APT annual review: What the world's threat actors got up to in 2020

By GReAT

Published: 2020-12-03 · Archived: 2026-04-05 13:14:37 UTC

We track the ongoing activities of more than 900 advanced threat actors; you can find our quarterly overviews here, here and here. Here we try to focus on what we consider to be the most interesting trends and developments of the last 12 months. This is based on our visibility in the threat landscape; and it's important to note that no single vendor has complete visibility into the activities of all threat actors.

Beyond Windows

While Windows continues to be the main focus for APT threat actors, we have observed a number of non-Windows developments this year. Last year we reported a malware framework called MATA that we attribute to Lazarus. This framework included several components such as a loader, orchestrator and plug-ins. In April, we learned that MATA extended beyond Windows and Linux to include macOS. The malware developers Trojanized an open-source two-factor authentication application and utilized another open-source application template. The MATA framework was not the only way that Lazarus targeted macOS. We found a cluster of activity linked to Operation AppleJeus. We also discovered malware similar to the macOS malware used in a campaign that we call TangDaiwbo – a multi-platform cryptocurrency exchange campaign. Lazarus utilizes macro-embedded Office documents and spreads PowerShell or macOS malware, depending on the victim's system.

Kaspersky has publicly documented the Penquin family, tracing it back to its Unix ancestors in the Moonlight Maze operation of the 1990s. When researchers at Leonardo published a report in May about Penquin_x64, a previously undocumented variant of Turla's Penquin GNU/Linux backdoor, we followed up on this latest research by generating network probes that detect Penquin_x64-infected hosts at scale, allowing us to discover that tens of internet hosting servers in Europe and the US are still compromised today. We think it's possible that, following public disclosure of Turla's GNU/Linux tools, the Turla threat actor may have been repurposing Penquin to conduct operations other than traditional intelligence.

In our 2020 Q3 APT trends report we described a campaign we dubbed TunnelSnake. By analyzing the activity in this campaign, we were able to uncover the network discovery and lateral movement toolset used by the threat actor after deploying the Moriya rootkit. We saw that the actor also made use of the open-source tools Earthworm and Termite, capable of spawning a remote shell and tunneling traffic between hosts. These tools are capable of operating on multiple architectures widely used by IoT devices, demonstrating a readiness to pivot to such devices.

Infecting UEFI firmware

During an 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 was 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 that have different infection vectors. While the business logic of most of them is identical, we saw that some had additional features or differed in their implementation. Because of this, we infer that the bulk of samples originate from a bigger framework, which we dubbed MosaicRegressor. The targets, diplomatic entities and NGOs in Asia, Europe and Africa, all appear to be connected in some way to North Korea.

Mobile implants

The use of mobile implants by APT threat actors is no longer a novelty: this year we have observed various groups targeting mobile platforms.

In January, we discovered a watering hole utilizing a full remote iOS exploit chain. The 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 implants for Windows, Linux and macOS. We have named 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 of their 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.

In August, we published the second of our reports on the recent activities of the Transparent Tribe threat actor. This included an Android implant used by the group to spy on mobile devices. One of the methods used to distribute the app was by disguising it as the Aarogya Setu COVID-19 tracking app developed by the government of India. The fake app was used to target military personnel in India; and, based on public information, may have been distributed by sending a malicious link via WhatsApp, SMS, email or social media.

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. The authors spread the malware by mimicking 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 the publication, the 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.

Big game hunting

In April, we released an early warning about the VHD ransomware, which was first spotted in late March. This ransomware stood out because of its self-replication method. The use of a spreading utility compiled with victim-specific credentials was reminiscent of APT campaigns, but at the time we were unable to link the attack to an existing group. However, we were able to identify an incident in which the VHD ransomware was deployed, in close conjunction with known Lazarus tools, against businesses in France and Asia. This indicates that Lazarus is behind the VHD ransomware campaigns that have been documented so far. As far as we know, this is the first time it has been established that the Lazarus group has resorted to targeted ransomware attacks (known as "big game hunting") for financial gain.

Continued use of 'naming and shaming'

Some years ago, we predicted that governments would resort to the "court of public opinion" as a strategy to draw attention to the activities of hostile APT groups; and this trend has developed further in the last year or so.

In February, the US Department of Justice (DoJ) charged four Chinese military officers with computer fraud, economic espionage and wire fraud for hacking into the credit reporting agency Equifax in 2017. The following month, the DoJ charged two Chinese nationals with laundering more than $100 million in cryptocurrency on behalf of North Korea. The indictment alleged that the two men laundered cryptocurrency stolen by North Korean hackers between December 2017 and April 2019, helping to hide the stolen currency from police.

