AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on APT Groups

April 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

May 4, 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.

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.

The version information of this report is as follows:

Version	Date	Details
1.0	2023-05-04	First version

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 intelligence or destructive activities 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 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.

The details on APT groups may change without prior notice when new information or category is found.

APT Group Trends

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

1) APT28 (Fancy Bear, Sofacy)

Intelligence agencies in the UK[1] and the US[2] stated that APT28, suspected to be backed by the Russian government, used the vulnerability in Cisco routers (CVE-2017-6742) discovered in 2017 for reconnaissance and the distribution of Jaguar Tooth malware. As this is an old vulnerability, Cisco provides a patch as a countermeasure; enterprises or organizations that

[1] https://www.ncsc.gov.uk/news/uk-and-us-issue-warning-about-apt28-actors-exploiting-poorly-maintained-cisco-routers

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108

use Cisco routers must download the patch to protect themselves from the attack.

CERT-UA stated that the APT28 group attacked a Ukrainian government agency with an email titled "Windows Update".[3]

2) APT29 (Cozy Bear, Nobelium)

The Polish Military Counterintelligence Service and CERT Polska (CERT.PL) announced that the APT29 (Cozy Bear) group, which is suspected to be under the support of the Russian government, has been attacking NATO member countries, the EU, and Africa.[4]

The threat actor impersonated the embassy of a European country to send attack emails to diplomats. The main body of the message or attached PDF file included the ambassador's agenda, meeting details, or links to files that could be downloaded. When the user clicks the link, they are redirected to a malicious website. It was reported that malware, such as Snowyamber, Halfrig, and Quarterrig, was used for the attack.

3) Bitter

ASEC announced that the Bitter group has been attacking Chinese institutes with CHM file malware.[5] The CHM file inside the compressed file usually generates empty help windows, but some contain content related to Chinese institutes.

4) CNC

Antiy reported that the CNC group, active since 2019, has been attacking Chinese industries, including the military, scientific research, and education sectors.[6] The CNC group was named after "cnc_client", which was included in the PDB path information. The group sends an email with an attachment disguised as the "National Scientific Technology Performance Certification"

[3] https://cert.gov.ua/article/4492467

[4] https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services

[5] https://asec.ahnlab.com/en/51043/

[6] https://www.antiy.cn/research/notice&report/research_report/20230416.html

program, inducing the reader to open it. When the malware is triggered, it performs behaviors such as download and execution, host remote control, theft of sensitive files, theft of browser credentials, and propagation through removable storage devices.

5) Educated Manticore

Check Point released the information on the Educated Manticore group, stating that its activity coincides with the Phosphorus ransomware operating in the Middle East and North America suspected to originate from Iran.[7]

The group uses ISO images and other archive files with Iraq-themed lures to attack, which makes it highly likely that the targets were Israeli organizations. Implant PowerLess is the payload for final execution, and it is connected to some of the previous tasks of the Phosphorus ransomware, which performed the attack from an Iranian threat actor.[8]

6) Evasive Panda (Bronze Highland, Daggerfly)

Broadcom (formerly Symantec)[9] and Eset[10] released the activities of the Evasive Panda group, which is suspected to be supported by China.

Broadcom found plugins related to the MgBot malware in a campaign targeting an African telecommunications company, confirmed to utilize the PlugX loader and AnyDesk remote desktop software.[11]

[7] https://research.checkpoint.com/2023/educated-manticore-iran-aligned-threat-actor-targeting-israel-via-improved-arsenal-of-tools/

[8] https://www.microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/

[9] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot

[10] https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

[11] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/apt-attacks-telecoms-africa-mgbot

ESET announced that an attack targeting a Chinese non-governmental organization (NGO) was found, and the threat actor interfered with the update of Chinese software to distribute the MgBot malware.

The Evasive Panda group uses this malware, and it consists of the dropper, loader, and plugin.

7) Gallium (Alloy Taurus, Softcell)

The Gallium group is speculated to be backed by China, and they have been attacking telecommunications, financial, and government organizations across Southeast Asia, Europe, and Africa since 2012.

Unit 42 of Palo Alto Networks announced that they had found Gallium's PingPull variant[12] designed to target Linux systems and Sword2033.[13]

8) Gamaredon

In February 2023, EclecticIQ identified a spear phishing campaign targeting Ukrainian government agencies.[14]

Through investigations, the company found that the threat actor's Simple Mail Transfer Protocol (SMTP) server was exposed, and it contained a web panel designed to create and distribute spear phishing emails.

