AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on APT Groups

June 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Jul. 07, 2023

Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Precautions
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can only be accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded,
meaning that the sum of each item may not match the total.

This report is a work of authorship protected by the Copyright Act.
Unauthorized copying or reproduction for profit is strictly prohibited under any circumstances.

Seek permission from AhnLab in advance
if you wish to use a part or all of the report.

If you reprint or reproduce the material without the permission of the organization mentioned above, you may be held accountable for criminal or civil liabilities.

Contents

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Objectives and Scope

In this report, we cover nation-led threat groups presumed to conduct cyber espionage or sabotage under the support of the governments of certain countries or organizations, referred to as "Advanced Persistent Threat (APT) groups" for the sake of convenience. Therefore, this report does not contain information on cyber criminal groups aiming to gain financial profits.

We organized analyses related to APT groups disclosed by security companies and institutions including AhnLab during the previous month; however, the content of some APT groups may not have been included.

The names and classification criteria may vary depending on the security company or researcher, and in this report, we used well-known names of AhnLab Threat Intelligence Platform (ATIP)'s threat actors.

APT Group Trends

The cases of major APT groups for June 2023 gathered from materials made public by security companies and institutions are as follows.

1) Andariel

Kaspersky recently discovered numerous English typos in the activities conducted by the Andariel group.[1]

The Andariel group actively exploited the Log4j vulnerability and incorporated several new malware such as YamaBot and MagicRat. Additionally, they continued to utilize updated versions of previously used malware like NukeSped and DTrack.

[1] https://securelist.com/lazarus-andariel-mistakes-and-easyrat/110119/

Commercial programs such as 3Proxy, Dumpert, ForkDump, Powerline, Putty, NTDSDumpEx, and Supremo remote desktop were also used. The newly identified EarlyRat was also observed connecting to the servers used in the HolyGhost and Maui ransomware campaigns.

2) APT28

In collaboration with Ukraine's Computer Emergency Response Team (CERT-UA), Recorded Future[2] uncovered attacks by the APT28 (Blue Delta) group targeting prominent Ukrainian companies.[3]

The attacks employed social engineering techniques, enticing targets with war-related news topics to make them open the emails. Additionally, they took advantage of a server vulnerability (CVE-2020-35730) in Roundcube, an open-source web mail product.

Recorded Future also discovered a connection between this campaign and past activities involving the exploitation of the Microsoft Outlook notification vulnerability (CVE-2023-23397).

3) Cadet Blizzard (DEV-0586)

Microsoft publicly disclosed information about the threat group Cadet Blizzard (DEV-0586), which is sponsored by the Russian General Staff Main Intelligence Directorate (GRU). The group was traced to its involvement in destructive incidents targeting various government agencies in Ukraine that occurred in mid-January 2022.[4]

The Cadet Blizzard group was identified as the perpetrator behind the WhisperGate Wiper attack in January 2022. They disclosed the information they stole from Ukrainian websites on the "Free Civilian" Telegram channel.

[2] https://www.recordedfuture.com/bluedelta-exploits-ukrainian-government-roundcube-mail-servers

[3] https://cert.gov.ua/article/4905829

[4] https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

In addition to their activities in Ukraine, the group has been found to be active in Europe, Central Asia, and Latin America. They have launched destructive attacks against government services, non-profit/non-government organizations, IT service providers, and consulting firms.

To gain initial access, the Cadet Blizzard group abused web servers commonly found in network boundaries and DMZs. They exploited a variety of vulnerabilities, such as the Confluence server vulnerability (CVE-2021-26084), Microsoft Exchange server privilege escalation vulnerability (CVE-2022-41040), ProxyShell (CVE-2021-31207, CVE-2021-34473), among others.

4) Camaro Dragon

Check Point released the analysis of the Tinynote backdoor used by the Camaro Dragon group,[5] along with instances of attacks targeting USB flash drives.[6]

In early 2023, the Camaro Dragon group's malware, which used USB flash drives, were found in South Korea, Myanmar, Russia, the UK, and India.

