AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on APT Groups

August 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Sep. 08, 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, 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 August 2023 gathered from materials made public by security companies and institutions are as follows.

1) Andariel

AhnLab has revealed cases of attacks on Korean companies carried out by the Andariel Group,[1] a group that may be a cooperative or subgroup of the Lazarus Group.

Malware infection occurred through the file transfer program Innorix, but it has not been confirmed whether the file transfer feature or a product vulnerability was used. Although the malware used in the attacks included the TigerRat variant, which was first discovered in 2020, new variants developed in Go were also discovered, such as BlackRat, Durianbeacon, and GoatRat. Credential-stealing malware used to only steal web browser login information, but the newly discovered variants now also exfiltrate the web browser history.

[1] https://asec.ahnlab.com/en/56405/

Cisco has discovered attacks by the Andariel group targeting Internet backbone infrastructures and medical institutions in Europe and the US.[2] In this campaign, the Zoho ManageEngine ServiceDesk vulnerability was exploited, and a new malware named QuiteRAT was discovered.[3]

Malware similar to QuiteRAT disclosed by Cisco was also discovered in Korea in June 2022. QuiteRAT shares similar features with MagicRAT and was developed based on the cross-platform framework Qt.

2) APT29

EclecticIQ discovered attacks targeting diplomatic institutions of countries that are members of NATO, masquerading as an invitation email from the German Embassy.[4]

It is suspected that the attacks were carried out by the Russian APT29 group due to the transfer of the Duke malware variant discovered in the PDF file. The threat actor utilized the Amazon web service to use the open-source chat application Zulip as their C2 server.

3) APT31

Kaspersky investigated attacks targeting industrial organizations in Eastern Europe and attributed them to the APT31 group.[5] This threat group abuses cloud-based data storage and temporary file-sharing services like Dropbox or Yandex Disk to exfiltrate data and transfer subsequent-stage malware.

Germany's intelligence agency, the Federal Office for the Protection of the Constitution (BfV),

[2] https://blog.talosintelligence.com/lazarus-collectionrat/

[3] https://blog.talosintelligence.com/lazarus-quiterat/

[4] https://blog.eclecticiq.com/german-embassy-lure-likely-part-of-campaign-against-nato-aligned-ministries-of-foreign-affairs

[5] https://securelist.com/common-ttps-of-attacks-against-industrial-organizations/110319/

has warned that APT15 and APT31 used the control system of routers and smart homes.[6]

4) Bitter

Qianxin revealed that the Bitter (蔓灵花, APT-C-08) group transferred CHM files or Excel files that abuse vulnerabilities as email attachments to China and Pakistan.[7]

The selectively used MSI files contain the wmRAT malware. wmRAT has continued to evolve over the past two years and supports over ten remote commands.

5) Bronze Starlight

SentinelOne released information on the Bronze Starlight (Emperor Dragonfly, Storm-0401) group, which targets the Southeast Asian gambling industry.[8] This group is partially related to Operation ChattyGoblin, which ESET revealed in May 2023.

The threat actor loaded the Cobalt Strike beacon using executable files from Adobe Creative Cloud, Microsoft Edge, and McAfee VirusScan. A certificate issued by PMG PTE LTD, a Singaporean Ivacy VPN service provider, was used to sign the malware file.

The HuiLoader variant used in the attacks is also being used by other Chinese threat groups, making it challenging to accurately distinguish between these groups as they share infrastructure and malware.

6) Callisto

Recorded Future observed the Callisto (BlueCharlie, Calisto, COLDRIVER, SEABORGIUM, Star Blizzard, TAG53) group setting up infrastructure, which includes the creation of 94 new

[6] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.html

[7] https://ti.qianxin.com/blog/articles/Persistence-in-Shadows-Recent-Analysis-of-Magnolia-Attacks-CN/

[8] https://www.sentinelone.com/labs/chinese-entanglement-dll-hijacking-in-the-asian-gambling-sector/

domains, for the purpose of conducting phishing campaigns and collecting credentials.[9]

While their exact targets have not been pinpointed, the Callisto group has previously conducted attacks against political figures, non-governmental organizations (NGO), activists, journalists, and similar individuals in the past.

7) Carderbee

Symantec (Broadcom) announced that the Carderbee group infected computers with the Plugx backdoor through Cobra DocGuard, a security software from the Chinese company EsafeNet.[10] Most of the victims of this supply chain attack were residents of Hong Kong, with some located in the broader Asia region.

The malware used in the attacks was signed with a certificate labeled 'Microsoft Windows Hardware Compatibility Publisher'.

