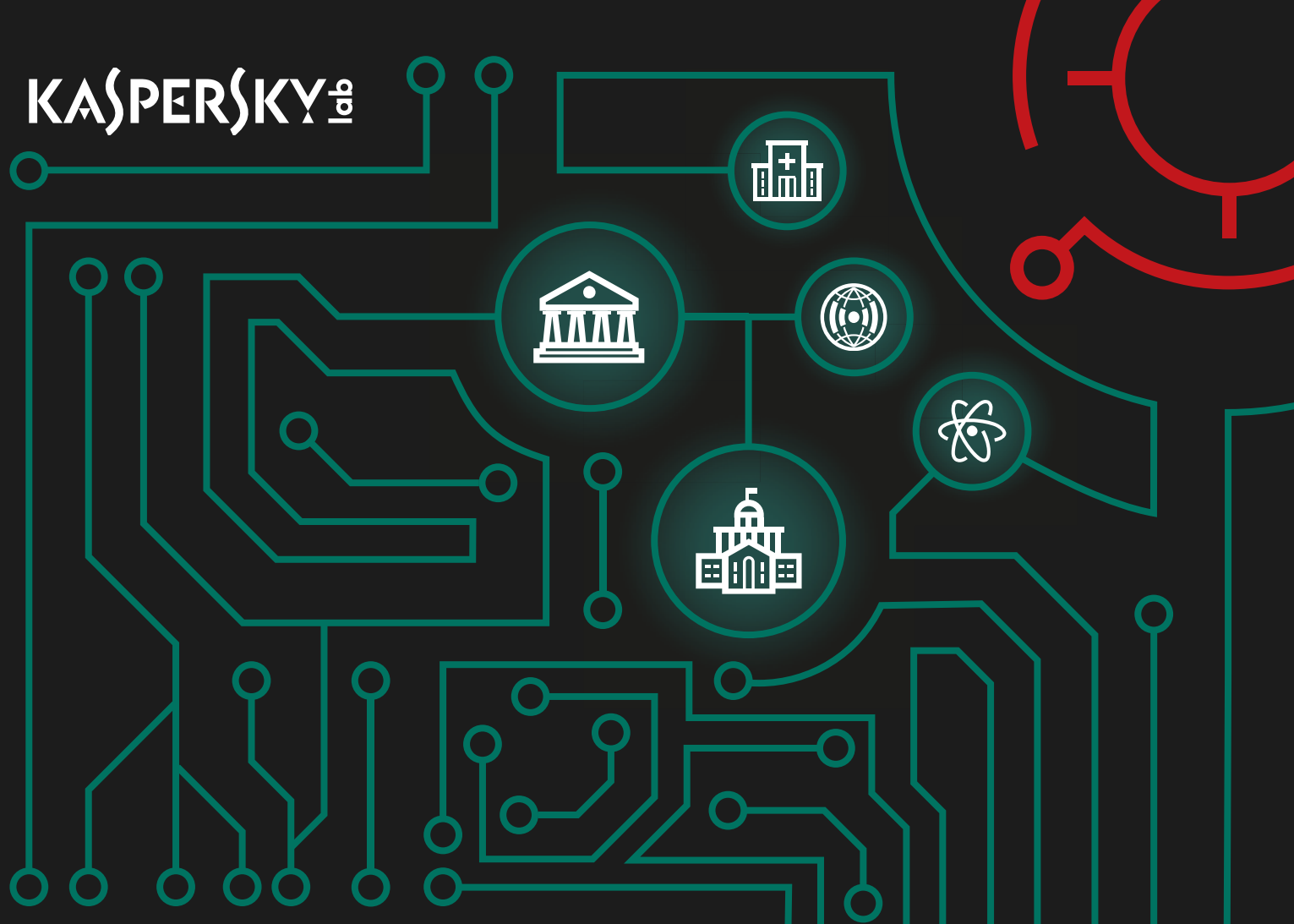
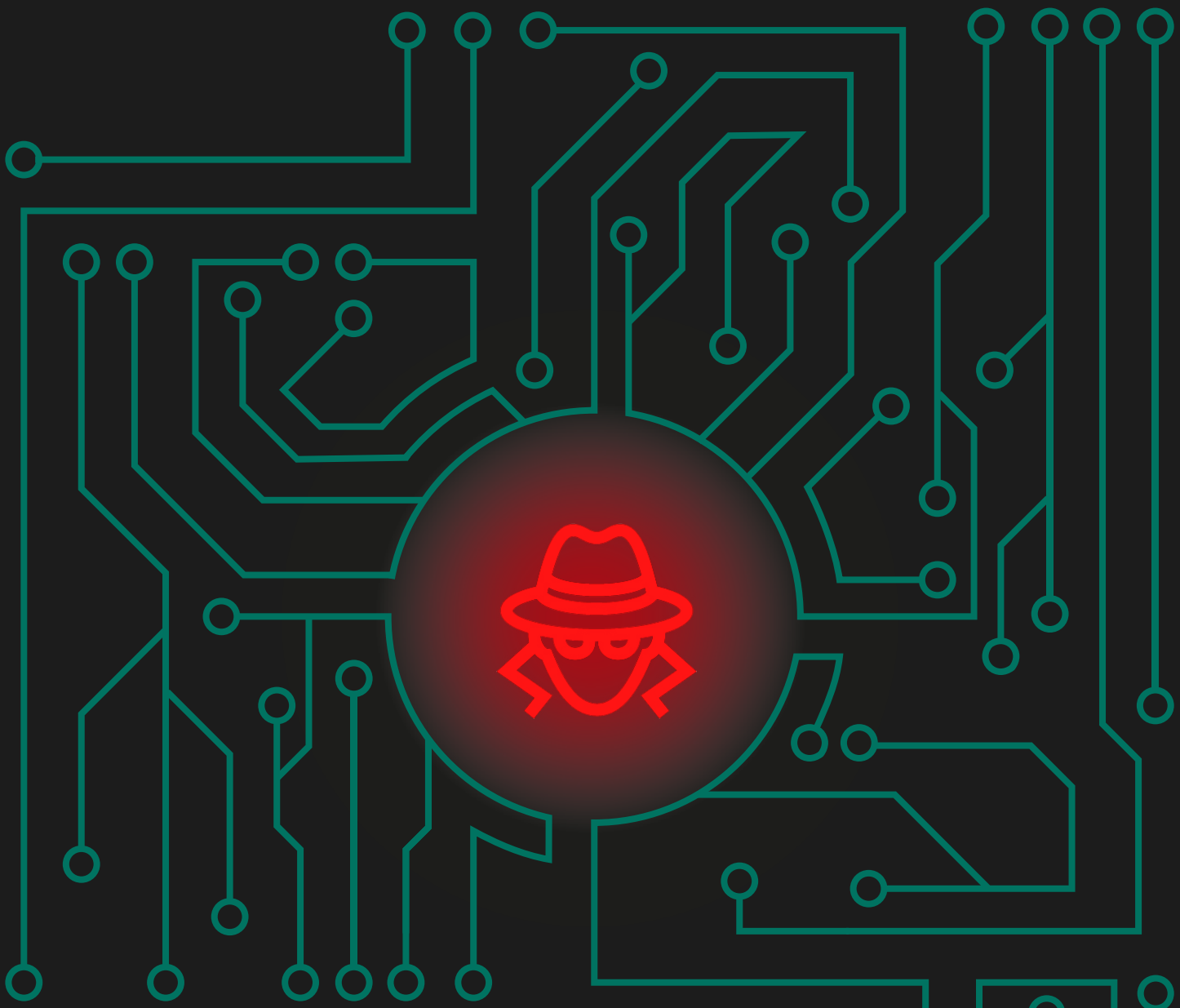
KASPERSKY lab



