



Ankura Cyber Threat Intelligence Bulletin

January 2022

CONTENTS

Observations..... 3

The Ever-Evolving Log4Shell Vulnerability 3

Russian Activity Surrounding the New Year 4

Meta Targets Phishing Campaigns and Cyber Mercenaries..... 5

Gophers Going Dark 7

Threat Actor of the Month 8

Trending IOCs 10



Observations

Over the past sixty (60) days, the Ankura Cybersecurity team has worked with clients to solve cybersecurity challenges involving the rampantly exploited Log4Shell vulnerability, recent security changes within Meta (Facebook), and Russian government crackdowns against malicious cyber-activity, as well as a piece on the exponential growth seen in the use of obscure coding languages by threat actors.

For this month's report, Ankura's Cyber Threat Investigations and Expert Services (CTIX) team has compiled detailed metrics surrounding the technical, and legal tactics employed by Meta to pursue and prosecute cyber mercenaries leveraging spyware on Meta's platforms. Additionally, malware developers are beginning to leverage the Golang coding language to bypass traditional security measures and personnel who have historically been in contest with threat actors who were using languages that the security researchers were already quite familiar with. For this issue's threat actor of the month, the CTIX team is reporting on the tactics, techniques, and procedures (TTPs) and activity of the MuddyWater advanced persistent threat (APT) group.

THE EVER-EVOLVING LOG4SHELL VULNERABILITY

Disclosed back in early December, Log4Shell (CVE-2021-44228) is a vulnerability in Apache Log4j, which is a Java library used to add log management capabilities to Java web and desktop applications. Quickly gaining recognition, since targeting the vulnerability has become an extremely widespread technique. For example, the cybersecurity company Akamai Technologies Inc. reported on tracking 10 million attempts to exploit the Log4j vulnerability on an hourly basis in the U.S. alone. Threat actors are continuing to use the vulnerability to target the retail sector above all others, and the technology, financial-services, and manufacturing industries have also observed an increase of these types of attacks. The CTIX team has closely monitored this situation as larger threat actors have started to target this new vulnerability. Examples include nation sponsored groups from China, Russia, North Korea, Iran, and Turkey, who have started to target the vulnerability in recent campaigns.¹

Ransomware groups both big and small have also started to target victims by leveraging the Log4Shell vulnerability. The first ransomware group to target Log4Shell, was a newly emerging ransomware group calling themselves Khonsari. Khonsari ransomware demands left no way to contact the operators, even if the victim intended on paying. For now, this group has only targeted game servers, having their ransomware act more as a wiper and ultimately forcing the victim to shut down their servers. While another more infamous group CONTI, has now built up a holistic attack chain.² Targeting specific vulnerable Log4J2 VMware vCenter for lateral movement directly from the compromised network, resulting in vCenter access affecting U.S. and European victim networks from the pre-existent Cobalt Strike sessions.

VMWare Horizon is one of many products made by VMWare which has been affected by the Log4j vulnerabilities. This product from VMWare has drawn particular interest from cybercriminals since Log4js vulnerabilities have been disclosed due to the number of implementations that have remained unpatched. Recently, Prophet Spider, a well-known access broker for ransomware groups has recently been seen exploiting VMWare Horizon products. VMWare has issued extensive guides and have also posted more than enough information for these products not to be vulnerable to Log4j, it simply comes down to end

¹ <https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/>

² <https://threatpost.com/conti-ransomware-gang-has-full-log4shell-attack-chain/177173/>



users of the products failing to implement critical security updates. It is also worth noting that the exploit within the VMware Horizon product can be reliably detected by monitoring the child processes of “ws_TomcatService.exe”.³ Exploitation of this process spawns either “cmd.exe” or “powershell.exe” as a child process.

SolarWinds and ZyXEL devices are two (2) more types of products that have been exploited due to the Log4Shell vulnerability. The most notable attack that occurred was when a threat actor utilizing the Log4Shell exploit in conjunction with a zero-day vulnerability that affects SolarWinds Serv-U file sharing server. This zero-day vulnerability can be tracked as CVE-2021-35247.⁴ Threat actors utilizing both vulnerabilities would first deploy an exploit for the SolarWinds Serv-U server; this is an input validation issue within the web login screen for Serv-U. Attackers utilizing the exploit are able to bypass input validation utilizing nonstandard characters. Once login to the server is bypassed, the Log4Shell exploit is utilized to take control of the Serv-U server. ZyXEL devices have also been targeted by the Mirai botnet. There is speculation that ZyXEL devices were targeted due to them publishing a blog where they stated they were impacted by the Log4Shell vulnerability. Although Apache has released a patch for the Log4j library, attacks are still expected to continue as applications utilizing the library also need to deploy their updates.

