful interception’ to collect evidence on computers. One likely response from criminal groups will be greater use of encryption and the Darknet to conceal their operations.

It could enable more aggressive use of technology, as several justice departments seem keen to open the door to different kinds of ‘lawful interception’ to collect evidence on computers

Increasing sophistication of attack methods

It is hard to know exactly how advanced the top-class attackers really are and what kind of resources they have in their pockets. Of course, every year we learn a bit more: for instance, a few years ago we observed an apparent endless supply of zero-days for resourceful attackers who were ready to pay for them. This year we observed several examples, but probably the most interesting is the one involving at least 14 exploits for iOS during the last two years, as exposed by Google in August.

The new isolation methods implemented for Microsoft Word and other software traditionally targeted in spear-phishing campaigns might have a significant impact in malware delivery methods, forcing less sophisticated actors to change the way they spread malware.

We believe it is likely that additional interception capabilities, similar to the Quantum insert attacks described a few years ago, are already being used; and hopefully we will be able to discover some of them.

It also seems likely that attackers will exfiltrate data with non-conventional methods, such as using signaling data or Wi-Fi/4G, especially when using physical implants (something we also believe is probably being overlooked). In a similar vein, we believe more attackers will use DoH (DNS over HTTPS) in the future to conceal their activities and make discovery more difficult. Finally, it is possible that during the coming months we will start discovering more UEFI malware and infections as our ability to see such systems is slowly improving.

Use of supply chains will continue to be one of the most difficult delivery methods to address. It is likely that attackers will continue to expand this method through manipulated software containers, for example, and abuse of packages and libraries.

During the last 10 years, an important transition has taken place: the main storage for our digital lives has moved from the PC to mobiles.

A change of focus towards mobile attacks

During the last 10 years, an important transition has taken place: the main storage for our digital lives has moved from the PC to mobiles. Some threat actors were quick to notice this and begin focusing on developing attack tools for mobiles. While we have constantly been predicting a huge increase in the number of attacks against mobiles, the observations from the field haven't always reflected this inferred evolution. However, the lack of observations of a phenomenon doesn't necessarily imply that it's not happening.

We have already discussed how an attacker abused at least 14 zero-day vulnerabilities in iOS to target certain minorities in Asia. We also saw recently how Facebook sued the Israeli company NSO for allegedly misusing its servers (to deploy malware to intercept user data). We also saw how Android zero-click, full persistence exploits are now more expensive (according to Zerodium's price list) than those for the iPhone.

All of this is telling us how much money attackers are investing in developing these technologies. It is clear to all of them how nearly everyone has a phone in his/her pocket and how valuable the information on those devices is. Every year we see new movements in this direction. We also see how complicated it might be for security researchers to obtain more technical details about attacks on such platforms, given the lack of visibility or accessibility.

There are no good reasons to think this will stop any time soon. However, due to the increased attention given to this subject by the security community, we believe the number of attacks being identified and analyzed in detail will also increase.

The abuse of personal information: from deep fakes to DNA leaks

We have previously discussed how data leaks help attackers to craft more convincing social engineering attacks. Not every adversary has a complete profile of potential victims to abuse, which makes the increasing amount of leaked data very valuable. This is also true for 'less targeted' attacks like the ransomware cases we have already discussed.

In a world where logged data continues to grow, we can see the danger in what could be considered especially sensitive leaks, for instance when it comes to biometric data. Also, widely discussed deepfakes are providing the technology to make such attacks a possibility, especially when combining this with less obvious attack vectors such as video and audio. We should not forget how this can be automated, and how AI can help with the profiling and creation of such scams.

Yes, all this sounds futuristic, but it is very similar to some of the techniques discussed for driving election advertisements through social media. This technology is already in use and it is just a matter of time before some attackers take advantage of it.