The activity is speculated to be from Gamaredon, a group known to have links with the Russian Federal Security Service (FSB), as its IP address matched the group's activities.

[12] https://atip.ahnlab.com/ti/contents/asec-notes?i=648dac47-24c2-4dfd-8fa8-2423a2a224f3

[13] https://unit42.paloaltonetworks.com/alloy-taurus/

[14] https://blog.eclecticiq.com/exposed-web-panel-reveals-gamaredon-groups-automated-spear-phishing-campaigns

9) Kimsuky

ASEC announced that there was a change in the number of arguments used for the execution of the AppleSeed malware from Kimsuky, a group suspected to be backed by North Korea.[15] Also, ASEC found that the installation script of "Google Chrome Remote Desktop" was distributed through the domain used for the spread of AppleSeed.[16] Generally, the Kimsuky group uses VNC-based remote control programs, such as TightVNC or TinyNuke.[17] Further research is therefore required to determine whether this means a change to Kimsuky's remote control program or merely a temporary usage.

10) Lazarus

Kaspersky released information on the recent activities related to Lazarus's DeathNote (Operation Dream Job) campaign. [18] Starting with the attack on areas related to cryptocurrency (virtual currency) in 2019, the campaign's attack has been focused on the defense industry since 2020. It is speculated that the attack on Korea involved malware distribution through software widely used in the country. Kaspersky provided an analysis of the malware used in the campaign, domain, C&C server, and technique. This information was also released at the BotConf 2023 under the title, "Perfect Smoke and Mirrors of Enemy: Following Lazarus group by tracking DeathNote".[19]

At the end of March 2023, 3CX software containing malware was installed due to damage to the software supply network. From its initial stage, the activity was suspected to be linked to Lazarus, a group backed by North Korea.[20]

[15] https://atip.ahnlab.com/ti/contents/asec-notes?i=490a3d22-d836-4b32-ba22-b0beeeeff037

[16] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=d7cbf437-188b-43f5-abc9-f8de6b69e3fe

[17] https://asec.ahnlab.com/en/27346/

[18] https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

[19] https://www.youtube.com/watch?v=ggsthAEH5LQ

[20] https://therecord.media/3cx-attack-north-korea-lazarus-group

In mid-April, Broadcom (formerly Symantec)[21] and Mandiant[22] released information on the malware used in the X-Trader supply chain attack related to the initial breach.

The United States Cybersecurity and Infrastructure Security Agency (CISA)[23] announced its analysis of the ICONICSTEALER malware downloaded by the malware inside the 3CX program, which is equipped with a backdoor feature that steals user credentials and receives commands.

Eset released information on the Linux malware discovered through the 3CX supply chain attack, stating its link to Lazarus.[24]
Through research and analysis, various security companies and the United States government institutes concluded that the malware shares relevance with the AppleJeus activity of the North Korea-backed Lazarus group.

11) Mantis (APT-C-23, Arid Viper, Desert Falcon)

The Mantis group has been active in the Middle East since 2014 (or 2011, according to some research). Broadcom (formerly Symantec) observed the group's attack on Palestinian organizations from September 2022 to February 2023.[25] The threat actors used updated versions of custom built Micropsia and Arid Gopher backdoors, but the specific infection method of this campaign is yet to be identified.

12) MuddyWater (Mango Storm)

MuddyWater, a group speculated to be supported by the Iranian Ministry of Intelligence and Security (MOIS), has been known to perform targeted attacks on insurance, manufacturing, and telecommunications companies in Israel and Egypt through legitimate remote control

[21] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

[22] https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

[23] https://www.cisa.gov/news-events/analysis-reports/ar23-110a

[24] https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

[25] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mantis-palestinian-attacks

tools such as ScreenConnect, RemoteUtilities, and Syncro.

Group-IB discovered that MuddyWater used SimpleHelp in the fall of 2022 and released related information.[26] MuddyWater is known to have first used SimpleHelp on June 30, 2022.

Meanwhile, K7Computing's K7 Labs announced information on the DarkBit malware that MuddyWater used.[27] The DarkBit ransomware uses an LNK file to execute PowerShell commands and collect user credentials. It encrypts files as its final step and initiates an attack that deletes them if the requirements are not met.