Threat actors may not be the only concern for companies when it comes to Log4Shell. The U.S. Federal Trade Commission (FTC) released a statement earlier this month detailing that it intends to start legal actions and sue companies who leak consumer data by not patching applications vulnerable to the Log4Shell vulnerability. “The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future,” the agency said during the press release.⁵ The FTC highlighted the Federal Trade Commission Act and the Gramm Leach Bliley Act allow it to take actions against companies that ignore their duties to their own consumers. This wouldn’t be the first time the FTC would be taking legal action against companies that fail to patch security flaws; in 2017, the FTC filed a lawsuit against Equifax for experiencing a breach that affected more than 147 million Americans. With the Log4j library being so widely used, we are sure to encounter several new techniques on targeting Log4Shell.

RUSSIAN ACTIVITY SURROUNDING THE NEW YEAR

Over the past weeks, analysts have seen a significant increase in cyber activity throughout Russia and from Russian-backed threat intelligence operatives. With growing tensions between Ukraine and Russia, after a meeting between the United States and Russia over militarization along the Russia/Ukraine border occurred, United States intelligence agencies issued Alert AA22-011A.⁶ The alert issued warnings for critical infrastructure organizations, citing threats by Russian nation-state threat groups. Agencies warned against common but highly effective tactics allowing threat actors to breach a network, including unpatched vulnerabilities, sophisticated phishing attacks, spear-phishing, executive-whaling, brute force attacks, and more. Throughout the past few years, Russian threat actors commonly utilized numerous highly vulnerable exploits within Microsoft Exchange, F5 Big-IP, Kibana, Oracle WebLogic, and FortiGate VPN applications in order to compromise their target(s). The latest critical infrastructure cyberattack from Russian threat

³ <https://blogs.blackberry.com/en/2022/01/log4u-shell4me>

⁴ <https://nvd.nist.gov/vuln/detail/CVE-2021-35247>

⁵ <https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>

⁶ <https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>



actors was against Ukrainian energy companies, which ultimately lead to massive power blackouts and outages throughout the country.

In addition, the Federal Security Service of the Russian Federation (FSB) reported earlier this month that they "shut down the REvil ransomware gang after U.S. authorities reported on [their] leader".⁷ Russian agents and local authorities raided several properties and detained fourteen (14) individuals suspectedly linked to the REvil organization, along with seizing 426 million rubles (~\$5.5 million), \$600,000, 500,000 euros (~\$570,000), computer equipment, luxury cars, and cryptocurrency wallets; totaling over \$6.6 million.⁸ Of the fourteen (14) arrested, eight (8) have been identified and detained on current charges of illegal circulation of means of payment, carding, and counterfeit documentation. According to the Criminal Code of the Russian Federation, these listed charges carry a prison sentence of five (5) to eight (8) years, with the possibility for additional fines from the courts. The ranks of those arrested within the REvil organization have not yet been confirmed by authorities, however an anonymous White House official came forward and stated, "we understand that one of the individuals who was arrested today [January 14] was responsible for the attack against Colonial Pipeline last spring".⁸

Russian FSB agents and local authorities have also arrested the leader of the Infraud Organization, a sophisticated threat group responsible for over \$560 million in stolen payment losses throughout their seven (7) year lifespan.⁹ This is not the first time the Infraud Organization has come under fire by authorities. Back in 2018, the United States Department of Justice indicted thirty-six (36) suspects in connection with the group, leading to thirteen (13) arrests including the threat group's portal administrator. The FSB arrested a total of four (4) individuals from the associated raids including the suspected leader of the group, Andrey Novak. Currently, Novak has been detained by authorities and will be held for two (2) months while the investigation plays out, and the remaining three (3) individuals, Kirill Samokutyaev, Konstantin Vladimirovich, and Mark Avramovich Bergman, have been subjected to house arrest. This is just one (1) of many apprehensions conducted between United States agencies and Russian authorities over the past six (6) months, which has led to the arrest of several key players in varying threat groups. Researchers expect more arrests, seizures, and raids in the coming months as both countries crack down on cyber criminals.

