APT trends report Q1 2019

SL **securelist.com**/apt-trends-report-q1-2019/90643

By GReAT

For just under two years, the Global Research and Analysis Team (GReAT) at Kaspersky Lab 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 aim 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 Q1 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'.

The most remarkable finding

Targeting supply-chains has proved very successful for attackers in recent years – ShadowPad, CCleaner and ExPetr are good examples. In our threat predictions for 2019, we flagged this as a likely continuing attack vector; and we didn't have to wait very long to see this prediction come true. In January, we discovered a sophisticated supply-chain attack involving the ASUS Live Update Utility, the mechanism used to deliver BIOS, UEFI and software updates to ASUS 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 were found to have 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.

Russian-speaking activity

Russian-speaking groups were not especially active during the first part of the year, with no noteworthy technical or operational changes. However, they continued their non-stop activity in terms of spreading, with a special interest in political activity.

This was apparent in an attack focused on the Ukraine elections. The attack surfaced after we discovered a malicious Word document targeting a German political advisory organization. This organization, according to its website, "advises political decision-makers on international politics and foreign and security policy". Our technical analysis of the attack suggests that the Sofacy or Hades groups are behind it, though we're unable to say for sure which of these groups is responsible.

Such political interests are not new. Recently, a court in Virginia gave Microsoft control of a group of websites that were intended to look like login sites for a Washington think tank, but are believed to be part of the infrastructure of a “Russian group suspected in the DNC hack”.

Additionally, Microsoft revealed that a “Russian nation-state hacking group” targeted political organizations engaged in the 2019 European Parliament elections scheduled for the end of May.

On the technical side, since mid-January we have been tracking an active Turla campaign targeting government bodies in Turkmenistan and Tajikistan. This time the actor delivered its known KopiLuwak JavaScript using new .NET malware, called “Topinambour” (aka Sunchoke) by its developers. The Topinambour dropper is delivered along with legitimate software and consists of a tiny .NET shell that waits for Windows shell commands from operators. Interestingly, in this campaign the attackers used different artefacts implemented in JavaScript, .NET and PowerShell – all of them with similar functionality.

We also published details on how Zebrocy has added the “Go” language to its arsenal – the first time that we have observed a well-known APT threat actor deploy malware with this compiled, open source language. Zebrocy continues to target government-related organizations in Central Asia, both in-country and in remote locations, as well as a new diplomatic target in the Middle East.

Finally, during February 2019 we observed a highly targeted attack in Crimea using a previously unknown malware. The spy program was spread by email and masqueraded as the VPN-client of a well-known Russian security company that, among other things, provides solutions to protect networks. At this point we can’t relate this activity to any known actor.

Chinese-speaking activity

Recent APT trend summaries included analyses of new Chinese-speaking threat actors as well as the resurgence of old activity sets. This has continued into 2019.

In the early months of 2019, Chinese-speaking actors were the most active, with a traditional interest in targeting different countries in South East Asia. A recent indictment of two Chinese nationals by the US Department of Justice on charges of computer hacking, conspiracy to commit wire fraud and aggravated identity theft, alleged that they were members of the APT10 group, carrying out illegal activity on behalf of the Chinese Ministry of State Security.

Similarly, CactusPete (aka LoneRanger, Karma Panda, and Tonto Team), is reported to have targeted South Korean, Japanese, US, and Taiwanese organizations in the 2012 – 2014 timeframe. The actor has quite likely relied on much the same codebase and implant variants for the past six years. However these have broadened substantially since 2018. The group spear-phishes its targets, deploys Word and Equation Editor exploits and an appropriated/repackaged DarkHotel VBScript zero-day, delivers modified and compiled unique Mimikatz variants, GSEC and WCE credential stealers, a keylogger, various Escalation of Privilege exploits, various older utilities and an updated set of backdoors, and what appear to be new variants of custom downloader and backdoor modules.

We have been monitoring a campaign targeting Vietnamese government and diplomatic entities abroad since at least April 2018. We attribute the campaign, which we call "SpoiledLegacy", to the LuckyMouse APT group (aka EmissaryPanda and APT27). The operators use penetration testing frameworks such as Cobalt Strike and Metasploit. While we believe that they exploit network services vulnerabilities as their main initial infection vector, we have also seen spear-phishing messages containing decoy documents. We believe that, as in a previous LuckyMouse campaign internal database servers are among the targets. For the last stage of their attack they use different in-memory 32- and 64-bit Trojans injected into system process memory. It is worth highlighting that all the tools in the infection chain dynamically obfuscate Win32 API calls using leaked HackingTeam code.

FireEye defined APT40 as the Chinese state-sponsored threat actor previously reported as TEMP.Periscope, Leviathan and TEMP.Jumper. According to FireEye, the group has conducted operations in support of China's naval modernisation effort since at least 2013, specifically targeting engineering, transportation and defence industries, especially where these sectors overlap with maritime technologies. Recently, FireEye also observed specific targeting of countries strategically important to the "Belt and Road" Initiative, including Cambodia, Belgium, Germany, Hong Kong, the Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States and the United Kingdom.

Interestingly, the use of newer ANEL versions by APT10, targeting Japan, allowed us to find similarities between this malware and Emdivi, malware previously used by BlueTermite. This suggests a potential connection between both actors.

South East Asia and Korean peninsula

Once again, this seems to be the most active region of the world in terms of APT activity.

In January, we identified new activity by the Transparent Tribe APT group (aka PROJECTM and MYTHIC LEOPARD), a threat actor with interests aligned with Pakistan that has shown a persistent focus on Indian military targets.

