Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

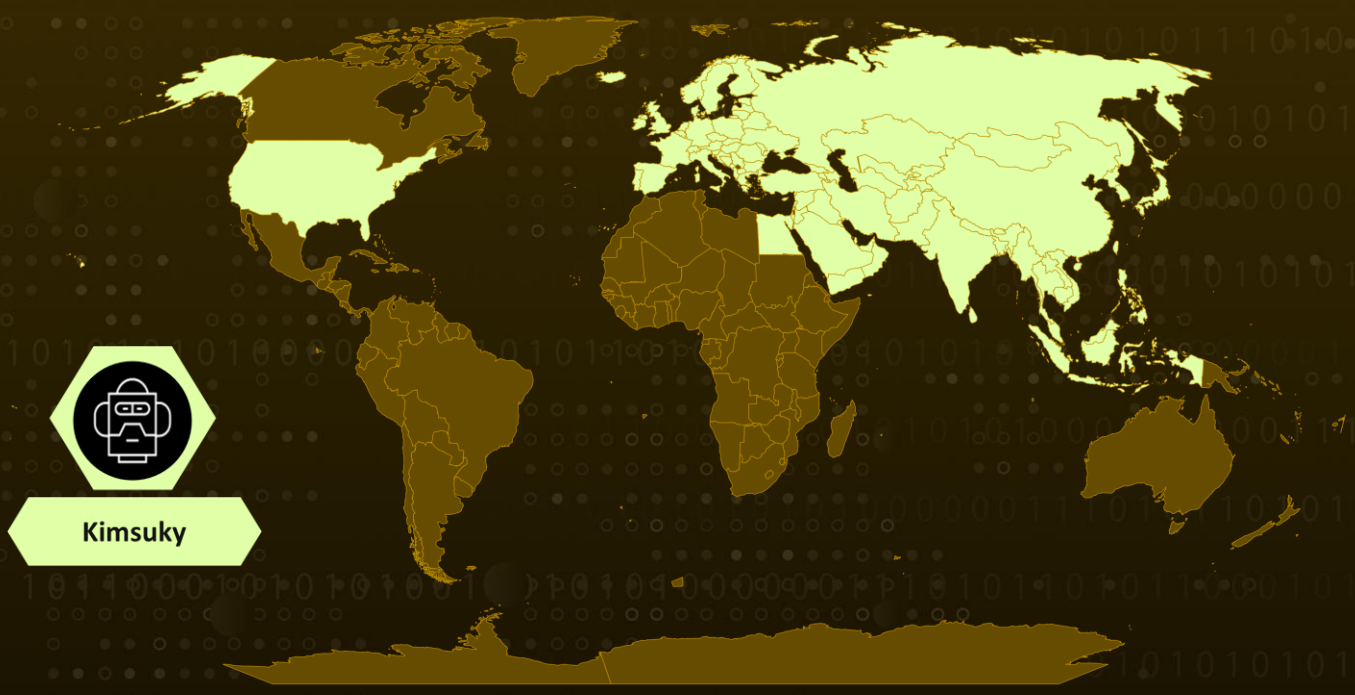
# Kimsuky APT Group Employs ReconShark

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| May 9, 2023 | A1 | TA2023218 |

# Summary

**Attack Began:** 2023
**Actor:** Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)
**Reconnaissance Tool:** ReconShark
**Affected Platform:** Microsoft OneDrive
**Attack Region:** United States, Europe, and Asia
**Targeted Sector:** Think tanks, Research universities, and government entities.
**Attack:** Kimsuky, a North Korean APT group, is using a new malware tool called ReconShark to conduct global cyberattacks.

## Attack Regions



# Attack Details

**#1**

Kimsuky, a state-sponsored Advanced Persistent Threat (APT) group from North Korea, is currently engaged in persistent attacks utilizing a newly developed malware component called ReconShark that functions as a reconnaissance tool. This malware is being distributed to specifically targeted individuals via spear-phishing emails, OneDrive links leading to document downloads, and malicious macros.

**#2**

Kimsuky's recent campaigns demonstrate a continued focus on various ongoing geopolitical topics, with the most recent ones centering on nuclear agendas between China and North Korea and the ongoing conflict between Russia and Ukraine. In these nefarious emails, Kimsuky employs tactics to entice the target to open a link to download a password-protected document.

**#3**

ReconShark uses Windows Management Instrumentation (WMI), much like previous BabyShark variants, to retrieve information about running processes and endpoint threat detection mechanisms. In addition to extracting data, ReconShark also deploys additional payloads in a multi-stage process that involves various types of scripts, including VBS, HTA, and Windows Batch, as well as macro-enabled Microsoft Office templates or Windows DLL files.

# Recommendations

Regular phishing simulations, education, and awareness training are vital. Also, verifying the authenticity of email attachments and untrusted links before opening them is crucial to prevent attacks.