8) Charcoal Typhoon (RedHotel)

Recorded Future released an analysis of the RedHotel (Aquatic Panda, Bronze University, Charcoal Typhoon, Earth Lusca, Red Scylla, TAG22) group, which is suspected to be a threat group sponsored by the country of China.[11]

This group has been active since 2021, targeting government organizations, media, academia, aerospace, research and development sectors, and more across 17 countries in Asia, Europe, and North America.

Recorded Future identified the use of a multi-layered infrastructure network for command and control (C2), reconnaissance, and exploitation. They also observed that this infrastructure

[9] https://www.recordedfuture.com/bluecharlie-previously-tracked-as-tag-53-continues-to-deploy-new-infrastructure-in-2023

[10] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

[11] https://www.recordedfuture.com/redhotel-a-prolific-chinese-state-sponsored-group-operating-at-a-global-scale

may be managed from a China-based IP address, potentially pinpointing the geographic location to Chengdu, Sichuan Province, China.

9) Earth Estries

Trend Micro released information on the Earth Estries group, which targets government and technology industry organizations based in South Africa, Taiwan, India, Singapore, Malaysia, the US, the Philippines, Germany, and Canada.[12]
Some of their tactics, techniques, and procedures (TTP) overlap with those used by the FamousSparrow group.

Earth Estries attempted to bypass detection by Windows Antimalware Scan Interface (AMSI) logging mechanisms and abused public services such as GitHub, Gmail, AnonFiles, File.io, etc., to exchange or transmit commands and stolen data. Malware such as HemiGate, TrillClient, and Zingdoor were used.

10) Flax Typhoon

Microsoft observed espionage activities conducted by the Flax Typhoon (Ethereal Panda) group, a group based in China, against government agencies and education, critical manufacturing, and information technology organizations in Taiwan since mid-2021.[13]

The Flax Typhoon group performs their initial infiltration by leveraging vulnerabilities in servers such as VPN, web, Java, and SQL. They then abuse internal features of operating systems for privilege escalation and information collection.

This group employs tools such as China Chopper, Metasploit, Juicy Potato, Mimikatz, and SoftEther, along with valid accounts and legitimate programs (LOLBins, Living off-the-land) in their attacks, making them difficult to detect.

[12] https://www.trendmicro.com/en_us/research/23/h/earth-estries-targets-government-tech-for-cyberespionage.html

[13] https://www.microsoft.com/en-us/security/blog/2023/08/24/flax-typhoon-using-legitimate-software-to-quietly-access-taiwanese-organizations/

11) GroundPeony

Nao-Sec discovered the GroundPeony group, which targets government organizations, research institutes, and telecommunications companies in Asian regions like Nepal, Taiwan, India, Korea, and Hong Kong.[14] They use spear phishing attacks on their targets and have been abusing the Follina (CVE-2022-30190) vulnerability even before it was publicly disclosed.

Related details were presented at the HITCON CMT conference.[15]

12) Infamous Chisel

Cyber security and intelligence organizations from New Zealand, the UK, the US, Canada, and Australia released information on the mobile malware Infamous Chisel, which targets Android-based devices used by the Ukrainian military.[16]

Russian forces seized tablet devices used by the Ukrainian military on the battlefield and used them as a hub to remotely propagate the malware to other devices using the Android Debug Bridge (ADB) command line tool.

The malware also includes a feature that periodically scans the local network and provides SSH access.

13) Kimsuky

The Korean police released their investigation findings regarding the Kimsuky group, revealing that the group targeted employees of a Korean war game operation company who were involved in the 'Freedom Shield' military exercise, a joint US-Korea military drill conducted in

[14] https://nao-sec.org/2023/08/groundpeony-crawling-with-malice.html

[15] https://hitcon.org/2023/CMT/en/agenda/e8fe6942-9c60-419a-b9a0-dbda80a27ad0/

[16] https://www.ncsc.gov.uk/section/keep-up-to-date/malware-analysis-reports

February and March 2023.[17]

Hauri disclosed analysis results of the Kimsuky group's BabyShark-related malicious script that accesses the C&C server, retrieves the AES key, and decrypts and executes malware.[18]

360 revealed an analysis of a case where the Kimsuky group used a domain with a Korean name instead of a general English name.[19]

AhnLab, in their monthly threat trend report on the Kimsuky group, revealed that phishing pages and bait documents, disguised as advisories related to national defense and intended for use in attacks, were discovered on the group's C&C server.[20] A web shell and phishing page was also found in another C&C server that distributes BabyShark.

14) Lazarus

SentinelLabs revealed that North Korea's Lazarus and Red Eyes groups infiltrated the Russian defense industry in May 2022.[21] The Lazarus Group's backdoor was used to attack the internal network, and the infrastructure previously used by the Red Eyes group was utilized. Many of the malware used in the attack were also discovered in South Korea in the fall of 2022.

