Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

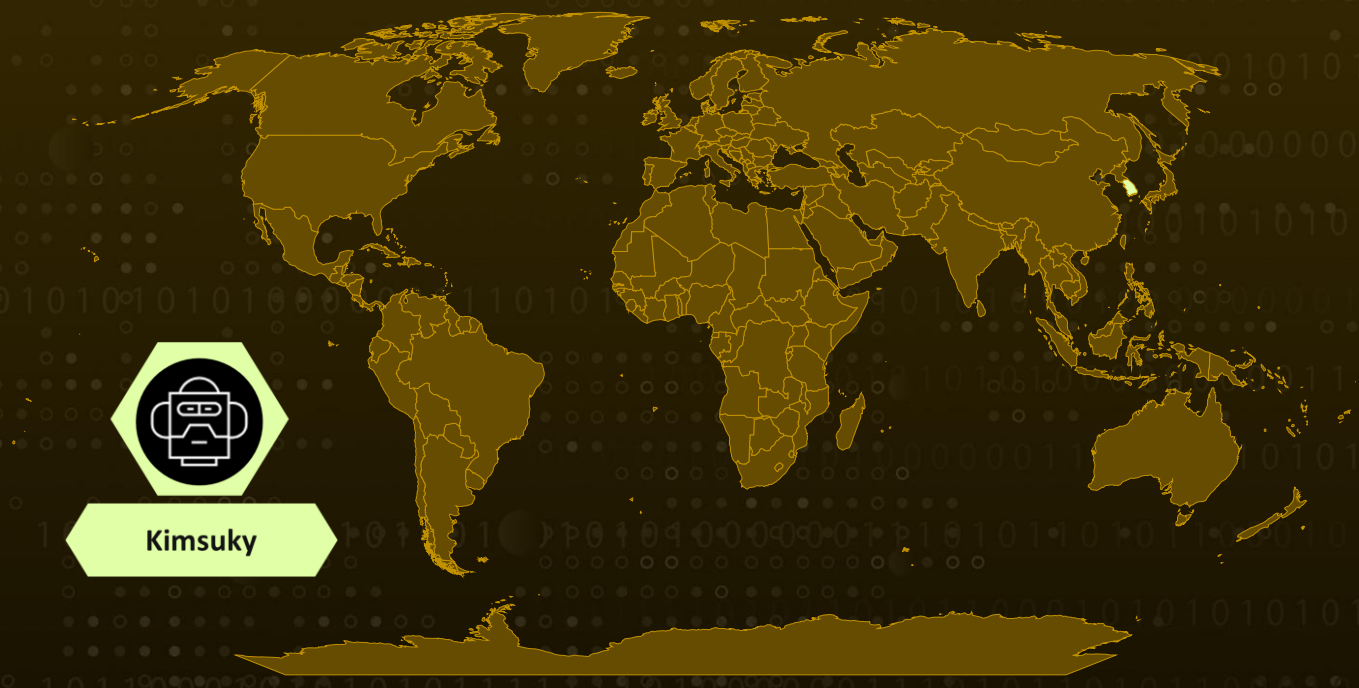
DEEP#DRIVE: Kimsuky Exploits Cloud Platforms for Stealthy Cyber Espionage

Date of Publication	Admiralty Code	TA Number
February 14, 2025	A1	TA2025041

Summary

Attack Discovered: 2024
Targeted Country: South Korea
Campaign: DEEP#DRIVE
Targeted Industries: Business, Cryptocurrency and Government sectors
Actor: Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394, Sparkling Pisces, Springtail)
Attack: The DEEP#DRIVE cyber campaign, attributed to Kimsuky, a North Korean state-sponsored hacking group, is actively targeting South Korea's business, government, and cryptocurrency sectors. The operation relies heavily on PowerShell scripts for delivering malware, gathering intelligence, and executing follow-up attacks. A notable tactic in this campaign is the use of Dropbox, which serves both as a delivery channel for malicious payloads and as a storage point for exfiltrated system data.

Attack Regions



Attack Details

#1 The DEEP#DRIVE campaign is a sophisticated cyber-espionage operation linked to North Korean threat actors, the Kimsuky group. This attack begins with a phishing email containing a ZIP file, which includes a malicious shortcut (.lnk) disguised as a legitimate document. When clicked, the shortcut executes an embedded PowerShell script that extracts and opens a benign PDF file as a decoy while simultaneously connecting to a Dropbox account controlled by the attackers to retrieve additional malicious scripts.

