APT trends report Q3 2020

By GReAT

Published: 2020-11-03 · Archived: 2026-04-05 19:07:00 UTC

For more than three 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 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.

We have already partly documented the activities of DeathStalker, a unique threat group that seems to focus mainly on law firms and companies operating in the financial sector. The group's interest in gathering sensitive business information leads us to believe that DeathStalker is a group of mercenaries offering hacking-for-hire services, or acting as an information broker in financial circles. The activities of this threat actor first came to our attention through a PowerShell-based implant called Powersing. This quarter, we unraveled the threads of DeathStalker's LNK-based Powersing intrusion workflow. While there is nothing groundbreaking in the whole toolset, we believe defenders can gain a lot of value by understanding the underpinnings of a modern, albeit low-tech, infection chain used by a successful threat actor. DeathStalker continues to develop and use this implant, using tactics that have mostly been identical since 2018, while making greater efforts to evade detection. In August, our public report of DeathStalker's activities summarized the three scripting language-based toolchains used by the group – Powersing, Janicab and Evilnum.

Following our initial private report on Evilnum, we detected a new batch of implants in late June 2020, showing interesting changes in the (so far) quite static modus operandi of DeathStalker. For instance, the malware directly connects to a C2 server using an embedded IP address or domain name, as opposed to previous variants where it made use of at least two dead drop resolvers (DDRs) or web services, such as forums and code sharing platforms, to fetch the real C2 IP address or domain. Interestingly, for this campaign the attackers didn't limit themselves merely to sending spear-phishing emails but actively engaged victims through multiple emails, persuading them to open the decoy, to increase the chance of compromise. Furthermore, aside from using Python-based implants throughout the intrusion cycle, in both new and old variants, this was the first time that we had seen the actor dropping PE binaries as intermediate stages to load Evilnum, while using advanced techniques to evade and bypass security products.

We also found another intricate, low-tech implant that we attribute to DeathStalker with medium confidence. The delivery workflow uses a Microsoft Word document and drops a previously unknown PowerShell implant that relies on DNS over HTTPS (DoH) as a C2 channel. We dubbed this implant PowerPepper.

During a recent investigation of a targeted campaign, we found a UEFI firmware image containing rogue components that drop previously unknown malware to disk. Our analysis showed that the revealed firmware modules were based on a known bootkit named Vector-EDK, and the dropped malware is a downloader for further components. By pivoting on unique traits of the malware, we uncovered a range of similar samples from our telemetry that have been used against diplomatic targets since 2017 and have different infection vectors. While the business logic of most is identical, we could see that some had additional features or differed in implementation. Due to this, we infer that the bulk of samples originate from a bigger framework that we have dubbed MosaicRegressor. Code artefacts in some of the framework's components, and overlaps in C2 infrastructure used during the campaign, suggest that a Chinese-speaking actor is behind these attacks, possibly one that has connections to groups using the Winnti backdoor. The targets, diplomatic institutions and NGOs in Asia, Europe and Africa, all appear to be connected in some way to North Korea.

Europe

Since publishing our initial report on WellMess (see our *APT trends report Q2 2020*), the UK National Cyber Security Centre (NCSC) has released a joint technical advisory, along with Canadian and US governments, on the most recent activity involving WellMess. Specifically, all three governments attribute the use of this malware targeting COVID-19 vaccine research to The Dukes (aka APT29 and Cozy Bear). The advisory also details two other pieces of malware, SOREFANG and WellMail, that were used during this activity. Given the direct public statement on attribution, new details provided in the advisory, as well as new information discovered since our initial investigation, we published our report to serve as a supplement to our previous reporting on this threat actor. While the publication of the NCSC advisory has increased general public awareness on the malware used in these recent attacks, the attribution statements made by all three governments provided no clear evidence for other researchers to pivot on for confirmation. For this reason, we are currently unable to modify our original statement; and we still assess that the WellMess activity has been conducted by a previously unknown threat actor. We will continue to monitor for new activity and adjust this statement in the future if new evidence is uncovered.

Russian-speaking activity

In summer, we uncovered a previously unknown multimodule C++ toolset used in highly targeted industrial espionage attacks dating back to 2018. So far, we have seen no similarities with known malicious activity regarding code, infrastructure or TTPs. To date, we consider this toolset and the actor behind it to be new. The malware authors named the toolset MT3, and based on this abbreviation we have named the toolset MontysThree. The malware is configured to search for specific document types, including those stored on removable media. It contains natural language artefacts of correct Russian and a configuration that seek directories that exist only in Cyrilic version of Windows, while presenting some false flag artefacts suggesting a Chinese-speaking origin. The malware uses legitimate cloud services such as Google, Microsoft and Dropbox for C2 communications.

