AhnLab Cyber Threat Intelligence Report

TLP: GREEN

Threat Trend Report on APT Groups

September 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Oct 12, 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.

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

1) APT28

CERT-UA discovered targeted attacks by the APT28 group on critical energy infrastructure facilities in Ukraine.[1]

The attack was carried out via email. When a user clicks on a link, a bait JPG image and a ZIP file with a CMD extension are downloaded.

When the CMD file is executed, several bait web pages are opened, followed by the generation of BAT and VBS files. Afterward, the TOR program is downloaded, and communication is established through TOR for the group to attempt information gathering on the affected

[1] https://cert.gov.ua/article/5702579

system.

Remote execution is enabled through the webhook.site service's API. Additional details were disclosed by Splunk.[2]

2) APT29

Mandiant disclosed that during the first half of 2023, APT29 expanded its phishing operations in the diplomatic sector, observing various changes in security technologies as the attacker group sought to achieve its aim.[3]

These activities are primarily related to Ukraine, and Russia's Foreign Intelligence Service (SVR) is currently utilizing them for tactical information gathering. APT29 employs methods such as sending malicious file attachments in emails and including links to hacked websites.

3) APT33 (Peach Sandstorm)

Microsoft announced that the APT33 (Peach Sandstorm) group has been conducting a password spray campaign targeting thousands of organizations since February 2023.[4] Password spraying is a form of brute force attack that involves using password combinations that have been carefully calculated with high chances of success against the targeted user base to perform preemptive attacks. This method is used because too many failed login attempts can lock an account.

Microsoft assessed that APT33 (Peach Sandstorm)'s initial access campaign may be aimed at supporting Iran's national interests through information collection.

Between February and July 2023, the group conducted password spray attacks that attempted authentication on thousands of environments. If an account was successfully

[2] https://www.splunk.com/en_us/blog/security/mockbin-and-the-art-of-deception-tracing-adversaries-going-headless-and-mocking-apis.html

[3] https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing

[4] https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

authenticated via password spraying, APT33 members used AzureHound or Roadtools to perform reconnaissance on the Microsoft Entra ID (formerly Azure Active Directory).

In their efforts to access target environments, they also attempted attacks exploiting vulnerabilities in Zoho ManageEngine (CVE-2022-47966) and Confluence (CVE-2022-26134).

4) Andariel

360 released information on the Andariel group's EarlyRat malware variant.[5] The threat actor sent bait file download links through Skype. When a user activates the malicious macro, the threat actor would exfiltrate the user's information and execute malicious commands.

5) BlackTech

A government organization from the US issued a warning in collaboration with Japan regarding the BlackTech group suspected of being backed by China.[6] BlackTech primarily targets overseas subsidiaries of US and Japanese companies. After gaining initial access to the target company's network, the group obtains network administrator privileges and modifies the firmware of network equipment.

6) Charming Kitten

ESET discovered that the Charming Kitten group's new backdoor, Sponsor, has been used in attacks targeting Brazil, Israel, and the United Arab Emirates.[7]

The group exploited the Microsoft Exchange server vulnerability (CVE-2021-26855) for infection and utilized open-source tools such as Chisel, Mimikatz, Plink, and ProcDump.

The threat actors distributed batch files to the victim's system before deploying the Sponsor

[5] https://cn-sec.com/archives/2030846.html

[6] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-270a

[7] https://www.welivesecurity.com/en/eset-research/sponsor-batch-filed-whiskers-ballistic-bobcats-scan-strike-backdoor/

backdoor. The batch file does not operate without configuration files.

7) Dark River

Positive Technologies conducted an investigation into incidents in Russian industrial companies and discovered a new malware called MataDoor with the threat actor named as the DarkRiver group.[8]

Its initial attack method is suspected of involving phishing emails with DOCX document attachments, and a portion of the MataDoor that was used in the attacks is also linked to Lazarus' meta cluster.[9]

The names of the malware executables were similar to the names of legitimate software installed on systems, and a number of samples had valid digital signatures. The executable files and libraries were packed with Themida to make them more difficult to analyze.