Among the malware strains that were used in the attack, there is a high possibility that one was used to attack the Southeast Asia region as it attempted to bypass SmadAV, an Indonesian security product.

Trend Micro's analysis of the Mustang Panda group also revealed certain similarities in characteristics with Camaro Dragon's activities.

5) Charming Kitten (Mint Sandstorm)

Volexity came across an instance where the Charming Kitten (Mint Sandstorm) group was

[5] https://research.checkpoint.com/2023/malware-spotlight-camaro-dragons-tinynote-backdoor/

[6] https://research.checkpoint.com/2023/beyond-the-horizon-traveling-the-world-on-camaro-dragons-usb-flash-drives

found distributing the POWERSTAR malware while posing as a journalist from an Israeli media organization, with the intention of collecting credentials.[7]

During their spear phishing campaign, the Charming Kitten group conversed with their target over a period of several days before sending a malicious link or attachment. This approach is aimed at gaining the trust of the target, and it is employed by both the RedEyes (APT) and Kimsuky groups, both of which are suspected to be associated with North Korea.

6) Gamaredon (Shuckworm)

Broadcom announced that the Gamaredon (Shuckworm) group is conducting cyber attacks against the Ukrainian military, security, and government organizations.[8]

The threat actor persistently attempted to access and steal sensitive information, such as reports on Ukrainian soldiers' deaths, conflicts and airstrikes, weapon inventories, and military training.

Furthermore, the group developed malware capable of propagating through USB flash drives, and they updated their known tools and short-lived infrastructure to new versions.

7) Ke3chang (APT15, Nickel)

Broadcom announced that between December 2022 and early 2023, the Ke3chang (APT15, Flea, Nickel) group used the Graphican malware to attack US diplomatic institutions, product-selling companies in Central and South America, and government financial departments.[9]

[7] https://www.volexity.com/blog/2023/06/28/charming-kitten-updates-powerstar-with-an-interplanetary-twist

[8] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military

[9] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/flea-backdoor-microsoft-graph-apt15

In the past, this group has conducted attacks in regions such as Europe, Asia, and Africa, utilizing backdoors to exfiltrate data from their targets.

8) Kimsuky

The active operations of the Kimsuky group have been detected by multiple security firms.

SentinelOne discovered attack cases that involved the impersonation of NK News, an organization that provides North Korea-related news and analyses.[10] The Kimsuky group requested experts on North Korean affairs to review draft articles analyzing North Korea's nuclear threats. Once an expert responded, they would then be directed to a malicious website to steal their Google credentials. Additionally, the group employed the ReconShark malware in their operations.

AhnLab[11] and ESTsecurity have revealed multiple attack instances in Korea, where malware was disguised as a security update,[12] a mail online security program,[13] a HWP document,[14] a document viewer,[15] and CHM files under various subjects.[16] There have also been identified cases of the Kimsuky group using Chrome Remote Desktop.[17]

9) Lazarus

Attacks carried out by the Lazarus group exploiting vulnerabilities in South Korean financial

[10] https://www.sentinelone.com/labs/kimsuky-new-social-engineering-campaign-aims-to-steal-credentials-and-gather-strategic-intelligence/

[11] https://asec.ahnlab.com/en/54375/

[12] https://blog.alyac.co.kr/5167 (This report supports Korean only)

[13] https://blog.alyac.co.kr/5185 (This report supports Korean only)

[14] https://asec.ahnlab.com/en/54736/

[15] https://asec.ahnlab.com/en/55219/

[16] https://asec.ahnlab.com/en/54678/

[17] https://asec.ahnlab.com/en/55145/

security solutions and asset management software have been observed continuously.

