AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on APT Groups

July 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Aug. 8, 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.

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 liability.

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 July 2023 gathered from materials made public by security companies and institutions are as follows.

1) APT28

CERT-UA, a governmental computer emergency response team of Ukraine, found an HTML that imitates the web interface of an email service and leaks the verification data entered by the victim.[1]

The designated address is the Iranian Embassy in Tirana, Albania. The threat actor seems to have launched a cyber attack against the diplomatic organizations of Iran in May 2023. CERT-UA views this to be a phishing attack by the APT28 group.

[1] https://cert.gov.ua/article/5105791

2) APT29

Palo Alto revealed that the APT 29 (Cozy Bear) group, which has been attacking diplomatic organizations of multiple countries, has been launching phishing attacks with content regarding verbal memos, updates on the operation status of embassies, diplomat schedules, and event invites.[2]

One of their recent campaigns was against a diplomatic organization situated in Kyiv, Ukraine. Out of over 80 diplomatic organizations there, it is said that at least 22 fell victim to the attacks. It is said that first, a normal car sales advertisement was sent via email before an email containing malware was sent two weeks later.

Recorded Future revealed that the APT29 is enhancing their efforts to conceal their command and control network traffic using legal Internet services (LIS).[3] The group prioritizes cyber espionage against European government organizations and evades detection using various online services.

3) APT31

AhnLab revealed that the APT31 (Judgment Panda, Zirconium) group has been using the Rekoobe malware to constantly attack Korean clients.[4] Rekoobe targets Linux servers and was created based on Tiny SHell, an open-source backdoor. This malware has features to download, upload, and execute commands on order from the C2 server.

Kaspersky shared that the APT31 group has been launching a series of attacks against industrial organizations.[5] The purpose of such attacks is to establish a channel for data leaks, and second-stage malicious software is used to collect data from the infected systems.

[2] https://unit42.paloaltonetworks.com/cloaked-ursa-phishing/

[3] https://www.recordedfuture.com/bluebravo-adapts-to-target-diplomatic-entities-with-graphicalproton-malware

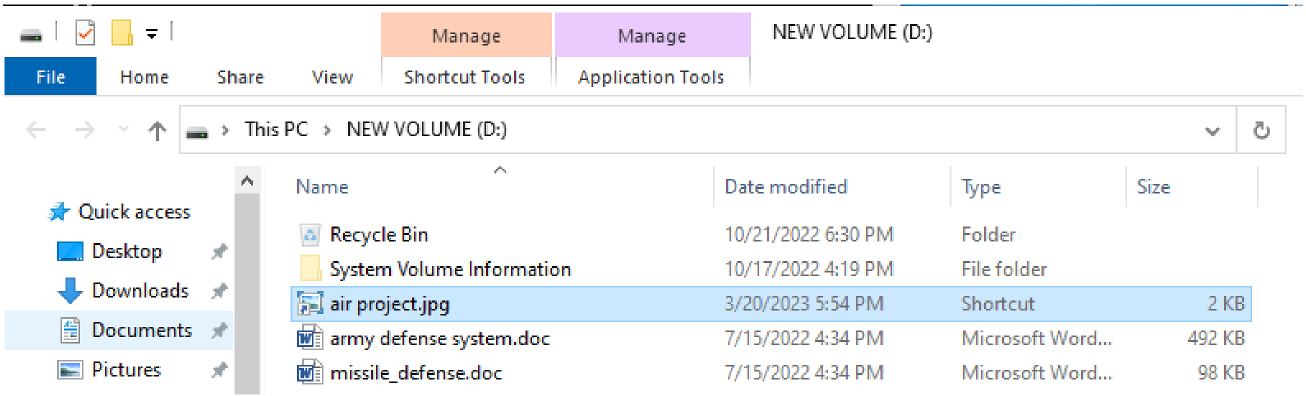
[4] https://asec.ahnlab.com/en/55229/

[5] https://ics-cert.kaspersky.com/publications/reports/2023/07/31/common-ttps-of-attacks-against-industrial-organizations-implants-for-gathering-data/

Attempts at data leaks are also made using portable storage devices (USB flash drives) on air-gapped systems.

4) Camouflaged Hunter

ThreatBook discovered the Camouflaged Hunter (APT-C-60) group launching attacks using military-related topics, such as "missile defense.doc" and "army defense system.doc".[6] When a user clicks the LNK file within the virtual hard disk (VHD) file, malware is downloaded and executed.



Name	Date modified	Type	Size
Recycle Bin	10/21/2022 6:30 PM	Folder	
System Volume Information	10/17/2022 4:19 PM	File folder	
air project.jpg	3/20/2023 5:54 PM	Shortcut	2 KB
army defense system.doc	7/15/2022 4:34 PM	Microsoft Word...	492 KB
missile_defense.doc	7/15/2022 4:34 PM	Microsoft Word...	98 KB

Figure 1. Malicious LNK file within the VHD file

This threat actor updated the malware they were using before, and some codes only run on systems with Windows 10 or later.