Kaspersky Security Bulletin:

REVIEW OF THE YEAR 2017

CONTENTS



A YEAR OF BLURRED BOUNDARIES

David Emm
Principal Security Researcher
Global Research and Analysis Team (GReAT)

INTRODUCTION

Connected technologies are everywhere, an integral part of our lives, and they offer cybercriminals a bigger attack surface than ever before. Across the world, organizations and individuals are increasingly under fire from cybercriminals in search of money, data, disruption, physical or reputational damage, or simply 'for the lulz'. The cyberthreat ecosystem has been building and evolving for years, and our annual review of key security trends and incidents forms part of this much longer timeline.

In 2017, what stood out most for us for the gradual disappearance of boundaries – the traditional lines between different types of threat and different types of threat actor. It will be interesting to see how this develops over 2018.

Examples of this trend include the ExPetr attack in June. At first sight, this seemed to be yet another ransomware program, but it turned out to be a destructive data wiper instead. Another example is the dumping of code by the Shadow Brokers group, which placed advanced exploits allegedly developed by the NSA at the disposal of criminal groups that would otherwise not have had access to such sophisticated code. Yet another is the emergence of advanced targeted threat (APT) campaigns focused not on cyber-espionage, but on theft, stealing money to finance other activities the APT group is involved in.

The evolution of ransomware in 2017, and the use of Shadow Broker's leaked exploits by lower grade groups is covered in the stand-alone report, Ransomware's new menace, available here. The other trends are covered in more detail below.

TARGETED ATTACKS

In 2017, the world's big cyberespionage threat actors continued to do what they do, but with new, harder-to-detect tools and approaches. We reported on a wide range of campaigns.

