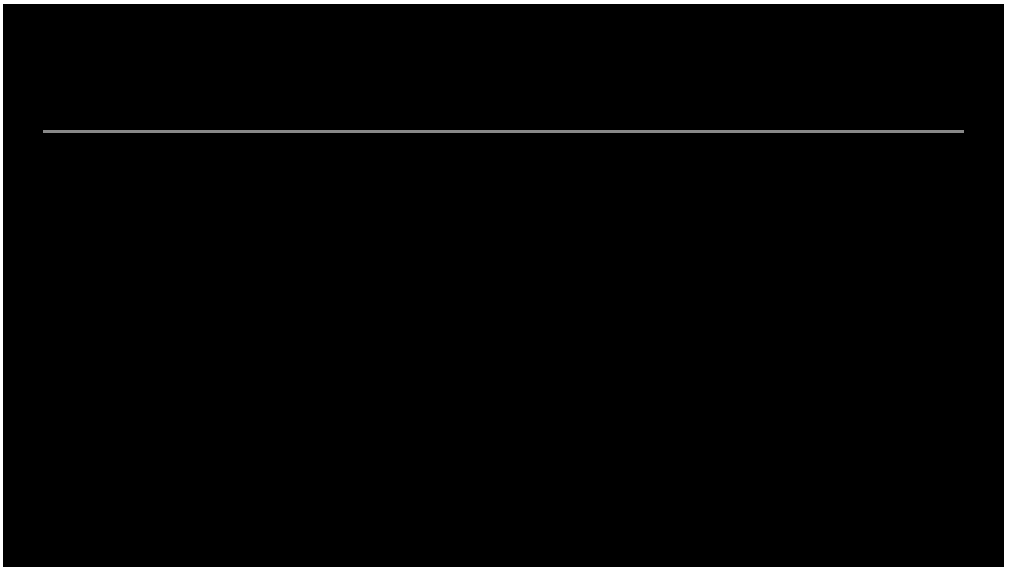
APT trends report Q2 2021

By GReAT

Published: 2021-07-29 · Archived: 2026-04-05 14:26:26 UTC

For more than 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 Q2 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.

Investigating the recent Microsoft Exchange vulnerabilities we and our colleagues from AMR found an attacker deploying a previously unknown backdoor, “FourteenHi”, in a campaign that we dubbed ExCone, active since mid-March. During our investigation we revealed multiple tools and variants of FourteenHi, configured with infrastructure that FireEye reported as being related to the UNC2643 activity cluster. Moreover, we saw ShadowPad detections coincide with FourteenHi variant infections, possibly hinting at a shared operator between these two malware families.

FourteenHi abuses the popular VLC media player to execute its loader. It is capable of performing basic backdoor functions. Further investigation also revealed scripts used by the actor to gain situational awareness post-exploitation, as well as previous use of the infrastructure to operate Cobalt Strike Beacon.

Although we couldn’t directly attribute this activity to any known threat actor, we found older, highly similar 64-bit samples of the backdoor used in close proximity with ShadowPad malware, mostly known for its operations

involving supply-chain attacks as an infection vector. Notably, we also found one C2 IP used in a 64-bit sample reportedly used in the UNC2643 activity set, associated with the HAFNIUM threat actor, also using Cobalt Strike, DLL side-loading and exploiting the same Exchange vulnerabilities.

Russian-speaking activity

On May 27 and 28, details regarding an ongoing email campaign against diplomatic entities throughout Europe and North America were released by Volexity and Microsoft. These attacks were attributed to Nobelium and APT29 by Microsoft and Volexity respectively. While we were able to verify the malware and possible targeting for this cluster of activity, we haven't been able to make a definitive assessment at this time about which threat actor is responsible, although we found ties to Kazuar. We have designated it as a new threat actor and named it "HotCousin". The attacks began with a spear-phishing email which led to an ISO file container being stored on disk and mounted. From here, the victim was presented with a LNK file made to look like a folder within an Explorer window. If the victim double clicked on it, the LNK then executed a loader written in .NET referred to as BoomBox, or a DLL. The execution chain ultimately ended with a Cobalt Strike beacon payload being loaded into memory. According to public blogs, targeting was widespread but focused primarily on diplomatic entities throughout Europe and North America: based on the content of the lure documents bundled with the malware, this assessment appears to be accurate. This cluster of activity was conducted methodically beginning in January with selective targeting and slow operational pace, then ramping up and ending in May. There are indications of previous activity from this threat actor dating back to at least October 2020, based on other Cobalt Strike payloads and loaders bearing similar toolmarks.

