Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

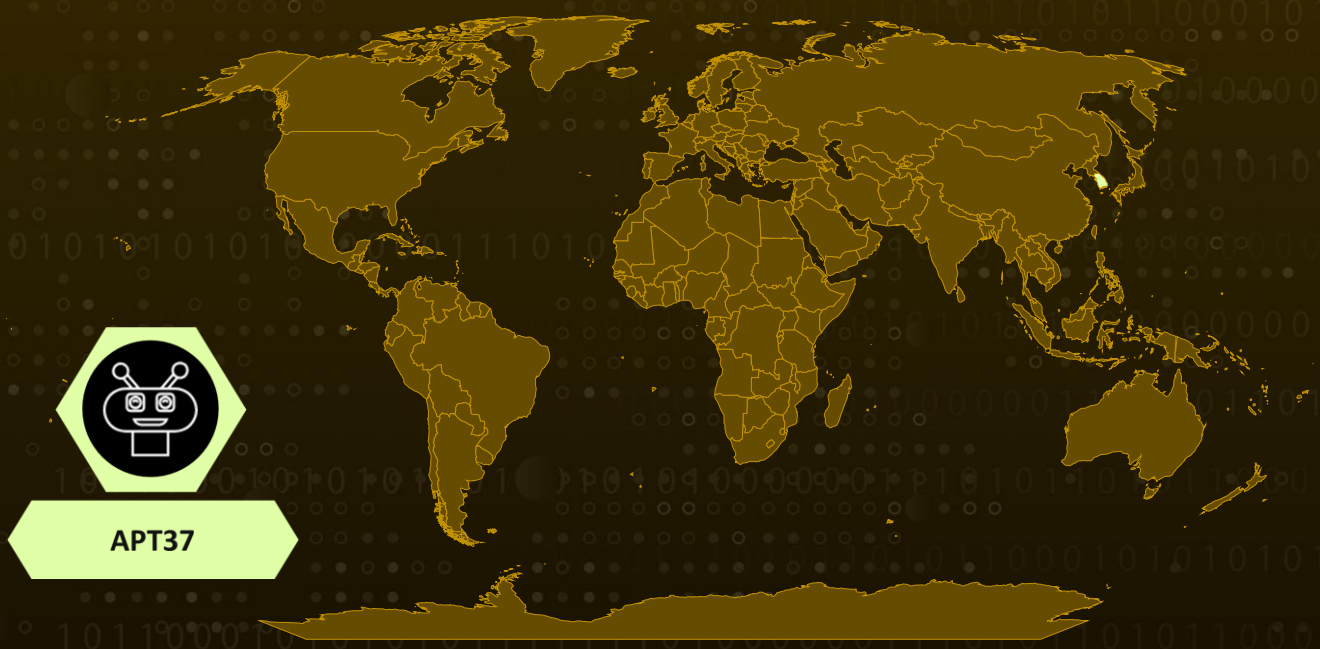
Operation HanKook Phantom: APT37's Stealthy Espionage Campaign

Date of Publication	Admiralty Code	TA Number
September 3, 2025	A1	TA2025265

Summary

Attack Discovered: 2025
Targeted Countries: South Korea
Targeted Industries: Academic, Government officials, and Researchers
Affected Platform: Windows
Malware: RokRAT
Actor: APT37 (aka Reaper, TEMP.Reaper ,Ricochet Chollima, ScarCruft, Cerium, Group 123,Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet, TA-RedAnt, G0067)
Campaign: Operation HanKook Phantom
Attack: APT37, a North Korean hacking group, is running a stealthy espionage campaign called Operation HanKook Phantom. Using fake newsletters and weaponized shortcut files, they trick victims into opening decoys that silently unleash fileless malware. Once inside, the attackers steal sensitive data and hide their tracks, relying on trusted cloud services like Dropbox and pCloud to move information out unnoticed. The campaign highlights how something as ordinary as a shortcut file can open the door to a full-scale espionage operation.