Regularly back it up offline to protect critical data and install reliable anti-virus and internet security software on all connected devices. Enable automatic software updates whenever possible and practical. Additionally, consider implementing proactive security measures, such as blocking indicators of compromise (IoCs), to stay ahead of potential threats.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0007<br>Discovery | TA0011<br>Command and Control | T1053<br>Scheduled Task/Job |
| T1059<br>Command and Scripting Interpreter | T1090<br>Proxy | T1566<br>Phishing | T1566.002<br>Spearphishing Link |
| T1547<br>Boot or Logon Autostart Execution | T1547.001<br>Registry Run Keys / Startup Folder | T1132<br>Data Encoding | T1012<br>Query Registry |
| T1047<br>Windows Management Instrumentation | T1070<br>Indicator Removal | T1070.004<br>File Deletion | T1059.005<br>Visual Basic |
| T1204<br>User Execution | T1204.002<br>Malicious File | T1104<br>Multi-Stage Channels | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domain | yonsei[.]lol |
| URLs | https[:]//rfa[.]ink/bio/r.php https[:]//mitmail.tech/gorgon/r.php<br>https[:]//rfa[.]ink/bio/t1.hta https[:]//mitmail[.]tech/gorgon/t1.hta<br>https[:]//rfa[.]ink/bio/ca.php?na=reg.gif<br>https[:]//mitmail.tech/gorgon/ca.php?na=reg.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=secur32.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=secur32.gif<br>https[:]//newshare[.]online/lee/ca.php?na=secur32.gif |

| TYPE | VALUE |
| --- | --- |
| URLs | https[:]//rfa[.]ink/bio/ca.php?na=dot_eset.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_eset.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=video.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=video.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=start2.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=start2.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=start4.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=start4.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=start3.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=start3.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=videop.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=videop.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=start1.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=start1.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=vbs_esen.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs_esen.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=start0.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=start0.gif<br>https[:]//rfa[.]ink /bio/d.php?na=vbtmp<br>https[:]//rfa[.]ink/bio/ca.php?na=vbs.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs.gif<br>https[:]//rfa[.]ink/bio/d.php?na=battmp<br>https[:]//rfa[.]ink/bio/ca.php?na=dot_v3.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_v3.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=dot_esen.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_esen.gif<br>http[:]//rfa[.]ink/bio/ca.php?na=dot_avg.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_avg.gif<br>https[:]//rfa[.]ink/bio/ca.php?na=dot_kasp.gif<br>https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_kasp.gif |
| SAH1 | 86a025e282495584eabece67e4e2a43dca28e505<br>c8f54cb73c240a1904030eb36bb2baa7db6aeb01 |

## References

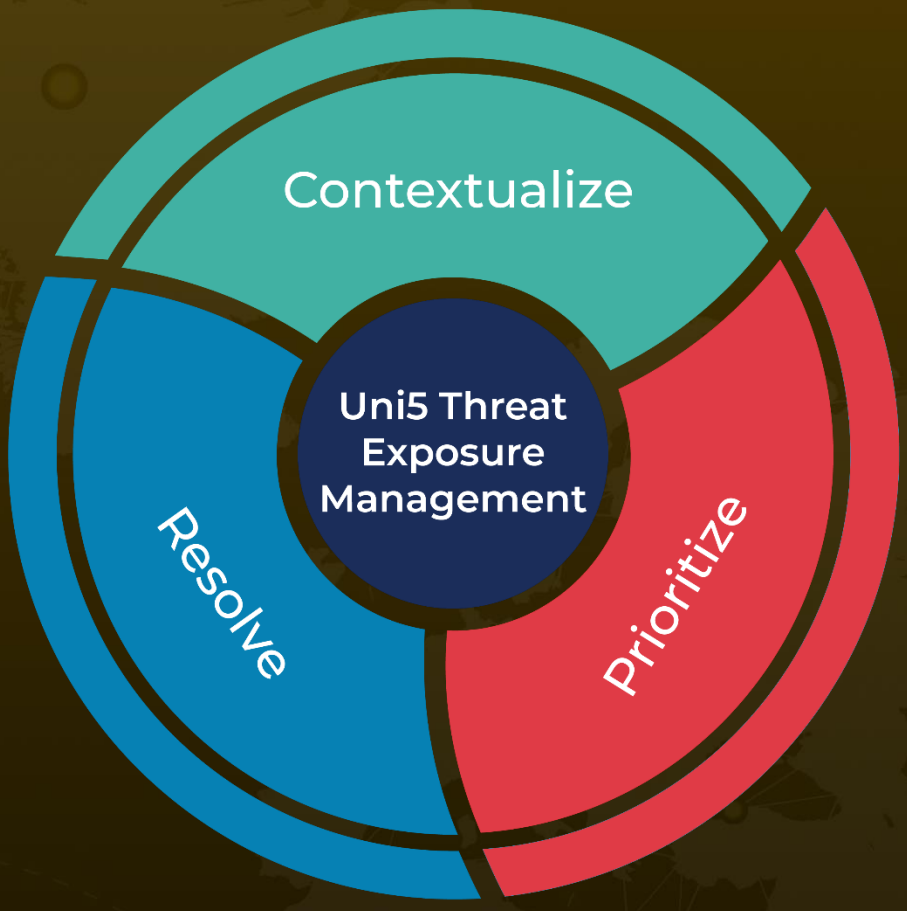

https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/

https://www.hivepro.com/kimsuky-targets-south-korean-entities-with-phishing-campaign/

# 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

**May 9, 2023 • 6:57 AM**



More at www.hivepro.com