Chinese-speaking activity

While investigating a recent rise of attacks against Exchange servers, we noticed a recurring cluster of activity that appeared in several distinct compromised networks. This cluster stood out because it used a formerly unknown Windows kernel mode rootkit and a sophisticated multi-stage malware framework aimed at providing remote control over the attacked servers. The former is used to hide the user mode malware's artefacts from investigators and security solutions, while demonstrating an interesting loading scheme involving the kernel mode component of an open source project named "Cheat Engine" to bypass the Windows Driver Signature Enforcement mechanism. We were able to determine that this toolset had been in use from as early as July 2020; and that the threat actor was mostly focused on Southeast Asian targets, including several governmental entities and telecoms companies. Since this was a long-standing operation, with high-profile victims, an advanced toolset and no affinity to a known threat actor, we decided to name the underlying cluster "GhostEmperor".

APT31 (aka ZIRCONIUM) is a Chinese-speaking intrusion set. This threat actor set up an ORB (Operational Relay Boxes) infrastructure, composed of several compromised SOHO routers, to target entities based in Europe (and perhaps elsewhere). As of the publication of our report in May, we had seen these ORBs used to relay Cobalt Strike communications and for anonymization proxying purposes. It is likely that APT31 uses them for other implants and ends as well (for example, exploit or malware staging). Most of the infrastructure put in place by APT31 comprises compromised Pakedge routers (RK1, RE1 and RE2). This little-known constructor specializes in small enterprise routers and network devices. So far, we don't know which specific vulnerability has been

exploited by the intrusion set to compromise the routers. Nor do we currently possess telemetry that would provide further visibility into this campaign. We will, of course, continue to track these activities.

Following our previous report on EdwardsPheasant, DomainTools and BitDefender published articles about malicious activities against targets in Southeast Asia which we believe, with medium to high confidence, are parts of EdwardsPheasant campaigns. While tracking the activities of this threat actor, analyzing samples discovered or provided by third parties, and investigating from public IoCs, we discovered an updated DropPhone implant, an additional implant loaded by FoundCore's shellcode, several possible new infection documents and malicious domain names, as well as additional targets. While we do not believe we have a complete picture of this set of activities yet, our report this quarter marks a significant step further in understanding its extent.

A Chinese-speaking APT compromised a certificate authority in Mongolia and replaced digital certificate management client software with a malicious downloader in February. We are tracking this group as BountyGlad. Related infrastructure was identified and used in multiple other incidents: interesting related activity included server-side attacks on WebSphere and WebLogic services in Hong Kong; and on the client-side, Trojanized Flash Player installers. The group demonstrated an increase in strategic sophistication with this supply-chain attack. While replacing a legitimate installer on a high value website like a certificate authority requires a medium level of skill and coordination, the technical sophistication is not on par with ShadowHammer. And while the group deploys fairly interesting, but simplistic, steganography to cloak its shellcode, we think it was probably generated with code that has been publicly available for years. Previous activity also connected with this group relied heavily on spear-phishing and Cobalt Strike throughout 2020. Some activity involved PowerShell commands and loader variants different from the downloaders presented in our recent report. In addition to spear-phishing, the group appears to rely on publicly available exploits to penetrate unpatched target systems. They use implants and C2 (Command and Control) code that are a mix of both publicly available and privately shared across multiple Chinese-speaking APTs. We are able to connect infrastructure across multiple incidents. Some of those were focused on Western targets in 2020. Some of the infrastructure listed in an FBI Flash alert published in May 2020, targeting US organizations conducting COVID-19 research, was also used by BountyGlad.

