Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

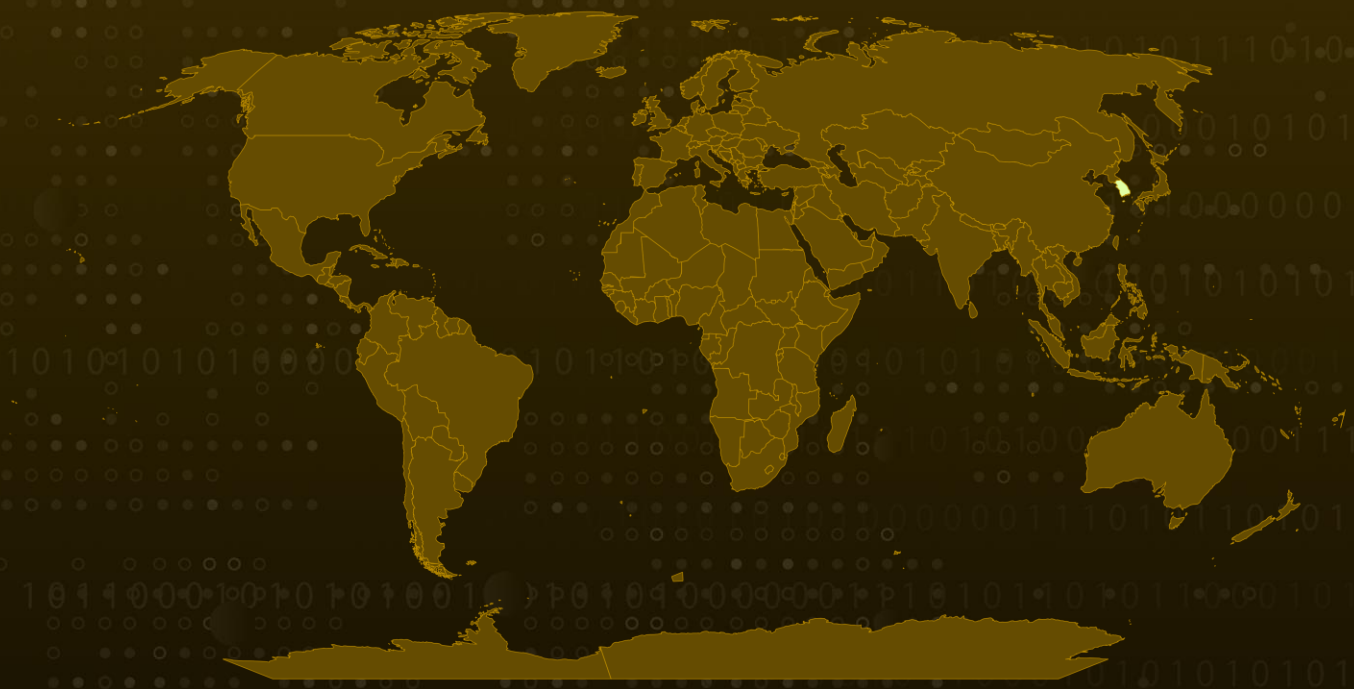
STARK#MULE Targets South Korea with US Military-themed Baits

Date of Publication	Admiralty Code	TA Number
August 3, 2023	A1	TA2023319

Summary

Campaign: STARK#MULE
Targeted Industry: Government, E-commerce
Attack Region: South Korea
Attack: The STARK#MULE cyber attack campaign is ongoing, with a focus on targeting Korean-speaking individuals. It employs U.S. Military-themed document baits to deceive its targets, leading them into unwittingly running malware, thus compromising their systems.

Attack Regions



Attack Details

#1 An ongoing and sophisticated STARK#MULE attack campaign strategically entices its victims through the use of US military-related documents, exploiting legitimate compromised Korean e-commerce websites as staging grounds for their malicious activities. The attack commences with a social engineering phishing email ingeniously designed to contain a zip file attachment that seemingly offers valuable information about US Army and military recruitment resources.

#2 These cunningly crafted attacks bear resemblance to previous offenses attributed to typical North Korean groups, such as APT37, which have historically focused on South Korea, particularly its government officials. Within the deceptive zip file lies a crafty shortcut file masquerading as a harmless PDF document.

#3 Once launched, the shortcut displays a decoy PDF to deceive the target, all while covertly executing a rogue "Thumbs.db" file concealed within the archive. This clandestine file serves multiple purposes, including the downloading of further stagers and the strategic utilization of schtasks.exe to establish persistence.

#4 Notably, this new campaign demonstrates a unique trait by employing compromised Korean e-commerce websites for both staging payloads and operating the command-and-control (C2) infrastructure, a cunning move to evade detection by security solutions on targeted systems. The culmination of this attack chain involves embedding intriguing and resilient malware into the victim's machine, setting it to run on scheduled tasks, and immediately initiating communication over HTTP channels.