Microsoft detected the destructive task speculated to be linked to the Iranian government that attacks both on-premise and cloud environments.[28]

After gaining permission for initial access, the task attempted to maintain persistence through means such as web shell installation, the addition of a local user account and elevation of the administrator's privilege, installation of legitimate remote access tools, including RPort, Ligolo, and eHorus, installation of a custom-built PowerShell script backdoor, and credential theft. Upon setting up for persistence, the threat actor utilizes general default Windows tools and commands, such as netstat and nltest, for an extensive search.

The group used the credentials collected from the target environment to consistently perform widespread lateral movement tasks. They also utilized remote services to execute Windows Management Instrumentation (WMI) that carries out commands from the device, encoded PowerShell commands, and remote scheduled tasks that run the custom PowerShell backdoor.

13) Mustang Panda

K7Computing discovered that Mustang Panda APT uses a normal executable file of Opera Mail

[26] https://www.group-ib.com/blog/muddywater-infrastructure/

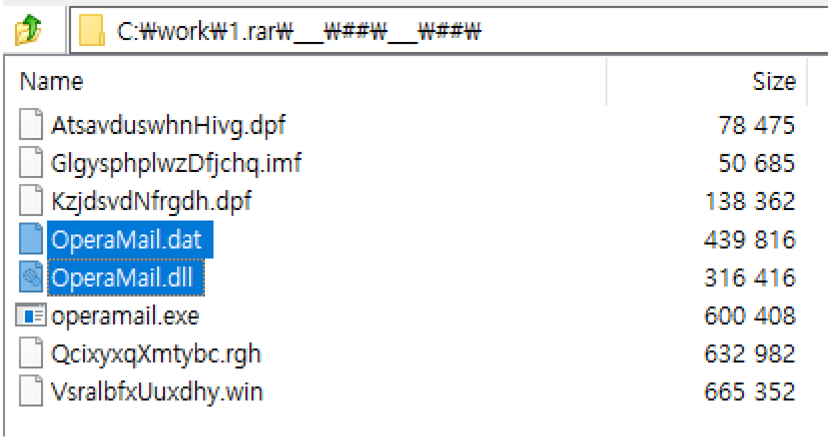
[27] https://labs.k7computing.com/index.php/muddywater-back-with-darkbit/

[28] https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/

to load a malicious DLL file and inject malware into the Mshta.exe process.[29]

A RAR file was used for the activity and inside it was a file named "2023 03 26 Vonulásos gyűlés – Körjegyzék.lnk", which translates to "March meeting – Circular list." When the user mistakes the LNK file for a document and clicks it, the PDF document about a rally in Budapest on March 26 opens before the malware is executed.

The file path inside the RAR file is similar to the details in Trend Micro's blog post on Mustang Panda.[30]



C:₩work₩1.rar₩__₩##₩__₩##₩

Name	Size
AtsavduswhnHivg.dpf	78 475
GlgysphplwzDfjchq.imf	50 685
KzjdsvdNfrgdh.dpf	138 362
OperaMail.dat	439 816
OperaMail.dll	316 416
operamail.exe	600 408
QcixyxqXmtybc.rgh	632 982
VsralbfxUuxdhy.win	665 352

Figure 1. Structure within the RAR file

14) RedEyes (APT37, ScarCruft)

ASEC discovered that the RedEyes attack group (also known as APT37 or ScarCruft) that had distributed the CHM malware disguised as a security email from a Korean financial company was also spreading the RokRAT malware through LNK files.[31] RokRAT can collect user credentials and download additional malware. In the past, the malware was distributed through Korean documents and Word files; however, the recently confirmed LNK file contains malicious PowerShell commands and disguises itself as a PDF icon related to seminars and North Korea. When the user clicks the LNK file, the malicious script code is executed along with the normal PDF file data.

[29] https://labs.k7computing.com/index.php/mustang-panda-pe-injection-through-opera-mail/

[30] https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html

[31] https://asec.ahnlab.com/en/51751/

Meanwhile, the RedEyes samples uploaded to GitHub[32] have been shared with malware detection services such as VirusTotal, which led to the release of related analyses[33] by various security companies.[34]

15) Tick and Tonto

Eset made a blog post about the attack on an East Asian DLP company in March, concluding that the threat actor responsible was Tick, a group speculated to be under the support of the Chinese government.[35] ASEC confirmed Tick's additional activities in Korea by analyzing the released IOC.[36]

Among various attack cases, ASEC was able to assume that Tick was also behind this incident after observing its similarities with the malware that used a CHM file in "Operation Triple Tiang". However, while investigating the attack using CHM files, the center discovered another case where the Tonto group used Bisonal-based malware.[37] Therefore, further research is required to determine which of the two groups, Tick or Tonto, was behind the attack related to Operation Triple Tiang. Some state the two were in a cooperative relationship, which may also lead to an argument that it was a joint attack by Tick and Tonto.