Attack Regions



Attack Details

#1 APT37, a North Korean cyber espionage group, has launched a new campaign dubbed Operation HanKook Phantom, using carefully crafted decoy documents to trick victims into opening malicious files. One such lure is the newsletter, disguised as a legitimate publication from a South Korean research association. Alongside this PDF, attackers distribute a weaponized LNK file that triggers the download of hidden payloads or executes remote commands, ultimately compromising the victim's system. The primary focus appears to be individuals tied to the National Intelligence Research Association, with the likely goal of stealing sensitive intelligence and conducting long-term surveillance.

#2 APT37 has also deployed other spear-phishing lures. By leveraging trusted content related to intelligence and national security, the group effectively disguises its operations. Once executed, these files kickstart a multi-stage infection chain designed to quietly infiltrate systems and extract valuable data without raising immediate alarms.

#3 The malicious LNK file reveals a sophisticated infection process. When launched, embedded PowerShell scripts extract multiple payloads from within the file, including disguised PDFs and binary loaders. These components are written to the system's temporary directory, where a batch script executes further stages of the attack. The infection unfolds in memory, relying on fileless techniques that make detection and forensic analysis significantly harder. The final payload, ROKRAT malware, is then deployed, equipped to fingerprint the host, capture screenshots, and gather detailed system information, all while communicating with cloud services like pCloud, Yandex, and Dropbox to evade traditional security monitoring.

#4 APT37's operations also extend beyond intelligence lures to politically charged content. In another wave of attacks, the group weaponized a document attributed to Kim Yo-jong, criticizing South Korea's reconciliation efforts under President Lee Jae-myung. The malicious file followed the same LNK-based execution chain, dropping obfuscated scripts and encoded payloads into the victim's system. By decoding and running these payloads directly in memory, attackers avoided leaving permanent traces, allowing them to stealthily exfiltrate files disguised as PDF uploads via HTTP POST requests before erasing evidence from local machines.

#5 These activities reinforce the urgency for defenders to closely monitor LNK-based delivery mechanisms and deploy advanced detection strategies capable of catching memory-resident threats before they slip away unseen.

Recommendations

- **Be cautious with unexpected files:** Avoid opening newsletters, PDFs, or shortcut (LNK) files received over email unless you are absolutely sure of the sender. Even if a file looks familiar, attackers often disguise malware inside trusted-looking documents.
- **Watch for suspicious LNK files:** Malicious shortcuts often come with double extensions (like filename.pdf.lnk) to trick you into thinking they are safe. Train staff to spot and report such files instead of opening them.
- **Encourage a "pause before click" culture:** Attackers thrive on trust. Remind employees, especially those in sensitive departments, to slow down before interacting with unsolicited attachments or documents, and to verify with the sender when in doubt.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1566 Phishing
T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1204 User Execution
T1204.001 Malicious Link	T1204.002 Malicious File	T1574 Hijack Execution Flow	T1574.001 DLL

T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1055 Process Injection	T1055.001 Dynamic-link Library Injection
T1055.009 Proc Memory	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1140 Deobfuscate/Decode Files or Information
T1070 Indicator Removal	T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1027.009 Embedded Payloads
T1027.013 Encrypted/Encoded File	T1056 Input Capture	T1056.002 GUI Input Capture	T1087 Account Discovery
T1087.001 Local Account	T1217 Browser Information Discovery	T1083 File and Directory Discovery	T1082 System Information Discovery
T1123 Audio Capture	T1005 Data from Local System	T1113 Screen Capture	T1102 Web Service
T1102.002 Bidirectional Communication	T1041 Exfiltration Over C2 Channel	T1529 System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1aec7b1227060a987d5cb6f17782e76e, 591b2aaf1732c8a656b5c602875cbdd9, d035135e190fb6121faa7630e4a45eed, cc1522fb2121cf4ae57278921a5965da, 2dc20d55d248e8a99afbe5edaae5d2fc, f34fa3d0329642615c17061e252c6afe, 051517b5b685116c2f4f1e6b535eb4cb, da05d6ab72290ca064916324cbc86bab, 443a00feeb3beaea02b2fbcd4302a3c9, f6d72abf9ca654a20bbaf23ea1c10a55

