TLP: GREEN

Threat Trend Report on APT Groups

May 2023 Major Issues on APT Groups

V1.0

AhnLab Security Emergency response Center (ASEC)

Jun. 09, 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 liabilities.

Contents

Objectives and Scope 5
APT Group Trends 5
1) Agrius 5
2) Andariel 6
3) APT28 6
4) APT29 6
5) APT-C-36 (Blind Eagle) 6
6) Camaro Dragon 7
7) CloudWizard 7
8) Earth Longzhi (APT41) 8
9) GoldenJackal 8
10) Kimsuky 9
11) Lazarus 10
12) Lancefly 10
13) OilAlpha 11
14) Red Eyes (APT37, ScarCruft) 11
15) SideCopy 12
16) SideWinder 12
17) Transparent Tribe (APT36) 13
18) Volt Typhoon (Bronze Silhouette) 14
Conclusion 14

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

1) Agrius

Check Point analyzed the Moneybird ransomware that had attacked an Israeli organization and concluded that an Iran-based Agrius group was behind the attack.[1] The Agrius group, first discovered in 2021, targets Israeli organizations.

While new Moneybird ransomware was used, the Agrius group's tactics, techniques, and protocols (TTP) had not changed much.

[1] https://research.checkpoint.com/2023/agrius-deploys-moneybird-in-targeted-attacks-against-israeli-organizations/

2) Andariel

In 2023, DSCO identified new malware which they judged to be recent activities of the Andariel group's Jupiter malware.[2]

The Jupiter malware was first discovered in 2020 and is also included in CISA's IOC of the North Korean ransomware attacks. DSCO announced that the Jupiter malware is connected to an incident in Germany and to the sample found in the H0lyGhost ransomware IOC from CISA, US.

3) APT28

Sekoia announced that APT28, known to have ties to Russia's GRU, is attacking Ukrainian civil society.[3] Most phishing websites were disguised as a web email service popular in Ukraine.

4) APT29

Lab52 stated that the file uploaded to VirusTotal is similar to APT29's Quarterrig analyzed by CERT.PL in April 2023 and changes have been observed in Quarterrig since April.[4]

5) APT-C-36 (Blind Eagle)

While tracking the APT-C-36 (APT-Q-98, Blind Eagle) group that targeted Columbia since April 2018, the RedDrip team of QianXin Threat Intelligence Center found hundreds of bait PDF files having been uploaded from Columbia since 2022.[5]

---

[2] https://medium.com/@DCSO_CyTec/andariels-jupiter-malware-and-the-case-of-the-curious-c2-dbfe29f57499

[3] https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/

[4] https://lab52.io/blog/2162-2/

[5] https://ti.qianxin.com/blog/articles/Subgroup-of-Blind-Eagle-Analysis-of-Recent-Attack-Activities-from-Hagga-Group-EN/

Because the APT-C-36 and Hagga groups share very similar TTPs, the RedDrip team speculated the following three possibilities: the Hagga group is a subsidiary group of the Blind Eagle group, the Hagga group provided the Blind Eagle group with cyber weapons, or it is a simple case of TTP imitation.

6) Camaro Dragon

Check Point has been monitoring a series of targeted attacks against European diplomatic organizations since January 2023, which they named Camero Dragon.[6] They stated that many of this group's infrastructures have ties with the Mustang Panda group, but no specific details were given. There is a possibility that this group is a part of the activities of the Mustang Panda group.

During the investigation, a modified custom firmware for the TP-Link router was discovered, and Horse Shell was found in the firmware image. Horse Shell provides threat actors with a remote shell, file transfer, and SOCKS tunneling features. Check Point stated that the method of distributing the firmware image to infected routers and its use in and connection to actual infiltration incidents are unknown.

7) CloudWizard

Kaspersky found CloudWizard active in mid-West Ukraine.[7]

CloudWizard's malware used parts of leaked source codes or those uploaded to GitHub and included features such as taking screenshots, recording the mic, and keylogging.

Through similar codes and PDB paths, Kaspersky found evidence of the group's connection to Operation Groundbait and Operation BugDrop disclosed in 2017 and announced that this

[6] https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/

[7] https://securelist.com/cloudwizard-apt/109722/

group is behind PowerMagic and CommonMagic disclosed in March 2023.[8]

Because the initial version of the Prikormka malware used by this group was discovered in 2008, this group seems to have been active for over 15 years.

Relevant information was presented at the Positive Hack Days conference.[9]

8) Earth Longzhi (APT41)

Trend Micro announced that Earth Longzhi, a subsidiary group of APT41, has been launching attacks against governments as well as medical, technical, and manufacturing industries of the Philippines, Thailand, Taiwan, and Fiji.[10]

Earth Longzhi had also launched attacks on various sectors such as government organizations and financial and military industries. Recently, the group has been launching attacks against major corporations in the field of security.

Bait documents in Vietnamese and Indonesian were also found, so it is highly likely that users in these countries will also become targets of attack.

Croxloader is the malware used in the attacks.