8) Earth Lusca

Trend Micro confirmed attacks by the Earth Lusca group targeting government organizations related to diplomacy, technology, and communication sectors in Southeast Asian and Balkan Peninsula countries.[10]

The Earth Lusca group exploits vulnerabilities in public servers such as Fortinet (CVE-2022-40684 and CVE-2022-39952), GitLab (CVE-2021-22205), Zimbra Collaboration (CVE-2019-9670 and CVE-2019-9621), and Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207).

A new backdoor has also been discovered. This backdoor, called SprySOCKS, is built on the Linux platform and based on the open-source Windows backdoor Trochilus.

[8] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/dark-river-you-can-t-see-them-but-they-re-there/

[9] https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/dark-river-you-can-t-see-them-but-they-re-there/

[10] https://www.trendmicro.com/en_us/research/23/i/earth-lusca-employs-new-linux-backdoor.html

SprySOCKS provides robust features to perform various network activities alongside a SOCKS proxy. The group utilized this backdoor to infiltrate systems and deploy Cobalt Strike.

9) EvilBamboo

Volexity identified the EvilBamboo (EvilEye) group as actively targeting Tibet, Uyghur, and Taiwan individuals and organizations.[11]

It is suspected that this group operates in the interest of the Chinese government. In September 2019, it conducted operations using Android malware targeting Uyghur and Tibetan communities. In April 2020, the group used a Safari vulnerability to infect the iOS devices of Uyghur users with iOS malware.

10) Gallium (Alloy Taurus)

Palo Alto announced that the Gallium group suspected of having Chinese backing is conducting ongoing cyber espionage activities targeting government organizations in Southeast Asia.[12]

This group has been exploiting vulnerabilities in Exchange servers from early 2022 to the middle of 2023, infecting them with malware including web shells, GhostRAT, QuasarRAT, Reshell, and Winnti.

11) Gelsemium

Palo Alto disclosed the activities suspected to be from the Gelsemium group, which has attacked Southeast Asian government organizations.[13]

[11] https://www.volexity.com/blog/2023/09/22/evilbamboo-targets-mobile-devices-in-multi-year-campaign/

[12] https://unit42.paloaltonetworks.com/alloy-taurus-targets-se-asian-government/

[13] https://unit42.paloaltonetworks.com/rare-possible-gelsemium-attack-targets-se-asia/

Over a period of more than six months from 2022 to 2023, the threat actors secured a secret foothold and collected information from sensitive IIS servers within government organizations in Southeast Asia.

Major backdoors used in these activities include OwlProxy and SessionManager, which were employed in attacks on several organizations in 2020.

12) Kimsuky

AhnLab revealed an increase in the RandomQuery activity of the Kimsuky group.[14] PowerShell scripts are being obfuscated.

13) Konni

Knownsec404 Team revealed that the Konni group, which is suspected to be backed by North Korea, is exploiting the WinRAR vulnerability (CVE-2023-38831) to target the cryptocurrency industry.[15]

The threat actor sent a file named wallet_Screenshot_2023_09_06_Qbao_Network.rar to the victim. When the victim opens the Screenshot_2023_09_06_Qbao_Network.html file within the compressed archive, the system becomes infected with malware using the vulnerable WinRAR.

The malware checks system information and User Account Control (UAC) settings and uses the appropriate UAC bypass techniques to execute malicious programs with cryptocurrency-related features.

Genians disclosed cases of targeted attacks against personnel in the unification and North Korean human rights sectors.[16] The threat actor used email addresses similar to official emails

[14] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=a2fd94d8-5878-4855-a018-2bdc41677332 (This report supports Korean only for now.)

[15] https://medium.com/@knownsec404team/konni-apt-exploits-winrar-vulnerability-cve-2023-38831-targeting-the-cryptocurrency-industry-d97f6ea7d584

[16] https://www.genians.co.kr/blog/konniapt

to disguise the email as being sent from South Korea's Ministry of Unification and North Korean human rights organizations.

14) Lazarus

ESET revealed an attack case of the Lazarus group targeting an employee of a Spanish aerospace company through LinkedIn.[17]

The threat actor posed as a recruitment manager and contacted the victim through LinkedIn Messaging, deceiving the person into running the malware disguised as coding questions or quizzes seemingly as part of the hiring process.

In this attack, a new malware named LightlessCan was discovered. This malware exhibits more advanced features compared to the previous one BlindingCan and includes techniques to obstruct detection and analysis by security programs.