While investigating users infected with the TPCon backdoor, previously discussed in a private report, we detected loaders which are part of a new multi-plugin malware framework that we named "QSC", which allows attackers to load and run plugins in-memory. We attribute the use of this framework to Chinese-speaking groups, based on some overlaps in victimology and infrastructure with other known tools used by these groups. We have so far observed the malware loading a Command shell and File Manager plugins in-memory. We believe the framework has been used in the wild since April 2020, based on the compilation timestamp of the oldest sample found. However, our telemetry suggests that the framework is still in use: the latest activity we detected was in March this year.

Earlier this month, Rostelecom Solar and NCIRCC issued a joint public report describing a series of attacks against networks of government entities in Russia. The report described a formerly unknown actor leveraging an infection chain that leads to the deployment of two implants – WebDav-O and Mail-O. Those, in conjunction with other post-exploitation activity, have led to network-wide infections in the targeted organizations that resulted in exfiltration of sensitive data. We were able to trace the WebDav-O implant's activity in our telemetry to at least 2018, indicating government affiliated targets based in Belarus. Based on our investigation, we were able to find

additional variants of the malware and observe some of the commands executed by the attackers on the compromised machines.

We discovered a cluster of activity targeting telecom operators within a specific region. The bulk of this activity took place from May to October 2020. This activity made use of several malware families and tools; but the infrastructure, a staging directory, and in-country target profiles tie them together. The actors deployed a previously unknown passive backdoor, that we call “TPCon”, as a primary implant. It was later used to perform both reconnaissance within target organizations and to deploy a post-compromise toolset made up mostly of publicly available tools. We also found other previously unknown active backdoors, that we call “evsroin”, used as secondary implants. Another interesting find was a related loader (found in a staging directory) that loaded a KABA1 implant variant. KABA1 was an implant used against targets throughout the South China Sea that we attributed to the Naikon APT back in 2016. On another note, on the affected hosts we found additional multiple malware families shared by Chinese-speaking actors, such as ShadowPad and Quarian backdoors. These did not seem to be directly connected to the TPCon/evsroin incidents because the supporting infrastructure appeared to be completely separate. One of the ShadowPad samples appears to have been detected in 2020, while the others were detected well before that, in 2019. Besides the Naikon tie, we found some overlaps with previously reported IceFog and IamTheKing activities.

Middle East

BlackShadow is a threat group that became known after exfiltrating sensitive documents from Shirbit, an Israeli insurance company, and demanding a ransom in exchange for not releasing the information in its possession. Since then, the group has made more headlines, breaching another company in Israel and publishing a trove of documents containing customer related information on Telegram. Following this, we found several samples of the group’s unique .NET backdoor in our telemetry that were formerly unknown to us, one of which was recently detected in Saudi Arabia. By pivoting on new infrastructure indicators that we observed in those samples, we were able to find a particular C2 server that was contacted by a malicious Android implant and shows ties to the group’s activity.

We previously covered a WildPressure campaign against targets in the Middle East . Keeping track of the threat actor’s malware this spring, we were able to find a newer version (1.6.1) of their C++ Trojan, a corresponding VBScript variant with the same version and a completely new set of modules, including an orchestrator and three plugins. This confirms our previous assumption that there are more last-stagers besides the C++ ones, based on one of the fields in the C2 communication protocol which contains the “client” programming language. Another language used by WildPressure is Python. The PyInstaller module for Windows contains a script named “Guard”. Perhaps the most interesting finding here is that this malware was developed for both Windows and macOS operating systems. In this case, the hardcoded version is 2.2.1. The coding style, overall design and C2 communication protocol is quite recognisable across all programming languages used by the attackers. The malware used by WildPressure is still under active development in terms of versions and programming languages in use. Although we could not associate WildPressure’s activity with other threat actors, we did find minor similarities in the TTPs (Tactics, Techniques and Procedures) used by BlackShadow, which is also active in the same region. However, we consider that these similarities serve as minor ties and are not enough to make any attribution.