Russian-language threat actors

At April's Security Analyst Summit, researchers from Kaspersky Lab and King's College London presented their findings on a possible link between Moonlight Maze, a 20 year old cyberespionage attack that targeted the Pentagon, NASA and others, and Turla – a very modern APT group. Data stored on a server that had been hijacked for use as a proxy by the Moonlight Maze attackers helped them to reconstruct the operations, tools, and techniques used by the original attackers. They also conducted a parallel investigation into Turla. In particular, both operations made use of backdoors based on LOKI2, a program released in 1996 that allows data to be extracted via covert channels. You can find details of the research here.

In August, we provided an update on another Turla-related APT that we call WhiteBear. In mid-2017, WhiteBear extended its focus from embassies and consulates around the world to include defense-related organizations. We strongly suspect that the group uses spear-phishing e-mails to deliver malicious PDF files to its victims. The main module, the WhiteBear orchestrator, is particularly interesting. The attackers encrypt/decrypt, and pack/decompress the resource section with RSA+3DES+BZIP2 – something that is unique. Most WhiteBear samples are signed with a valid code-signing certificate issued for 'Solid Loop Ltd', a once-registered British organization. This is probably a front organization or a defunct organization; and the attackers have assumed its identity to abuse the name and trust, in order to create deceptive digital certificates.

English-language threat actors

In April, we also uncovered the most recent toolkit of the Lamberts, an advanced threat actor that can be compared with Duqu, Equation, Regin or ProjectSauron in terms of complexity. We found that this group, which first came to the attention of the security community in 2014, has been developing a range of sophisticated attack tools – including network-driven backdoors, several generations of modular backdoors, harvesting tools, and wipers – since at least 2008. There are currently known versions for Windows and OS X – with white, blue, green, blue, black, pink and gray variants, and we think that it is highly possible that other Lamberts exist for other platforms, such as Linux.

Chinese-speaking threat actors

We also uncovered more technical details about the Spring Dragon group, whose activities date back to 2012, and which makes extensive use of spear-phishing and watering-hole attacks. Targets include high-profile government agencies, political parties, educational institutions and telecommunication around the South China Sea – including Taiwan, Indonesia, Vietnam, the Philippines, Hong Kong, Malaysia and Thailand. In particular, we investigated the backdoors used by the group to steal data, execute additional malware components and run system commands on victim's computers. These give the attackers the ability to undertake a variety of different malicious activities on their victims' computers. The group maintains a large C&C (Command-and-Control) infrastructure, comprising more than 200 unique IP addresses and C&C domains.

Other language threat actors

In October, our advanced exploit prevention systems identified a new Adobe Flash zero-day exploit used in the wild against our customers, delivered through a Microsoft Office document. The final payload was the latest version of FinSpy malware. Only one attack has been observed in our customer base, so we believe that the number of attacks are minimal and highly-targeted. Our analysis of the payload allowed us to confidently link this attack to an actor we track as BlackOasis. We are highly confident that the same group was also responsible for another zero-day exploit (CVE-2017-8759) discovered by FireEye in September. We first became aware of BlackOasis activities in May 2016, while investigating another Adobe Flash zero-day (CVE-2016-4117), a vulnerability that was actively exploited in the wild. Data from the Kaspersky Security Network also helped us to identify two other similar exploit chains used by BlackOasis in June 2015 – which were also zero-days at the time (CVE-2015-5119 and CVE-2016-0984): these exploit chains also delivered FinSpy installation packages. The BlackOasis group targets people involved in Middle Eastern politics and others connected to the region. This includes prominent figures in the United Nations, opposition bloggers and activists, and regional news correspondents.

Other targeted threat actors active in the shadows include Black Energy, which may have been behind the ExPetr and BadRabbit ransomware attacks: researchers believe there might be a connection between ExPetr and the BlackEnergy KillDisk ransomware from 2015 and 2016.

DESTRUCTIVE ATTACKS

In 2017 we observed a resurgence of targeted attacks designed to destroy data, either instead of, or as well as data theft.

There have been several wiper attacks in recent years and in 2017 we reported on two more: Shamoon 2.0 and StoneDrill. Shamoon 2.0, a development of the malware believed to have been used to erase data on more than 30,000 computers at Saudi Aramco in 2012, re-appeared in November 2016 and early 2017, targeting organisations in various critical and economic sectors in Saudi Arabia. The new version featured new tools and techniques, including a custom wiper that used stolen credentials for lateral movement across the organization. The wiper, once installed in the network, activates on a pre-defined date, leaving infected computers unusable. Shamoon 2.0 also includes a ransomware component, although we have yet to see this used in the wild.

While investigating the Shamoon attacks, we discovered a previously unknown wiper, which we called StoneDrill. This also seems to target organizations in Saudi Arabia. There are similarities in style to Shamoon, with additional features designed to prevent detection. One of the victims of StoneDrill, observed via the Kaspersky Security Network (KSN) was located in Europe (and operates in the petro-chemicals sector), suggesting that the attackers might be expanding their wiping operations beyond the Middle East. The most significant difference between the two relates to the wiping process. Shamoon uses a disk driver for direct access to the disk, whereas StoneDrill injects the wiper directly into the victim's preferred browser. StoneDrill also includes a backdoor that has been used to run espionage operations against a number of targets.

