APT trends report Q1 2021

By GReAT

Published: 2021-04-27 · Archived: 2026-04-06 00:14:20 UTC

For four 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 2021.

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.

In December, SolarWinds, a well-known IT managed services provider, fell victim to a sophisticated supply-chain attack. The company's Orion IT, a solution for monitoring and managing customers' IT infrastructure, was compromised. This resulted in the deployment of a custom backdoor, named Sunburst, on the networks of more than 18,000 SolarWinds customers, including many large corporations and government bodies, in North America, Europe, the Middle East and Asia. In our initial report on Sunburst, we examined the method used by the malware to communicate with its C2 (command-and-control) server and the protocol used to upgrade victims for further exploitation. Further investigation of the Sunburst backdoor revealed several features that overlap with a previously identified backdoor known as Kazuar, a .NET backdoor first reported in 2017 and tentatively linked to the Turla APT group. The shared features between Sunburst and Kazuar include the victim UID generation algorithm, code similarities in the initial sleep algorithm and the extensive usage of the FNV1a hash to obfuscate string comparisons. There are several possibilities: Sunburst may have been developed by the same group as Kazuar; the developers of Sunburst may have adopted some ideas or code from Kazuar; both groups obtained their malware from the same source; some Kazuar developers moved to another team, taking knowledge and tools with them; or the developers of Sunburst introduced these links as a form of false flag. Hopefully, further analysis will make things clearer.

On March 2, Microsoft reported a new APT actor named HAFNIUM, exploiting four zero-days in Exchange Server in what they called "limited and targeted attacks". At the time, Microsoft claimed that, in addition to HAFNIUM, several other actors were exploiting them as well. In parallel, Volexity also reported the same Exchange zero-days being in use in early 2021. According to Volexity's telemetry, some of the exploits in use are shared across several actors, besides the one Microsoft designates as HAFNIUM. Kaspersky telemetry revealed a spike in exploitation attempts for these vulnerabilities following the public disclosure and patch from Microsoft. During the first week of March, we identified approximately 1,400 unique servers that had been targeted, in which one or more of these vulnerabilities were used to obtain initial access. Prior to the posts, on February 28, we identified related exploitation on less than a dozen Exchange systems; we also found more than a dozen Exchange artefacts indicating exploitation uploaded to multi-scanner services. According to our telemetry, most exploitation

attempts were observed for servers in Europe and the United States. Some of the servers were targeted multiple times by what appear to be different threat actors (based on the command execution patterns), suggesting the exploits are now available to multiple groups.

We have also discovered a campaign active since mid-March targeting governmental entities in the Russian Federation, using the aforementioned Exchange zero-day exploits. This campaign made use of a previously unknown malware family we dubbed FourteenHi. Further investigation revealed traces of activity involving variants of this malware dating back a year. We also found some overlaps in these sets of activities with HAFNIUM in terms of infrastructure and TTPs as well as the use of ShadowPad malware during the same timeframe.

Europe

During routine monitoring of detections for FinFisher spyware tools, we discovered traces that point to recent FinFly Web deployments. In particular, we discovered two servers with web applications that we suspect, with high confidence, were generated using FinFly Web. FinFly Web is, in essence, a suite of tools and packages that implement a web-based exploitation server. It was first publicly documented in 2014, in the aftermath of the Gamma Group hacking incident. One of the suspected FinFly Web servers was active for more than a year between October 2019 and December 2020. This server was disabled a day after our discovery last December. Nevertheless, we were able to capture a copy of its landing page, which included JavaScript used to profile victims using what appears to be previously unknown code. In the second case, the server hosting FinFly Web was already offline at the moment of discovery, so we drew our conclusions using available historical data. As it turned out, it was active for a very short time around September 2020 on a host that appears to have been impersonating the popular Mail.ru service. Surprisingly, this server began answering queries again on January 12. So far, we haven’t seen any related payloads being dropped by these web pages.

Russian-speaking activity

Kazuar is a .NET backdoor usually associated with the Turla threat actor (aka Snake and Uroboros). Recently, Kazuar received renewed interest due to its similarities with the Sunburst backdoor. Although the capabilities of Kazuar have already been exposed in public research, many interesting facts about this backdoor were not made public. Our latest reports focus on the changes the threat actor made to the September and November versions of its backdoor.