The future holds so many possibilities that there are likely to be things that are not included in our predictions. The extent and complexity of the environments in which attacks play out offer so many possibilities. In addition, no single threat research team has complete visibility of the operations of APT threat actors. We will continue to try and anticipate the activities of APT groups and understand the methods they employ, while providing insights into their campaigns and the impact they have.

Corporate security prediction 2020

kaspersky

CORPORATE SECURITY PREDICTIONS 2020

The popularity of cloud services is growing, and threat actors are here to exploit the trend.

We are observing more and more cases where our customers' infrastructure is partially or entirely located in the cloud – cloud migration has been the dominant trend of the past couple of years. This is resulting in a blurring of infrastructure boundaries. In 2020, we expect the following trends to emerge:

- It will become more difficult for attackers to separate the resources of the targeted company from those of cloud providers. It will be much more difficult for companies to detect an attack on their resources in the initial stages.

The transition to the cloud has blurred the boundaries of company infrastructures. As a result, it is becoming very difficult to target an organization's resources in a precise manner. So, conducting an attack will become harder and the actions of threat actors will become more sophisticated or more frequent – relying on chance rather than planning. On the other hand, it will also be difficult for a company to identify targeted attacks at an early stage and separate them from the overall mass of attacks on the ISP.

- Investigating incidents will become more complex and in some cases less effective.

Those who plan to deploy cloud infrastructure in 2020 need to talk in advance with their provider about a communications plan in the event of an incident, because time is of the essence when it comes to security incidents. It's very important to discuss what data is logged, and how to back it up. Lack of clarity on such information can lead to complications or even make successful incident investigation impossible. We note, however, that awareness of cloud infrastructure security is not growing as fast as the the popularity of cloud services, so we expect to see an increase in the complexities of investigating incidents as well as a decrease in the effectiveness of incident response.

It's also worth noting that when companies pass on their data to a cloud provider for storage or processing, they also need to consider whether the provider possesses the necessary level of cybersecurity. Even then, it is hard to be absolutely certain that the services they are paying for are really secure, as it requires a level of expertise in information security that not all technical officers possess.

There is a number of ways such insiders can be recruited:

- By simply posting an offer on forums and offering a reward for certain information.
- The attackers may disguise their actions so that employees don't realize they are acting illegally, disclosing personal information or engaging in insider activity. For example, the potential victims may be offered a simple job on the side to provide information, while being reassured that the data is not sensitive, though it may in fact relate to the amount of funds in a bank client's personal account or the phone number of an intended target.
- Blackmailing. We also expect to see increased demand for the services of groups engaged in corporate cyber-blackmail and, as a consequence, an increase in their activity.

- Criminals will migrate to the cloud and forge ahead.

The increase in the availability of cloud services will allow not just companies but also attackers to deploy infrastructure in the cloud. This will reduce the complexity of an attack and, consequently, will increase their number and frequency. This could potentially affect the reputation of the cloud services themselves, as their resources will be used in large-scale malicious activity. To avoid this, providers will have to consider reviewing their security procedures and change their service policies and infrastructure.

Insiders market is expanding

The good news is that we are observing an increase in the overall level of security of businesses and organizations. In this regard, direct attacks on infrastructure (for example, penetrating the external perimeter through the exploitation of vulnerabilities) is becoming much more expensive, requiring more and more skills and time for the attacker. As a result, we predict:

- Growth in the number of attacks using social engineering methods.

In particular, this means phishing attacks on company employees. As the human factor remains a weak link in security, the focus on social engineering will increase as other types of attacks become more difficult to carry out.

- Growth of the insider market.

Due to the increasing cost of other attack vectors, attackers will be willing to offer large amounts of money to insiders. The price for insiders varies from region to region and depends on the target's position in the company, the company itself, its local rating, the type and complexity of insider service that is requested, the type of data that is exfiltrated and the level of security at the company.

