Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

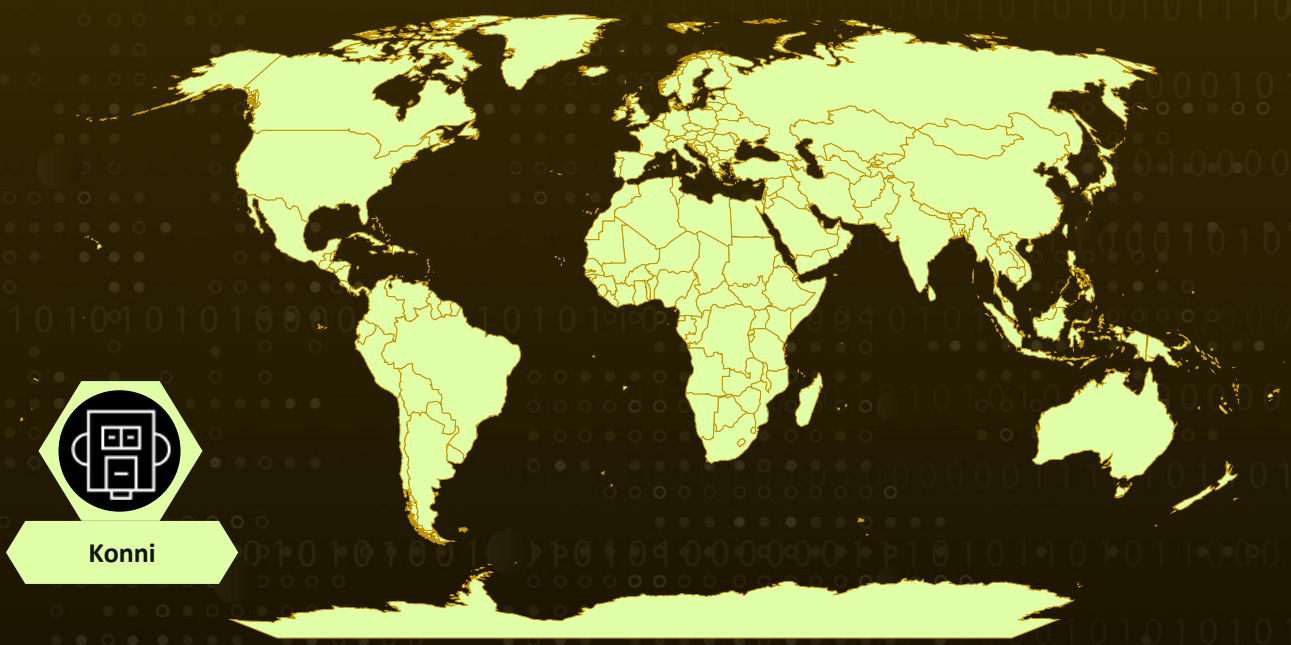
Konni APT's Covert RAT Deployment

Date of Publication	Admiralty Code	TA Number
March 18, 2026	A1	TA2026075

Summary

First Seen: February 2026
Targeted Region: Worldwide
Targeted Platform: Windows
Targeted Product: KakaoTalk PC Application
Targeted Industry: Human Rights Organizations
Threat Actor: Konni
Malware: EndRAT, RftRAT, RemcosRAT
Attack: The Konni APT group conducted a multi-stage attack operation beginning with spear-phishing emails disguised as North Korean human rights lecturer appointment notices. Upon initial compromise via malicious LNK files, the threat actor deployed EndRAT for persistent remote access, stole sensitive documents over an extended dwell period, and subsequently abused the victim's KakaoTalk PC messenger session to selectively redistribute malicious payloads to contacts, turning compromised victims into intermediaries for further attacks.

Attack Regions



Attack Details

#1

In a carefully orchestrated intrusion, the Konni APT group has resurfaced with a multi-stage campaign that blends social engineering with stealthy malware delivery, turning trust into its most effective weapon. The attack begins with a highly targeted spear-phishing email, posing as an official notice appointing the recipient as a North Korean human rights lecturer. By aligning the lure with the victim's professional interests, the attackers increase the likelihood of engagement, ultimately convincing the target to open a ZIP archive containing a seemingly legitimate file.

#2

Once extracted, the archive reveals a malicious Windows shortcut (LNK) file cleverly disguised with a document icon. When executed, it silently triggers a PowerShell-based dropper via cmd.exe using the SysWOW64 path, likely a deliberate choice to bypass certain defenses or ensure compatibility. The script employs a subtle technique to identify its payload based on file size rather than filename, then decodes embedded data using an XOR routine. Meanwhile, a decoy PDF is dropped and opened to maintain the illusion of legitimacy, while the original LNK file is removed to reduce forensic traces.

#3

The attack then escalates as the malware shifts execution to a public directory and retrieves additional payloads from its command-and-control infrastructure. These include a legitimate AutoIt interpreter and a malicious AutoIt script disguised as a PDF, cleverly wrapped within layers of benign-looking data to evade detection. Persistence is firmly established through a scheduled task configured to execute every minute for nearly a year, ensuring a continuous foothold even after reboots or user inactivity.

#4

At the core of the operation is EndRAT, an AutoIt-based remote access trojan equipped with a wide range of capabilities, from file manipulation and remote shell access to controlled data exfiltration. Its communication avoids standard HTTP patterns, instead relying on custom socket protocols over common ports like 80 and 443, allowing it to blend into normal network traffic. Additional safeguards, such as mutex-based execution control, help maintain stability and prevent redundant infections.