On February 24, the National Security Defense Council of Ukraine (NSDC) publicly warned that a threat actor had exploited a national documents circulation system (SEI EB) to distribute malicious documents to Ukrainian public authorities. The alert contained a few related network IoCs, and specified that the documents used malicious macros in order to drop an implant onto targeted systems. Thanks to the shared IoCs, we were able to attribute this attack, with high confidence, to the Gamaredon threat actor. The malicious server IP mentioned by the NSDC has been known to Kaspersky since February as Gamaredon infrastructure.

On January 27, the French national cybersecurity agency (ANSSI) published a report describing an attack campaign that targeted publicly exposed and obsolete Centreon systems between 2017 and 2020, in order to deploy Fobushell (aka P.A.S.) webshells and Exaramel implants. ANSSI associated the campaign with the

Sandworm intrusion-set, which we refer to as Hades. Although we specifically looked for additional compromised Centreon systems, Exaramel implant samples or associated infrastructure, we were unable to retrieve any useful artifacts from which we could initiate a comprehensive investigation. However, we did identify three Centreon servers where a Fobushell webshell had been deployed. One of those Fobushell samples was identical to another we previously identified on a Zebrocy C2 server.

Chinese-speaking activity

We discovered a set of malicious activities, which we named EdwardsPheasant, targeting mainly government organizations in Vietnam since June 2020. The attackers leverage previously unknown and obfuscated backdoors and loaders. The activities peaked in November 2020, but are still ongoing. The associated threat actor continues to leverage its tools and tactics (described in our private report) to compromise targets or maintain access in their networks. While we could identify similarities with the tools and tactics associated with Cycldek (aka Goblin Panda) and Lucky Mouse (aka Emissary Panda), we have been unable to attribute this set of activities to either of them conclusively.

We investigated a long-running espionage campaign, dubbed A41APT, targeting multiple industries, including the Japanese manufacturing industry and its overseas bases, which has been active since March 2019. The attackers used vulnerabilities in an SSL-VPN product to deploy a multi-layered loader we dubbed Ecipekac (aka DESLoader, SigLoader and HEAVYHAND). We attribute this activity to APT10 with high confidence. Most of the discovered payloads deployed by this loader are fileless and have not been seen before. We observed SodaMaster (aka DelfsCake, dfls and DARKTOWN), P8RAT (aka GreetCake and HEAVYPOT), and FYAnti (aka DILLJUICE Stage 2) which in turn loads QuasarRAT. In November and December 2020, two public blog posts were published about this campaign. One month later, we observed new activities from the actor with an updated version of some of their implants designed to evade security products and make analysis harder for researchers. You can read more in our public report.

Middle East

We recently came across previously unknown malicious artifacts that we attributed to the Lyceum/Hexane threat group, showing that the attackers behind it are still active and have been developing their toolset during the last year. Although Lyceum still prefers taking advantage of DNS tunneling, it appears to have replaced the previously documented .NET payload with a new C++ backdoor and a PowerShell script that serve the same purpose. Our telemetry revealed that the threat group's latest endeavors are focused on going after entities within one country – Tunisia. The victims we observed were all high-profile Tunisian organizations, such as telecommunications or aviation companies. Based on the targeted industries, we assume that the attackers may have been interested in compromising these entities to track the movements and communications of individuals that are of interest to them. This could mean that the latest Lyceum cluster has an operational focus on targeting Tunisia, or that it is a subset of broader activity that is yet to be discovered.

On November 19, 2020, Shadow Chaser Group tweeted about a suspected MuddyWater APT malicious document potentially targeting a university in the United Arab Emirates. Based on our analysis since then, we suspect this intrusion is part of a campaign that started at least in early October 2020 and was last seen active in late December 2020. The threat actor relied on VBS-based malware to infect organizations from government, NGO and

education sectors. Our telemetry, however, indicates that no further tools were deployed and we do not believe that data theft took place either. This indicates to us that the attackers are currently in the reconnaissance phase of their operation, and we expect subsequent waves of attacks to follow in the near future. In our private report, we provide an in-depth analysis of the malicious documents used by this threat actor and study their similarities to known MuddyWater tooling. The infrastructure setup and communications scheme are also similar to past incidents attributed to this group. The actor maintains a small set of first-stage C2 servers to connect back from the VBS implant for initial communications. Initial reconnaissance is performed by the actor and communication with the implant is handed off to a second-stage C2 for additional downloads. Finally, we present similarities with known TTPs of the MuddyWater group and attribute this campaign to them with medium confidence.

