APT trends report Q3 2021

securelist.com/apt-trends-report-q3-2021/104708

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 Q3 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.

The most remarkable findings

The SolarWinds incident reported last December stood out because of the extreme carefulness of the attackers and the high-profile nature of their victims. The evidence suggests that the threat actor behind the attack, DarkHalo (aka Nobelium), had spent six months inside OrionIT's networks to perfect their attack. In June, more than six months after DarkHalo had gone dark, we observed the DNS hijacking of multiple government zones of a CIS member state that allowed the attacker to redirect traffic from government mail servers to computers under their control – probably achieved by obtaining credentials to the control panel of the victims' registrar. When victims tried to access their corporate mail, they were redirected to a fake copy of the web interface. Following this, they were tricked into downloading previously unknown malware. The backdoor, dubbed Tomiris, bears a number of similarities to the second-stage malware, Sunshuttle (aka GoldMax), used by DarkHalo last year. However, there are also a number of overlaps between Tomiris and Kazuar, a backdoor that has been linked to the Turla APT threat actor. None of the similarities is enough to link Tomiris and Sunshuttle with high confidence. However, taken together they suggest the possibility of common authorship or shared development practices. You can read more about our findings here.

Disclaimer: when referring to APT groups as Russian-speaking, Chinese-speaking or "speaking" other languages, we refer to various artefacts used by the groups (such as malware debugging strings, comments found in scripts, etc.) containing words in these languages, based on the information we obtained directly or which was otherwise publicly known and reported widely. The use of certain languages does not necessarily indicate a specific geographic relation but rather points to the languages that the developers behind these APT artefacts use.

Russian-speaking activity

This quarter we identified several malicious infection documents, droppers and implants that are typical of Gamaredon; and which may suggest an ongoing malicious campaign against the Ukrainian government, possibly active since May. We could not precisely identify the associated infection chains, as we could only retrieve parts of them from any live exploitation context. However, we were able to attribute the activity with medium to high confidence to Gamaredon. Our private report gave details about the various droppers along with decoder scripts, as well as analysis of the DStealer backdoor and the large infrastructure we observed associated with the campaign.

ReconHellcat is a little-known threat actor that was spotted publicly in 2020. The first accounts of its activity date back to March last year, in which archives carrying COVID-related decoy file names that contained a malicious executable were described in a tweet by MalwareHunterTeam. The malicious implant within the archive, dubbed

BlackWater, would in turn drop and open a lure document and subsequently contact Cloudflare Workers as C2 servers – an unusual choice that is not often encountered in use by other actors. Since the first sightings of this intrusion set, similar TTPs have been used as part of other attacks that were covered by QuoIntelligence, suggesting the underlying actor is operating in a targeted fashion while going after high-profile government-related targets. This activity seems to have continued and stretched into 2021, when we spotted a set of recent attacks using the same techniques and malware to gain a foothold in diplomatic organizations based in Central Asia. In our private report we described this activity, with an eye to the various changes the actor made to elements in the infection chain, likely as a result of previous public exposure of its activity.

Since then, we have identified additional documents operated by ReconHellcat; and a new campaign emerged from August through to September with an evolved infection chain. This campaign was also covered by researchers at Zscaler in a blog post. Some of the changes introduced in the renewed activity include relying on Microsoft Word templates (.dotm) for persistence, instead of the previously used Microsoft Word add-ons

(.wll). Nevertheless, some TTPs remain unchanged, as the new infection chain still delivers the same final implant, the Blacksoul malware, and still uses Cloudflare Workers as C2 servers. ReconHellcat goes after government organizations and diplomatic entities related to countries in Central Asia, such as Tajikistan, Kyrgyzstan, Pakistan and Turkmenistan. Additionally, we identified victims from two countries we did not encounter in the previous wave of attacks: Afghanistan and Uzbekistan. We assess, with a medium level of confidence, that ReconHellcat is a Russian-speaking threat actor.

