APT trends report Q2 2020

securelist.com/apt-trends-report-q2-2020/97937

Authors

Expert GReAT

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 Q2 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'.

The most remarkable findings

On May 11, the UK-based supercomputing center, ARCHER, announced that it would shut down access to its network while it investigated a security incident. The website stated that the "ARCHER facility is based around a Cray XC30 supercomputer (with 4920 nodes) that provides the central computational resource". At the same time, the German-based bwHPC also announced a security incident and decided to restrict access to its resources. The Swiss National Supercomputing Centre, at the time involved in a project to study the small membrane protein of the coronavirus, confirmed that it, and other European high-performance computer facilities, had been attacked and that it had temporarily closed. On May 15, the EGI Computer Security and Incident Response Team (EGI-CSIRT) published an alert covering two incidents that, according to its report, may or may not be related. Both incidents describe the targeting of academic data centers for "CPU mining purposes". The alert includes a number of IoCs, which complement other OSINT (open-source intelligence) observations. Although we weren't able to establish with a high degree of certitude 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.

Interestingly, last July 16th 2020, NCSC published an advisory describing malicious activity targeting institutions related to research to find a vaccine for COVID-19. In this case, the malware used in the attacks belongs to a family called WellMess, as originally described by LAC Co back in 2018. Until recently, this malware was not believed to be related to any APT activity. Surprisingly, NCSC attributes this activity to the APT-29 threat actor. However, it does not provide any public proof.

From our own research, we can confirm that WellMess's activity seems to follow a cycle, being used in campaigns every three months or so since its discovery. We observed a peak of activity in fall of 2019, followed by an increase in the number of C2s in February 2020. We also observed high-profile targeting, including telcos, government and contractors in MENA and the EU. However, from our side we cannot confirm attribution or targeting of health institutions at the moment.

For more details about WellMess, you can check our presentation from GReAT ideas here: https://youtu.be/xeTYLRCwnFo

Russian-speaking activity

In May, researchers at Leonardo published a report about "Penquin_x64", a previously undocumented variant of Turla's Penquin GNU/Linux backdoor. Kaspersky has publicly documented the Penquin family, tracing it back to its Unix ancestors in the Moonlight Maze operation of the 1990s. 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

hoster's 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 June, we discovered two different domain names, "emro-who[.]in" and "emro-who[.]org", typo-squatting the World Health Organization (WHO) Regional Office for the Eastern Mediterranean (EMRO). These domains, registered on June 21 using the Njalla.no registrar, seem to be used as sender domains for a spear-phishing campaign. This type of typo-squatting is reminiscent of Sofacy campaigns against other international organizations. Moreover, we have seen Njalla.no recently used to register SPLM and XTUNNEL C2 (command-and-control) servers and we have seen this autonomous system used by Sofacy in the past for a SPLM C2.

Hades is an elusive, highly dynamic threat actor that commonly engages in tailored hacking and special access operations, such as the OlympicDestroyer attack or the ExPetr (aka NotPetya) and Badrabbit attacks. On May 28, the US National Security Agency (NSA) published an alert detailing the use by Hades of an Exim vulnerability (CVE-2019-10149) for what appears to be a potentially large hacking operation designed for mass access. Our own report expanded on the scripts used in this operation, as well as providing other IoCs that we discovered.

Chinese-speaking activity

In late 2019, and again in March this year, we described ongoing malicious activities from a previously unknown threat actor that we named Holy Water. Holy Water notably leveraged a Go language and Google Drive-command-driven implant that we dubbed Godlike12. Following the publication of our report, and notifications to relevant incident response organizations, new Holy Water samples were submitted to VirusTotal. The newly discovered samples include Telegram-controlled and open-source-based Python implants that were probably deployed on the victim's networks after a successful intrusion.

In March, one of our YARA rules from previous research on ShadowPad attacks detected a recently compiled executable file uploaded to VirusTotal. Later we found a few other samples from our own telemetry. ShadowPad is a modular attack platform consisting of a root module and various plugin modules responsible for diverse functionalities. ShadowPad was first discovered by Kaspersky in 2017. In August of that year, one of our customers detected suspicious network activities. After thorough investigation, we found a legitimate software module that had been compromised and backdoored by an advanced threat actor in a sophisticated software supply-chain attack. We notified the software vendor and also published the outcome of our investigations in a technical white paper. Since then, ShadowPad malware has been deployed in a number of major cyberattacks, with a different subset of plugins used in different attack cases: the CCleaner incident in 2017 and the ShadowHammer attacks in 2018 are the major examples of such attacks.