We don't know whether the groups behind Shamoon and StoneDrill are the same, or are just aligned in terms of interests and the regions they target, although the latter seems most likely to us.

Incidentally, ExPetr, the attack that keeps reappearing throughout this annual review, belongs in this category too, as it was an operation designed purely for data destruction, disguised as ransomware. It is interesting to speculate whether the unused ransomware component of Shamoon 2.0 was also intended to serve as a distraction tool for a secondary attack, if needed?

SUCCESS WITHOUT SOPHISTICATION

In 2017 we uncovered threat actors achieving success, sometimes for years, with simple and poorly executed campaigns.

Targeted attacks don't have to be technically advanced in order to be successful. In January 2016, the arrest of two suspects by the Italian police brought to light a series of cyber-attacks that targeted prominent politicians, bankers, freemasons and members of law enforcement agencies. The malware used in the EyePyramid attack was unsophisticated and the OPSEC of the criminals behind the campaign was poor. Nevertheless, the attackers were successful enough to compromise the computers of up to 1,600 victims, mainly in Italy, before the police apprehended them. While the police report didn't include much technical information, it did contain details of C&C servers, e-mail addresses and IP addresses used to exfiltrate stolen data.

We used this to create a YARA rule to search our systems for a match on any known samples. Our initial YARA rule highlighted two samples, which enabled us to create a more specific YARA rule that identified a further 42 samples in our collection. From this we were able to learn more about EyePyramid. The attacks relied heavily on social engineering, tricking victims into opening and running infected files attached to the spear-phishing e-mails. The timestamps of the samples indicate that they were compiled in 2014-15. So despite the lack of technical sophistication, the attackers went undetected for several years and managed to steal gigabytes of data from their victims.

Microcin provided another example of how cybercriminals can achieve their goals by using cheap tools and selecting their targets with care. The attackers used a watering-hole attack using a Microsoft Office exploit. They compromised a forum hosting discussions on the state-subsidised housing that Russian military personnel and their families are entitled to. The attackers created an executable file on the victim's computer that downloaded further add-on modules, thereby extending the functionality of the malware. The attackers used a PowerShell script and other utilities to steal files and passwords found on the victim's computer. The methods used by the criminals are neither complicated nor expensive, but they are effective. There are two aspects of this attack that are of particular interest. First, the attackers chose to exploit human fallibilities, instead of spending time and money developing exploit code to launch a direct attack on corporate resources. Second, they made use of standard corporate tools to gain lateral movement within the target organisation.

STEAL TO SPY?

2017 also revealed the extent to which advanced threat actors were diversifying into common theft to fund their expensive operations.

In February 2016, a group of hackers (unidentified at that time) attempted to steal $851 million – and succeeded in transferring $81 million from the Central Bank of Bangladesh – in what is considered to be the largest and most successful cyber-heist ever. Research by Kaspersky Lab and others revealed that the attacks were almost certainly conducted by Lazarus, a notorious cyber-espionage and sabotage group – responsible for the attack on Sony Pictures in 2014, as well attacks on manufacturing companies, media and financial institutions in at least 18 countries around the world since 2009. The group's interest in financial gain is relatively new and it seems as though a different team within Lazarus, which we dubbed Blurnoroff, is responsible for the generation of illegal profits. So far, we have seen four main types of target: financial institutions, casinos, companies developing financial trade software and those in the crypto-currency business.

One of the most notable Bluenoroff campaigns was its attacks on financial institutions in Poland. The attackers were able to compromise a government web site that is frequently accessed by many financial institutions – making it a particularly powerful attack vector.

Lazarus is not just another APT group. The scale of its operations is shocking: it appears that Lazarus operates a malware factory, generating new tools as old ones are 'burned'. The group uses various code obfuscation techniques, re-writes its own algorithms, applies commercial software protectors, and uses its own and underground packers. All this costs money – which may explain why Lazarus has diversified into theft.

The Lazarus group also appears to be behind the WannaCry ransomware epidemic from May 2017 – further details of which can be found in *Ransomware's new menace*. It remains a mystery why such an advanced attack group would be behind the release of imperfect and uncontrolled, if devastating malicious code.

OTHER FINANCIAL ATTACKS

Attacks on ATMs continued to rise in 2017, with attackers targeting bank infrastructure and payment systems, using sophisticated fileless malware, taping over CCTVs and drilling holes.

At this year's Security Analyst Summit two of our researchers, Sergey Golovanov and Igor Soumenkov, discussed three cases where cybercriminals had stolen money from ATMs.

