Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

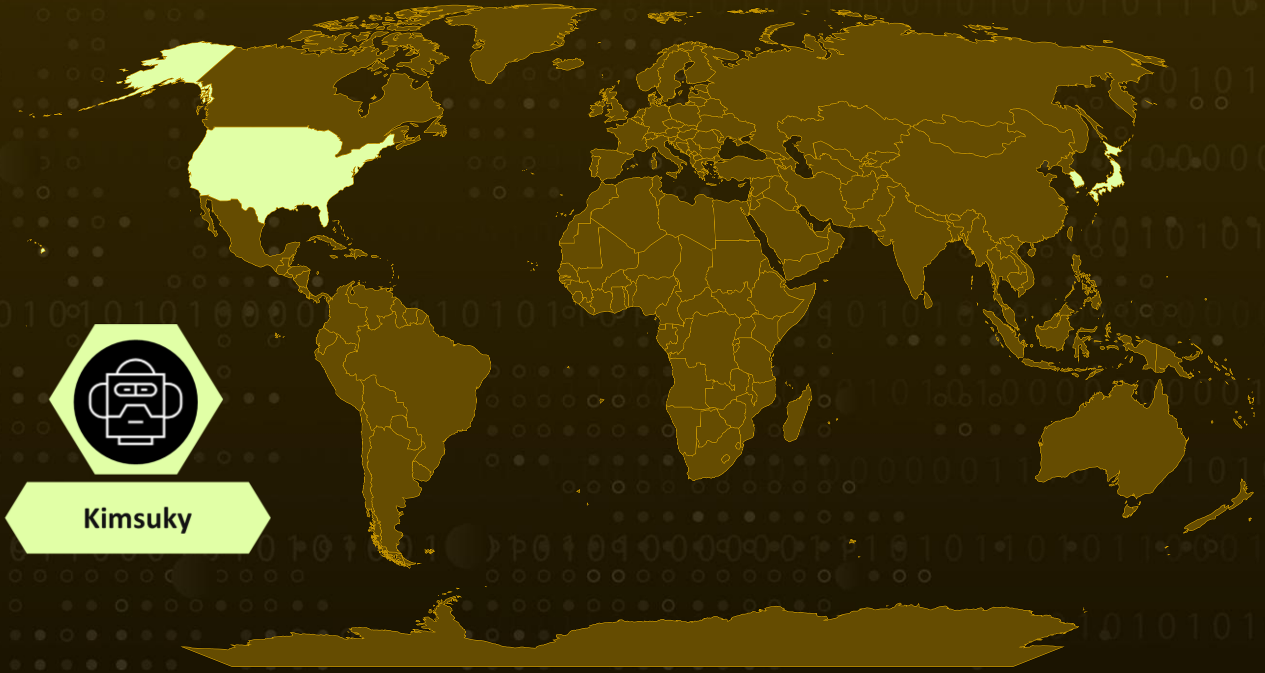
Kimsuky's Evolving Phishing Playbook: URL Tactics and Global Deception

Date of Publication	Admiralty Code	TA Number
December 5, 2024	A1	TA2024451

Summary

Attack Discovered: October 2023
Targeted Countries: Japan, South Korea, US
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 North Korea-aligned threat actor Kimsuky has been implicated in a wave of phishing attacks targeting credential theft. These campaigns involve email messages originating from Russian sender addresses, employing sophisticated tactics to evade detection. While email phishing remains a widespread global threat, URL phishing, which does not involve malware attachments in inbox emails, exclusively a malware-less attack often flies under the radar. Unlike traditional phishing attempts that rely on malware-laden links, Kimsuky frequently leverages URL phishing tactics, particularly in Korea, demonstrating a strategic focus on this less-detected attack vector.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

The North Korea-aligned **Kimsuky** group has orchestrated sophisticated phishing campaigns using URL-based tactics to compromise victims. These operations focus on credential theft through carefully crafted emails containing deceptive links, bypassing traditional malware deployment. By impersonating trusted organizations and leveraging international email services, Kimsuky effectively evades conventional detection mechanisms, making their campaigns difficult to identify and disrupt.

#2

In October 2023, phishing attacks targeted users in Korea, disguised as official notifications from the electronic civil document service 'National Secretary'. The attackers used domains provided by Japanese services and linked them to phishing websites registered through Korean platforms.

#3

Between April and October 2024, Kimsuky refined its phishing tactics, launching attacks themed around Naver MYBOX notifications. Initially relying on Japanese and Korean email domains, they later shifted to fabricated Russian domains to obscure their tracks further. These domains, generated using tools like Star 3.0, enabled the manipulation of email origins. Meanwhile, command-and-control servers transitioned from UK-based IP addresses to Russian domains, adding another layer of complexity to their infrastructure.

#4

Kimsuky adopted Russian email services to target Korean users, impersonating financial institutions or portal companies to deceive recipients. The attackers obscured sender details through random domain selection during email registration, further complicating attribution.

#5

One notable tactic involved emails falsely claiming malicious activity in the MYBOX cloud service, often containing code snippets linked to legitimate sites of private U.S. university.

#6

Kimsuky's campaigns present a dual threat, initial credential theft and potential secondary attacks on compromised networks. Once access is gained, stolen accounts can be exploited to infiltrate broader systems, target associates, or launch further phishing operations. To counter these evolving threats, organizations must prioritize a proactive defense strategy which can significantly reduce vulnerability to Kimsuky's persistent campaigns.