Cyber-blackmailing groups that collect compromising info on company employees (e.g. evidence of crimes, personal records and personal data such as sexual preferences) for the purpose of blackmail will become more active too in the corporate sector. Usually this happens in the following way: the threat actors take a pool of leaked emails and passwords, find those that are of interest to them and exfiltrate compromising data that is later used for blackmail or cyberespionage. The stronger the cultural specifics and regional regulations, the faster and more effective the attackers' leverage is. As a result, attacks on users in order to obtain compromising data are predicted to increase.

Cyberthreats to financial institutions 2020

Overview and predictions

KEY EVENTS 2019

- Large-scale anti-fraud bypass: Genesis digital fingerprints market uncovered
- Multi-factor authentication (MFA) and biometric challenges
- Targeted attack groups specializing in financial institutions: splitting and globalization
- ATM malware becomes more targeted
- Card info theft and reuse: magecarting everywhere and battle of POS malware families in Latin America

Large-scale anti-fraud bypass: Genesis digital fingerprints market uncovered

During the last few years, cybercriminals have invested a lot in methods to bypass anti-fraud systems, because now it's not enough just to steal the login, password and PII – they now need a digital fingerprint to bypass anti-fraud systems in order to extract money from the bank. During 2019, we identified a huge underground market called Genesis, which sells digital fingerprints of online banking users from around the globe.

From an anti-fraud system perspective, the user's digital identity is a digital fingerprint – a combination of system attributes that are unique to each device, and the personal behavioral attributes of the user. It includes the IP address (external and local), screen information (screen resolution, window size), firmware version, operating system version, browser plugins installed, time zone, device ID, battery information, fonts, etc. The device may have over 100 attributes used for browsing. The second part of a digital identity is the behavioral analysis.

As criminals are continuously looking for ways to defeat anti-fraud safeguards, they try to substitute the system's real fingerprint with a fake one, or with existing ones stolen from someone else's PC.

The Genesis Store is an online invitation-only private cybercriminal market for stolen digital fingerprints. At the time of our research, it offered more than 60 thousand stolen bot profiles. The profiles include browser fingerprints, website user logins and passwords, cookies, credit card information, etc. By uploading this fingerprint to the Tenebris Linken Sphere browser, criminals are able to masquerade as legitimate online banking users from any region, country, state, city, etc.

This type of attack shows that criminals have in-depth knowledge of how internal banking systems work and it's a real challenge to protect against such attacks. The best option is to always use multi-factor authentication.

Multi-factor authentication (MFA) and biometric challenges

MFA is a challenge for cybercriminals. When MFA is used, they have to come up with techniques to bypass it. The most common methods used during the last year were:

- Exploiting vulnerabilities and flaws in the configuration of the system. For example, criminals were able to find and exploit several flaws in remote banking systems to bypass OTPs (one time passcodes);
- Using social engineering, a common method among Russian-speaking cybercriminals and in APAC region;
- SIM swapping, which is especially popular in regions like Latin America and Africa. In fact, despite SMS no longer being considered a secure 2FA, low operational costs mean it's the most popular method used by providers.

In theory, biometrics should solve a lot of problems associated with two-factor authentication, but practice has shown that it may not be so simple. Over the past year, several cases have been identified that indicate biometrics technology is still far from perfect.

Firstly, there are quite a few implementation problems. For example, Google Pixel 4 does not check if your eyes are open during the unlocking process using facial characteristics. Another example is the possibility of bypassing fingerprint authentication using the sensor under the screen on smartphones made by various manufacturers, including popular brands such as Samsung.

There is another trick that has been exploited in Latin America: a visual capturing attack. Cybercriminals installed rogue CCTV cameras and used them to record the PINs people used to unlock their phones. Such a simple technique is still very effective for both types of victims: those who use biometrics and those who prefer PINs to fingerprints or facial recognition. This is because, when a device is dusty or greasy (and the same applies to a user's fingers), the best way to unlock a phone is to use a PIN.

