Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

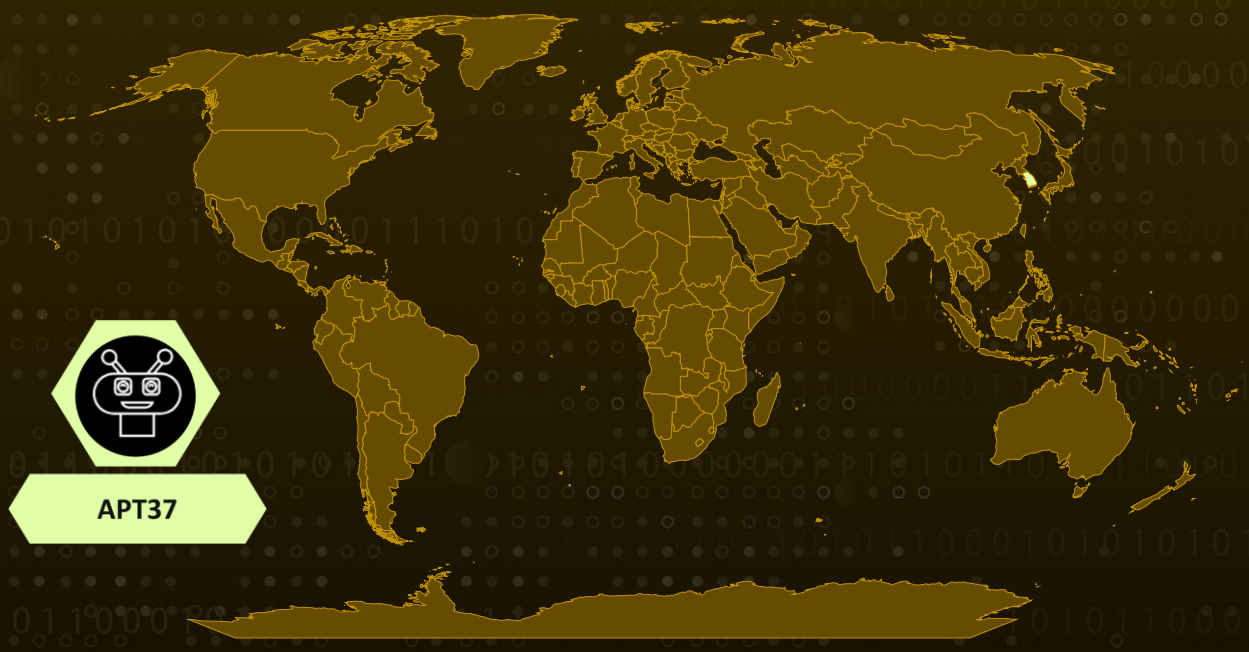
RoKRAT Resurfaces: APT37's Fileless Shortcut to Espionage

Date of Publication	Admiralty Code	TA Number
August 5, 2025	A1	TA2025238

Summary

Attack Discovered: 2025
Targeted Country: South Korea
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)
Attack: APT37, a North Korean-linked threat group, is back in action with a stealthy new variant of its RoKRAT malware, using shortcut (.lnk) files and image-based steganography to infect targets primarily in South Korea. The malware hides inside compressed archives and JPEG images, deploying a series of scripts and shellcode to spy on infected systems. It collects screenshots, system info, and documents, then exfiltrates the data through trusted cloud services like Dropbox and pCloud. This sophisticated, fileless attack chain highlights the growing challenge for traditional security tools and stresses the importance of advanced threat detection.

Attack Regions



Attack Details

#1 A newly discovered variant of the **RoKRAT** malware, attributed to the North Korean APT group **APT37**, is raising alarms particularly in South Korea. This latest attack campaign uses malicious shortcut (.lnk) files to deliver its payload, hidden inside a zipped file titled “국가정보와 방첩 원고.zip” (translated: National Intelligence and Counterintelligence Manuscript). When opened, it lures victims with a legitimate-looking HWP document while silently triggering a chain of scripts and shellcode in the background. The attackers use a combination of PowerShell and batch scripts to decode and load malicious components embedded in the archive.