The first, ATMitch, involved compromising the bank's infrastructure in order to remotely control the ATM's operation. The attackers exploited an unpatched vulnerability to penetrate the target bank's servers. They used open source code and publicly available tools to infect computers in the bank. However, the malware they created resided in memory only, not on the hard drives, and almost all traces of the malware were removed when the computer was re-booted. Following the infection, the attackers established a connection to their C&C server, allowing them to remotely install malware on the ATMs. Since this looked like a legitimate update, it didn't trigger any alerts at the bank. Once installed, the malware looked for the commands that control the ATM. The malware first issues a command to find out how much money is in the ATM, then issues a further command to dispense money – collected by a money mule waiting at the ATM. After this, the malware wipes away the evidence.

One of the other bank attacks also started with a request from the bank. Money was missing, but the ATM logs were clear and the criminals had taped over the CCTV camera, so that there was no recording of the attack. The bank delivered the ATM to our office and, after disassembling it, we discovered that the criminals had installed a Bluetooth adaptor on the ATM and waited three months for the log to clear. Then they returned to the ATM, covered the security cameras and used a Bluetooth keyboard to re-boot the ATM in service mode and empty the cash dispenser.

The third attack, which, like those mentioned above, started with a bank asking us to investigate an ATM theft, turned out to be much cruder in its approach. We found a hole, approximately 4cm in diameter, drilled near the PIN pad. Not long after, we learned of similar attacks in Russia and Europe. When police caught a suspect with a laptop and some wiring, things became clearer. We disassembled the ATM to try to find out what the attacker could be trying to access from the hole. What we found was a 10-PIN header, connected to a bus that connects all of the ATMs components and weak encryption that could be broken very quickly. Any single part of the ATM could be used to control all the others; and since there was no authentication between the parts, any one of them could be replaced without the others realising. It cost us around $15 and some time to create a simple circuit board that could control the ATM once we connected it to the serial bus, including dispensing money. Fixing the problem, as our researchers highlighted, isn't straightforward. Patching requires a hardware update and can't be done remotely: a technician must visit all the affected ATMs to install it.

More recently, we discovered a new targeted attack on financial institutions - mainly banks in Russia, but also some in Malaysia and Armenia. The attackers behind the Silence Trojan use a similar approach to Carbanak. They gain persistent access to the internal bank network, make video recordings of the day-to-day activities of bank employees, to learn the bank's procedures and the software installed, then they use this information to steal money. The infection vector is a spear-phishing e-mail with a malicious attachment. However, an interesting twist in the Silence attack is that the cybercriminals had already compromised banking infrastructure in order to send their spear-phishing e-mails from the addresses of real bank employees, thereby looking unsuspicious to future victims.

USING THE SUPPLY-CHAIN AS A STEPPING-STONE

An emerging business threat in 2017 that looks set to increase further in 2018.

This year we've seen a number of 'stepping-stone' attacks, where attackers compromise a company that is part of the supply-chain of another company, taking advantage of the fact that they can be easier to breach. This was one of the most notable features of June's ExPetr attack: the attackers specifically targeted a company supplying accounting software to Ukrainian companies. Most victims were located in Ukraine, but the attack had an impact on companies that operate worldwide. Among them were Maersk, the world's largest container ship and supply vessel company. The company indicated in its earnings report that it expected losses of between $200 and $300 as a result of 'significant business interruption' caused by the ExPetr attack. Another was FedEx, which revealed that the operations of its TNT Express unit in Europe were 'significantly affected' by the attack, costing the company around $300 in lost earnings.

The attackers behind ShadowPad, reported on in August adopted a similar approach, gaining access to the network of NetSarang, a vendor of popular server management software, in order to compromise some of its customers – including companies working in financial services, energy, retail, technology and media. The attackers modified one of the updates to include a backdoor designed to allow the attackers to download and execute arbitrary code, create processes and maintain a virtual file system in the registry, all of which are encrypted and stored in locations unique to each victim.

Another supply-chain attack occurred in September, when attackers compromised an update to the Windows clean-up utility CCleaner, published by Avast. They modified the installer for CCleaner 5.3 to drop malware on the computers of anyone who downloaded the utility. The malware, which was signed with a valid certificate, was active for a month and infected around 700,000 computers. The attackers used a two-stage infection process: the first delivered a profile of the victim to the attackers C&C servers, while the second was reserved for specific targets.

THE INTERNET OF HACKABLE THINGS

A year on from the Mirai botnet in 2016, the Hajime botnet was able to compromise 300,000 connected devices – just one of many campaigns focused on connected devices and systems.

These days we're surrounded by smart devices. This includes everyday household such as telephones, televisions, thermostats, refrigerators, baby monitors, fitness bracelets and children's toys. But it also includes cars, medical devices CCTV cameras and parking meters. Some homes are now designed with 'smartness' built-in. Ubiquitous Wi-Fi brings all these devices online, as part of the internet of things (IoT). These things are designed to make our lives easier. However, a world of connected everyday objects means a bigger attack surface for cybercriminals. Unless IoT devices are secured, the personal data they exchange can be compromised, they can be subject to an attack, or they can be used in an attack.