15) Lucky Mouse (APT27, Budworm)

Symantec discovered the activities of the LuckyMouse (Budworm, Emissary Panda, and APT27) group targeting telecommunication companies in the Middle East and governments in Asia.[18]

In this attack, a new version of the SysUpdate backdoor was discovered. However, aside from collecting authentication information, it did not exhibit other malicious activities.

16) Mustang Panda (Steately Taurus)

Palo Alto disclosed that the Mustang Panda (Stately Taurus) group, suspected to have Chinese backing, is conducting persistent cyberattacks against Southeast Asian governments.[19]

[17] https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/

[18] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-tool-update-telecoms-govt

[19] https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/

This group has been active from at least the second quarter of 2021 through the third quarter of 2023 and has exfiltrated sensitive documents and other file types.

Malware types such as Cobalt Strike, Shadowpad, and Toneshell were used in its attacks.

17) OilRig

ESET analyzed the attacks by the OilRig group against Israeli organizations in 2021 and 2022.[20] In both campaigns, Visual Basic Script (VBS) droppers were used.

Trend Micro discovered activities believed to be associated with the OilRig group that attacked Saudi Arabia.[21] The group distributed a new malware called Menorah, which bears similarities to the SideTwist backdoor.

18) Red Eyes (APT37)

AhnLab revealed that the Red Eyes group is still conducting attacks using CHM and LNK files.[22]

The group employs highly interesting topics to lure users into clicking, such as the release of Fukushima wastewater[23] and the North Korean leader's visit to Russia[24].

The malicious CHM or LNK files used in the attacks execute PowerShell scripts to carry out malicious activities.

19) Redfly

Symantec found evidence that the Redfly group used the ShadowPad malware to compromise

[20] https://www.welivesecurity.com/en/eset-research/oilrigs-outer-space-juicy-mix-same-ol-rig-new-drill-pipes/

[21] https://www.trendmicro.com/en_us/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html

[22] https://asec.ahnlab.com/en/56756/

[23] https://asec.ahnlab.com/en/56857/

[24] https://blog.alyac.co.kr/52519 (This link is only available in Korean.)

the national grid of an Asian country for up to six months.[25]

Although Redfly shares some similarities with APT41, it appears the group focuses more on attacking critical national infrastructures. It used ShadowPad, Keylogger, Packerloader, and other malware types in its attacks.

20) Sandman

SentinelLabs monitored the activities of the Sandman group which primarily targets telecommunications providers in the Middle East, Western Europe, and South Asia.[26]

The LuaDream malware used by the group relies on the LuaJIT platform which is relatively rarely used.

LuaJIT is typically used as a scripting middleware in games as well as special embedded applications and appliances.

21) Stealth Falcon

ESET discovered the Deadglyph malware attributed to the Stealth Falcon group which is suspected to be backed by the United Arab Emirates (UAE).[27] The Stealth Falcon group is carrying out espionage activities in the Middle East region.

Deadglyph is composed to have the x64 executable and .NET file work together, and backdoor commands are configured through the additional modules received from the C&C server.

22) Transparent Tribe

SentinelOne discovered the Transparent Tribe group's Android version of CapraRAT.[28]

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

[26] https://www.sentinelone.com/labs/sandman-apt-a-mystery-group-targeting-telcos-with-a-luajit-toolkit/

[27] https://www.welivesecurity.com/en/eset-research/stealth-falcon-preying-middle-eastern-skies-deadglyph/

[28] https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-

CapraRAT is based on the AndroRAT source code and is disguised as popular apps like YouTube. It can collect data from the microphones, cameras, SMS, etc. of infected Android devices and control that data.

Conclusion

Information on a total of 22 APT groups was released in September 2023. The ongoing Russia-Ukraine conflict has heightened espionage activities in the conflict area, and the activities of Chinese groups in Southeast Asia have also garnered attention. A few months ago, the activities of a North Korean threat group were identified targeting Russian defense companies. There is a possibility for attacks to be reduced in the future after the summit meeting between North Korea and Russia. Additionally, the Israel-Hamas war that started in early October 2023 raises concerns about cyberattacks by threat groups supporting either side.

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 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 prepare against their attack targets and techniques.

phones/

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 endpoints, networks, and clouds, 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