In May, the UK National Cyber Security Centre (NCSC) and the US Department of Homeland Security (DHS) issued a joint advisory warning that both countries are investigating a number of incidents in which other nation states are targeting pharmaceutical companies, medical research organizations and universities, looking for intelligence and sensitive data, including research on COVID-19. The FBI and CISA (Cybersecurity and Infrastructure Security Agency) also issued a warning that threat actors related to the People's Republic of China have been targeting US organizations engaged in COVID-19-related research.

On July 30, the European Council announced that it was imposing sanctions against six individuals and three entities that it believes are responsible for, or involved in, various cyberattacks, including the attempted attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) and the WannaCry, NotPetya and Operation Cloud Hopper attacks. The sanctions include a travel ban and asset freeze. In addition, EU persons and entities are forbidden from making funds available to those listed.

In September, the US DoJ released three indictments associated with hackers allegedly connected with APT41 and other intrusions 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 Government of Malaysia, including the Attorney General's Chambers of Malaysia and the Royal Malaysia Police. The indictments contain several indirect IoCs, which allowed us to connect these intrusions to Operation ShadowPad and Operation ShadowHammer, two massive supply-chain attacks that we discovered and investigated.

In October, the US DoJ indicted six Russian military intelligence officers for a number of cyberattacks, including NotPetya, the Olympic Destroyer attacks on the 2018 Winter Olympics and attacks affecting France, Georgia, the Netherlands, Ukraine and the investigation into the 2018 Novichok poisonings in the UK. The UK NCSC also accused Russia's GRU military intelligence service of attacks on officials and organizations involved in the 2020 Tokyo games, prior to their postponement.

'Good enough' is enough

The malware developed by APT threat actors doesn't always need to be technically sophisticated in order to be effective. The activities of DeathStalker illustrates this. This is a unique threat actor 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. The group continues to develop and use this implant, employing 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 chances 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 used since Q2 2020 that we attribute with high confidence to DeathStalker. 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. In October 2020, we identified new samples of DeathStalker's PowerPepper toolset, containing improvements that included improved sandbox detection techniques. The group also leveraged a new infection chain to deliver PowerPepper.

DeathStalker offers a good example of what small groups or even skilled individuals can achieve, without the need for innovative tricks or sophisticated methods. DeathStalker should serve as a baseline of what organizations in the private sector should be able to defend against, since groups of this sort represent the type of cyberthreat that companies today are most likely to face. We advise defenders to pay close attention to any process creation related to native Windows interpreters for scripting languages, such as powershell.exe and cscript.exe: wherever possible, these utilities should be made unavailable. Security awareness training and security product assessments should also include infection chains based on LNK files.

Exploiting COVID-19

In the wake of the COVID-19 pandemic, and the lockdowns imposed by many countries in response, attackers of all kinds sought to capitalize on people's fears about the disease. Most of the phishing scams related to COVID-19 have been launched by cybercriminals using the disease as a springboard to make money. However, the list of attackers also includes APT threat actors such as Lazarus, Sidewinder, Transparent Tribe, GroupA21, which we observed using COVID-19-themed lures to target their victims, as well as Kimsuky, APT27, IronHusky and ViciousPanda who did the same, according to OSINT (open source intelligence). In March, we discovered a suspicious infrastructure that could have been used to target health and humanitarian organizations, including the WHO. We weren't able to firmly attribute this to any specific actor, and it was registered before the COVID-19 crisis. Some private sources suggested it might be related to DarkHotel.

A few months later, there were a series of attacks on supercomputing centers around Europe, including the UK-based ARCHER, the German-based bwHPC and the Swiss National Supercomputing Centre. The EGI Computer Security and Incident Response Team (EGI-CSIRT) also published an alert in May covering two incidents that, according to its report, may or may not be related. Although we weren't able to establish with a high degree of certainty that the ARCHER hack and the incidents described by EGI-CSIRT are related, we suspect they might be. Some media speculated that all these attacks might be related to COVID-19 research being carried out at the supercomputing centers.

Following publication of our initial report on WellMess (see our APT trends report Q2 2020), the UK National Cyber Security Centre (NCSC) released a joint advisory, along with the 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). While the publication of the NCSC advisory 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 still assess that the WellMess activity has been conducted by a previously unknown threat actor.

We do not believe that the interest of APT threat actors in COVID-19 represents a meaningful change in terms of TTPs (Tactics Techniques and Procedures): they're simply using it as a newsworthy topic to lure their victims.

Final thoughts

We will continue to track the activities of APT threat actors and will regularly highlight the most interesting findings. However, if you wish to learn more about what the world's most sophisticated threat groups get up to, please reach out to us at intelreports@kaspersky.com.