Recommendations

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.

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

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0005 Defense Evasion	TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment
T1566.002 Spearphishing Link	T1568 Dynamic Resolution	T1588 Obtain Capabilities	T1588.002 Tool
T1589 Gather Victim Identity Information	T1589.001 Credentials	T1071 Application Layer Protocol	T1204 User Execution
T1036 Masquerading			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	adb30d4dd9e1bbe82392b4c01f561e46, b591cbd3f585dbb1b55f243d5a5982bc, d8249f33e07479ce9c0e44be73d3deac, 0def51118a28987a929ba26c7413da29, 2ff911b042e5d94dd78f744109851326, 3cd67d99bcc8f3b959c255c9e8702e9f, 6ead104743be6575e767986a71cf4bd9, 7ca1a603a7440f1031c666afbe44afc8, 658a8856d48aabc0ecfeb685d836621b, a6588c10d9c4c2b3837cd7ce6c43f72e, a75196b7629e3af03056c75af37f37cf, aa41e4883a9c5c91cdab225a0e82d86a, ab75a54c3d6ed01ba9478d9fecd443af
Domains	cookiemanager[.]ne[.]kr, nidiogln[.]ne[.]kr, naverbox[.]pe[.]kr, covd[.]2kool4u[.]net, ned[.]kesug[.]com, wud[.]wuaze[.]com, owna[.]loveslife[.]biz, online[.]korea[.]article-com[.]eu, evangelia[.]edu, National Secretary[.]Main[.]Korea, National Pension Service[.] Server[.] Korea, National Secretary[.] Community[.] Korea, National Health Insurance Service[.] Confirmation[.] Server[.] Korea, Payment Due Date-Notice-Notice[.] Online[.] Korea, Financial payment-guidance-document-confirmation[.]Web[.]Korea, National Tax Service-Payment deadline-notification-guidance-guidance-confirmation[.]Online[.]Korea, National Tax Service-Payment deadline-variation notice[.]re[.]kr, Naver-blog-post -Restriction-Guide[.]kro[.]kr
IPv4	185[.]27[.]134[.]201, 185[.]105[.]33[.]106, 185[.]27[.]134[.]140, 185[.]27[.]134[.]93, 185[.]27[.]134[.]120, 185[.]27[.]134[.]144

References

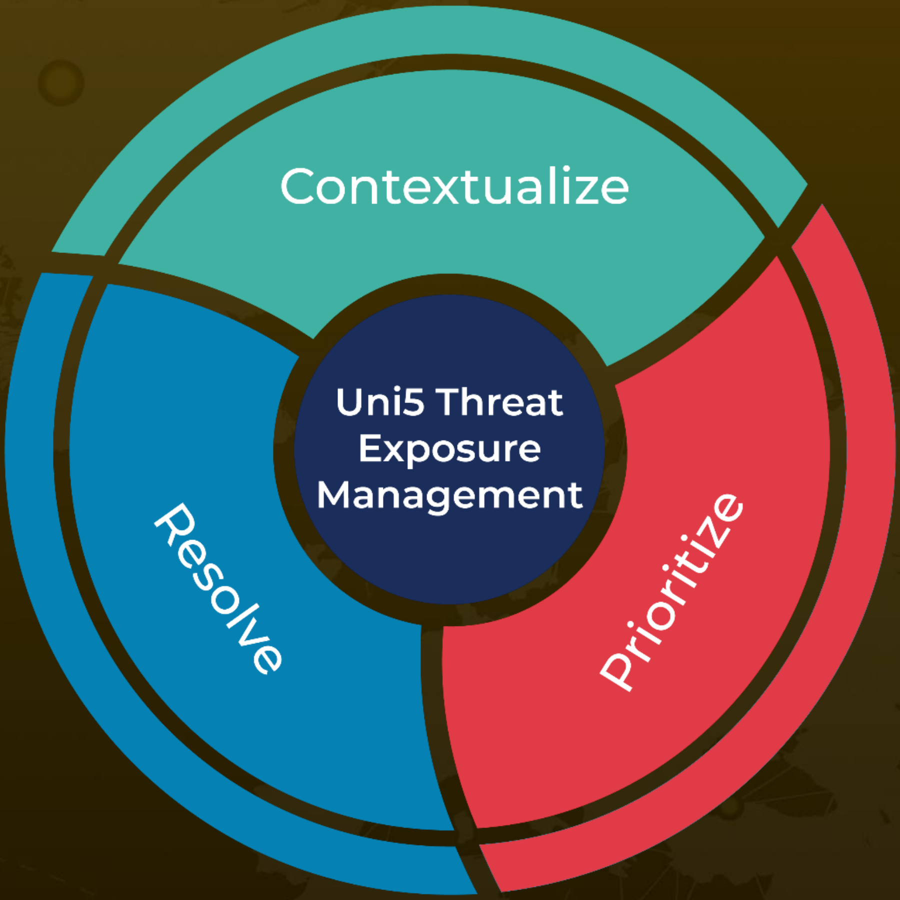
https://www.genians.co.kr/blog/threat_intelligence/kimsuky-cases

https://www.hivepro.com/kimsuky-unveils-new-addition-to-its-malware-arsenal/

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

December 5, 2024 • 5:00 AM

More at www.hivepro.com