#2 What makes this malware particularly deceptive is the use of XOR-based obfuscation, which helps it stay under the radar of traditional antivirus tools. By reverse-engineering the shellcode, it was discovered it begins decoding at a specific memory offset using a single-byte XOR key. The decoded result turns out to be a 32-bit executable created back in April 2025. Interestingly, the malware tries to blend in by launching mspaint.exe, a common Windows app and then injecting its payload into it, helping the malicious code operate unnoticed.

#3 In another wave of attacks, APT37 disguised RoKRAT as a legitimate system file called mpr.dll. These variants were delivered via weaponised HWP documents containing malicious OLE objects. If a victim clicks a hyperlink embedded in the document, a fake prompt encourages them to run ShellRunas.exe. If they comply, a second malicious module, credui.dll, is silently activated. This module downloads an image file from Dropbox that, on the surface, appears to be a harmless JPEG. However, it secretly contains the RoKRAT malware hidden through steganography, a technique where malicious code is embedded inside seemingly harmless files.

#4 The image file is decoded in two XOR stages, eventually revealing the malware hidden within. This is a sophisticated example of fileless malware, meaning it runs entirely in memory, leaving minimal forensic trace on the hard drive. It is also discovered that the access tokens tied to cloud services like Dropbox, pCloud, and Yandex, which RoKRAT uses to exfiltrate stolen data. This includes sensitive documents, screenshots, and system information. While some of the Dropbox accounts were traced back to Yandex email addresses.

#5 Given the advanced evasion techniques, from masquerading as trusted files to hiding in images, traditional signature-based detection methods may not be enough. Organisations especially in high-risk regions like South Korea should strengthen their defenses with EDR or MDR solutions capable of detecting fileless activity and unusual outbound cloud communications.

Recommendations

Be Careful with Documents and Emails: The first line of defense is you! Be suspicious of unexpected files or emails, even if they look legitimate. If a coworker sends you an odd document or if a message seems a little off, it's best to double-check with them directly. Never click on a link or enable content in a document unless you are 100% sure it's safe.

Keep Your Software Updated: Always make sure your operating system and all your applications are up to date. These updates often include patches that fix vulnerabilities the little cracks in your security that attackers love to exploit.

Monitor for Unusual Activity: Set up alerts for unusual behavior, such as unexpected logins, privilege escalations, or changes in virtualization infrastructure. Use behavioral analytics where possible.

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	TA0005 Defense Evasion
TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1204 User Execution

T1027 Obfuscated Files or Information	**T1027.003** Steganography	**T1140** Deobfuscate/Decode Files or Information	**T1574** Hijack Execution Flow
T1574.001 DLL	**T1036** Masquerading	**T1113** Screen Capture	**T1041** Exfiltration Over C2 Channel
T1071 Application Layer Protocol	**T1218** System Binary Proxy Execution	**T1218.011** Rundll32	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a2ee8d2aa9f79551eb5dd8f9610ad557, ae7e18a62abb7f93b657276dcae985b9, d5fe744b9623a0cc7f0ef6464c5530da, f6d72abf9ca654a20bbaf23ea1c10a55, fd9099005f133f95a5b699ab30a2f79b, 5ed95cde6c29432a4f7dc48602f82734, 16a8aaaf2e3125668e6bfb1705a065f9, 64d729d0290e2c8ceaa6e38fa68e80e9, 443a00feeb3beaea02b2fbcd4302a3c9, e13c3a38ca58fb0fa9da753e857dd3d5, e4813c34fe2327de1a94c51e630213d1
SHA256	e27467f7fdfa721e917384542ce10cc6108dfd78df14e23872cf8df916e0b8c6, 7d514021c472e6e17f587ed30555d3f120653e6c7f8dc25d2331514b92ffd7bc, 41d9b6d8cf0fff85bf35327d4b94db629cd9f754c487672911b7f701fe8c5539, 90bf1f20f962d04f8ae3f936d0f9046da28a75fa2fb37f267ff0453f272c60a0, ca56720610400d6da773ffa4cce5b2447d4a665087604c9c6e1c9e71c048ccfc, 9eca7ab62e3ad40b79116ad713462e3ae4d9610345952e5dd279f0b481870d4f, 3fa06c290c477c133ca58512c7852fc998632721f2dc3a0984f18fbe86451e18, 7ee4326c5d0e6a30c1a9bdec045d670758fa1b36477992d61b03cb270113b196, ccb6ca4cb385db50dad2e3b7c68a90ddee62398edb0fd41afdb793287cfbe8e6, 6a2d984ef3fa0de9b9feb5f558381201e6dff42ef5efe4867fb24e47c6a2aade