We discovered an ongoing campaign that we attribute to an actor named WIRTE, beginning in late 2019, targeting multiple sectors, focused on the Middle East. WIRTE is a lesser-known threat actor first publicly referenced in 2019, which we suspect has relations with the Gaza Cybergang threat actor group. During our hunting efforts, in February, for threat actor groups that are using VBS/VBA implants, we came across MS Excel droppers that use hidden spreadsheets and VBA macros to drop their first stage implant – a VBS script. The VBS script's main function is to collect system information and execute arbitrary code sent by the attackers. Although we recently reported on a new Muddywater first stage VBS implant used for reconnaissance and profiling activities, these intrusion sets have slightly different TTPs and wider targeting. To date, we have recorded victims focused in the Middle East and a few other countries outside this region. Despite various industries being affected, the focus was mainly towards government and diplomatic entities; however, we also noticed an unusual targeting of law firms.

GoldenJackal is the name we have given to a cluster of activity, recently discovered in our telemetry, that has been active since November 2019. This intrusion set consists of a set of .NET-based implants that are intended to control victim machines and exfiltrate certain files from them, suggesting that the actor's primary motivation is espionage. Furthermore, the implants were found in a restricted set of machines associated with diplomatic entities in the Middle East. Analysis of the aforementioned malware, as well as the accompanied detection logs, portray a capable and moderately stealthy actor. This can be substantiated by the successful foothold gained by the underlying actor in the few organizations we came across, all the while keeping a low signature and ambiguous footprint.

Southeast Asia and Korean Peninsula

The ScarCruft group is a geo-political motivated APT group that usually attacks government entities, diplomats and individuals associated with North Korean affairs. Following our last report about this group, we had not seen its activities for almost a year. However, we observed that ScarCruft compromised a North Korea-related news media website in January, beginning a campaign that was active until March. The attackers utilized the same exploit chains, CVE-2020-1380 and CVE-2020-0986, also used in Operation Powerfall. Based on the exploit code and infection scheme characteristics, we suspect that Operation PowerFall has a connection with the ScarCruft group. The exploit chain contains several stages of shellcode execution, finally deploying a Windows executable payload in memory. We discovered several victims from South Korea and Singapore. Besides this watering-hole attack, this group also used Windows executable malware concealing its payload. This malware, dubbed "ATTACK-SYSTEM", also used multi-stage shellcode infection to deliver the same final payload named "BlueLight". BlueLight uses OneDrive for C2. Historically, ScarCruft malware, especially RokRat, took advantage of personal cloud servers as C2 servers, such as pCloud, Box, Dropbox, and Yandex.

In May 2020, the Criminal Investigation Bureau (CIB) of Taiwan published an announcement about an attack targeting Taiwanese legislators. Based on their information, an unknown attacker sent spear-phishing emails using a fake presidential palace email account, delivering malware we dubbed "Palwan". Palwan is malware capable of performing basic backdoor functionality as well as downloading further modules with additional capabilities. Analysing the malware, we discovered another campaign, active in parallel, targeting Nepal. We also found two more waves of attacks launched against Nepal in October 2020 and in January this year using Palwan malware variants. We suspect that the targeted sector in Nepal is similar to the one reported by the CIB of Taiwan. Investigating the infrastructure used in the Nepal campaigns, we spotted an overlap with Dropping Elephant

activity. However, we don't deem this overlap sufficient to attribute this activity to the Dropping Elephant threat actor.

BlueNoroff is a long-standing, financially motivated APT group that has been targeting the financial industry for years. In recent operations, the group has focused on cryptocurrency businesses. Since the publication of our research of BlueNoroff's "SnatchCrypto" campaign in 2020, the group's strategy to deliver malware has evolved. In this campaign, BlueNoroff used a malicious Word document exploiting CVE-2017-0199, a remote template injection vulnerability. The injected template contains a Visual Basic script, which is responsible for decoding the next payload from the initial Word document and injecting it into a legitimate process. The injected payload creates a persistent backdoor on the victim's machine. We observed several types of backdoor. For further surveillance of the victim, the malware operator may also deploy additional tools. BlueNoroff has notably set up fake blockchain, or cryptocurrency-related, company websites for this campaign, to lure potential victims and initiate the infection process. Numerous decoy documents were used, which contain business and nondisclosure agreements as well as business introductions. When compared to the previous SnatchCrypto campaign, the BlueNoroff group utilized a similar backdoor and PowerShell agent but changed the initial infection vector. Windows shortcut files attached to spear-phishing emails used to be the starting point for an infection: they have now been replaced by weaponized Word documents.