We saw this in October 2016 when the Mirai botnet was used to take down a portion of the Internet by hijacking connected home devices (such as DVRs, CCTV cameras and printers). In April this year, the attackers behind the Hajime botnet compromised more than 300,000 devices, although it has so far not been used for malicious purposes: it is possible that the attackers simply wanted to draw attention to the woeful lack of security in some connected devices. Researchers have highlighted plenty of instances of insecure connected IoT devices. Concerns about the risk of an attacker using the My Friend Cayla doll led the Federal Network Agency, the German telecommunications watchdog, to suggest that parents that had bought the doll should destroy it because of these worries. At the Security Analyst Summit, security expert Jonathan Andersson showed how a skilled attacker could create a device to hijack a drone in seconds. Hacking drones might seem a bit far-fetched, but the use of drones is no longer just a niche activity: last December, Amazon tested the use of drones to deliver parcels.

This isn't something confined to everyday objects that consumers use. Organizations that previously didn't need to think about cybersecurity now face cyberattacks. One example of this is the healthcare industry. Medical information that has traditionally existed in paper form is now to be found in databases, portals and medical equipment. The danger is that an attack on a connected hospital could result not only in the theft of patient data, but also the modification of diagnostic data – resulting in a patient being prescribed the wrong treatment or medication. Earlier this year we reported on the potential dangers and provided recommendations on securing medical facilities.

DATA LEAKS

2017 was the year of the Equifax data breach, among others, with millions of records exposed overall – the aftershocks could be felt for years.

Personal information is a valuable commodity, so it's no surprise that cybercriminals target online providers, looking for ways to obtain data that they can sell or use for future attacks on consumers or businesses. Once more we can look back on a year peppered with data leaks. These include Yahoo (strictly-speaking a report of a breach that occurred earlier, in 2013), Avanti Markets, Election Systems & Software, Dow Jones, America's Job Link Alliance and Equifax. The Uber data breach which took place in October 2016 and exposed the data of 57 million customers and drivers was only made public in November 2017.

Some of these attacks resulted in the theft of huge amounts of data. In most of them, the leaks were entirely preventable. The incidents at Election Systems & Software and Dow Jones (plus others that are not listed above) resulted from misconfiguration of Amazon Web Services buckets. In the case of the breach at America's Job Link Alliance, the hackers exploited a known vulnerability in a web application. The Equifax breach resulted from a vulnerability that Oracle had fixed several months before the attack, but the patch had not been applied.

CONCLUSION

2017 was a year many things turned out to be very different from what they initially seemed to be. Ransomware was a wiper; legitimate business software was a weapon; advanced threat actors made use of simple tools while attackers farther down the food chain got their hands on highly sophisticated ones. These shifting sands of the cyberthreat landscape represent a growing challenge for security defenders.

This is not just an issue for enterprise. As the growing number of supply chain attacks showed this year, any company can become a victim, particularly when in the crosshairs of a determined threat actor seeking to breach their customer base. There's no such thing as 100 per cent security, but there is much organizations and individuals can do to stay safe.