TYPE	VALUE
SHA256	eb9ab1de159d7bf96af0fe0c6e6e1acd120b76d339b8f8acd38b2e3279c21f5f, 06a297eb80274e0821516cb1b0025a231c5b63ae5ab30b84b2d10f6350d4f484, 863295b41441bfe25b970f1f89768fad33826f5e3c379cea595c174ad37244f9, f69e102fa65174b2c4821003bde36af264f8ef73bc7ca2ce0d97c43ee3e9e21a, d8d86b15e68889bf76b3cf8e335f43afe0287b9b20aeb18b136b90a516695989, ccb6ca4cb385db50dad2e3b7c68a90ddee62398edb0fd41afdb793287cfbe8e6, 90bf1f20f962d04f8ae3f936d0f9046da28a75fa2fb37f267ff0453f272c60a0
Filenames	aio02.dat, aio03.bat, aio01.dat, *.Zip, tony31.dat, tony32.dat, tony33.bat, *.LNK

References

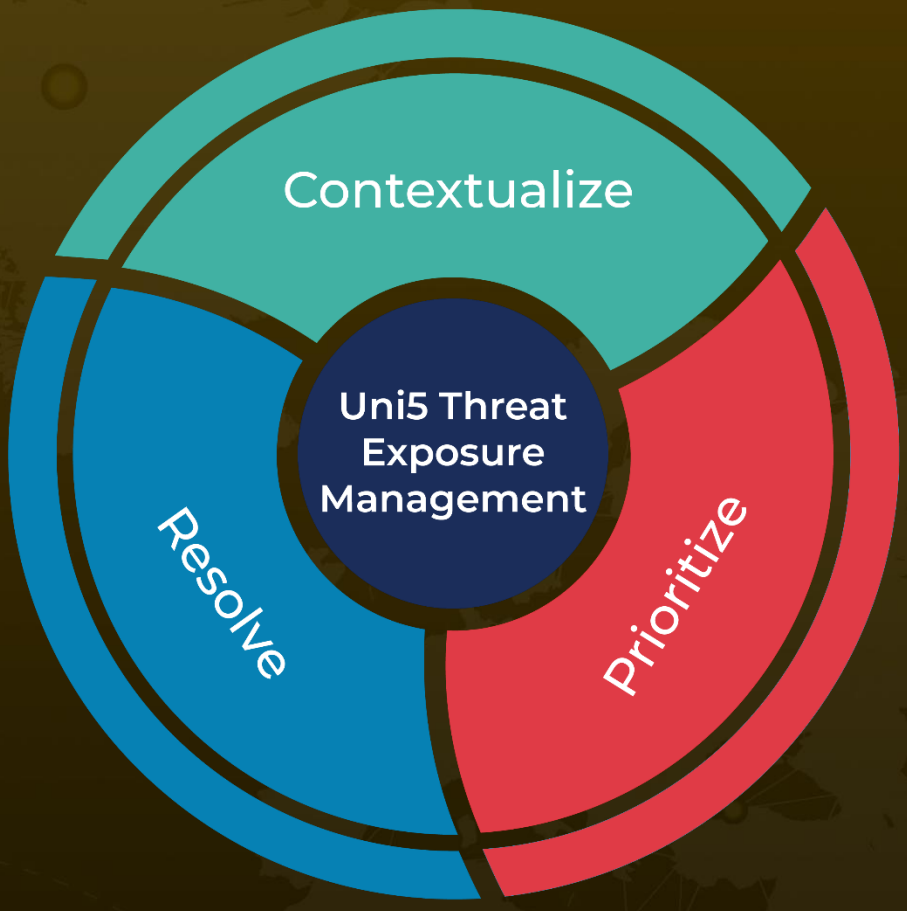
https://www.seqrite.com/blog/operation-hankook-phantom-north-korean-apt37-targeting-south-korea/

https://hivepro.com/threat-advisory/rokrat-resurfaces-apt37s-fileless-shortcut-to-espionage/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 3, 2025 • 5:20 AM

More at www.hivepro.com