Researchers from KrCERT presented the Lazarus group's activities in South Korea in 2022

[17] https://www.yna.co.kr/view/AKR20230818133200061?input=1195m (This link is only available in Korean)

[18] https://www.hauri.co.kr/security/security_view.html?intSeq=53&page=1&keyfield=&key= (This link is only available in Korean)

[19] https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA==&mid=2247493300&idx=1&sn=614dda72d95b5dfd732916aec0662598&chksm=f9c1d5bdceb65cab316de9e368fef6a997b82e96ed1a70b9b53ea8ae3c5698a8d4c95488e956&scene=132 (This link is only available in Chinese)

[20] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=f14822dd-03d5-4f25-8a10-cac4f008a25d

[21] https://www.sentinelone.com/labs/comrades-in-arms-north-korea-compromises-sanctioned-russian-missile-engineering-company/

and 2023 at the HITB conference.[22][23]

ReversingLabs has linked the VMConnect campaign,[24] which involved 24 malicious Python packages that were posted on the Python Package Index (PyPI) open-source repository,[25] to North Korea's Lazarus group.

15) MoustachedBouncher

Eset released information on the MoustachedBouncer group, which has been involved in espionage activities against foreign embassies in Belarus since 2014.[26]

MoustachedBouncer operates using email-based C&C protocols, C++ modular backdoors, and Adversary-in-the-Middle (AitM) attacks. Since 2020, they have been using devices managed with the AitM technique to redirect user authentication for captive portal scans in a network to their C&C server before infecting devices with malware via SMB shares. Recently, the group has been targeting diplomats by conducting AitM attacks at the ISP level in Belarus.

Disco and NightClub, which support features such as screen capture, audio recording, and exfiltrating, are the malware used in their attacks.

[22] https://conference.hitb.org/hitbsecconf2023hkt/session/lazarus-groups-undercover-operations/

[23] https://conference.hitb.org/hitbsecconf2023hkt/materials/D1T2%20-%20Lazarus%20Groups%20Undercover%20Operations%20-%20Large-Scale%20Infection%20Campaigns%202022%20%e2%80%93%202023%20-%20Lee%20Taewoo,%20Seulgi%20Lee,%20Dongwook%20Kim.pdf

[24] https://www.reversinglabs.com/blog/vmconnect-malicious-pypi-packages-imitate-popular-open-source-modules

[25] https://www.reversinglabs.com/blog/vmconnect-supply-chain-campaign-continues

[26] https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/

16) Mysterious Elephant (APT-K-47)

The Knownsec 404 Advanced Threat Intelligence team discovered the ORPCBackdoor malware targeting the Pakistani Ministry of Foreign Affairs in March 2023.[27] Initially, it was thought to be new malware from the Bitter group,[28], but it was later found to share similarities with Mysterious Elephant, a new APT group discovered by Kaspersky.

The threat actor sent emails containing a malicious CHM file to their attack targets. The attack tactics and code of the Mysterious Elephant group resemble those of the Bitter group.

17) Nobelium (Midnight Blizzard)

Microsoft identified the Nobelium (Midnight Blizzard) group conducting credential theft phishing attacks via Microsoft Teams chats in government, non-government organizations (NGOs), IT services, technology, individual manufacturing, and media sectors.[29]

The threat actor used hacked Microsoft 365 tenants owned by small businesses to create new domains that appear like technical support entities. They sent messages via Microsoft Teams while impersonating tech support or security teams to convince users to approve multi-factor authentication (MFA) prompts related to their accounts.

18) Red Eyes (APT37)

The Knownsec 404 team discovered a malicious CHM file and named it Fakecheck.[30] The CHM

[27] https://medium.com/@knownsec404team/apt-k-47-mysterious-elephant-a-new-apt-organization-in-south-asia-5c66f954477

[28] https://paper.seebug.org/2092/

[29] https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams

[30] https://medium.com/@knownsec404team/suspected-apt37-new-attack-weapon-fakecheck-analysis-report-c54a6991dd46

file attack that targeted Koreans is related to the blog post published by AhnLab in July 2023.[31] However, while some security researchers attributed this attack to the Red Eyes group, the Knownsec 404 team determined that there is a low level of connection between the two.

Conclusion

Information on a total of 18 APT groups was released in August 2023. The activities of the Andariel and Lazarus groups, which are believed to be backed by North Korea, have been observed outside their traditional conflict region in Korea. It has been revealed that these threat groups, which are suspected to have ties to North Korea, targeted the Russian defense industry.

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, CHM, or LNK disguised as a document file.

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 initiate preparation of the targeted attacks and techniques.

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

More security, More freedom

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.