AhnLab has confirmed instances of the Lazarus group exploiting zero-day vulnerabilities in the financial security solution VestCert and the asset management program TCO!Stream.[18]

The Korea National Cyber Security Center (NCSC) advised the patching of Dream Security's MagicLine4NX vulnerability.[19] On the same day, KrCERT disclosed investigation details of the Lazarus group's attacks using zero-day vulnerabilities in Korean software through Operation GoldGoblin.[20] KrCERT estimates that the vulnerabilities were researched using resources obtained from previous breaches such as the incident in 2020 where a security software development company's source code was stolen during Operation BookCodes. Therefore, it is predicted that the Lazarus group will continue to conduct zero-day attacks on Korean software in the future.

Recorded Future has uncovered activities by the BlueNoroff group, a subgroup of the Lazarus group, where they impersonated various financial institutions and venture capital companies in Japan, Vietnam, and the United States.[21] Elastic disclosed that the BlueNorOff group is carrying out attacks on cryptocurrency service providers using the Rustbucket malware.[22]

10) Muddy Water

DeepInstinct announced that they have identified Phonyc2, the new Command and Control (C2) framework utilized by the MuddyWater group.[23]

[18] https://asec.ahnlab.com/en/54195/

[19] https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=54336&menuNo=020000&subMenuNo=020200&thirdMenuNo= ((This report supports Korean only)

[20] https://thorcert.notion.site/TTPs-10-Operation-GoldGoblin-bab695345e984edbb8fe5e16e36face6

[21] https://www.recordedfuture.com/north-korea-aligned-tag-71-spoofs-financial-institutions

[22] https://www.elastic.co/kr/security-labs/DPRK-strikes-using-a-new-variant-of-rustbucket

[23] https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater

The MuddyWater group has been utilizing PhonyC2 since at least 2021, and it bears similarities to their previous creation, MuddyC2. It has also been revealed that the group is currently using PhonyC2 in a campaign that exploits the PaperCut vulnerability (CVE-2023-27350).

11) Mustang Panda

Trend Micro announced that the Mustang Panda (Earth Preta) group is not only active in Asia-Pacific (APAC) regions such as Australia, the Philippines, and Taiwan, but has also expanded to Eastern Europe and Western Asia.[24]

Trend Micro has observed various campaigns conducted by the Mustang Panda group, revealing their use of diverse techniques to bypass security solutions and the continued use of similar C&C protocols and features. Additionally, insight into their attack workflow was gained thanks to their operation security mistake.

Related details were shared at Botconf 2023,[25] with some details linking the group to the Camaro Dragon group.

12) OceanLotus

Elastic disclosed the information on REF2754, which has been targeting major Vietnamese companies, and attributed it to the OceanLotus group.[26]

The Spectralviper, P8Loader, and Powerseal malware were used in the attacks. A normal ProcDump process was used to load the SPECTRALVIPER malware. SPECTRALVIPER is an obfuscated backdoor that provides functionalities such as PE loading, injection, file upload and

[24] https://www.trendmicro.com/en_us/research/23/f/behind-the-scenes-unveiling-the-hidden-workings-of-earth-preta.html

[25] https://www.botconf.eu/botconf-presentation-or-article/catching-the-big-phish-earth-preta-targets-government-educational-and-research-institutes-around-the-world/

[26] https://www.elastic.co/kr/security-labs/elastic-charms-spectralviper

download, file and directory manipulation, and token impersonation. Depending on the situation, the P8Loader or PowerSeal were also loaded.

13) Patchwork (White Elephant)

ThreatBook revealed that the Patchwork group targeted the Chinese government and universities using subjects such as 'National Key Research and Development Programs' and 'Advanced Structures and Composite Materials' as lures.[27] The Patchwork group primarily targets national defense and foreign affairs sectors of China, Pakistan, and Bangladesh.

The group employed the BADNEWS malware for remote control of their targets and were also found to use the commercial malware, Remcos, and the open-source penetration framework Havoc.

