APT trends report Q3 2019

By GReAT

Published: 2019-10-16 · Archived: 2026-04-05 14:09:21 UTC

For more than two years, the Global Research and Analysis Team (GReAT) at Kaspersky has been publishing quarterly summaries of advanced persistent threat (APT) activity. The summaries are based on our threat intelligence research and provide a representative snapshot of what we have published and discussed in greater detail in our private APT reports. They are designed to highlight the significant events and findings that we feel people should be aware of.

This is our latest installment, focusing on activities that we observed during Q3 2019.

Readers who would like to learn more about our intelligence reports or request more information on a specific report are encouraged to contact intelreports@kaspersky.com.

On August 30, Ian Beer from 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. Although the use of watering-hole attacks was popular in the early 2010s, it has now become less common. According to Google, a number of waterholed websites were delivering the exploits, possibly as far back as three years ago (based on September 2016 usage of the first exploit chain). While the blog contains no details about the compromised sites or if they are still active, it claims that these websites receive "thousands of visitors per week". The first stage Webkit exploit used to infect visitors makes no discrimination other than that the victim uses an iPhone and browses the website with Safari, although the vulnerability would also have worked in other browsers such as Chrome. The lack of victim discrimination would point to a relatively non-targeted attack, but the not-so-high estimate of the number of visitors to the waterholed sites seems to indicate that the attack was targeted at some communities: it is likely that these waterholed sites were all dedicated to some common topic. The blog does not contains many details regarding who the actor behind this attack is, but the high technical 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. Upon infection, the malware itself will be invisible to the victim. It pings its C2 every 60 seconds for new commands. It is able to get access to all kinds of files in the system, as well as tracking GPS position. There is no mechanism to survive a reboot, but the capability to steal signing-in cookies from a victim's account can keep providing the attackers with access to this data.

Shortly after the Google blogpost, Volexity published more details about the waterholing websites used in the attack to distribute the malware, pointing to a "strategic web compromise targeting Uyghurs". Citizen Lab published the Android counterpart for this story, stating that between November 2018 and May 2019, senior members of Tibetan groups were targeted by the same actor (this time dubbed POISON CARP by Citizen Lab) using malicious links in WhatsApp text exchanges, with the attackers posing as NGO workers, journalists and other fake personas. The links led to code designed to exploit web browser vulnerabilities to install spyware on iOS and Android devices, and in some cases to OAuth phishing pages.

At the beginning of September 2019, Zerodium, a zero-day brokerage firm, indicated that a zero-day for Android was now worth more than one for iOS: the exploit broker 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, a high-severity zero-day was found 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.

Russian-speaking activity

Turla (aka Venomous Bear, Uroburos and Waterbug) has made significant changes to its toolset. While investigating malicious activity in Central Asia, we identified a new backdoor that we attribute with medium confidence to this APT group. The malware, named Tunnus, is a.NET-based backdoor with the ability to run commands or perform file actions on an infected system and send the results to its C2. So far, the C2 infrastructure has been built using compromised sites with vulnerable WordPress installations. According to our telemetry, Tunnus activity started in March and was still active when we published our private report in July.

Turla has also wrapped its notorious JavaScript KopiLuwak malware in a dropper called Topinambour, a new.NET file that the group is using to distribute and drop KopiLuwak through infected installation packages for legitimate software programs such as VPNs. Some of the changes are to help Turla evade detection. For example, the C2 infrastructure uses IP addresses that appear to mimic ordinary LAN addresses. 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. Two KopiLuwak analogues – the.NET RocketMan Trojan and the PowerShell MiamiBeach Trojan – are used for cyber-espionage. We think that the threat actor deploys these versions where their targets are protected with security software capable of detecting KopiLuwak. All three implants can fingerprint targets, gather information on system and network adapters, steal files and download and execute additional malware. MiamiBeach is also able to take screenshots.

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.