References

https://www.genians.co.kr/en/blog/threat_intelligence/rokrat_shellcode_steganographic

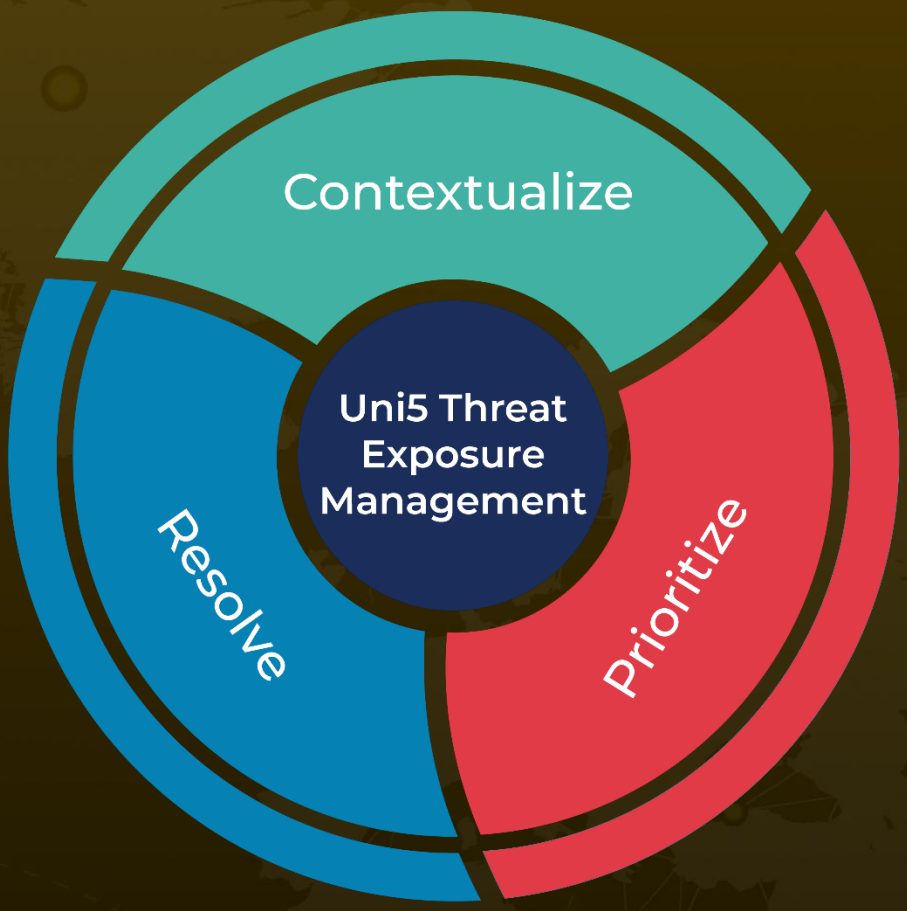
https://hivepro.com/threat-advisory/scarcruft-unleashes-tailored-attacks-on-cybersecurity-frontlines/

https://hivepro.com/threat-advisory/apt37-operation-toybox-story-exposes-cybersecurity-blind-spots/

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

August 5, 2025 • 6:30 AM

More at www.hivepro.com