Domestic Kitten is a threat group mainly known for its mobile backdoors. The group's operations were exposed in 2018, showing that it was conducting surveillance attacks against individuals in the Middle East. The threat group targeted Android users by sending them popular and well-known applications that were backdoored and contained malicious code. Many of the applications had religious or political themes and were intended for Farsi, Arabic and Kurdish speakers, possibly alluding to this attack's main targets. We have discovered new evidence showing that Domestic Kitten has been using PE executables to target victims using Windows since at least 2013, with some evidence that it goes back to 2011. The Windows version, which, to the best of our knowledge, has not been described in the past, was delivered in several versions, with the more recent one used for at least three and a half years to target individuals in parallel to the group's mobile campaigns. The implant functionality and infrastructure in that version have remained the same all along, and have been used in the group's activity witnessed this year.

Ferocious Kitten is an APT group that has been active against Persian-speaking individuals since 2015 and appears to be based in Iran. Although it has been active over a large timespan, the group has mostly operated under the radar and, to the best of our knowledge, has not been covered by security researchers. It only recently attracted attention when a lure document was uploaded to VirusTotal and was brought to public knowledge by researchers on Twitter. Subsequently, one of its implants was analyzed by a Chinese intelligence firm. We have been able to expand some of the findings on the group and provide insights on additional variants. The malware dropped from the aforementioned document is dubbed MarkiRAT and is used to record keystrokes and clipboard content, provide file download and upload capabilities as well as the ability to execute arbitrary commands on the victim's machine. We were able to trace the implant back to at least 2015, along with variants intended to hijack the execution of the Telegram and Chrome applications as a persistence method. Interestingly, some of the TTPs used by this threat actor are reminiscent of other groups operating in the domain of dissident surveillance. For example, it used the same C2 domains across its implants for years, which was witnessed in the activity of Domestic Kitten. In the same vein, the Telegram execution hijacking technique observed in this campaign by Ferocious Kitten was also observed being used by Rampant Kitten, as covered by Check Point. In our private report, we expand the details on these findings as well as provide analysis and mechanics of the MarkiRAT malware.

Karkadann is a threat actor that has been targeting government bodies and news outlets in the Middle East since at least October 2020. The threat actor leverages tailor-made malicious documents with embedded macros that trigger an infection chain, opening a URL in Internet Explorer. The minimal functionality present in the macros and the browser specification suggest that the threat actor might be exploiting a privilege-escalation vulnerability

in Internet Explorer. Despite the small amount of evidence available for analysis in the Karkadann case, we were able to find several similarities to the Piwiks case, a watering-hole attack we discovered that targeted multiple prominent websites in the Middle East. Our private report presents the recent Karkadann campaigns and the similarities between this campaign and the Piwiks case. The report concludes with some infrastructure overlaps with unattributed clusters that we have seen since last year that are potentially linked to the same threat actor.

Southeast Asia and Korean Peninsula

We discovered that the Kimsuky group adopted a new method to deliver its malware in its latest campaign on a South Korean stock trading application. In this campaign, beginning in December 2020, the group compromised a website belonging to the vendor of stock trading software, replacing the hosted installation package with a malicious one. Kimsuky also delivered its malware by utilizing a malicious Hangul (HWP) document containing COVID-19-related bait that discusses a government relief fund. Both infection vectors ultimately deliver the Quasar RAT. Compared to Kimsuky's last reported infection chain, composed of various scripts, the new scheme adds complications and introduces less popular file types, involving VBS scripts, XML and Extensible Stylesheet Language (XSL) files with embedded C# code in order to fetch and execute stagers and payloads. Based on the lure document and characteristics of the compromised installation package, we conclude that this attack is financially motivated, which, as we have previously reported, is one of Kimsuky's main focus areas.

On January 25, the Google Threat Analysis Group (TAG) announced that a North Korean-related threat actor had targeted security researchers. According to Google TAG's blog, this actor used highly sophisticated social engineering, approached security researchers through social media, and delivered a compromised Visual Studio project file or lured them to their blog and installed a Chrome exploit. On March 31, Google TAG released an update on this activity showing another wave of fake social media profiles and a company the actor set up mid-March. We can confirm that several infrastructures on the blog overlap with our previously published reporting about Lazarus group's ThreatNeedle cluster. Moreover, the malware mentioned by Google matched ThreatNeedle – malware that we have been tracking since 2018. While investigating associated information, a fellow external researcher confirmed that he was also compromised by this attack, sharing information for us to investigate. We discovered additional C2 servers after decrypting configuration data from the compromised host. The servers were still in use during our investigation, and we were able to get additional data, analyzing logs and files present on the servers. We assess that the published infrastructure was used not only to target security researchers but also in other Lazarus attacks. We found a relatively large number of hosts communicating with the C2s at the time of our research. You can read our public report here.

