August 2025 Threat Trend Report on APT Groups

Source: AHNLAB

URL: https://asec.ahnlab.com/en/90104/

Published: N/A

Crawled: 2026-01-18T21:49:36.753783

Purpose and Scope

This report covers nation-led threat groups, presumed to conduct cyber espionage or sabotage supported by certain governments. These groups are 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.

By understanding their attack motivations, strategies, and technical characteristics, we aim to improve an organization's security response capabilities and use this report as a reference to prepare for future threats.

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.

Major APT Group Trends by Region

1) North Korea

North Korea-linked APT groups focused on South Korea, targeting the diplomatic, financial, technological, media, and policy research sectors with sophisticated cyberattacks. They utilized various malware strains, social engineering techniques, and cloud-based C2 infrastructure, and were notable for their detailed spear phishing campaigns. The groups combined various infiltration techniques such as LNK-based and PowerShell-based loaders, steganography (JPEG hiding), and fileless methods to distribute RAT and information-stealing malware. Also, there have been cases of legitimate platforms like GitHub, pCloud, Dropbox, Yandex, and PubNub being leveraged as command and control servers. The technical diversity and expansion of attack targets have become evident with cryptocurrency wallet and credential exfiltration, attacks targeting macOS users, and Rust-based backdoor and ransomware deployment.

Kimsuky

The state-sponsored group linked to North Korea, Kimsuky impersonated Korean media employees to conduct spear phishing attacks targeting individuals affiliated with policy research institutes, using malicious LNK files and PowerShell to induce RAT infections.

Case 1.	
Period	Unknown
Attack Target	A specific individual affiliated with a Korean non-profit private policy research institute
Initial Breach	· An email reply posing as a media representative includes a large attachment link from a Korean portal mail service, inducing the victim to download an encrypted ZIP file · There is an LNK file disguised as a Chrome icon inside the zip file, which runs the PowerShell code upon execution
Vulnerability Used	· None
Malware and Tools	· Trojan.Agent.LNK.Gen · Trojan.PowerShell.Agent · 7hweuyd.ps1, chrome.ps1, temp.ps1, and system_first.ps1 (malicious LNK files and PowerShell

	scripts)
Technique	· Executing the Base64-encoded PowerShell code · Saving scripts in the %TEMP% and %APPDATA% paths and executing them · Registering to the scheduler (30-minute interval, “MicrorfteguesoftUpdata1logiveKentwuerwtySchule”) · Downloading decoy PDF and additional scripts (ofx.txt and onf.txt) from the C2 server
Damage	· Unknown
Description	· An attack method that impersonates legitimate media company emails to gain the victim’s trust and prompts the execution of malicious files · Performs a step-by-step attack in the order of LNK–PowerShell–maintaining persistence–downloading C2 · Analysis shows a high similarity to the typical attack patterns of the North Korean state-sponsored group Kimsuky, suggesting the group’s involvement
Source	· North Korean hacking groups posing as media companies in spear phishing attacks![1]

In the first half of 2025, a spear phishing campaign was conducted targeting diplomatic missions in Korea, abusing GitHub as a C2 and distributing XenoRAT variants.

Case 2.	
Period	· Attack activities from March 6th, 2025 to July 28th, 2025
Attack Target	Seoul-based European diplomatic missions and Ministry of Foreign Affairs personnel (Western Europe, Central Europe, Eastern Europe, and Southern Europe)
Initial Breach	· Spear phishing emails impersonating diplomats or embassy officials · Password-protected ZIP attachment (including cloud link) executes a double extension LNK disguised as a PDF
Vulnerability Used	· None
Malware and Tools	· XenoRAT variant (.NET, obfuscated with Confuser Core 1.6.0) · LNK dropper and PowerShell script · GitHub (Contents API), Dropbox, and Daum large file attachment service
Technique	· Emails disguised as diplomatic events and documents, customized based on social engineering techniques · PowerShell script in-memory load (Base64 decoding and .NET assembly reflection after modifying the GZIP header)

	· Uploading data through GitHub API and requesting RAT payload via the onf.txt file · Maintaining persistence by registering to the scheduler · Evading detection by using cloud-based infrastructure and quickly replacing payloads
Damage	· Unknown
Description	· The state-sponsored group Kimsuky (APT43) linked to North Korea sent phishing emails impersonating diplomats and embassy staff and distributed malicious LNK files · If the files are executed, XenoRAT is downloaded through PowerShell, allowing access to diplomatic secrets and enabling long-term spying activities · The use of GitHub and Dropbox-based C2, ensuring persistence through a scheduler, and multilingual diplomatic document disguise techniques in the campaign are similar to past Kimsuky operations, attributing the case to this group
Source	· The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign[2]

[1] https://blog.alyac.co.kr/5620

[2] https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

Tags:

APT41 APTDown APTGroups APTGroupsReport bitter CurlyCOMrades Gamaredon HAFNIUM Kimsuky Larva-25010 Lazarus MuddyWater Patchwork ShadowSilk SideWinder StaticTundra TA-RedAnt TransparentTribe UAT-7237 UNC6384