We have discovered Andariel activity using a revised infection scheme and custom ransomware targeting a broad spectrum of industries located in South Korea. In April, we observed a suspicious document containing a Korean file name and decoy uploaded to VirusTotal. It revealed a novel infection scheme and an unfamiliar payload. During the course of our research, Malwarebytes published a report with technical details about the same series of attacks, which attributed it to the Lazarus group. After a deep analysis we reached a different conclusion – that the Andariel group was behind these attacks. Code overlaps between the second stage payload in this campaign and previous malware from the Andariel group allowed for this attribution. Apart from the code similarity and the victimology, we found additional connections with the Andariel group. Each threat actor has a characteristic habit when they interactively work with a backdoor shell in the post-exploitation phase. The way Windows commands and their options were used in this campaign is almost identical to previous Andariel activity. The threat actor has been spreading the third stage payload since the middle of 2020 and leveraged malicious Word documents and files mimicking PDF documents as infection vectors. Notably, in addition to the final backdoor, we discovered one victim infected with custom ransomware. This ransomware adds another facet to this Andariel campaign, which also sought financial profit in a previous operation involving the compromise of ATMs.

We recently uncovered a large-scale and highly active attack in Southeast Asia coming from a threat actor we dubbed LuminousMoth. Further analysis revealed that this malicious activity dates back to October 2020 and was still ongoing at the time we reported it in June. LuminousMoth takes advantage of DLL sideloading to download and execute a Cobalt Strike payload. However, perhaps the most interesting part of this attack is its capability to spread to other hosts by infecting USB drives. In addition to the malicious DLLs, the attackers also deployed a signed, but fake version of the popular application Zoom on some infected systems, enabling them to exfiltrate files; and an additional tool that accesses a victim's Gmail session by stealing cookies from the Chrome browser. Infrastructure ties as well as shared TTPs allude to a possible connection between LuminousMoth and the HoneyMyte threat group, which was seen targeting the same region and using similar tools in the past. Most early sightings of this activity were in Myanmar, but it now appears that the attackers are much more active in the

Philippines, where the number of known attacks has grown more than tenfold. This raises the question of whether this is caused by a rapid replication through removable devices or by an unknown infection vector, such as a watering-hole focusing on the Philippines.

We recently reported SideCopy campaigns attacking the Windows platform together with Android-based implants. These implants turned out to be multiple applications working as information stealers to collect sensitive information from victims' devices, such as contact lists, SMS messages, call recordings, media and other types of data. Following up, we discovered additional malicious Android applications, some of them purporting to be known messaging apps like Signal or an adult chat platform. These newly discovered applications use the Firebase messaging service as a channel to receive commands. The operator is able to control if either Dropbox or another, hard coded server is used to exfiltrate stolen files.

Other interesting discoveries

Expanding our research on the exploit targeting CVE-2021-1732, originally discovered by DBAPPSecurity Threat Intelligence Center and used by the Bitter APT group, we discovered another possible zero-day exploit used in the Asia-Pacific (APAC) region. Interestingly, the exploit was found in the wild as part of a separate framework, alongside CVE-2021-1732 as well as other previously patched exploits. We are highly confident that this framework is entirely unrelated to Bitter APT and was used by a different threat actor. Further analysis revealed that this Escalation of Privilege (EoP) exploit has potentially been used in the wild since at least November 2020. Upon discovery, we reported this new exploit to Microsoft in February. After confirmation that we were indeed dealing with a new zero-day, it received the designation CVE-2021-28310.