Secondly, there were several high-profile leaks of biometric databases. The most notorious was the leak of the Biostar 2 database that included the biometric data of over 1 million people. The company stored unencrypted data, including names, passwords, home addresses, email addresses and, most importantly, unencrypted biometric data that included fingerprints and facial recognition patterns as well as the actual photos of faces. A similar leak occurred at a US Customs and

Border Patrol contractor, where biometric information of over 100,000 people was leaked.

There have already been several proof-of-concept attacks that use biometric data to bypass security controls, but those attacks could still be countered with system updates. With these latest leaks, on the other hand, this won't work because your biometric data cannot be changed – it stays with you forever.

The cases mentioned above, combined with the high-quality research carried out by cybercriminals to obtain a complete digital fingerprint of a user in order to bypass anti-fraud systems, suggest that relying solely on biometric data will not solve the current problems. Today's implementations need a lot of effort and more research to make them truly secure.

Targeted attack groups specializing in financial institutions: splitting and globalization

FIN7

In 2018, Europol and the US Department of Justice announced the arrest of the leader of the FIN7 and Carbanak/CobaltGoblin cybercrime groups. Some believed that the arrest would have an impact on the group's operations, but this does not seem to have been the case. In fact, the number of groups operating under the umbrella of CobaltGoblin and FIN7 has grown: there are several interconnected groups using very similar toolkits and the same infrastructure to conduct their cyberattacks.

The first operating under this umbrella is the now-notorious FIN7 that specializes in attacking various companies to get access to financial data or their PoS infrastructure. It relies on the Griffon JScript backdoor and Cobalt/Meterpreter and, in more recent attacks, PowerShell Empire.

The second is CobaltGoblin/Carbanak/EmpireMonkey. It uses the same toolkit, techniques and a similar infrastructure, but targets only financial institutions and associated software and service providers.

The final group is the newly discovered CopyPaste group, which has targeted financial entities and companies in one African country – leading us to believe that this group is associated with cyber-mercenaries or a training center.
The links between CopyPaste and FIN7 are still very weak. It's possible that the operators of this cluster of activity were influenced by open-source publications and don't actually have any ties to FIN7.

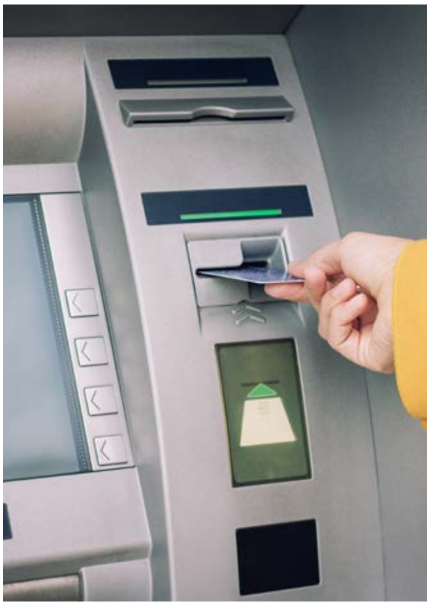
All of these groups benefit greatly from unpatched systems in corporate environments and continue to use effective spear-phishing campaigns in conjunction with well-known Microsoft Office exploits generated by their exploitation framework. So far, the groups have not used any zero-day exploits. FIN7/Cobalt phishing documents may seem basic, but when combined with their extensive social engineering and focused targeting, they have proved to be quite successful.

In the middle of 2019, FIN7 fell silent, but returned at the end of the year with new attacks and new tools. We suspect that the silent period is connected to their infrastructure shutdown that occurred after closing a bulletproof hosting company in Eastern Europe.

In contrast to FIN7, the activity of the Cobalt Goblin Group was stable throughout the year, which once again proves that these groups are connected, but operate on their own: their toolsets and TTPs are very similar, but operate independently; and only occasionally can we spot overlaps in infrastructure. At the same time, the intensity of attacks is slightly lower than in 2018. Cobalt Goblin's tactics have remained the same: they use documents with exploits that first load a small downloader and then a Cobalt beacon. The main targets also remain the same: small banks in a variety of countries. Perhaps we have detected a lower number of attacks due to diversification, because some indicators suggest the group could also be engaging in JS sniffing (MageCarting) in order to obtain data about payment cards directly from websites.