9) GoldenJackal

Kaspersky released information on the GoldenJackal group which targets government and diplomatic organizations of Afghanistan, Azerbaijan, Iran, Iraq, Pakistan, and Türkiye.[11]

Infections through a fake Skype installer, malicious Word documents, and malicious HTML web pages which exploit the Follina vulnerability were found.

---

[8] https://securelist.com/bad-magic-apt/109087/

[9] https://phdays.com/en/broadcast/?tag=defense&talk=228

[10] https://www.trendmicro.com/en_us/research/23/e/attack-on-security-titans-earth-longzhi-returns-with-new-tricks.html

[11] https://securelist.com/goldenjackal-apt-group/109677/

The malware used by this group are JackalControl, JackalWorm, JackalSteal, JackalPerInfo, and JackalScreenWatcher.

10) Kimsuky

SentinelOne discovered the Kimsuky group's attempt at ReconShark malware infection against a certain individual by sending a malicious OneDrive link and a document containing a macro.[12] A few days later, SentinelOne additionally revealed that the group is continuously attacking North Korean intelligence services, human rights activists, and support groups for North Korean defectors by using the RandomQuery malware in the Microsoft Compiled HTML Help (CHM) format.[13]

S2W released analysis details on AlphaSeed, new malware used by the Kimsuky group.[14] AlphaSeed is a new version of AppleSeed developed in Go programming language. This malware, containing the path "E:/Go_Project/src/alpha/naver_crawl_spy/", was named AlphaSeed by S2W Talon, and it has been confirmed that the Kimsuky group is recently using the Go language to build malware. It has a similar file encryption method, mail transfer thread, and email inbox names to the past AppleSeed.

In the May 2023 Threat Trend Report on Kimsuky Group,[15] AhnLab announced that the number of identified malware has increased slightly in comparison to April. Additionally, it stated that new top-level domains (TLD) have begun to be detected and that there were slight changes to the FlowerPower malware code as well.

---

[12] https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/

[13] https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/

[14] https://medium.com/s2wblog/detailed-analysis-of-alphaseed-a-new-version-of-kimsukys-appleseed-written-in-golang-2c885cce352a

[15] https://atip.ahnlab.com/ti/contents/regular-report/monthly?i=80818237-c5e4-43f6-944d-705cf350c1db

11) Lazarus

AhnLab has confirmed that the Lazarus group is launching attacks against Windows IIS web servers.[16] It is assumed that the threat actor uses poorly managed or vulnerable web servers as their initial intrusion points after which they executed malicious commands. The threat actor installed a backdoor and used port 3389 for lateral movement.

Sekoia.io discovered new malware targeting MacOS platforms in the RustBucket campaign of Bluenoroff, a subsidiary group of Lazarus.[17]

12) Lancefly

Broadcom (formerly Symantec) announced that since mid-2022, the Lancefly group has been using the Merdoor backdoor for many years to attack government and aviation organizations of South and Southeast Asia.[18]

In 2020, the group launched attacks with phishing emails with the subject '37th ASEAN Summit', but the infection route has not been confirmed in recent activities. While not conclusive, it is said that in two attack targets, signs of SSH brute forcing and exposure of the shared server were found.

The Lancefly group uses the Merdoor malware and ZXShell Rootkit. The Merdoor malware which is comprised of a normal file, a loader, and an encrypted file, was first found in 2018. It was used very selectively, being detected in only a small number of networks and systems over many years.

[16] https://asec.ahnlab.com/en/53132/

[17] https://blog.sekoia.io/bluenoroffs-rustbucket-campaign/

[18] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lancefly-merdoor-zxshell-custom-backdoor

13) OilAlpha

Recorded Future released information on OilAlpha which has been active since May 2022.[19]

This threat group is thought to be connected with Yemen's Houthis (armed group of Islamic Zaidiyyah Shia), but there is no evidence that their attacks are being performed by Yemeni agents.

Attack targets include non-governmental organizations, media, and organizations related to international humanity and development. This group usually targets organizations that show an interest in Yemen-related issues in the field of security, humanity, and restoration, but they have a variety of targets, such as individuals that participate in Saudi Arabian government-led negotiations.

For this, they employ a method of spoofing through an app they developed, impersonating organizations such as those related to the Saudi government and humanitarian organizations of UAE who have similar purposes as theirs.

14) Red Eyes (APT37, ScarCruft)

Check Point,[20] 360,[21] Genians,[22] and ThreatMon[23] released analysis details on the Rokrat malware of the Red Eyes (APT37, Inky Squid, Reaper, ScarCruft) group.

Following its first discovery in 2017, not only Windows, Rokrat was found to have versions for Windows, Android, and even macOS. While no significant changes have been made to the malware, its distribution methods have evolved to use ISO and LNK files. Bait documents usually focus on diplomacy and issues in Korea, and their targets seem to be Korean users as

[19] https://www.recordedfuture.com/oilalpha-likely-pro-houthi-group-targeting-arabian-peninsula

[20] https://research.checkpoint.com/2023/chain-reaction-rokrats-missing-link/

[21] https://mp.weixin.qq.com/s/RjvwKH6UBETzUVtXje_bIA

[22] https://www.genians.co.kr/blog/threat_intelligence_report_apt37

[23] https://threatmon.io/reverse-engineering-rokrat-a-closer-look-at-apt37s-onedrive-based-attack-vector/

most are written in Korean.