In February, we identified a campaign targeting military organizations, this time in India. We are currently unable to attribute this campaign to any known threat actor. The attackers rely on watering-holes and spear-phishing to infect their victims. Specifically, they were able to compromise a website belonging to a think tank related to warfare studies, using it to host a malicious document that distributed 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 time period.

OceanLotus was another actor active during this period, using a new downloader called KerrDown, as reported by Palo Alto. The actor was discovered at the beginning of the year using freshly-compiled samples in a new wave of attacks. ESET recently uncovered a new addition to this actor's toolset targeting Mac OS.

In mid-2018, our report on "Operation AppleJeus" highlighted the focus of the Lazarus threat actor on cryptocurrency exchanges. In this operation, the group used a fake company with a backdoored product aimed at cryptocurrency businesses. One of the key findings was the group's new ability to target Mac OS. Since then, Lazarus has expanded its operations for this platform. Further tracking of the group's activities has enabled us to discover a new operation, active since at least November 2018, which utilizes PowerShell to control Windows systems and Mac OS malware to target Apple customers. Lazarus isn't the only APT group targeting cryptocurrency exchanges. The Kimsuky group has also extended its activities to include individuals and companies in this sector, mainly in South Korea.

Finally, at the start of the year, the South Asian Bitter group used a new simple downloader (called ArtraDownloader by Palo Alto) that delivers the BitterRat Trojan to target organizations in Saudi Arabia and Pakistan.

Middle East

Surprisingly, during the first months of the year activity in the Middle East has, apparently, been less intense than in the past. Even so, it was the target of several groups already discussed, such as Chafer and Bitter.

We also observed some activity from Gaza Team and MuddyWater. Still, this can be considered part of their continued targeting of the region, showing nothing new in terms of operational or technical improvements.

Other interesting discoveries

Late in 2018 we observed a new version of the FinSpy iOS implant in the wild. This is part of FinSpy Mobile, a product provided by the surveillance solutions developer, Gamma Group. FinSpy for iOS implements extensive spyware features that allow someone to track almost everything on infected devices, including keypresses, messages and calls. A big limitation is that the current version can only be installed on jailbroken devices. We believe that Gamma Group does not provide an exploit tool to jailbreak victims' phones, but it provides advice and support to customers on how to do the jailbreaking themselves. Our telemetry shows implant traces in Indonesia and Mongolia. However, due to the large number of Gamma customers, this is probably only a fraction of the victims.

Following this research, we discovered a new version for Android also dated circa June 2018. While it is quite similar in terms of functionality, it implements unique capabilities specific to the platform such as obtaining root privileges by abusing the DirtyCow exploit (CVE-2016-5195). Just like the iOS version, this implant has features to exfiltrate data from Instant Messengers including Threema, Signal, Whatsapp and Telegram, as well as internal device information including, but not limited to, emails and SMS messages.

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 have recently discovered using our technologies. Further analysis led us to uncover a zero-day vulnerability in “win32k.sys”. We reported this to Microsoft on 22 February. The company confirmed the vulnerability and assigned it CVE-2019-0797. Microsoft released a patch on 12 March 2019, crediting Kaspersky Lab researchers Vasiliy Berdnikov and Boris Larin with the discovery. We believe that this exploit is being used by several threat actors – including, but possibly not limited to, FruityArmor and SandCat. FruityArmor is known to have used zero-days before, while SandCat is a new APT actor that we discovered only recently. The exploit found in the wild was targeting 64-bit operating systems in the Windows 8 to Windows 10 build 15063 range.

FrutiyArmor and SandCat, interestingly, 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 with such artefacts.

Ransomware has become an interesting tool for APT actors, as it can be used to delete traces, conduct cyber-sabotage, or as a powerful distraction. There is an interesting wave of ransomware attacks that we have been following, as they seem to be mainly interested in big targets. LockerGoga recently compromised the systems of Altran, Norsk Hydro and other companies. It’s unclear who’s behind the attacks, what they want and the mechanism used to first infect its victims. It’s not even clear if LockerGoga is ransomware or a wiper. The malware encrypts data and displays a ransom asking victims to get in touch to arrange decryption, in return for an (unspecified) payment in bitcoins. However, later versions were observed by researchers that forcibly log victims off infected systems by changing their passwords and removing their ability to log back into the system. In such cases, the victims may not even get to see the ransom note.

Final thoughts

Looking back at what has happened during the first months of the year is always a surprising experience for us. Even when we have the feeling that “nothing groundbreaking” has occurred, we always uncover a threat landscape that is full of many interesting stories and evolution on different fronts.

If we are to provide a few general highlights, we can conclude that:

- Geopolitics keeps gaining weight as the main driver of APT activity
- South East Asia is still the most active region of the world in terms of APT activity, but probably this is also related to the “noise” that some of the less experienced groups make
- Russian-speaking groups keep a low profile in comparison with recent years: maybe this is part of internal restructuring, but this is just a hypothesis
- Chinese-speaking actors maintain a high level of activity, combining low and high sophistication depending on the campaign
- Providers of “commercial” malware available for governments and other entities seem to be doing well, with more customers

If we are to highlight one thing from the whole period, in our opinion operation ShadowHammer combines several factors that define the current status of APT activity. This is an advanced and targeted campaign using the supply-chain for distribution on an incredibly wide scale. It involves several steps in a combined operation, including the initial collection of MAC addresses for their targets. This seems to be a new trend, as the actor also targeted other victims for malware distribution, showing how worrisome and difficult it is to fight supply-chain attacks.

As always, this is only our visibility. We always have to keep in mind other sophisticated attacks that happen under our radar, but we continue to try and improve, to uncover every single one of them.