Various marks and artifacts left in the exploit mean that we are also highly confident that CVE-2021-1732 and CVE-2021-28310 were created by the same exploit developer that we track as "Moses". "Moses" appears to be an exploit developer who makes exploits available to several threat actors, based on other past exploits and the actors observed using them. To date, we have confirmed that at least two known threat actors have utilized exploits originally developed by Moses: Bitter APT and Dark Hotel. Based on similar marks and artifacts, as well as privately obtained information from third parties, we believe at least six vulnerabilities observed in the wild in the last two years have originated from "Moses". While the EoP exploit was discovered in the wild, we are currently unable to directly tie its usage to any known threat actor that we are currently tracking. The EoP exploit was probably chained together with other browser exploits to escape sandboxes and obtain system level privileges for further access. Unfortunately, we weren't able to capture a full exploit chain, so we don't know if the exploit is used with another browser zero-day, or coupled with exploits taking advantage of known, patched vulnerabilities.

In another, more recent investigation into the surge of attacks by APT actors against Exchange servers following the revelation of ProxyLogon and other Exchange vulnerabilities, we took note of one unique cluster of activity. It attracted our attention because the actor behind it seemed to have been active in compromising Exchange servers since at least December 2020, all the while using a toolset that we were not able to associate with any known threat group. During March, several waves of attacks on Exchange servers were made public, partially describing the same cluster of activity that we had observed. One of them, reported by ESET, contained an assessment that the actor behind this activity had access to the Exchange exploits prior to their public release, which aligns with our observations of the early activity of it last year. That said, none of the public accounts described sightings of the full infection chain and later stages of malware deployed as part of this group's operation. Adopting the name

Websiic, given publicly to this cluster of activity by ESET, we reported the TTPs of the underlying threat actor. Namely, we focused on the usage of both commodity tools like the China Chopper webshell and a proprietary .NET backdoor used by the group, which we dubbed “Samurai”, as well as describing a broader set of targets than the one documented thus far.

On 15 April, Codecov publicly disclosed that its Bash Uploader script had been compromised and was distributed to users between the 31 January and the 1 April. The Bash Uploader script is publicly distributed by Codecov and aims to gather information on the user’s execution environments, collect code coverage reports, and send them to the Codecov infrastructure. As a result, this script compromise effectively constitutes a supply-chain attack. The Bash uploader script is typically executed as a trusted resource in development and testing environments (including as part of automated build processes, such as continuous integration or development pipelines); and its compromise could enable malicious access to infrastructure or account secrets, as well as code repositories and source code. While we haven’t been able to confirm the malicious script deployment, retrieve any information on the compromise goals, or identify further associated malicious tools yet, we were able to collect one sample of a compromised Bash uploader script, as well as identify some possibly associated additional malicious servers.

An e-mail sent by Click Studios to its customers on 22 April informed them that a sophisticated threat actor had gained access to the Passwordstate automatic updating functionality, referred to as the in-place upgrade. Passwordstate is a password management tool for enterprises, and on 20 April, for a period of about 28 hours, a malicious DLL was included in the software updates. On 24 April, an incident management advisory was also released. The purpose of the campaign was to steal passwords stored in the password manager. Although this attack was only active for a short time, we managed to obtain the malicious DLLs and reported our initial findings. Nevertheless, it’s still unclear how the attackers gained access to the Passwordstate software to begin with. Following a new advisory published by Click Studio on 28 April, we discovered a new variant of the malicious DLL used to backdoor the Passwordstate password manager. This DLL variant was distributed in a phishing campaign, most likely by the same actor.

A few days after April’s Patch Tuesday updates from Microsoft (13 April), a number of suspicious files caught our attention. These files were binaries, disguised as “April 2021 Security Update Installers”. They were signed with a valid digital signature, delivering Cobalt Strike beacon modules. It is likely that the modules were signed with a stolen digital certificate. These Cobalt Strike beacon implants were configured with a hardcoded C2, “code.microsoft.com”. Contrary to a (now redacted) publication from the Qihoo 360 team revolving around this activity, we can confirm that there was no compromise of Microsoft’s infrastructure. In fact, an unauthorized party took over the dangling subdomain “code.microsoft.com” and configured it to resolve to their Cobalt Strike host, setup around 15 April. That domain hosted a Cobalt Strike beacon payload served to HTTP clients using a specific and unique user agent. According to Microsoft and the initial Qihoo notification, the impact in this case was very limited and didn’t affect unsuspecting visitors to this website because of the required unique user agent.