The multi-stage infection chain used to load Rokrat signifies that this can be used in other attacks and lead to the distribution of additional tools related to the same operator, including Goldbackdoor, another tailor-made backdoor, and Amadey, commercial malware.

AhnLab[24] found traces of the distribution of malware disguised as a Hancom Office document file. The name of the distributed malware is 'Who and What Threatens the World (Column).exe' and has a similar icon to the Hancom office document to deceive users into perceiving the file as one. Upon execution, it maintains persistence by registering to the Task Scheduler, then connects to the C2 to download and execute the Chinotto script. Traces of malware distribution using websites created by a certain website development company have also been found.[25]

15) SideCopy

Fortinet found files that mention India's state-run military research institute and nuclear missiles in development and stated that their characteristics match those of the SideCopy group.[26]

The initial infection vector is suspected to be phishing emails. Starting with an LNK file, it downloads and executes an HTA file from the C2 before ultimately infecting the target system with a DLL-type backdoor.

16) SideWinder

BlackBerry identified the latest campaign targeting Pakistani government organizations and Türkiye.[27]

---

[24] https://asec.ahnlab.com/en/53377/

[25] https://atip.ahnlab.com/ti/contents/asec-notes?i=9973a52b-a27b-41a6-b4ec-8fa4536f20d5

[26] https://www.fortinet.com/blog/threat-research/clean-rooms-nuclear-missiles-and-sidecopy

[27] https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

This seems to be a new campaign of the SideWinder group, and it used the server-side polymorphism technique to deliver the next stage payload. The attacks began in late November of 2022.

The malicious documents used in this campaign were written for Pakistani government officials and were disguised to look like proposals and acceptance letters for defense items and service purchases. None of the documents used malicious embedded macro codes to deliver the next payload; instead, the threat group exploited the CVE-2017-0199 vulnerability (remote template injection). While the malicious server was in service, this threat group configured the server to redirect users/victims to a legal Pakistani marine website when they enter a portion of the malicious URL in their browser.

Group-IB[28] and Bridewell[29] provided specific details on SideWinder's infrastructure that had not been known before. The identified phishing domains were disguised as various organizations in the news, government, communications, and financial sectors, signifying that SideWinder not only planned attacks on Pakistani and Chinese e-commerce and mass media companies but also on financial and government organizations.

17) Transparent Tribe (APT36)

The Quick Heal APT team disclosed information on the activities of the Transparent Tribe group that attacks the national defense and education sectors of India.[30] The group attacked the Indian military with a file named 'Officers posting policy reviseed final.ppam', and their attacks against the education sector using documents containing macro have been increasing since 2022. Opening the document file infects the system with the CrimsonRAT malware.

[28] https://www.group-ib.com/blog/hunting-sidewinder/

[29] https://www.bridewell.com/insights/news/detail/the-distinctive-rattle-of-apt-sidewinder

[30] https://www.seqrite.com/blog/transparent-tribe-apt-actively-lures-indian-army-amidst-increased-targeting-of-educational-institutions

18) Volt Typhoon (Bronze Silhouette)

CISA[31] and Microsoft[32] released information on the Volt Typhoon group deemed to be backed by China and known for its attack on the core infrastructure systems of Guam and other regions of the US.

Volt Typhoon is also known as Bronze Silhouette[33] and has apparently been active since mid-2021, targeting organizations related to manufacturing, construction, marine, government, information technology (IT), and education.

It utilizes damaged small office/home office (SOHO) network devices as an intermediary infrastructure and has most of the command and control (C2) traffic emanate from a local ISP in the geographical location of the user, concealing the group's activities.

Conclusion

In May 2023, information on a total of 18 APT groups (19 APT groups according to the information that was removed after its release) was released, the same number as that of April. Strong levels of espionage activities were detected in areas of conflict including Russia-Ukraine, India-Pakistan, and South Korea-North Korea. Information on new threat groups that target various Asian countries was also released.

The trends of this month showed that threat groups mostly use executable files disguised as links or documents with content that the target may be interested in instead of developing new methods of attacks. On the other hand, network device firmware manipulation by the Camero Dragon group and network device attacks by the Volt Typhoon group are notable.

---

[31] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[32] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[33] https://www.secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations

Attacking network devices and programs instead of through email is more efficient for attack concealment, and thus similar attack attempts are forecasted.

The main targets of state-supported threat groups are research institutes and industries related to national security, energy, diplomacy, politics, and cutting-edge technology. As such, these sectors must prepare a stage-by-stage response system to defend against state-led attacks and ensure visibility for their internal systems. It is also advised to be aware of the trends of major threat groups through threat intelligence (TI) services in preparation for 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

© AhnLab, Inc. All rights reserved.

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