Following up our previous investigation into Lazarus attacks on the defense industry using ThreatNeedle, we discovered another malware cluster named CookieTime used in a campaign mainly focused on the defense industry. We detected activity in September and November 2020, with samples dating back to April 2020. Compared to the already known malware clusters of the Lazarus group, CookieTime shows a different structure and functionality. This malware communicates with the C2 server using the HTTP protocol. In order to deliver the request type to the C2 server, it uses encoded cookie values and fetches command files from the C2 server. The C2 communication takes advantage of steganography techniques, delivered in files exchanged between infected clients and the C2 server. The contents are disguised as GIF image files, but contain encrypted commands from the C2 server and command execution results. We had a chance to look into the command and control script as a

result of working closely with a local CERT to take down the threat actor's infrastructure. The malware control servers are configured in a multi-stage fashion and only deliver the command file to valuable hosts.

While investigating the artifacts of a supply-chain attack on the Vietnam Government Certification Authority's (VGCA) website, we discovered that the first Trojanized package dates to June 2020. Unravelling that thread, we identified a number of post-compromise tools in the form of plugins deployed using PhantomNet malware, which was delivered using Trojanized packages. Our analysis of these plugins revealed similarities with the previously analyzed CoughingDown malware. In our private report, we offer a detailed description for each post-compromise tool used in the attack, as well as other tools belonging to the actor's arsenal. Finally, we also explore CoughingDown attribution in the light of recent discoveries.

On February 10, DBAPPSecurity published details about a zero-day exploit they discovered last December. Aside from the details of the exploit itself, researchers also mentioned it being used in the wild by BitterAPT. While no such subsequent information was given in the initial report to explain the attribution claims, our investigation into this activity confirms the exploit was in fact being used exclusively by this actor. We assigned the name TurtlePower to the campaign that makes use of this exploit, along with the other tools used to target governmental and telecom entities in Pakistan and China. We have also confidently linked the origin of this exploit to a broker we refer to as Moses. Moses has been responsible for the development of at least five exploits patched in the last two years. We have also been able to tie the usage of some of these exploits to at least two different actors thus far – BitterAPT and DarkHotel. At this time, it is unclear how these threat actors are obtaining exploits from Moses, whether it is through direct purchase or another third-party provider. During the TurtlePower campaign, BitterAPT used a wide array of tools on its victims to include a stage one payload named ArtraDownloader, a stage two payload named Splinter, a keylogger named SourLogger, an infostealer named SourFilling, as well as variations of Mimikatz to gather specific files and maintain its access. This particular campaign also appears to be narrowly focused on targets within Pakistan and China (based on the initial report referenced). While we can verify specific targeting within Pakistan using our own data, we have not been able to do the same regarding China. Use of CVE-2021-1732 peaked between June and July 2020, but the overall campaign is still ongoing.

In 2020, we observed new waves of attacks related to Dropping Elephant (aka Patchwork, Chinastrats), focusing on targets in China and Pakistan. We also noted a few targets outside of the group's traditional area of operations, namely in the Middle East, and a growing interest in the African continent. The attacks followed the group's well-established TTPs, which include the use of malicious documents crafted to exploit a remote code execution vulnerability in Microsoft Office, and the signature JakyllHyde (aka BadNews) Trojan in the later infection stages. Dropping Elephant introduced a new loader for JakyllHyde, a tool we named Crypta. It contains mechanisms to hinder detection and appears to be a core component of this APT actor's recent toolset. Crypta and its variants have been observed in multiple scenarios loading a wide range of subsequent payloads, such as Bozok RAT, Quasar RAT and LokiBot. An additional Trojan discovered during our research was PubFantacy. To our knowledge, this tool has never been publicly described and has been used to target Windows servers since at least 2018.

