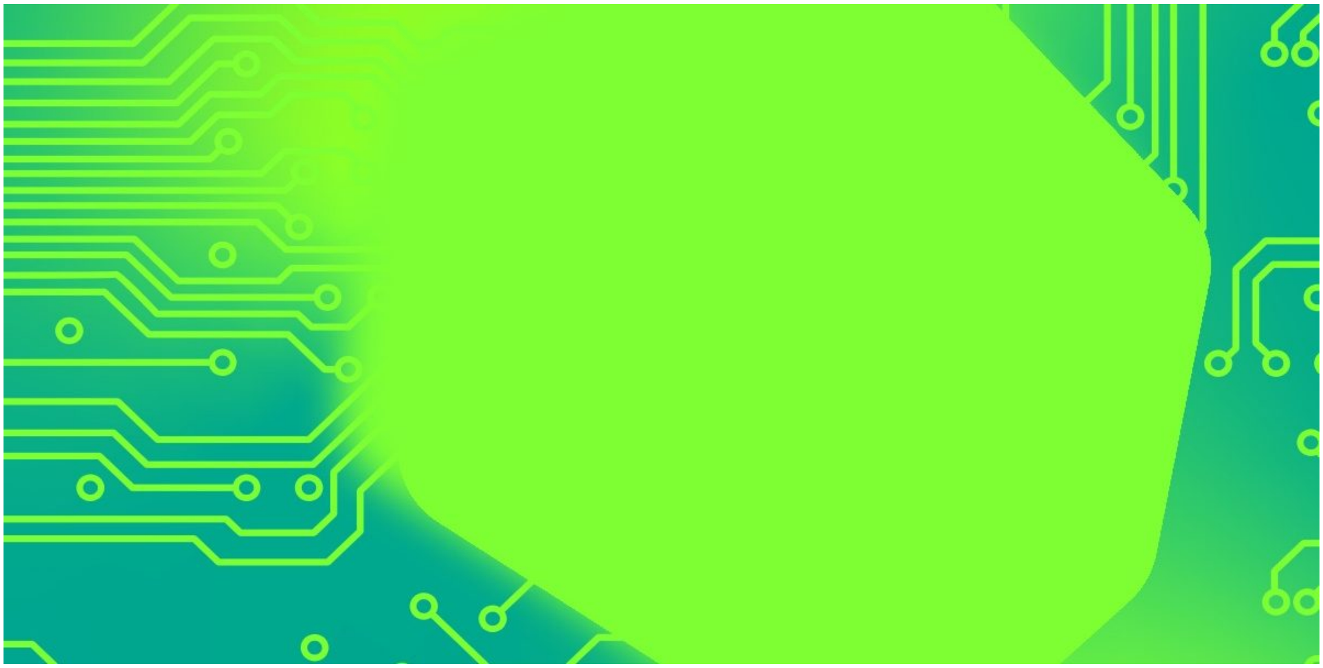
APT review: what the world’s threat actors got up to in 2019

securelist.com/ksb-2019-review-of-the-year/95394/



Authors

David Emm

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

- APT
- Mobile Malware
- Privacy
- Supply-chain attack
- Targeted attacks
- Vulnerabilities and exploits
- Zero-day vulnerabilities

Authors

David Emm

APT review: what the world’s threat actors got up to in 2019

Your email address will not be published. Required fields are marked *