META TARGETS PHISHING CAMPAIGNS AND CYBER MERCENARIES

According to The Record in late December of 2021, a lawsuit was filed by Meta, formally known as Facebook, against operators that allegedly have control of approximately forty thousand malicious phishing sites.¹⁰ Meta has also reported damages of approximately five-hundred thousand U.S. dollars. The lawsuit describes that Meta believes approximately one hundred individuals have created said phishing sites with fraudulent login pages of famous social media platforms including Facebook Messenger, Instagram, and WhatsApp.¹⁰ "This phishing scheme involved the creation of more than 39,000 websites", said Jessica Romero, Meta's director of Platform Enforcement and Litigation.¹¹

The individuals responsible for the formation of the phishing sites used an application called Ngrok, a program which is used to expose local server ports to the internet. The application was used as a relay

⁷ <https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/>

⁸ <https://therecord.media/biden-official-one-of-arrested-russian-hackers-carried-out-the-colonial-pipeline-attack/>

⁹ <https://www.bleepingcomputer.com/news/security/russia-arrests-leader-of-infraud-organization-hacker-group/>

¹⁰ <https://therecord.media/meta-facebook-sues-operators-of-39000-phishing-sites/>

¹¹ <https://www.bleepingcomputer.com/news/security/meta-sues-people-behind-facebook-and-instagram-phishing/>



service to prevent the victims' detection. This method masked the identities of both the online providers as well as the location of hackers using these phishing sites.¹¹ Following the great monetary loss due to the number of damages incurred from this attack, Meta took measures to respond to the incident as well as mitigate future attacks.

Following the phishing attack on Meta, steps were taken to de-platform seven (7) of the many cyber mercenaries operating in the cybersecurity realm. According to Bleeping Computer, in October 2019, Facebook filed a similar lawsuit against the domain name "Online NIC" for "allowing the registration of lookalike domains used in malicious campaigns."¹¹ Again in March of 2020, Facebook sued the domain name provider NameCheap and charged them with "registering domain names that aim to deceive people by pretending to be affiliated with Facebook Apps."¹¹ Meta alerted about fifty thousand Facebook and Instagram users that their accounts have been compromised as well as removed one thousand five hundred Facebook and Instagram accounts that linked to those firms.¹² Meta believes such firms operated tools and created fraudulent personas or "sock puppets" and were successful through social engineering and delivery of malware through phishing sites. Facebook took down these phishing sites and addressed the disadvantages and downfalls of the surveillance-for-hire industry.

Surveillance-for-hire is an industry that targets specific individuals to collect information and use that information to compromise devices and accounts found on the web.¹³ Providers were found to be in several different countries such as China, Israel, India, and North Macedonia. The seven (7) cyber mercenaries banned by Meta include Cobwebs Technologies, Cognyte, Black Cube, Blue Hawk CI, BellTroX, Cytrox, and an unknown Chinese entity.¹⁴ About two hundred accounts were removed from Cobwebs Technologies, an entity that was founded in Israel with offices located in the United States that sells access to platforms and enables reconnaissance across the internet to include public social media sites as well as "dark web" sites. About one hundred accounts were removed from Cognyte, another cyber mercenary based in Israel and sells access to platforms enabling fake accounts for Facebook, Instagram, and YouTube. Black Cube had three hundred accounts removed with offices located in the United Kingdom, Spain, and Israel. This mercenary group provides surveillance services to include gathering of information and creating fraudulent personas. Bluehawk CI is a firm based in Israel with other offices in the United States and the United Kingdom and sells surveillance for hire activities and had another hundred accounts removed. BellTroX is used to send malicious links, use social engineering, and impersonate legitimate politicians, and about four hundred accounts were removed by Meta. Cytrox is based in North Macedonia and had three hundred accounts on Facebook and Instagram removed. This cyber mercenary develops exploits as well as sells tools used for surveillance and malware to enable compromise to iOS and Android devices. The very last cyber mercenary mentioned was an unknown Chinese entity responsible for developing surveillance spyware for Android, iOS, and Windows. This unknown entity had one hundred Instagram and Facebook accounts removed.¹⁴ Meta explained that given the level of severity for surveillance for hire violations, the cyber mercenaries had to be banned from their services. "To help disrupt these activities, we blocked related internet infrastructure and issued Cease and Desist letters, putting them on notice that their targeting of people has no place on our platform."¹⁵ Meta has taken measures to respond

¹² <https://thehackernews.com/2021/12/facebook-bans-7-cyber-mercenaries.html>

¹³ <https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/>

¹⁴ <https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf>

¹⁵ <https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/>



to this incident and shared these discoveries with various security researchers and other platforms with policy makers so they can also take appropriate action.

