APT trends report Q1 2020

By GReAT

Published: 2020-04-30 · Archived: 2026-04-02 10:44:28 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 Q1 2020.

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'.

Given the exceptional situation the world is living in because of the COVID-19 pandemia, it is mandatory we to start with a summary of how APT groups have been abusing this topic for different types of attacks.

COVID-19 APT activity

Since the World Health Organization (WHO) declared the COVID-19 a pandemic, this topic has received increased attention from different attackers. Many of the phishing scams we've seen have been launched by cybercriminals trying to cash-in on people's fears about the virus. However, the list of attackers also includes APT threat actors such as Kimsuky, APT27, Lazarus or ViciousPanda who, according to OSINT, have used COVID-19-themed lures to target their victims. We recently discovered a suspicious infrastructure that could have been used to target health and humanitarian organizations, including the WHO. Even though the infrastructure cannot be attributed to any particular actor at the moment, and was registered before the COVID-19 crisis in June 2019, according to some private sources it might be related to the DarkHotel actor. However, we cannot confirm this information at the moment. Interestingly, some groups have used the current situation to try to soften their reputation by declaring that they would not target health organizations during the crisis.

There are different publications reporting activity related to other APT actors using this lure, but in general, we do not believe this implies a meaningful change in terms of TTPs other than using a trendy topic for luring victims. We are closely monitoring the situation.

In January 2020, we discovered a watering-hole utilizing a full remote iOS exploit chain. This site appears to have been designed to target users in Hong Kong, based on the content of the landing page. While the exploits currently being used are known, the actor responsible is actively modifying the exploit kit to target more iOS versions and devices. We observed the latest modifications on February 7. The project is broader than we initially thought, supporting an Android implant, and probably supporting implants for Windows, Linux, and MacOS. For the time being, we are calling this APT group TwoSail Junk. We believe this is a Chinese-speaking group; it maintains infrastructure mostly within Hong Kong, along with a couple of hosts located in Singapore and Shanghai. TwoSail

Junk directs visitors to its exploit site by posting links within the threads of forum discussions, or creating new topic threads ofrtheir own. To date, dozens of visits were recorded from within Hong Kong, with a couple from Macau. The technical details around the functionality of the iOS implant, called LightSpy, and related infrastructure, reveal a low-to-mid capable actor. However, the iOS implant is a modular and exhaustively functional iOS surveillance framework.

Russian-speaking activity

In January, a couple of recently compiled SPLM/XAgent modules were detected in an Eastern European telecoms company. The initial point of entry is unknown, as is their lateral movement within this organization. It has become rare to identify SPLM infections, compared to past levels of Sofacy activity, so it seems that portions of this network may have been infected for some time. In addition to these SPLM modules, Sofacy also deployed .NET XTUNNEL variants and their loaders. These 20KB XTUNNEL samples themselves seem minimal in comparison to past XTUNNEL samples, which weighed in at 1-2MB. This shift to C# by the long-standing Sofacy XTunnel codebase reminds us of Zebrocy's practice of re-coding and innovating long-used modules in multiple languages.

Gamaredon, a well-known APT group that has been active since at least 2013, has traditionally focused on Ukrainian entities. In recent months we have observed a campaign, made up of different waves, that has also been reported by multiple researchers on different social networks. The attackers sent malicious documents with remote template injection, resulting in a multi-level infection scheme to deploy a malicious loader that periodically contacts a remote C2 to download additional samples. Based on past research, we know that the Gamaredon's toolkit includes many different malware artefacts, developed to achieve different goals. These include scanning drives for specific system files, capturing screenshots, executing remote commands, downloading additional files and managing the remote machine with programs such as UltraVNC. In this case, we observed an interesting new second stage payload that includes spreading capabilities, that we call "Aversome infector". This malware seems to have been developed to maintain a strong persistence in the target network and to move laterally by infecting Microsoft Word and Excel documents on external drives.

Chinese-speaking activity

CactusPete is a Chinese-speaking cyber-espionage group active since at least 2012 characterized by medium-level technical capabilities. Historically, this threat actor has targeted organizations within a limited range of countries – South Korea, Japan, the US and Taiwan. At the end of 2019 the group seemed to shift towards a heavier focus on Mongolian and Russian organizations. CactusPete offensive activity against the Russian defense industry and Mongolian government appears to be mostly delineated from its Russian-Mongolian commercial and border relationships. However, one bait exploit document dropping its Flapjack backdoor (tmplogon.exe, primarily focused on new Russian targets) is authored in Mongolian. The group's broadening of techniques, exploit re-purposing, targeting shift and possible expansion suggests changes in the group's resources and operations.

Rancor is a group that has been publicly reported since 2018, with connections to DragonOK. This actor traditionally had a focus on Southeast Asian targets, namely Cambodia, Vietnam and Singapore. We noted several updates to the group's activity in the last few months, namely the discovery of a new variant of the Dudell malware that we are calling ExDudell, a new tool for bypassing UAC (User Account Control), and new

infrastructure utilized in the attacks. Apart from this, we have also identified that the initial lure documents that were previously sent via mail, are now found in the Telegram Desktop directory, suggesting the group is possibly making a shift in its initial delivery method.