JS sniffing was extremely popular throughout the year and we found thousands of e-commerce websites infected with these scripts. The injected scripts act in different ways and the infrastructure of the attackers is very different, which suggests that this type of fraud is used by at least a dozen cybercrime groups.

The Silence group actively expanded its operations into different countries throughout the year. We detected attacks in regions where we have never seen them before. For example, we recorded attacks in Southeast Asia and Latin America. This indicates that they have either expanded their operations themselves or started cooperating with other regionally installed cybercrime groups. However, when we look at the development of their main backdoor, we see that their technologies have barely changed over the last two years.



ATM malware becomes more targeted

When it came to ATM malware, we discovered a number of completely new families in 2019. The most notable were ATMJadi and ATMDtrack.

ATMJadi is an interesting one because it doesn't use the standard XFS, JXFS or CSC libraries. Instead, it uses the victim bank's ATM software Java proprietary classes: meaning the malware will only work on a small subset of ATMs. It makes this malware very targeted (towards one specific bank).

This is reminiscent of the FASTcach case from 2018, when criminals targeted servers running AIX OS. With a decrease in the number of general-purpose cashout tools, we can say that ATM malware is becoming rarer and more targeted.

Another interesting piece of malware is ATMDtrack, which was first detected in financial institutions in India and is programmed to cash out ATMs. Using the Kaspersky Targeted Attack Attribution Engine (KTAE), we were able to attribute these attacks to the Lazarus group, which supports our prediction from 2018 that there will be "more nation-state sponsored attacks against financial organizations". Moreover, similar spyware has been found in research centers, with Lazarus APT group using almost identical tools to steal research results from scientific institutes.

Card info theft and reuse

During the year we saw a lot of malware targeting end users and businesses looking for credit card data. In Brazil, in particular, we saw a couple of malware families fighting it out between themselves to maintain control of infected devices. HydraPOS and ShieldPOS were very active during the year, with new versions that included a lot of new targets; Prilex, meanwhile, reduced its activities in the second half of the year.

ShieldPOS has been active since at least 2017 and, after being malware only, it has finally evolved into a MaaS (malware-as-a-service). This fact shows there's great interest from Latin American cybercriminals in running their own "business" to steal credit cards. HydraPOS has been mostly focused on stealing money from POS systems in restaurants, parking slot machines and different retail stores.

Compared to ShieldPOS, HydraPOS is an older campaign from an actor we named Maggler, which has been in the credit card business since at least 2016. The main difference is that, unlike ShieldPOS, it doesn't work as MaaS. In both cases, we suspect that the initial infection vector is a carefully prepared social engineering campaign involving telephone calls to the victims.

ANALYSIS OF FORECASTS FOR 2019

Before giving our forecasts for 2020, let's see how accurate our forecasts for 2019 turned out to be:

The emergence of new groups due to the fragmentation of Cobalt/Carbanak and FIN7: new groups and new geography.

- **Yes,** we saw CobaltGoblin activity, FIN7 activity, CopyPaste activity and the intersection of IoCs and the Silence group.

The first attacks through the theft and use of biometric data.

- **Yes,** hacking of various biometric data databases regularly appeared throughout the year. We also revealed a digital fingerprint market where criminals can buy digital fingerprints, which includes, among other things, behavioral data (component of biometrics).

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

- **No.** It turned out that well-known groups such as Lazarus, Silence and CobaltGoblin took their place and very actively attacked financial institutions in these regions.

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

- **Yes.**

Traditional cybercrime will focus on the easiest targets and bypass anti-fraud solutions: replacement of POS attacks with attacks on systems accepting online payments (Magecarting/JS skimming).