When analyzing new samples from ShadowPad malware, compiled and used in attacks since late 2019, our investigation revealed a strong connection between these recent ShadowPad malware samples and the CactusPete threat actor. CactusPete started deploying ShadowPad malware to a few victims at the beginning of 2019 through its HighProof backdoor. However, since late 2019, ShadowPad has been commonly used in CactusPete attacks.

This quarter, we described another CactusPete attack campaign which started in December 2019 In this campaign, the CactusPete threat actor used a new method to drop an updated version of the DoubleT backdoor onto the computers. The attackers implanted a new dropper module in the Microsoft Word Startup directory, most likely through a malicious document. This malicious dropper is responsible for dropping and executing a new version of the DoubleT backdoor, which utilizes a new method of encrypting the C2 server address.

While analysing compromised machines in Central Asia, we revealed an additional infection that was unrelated to the initial subject of our investigation. This led us to detect previously unknown malware that we dubbed B&W, which provides an attacker with the capabilities to remotely control a victim's machine. Further analysis of the samples, infrastructure and other related artefacts allowed us to conclude, with medium confidence, that the newly found malware is related to the SixLittleMonkeys APT. This group is known to have been active for several years, targeting government entities in Central Asia.

HoneyMyte is an APT threat actor that we have been tracking for several years. In February, our fellow researchers at Avira blogged about HoneyMyte PlugX variants that they had recently observed targeting Hong Kong. PlugX has been used by multiple APT groups over the past decade, especially shared among Chinese-speaking threat actors, and has changed in many ways. Avira´s post covers the PlugX loader and backdoor payload, including its USB capabilities. In May, we published an update on this threat actor, specifically providing timely indicators to aid in threat hunting for some of the PlugX variants found in the wild between January and May this year.

In May, we discovered a watering hole on the website of a Southeast Asian top official. This watering hole, set up in March, seemed to leverage allowlisting and social engineering techniques to infect its targets. The final payload was a simple ZIP archive containing a readme file prompting the victim to execute a CobaltStrike implant. The mechanism used to execute CobaltStrike was DLL side-loading, which decrypted and executed a CobaltStrike stager shellcode. Analysis of the code, the infrastructure and the victimology led us to attribute this watering-hole, with high confidence, to the HoneyMyte APT threat actor.

Quarian is a little-known malicious program that Chinese-speaking actors have used since around 2012. We hadn't spotted any further activity until we observed a resurgence in an attack by the Icefog group in 2019. We tracked the activity of the malware following this and noticed a new variant that was used during several attacks on Middle Eastern and African

governments during 2020. In one case, we could see that this variant was deployed following exploitation of the CVE-2020-0688 vulnerability on the network of a government entity. This vulnerability, which was publicly reported in February 2020, allows an authenticated user to run commands as SYSTEM on a Microsoft Exchange server. In this case, the server was indeed compromised and was hosting the ChinaChopper webshell, which was used to obtain, and later launch, the Quarian and PlugX backdoors. Our analysis led us to assume, with medium to high confidence, that the group behind these attacks is one we track under the name CloudComputating – a Chinese-speaking actor that, based on previous reports, has targeted high-profile Middle Eastern diplomatic targets.

In March, researchers at Check Point Research published a report describing an APT campaign that targeted Mongolia's public sector and leveraged a coronavirus-themed lure to conduct its initial intrusion. We were able to discover further samples and another COVID-themed document with the same targeting, as well as additional targets in Russia. We attribute this activity with medium confidence to IronHusky.

Middle East

The MuddyWater APT was discovered in 2017 and has been active in the Middle East ever since. In 2019, we reported activity against telecoms providers in Iraq and Iran, as well as government bodies in Lebanon. We recently discovered MuddyWater using a new C++ toolchain in a new wave of attacks in which the actor leveraged an open-source utility called Secure Socket Funneling for lateral movement.

At the end of May, we observed that Oilrig had included the DNSExfitrator tool in its toolset. It allows the threat actor to use the DNS over HTTPS (DoH) protocol. Use of the DNS protocol for malware communications is a technique that Oilrig has been using for a long time. The difference between DNS- and DoH-based requests is that, instead of plain text requests to port 53, they would use port 443 in encrypted packets. Oilrig added the publicly available DNSExfiltrator tool to its arsenal, which allows DoH queries to Google and Cloudflare services. This time, the operators decided to use subdomains of a COVID-related domain which are hardcoded in the DNSExfitrator detected samples.