14) Red Eyes (APT37)

IBM released information about the activities of the Red Eyes (APT37, ScarCruft) group within South Korea.[28]

AhnLab confirmed the distribution of malware through websites created by a specific web development company[29] and disclosed the additional activities that were carried out using the Ably platform.[30]

Genians shared details on cases of attacks targeting North Korean defectors in South Korea using macOS malware.[31]

[27] https://mp.weixin.qq.com/s?__biz=Mzg5MTc3ODY4Mw==&mid=2247502126&idx=1&sn=d7e47e213ca8c78c2bff8955aede84e6

[28] https://securityintelligence.com/posts/itg10-targeting-south-korean-entities/

[29] https://asec.ahnlab.com/en/54369/

[30] https://asec.ahnlab.com/en/54349/

[31] https://www.genians.co.kr/blog/threat_intelligence_report_macos (This report supports Korean only)

15) Sharp Panda

Cyble announced that the SharpPanda group has been observed conducting attacks targeting high-level government officials from G20 nations.[32]

The SharpPanda group employs a forged document linked to G7 to target various governments within the G20 forum. They exploit vulnerabilities in Microsoft Office, including CVE-2018-0802, CVE-2018-0798, and CVE-2017-11882. Systems were infected with a backdoor that can exfiltrate system information, files, and other sensitive data. The PDB path for the backdoor file is 'D:₩Project₩Downloader₩dll_rls₩Downloader.pdb'.

16) SideCopy

Seqrite discovered a new attack campaign by the SideCopy group, targeting the national defense sector of India.[33]

This group utilizes phishing emails with malicious attachments and URLs to download malicious archive files, infecting systems with Action RAT and a new .NET-based malware.

17) Stealth Soldier

Check Point uncovered espionage activities against specific targets in Libya and Egypt that use a new custom modular backdoor.[34]

The Stealth Soldier malware used in these attacks is a backdoor with surveillance features, such as file exfiltration, screen and microphone recording, keylogging, and browser data theft.

[32] https://blog.cyble.com/2023/06/01/sharppanda-apt-campaign-expands-its-arsenal-targeting-g20-nations/

[33] https://www.seqrite.com/blog/double-action-triple-infection-and-a-new-rat-sidecopys-persistent-targeting-of-indian-defence

[34] https://research.checkpoint.com/2023/stealth-soldier-backdoor-used-in-targeted-espionage-attacks-in-north-africa/

It was found that Stealth Soldier's infrastructure shares some similarities with the infrastructure of The Eye on the Nile, which was previously disclosed by Check Point in 2019.[35]

Conclusion

In June 2023, information on a total of 17 APT groups (19 APT groups if you include the UNC of Mandiant which has not been given a specific name) was released.

Among these, the activities of groups suspected to be backed by North Korea, including Kimsuky, Lazarus, and Red Eyes, have come into focus.

For several years now, the Kimsuky and Red Eyes groups have been utilizing a technique involving email exchanges with their targets to establish trust. They then proceed to send phishing sites or files containing malware. The Charming Kitten group is also said to have used a similar technique. If new attack methods or vulnerabilities are not developed, it is expected that attempts to use social engineering techniques based on such trust will continue to increase in the future.

Attacks by the Lazarus group using the zero-day vulnerabilities of Korean software are continuing to be detected. According to KrCERT, the Lazarus group has been stealing source code from software development companies since 2020 and analyzing the stolen code. Hence, there is a high possibility that other undiscovered zero-day vulnerabilities may exist. It is crucial to promptly apply software security updates as soon as they become available to mitigate potential damages.

The main targets of nation-supported threat groups are security, energy, diplomacy, politics, cutting-edge technology, and aerospace sectors. As such, these sectors must prepare a stage-by-stage response system to defend against nation-led attacks and ensure visibility for their internal systems. It is also advised to be aware of the trends of major threat groups through threat intelligence (TI) services in preparation for their attack targets and techniques.

[35] https://research.checkpoint.com/2019/the-eye-on-the-nile/

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
https://www.ahnlab.com
https://asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency response (ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab