TLP: GREEN

Threat Trend Report on APT Groups

October 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Nov. 9, 2023

AhnLab

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.

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, referred to as "Advanced Persistent Threat (APT) groups" for the sake of convenience. Therefore, this report does not contain information on cybercriminal 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 October 2023 gathered from materials made public by security companies and institutions are as follows.

1) Andariel

AhnLab observed the circumstances of the Andariel group using NetClient, an asset management program, to distribute malware.[1] The threat actor used the wget command with NetClient to execute a PowerShell script that downloads the TigerRAT malware.

2) DarkPink

NSFOCUS Security Labs announced that the DarkPink group has been exploiting a vulnerability in WinRAR (CVE-2023-38831) to attack Vietnamese and Malaysian government

[1] https://atip.ahnlab.com/ti/contents/asec-notes?i=0458635b-ff75-4444-bd78-a5b1d15a92dc

organizations.[2] The DarkPink group put documents related to the Ministry of Foreign Affairs of the Socialist Republic of Vietnam and the State Securities Commissions of Vietnam as bait inside the compressed file that triggered the WinRAR vulnerability.

The TelePowerBot malware was used, and Telegram served as the C&C server.

3) Desert Falcon (Arid Viper)

Cisco shared details on a hacking campaign where the Desert Falcon (Arid Viper) group used a malicious mobile app and targeted Arabic-speaking Android users.[3]

The group transmitted videos and links disguised as updates for dating or utility apps to infect mobile devices. The mobile malware used in this campaign is similar to the online dating app "Skipped". This implies that the Desert Falcon operators have connections with the developers of Skipped or have illegally approached the shared project database.

The malicious app has features to deactivate notifications from security apps, collect sensitive user information, and install additional malicious apps in the infected device. Google's Firebase platform was used for communications.

The Desert Falcon operator is expected to use the infrastructure or names of more applications in the fu
ture.

4) Grayling

Symantec announced that the Grayling group has been attacking the manufacturing, IT, and bioengineering industries of Taiwan, as well as government bodies of the Pacific Islands and organizations in Vietnam and the US from February to May 2023.[4]

---

[2] https://nsfocusglobal.com/apt-group-darkpink-exploits-winrar-0-day-to-target-multiple-entities-in-vietnam-and-malaysia/

[3] https://blog.talosintelligence.com/arid-viper-mobile-spyware/

[4] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks

Details on the Grayling group's operating organizations are yet to be known, but their attacks on Taiwanese organizations indicate that there is a high possibility of the group being operated in an area that has some kind of a strategic relationship with Taiwan.

Grayling uses customized malware strains and public tools such as Cobalt Strike, Havoc, and NetSpy. The threat actor was also seen loading and decoding the imfsb.ini file.

5) Imperial Kitten (Yellow Liderc)

pwc announced that the Imperial Kitten (Yellow Liderc) group is launching attacks mainly against the marine, shipping, and logistics sectors.[5]

The group hacked into websites and embedded malicious JavaScript codes. The malicious JavaScript codes fetched the user location, device, and visit times of visitors and infected the systems of their chosen targets.

The IMAPLoader malware was newly discovered, and it has the feature to download an additional payload. IMAPLoader uses the "AppDomain Manager Injection" technique in which the .NET program loads a specially made .NET assembly.

6) Kimsuky

AhnLab announced that the Kimsuky group is infecting systems with BabyShark and controlling them with RDP (Remote Desktop Protocol).[6] The threat actor patched the RDP-related termsrv.dll file.

A new feature was added in October, and this feature can download the FlowerPower malware to the HWP document downloaded from RandomQuery.[7] While normally it downloads a bait

[5] https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellow-liderc-ships-its-scripts-delivers-imaploader-malware.html

[6]https://asec.ahnlab.com/en/57873/

[7] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=c8f657a6-4d16-4fa7-a14e-

document, the document disguised as a news survey included malicious OLE objects.

S2W discovered a new malicious app by the Kimsuky group.[8] The app prompts users to install it with a repackaged APK file where malware is included within a legitimate app. In the past, malicious apps were divided into FastViewer, which was for downloading and loading, and FastSpy, which was for remote control. But in this case, the two were combined into one.

Genians revealed that the email attacks against personnel of diplomatic and unification-related fields between June and early September, impersonating the Ministry of Foreign Affairs and Ministry of Unification, had some kind of connection to the BabyShark malware.[9] Usernames such as 'Coyote', 'Leopard', 'Puma', and 'Storm' were found in the bait document used in these attacks. Some of these were also used in attacks using BabyShark.

7) Lazarus

AhnLab analyzed Lazarus group's Volgmer backdoor and Scout downloader and released the results.[10] Volgmer is a backdoor used from 2014 and was replaced with the Scout downloader in 2022. The early Scout downloader looked up the registry value where configuration data is saved based on file names much like Volgmer, but after 2022, Scout v2, with a wider range of features for downloading and executing commands made its appearance.

AhnLab also analyzed and released the results on cases of watering hole attacks by the Lazarus group which exploited a vulnerability in a Korean certificate solution, MagicLine4NX.[11] In this attack campaign, named 'Operation Dream Magic', corporations in the Korean defense, media, finance, and IT industries were attacked.

Kaspersky released analysis results of a software supplier attacked by the Lazarus group.[12]

---

e4e6f8f43a47 (This report supports Korean only for now.)

[8] https://medium.com/s2wblog/fastviewer-variant-merged-with-fastspy-and-disguised-as-a-legitimate-mobile-application-f3004588f95c

[9] https://www.genians.co.kr/blog/kimsuky (This report supports Korean only for now.)

[10] https://asec.ahnlab.com/en/57685/

[11] https://asec.ahnlab.com/en/57736/

[12] https://securelist.com/unveiling-lazarus-new-campaign/110888/

The LPEClient and SIGNBT malware strains were used in the attacks. LPEClient was also used in other attacks such as those against munitions and cryptocurrency companies.

8) Lucky Mouse

EclecticIQ announced that a cyber threat group led by China is launching attacks against the semiconductor industries of Taiwan, Hong Kong, and Singapore.[13]

The threat actor used content related to TSMC (Taiwan Semiconductor Manufacturing) to deliver the HyperBro loader malware and infect the system with Cobalt Strike Beacon. ChargeWeapon, a new Go-based backdoor, was found in the server used by the threat actor.

9) OilRig (APT34, Crambus)

Symantec (Broadcom) discovered activities of the OilRig group (Crambus, APT34) thought to be from Iran, that targeted government organizations in the Middle East between February and September 2023.[14]

Passwords were stolen in these attacks and malware strains including Dirps, Toekl, and PowerExchange were installed to execute commands through emails sent by the threat actor.

In addition, the threat actor enabled remote access using Plink, a network management tool and also changed Windows Firewall rules to activate remote access.

10) Scarred Manticore

Check Point announced that the Scarred Manticore group, presumed to be affiliated with the Ministry of Intelligence of Iran (MOIS), has been attacking the government, communications,

[13] https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia

[14] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government

and financial sectors of Israel, Jordan, Iraq, Saudi Arabia, UAE, and Oman.[15]

This group attacks Windows web servers to infect them with Liontail and Webshell. Liontail is a malware framework that includes a custom shellcode loader and a shellcode payload that remains in the memory.

The Scarred Manticore group is partially connected to the OilRig group and there is a possibility that the two are the same group.

11) ToddyCat

Check Point released information on Stayin' Alive, an active campaign that has been targeting the communications industry and government organizations of Kazakhstan, Uzbekistan, Pakistan, and Vietnam since 2021.[16] Malware strains including CurCore, CurLu Loader, and CurKeep were used in the Stayin' Alive campaign.