Southeast Asia and Korean Peninsula

BlueNoroff is one of the most prolific financially motivated APT actors and we have published several reports of BlueNoroff campaigns targeting financial institutions. Recently, we uncovered another campaign that has been active since at least 2017. In this campaign, the group sends spear-phishing emails containing an archived Windows shortcut file. The file names are disguised as security or cryptocurrency related files in order to entice users into executing them. The infection chain started from this shortcut file is a complex multi-stage infection procedure. Before delivering the Windows executable payload, the actor uses two VBS and three PowerShell scripts in order to collect system information. The actor very

carefully delivers the final payload only to the intended targets. The backdoor payload also utilizes a multi-stage infection procedure. The actor uses it to control infected hosts and implants additional malware for surveillance. These malicious programs are responsible for stealing the user's keystrokes and saving a screenshot of the infected machine. The main targets of this campaign are financial institutions, such as cryptocurrency businesses, and fintech companies. We identified diverse victims from 10 countries, as well as more potential victims from open source intelligence.

The Lazarus group has been a major threat actor for several years. Alongside goals like cyber-espionage and cyber-sabotage, this threat actor has targeted banks and other financial companies around the globe. The group continues to be very active. We recently observed the Lazarus group attacking a software vendor in South Korea using Bookcode, malware that we evaluate to be a Manuscrypt variant, utilizing a watering-hole attack to deliver it. Manuscrypt is one of the Lazarus group's tools that is actively being updated and used. The group attacked the same victim twice. Almost a year prior to compromising this victim, Lazarus attempted to infect it by masquerading as a well-known security tool, but failed. We were able to construct the group's post-exploitation activity, identifying various freeware and red-teaming tools used. Although Lazarus has recently tended to focus more on targeting the financial industry, we believe that in this campaign they were seeking to exfiltrate intellectual property. We also observed that they previously spread Bookcode using a decoy document related to a company working in the defense sector. Based on our observations, we evaluate that the Bookcode malware is being used exclusively for cyber-espionage campaigns.

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, Kaspersky was 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 also the first time it has been established that the Lazarus group has resorted to targeted ransomware attacks for financial gain.

Last year we created a private report on a malware framework that we named MATA, which we attribute, with low confidence, to the Lazarus group. This framework included several components, such as a loader, orchestrator and plug-ins. Initially, this framework targeted Windows and Linux. However, in April we discovered a suspicious macOS file uploaded to VirusTotal using a rule to detect the MATA malware framework. After looking into this malware, we confirmed that it was a macOS variant of the MATA malware. The malware developers Trojanized an open-source two-factor authentication application and utilized

another open-source application template. While investigating, to find more solid evidence for attribution, we found an old Manuscrypt strain that used a similar configuration structure. We also discovered a cluster of C2 servers probably related to this campaign.

The MATA framework was not the only way that Lazarus targeted macOS. We also observed a cluster of activity linked to Operation AppleJeus. The other was similar to the macOS malware used in a campaign that we call TangDaiwbo. This is a multi-platform cryptocurrency exchange campaign: Lazarus utilizes macro-embedded Office documents and spreads PowerShell or macOS malware, depending on the victim's system.

Early this year, we reported improvements in a Lazarus campaign targeting a cryptocurrency business. In this campaign, Lazarus adopted a downloader that sends compromised host information and selectively fetches the next-stage payload. Recently, we identified a Lazarus campaign with similar strategies, but targeting academic and automotive sectors. Lazarus also adopted new methods to deliver its tools. First of all, the group elaborated its weaponized document by adopting remote template injection techniques. Previously, Lazarus delivered macro-embedded documents to the victim, but the group has now applied one more stage to hinder detection. The group also utilized an open-source PDF reader named Sumatra PDF to make Trojanized applications. They created a Trojanized PDF reader, sending it to the victim with a crafted PDF file. If the victim opens this file, the Trojanised PDF viewer implants malicious files and shows decoy documents to deceive the victim. The actor delivers the final payload very carefully, and executes it in memory. Fortunately, we were able to get the final payload and confirm that it was a Manuscrypt variant that we had already described. We also found that it's the same malware variant that the US CISA (Cybersecurity and Infrastructure Security Agency) recently reported, named COPPERHEDGE.

Following our report describing the long-standing PhantomLance campaign in Southeast Asia, we published a private report providing detailed attribution based on discovered overlaps with reported campaigns of the OceanLotus APT. In particular, we found multiple code similarities with the previous Android campaign, as well as similarities in macOS backdoors, infrastructure overlap with Windows backdoors and a couple of cross-platform resemblances. Based on our research, we believe, with medium confidence, that PhantomLance is a modern Android campaign conducted by OceanLotus. Apart from the attribution details, we described the actor's spreading strategy using techniques to bypass app market filters. We also provided additional details about samples associated with previously reported suspected infrastructure, as well as the latest sample deployed in 2020 that uses Firebase to decrypt its payload.