- **Yes,** the number of groups that started carrying out attacks on online payment systems grew constantly over the year. We detected thousands of websites that were affected by JS skimming.

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

- **Yes,** and not only in financial institutions but even the aerospace industry, namely NASA, has suffered from this type of attack.

Attacks on mobile banking for business users.

- **No.**

Advanced social engineering campaigns targeting operators, secretaries and other internal employees in charge of wire transfers.

- **Yes,** BEC (business email compromise) attacks have been on the rise worldwide. We have seen major attacks in Japan, while there have also been campaigns in South America, particularly in Ecuador.
- Additionally, advanced social attacks have been actively used in Brazil to make POS operators go to a malicious website to download specially crafted remote control modules and run them, for example, in HydraPOS attacks.

FORECAST 2020

Attacks against Libra and TON/Gram

The successful launch of cryptocurrencies such as Libra and Gram might lead to the worldwide spread of this type of asset, which naturally will attract the attention of criminals. Given the serious surge in cybercriminal activity during the rapid growth of Bitcoin and altcoins in 2018, we predict that a similar situation will most likely unfold around Gram and Libra. Large players in this market should be especially careful, as there are a number of APT groups, such as WildNeutron and Lazarus, whose interests include crypto assets. They are very likely to exploit these developments.

Reselling bank access

During 2019, we witnessed cases where groups who specialize in targeted attacks on financial institutions appeared in the victims' networks after intrusions by other groups that specialize in selling rdp/vnc access, such as FXMSP and TA505. These facts are also confirmed by underground forums and chat monitoring.

In 2020, we expect an increase in the activity of groups specializing in the sale of network access in the African and Asian regions, as well as in Eastern Europe. Their prime targets are small banks, as well as financial organizations recently bought by big players who are rebuilding their cybersecurity system in accordance with the standards of their parent companies.

Ransomware attacks against banks

This forecast logically follows from the previous one. As mentioned above, small financial institutions often become the victims of opportunistic cybercriminals. If these criminals cannot resell access, or even if it becomes less likely that they will be able to withdraw money, then the most logical monetization of such access is ransomware. Banks are among those organizations that are more likely to pay a ransom than accept the loss of data, so we expect the number of such targeted ransomware attacks to continue to rise in 2020.

Another ransomware attack vector against small and medium financial institutions will be a "pay-per-install" scheme. Traditional botnets will eventually turn into increasingly popular delivery mechanisms against those financial institutions.

2020: the return of custom tooling

Measures taken by antivirus products to effectively detect open source tools used for pen testing purposes, and the adoption of the latest cyberdefense technologies, will push cybercrime actors to return to custom tooling in 2020 and also invest in new Trojans and exploits.

Global expansion of mobile banking Trojans: result of leaked source

Our research and monitoring of underground forums suggests that the source code of some popular mobile banking Trojans was leaked into the public domain. Given the popularity of such Trojans, we expect a repeat of the situation when the source code of ZeuS and SpyEye Trojans were leaked: the number of attempts to attack users will increase at times, and the geography of attacks will expand to almost every country in the world.

Investment apps on the rise: new target for criminals

Mobile investment apps are becoming more popular among users around the globe. This trend won't go unnoticed by cybercriminals in 2020. Given the popularity of some fintech companies and exchanges (for both real and virtual money), cybercriminals will realize that not all of them are prepared to deal with massive cyberattacks, as some apps still lack basic protection for customer accounts, and do not offer two-factor authentication or certificate pinning to protect app communication. Several governments are deregulating this area and new players are appearing every day, becoming popular very quickly. In fact, we have already seen attempts by cybercriminals to substitute the interfaces of these apps with their own malicious versions.