Chinese-speaking activity

Earlier this year, we discovered an active and previously unknown stealthy implant dubbed Moriya in the networks of regional inter-governmental organizations in Asia and Africa. This tool was used to control public facing servers in those organizations by establishing a covert channel with a C2 server and passing shell

commands and their outputs to the C2. This capability is facilitated using a Windows kernel mode driver. Use of the tool is part of an ongoing campaign that we have named TunnelSnake. The rootkit was detected on the targeted machines in May, with activity dating back as early as November 2019, persisting in networks for several months following the initial infection. We found another tool showing significant code overlaps with this rootkit, suggesting that the developers have been active since at least 2018. Since neither rootkit nor other lateral movement tools that accompanied it during the campaign relied on hard-coded C2 servers, we could gain only partial visibility into the attacker's infrastructure. That said, the bulk of detected tools, apart from Moriya, consisted of both proprietary and well-known pieces of malware that were previously used by Chinese-speaking threat actors, giving a clue to the attacker's origin.

PlugX continues to be effectively and heavily used across Southeast and East Asia, and also Africa, with some minimal use in Europe. The PlugX codebase has been in use by multiple Chinese-speaking APT groups, including HoneyMyte, Cycldek and LuckyMouse. Government agencies, NGOs and IT service organizations seem to be consistent targets. While the new USB spreading capability is opportunistically pushing the malware throughout networks, compromised MSSPs/IT service organizations appear to be a potential vector of targeted delivery, with CobaltStrike installer packages pushed to multiple systems for initial PlugX installation. Based on our visibility, the majority of activity in the last quarter appears to be in Mongolia, Vietnam and Myanmar. The number of systems in these countries dealing with PlugX in 2020 is at the very least in the thousands.

We discovered an ongoing campaign, dating back to May, utilizing a new version of the Okrum backdoor, attributed to Ke3chang. This updated version of Okrum uses an Authenticode-signed Windows Defender binary using a unique side-loading technique. The attackers used steganography to conceal the main payload in the Defender executable while keeping its digital signature valid, reducing the chance of detection. We haven't previously seen this method being used in the wild for malicious purposes. We have observed one affected victim, a telecoms company located in Europe.

On September 16, the US Department of Justice released three indictments associated with hackers allegedly connected with APT41 and other intrusion sets tracked as Barium, Winnti, Wicked Panda and Wicked Spider. In addition, two Malaysian nationals were also arrested on September 14, in Sitiawan (Malaysia), for "conspiring to profit from computer intrusions targeting the video game industry", following cooperation between the US DoJ and the Malaysian government, including the Attorney General's Chambers of Malaysia and the Royal Malaysia Police. The first indictment alleges that the defendants set up an elite "white hat" network security company, called Chengdu 404 Network Technology Co, Ltd. (aka Chengdu Si Lingsi Network Technology Co., Ltd.), and under its guise, engaged in computer intrusions targeting hundreds of companies around the world. According to the indictment, they "carried out their hacking using specialized malware, such as malware that cyber-security experts named 'PlugX/Fast', 'Winnti/Pasteboy', 'Shadowpad', 'Barlaiy/Poison Plug' and 'Crosswalk/ProxIP'". The indictments contain several indirect IoCs, which allowed us to connect these intrusions to Operation ShadowPad and Operation ShadowHammer, two massive supply-chain attacks discovered and investigated by Kaspersky in recent years.

Middle East

In June, we observed new activity by the MuddyWater APT group, involving use of a new set of tools that constitute a multistage framework for loading malware modules. Some components of the framework leverage

code to communicate with C2s identical to code we observed in the MoriAgent malware earlier this year. For this reason, we decided to dub the new framework MementoMori. The purpose of the new framework is to facilitate execution of further in-memory PowerShell or DLL modules. We detected high-profile victims based in Turkey, Egypt and Azerbaijan.

Southeast Asia and Korean Peninsula

In May, we found new samples belonging to the Dtrack family. The first sample, named Valefor, is an updated version of the Dtrack RAT containing a new feature enabling the attacker to execute more types of payload. The second sample is a keylogger called Camio which is an updated version of its keylogger. This new version updates the logged information and its storage mechanism. We observed signs indicating that these malware programs were tailored for specific victims. At the time of our research our telemetry revealed victims located in Japan.

We have been tracking LODEINFO, fileless malware used in targeted attacks since last December. During this time, we observed several versions as the authors were developing the malware. In May, we detected version v0.3.6 targeting diplomatic organizations located in Japan. Shortly after that, we detected v0.3.8 as well. Our investigation revealed how the attackers operate during the lateral movement stage: after obtaining the desired data, the attackers wipe their traces. Our private report included a technical analysis of the LODEINFO malware and the attack sequence in the victim's network, to disclose the actor's tactics and methods.

While tracking Transparent Tribe activity, we discovered an interesting tool used by this APT threat actor: the server component used to manage CrimsonRAT bots. We found different versions of this software, allowing us to look at the malware from the perspective of the attackers. It shows that the main purpose of this tool is file stealing, given its functionalities for exploring the remote file system and collecting files using specific filters. Transparent Tribe (aka PROJECTM and MYTHIC LEOPARD) is a very prolific APT group that has increased its activities in recent months. We reported the launch of a new wide-ranging campaign that uses the CrimsonRAT tool where we were able to set up and analyze the server component and saw the use of the USBWorm component for the first time; we also found an Android implant used to target military personnel in India. This discovery also confirms much of the information already discovered during previous investigations; and it also confirms that CrimsonRAT is still under active development.

In April, we discovered a new malware strain that we named CRAT, based on the build path and internal file name. The malware was spread using a weaponized Hangul document as well as a Trojanized application and strategic web compromise. Since its discovery the full-featured backdoor has quickly evolved, diversifying into several components. A downloader delivers CRAT to profile victims, followed by next-stage orchestrator malware named SecondCrat: this orchestrator loads various plugins for espionage, including keylogging, screen capturing and clipboard stealing. During our investigation, we found several weak connections with ScarCruft and Lazarus: we discovered that several debugging messages inside the malware have similar patterns to ScarCruft malware, as well as some code patterns and the naming of the Lazarus C2 infrastructure.

In June, we observed a new set of malicious Android downloaders which, according to our telemetry, have been actively used in the wild since at least December 2019; and have been used in a campaign targeting victims almost exclusively in Pakistan. Its authors used the Kotlin programming language and Firebase messaging system for the downloader, which mimics Chat Lite, Kashmir News Service and other legitimate regional Android applications.

A report by the National Telecom & Information Technology Security Board (NTISB) from January describes malware sharing the same C2s and spoofing the same legitimate apps. According to this publication, targets were Pakistani military bodies, and the attackers used WhatsApp messages, SMS, emails and social media as the initial infection vectors. Our own telemetry shows that this malware also spreads through Telegram messenger. The analysis of the initial set of downloaders allowed us to find an additional set of Trojans that we believe are strongly related, as they use the package name mentioned in the downloaders and focus on the same targets. These new samples have strong code similarity with artefacts previously attributed to Origami Elephant.

In mid-July, we observed a Southeast Asian government organization targeted by an unknown threat actor with a malicious ZIP package containing a multilayered malicious RAR executable package. In one of the incidents, the package was themed around COVID-19 containment. We believe that the same organization was probably the same target of a government web server watering-hole, compromised in early July and serving a highly similar malicious LNK. Much like other campaigns against particular countries that we have seen in the past, these adversaries are taking a long-term, multipronged approach to compromising target systems without utilizing zero-day exploits. Notably, another group (probably OceanLotus) used a similar Telegram delivery technique with its malware implants against the same government targets within a month or so of the COVID-19-themed malicious LNK, in addition to its use of Cobalt Strike.

In May 2020, Kaspersky technologies prevented an attack using a malicious script for Internet Explorer against a South Korean company. Closer analysis revealed that the attack used a previously unknown full chain that consisted of two zero-day exploits: a Remote Code Execution exploit for Internet Explorer and an Elevation of Privilege exploit for Windows. Unlike a previous full chain that we discovered, used in Operation WizardOpium (you can read more here and here), the new full chain targeted the latest builds of Windows 10, and our tests demonstrated reliable exploitation of Internet Explorer 11 and Windows 10 build 18363 x64. On June 8, we reported our discoveries to Microsoft, who confirmed the vulnerabilities. At the time of our report, the security team at Microsoft had already prepared a patch for vulnerability CVE-2020-0986 that was used in the zero-day Elevation of Privilege exploit; but before our discovery, the exploitability of this vulnerability had been considered less likely. The patch for CVE-2020-0986 was released on June 9. Microsoft assigned CVE-2020-1380 to a use-after-free vulnerability in JScript and the patch for this was released on August 11. We are calling this and related attacks Operation PowerFall. Currently, we are unable to establish a definitive link with any known threat actor, but due to similarities with previously discovered exploits we believe that DarkHotel may be behind this attack.