On April 14-15, Kaspersky technologies detected a wave of highly targeted attacks against multiple companies. Closer analysis revealed that all these attacks exploited a chain of Google Chrome and Microsoft Windows zero-day exploits. While we were not able to retrieve the exploit used for Remote Code Execution (RCE) in the Chrome web-browser, we were able to find and analyze an Escalation of Privilege (EoP) exploit used to escape the sandbox and obtain system privileges. The EoP exploit was fine-tuned to work against the latest and the most prominent builds of Windows 10 (17763 – RS5, 18362 – 19H1, 18363 – 19H2, 19041 – 20H1, 19042 – 20H2) and

it exploits two distinct vulnerabilities in the Microsoft Windows OS kernel. On April 20, we reported these vulnerabilities to Microsoft and they assigned CVE-2021-31955 to the Information Disclosure vulnerability and CVE-2021-31956 to the EoP vulnerability. Both vulnerabilities were patched on June 8, as a part of the June Patch Tuesday. The exploit-chain attempts to install malware in the system through a dropper. The malware starts as a system service and loads the payload, a "remote shell"-style backdoor which in turns connects to the C2 to get commands. So far, we haven't been able to find any connections or overlaps with a known actor. Therefore, we are tentatively calling this cluster of activity PuzzleMaker.

On April 16, we began hearing rumors about active exploitation of Pulse Secure devices from other researchers in the community. One day prior to this, the NSA, CISA, and FBI had jointly published an advisory stating that APT29 was conducting widespread scanning and exploitation of vulnerable systems, including Pulse Secure. For this reason, initial thoughts were that the two were related; and these were just rumors circulating the community about old activity that was being brought to light again. Following this, we were able to at least confirm that the initial rumors were part of a separate set of activities that had occurred between January and March and were not directly related to the advisory mentioned above. This new activity involved the exploitation of at least two vulnerabilities in Pulse Secure; one previously patched and one zero-day (CVE-2021-22893). We also became aware of affected organizations that were notified by a third party that they were potentially compromised by this activity. After exploitation, the threat actor proceeded to deploy a simple webshell to maintain persistence. On May 3, Pulse Secure delivered "out-of-cycle" update and workaround packages to provide a solution for the multiple vulnerabilities.

Cooperating with Check Point Research, we discovered an ongoing attack targeting a small group of individuals in Xinjiang and Pakistan, in regions mostly populated by the Uyghur minority. The attackers used malicious executables that collect information about the infected system and attempt to download a second-stage payload. The actor put considerable effort into disguising the payloads, whether by creating delivery documents that appear to be originating from the United Nations using up-to-date related themes, or by setting up websites for non-existing organizations claiming to fund charity groups. In our report, we examined the flow of both infection vectors and provided our analysis of the malicious artifacts we came across during this investigation, even though we were unable to obtain the later stages of the infection chain.

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 organisation 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 Q2 2021:

- We have reported several supply-chain attacks in recent months.. While some were major and have attracted worldwide attention, we observed equally successful low-tech attacks, such as BountyGlad, CoughingDown and the attack targeting Codecov.
- APT groups mainly use social engineering to gain an initial foothold in a target network. However, we've seen a rise in APT threat actors leveraging exploits to gain that initial foothold – including the zero-days

developed by the exploit developer we call “Moses” and those used in the PuzzleMaker, Pulse Secure attacks and the Exchange server vulnerabilities.

- APT threat actors typically refresh and update their toolsets: this includes not only the inclusion of new platforms but also the use of additional languages as seen by WildPressure’s macOS-supported Python malware.
- As illustrated by the campaigns of various threat actors – including BountyGlad, HotCousin, GoldenJackal, Scarcruft, Palwan, Pulse Secure and the threat actor behind the WebDav-O/Mail-O implants – geo-politics continues to drive APT developments.

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.