Magecarting 3.0: even more attacker groups and cloud apps to become prime targets

Over the past couple of years, JS skimming has gained immense popularity among attackers. Unfortunately, cybercriminals now have a huge attack surface that consists of vulnerable e-commerce websites and extremely cheap JS skimmer tools available for sale on various forums, starting at $200. At the moment we are able to distinguish at least 10 different actors involved in these types of attacks and we believe that their number will continue to grow during the next year. The most dangerous attacks will be on companies that provide services such as e-commerce as a service, which will lead to the compromise of thousands of companies.

Political instability leading to the spread of cybercrime in specific regions

Some countries are experiencing political and social upheaval, resulting in masses of people seeking refugee status in other countries. These waves of immigration include all sorts of people, including cybercriminals. This phenomenon will result in the spread of geographically localized attacks in countries that have not previously been affected by them.

Cybersecurity of connected healthcare 2020

Overview and predictions

kaspersky

CYBERSECURITY OF CONNECTED HEALTHCARE 2020: OVERVIEW AND PREDICTIONS

More than two years after the infamous Wannacry ransomware crippled medical facilities and other organizations worldwide, the healthcare sector seems to be learning its lesson, as the number of attacked medical devices – doctors' computers, medical servers and equipment – in 2019 decreased globally.

Our statistics showed that from 30% of computers and devices in medical organizations being infected in 2017, this number dropped to 28% in 2018, and we detect almost a third less attacks for the current year (19%).

As much as we want to believe everybody has woken up to the dangers of attacks like Wannacry, we still witnessed a number of ransomware attacks against healthcare facilities in several countries. There are two key reasons for such cyberattacks: a lack of attention to the risks of digitalization and a lack of cybersecurity awareness among staff at medical facilities.

Our conclusions about the human factor in cybersecurity are drawn from survey results. Kaspersky conducted a survey among healthcare sector employees in the US and Canada that revealed nearly a third of all respondents (32%) had never received any cybersecurity training from their workplace.

One-in-10 employees in management positions also admitted that they were unaware of a cybersecurity policy in their organization.

Another serious issue is the lack of proper security standards implemented in medical IoT devices. Throughout the year security researchers identified a number of vulnerabilities in different medical equipment. Hopefully, drawing attention to this subject will make manufacturers collaborate with the security community and contribute more to the creation of a safer environment in the world of smart medicine.

Forecast 2020

- Interest in medical records on the dark web will grow. From our research into underground forums we see that such records are sometimes even more expensive than credit card information. It also opens up potentially new methods of fraud: armed with someone's medical details it's easier to scam the patient or his/her relatives.

- Access to internal patient info makes it possible not only to steal but to modify records. This can lead to targeted attacks on individuals in order to mess up diagnostics. Diagnostic mistakes are the number one reason for patient deaths in the medical field according to statistics (even ahead of poorly qualified medical personnel).

- The number of attacks on medical facility devices in countries that are just starting the digitalization process in the field of medical services will grow significantly next year. We expect to see the emergence of targeted ransomware attacks against hospitals in developing countries. Medical institutions are turning into industrial infrastructures. Loss of access to internal data (e.g. digital patient records) or internal resources (e.g. connected medical equipment inside a hospital) can halt patient diagnostics and even disrupt emergency aid.

- Growing numbers of targeted attacks against medical research institutes and pharmaceutical companies conducting innovative research. Medical research is extremely expensive and some APT groups that are specialized in intellectual property theft will attack such institutions more frequently in 2020.

- Thankfully, we've never seen attacks on implanted medical devices (e.g. neuro-stimulators) in the wild. But the fact that there are numerous security vulnerabilities in such devices means that it's just a matter of time. The creation of centralized networks of wearable and implanted medical devices (as in the case of cardio stimulators) will lead to the emergence of a new threat: a single point of entry to attack all the patients using such devices.

Predictions about what security implications 5G technology will bring in 2020

kaspersky

5G TECHNOLOGY PREDICTIONS 2020

It is estimated that data will reach 175 zettabytes worldwide by 2025, up from 1.2 zettabytes in 2010, when 4G was first being deployed globally. 5G is known as the fifth generation cellular network technology. It is expected to be as much as 100 times faster than the present 4G systems, with up to 25 times lower latency or lag time, and as many as one million devices supported within one square kilometer. The foundation of 5G can be summarized in five technologies: millimeter waves, small cell networks, massive MIMO (multiple input multiple output), beamforming, and bytes full duplex.