On July 22, we came across a suspicious archive file that was uploaded to VirusTotal from an Italian source. The file seemed to be a triage consisting of malicious scripts, access logs, malicious document files and several screenshots related to suspicious file detections from security solutions. After looking into these malicious document files, we identified that they are related to a Lazarus group campaign that we reported in June. This campaign, dubbed DeathNote, targeted the automobile industry and individuals in the academic field using lure documents containing aerospace and defense-related job descriptions. We are confident that these documents are related to a recently reported attack on an Israeli defense company. We have uncovered webshell scripts, C2 server scripts and malicious documents, identified several victims connected to the compromised C2 server, as well as uncovering the method used to access the C2 server.

We have observed an ongoing Sidewinder campaign that started in February, using five different malware types. The group made changes to its final payloads and continues to target government, diplomatic and military entities

using current themes, such as COVID-19, in its spear-phishing efforts. While the infection mechanism remains the same as before, including the group's exploit of choice (CVE-2017-1182) and use of the DotNetToJScript tool to deploy the final payloads, we found that the actor also used ZIP archives containing a Microsoft compiled HTML Help file to download the last-stage payload. In addition to the existing .NET-based implant, which we call SystemApp, the threat actor added JS Orchestrator, the Rover/Scout backdoor and modified versions of AsyncRAT, warzoneRAT to its arsenal.

Other interesting discoveries

Attribution is difficult at the best of times, and sometimes it's not possible at all. While investigating an ongoing campaign, we discovered a new Android implant undergoing development, with no clear link to any previously known Android malware. The malware is able to monitor and steal call logs, SMS, audio, video and non-media files, as well as identifying information about the infected device. It also implements an interesting feature to collect information on network routes and topology obtained using the "traceroute" command as well as using local ARP caches. During this investigation we uncovered a cluster of similar Android infostealer implants, with one example being obfuscated. We also found older Android malware that more closely resembles a backdoor, with traces of it in the wild dating back to August 2019.

In April, Cisco Talos described the activities of an unknown actor targeting Azerbaijan's government and energy sector using new malware called PoetRAT. In collaboration with Kaspersky ICS CERT, we identified supplementary samples of associated malware and documents with broader targeting of multiple universities, government and industrial organizations as well as entities in the energy sector in Azerbaijan. The campaign started in early November 2019; and the attackers switched off the infrastructure immediately following publication of the Cisco Talos report. We observed a small overlap in victimology with Turla, but since there is no technically sound proof of relation between them, and we haven't been able to attribute this new set of activity to any other previously known actor, we named it Obsidian Gargoyle.

Final thoughts

The TTPs of some threat actors remain fairly consistent over time (such as using hot topics such (COVID-19) to entice users to download and execute malicious attachments sent in spear-phishing emails), while other groups reinvent themselves, developing new toolsets and widening their scope of activities, for example, to include new platforms. And while some threat actors develop very sophisticated tools, for example, MosiacRegressor UEFI implant, others have great success with basic TTPs. Our regular quarterly reviews are intended to highlight the key developments of APT groups.

Here are the main trends that we've seen in Q3 2020:

- Geo-politics continues to drive the development of many APT campaigns, as seen in recent months in the activities of Transparent Tribe, Sidewinder, Origami Elephant and MosaicRegressor, and in the 'naming and shaming' of various threat actors by the NCSC and the US Department of Justice.
- Organizations in the financial sector also continue to attract attention: the activities of the mercenary group DeathStalker is a recent example.

- We continue to observe the use of mobile implants in APT attacks with recent examples including Transparent Tribe and Origami Elephant.
- While APT threat actors remain active across the globe, recent hotspots of activity have been Southeast Asia, the Middle East and various regions affected by the activities of Chinese-speaking APT groups.
- Unsurprisingly, we continue to see COVID-19-themed attacks – this quarter they included WellMess and Sidewinder.
- Among the most interesting APT campaigns this quarter were DeathStalker and MosaicRegressor: the former underlining the fact that APT groups can achieve their aims without developing highly sophisticated tools; the latter representing the leading-edge in malware development.

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.