The takedown of phishing sites and banning cyber mercenaries involved in the attack is a huge step in the direction of mitigation of social engineering and responding to similar incidents in the future. Social engineering and phishing should be taken extremely seriously because it can cause a great deal of financial losses, negative reputation, theft of sensitive and critical information and much more. Measures are being taken by big social media companies such as Meta to mitigate these types of attacks and prevent any other attacks in the future. Meta also explained that these efforts and actions being taken are only going to benefit the greater majority in the community if everyone collaborates on findings and monitoring. Efforts to continue to stop cyber mercenaries and such attacks are only going to be effective if everyone in the community such as policy makers, government agencies, and other service providers work together.

GOPHERS GOING DARK

Since its first public release in 2012, Golang (a.k.a. Go) has quickly gained traction amongst developers and threat actors alike. In fact, CrowdStrike has recently reported that from June through August 2021 analysts saw an 80% increase in malware written in Golang¹⁶. This increase stems from the several advantages Go offers to its developers. These advantages include Golang's barrier to entry, its ability to bundle dependencies into a single binary, and most importantly its ability to run cross-platform.

The first major benefit of using Golang would be the barrier to entry and its development experience. Golang was created to be syntactically similar to C like languages¹⁷. The idea behind this was that Google wanted its developers to spend as little time learning and implementing a new language. Coincidentally, the most common language used to write malware happens to be C¹⁸. In other words, no matter the level of expertise, a malware developer will spend less time learning the language and more time writing malware. C is often preferred since it is a mid-level language, meaning it bridges the gap between machine level languages (Assembly) to high level languages.

Golang also comes with some great tooling. An example of this would be its ability to cross compile. With a single command (GOOS and GOARCH) Golang can output a binary for several operating systems, most notably Linux, Windows, and macOS¹⁷. Considering that malware developers do not get to choose where their program is run, the ability to create multiple binaries for various operating systems is a huge benefit. This benefit also extends into the actual code base as well. In a recent report, CrowdStrike found an 85% similarity between the Linux and Windows samples of the TellYouThePass ransomware¹⁹.

As previously mentioned, Golang is a compiled language, meaning the code is converted directly to machine code a system can execute. Considering this fact, it is important to note that Golang includes its libraries inside the binary¹⁷. Albeit great for the threat actors, since they would not run into any issues with dependencies, this causes headaches for analysts. This is because some security tools are unable to handle large binaries²⁰. Another issue with these binaries is how threat actors can strip down useful

¹⁶ https://www.crowdstrike.com/blog/financial-motivation-drives-golang-malware-adoption/?&web_view=true

¹⁷ <https://go.dev/talks/2012/splash.article>

¹⁸ <https://www.cybrary.it/blog/top-programming-languages-for-malware-analysis/#:~:text=As%20one%20of%20the%20older,more%20memory%20efficient%20than%20others>

¹⁹ <https://www.crowdstrike.com/blog/tellyouthepass-ransomware-analysis-reveals-modern-reinterpretation-using-golang/>

²⁰ <https://cujo.com/reverse-engineering-go-binaries-with-ghidra/>



information inside the binary, such as function names. This lack of function names often leads to longer analysis times when reverse engineering the code²⁰.

Golang was created to address several issues Google experienced with its own development efforts. Things such as barrier to entry were considered, thus a C like syntax was needed. Threat actors also preferred the use of C, making a migration to Golang almost effortless. Golang is a modern language and with that comes the added benefit of updated tooling. Updated tooling such as the build commands GOOS and GOARCH which enable developers (and threat actors) to quickly compile a binary for several popular operating systems. Lastly, Golang is a compiled language that packages its dependencies with the code. The result of this is a larger binary that takes more effort from analyst to reverse engineer.

THREAT ACTOR OF THE MONTH

The MuddyWater (aka Seedworm, Temp.Zagros, Static Kitten) advanced persistent threat (APT) has been an active group since 2017 conducting espionage operations across the Middle East. Their attacks utilize in-memory malware, living off the land (LotL) techniques, deploy Powershell malware, tunneling into computers they infect in order to spread across the network. Initial attributions correctly identified MuddyWater to be an Iranian threat group, but in 2022, the U.S. Cyber Command (USCYBERCOM) linked the APT to the Iranian Ministry of Intelligence (MOIS).