16) Tomiris

Kaspersky released information on Tomiris, a group similar to Turla.[38] Tomiris attacked various

[32] https://www.zscaler.com/blogs/security-research/unintentional-leak-glimpse-attack-vectors-apt37

[33] https://m.blog.naver.com/PostView.naver?blogId=best_somansa&logNo=223065761016&navType=by (this link is only available in Korean)

[34] https://download.hauri.net/DownSource/down/dwn_detail_down.html?uid=49

[35] https://www.welivesecurity.com/2023/03/14/slow-ticking-time-bomb-tick-apt-group-dlp-software-developer-east-asia/

[36] https://asec.ahnlab.com/en/51340/

[37] https://asec.ahnlab.com/en/51746/

[38] https://securelist.com/tomiris-called-they-want-their-turla-malware-back/109552/

organizations, such as foreign ministries, military authorities, defense ministries, private companies, academic research institutes, and the press in Central Asia, Eurasia, Europe, and the Asia-Pacific. Kaspersky's analysis is that the Tomiris group initiated the attack that had been classified to have come from Turla.[39] As well as using malware unique to the group, such as Jlorat, Roopy, and Telemiris, Tomiris sometimes utilizes open-source or commercial tools.

17) Transparent Tribe (APT36)

SentinelLabs stated that the Transparent Tribe group, speculated to be backed by Pakistan, has been expanding its activities in the educational sector of India.[40] Previously focused on targeting Indian military and government personnel, Transparent Tribe has recently been widening its attack scope to educational institutions and students of the Indian continent. The infection is caused by the Crimson RAT malware.

Uptycs announced that they discovered Poseidon, new Linux malware distributed by the Transparent Tribe group.[41] The threat actors created a backdoor version of Kavach, a two-factor authentication (2FA) solution provided by the Indian government for security access to email services, to target the staff of Indian government agencies.

18) SideCopy

The SideCopy group mainly targets Indian defense force personnel and military agents, collecting their information and using spear phishing technology to lure their victims of the Indian national defense and other government authorities or infecting USB devices to attack governmental and military organizations.

Team Cymru revealed the activities of SideCopy, told to be under the support of the Pakistani government.[42] The company identified additional malware samples and the C2 infrastructure

[39] https://www.mandiant.com/resources/blog/turla-galaxy-opportunity

[40] https://www.sentinelone.com/labs/transparent-tribe-apt36-pakistan-aligned-threat-actor-expands-interest-in-indian-education-sector/

[41] https://www.uptycs.com/blog/cyber_espionage_in_india_decoding_apt_36_new_linux_malware

[42] https://www.team-cymru.com/post/allakore-d-the-sidecopy-train

related to SideCopy's targeting of the Indian Ministry of Defence and found evidence of management activities sourced from a mobile IP in Pakistan, focusing on the key IP address linked to the group's use of Action RAT. Therefore, it could be said that another reliable proof has been added to the claim that SideCopy is a Pakistan-related threat actor group involved in nation-level spy activities.

The RedDrip Team from QiAnXin Threat Intelligence Center identified SideCopy's new activity.[43] The group disguised a downloader as a shortcut file and sent it to the victim; when the bait file is decompressed and executed, the program downloads the data file from the remote server to the local system. When the password is decrypted and the file is executed, the remote control software called AckRAT is installed.

Conclusion

The trend of APT groups in April 2023 shows that intelligence activities are still prevalent in regions of conflict, including Russia-Ukraine, India-Pakistan, and North Korea-South Korea.

It is commonly believed that blocking APT attacks equipped with enhanced techniques is impossible. However, while some attacks are carried out through reliable software, such as the 3CX supply chain attack, many government-led APT groups also utilize old malware infection methods, either by exploiting outdated vulnerabilities or by executable files disguised as links or document files.

The primary objective of nation-led threat actors is to infiltrate research institutes and industries in energy, security, political, diplomatic, and advanced technology areas. Therefore, those in such fields must establish step-by-step response systems to react to nation-led attacks and secure visibility in their internal systems. Also, we recommend they understand the trends of major threat groups through the Threat Intelligence service to become aware of attack targets and techniques.

[43] https://ti.qianxin.com/blog/articles/Sidecopy-Group-Launches-Attacks-on-India-Using-a-New-Trojan-EN/

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