Chinese-speaking activity

An APT threat actor, suspected to be HoneyMyte, modified a fingerprint scanner software installer package on a distribution server in a country in South Asia. The APT modified a configuration file and added a DLL with a .NET version of a PlugX injector to the installer package. On installation, even without network connectivity, the .NET injector decrypts and injects a PlugX backdoor payload into a new svchost system process and attempts to beacon to a C2. Employees of the central government in a country in South Asia are required to use this biometric package to support recording attendance. We refer to this supply-chain incident and this particular PlugX variant as SmudgeX. The Trojanized installer appears to have been staged on the distribution server from March to June.

During 2020 and 2021, we detected a new ShadowPad loader module, dubbed ShadowShredder, used against critical infrastructure across multiple countries, including but not limited to India, China, Canada, Afghanistan and Ukraine. Upon further investigation we also discovered additional implants deployed through both ShadowPad and ShadowShredder, such as Quarian backdoor, PlugX, Poison Ivy and other hack tools. Notably, the Quarian backdoor and Poison Ivy showed similarities with previous IceFog activity targeting users in Central Asia. ShadowPad is a highly sophisticated, modular cyberattack platform that APT groups have used since 2017. We published a blog post at that time detailing the technical details of ShadowPad and its supply-chain attack campaign after its initial discovery, when it was deployed by an APT group known as Barium or APT41. In Q1 2020, we published private reports with the discovery of x64 ShadowPad dropper samples. The loader module used a unique anti-analysis trick that involves the loader module checking whether it’s been loaded via the specific EXE file by looking inside the memory space of the loader module for some hard coded bytes before the decryption of embedded shellcode. The ShadowShredder loaders we discovered more recently don’t make use of this technique, incorporating a new obfuscation method instead. Our report discusses the technical analysis of ShadowShredder and related activities using second-stage payloads linked to ShadowShredder and ShadowPad.

ESET published a blog post in June describing a campaign targeting foreign affairs ministries and telecoms companies in Africa and the Middle East by an actor they dubbed BackdoorDiplomacy and categorized as Chinese-speaking. We link this activity with high confidence to an actor we’re tracking under the alias CloudComputating, known to target high-profile entities in the Middle East. In their investigation ESET discovered a Quarian Linux variant sample sharing a C2 server with Windows variants, which was reportedly deployed by exploiting a known RCE vulnerability (CVE-2020-5902) in F5 Networks' BIG-IP traffic management user interface or configuration utility. The same Quarian ELF binary was also mentioned being deployed on an F5 BIG-IP server in a SANS ISC report in July 2020, one year earlier. Our private research report expanded the analysis of the Quarian Linux variant and its ties to the Windows version.

Last year, we described a campaign attributed to CloudComputating in which the APT actor exploited a known vulnerability to compromise publicly exposed Microsoft Exchange servers and infected them with the China Chopper web shell. The malicious payload was then used to upload additional malware, usually the Quarian backdoor that has been seen in use by Chinese-speaking actors since around 2010. This campaign affected Ethiopia, Palestine and Kuwait. ESET's blog post (see above) allowed us to link their campaign to the one we described in June last year and extend our previous investigation to find new unknown variants and victims. Our private report covered the version ESET dubbed Turian, two other formerly unknown Quarian versions, an overview of a builder component used to generate malicious Quarian libraries and an extended list of IoCs.

ExCone is a set of attacks that started in mid-March against targets in the Russian Federation. The attackers exploited Microsoft Exchange vulnerabilities to deploy a previously unknown Trojan that we dubbed FourteenHI. During our previous analysis, we found multiple ties in infrastructure and TTPs to the ShadowPad malware and UNC2643 activity. However, we were unable to attribute the attack to any known actor. Following our first report, we continued to monitor this cluster of activities and we found many other variants, which extended our knowledge of the attackers and the campaign itself. We found new malware samples used against a large number of targets, with victims in Europe, Central Asia and Southeast Asia. We also observed a cluster of publicly reported activities by various other vendors that we are able to link to ExCone with high confidence. Finally, we found a new malware sample that allows us to link ExCone to the SixLittleMonkeys APT group with low confidence. Specifically, we found a victim compromised by FourteenHI and another unknown backdoor. This new "unknown backdoor" presents similarities to both FourteenHI and Microcin, a Trojan exclusively attributed to SixLittleMonkeys that we described in other reports available on our Threat Intelligence Portal.