#5

Over time, the attackers quietly expand their reach within the compromised environment, harvesting sensitive data and leveraging the victim's trusted applications, such as KakaoTalk, to propagate further attacks. By sending malicious archives to selected contacts under the guise of North Korea-themed content, the campaign effectively turns the victim into an unwitting distributor. Further analysis reveals a broader toolkit in play, including multiple RAT variants like EndRAT, RftRAT, and RemcosRAT, each employing distinct obfuscation and persistence techniques. Together, these elements highlight a well-resourced operation focused on long-term access and sustained intelligence collection.

Recommendations

Block Known C2 Infrastructure: Immediately block all identified C2 domains and IP addresses at the firewall, proxy, and DNS levels to disrupt active command-and-control communications.

Quarantine Malicious LNK and Archive Attachments: Configure email security gateways to inspect, quarantine, or block ZIP archives containing LNK shortcut files, particularly those with document-like icons. Prioritize inspection of emails using socially and politically sensitive themes such as North Korea, human rights, national security, and public institution notices.

Hunt for AutoIt-Based Execution Chains: Conduct threat hunting across endpoints for indicators of AutoIt-based malware execution, including the presence of AutoIt3.exe in non-standard paths, .au3 or disguised .pdf files executed as AutoIt scripts, and scheduled tasks with short repetition intervals.

Audit Scheduled Tasks and Startup Entries: Review all endpoints for suspicious scheduled task registrations (particularly tasks named APDNHFU or those executing AutoIt scripts) and unexpected LNK files in the Windows Startup folder (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup).

Implement Messenger Security Controls: Establish security guidelines governing file transfers via KakaoTalk and similar desktop messaging platforms. Monitor for abnormal file-sharing behaviors such as bulk transfers, repeated ZIP file transmissions, or file-sharing patterns inconsistent with a user's normal messaging activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.010: AutoHotKey & AutoIt
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1036: Masquerading	
	T1027: Obfuscated Files or Information	T1027.002: Software Packing
	T1070: Indicator Removal	T1070.004: File Deletion
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	148405ff05bf15a6a053e4e7c1795d40, 2e1b0ac49313873a0e0b982c591a5264, 7dc50e8af0070e544bff5299405cd3b9, 61f65bd593ea0e52ac0dfdc6bc9cd73a, 461ade40b800ae80a40985594e1ac236, 01022facb38cf60b052e65a682f4a127, 3288c284561055044c489567fd630ac2
Domain	drfeysal[.]com
IPv4	185[.]21[.]14[.]249, 157[.]180[.]88[.]26, 96[.]62[.]214[.]5, 178[.]16[.]54[.]208

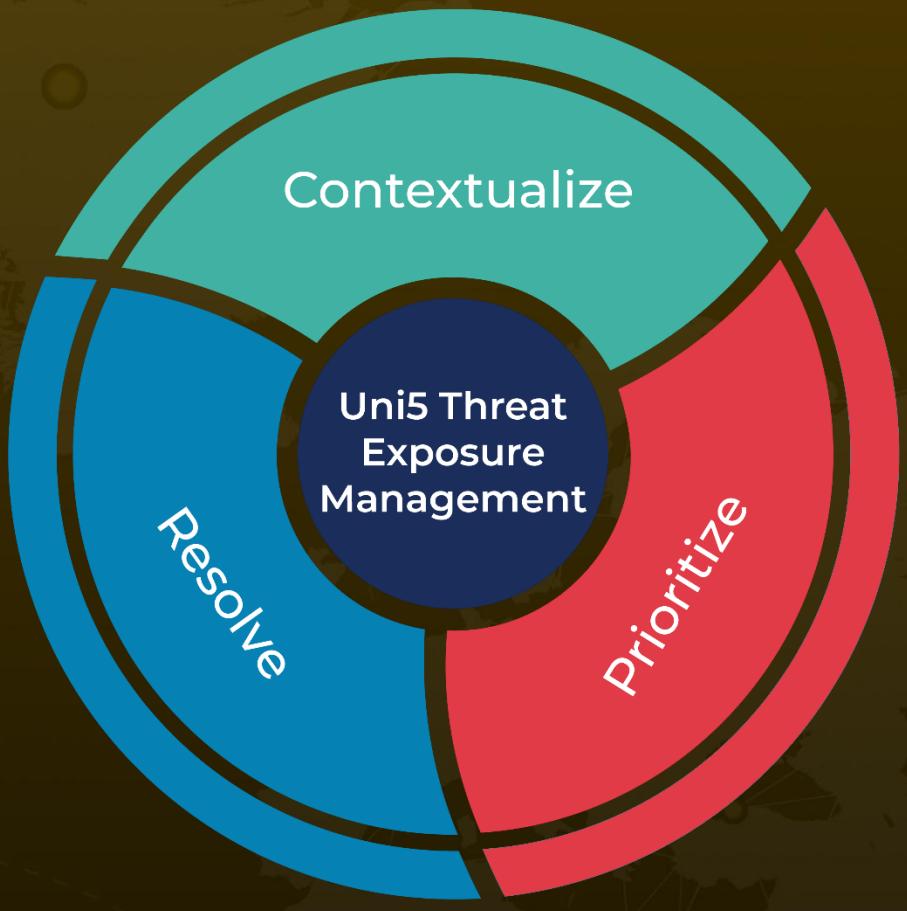
References

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

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

March 18, 2026 • 07:15 AM

More at www.hivepro.com