Recommendations

- Enhance email security measures and educate users on recognizing social engineering tactics to mitigate the risk of falling prey to phishing attacks leveraging deceptive zip file attachments.
- Revisit the security whitelist for Korean e-commerce platforms and ensure continuous monitoring for any phishing or C2 attempts.
- Implement advanced threat detection mechanisms that can identify and block suspicious file executions, particularly those attempting to leverage "Thumbs.db" files for persistent malware deployment.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0010 Exfiltration	TA0011 Command and Control	T1566 Phishing
T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1053 Scheduled Task/Job	T1053.005 Scheduled Task	T1573 Encrypted Channel
T1573.001 Symmetric Cryptography	T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1584 Compromise Infrastructure
T1584.004 Server	T1567 Exfiltration Over Web Service		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e4a8610461d3b3c534346b9c874edff6d37ca085d578365ff75b25f682ec5fd0, 6149d861f38db6d6f5110b234edb1ba31800f7eb621ad27b6cbf99f05ddeae18, 019e4327b8292dad32c92209a1e0fa03636381b1163ac57941cd8cc711a40097, 89062a28f33021539ab3d197c124040177e5ae94a05e1ac7a4f1c852d6b498cf, 7893c8b41a2e4281e73a1761061ac9eee52920b6840e43697aabf606f701d11a,

TYPE	VALUE
SHA256	c90ebf988f96c9a51d6ad0b23ad7260c6b7f8d3b7c905acc20e18a7227e46237, 6f11c52f01e5696b1ac0faf6c19b0b439ba6f48f1f9851e34f0fa582b09dfa48
Domain	www.jkmusic.co[.]kr
URLs	hxxp://www.jkmusic.co[.]kr/shop/data/theme/e6a137162c56087, hxxp://www.jkmusic.co[.]kr/shop/data/theme/c9665058c3ef16b, hxxp://www.notebooksell[.]kr/mall/m_schema.php
User-agent	Mozilla/88.0
IPv4	182.162.94[.]42, 183.111.169[.]84
FileName	Multi National Recruitment System Templete[.]pdf[.]zip

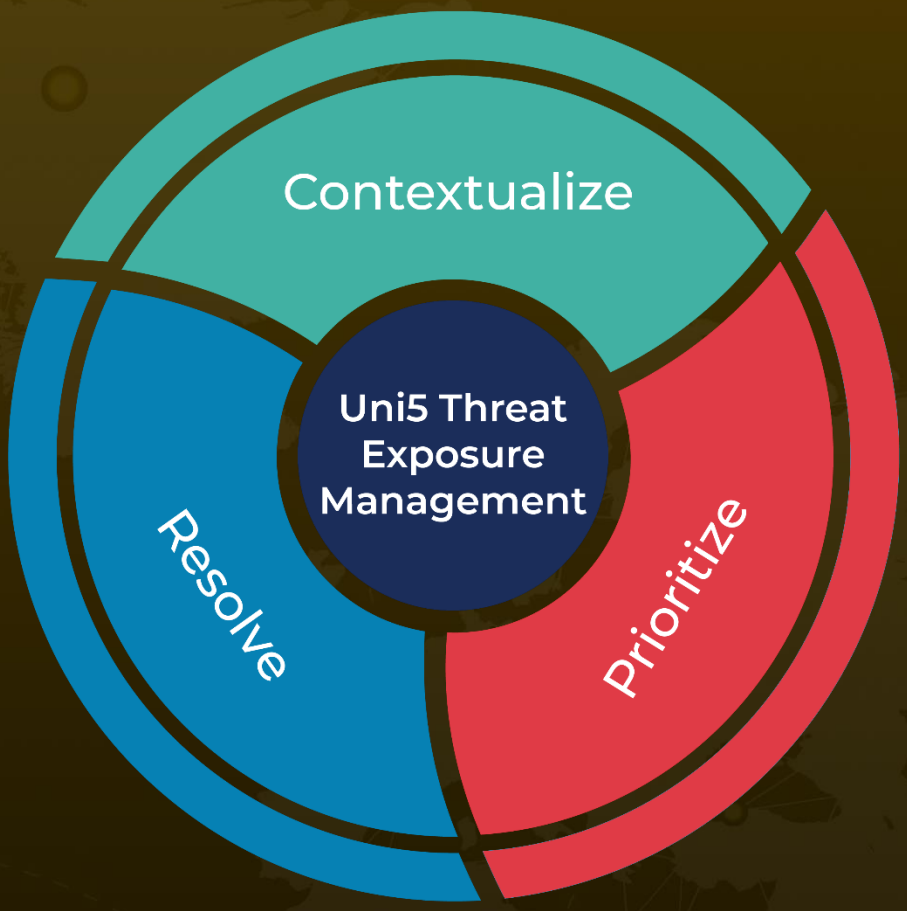
References

https://www.securonix.com/blog/detecting-ongoing-starkmule-attack-campaign-targeting-victims-using-us-military-document-lures/

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 3, 2023 . 6:30 AM

More at www.hivepro.com