This quarter, we also pursued our investigations of what is widely known to be Chinese-speaking activities in South Asia. We discovered another set of TTPs targeting aerospace and defense research establishments in India between 2019 and the end of June 2021, featuring two previously unknown backdoors: LGuarian and HTTP_NEWS. The former appears to be a new variant of the Quarian backdoor, which this attacker also uses. Thanks to our telemetry, we obtained extensive information on the attacker's post-exploitation process and were able to provide a detailed picture of the various tools they use during this phase, as well as actions performed on the victims' machines. This allowed us to gather a wide number of malware samples and subsequently discover a significant part of the attacker's infrastructure.

On June 3, Check Point published a report about an ongoing surveillance operation targeting a Southeast Asian government, and attributed the malicious activities to a Chinese-speaking threat actor named SharpPanda. We published a private report providing additional data on the associated malicious activities and tools, based on our own visibility of this threat.

In April, we investigated a number of malicious installer files mimicking Microsoft Update Installer files, signed with a stolen digital certificate from a company called QuickTech.com. These fake installers exhibited very convincing visuals, which reflect the amount of effort that went into making them look legitimate. The final payload, which was a Cobalt Strike beacon module, was also configured with a "microsoft.com" subdomain C2 server. The C2 domain code.microsoft[.]com was a dangling DNS subdomain, which was registered by the attackers around April 15 to masquerade as the official Visual Studio Code website. The victims were tricked into downloading and executing these installers on their machines through a fake Microsoft Update Catalog webpage, which was also hosted on another dangling subdomain of "microsoft.com". While investigating the malicious installer files, we came across other malicious binaries which, based on various indications, we assume were developed and used by the same threat actor, active since at least January and up until June. Our private report provided an analysis of the extended toolset of this threat actor, which we named CraneLand.

In July, we identified a suspicious JavaScript (JS) inclusion on two websites that openly criticize China and which appear to be legitimate. The obfuscated JS is loaded from a remote domain name that impersonates the Google brand and initiates a malicious JS payload chain. The compromised websites still include the JS, but we could not link any other malicious activities or infrastructure to this watering-hole attack. The malicious JS does not seem to fit traditional cybercriminal goals, and its activities are quite unusual compared to those we have observed in other watering-hole attacks. We believe the malicious JS payloads are aimed at profiling and targeting individuals from Hong Kong, Taiwan or China. Any connections to the described malicious domains should be carefully reviewed to look for subsequent malicious activities.

Middle East

Lyceum is a threat group operating against high-profile targets in the Middle East since at least 2018. This year, we uncovered significant activity by the group focused on Tunisia's aviation and telecoms sectors. Throughout this campaign the attackers demonstrated vigor and agility while developing two new C++ based malware implants that we dubbed Kevin and James. Both relied on techniques and communication protocols from older malware used by the group and coined DanBot. Following our report on this activity and the corresponding deployment of protection against the group's newly found implants, we observed recurring attempts by the attackers to deploy fresh samples that were not specified in our former report. Some of these samples revealed that the attackers have also made use of two new C2 domains, likely as means to bypass security mechanisms that mitigated communication to the already known domains. Such effort characterizes the group's persistence in compromising a targeted organization, and shows that it has not ceased to operate after being discovered, a fact that can be reinforced through yet another cluster of activity by the group that was recently exposed publicly. You can read more about our findings in the 'Lyceum group reborn' article.

Southeast Asia and Korean Peninsula

In June, we observed the Lazarus group attacking the defense industry using the MATA malware framework. Historically, Lazarus used MATA to attack various industries for cybercrime-like intentions: stealing customer databases and spreading ransomware. However, here we saw Lazarus using MATA for cyber-espionage purposes. The actor delivered a Trojanized version of an application known to be used by their victim of choice, representing a known characteristic of Lazarus. Executing this application starts a multi-staged infection chain beginning with a downloader. This downloader fetches additional malware from compromised C2 servers. We were able to acquire several MATA components, including plugins. The MATA malware discovered in this campaign has evolved compared to previous versions and uses a legitimate, stolen certificate to sign some of its components. Through this research, we discovered a stronger connection between MATA and the Lazarus group, including the fact that the downloader malware fetching MATA malware showed ties to TangoDaiwbo, which we had previously attributed to the Lazarus group.

We have also discovered Lazarus group campaigns using an updated DeathNote cluster. The first involved an attack on a think tank in South Korea in June. The second was an attack on an IT asset monitoring solution vendor in May. Our investigation revealed indications that point to Lazarus building supply-chain attack capabilities. In one case, we found that the infection chain stemmed from legitimate South Korean security software executing a malicious payload; and in the second case, the target was a company developing asset monitoring solutions in Latvia, an atypical victim for Lazarus. The DeathNote malware cluster consisted of a slightly updated variant of BLINDINGCAN, malware previously reported by the US CISA (Cybersecurity & Infrastructure Security Agency). BLINDINGCAN was also used to deliver a new variant of COPPERHEDGE, also reported in a CISA article. We had previously reported our initial finding of COPPERHEDGE in January 2020. As part of the infection chain, Lazarus used a downloader named Racket that they signed using a stolen certificate. As a result of taking over the attacker's infrastructure with a local CERT, we had a chance to look into several C2 scripts associated with the DeathNote cluster. The actor compromised vulnerable web servers and uploaded several scripts to filter and control the malicious implants on successfully breached victim machines.

The Kimsuky group is currently one of the most active APT groups. The threat actor is known for focusing on cyber-espionage but occasionally conducts cyberattacks for financial gain. Like other APT groups that constitute a big umbrella, Kimsuky contains several clusters: BabyShark, AppleSeed, FlowerPower, and GoldDragon.

Each cluster utilizes different methodologies and has different characteristics:

- BabyShark relies heavily on scripted malware and compromised web servers for C2 operations;
- AppleSeed uses a unique backdoor named AppleSeed;
- FlowerPower uses PowerShell scripts and malicious Microsoft Office documents;
- GoldDragon is the oldest cluster, closest to the original Kimsuky malware.

However, these clusters also show several overlaps. In particular, GoldDragon and FlowerPower share a strong connection in their C2 infrastructure. However, the other clusters also have a minor connection to the C2 infrastructure. We assess that BabyShark and AppleSeed are operating with different strategies.

Back in May, we published a report about the freshly discovered activity of Andariel. In this campaign, a broad spectrum of industries located in South Korea were targeted with custom ransomware. During our research, we discovered that the actor was using two vectors to compromise targets. The first was the use of weaponized Microsoft Office documents with malicious macros. At the time of our original report, the second vector was still unknown but we discovered artifacts containing the path of the tool ezPDF Reader, developed by a South Korean software company named Unidocs. We were missing clear evidence that the attack leveraged a vulnerability within this software, and to solve this mystery we decided to audit the binary of this application. Our analysis of the software led us to discover a remote code execution vulnerability in ezpdfwslauncher.exe that can be leveraged to break into computers on the network with ezPDF Reader without any user interaction. We assess with high confidence that the Andariel group used the same vulnerability in its attacks. After this discovery, we contacted the developers of Unidocs and shared the details of this vulnerability with them. It was fixed as CVE-2021-26605.

This quarter we described activity associated with the Origami Elephant threat actor (aka DoNot team, APT-C-35, SECTOR02) observed from the beginning of 2020 and continuing through to this year. Origami Elephant continues to utilize the known Backconfig (aka Agent K1) and Simple Uploader components, but we have also identified lesser-known malware named VTYREI (aka BREEZESUGAR) used as a first-stage payload. Additionally, we observed a unique technique of encoding the remote template used in the malicious documents that we have not seen utilized by other threat actors. Victimology is consistent with past operations: the adversary continues to focus on the South Asia region with special interest in government and military entities mainly in Pakistan, Bangladesh, Nepal and Sri Lanka.

We also tracked Origami Elephant activity targeting Android mobile phones from the end of 2020 up to the time of our report, picking up where we left off with last year’s report. We see that the infrastructure is still active, communicating with the same malware we previously reported, albeit with a few changes in code obfuscation. The targeting remained the same as last year, with victims located in the South Asian region: India, Pakistan and Sri Lanka in particular. The actor revised the infection chain compared with last year's campaign. Instead of delivering a downloader stager, we observed the Android Trojan being directly delivered. This is done via links to malicious landing pages or direct messages via some instant messaging platform such as WhatsApp. The samples we analyzed mimicked various applications such as private messaging, VPN, and media services. Our report covered the current state of Origami Elephant's activities against Android devices and provided additional IoCs linked to both the latest and historical group activities. Scanning the internet with available clues from our previous research, we are able to discover newly deployed hosts, in some cases even before they become active.

Other interesting discoveries

In September, we provided an overview of the FinSpy PC implant. This covered not only the Windows version, but also Linux and macOS ones, which share the same internal structure and features. FinSpy is a notorious surveillance toolset that several NGOs have repeatedly reported being used against journalists, political dissidents and human rights activists. Historically, its Windows implant was represented by a single-stage spyware installer. This version was detected and researched several times up to 2018. Since then, we have observed a decreasing detection rate for FinSpy for Windows. While the nature of this anomaly remained unknown, we began detecting some suspicious installer packages backdoored with Metasploit stagers. We were unable to attribute these packages until the middle of 2019 when we found a host that served these installers among FinSpy Mobile implants for Android. Over the course of our investigation, we found out that the backdoored installers are nothing more than first-stage implants that are used to download and deploy further payloads before the actual FinSpy Trojan. Apart from the Trojanized installers, we also observed infections involving usage of a UEFI or MBR bootkit. While the MBR infection has been known since at least 2014, details of the UEFI bootkit were only publicly revealed for the first time in our article. We decided to share some of our unseen findings about the actual state of FinSpy implants. You can read our public report here.

Towards the end of Q3, we identified a previously unknown payload with advanced capabilities, delivered using two infection chains to various government organizations and telecoms companies in the Middle East. The payload makes use of a Windows kernel-mode rootkit to facilitate some of its activities and is capable of being persistently deployed through an MBR or a UEFI bootkit. Interestingly enough, some of the components observed in this attack have been formerly staged in memory by Slingshot agent on multiple occasions, whereby Slingshot is a post-exploitation framework that we covered in several cases in the past (not to be confused with the 'Slingshot' APT). It is mainly known for being a proprietary commercial penetration testing toolkit officially designed for red team engagements. However, it's not the first time that attackers appear to have taken advantage of it. One of our previous reports from 2019 covering FruityArmor's activity showed that the threat group used it to target organizations across multiple industries in the Middle East, possibly by leveraging an exploit in Skype as an infection vector. In a recent private intelligence report, we provided a drill-down analysis of the newly discovered malicious toolkit that we observed in tandem with Slingshot and how it was leveraged in clusters of activity in the wild. Most notably, we outlined some of the advanced features that are evident in the malware as well as its utilization in a particular long-standing activity against a high profile diplomatic target in Iraq.

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 Q3 2021:

- We continue to see supply-chain attacks, including those of SmudgeX, DarkHalo and Lazarus.
- In this quarter we focused on researching and dismantling surveillance frameworks following malicious activities we detected. These include FinSpy and the use of advanced and highly capable payloads staged by a commercial post-exploitation framework known as Slingshot. These tools contain powerful covert capabilities, such as the use of bootkits for persistence. Bootkits remain an active component of some high profile APT attacks, notwithstanding various mitigations Microsoft has added to make them much less easy to deploy on the Windows operating system.
- We observed an abnormal spike in activity coming from what is widely known to be Chinese-speaking threat groups this quarter, particularly when compared to the start of the year. By contrast, we have seen a decrease in activity in the Middle East this quarter.
- Social engineering remains a key method for initiating attacks; but also exploits (CloudComputating, Origami Elephant, Andariel), including exploiting firmware vulnerabilities.
- As illustrated by the campaigns of various threat actors – including Gamaredon, CloudComputating, ExCone, Origami Elephant, ReconHellcat, SharpPanda – 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.