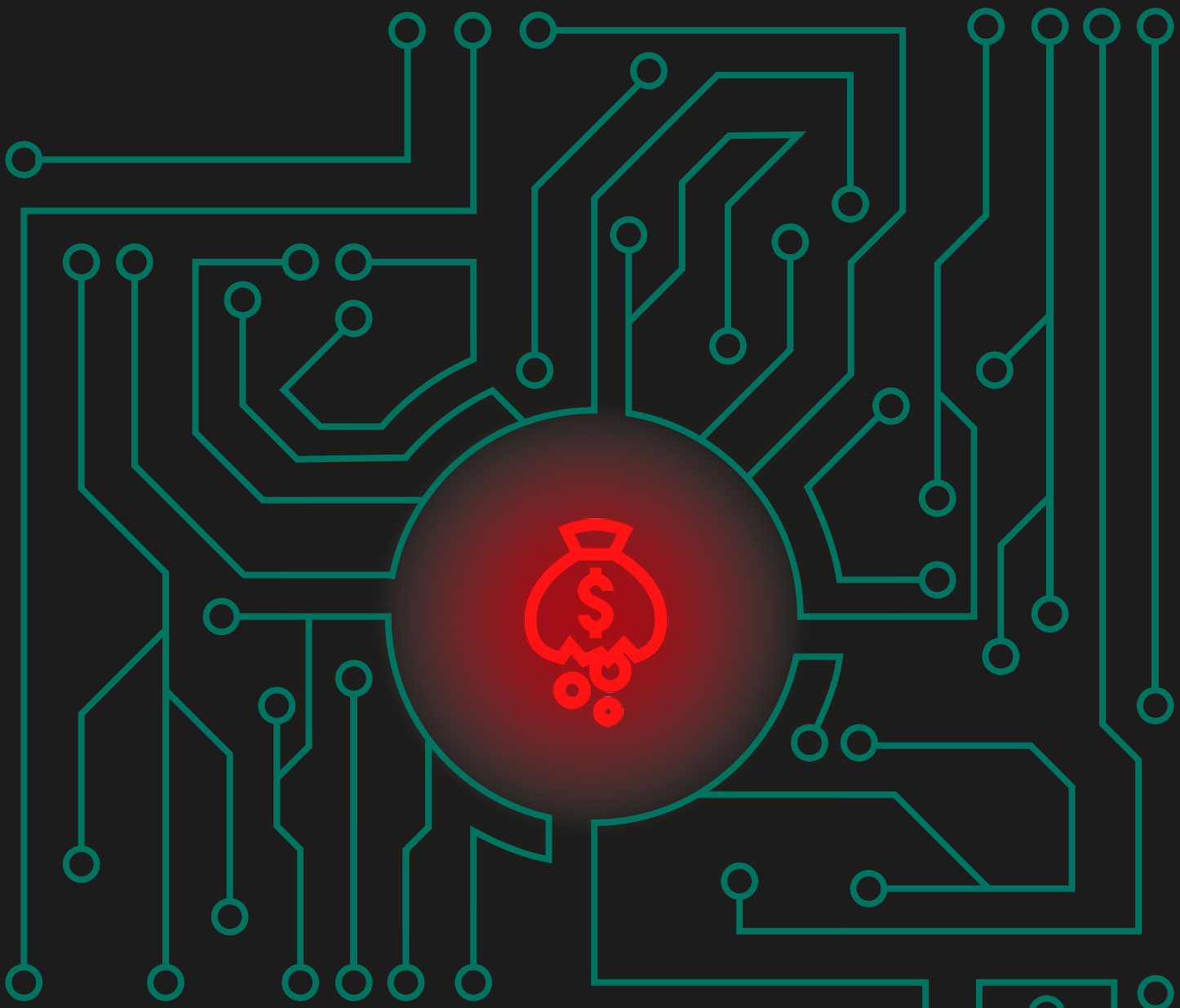
The best business defence against targeted attacks is a multi-layered approach that combines traditional anti-malware technologies with patch management, host intrusion detection, a default-deny whitelisting strategy and threat intelligence – regarding protection as an ongoing process to be supported with tools and expertise. Subscribing to our APT intelligence reports will provide access to our investigations and discoveries as they happen, including comprehensive technical data. Don't forget about 'patches' for human vulnerabilities. Social engineering remains a key entry point for cyberattackers, so it is important to educate and communicate with employees.

Any organisation that holds personal data has a duty of care to secure it effectively. Where a breach results in the theft of personal information, companies should alert their customers so they can take steps to limit any potential damage.

Last, but very definitely not least, never forget the power of security basics such as strong passwords, regular software updates and taking features offline that don't need to be connected. These will go a long way towards protecting any connected device, whether it's a home printer or critical hospital equipment.

2017 was a year of many lessons, particularly for business. In 2018 we shall discover if we have learned any of them.

For consumers, one of the main threats continued to be mobile malware. The following section considers the evolution of this threat over 2017.



MOBILE THREATS IN 2017

Roman Unuchek
Senior Malware Analyst

INTRODUCTION

For consumers, mobile malware is probably one of the most virulent threats, particularly for users of Android devices. In 2017, Trojanized apps were downloaded in their tens of thousands or more, resulting in victims being swamped with aggressive advertising or hit with ransomware or theft through SMS and WAP billing. Mobile malware added new tricks to avoid detection, bypass security and exploit new services. As in 2016, many such apps were readily available through reputable sources such as the Google Play Store.

Here's a roundup of the key mobile threats in 2017.

ROOTING MALWARE

For the last few years, rooting malware has been the biggest threat to Android users. Such Trojans are not only highly sophisticated, with lots of capabilities, they are also very popular. Their main goal is to show victims as many ads as possible and to silently install and launch promoted apps. In some cases, the popups and aggressive ad-showing can make the device essentially unusable.

This type of malware usually tries to get root rights by exploiting device vulnerabilities or using rights obtained in a previous infection. Root rights allow the Trojan to do almost everything, and it usually installs modules to gain persistence so that the malware can't be removed even after resetting the device to factory settings.

It is not unusual for rooting Trojans to be distributed from the Google Play Store: Dvmap (Trojan.AndroidOS.Dvmap.a) was installed from Google Play more than 50,000 times, injecting its malicious code into system libraries; and we detected almost 100 apps infected with the Ztorg Trojan uploaded onto Google Play, one of them installed more than one million times. These apps obtained root rights by exploiting old and well-known vulnerabilities on unpatched devices, after which they installed modules into system directories to become undeletable and to silently install apps.

Although the number of users attacked with rooting malware fell in 2017 compared to 2016, almost half (12) of the top 30 most popular Android Trojans this year were rooting ones, compared to 22 in 2016. We mainly associate the decreasing popularity of rooting Trojans with a declining use of older Android devices – as on modern smartphones and tablets such Trojans are unable to exploit vulnerabilities to get root rights.