In 2019, we detected activity by an unknown actor at the time deploying watering holes on websites representing Tibetan interests, fooling victims into installing fake Adobe Flash updates hosted on a GitHub repository. Kaspersky thwarted the attack by coordinating a takedown of this repository with GitHub. After a brief period of inactivity, we detected a new round of watering holes featuring a renewed toolset. We decided to call the group behind this activity Holy Water.

The threat actor's unsophisticated but creative toolset has been evolving a lot since the inception date, may still be in development, and leverages Sojson obfuscation, NSIS installer, Python, open-source code, GitHub distribution, Go language, as well as Google Drive-based C2 channels.

Middle East

We recently detected a new, ongoing data exfiltration campaign targeting victims in Turkey that started in February 2020. While StrongPity's TTPs in terms of targeting, infrastructure and infection vector haven't changed, we observed a somewhat peculiar change in the documents they attempt to exfiltrate. In this campaign, StrongPity updated its latest signature backdoor, named StrongPity2, and added more files to exfiltrate to its list of common Office and PDF documents, including Dagesh Pro Word Processor files used for Hebrew dotting, RiverCAD files used for river flow and bridge modelling, plain-text files, archives as well as GPG encrypted files and PGP keys.

In March, we discovered a targeted campaign to distribute Milum, a Trojan designed to gain remote control of devices in target organizations, some of which operate in the industrial sector. The first signs of this operation, which we have dubbed WildPressure, can be traced back to August 2019; still, the campaign remains active. The Milum samples we have seen so far do not share any code similarities with any known APT campaigns. The malware provides attackers with remote control over infected devices, allows downloading and executing commands, collecting and exfiltrating information and installing upgrades in the malware.

In late December 2019, Kaspersky Threat Attribution Engine detected a new variant of the Zerocleare wiper that had possibly been used in targeted attacks on energy sector targets in Saudi Arabia. This quarter, we identified a new variant of this wiper, called Dustman. It is similar to Zerocleare in terms of wiping and distribution, but changes in variables and technical names suggest this might have been in readiness for a new wave of attacks specifically targeting Saudi Arabia's energy sector, based on messages embedded in the malware and the mutex created by it. The PDB file of the Dustman wiper suggested that this destructive code was the release edition and was ready for deployment in a target network. These changes coincided with the New Year holidays, during which many employees take time off to celebrate. Shamoon was delivered with similar timing in 2012 during Ramadan celebrations.

Southeast Asia and Korean Peninsula

A Lazarus campaign outlined by the Italian security company Telsy in November 2019 allowed us to find a connection to previous activity from the group targeting cryptocurrency businesses. The malware mentioned on Telsy's blog is a first stage downloader that has been observed since mid-2018. We found that the second stage malware is a variant of Manuscrypt, uniquely attributed to Lazarus, deploying two types of payloads. The first is a manipulated Ultra VNC program, and the second is a multi-stage backdoor. This type of multi-stage infection procedure is typical of the Lazarus group's malware, especially when using the Manuscrypt variant. In this campaign, our telemetry indicates that the Lazarus group attacked cryptocurrency businesses in Cyprus, the US, Taiwan and Hong Kong, and the campaign extended until the beginning of 2020.

Kimsuky, an actor we have been tracking since 2013, was especially active during 2019. In December, Microsoft took down 50 domains used by the group and filed a lawsuit against the attackers in a Virginia court. However, the group has continued its activity without significant changes. We recently discovered a new campaign where the actor used a decoy image themed around New Year's greetings that delivers its old downloader with a new evolved next-stage payload designed to steal information that uses a new encryption method.

At the end of January, we stumbled upon a malicious script exploiting an Internet Explorer vulnerability, CVE-2019-1367. After closely examining the payload and finding connections with previous activity, we concluded that DarkHotel was behind this campaign, probably in progress since 2018. The campaign saw DarkHotel utilize a multi-stage binary infection phase using home-brewed malware. The initial infection creates a downloader which fetches another downloader to collect system information and fetch the final backdoor only for high-value victims. DarkHotel used a unique combination of TTPs in this campaign. The threat actor used diverse infrastructure to host malware and to control infected victims, including a compromised web server, a commercial hosting service, a free hosting service and a free source code tracking system. We were able to confirm targeted companies in South Korea and Japan in this campaign.

In March, researchers from Google revealed that a group of hackers used five zero-days to target North Koreans and North Korean-focused professionals in 2019. The group exploited flaws in Internet Explorer, Chrome, and Windows with phishing emails that carried malicious attachments or links to malicious sites, as well as watering-hole attacks. We were able to match two of the vulnerabilities – one in IE and one in Windows – to DarkHotel.