We recently discovered a previously publicly unknown Android implant used in 2018-2019 by the SideWinder threat group, which we dubbed BroStealer. The main purpose of the BroStealer implant is to collect sensitive information from a victim's device, such as photos, SMS messages, call recordings and files from various

messaging applications. Although SideWinder has numerous campaigns against victims using the Windows platform, recent reports have shown that this threat group also goes after its targets via the mobile platform.

Other interesting discoveries

In February 2019, multiple antivirus companies received a collection of malware samples, most of them associated with various known APT groups. Some of the samples cannot be associated with any known activity. Some, in particular, attracted our attention due to their sophistication. The samples were compiled in 2014 and, accordingly, were likely deployed in 2014 and possibly as late as 2015. Although we have not found any shared code with any other known malware, the samples have intersections of coding patterns, style and techniques that have been seen in various Lambert families. We therefore named this malware Purple Lambert. Purple Lambert is composed of several modules, with its network module passively listening for a magic packet. It is capable of providing an attacker with basic information about the infected system and executing a received payload. Its functionality reminds us of Gray Lambert, another user-mode passive listener. Gray Lambert turned out to be a replacement of the kernel-mode passive-listener White Lambert implant in multiple incidents. In addition, Purple Lambert implements functionality similar to, but in different ways, both Gray Lambert and White Lambert. Our report, available to subscribers of our APT threat reports, includes discussion of both the passive-listener payload and the loader functionality included in the main module.

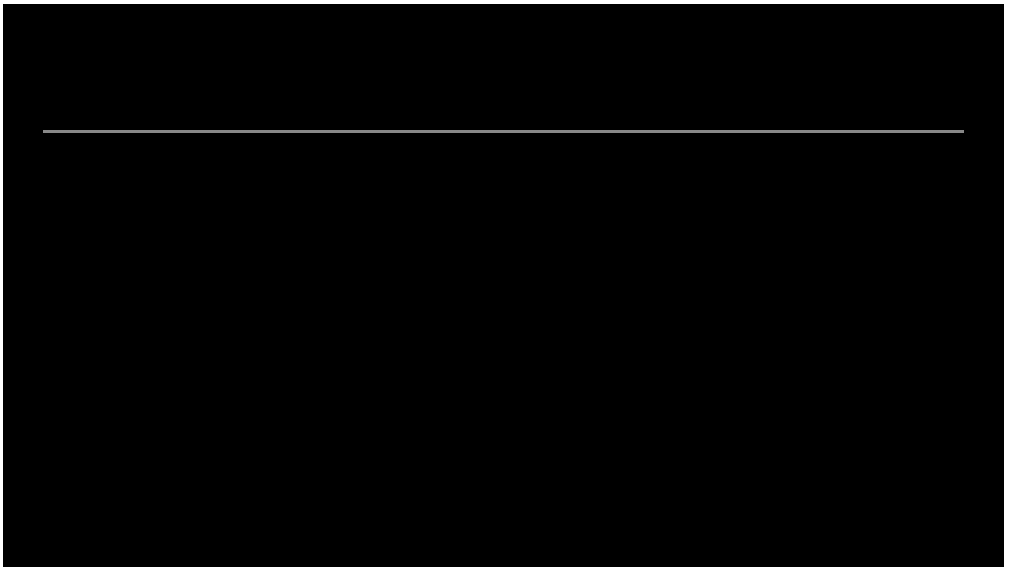
Final thoughts

While the TTPs of some threat actors remain consistent over time, relying heavily on social engineering as a means of gaining a foothold in a target organization or compromising an individual's device, others refresh their toolsets and extend the scope of their activities. Our regular quarterly reviews are intended to highlight the key developments of APT groups.

Here are the main trends that we've seen in Q1 2021:

- Perhaps the most predominant attack we researched in this quarter was the SolarWinds attack. SolarWinds showed once again how successful a supply-chain attack can be, especially where attackers go the extra mile to remain hidden and maintain persistence in a target network. The scope of this attack is still being investigated as more zero-day flaws are discovered in SolarWinds products.
- Another critical wave of attacks was the exploitation of Microsoft Exchange zero-day vulnerabilities by multiple threat actors. We recently discovered another campaign using these exploits with different targeting, possibly related to the same cluster of activities already reported.
- Lazarus group's bold campaign targeting security researchers worldwide also utilized zero-day vulnerabilities in browsers to compromise their targets. Their campaigns used themes centered on the use of zero-days to lure relevant researchers, possibly in an attempt to steal vulnerability research.

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.



Source: https://securelist.com/apt-trends-report-q1-2021/101967