However, it doesn't mean that the cybercriminals behind rooting Trojans have ceased their attacks. Some of them just gave up using root rights, but still aggressively show ads and download other apps. Moreover, it is still hard to remove such apps from the device because they can abuse system features.

We also discovered that the Ztorg Trojan started to explore new ways of getting money, for example, by attacking mobile payment systems. We found two apps with such malicious functionality – with tens of thousands of installations from Google Play Store between them. They were able to send Premium rate SMS and delete all incoming SMS, silently stealing money from the victim's mobile account. Furthermore, during our research we found that some of Ztorg's additional modules used a JS file so they could also steal money through clickjacking attacks on WAP-billing sites.

WAP-BILLING CLICKJACKING

They weren't the only ones targeting WAP-billing payment services. In 2017 we saw an increase in such malware. The functionality isn't new - Trojan-SMS.AndroidOS.Podec was attacking WAP-billing services back in 2015 - but we saw many new and popular Trojans in 2017. The number of users attacked was 2.4 times that seen in 2016.

Most of these Trojans receive URLs from their command centers. They can open the links or even visit them without the victim's knowledge, sometimes using special JS files to click on buttons in the web pages visited. These web pages could be advertising and essentially harmless for the victim (unless it involved malicious advertising like that spread by the Ztorg Trojans), but sometimes the pages contained WAP-billing, and we discovered some JS files created specially to click on pages with WAP-billing.

Usually, the mobile network operators use their own web pages to complete WAP payment transactions, but these Trojans can bypass those pages by clicking on 'agree' buttons. Another layer of security is SMS notifications about transactions, but this was bypassed too as most of the Trojans were capable of silently deleting incoming SMS.

BANKING MALWARE

Bank malware also introduced new features, and in 2017 we saw several new techniques used to steal money. Some of FakeToken's modifications attacked more than 2,000 financial apps. This Trojan overlays genuine apps with phishing windows to steal the user's credentials – and we found modifications of FakeToken that attacked apps for booking taxis, tickets and hotels and even one for paying traffic fines.

Usually, Android OS updates contain new security features, the main purpose of which is to protect users and prevent malware from doing harm. But malware always find a ways to bypass security features. In July 2017 we discovered that Svpeng (Trojan-Banker.AndroidOS.Svpeng.ae) could grant itself any permission by abusing accessibility services.

'Accessibility services' is a system feature that allows app developers to create apps for users with disabilities or those temporarily unable to interact fully with a device. However, the Trojan asked users to let it use accessibility services and then granted itself all needed permissions for sending SMS, reading contacts, making calls and more. Furthermore, the Trojan silently overlaid other apps and added itself to the device administrator list. It successfully prevented its uninstallation by clicking buttons in system dialogs. Using accessibility services also allowed this Trojan to steal entered data from apps' user interfaces and even to work as keylogger.

In August 2017, we found another modification of the Svpeng Trojan. This was also abusing accessibility rights, but its main purpose was to lock the device, encrypt the victim's files and demand money for unblocking and decrypting. This is not a new feature for mobile bankers, the FakeToken Trojan also has a modification with file encryption capabilities.

Overall, Svpeng (Trojan-Banker.AndroidOS.Svpeng.q) was the most popular mobile banking Trojan in 2017 even though the number of users attacked fell 1.5-fold, compared with 2016. Another popular Trojan in 2017 was Asacub (Trojan-Banker.AndroidOS.Asacub) distributed through SMS spam. There were three times as many Asacub modifications (12) among the top 30 mobile bankers in 2017, compared to just four in 2016.

RANSOMWARE RISE AND FALL

In the first half of 2017, we observed a huge rise in the number of mobile ransomware files: a 1.6-fold increase in installation packages compared to the whole of 2016. But, after June 2017, the number fell back to earlier levels. The vast majority (83%) of the mobile ransomware responsible for this surge belonged to the family known as Congur (Trojan-Ransom.AndroidOS.Congur). Most of them were pretty simple Trojans that asked for device administrator rights and then changed or set a new pin code for the device. They then showed a message in Chinese that asked the victim to contact them through QQ, a popular Chinese messenger service.

Mobile ransomware didn't change a lot in 2017; most of them still used the same techniques to block devices. We didn't see many examples of users attacked with mobile encryptors.

CONCLUSION

The more mobile devices are used, by more people, for more things, the more likely we are to see malware appear and evolve. It's a continuous race between the attackers, the device software developers and the security industry. But users don't need to become victims, there is much they can do to keep themselves, their devices and the data stored on them safe. This includes using reputable online stores and checking the developer behind an app before downloading it. The use of a reliable security solution, such as Kaspersky Mobile Antivirus: Web Security & Applock is also recommended.

KASPERSKY lab