AhnLab discovered activities of this group since 2021 in Korea, Japan, and Singapore, as well as their additional malware variants and tools.[7]

5) Charming Kitten

Proofpoint announced that the Charming Kitten (Mint Sandstorm, TA453) group launched attacks against a security specialist at a US-based think tank with an LNK file and Mac

[6] https://threatbook.io/blog/id/1090

[7] https://atip.ahnlab.com/ti/contents/issue-report/trend?i=61fbd787-5e08-45b3-9d1b-048b469282bd (This report supports Korean only for now.)

malware.[8]

The Charming Kitten group used various cloud hosting providers in an attempt to infect target systems with GorjolEcho and NokNok malware for macOS.

There is a possibility of this being linked with the information revealed by Volexity in June 2023.[9]

6) Gamaredon

CERT-UA shared the fact that the Gamaredon (UAC-0010) group is continuously undertaking cyber espionage and destructive activities against Ukrainian security and defense entities.[10] The group's attacks involved the use of portable media (USB flash drives and external hard disks), shortcut files (LNK), and Microsoft Office Word documents with embedded macros. The group uses the Gammasteel malware to collect a list of certain file extensions and create logs.

7) Kimsuky

AhnLab announced that the Kimsuky group has been distributing malware disguised with content related to coin exchanges and investment.[11] AhnLab also revealed that their attacks using FlowerPower have increased and that the group is diversifying their attack methods.[12] According to AhnLab, the BabyShark (RecornShark) malware, which collects system information and information on certain directories, uses a batch file during the infection process to check for security products being used in the system. After searching for four products that are widely used in Korea, it downloads and executes a different script depending on the product in use.

[8] https://www.proofpoint.com/us/blog/threat-insight/welcome-new-york-exploring-ta453s-foray-lnks-and-mac-malware

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

[10] https://cert.gov.ua/article/5160737

[11] https://asec.ahnlab.com/en/55944/

[12] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=4d57ae14-8929-4650-851d-e6a244de830e

8) Konni

Genians[13] and Antiy[14] revealed that the Konni group has been attacking Koreans by in disguise of the National Tax Service of Korea. Files used in the attack include a malicious LNK file in ZIP file. When the user executes this file, it connects to a malicious URL and installs an additional malicious file through PowerShell.

9) Lazarus

SentinelOne shared analysis details on RustBucket, the malware used by the BlueNoroff group against macOS users. BlueNoroff is a subsidiary group of the Lazarus group.[15] Attacks begin with an applet disguised as a PDF viewer, and the malware is executed through a process of several stages.

JPCERT shared information on the relationship between the attacks against cryptocurrency exchange developers and the DangerousPassword group.[16] Many researchers presume this group is connected to the Lazarus group. The group uses Python and Node.js to launch attacks against Linux, macOS, and Windows environments, and they use QR codes to distribute Python malware. Also, in macOS and Linux environments, a string encoded to Base64 is decoded to run the malware. The Node.js malware targets the Express framework and distributes and executes files containing malware.

AhnLab announced that the Lazarus group has been attacking Windows IIS web servers and distributing malware as a part of their activities in Korea.[17] The Lazarus group attacks web servers and infects target systems that use vulnerable versions of INISAFE CrossWeb EX V3

[13] https://www.genians.co.kr/blog/threat_intelligence_report_konni

[14] https://www.antiy.cn/research/notice&report/research_report/Konni_Analysis.html

[15] https://www.sentinelone.com/blog/bluenoroff-how-dprks-macos-rustbucket-seeks-to-evade-analysis-and-detection/

[16] https://blogs.jpcert.or.jp/en/2023/07/dangerouspassword_dev.html

[17] https://asec.ahnlab.com/en/55369/

with malware when it establishes a connection. A packed JuicyPotato was used as the privilege escalation tool, and JuicyPotato executes a loader.

10) Mustang Panda

Check Point discovered an attack campaign targeting government organizations of European countries such as the UK, Sweden, France, Czech Republic, Slovakia, Hungary, and Ukraine.[18] The threat actor employed the HTML smuggling technique of concealing malicious codes within HTML documents. Targets were infected with PlugX, which is widely used by Chinese threat actors. Check Point determined this to be connected with the activities of Mustang Panda.

11) Patchwork

Qianxin identified the Spyder malware that is linked to the Patchwork group.[19] The Spyder malware was not used by the Patchwork group. This malware is similar to the WarHawk backdoor, which was used by another APT group in South Asia. Qianxin revealed that there is a complex relationship among APT groups in South Asia.

12) Red Eyes

Qianxin stated that they observed the attacks of the Red Eyes (APT37, APT-C-28, ScarCruft) group targeting the energy sector and that the Rokrat backdoor was used.[20] The Rokrat backdoor, which was transmitted via malicious LNK files, is downloaded and executed using PowerShell. This backdoor is responsible for stealing sensitive information, uploading and downloading files, taking screenshots, and keylogging. It can also execute backdoor commands through a cloud storage API.