With the dramatic increase in the amount and transfer speed of connected devices comes a natural expansion and amplification of the threats. The evolution, development and connectivity of numerous systems within 5G opens the door to numerous threats, which can be summarized as follows.

Vulnerabilities of telco services and infrastructure

As 5G innovations spread, more shortcomings and imperfections will show up in 5G gear, customer frameworks and administration by authorities. This could enable an attacker to damage or bring down a telco infrastructure, spy on its clients or divert its traffic. Governments need to set up nationwide capabilities to utilize objective and specialized confirmation techniques to evaluate both 5G adopters and suppliers, to discover faults and stipulate fixes.

User safety and privacy concerns

On the privacy side, matters become more complex. The advent of 5G with its short range will definitely mean more cell communication towers being deployed into commercial centers and buildings. With the right toolset, someone could collect and track the precise location of users. Another issue is that 5G service providers will have extensive access to large amounts of data being sent by user devices, which could show exactly what is happening inside a user's home and at the very least describe via metadata their living environment, in-house sensors and parameters. Such data could expose a user's privacy or could be manipulated and misused. Service providers may also consider selling such data to other service

companies such as advertisers in an attempt to open up new revenue streams. In some cases, vulnerabilities could cause injuries or ill health, for instance, if a client's therapeutic gadgets are disconnected and not operational. The potential threats will be even greater when critical infrastructure components such as water and energy equipment are put at risk.

Critical infrastructure expansion and risks

5G will assist in spreading communication to a larger number of geographical areas than at present. It will also equip non-networkable gadgets with remote monitoring and control. However, increasing numbers of connected systems like this will no longer be non-critical infrastructure, expanding our exposure to risk. People are being enticed to adopt convenience and non-stop communications, but the related threats could pose public safety risks.

Action plan

5G is going to have a revolutionary impact on telecommunications because, in addition to the technology itself, it is going to become a basis for other technologies and inventions, giving way to technological advances, particularly in the fields of smart cities, intelligent power grids and defense facilities. It is the next generation of cellular network using the existing 4G LTE in addition to opening up millimeter wave band. 5G will be able to welcome more network-connected devices and considerably increase speeds for all users.

However, as with every major technology, especially while it is evolving, 5G is likely to draw the attention of threat actors looking for opportunities to attack it. We may, for instance, see large-scale DDoS attacks, or challenges in terms of protecting a sophisticated network of connected devices whereby the compromise of one device can lead to a whole network crashing. In addition, 5G is developing technology on top of the previous infrastructure, which means it will inherit the vulnerabilities and misconfigurations of its predecessor.

Furthermore, the communication trust model will not be identical to previous cellular generations. IoT and M2M devices are expected to occupy a greater portion of the network capacity. The interaction of all these devices in the 5G network will likely trigger unprecedented issues in product design and device behavior. Given these fears and the political challenges, encouraging a zero-trust network model and strict product quality compliance would help build trust between the technology adopters and providers.

Government and industry leaders should join forces to promote secure and safe 5G technology projects to enhance the services and quality of life for citizens of smart cities. Furthermore, the communication trust model will be different from previous cellular generations.

IoT and M2M devices are expected to occupy the 5G network bandwidth, and the interlinkage of all these devices in the 5G network will reveal previously unknown problems in the design and behavior of 5G. With regards to such worries and the additional political disputes, adopting a zero-trust network model and strict quality assessment along with compliance would help shape the relationship between the technology adopters and providers.

Hi-tech vendor and governmental structures should join forces to prevent the exploitation of 5G by threat actors and preserve its innovative features for technical progress and improving the quality of living conditions.