Additionally, OceanLotus has been using new variants of its multi-stage loader since the second half of 2019. The new variants use target-specific information (username, hostname, etc.) of the targeted host that they obtained beforehand, in order to ensure their final implant

is deployed on the right victim. The group continues to deploy its backdoor implant, as well as Cobalt Strike Beacon, configuring them with updated infrastructure.

Other interesting discoveries

The Deceptikons APT is a long-running espionage group believed to have been providing mercenary services for almost a decade now. The group is not technically sophisticated and has not, to our knowledge, deployed zero-day exploits. The Deceptikons infrastructure and malware set is clever, rather than technically advanced. It is also highly persistent and in many ways reminds us of WildNeutron. Deceptikon's repeated targeting of commercial and non-governmental organizations is somewhat unusual for APT actors. In 2019, Deceptikons spear-phished a set of European law firms, deploying PowerShell scripts. As in previous campaigns, the actor used modified LNK files requiring user interaction to initially compromise systems and execute a PowerShell backdoor. In all likelihood, the group's motivations included obtaining specific financial information, details of negotiations, and perhaps even evidence of the law firms' clientele.

MagicScroll (aka AcidBox) is the name we've given to a sophisticated malware framework, whose main purpose is to decrypt and load an arbitrary payload in kernel mode. The framework consists of several stages. The first stage is a Windows security provider that is loaded by the system on boot and executed in user mode. This decrypts and runs a second payload, which is physically stored in the registry. Although we weren't able to find a victim with this second stage, we were able to find a file that matches the expected format of the second stage. This second stage payload utilizes a well-known vulnerability in a VirtualBox driver (CVE-2008-3431) to load the third stage, which is designed to run in kernel mode. The kernel mode payload is decrypted from a resource from the second stage, using the key retrieved from the registry. Unfortunately, we couldn't find a decryption key to decrypt the third stage payload, so we don't know what the last part of this malware framework looks like. Although the code is quite sophisticated, we couldn't identify any similarity with other known frameworks.

Aarogya Setu is the name of a mandatory COVID-19 mobile tracking app developed by the National Informatics Centre, an organization that comes under the Ministry of Electronics and Information Technology in India. It allows its users to connect to essential health services in India. With cyber criminals and APT actors taking advantage of pandemic-tracking applications to distribute Trojanized mobile apps, we investigated and identified apps that mimic the appearance and behavior of the legitimate Aarogya Setu app while deploying Android RATs. We consider one of these to be a new version of a RAT that we previously reported being used by the Transparent Tribe threat actor.

Final thoughts

The threat landscape isn't always full of "groundbreaking" events. However, a review of the activities of APT threat actors indicates that there are always interesting developments. Our regular quarterly reviews are intended to highlight these key developments.

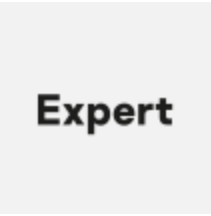
Here are the main trends that we've seen in Q2 2020.

- Geo-politics remains an important motive for some APT threat actors, as shown in the activities of MuddyWater, the compromise of the Middle East Eye website and the campaigns of CloudComputating and HoneyMyte groups.
- As is clear from the activities of Lazarus and BlueNoroff, financial gain is another driver for some threat actors – including the use of ransomware attacks.
- While Southeast Asia continues to be an active region for APT activities, this quarter we have also observed heavy activity by Chinese-speaking groups, including ShadowPad, HoneyMyte, CactusPete, CloudComputating and SixLittleMonkeys.
- APT threat actors continue to exploit software vulnerabilities – examples this quarter include Hades and MagicScroll.
- We have noted before that the use of mobile implants is no longer a novelty, and this quarter is no exception, as illustrated by the PhantomLance campaign.
- It is clear that APT actors, like opportunistic cybercriminals, continue to exploit the COVID-19 pandemic as a theme to lure potential victims. However, we would note once again that this doesn't represent a shift in TTPs.

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.

- APT
- Backdoor
- Chinese-speaking cybercrime
- Financial malware
- Lazarus
- Malware
- Ransomware
- Russian-speaking cybercrime
- Targeted attacks
- Turla

Authors



GReAT

Your email address will not be published. Required fields are marked *