[18] https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/

[19] https://ti.qianxin.com/blog/articles/Patchwork-Group-Utilizing-WarHawk-Backdoor-Variant-Spyder-for-Espionage-against-Multiple-Countries-EN/

[20] https://ti.qianxin.com/blog/articles/Cloud-Spy-Analysis-of-Recent-Attack-Activities-by-Group123-CN/

AhnLab revealed that the Red Eye group has been distributing malicious CHM files by impersonating Korean financial institutes and insurance companies.[21] In another attack, it was found that commands were being transmitted and received using pCloud as the C2 server.[22]

13) Space Pirates

PTSecurity released additional information on the Space Pirates group which has been attacking the aerospace and energy industries of Russia, Georgia, and Mongolia.[23]

The Space Pirates group is allegedly using Chinese and has been active since 2017. The Space Pirates group specifically pinpoints their attack targets and launches wide-range investigations to understand the network infrastructure and security systems used within organizations.

This group uses open-source malware such as PlugX, PoisonIvy, ReVBShell, and ShadowPad, as well as independent malware such as DeedRAT. They also build their C2 server using open-source platforms such as the GitHub repository.

The Space Pirates group is partially connected to other Chinese groups including APT27, APT41, TA428, and Mustang Panda.

14) Turla

Microsoft[24] and CERT-UA[25] announced that the Turla group has been using the Capibar and Kazuar malware to target the defense industry of Ukraine and Eastern Europe.

[21] https://asec.ahnlab.com/en/55569/

[22] https://atip.ahnlab.com/ti/contents/asec-notes?i=7028bff6-d931-4600-8583-57293cce94d1

[23] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/space-pirates-a-look-into-the-group-s-unconventional-techniques-new-attack-vectors-and-tools/

[24] https://twitter.com/MsftSecIntel/status/1681695399084539908

[25] https://cert.gov.ua/article/5213167

The threat actor used the open-source tool Rclone to collect information and attempted to leak the file containing message histories of Signal Messenger, a messaging service made to prevent wiretapping.

In order to use the Microsoft Exchange server as their C2 server, the threat actor used Desired State Configuration (DSC), a PowerShell management platform that helps administrators automate Windows system configuration.

15) Unclassified

Microsoft shared that Storm-0558 (a temporary group name given by MS) gained unauthorized access to Exchange Online (OWA) and Outlook.com.[26] It is said that a third party accessed the email data of about 25 organizations including US government organizations, as well as personal accounts seen as being related to these organizations. Another attack by Storm-0978 used Microsoft Office and the Windows HTML remote code execution zero-day vulnerability (CVE-2023-36884) against national defense and government entities in Europe and North America.[27]
Trend Micro identified a variant of ShadowPad that infected targets through a modified installation file of the Pakistani government's E-Office app, but because ShadowPad is used by many Chinese-speaking groups, it was unable to be linked with a specific APT group.[28]

On July 20, 2023, a cloud-based IT management service JumpCloud released the results of an internal investigation into an intrusion on their network.[29] SentinelOne associated the threat activity to a North Korean APT group,[30] and Mandiant announced that the JumpCloud

[26] https://msrc.microsoft.com/blog/2023/07/microsoft-mitigates-china-based-threat-actor-storm-0558-targeting-of-customer-email/

[27] https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

[28] https://www.trendmicro.com/en_us/research/23/g/supply-chain-attack-targeting-pakistani-government-delivers-shad.html

[29] https://jumpcloud.com/blog/security-update-incident-details

[30] https://www.sentinelone.com/labs/jumpcloud-intrusion-attacker-infrastructure-links-compromise-to-north-korean-apt-activity/

intrusion is attributed to UNC4899, a hacking group presumed to have North Korea origins.[31]

The zero-day vulnerabilities (CVE-2023-35078, CVE-2023-35081) in an Ivanti product, an IT management solution, were exploited in attacks against many Norwegian institutes and government organizations.[32] The specific malware and APT group are not yet known.

Conclusion

Information on a total of 14 APT groups was released in July 2023. Espionage in conflict areas such as Russia-Ukraine, Russia-Europe, and South Korea-North Korea are still strong.

The attack methods of many APT groups still involve sending emails with links, executable files disguised as document files, CHM files, and LNK files containing content that can lure targets. However, some APT groups attacked using zero-day vulnerabilities in Microsoft Office, cloud services, and Ivanti products (CVE-2023-35078, CVE-2023-35081). The Lazarus group is continuing their attacks using the zero-day vulnerability in Korean security software.

State-led threat actors' 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 make preparations on their attack targets and techniques.

[31] https://www.mandiant.com/resources/blog/north-korea-supply-chain

[32] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a

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.