Kaspersky announced that they have found ToddyCat group's new tools.[17] The newly discovered malware strains and tools are Loader, Ninja, LoFiSe, DropBox uploader, and Pcexter. The Loader hides the malware in the address of svchost.exe, and LoFiSe collects the target files. The collected data is exfiltrated using uploading tools such as DropBox uploader or Pcexter. There were also traces of the use of a UDP Backdoor, which receives commands through UDP packets before executing them, as well as CobaltStrike Beacon.

12) Tropic Trooper

ITOCHU shared that the Tropic Trooper group has been attacking the semiconductor and precious metal-related industries in East Asia since May 2023.[18]

---

[15] https://research.checkpoint.com/2023/from-albania-to-the-middle-east-the-scarred-manticore-is-listening/

[16] https://research.checkpoint.com/2023/stayin-alive-targeted-attacks-against-telecoms-and-government-ministries-in-asia/

[17] https://securelist.com/toddycat-keep-calm-and-check-logs/110696/

[18] https://blog-en.itochuci.co.jp/entry/2023/10/06/173200

Infection occurs via email, with the malware comprised of an installer and loader. Xiangoop Loader loads Cobalt Strike Beacon or EntryShell.

The CrowDoor malware was found, and the loader that loads the malware is SparrowDoor Loader used by the FamousSparrow threat group.

As it is confirmed that the threat actor installed CrowDoor using Xiangoop Loader, it can be assumed that there are connections between the FamousSparrow group which uses SparrowDoor Loader and the Tropic Trooper group which uses the Xiangoop Loader.

This topic was presented at a Virus Bulletin conference.[19]

13) Winter Vivern

Eset announced that the Winter Vivern group exploited a Roundcube webmail server zero-day vulnerability (CVE-2023-5631) in August and September 2023 to attack European government organizations and think tanks.[20]

The email sent by the threat actor to the target triggers the zero-day vulnerability, allowing JavaScript to be injected into Roundcube.

The Winter Vivern group is slightly connected to the MoustachedBouncer group in Belarus.

14) YoroTrooper

Cisco announced that the YoroTrooper group is attacking government officials and organizations of the Commonwealth of Independent States (CIS).[21]

---

[19] https://www.virusbulletin.com/conference/vb2023/abstracts/unveiling-activities-tropic-trooper-2023-deep-analysis-xiangoop-loader-and-entryshell-payload/

[20] https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

[21] https://blog.talosintelligence.com/attributing-yorotrooper/

Because the group uses the Kazakhstani Tenge (KZT), the currency of Kazakhstan, and speaks Kazakh, Russian, and Uzbek, which is widely used in Kazakhstan, it is deemed to be formed of members from Kazakhstan. However, this group employed various tactics to make their malicious activities seem to originate from Azerbaijan.

Aside from commercial and customized malware strains, the YoroTrooper group was found to be highly reliant on phishing emails that redirect victims to account credential collection sites as usual.

Conclusion

Information on a total of 14 APT groups was released in October 2023.

Due to the military conflict between Israel and Palestine's Hamas, cyber attacks in the Middle Eastern region are receiving more attention, and many attacks by hacktivists supporting either side were observed. Three pieces of information on the groups active in these regions were disclosed.

The attack methods of many APT groups often involve sending emails with content that may pique the recipient's interest along with a link or an executable file, CHM, or LNK disguised as a document file. Attacks that exploit a vulnerability in WinRAR (CVE-2023-38831) were also detected. Aside from attacks using emails, there was also exploitation of vulnerabilities in internet security programs or servers and cases of infection through asset management programs. As there have been cases of malware control via email, there is a need for monitoring of emails with suspicious content.

State-led threat groups' targets include the security, energy, diplomatic, political, cutting-edge technology, and aerospace sectors. Thus, these sectors must implement a phase-by-phase response system to defend against state-led attacks and ensure visibility for their internal system. It is also advised to use threat intelligence (TI) services to receive updates on the trends of major threat groups and prepare against their attack targets and techniques.

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