The first report detailing MuddyWater's operations was released by Palo Alto's Unit42 in November 2017.²¹ Between February and October of that year, MuddyWater conducted multiple attacks against entities in Saudi Arabia, Iraq, Israel, UAE, Georgia, India, Pakistan, Turkey, and the United States. These attacks all started with a drop of a tailored Word or Excel document that uses macros to download a custom-made backdoor PowerShell script dubbed "POWERSTATS"²¹. Once one (1) device was compromised, it was weaponized to distribute malware across the network. In one (1) instance, a legitimate Word document was injected with malware and sent to a likely recipient, increasing its legitimacy.²¹ The motivations behind this attack seemed to be strictly espionage and information gathering. The techniques exposed in their first attacks are continued to be seen throughout MuddyWater's campaigns, though their motivations evolved.

Throughout 2020, MuddyWater's attacks shifted from stealthy intelligence gathering to more destructive actions. This is clearly shown through Operation Quicksand, where the group deployed their custom "PowGoop" loader, a two-component malware downloader that utilizes DLLs and PowerShell scripts.²² First seen in September 2020, PowGoop attempts to disguise itself as a Google application by sideloads itself into a legitimate signed version of the "GoogleUpdate.exe" file.²³ The downloader then pulls a variant of the "Thanos" ransomware, a ransomware-as-a-service sold freely on the dark web to criminals looking to make money from the ransom. MuddyWater's intentions were not financially motivated; however, instead, they intended to destroy any data they encrypted.²⁴

The MuddyWater APT has been attributed to many different individuals and groups over the years. Starting in March 2019, a group known as the "Green Leakers" made a post on Telegram stating the Iranian Ministry of Intelligence and Security (MOIS) is behind the MuddyWater group.²⁵ The actor then released multiple

²¹ <https://unit42.paloaltonetworks.com/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/>

²² <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/seedworm-apt-iran-middle-east>

²³ <https://unit42.paloaltonetworks.com/thanos-ransomware/>

²⁴ <https://www.haaretz.com/israel-news/tech-news/iran-hackers-israel-new-phase-cyberwar-operation-quicksand-1.9243913>

²⁵ <https://malware-research.org/muddywater-ongoing/>



screenshots from hacked MuddyWater command-and-control (C2) servers to establish the leak's legitimacy. They also claimed the leader of MuddyWater is an Iranian individual²⁶ and later connected multiple operators as well. Nearly two (2) years after this leak, the U.S. Cyber Command released a report confirming the connection between the Iranian MOIS and the MuddyWater APT.²⁷ While it is unlikely the MuddyWater group will continue to conduct operations in the future, Iran's skilled hackers are still a threat to the Middle East and the United States alike.

²⁶ <https://www.flashpoint-intel.com/blog/muddywater-iranian-cyber-threat-actor/>

²⁷ <https://www.cybercom.mil/Media/News/Article/2897570/iranian-intel-cyber-suite-of-malware-uses-open-source-tools/>



Trending IOCs

The following technical indicators of compromise (IOCs) are associated with monitored threat groups and/or campaigns of interest within the past sixty (60) days. IOCs can be utilized by organizations to detect security incidents more quickly and easily, as indicators may not have otherwise been flagged as suspicious or malicious.

Indicator	Type	Attribution
AA48F06EA8BFEBDC0CACE9EA5A2F9CE00C094CE10DF52462C4B9E87FEFE70F94	Hash	MuddyWater – PowGoop variant
8FED2FF6B739C13BADB14C1A884D738C80CB6F34	Hash	MuddyWater – PowGoop variant
A5981C4FA0A3D232CE7F7CE1225D9C7E	Hash	MuddyWater – PowGoop variant
185.183.98[.]242	IP Address	MuddyWater
185.82.202[.]70	IP Address	MuddyWater
185.244.149[.]215	IP Address	MuddyWater
185.183.96[.]28	IP Address	MuddyWater
185.117.75[.]101	IP Address	MuddyWater
185.82.202[.]66	IP Address	MuddyWater
hxxps://webhook[.]site/7c1564f7-4e3c-4082-b1f8-3b52da3d9941	URL	MuddyWater
hxxps://webhook[.]site/861f0c6f-238a-4878-8e44-0ca078ad9b2c	URL	MuddyWater
hxxps://webhook[.]site/f4c2dba3-bdba-44a3-b8b8-f292b6fb8a7b	URL	MuddyWater