Chinese-speaking activity

HoneyMyte (aka Temp.Hex and Mustang Panda), which has been active for several years, has adopted different techniques to perform its attacks over the past couple of years, and has focused on various targeting profiles. In previous attacks, conducted from mid-2018, this threat actor deployed PlugX implants, as well as multi-stage PowerShell scripts resembling CobaltStrike. That campaign targeted government entities in Myanmar, Mongolia, Ethiopia, Vietnam and Bangladesh. We recently described a new set of activities from HoneyMyte involving

attacks that relied on several types of tools. They include: (a) PlugX implants; (b) a multi-stage package resembling the CobaltStrike stager and stageless droppers with PowerShell and VB scripts,.NET executables, cookie-stealers and more; (c) ARP poisoning with DNS hijacking malware, to deliver poisoned Flash and Microsoft updates over http for lateral movement; (d) various system and network utilities. Based on the targeting of government organizations related to natural resource management in Myanmar and a major continental organization in Africa, we assess that one of the main motivations of HoneyMyte is gathering geo-political and economic intelligence. While a military organization was targeted in

Bangladesh, it's possible that the individual targets were related to geopolitical activity in the region.

Since the beginning of 2019, we have observed a spike in LuckyMouse activity, both in Central Asia and 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. LuckyMouse hasn't changed any of its TTPs (Tactics, Techniques and Procedures), continuing to rely on its own tools to get a foothold in the victim's network. The new campaigns consist of HTTPBrowser as a first stage, followed by the Soldier Trojan as a second-stage implant. The attackers made a change to their infrastructure, as they seem to solely rely on IPv4 addresses instead of domain names for their C2s, which can be seen as an attempt by them to limit correlation. The campaigns from this actor were still active at the time we published our latest private report on LuckyMouse in September.

Our January 2018 private report 'ShaggyPanther – Chinese-speaking cluster of activity in APAC' introduced ShaggyPanther, a previously unseen malware and intrusion set targeting Taiwan and Malaysia. Related components and activity span back over a decade, with similar code maintaining compilation timestamps as far back as 2004. Since then ShaggyPanther activity has been detected in several more locations: the most recent detections occurred on servers 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 SinoChoper/ChinaChopper, a commonly used webshell shared across multiple Chinese-speaking actors. SinoChopper is not only used to perform host identification and backdoor delivery but also email archive theft and additional activity. Though 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.

Middle East

On August 1, Dragos published an overview of attacks called 'Oil and Gas Threat Perspective Summary', which references an alleged new threat actor they call Hexane. According to the report, "HEXANE targets oil and gas and telecommunications in Africa, the Middle East, and Southwest Asia". Dragos claims to have identified the group in May 2019, associating it with OilRig and CHRYSENE. Although no IoCs have been made publicly available, some researchers have shared hashes in a Twitter thread in response to the Dragos announcement. Our analysis reveals some low-confidence similarities with OilRig based on TTPs, which is something that Dragos also mentions in its research. If this is indeed the case, the recent leaks from Lab Dookhtegan and GreenLeakers offer several hypotheses about this group's emergence. Due to exposure and leaks, OilRig may simply have changed its toolset and continued to operate as usual: this would imply a quick and flexible response to the leaks

from this actor. Or perhaps some of the OilRig TTPs were adopted by a new group that seems to have similar interests. Hexane's activity appears to have started around September 2018 with a second wave of activity starting in May 2019. In all cases, the artefacts used in the attacks are relatively unsophisticated. The constant evolution of the droppers seems to indicate a trial-and-error period where attackers were testing how best to evade detection. The TTPs we can link to previous OilRig activity include the described trial-and-error process, the use of simplistic unsophisticated droppers distributed through spear phishing and DNS-based C2 exfiltration.