#2 Once downloaded, these scripts leverage PowerShell to dynamically load and execute further encrypted payloads in memory, allowing them to evade detection. The malware conducts extensive system reconnaissance, gathering details about running processes, antivirus solutions, and directory contents. It also establishes persistence through scheduled tasks and registry modifications to ensure continued access.

#3 The campaign's primary objective is data collection and exfiltration. Collected data is transmitted back to the attackers through encrypted channels, often using trusted cloud services like Dropbox. This strategy enables the attackers to blend their malicious activities within normal network traffic, making detection more difficult.

#4 A key characteristic of DEEP#DRIVE is its reliance on widely used platforms for command-and-control (C2) communications. By leveraging service such as Dropbox, the attackers effectively mask their activities, bypassing traditional security measures. In March 2024, Kimsuky launched **DEEP#GOSU**, a multi-stage attack using PowerShell and VBScript to deploy a remote access trojan (RAT) and gain full control over infected systems. To evade detection, they leveraged legitimate services like Dropbox for command-and-control (C2) communications.

#5 Recently, Kimsuky has been using phishing lures and malicious LNK files to deliver **PebbleDash** malware and a custom RDP Wrapper for remote access. The group remains highly active, particularly targeting the South Korea region with phishing campaigns. This highlights Kimsuky's evolving cyber tactics, focusing on stealth, persistence, and the abuse of legitimate services to evade detection.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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.

Enhanced Email Security: Enhance email security by Implementing advanced spam filters, anti-phishing solutions, and email authentication protocols. Educate employees about identifying and reporting suspicious emails to prevent successful phishing attempts. Deploy advanced email filtering solutions to detect and block phishing emails containing malicious links or attachments.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1132 Data Encoding
T1027 Obfuscated Files or Information	T1027.010 Command Obfuscation	T1036 Masquerading	T1036.007 Double File Extension
T1140 Deobfuscate/Decode Files or Information	T1620 Reflective Code Loading	T1059 Command and Scripting Interpreter	T1059.001 PowerShell

T1059.003 Windows Command Shell	**T1204** User Execution	**T1204.002** Malicious File	**T1102** Web Service
T1567 Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task
T1592 Gather Victim Host Information	**T1590** Gather Victim Network Information	**T1590.005** IP Addresses	**T1112** Modify Registry

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/slx06ol4jmjqn16icggin/[.]pptx, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/sumch8o12a4ko7wqqtrgo/kxsxhx-f[.]txt, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/gs58u6qvvxorzttv09yvt/kxsxhx-x[.]txt, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/lc7j7be3vtd2f3hadv0bz/V02_-D[.]pdf[.]pdf, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/vx23391zdxqu3qirc5z7g/241002-2024-GA-10-v2[.]pdf, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/nanwt6elsuxziz05hnlt4/cjfansgmlans1-x[.]txt, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/3br2y8fin0jqgrunrq3mf/cjfansgmlans1-f[.]txt, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/ffrwxyw5reunc12416rmp/V3[.]rtf, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/4qmp7p8fkmfwfsltt6imb/0607online[.]pdf, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/quo63qm8d3iqlhmpyib7p/20240608[.]bmp, hxxps[:]//dl[.]dropboxusercontent[.]com/scl/fi/p8f846myv0cbs5975uszw/loader[.]txt
SHA256	079907B7FEAB3673A1767DBFBC0626E656F5D3B03B6CFF471CC7CF8A1973AB34, 8D6DC026812420C5EF4B4FE72FB7067DA14196FEA45B6E99A594126246AC41FC, 2849D92E7E188F4B76559B7018D81F6C463388A1B05B2674594F70CF4858C6B3,