FunnyDream is a campaign that started in mid-2018, targeting high-profile entities in Malaysia, Taiwan and the Philippines, with the majority of victims in Vietnam. Our analysis revealed that it's part of a wider campaign that stretches back a few years and targets governments, and specifically foreign organizations, of countries in Southeast Asia. The attacker's backdoor downloads and uploads files from/to a C2, executes commands and runs new processes in the victim. It also collects information about other hosts on the network and is delivered to new hosts through remote execution utilities. The attacker also used an RTL backdoor and Chinoxy backdoor. The C2 infrastructure has been active since mid-2018 and domains show an overlap with the FFRAT malware family. In a number of cases, indications suggest the backdoor was delivered via a previous long-term compromise. The campaign is still active.

Operation AppleJeus was one of the more notable campaigns of Lazarus, and the first time the actor targeted macOS targets. Our January follow-up research revealed significant changes to the group's attack methodology: homemade macOS malware and an authentication mechanism to carefully deliver the next-stage payload, as well as loading the next-stage payload without touching the disk. To attack Windows victims, the group has elaborated

a multi-stage infection procedure and significantly changed the final payload. We believe that Lazarus has been more careful in its attacks since the release of Operation AppleJeus and has employed a number of methods to avoid detection. We identified several victims in the UK, Poland, Russia and China. Moreover, we were able to confirm that several of the victims are linked to cryptocurrency organizations.

Roaming Mantis is a financially motivated actor first reported in 2017, when it used SMS to distribute its malware to Android devices based in South Korea. Since then, the scope of the group's activities has widened considerably, supporting 27 languages, targeting iOS as well as Android, and even mining cryptocurrency. The actor also added new malware families, including Fakecop and Wroba.j to its arsenal, and is still active using 'SMiShing' for Android malware distribution. In a recent campaign it distributed malicious APKs masquerading as popular couriers and customized for the targeted countries, including Japan, Taiwan, South Korea and Russia.

Other interesting discoveries

TransparentTribe started using a new module named USBWorm at the beginning of 2019, as well as improving its custom .NET tool named CrimsonRAT. Based on our telemetry, USBWorm was used to infect thousands of victims, most of them located in Afghanistan and India, providing the attacker with the ability to download and execute arbitrary files, spread to removable devices and steal files of interest from infected hosts even those disconnected from the internet. As we previously reported, this group mainly focuses on military targets, which are usually compromised with Office documents armed with malicious VBA and open-source malware like Peppy RAT and CrimsonRAT. In its new campaign, which is still active, we noticed the group's focus shift more towards targeting entities located in Afghanistan in addition to India. Transparent Tribe has also developed a new implant designed to infect Android devices, a modified version of the AhMyth Android RAT which is open source malware available on GitHub.

During the last months of 2019, we observed an ongoing campaign conducted by Fishing Elephant. The group continues to use both Heroku and Dropbox in order to deliver its tool of choice, AresRAT. We discovered that the actor incorporated a new technique into its operations that is meant to hinder manual and automatic analysis – geo-fencing and hiding executables within certificate files. During our research, we also detected a change in victimology that may reflect the current interests of the threat actor: the group is targeting government and diplomatic entities in Turkey, Pakistan, Bangladesh, Ukraine and China.

Final thoughts

While the threat landscape isn't always full of "groundbreaking" events, when we cast our eyes back over the activities of APT threat actors, there are always interesting developments. Our regular quarterly reviews are intended to highlight the key developments.

These are some of the main trends that we've seen this year so far.

- It's clear from the activities of various APT groups, including CactusPete, LightSpy, Rancor, Holy Water, TwoSail Junk and others that geo-politics continues to be an important driver of APT activity. This was also underlined this quarter by the UK National Cyber Security Centre laying responsibility for disruptive attacks on Georgia at the feet of Russia's military intelligence service, indictments in the US of two

Chinese nationals for laundering $100 million in cryptocurrency on behalf of North Korea and the alleged 'catfishing' of IDF soldiers by Hamas.

- Financial gain remains a motive for some threat actors, as evidenced by the activities of Lazarus and Roaming Mantis.
- Southeast Asia is the most active region in terms of APT activities, including established actors such as Lazarus, DarkHotel and Kimsuky, and newer groups such as Cloud Snooper and Fishing Elephant.
- APT threat actors such as CactusPete, TwoSail Junk, FunnyDream, DarkHotel continue to exploit software vulnerabilities.
- APT threat actors continue to include mobile implants in their arsenal.
- APT threat actors such as (but not limited to) Kimsuky, Hades and DarkHotel, as well as opportunistic criminals, are exploiting the COVID-19 pandemic.

All in all, we see the continuous growth of activity in Asia and how some of the actors we called newcomers are now well established. On the other hand, the more traditional advanced actors seem to be more and more selective in their operations, probably following a change of paradigm. The use of mobile platforms for infections and the distribution of malware is on the rise. Every actor seems to have some artefacts for these platforms and in some campaigns they are the main target.

COVID-19 is clearly top of everyone's minds at the moment and APT threat actors have also been seeking to exploit this topic in spear-phishing campaigns. We do not believe this represents a meaningful change in terms of TTPs: they're simply using it as a newsworthy topic to lure their victims. However, we are closely monitoring the situation.

As always, we would note that our reports are the product of our visibility into the threat landscape. However, it should 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.