TortoiseShell is a new cluster of activities associated with an unknown APT actor, revealed by Symantec on September 18, 2019. Symantec claims that the first signs of activity were seen in July 2018, and are still active one year later; Kaspersky has seen different TortoiseShell artifacts dating back to January 2018. To date, all registered attacks, according to our telemetry, are in Saudi Arabia. Symantec's report also confirms that the majority of the infections they found were in the same location. The attackers deploy their Syskit backdoor and then use it for reconnaissance. Other tools deployed on the victim machines are designed to collect files and pack them using RAR, gathering further system information. In one case, the attackers deployed the TightVNC remote administration tool to obtain full access to a machine. Symantec mentions traces of OilRig tools in some of the victims, something which we cannot confirm. Also, they mention in their blogpost the possibility that this was distributed through a supply chain attack. We were able to see the malware being distributed through a fake application distributed from a specifically created website for war veterans around two months before the publication of our report. The website was activated shortly after we published our report during a national holiday period in Saudi Arabia. However, we didn't find any compromised application that could suggest a supply chain attack.

Southeast Asia and the Korean Peninsula

Recently we discovered new Android malware disguised as a mobile messenger or as cryptocurrency-related applications. The new malware has several connections with KONNI, a Windows malware strain that has been used in the past to target a human rights organization and an individual/organization with an interest in Korean Peninsula affairs. KONNI has also previously targeted cryptocurrencies. The infected apps don't steal cryptocurrencies from a specific trading application or switch wallet addresses; they implement full-featured functionalities to control an infected Android device and steal personal cryptocurrency using these features. We worked closely with a local CERT in order to take down the attacker's server, giving us a chance to investigate it.

We recently tracked new BlueNoroff activity. In particular, we identified a bank in Myanmar that was compromised by this actor and promptly contacted it to share the IoCs we had found. This 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.

Kaspersky observed a recent campaign utilizing a piece of malware referred to by FireEye as DADJOKE. This malware was first used in the wild in January 2019 and has undergone constant development since then. We have only observed this malware being 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 was conducted on August 29 and seems to have targeted only a select few individuals working for a military organization.

The Andariel APT group, considered to be a sub-group of Lazarus, was initially described by the South Korean Financial Security Institute (FSI) in 2017. This threat actor has traditionally focused on geopolitical espionage and financial intelligence in South Korea. We have released several private intelligence reports on the group. We recently 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. Thanks to the quick response of the South Korean CERT, this signature was soon revoked. The malware is a brand new type of backdoor, called ApolloZeus, 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. Indeed, we believe this attack is an early preparation stage for a new campaign, which also points to the attacker's intentions to replace their malware framework with the newly discovered artifacts.

Other interesting discoveries

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, 44 entries are listed in sigs.py, many of them related to unknown APTs that have not yet been publicly described. In 2018, 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 activity 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.

Since the beginning of 2019, we have observed the operation of new RCS (Remote Control System) implants for Android. RCS uses watermarks for different customers, which allowed us to correlate post-leak activity in the wild to obtain a global picture of how this malware is still being used, including the most recent cases. We detected RCS being used in Ethiopia in February, while additional samples with the same watermark were also detected in Morocco. The deployment method used depends on the actor, but the most common method consists of sending a legitimate backdoored application with RCS directly to the target using IM services (Telegram and WhatsApp).

Final thoughts

In seeking to evade detection, threat actors are refreshing their toolsets. This quarter, we have seen this clearly in Turla's development of its Tunnus backdoor and Topinambour dropper.

However, when a new campaign is observed, it's not always immediately clear whether the tools used are the result of an established threat actor revamping its tools or a completely new threat actor making use of the tools developed by an existing APT group. In the case of Hexane, for example, it's unclear if this is a new development by OilRig, or the use of OilRig TTPs by a new group with similar interests in the Middle East, Africa and Southwest Asia.

Korean-focused APT campaigns continue to dominate activities in Southeast Asia, a trend we first noted in our Q2 report.

Despite the lower payouts by Zerodium for iOS exploits relative to those for Android, it's clear that mobile exploits continue to fetch very high prices. Our research into the ongoing use of RCS implants for Android and the revelations about the use of multiple iOS zero-days as described by Google and Citizen Lab underline the fact that mobile platforms have now become a standard aspect of APT attacks.

As always, we would note that our reports are the product of our visibility into the threat landscape. However, it needs to be borne in mind that, while we strive to continually improve, there is always the possibility that other sophisticated attacks may fly under our radar.