TYPE	VALUE
SHA256	ACBC775087DA23725C3D783311D5F5083C93658DE392C17994A9151447AC2B63, 21CEFE1D3FE0C69C32BEBAFCA15D1AD3B17FAE37B11E6B6EFFE155327387A752, 71D56C61B765EEE74DCA65910AB9E0E2B35B21BCF6C97241CA7188A75F082F6F, 44FF60D352169F280801CF2075295AAB0A6151FF8F77B66D16C82776EFCE7FEA, 1D5D65F2EB065BAC629C82A3399FBDC28EBE33EB288C1CD556CCA6B4E6230B52, 074ADA5CC1947EBE5B9ACB7F2DBF0FA599B043661F4FE640D403BDCC8427AFCA, CE04F9074A4CC8FA74FABFF5A1FE21439FD8485220321C90BB06F5DBED50170C, DB3A5A3A8855A48D2AA3CA2FAEF14E35CB8F3416D10DF9C94576D9B5966DEF3D, B960C9DE6714C9951EC21CA685998BA49EB29EF57868E780521B212AD6356E9C, 79496BAA4BF17A73006A359E146F02F7A92DD0794A07844064C7268724B98560, B2B8D0AE6F521F7405305A7AFBE6D230C0DD22A18C4A852A6B69D9E54513E248, 6154932EF81ED274C492F55775713B25A54676E283932B9048718C1B4A837F65, 47DFA0061FDB021F3CEFE62AC8198733BE5ADCB756F6042CA62EFDC4F2502E97, FE84A4A119917F15418659ED30699D873B6445AA053D9303287B085E35BF1002, 8E51819E39E4FC73D71B31E49B6775E47EE3B11AF1FD9EB48A1E7D49DAD62BC0, DB6315274DC31BEA8F42C79EA8928A4BE2A5DD996C3E7A702F6A2BAC5C463FEE, 8CDD557CFF23CA7DDC3CF229F3B6D755878BF7AA864DD4E9D58E590B436987E5, D28E8041A0445271723842FA1D400B5B2AA93DA4DFCD68B1C763774C870DC3B1, 5171917E58A4E795A5E911F82560FA9B5C8F3D62EFD4054BF58A2579E78B76D7, 38B1CFB982C85AE89DA19BE83D502263C11DA1C1A5997E0F15DE2E5580D2161A

References

https://www.securonix.com/blog/analyzing-deepdrive-north-korean-threat-actors-observed-exploiting-trusted-platforms-for-targeted-attacks/

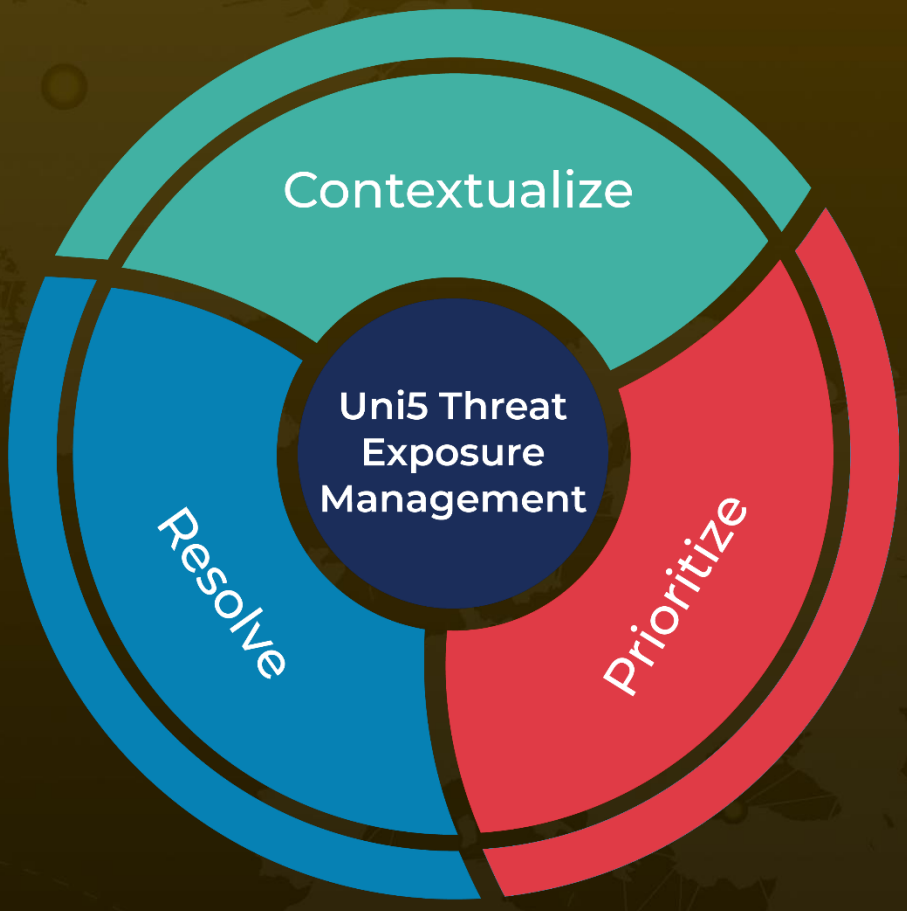
https://www.hivepro.com/threat-advisory/the-evolution-of-deepgosu-attack-campaign-by-kimsuky-group/

https://hivepro.com/threat-advisory/kimsuky-expands-rdp-wrapper-proxy-malware-in-spear-phishing-attacks/

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

February 14, 2025 • 6:50 AM

More at www.hivepro.com