Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

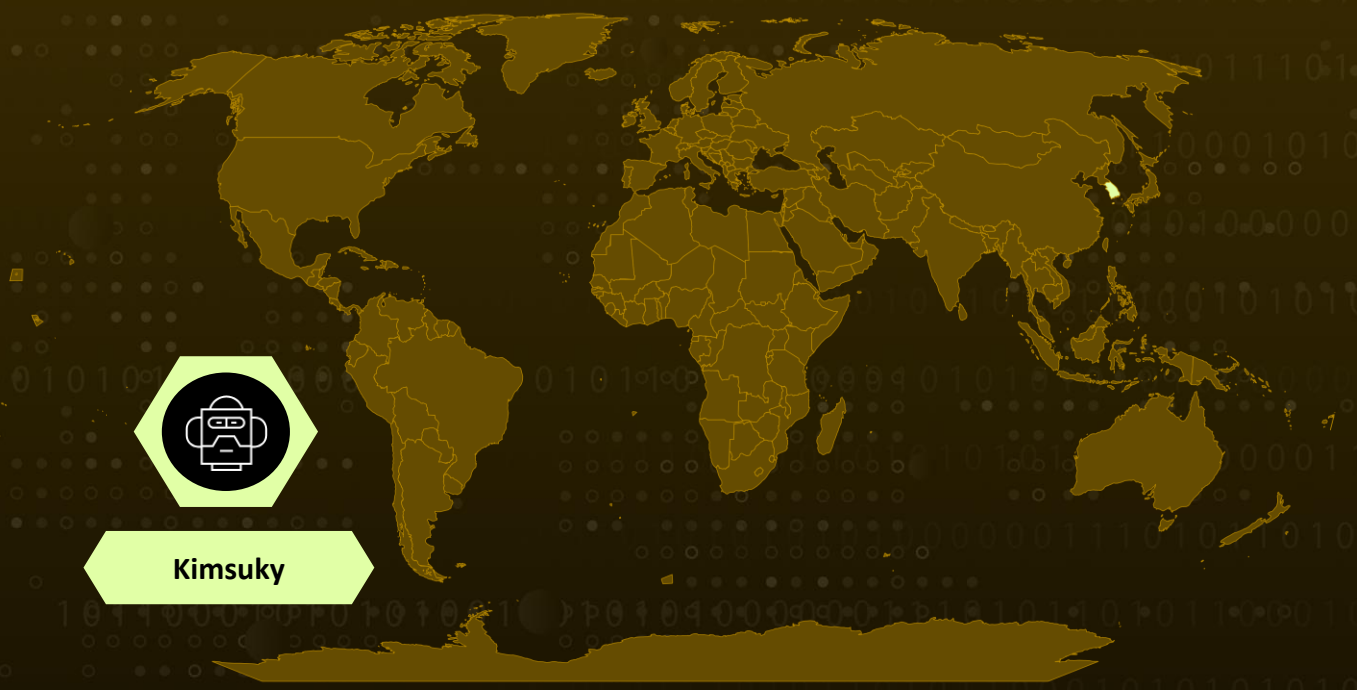
The Evolution of DEEP#GOSU Attack Campaign by Kimsuky Group

Date of Publication	Admiralty Code	TA Number
March 20, 2024	A1	TA2024108

Summary

First appeared: March 17, 2024
Attack Region: South Korea
Malware: TutClient, TutRAT, and xRAT
Campaign: DEEP#GOSU
Threat Actor: Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)
Affected Platform: Windows
Attack: A sophisticated multi-stage attack campaign linked to the North Korean Kimsuky group, dubbed DEEP#GOSU. Using PowerShell and VBScript, the attackers leverage remote access trojan (RAT) software for full control over infected hosts, while employing legitimate services like Dropbox for command and control communication to evade detection.

Attack Regions



Attack Details

#1 A complex multi-stage attack campaign linked to the North Korean Kimsuky group, dubbed DEEP#GOSU. This campaign employs new code and tactics alongside recycled methods. Initially targeting South Korean victims, the group now utilizes a script-based attack chain using PowerShell and VBScript stagers to infiltrate systems discreetly.

#2 The attackers leverage remote access trojan (RAT) software for full control over infected hosts, while maintaining persistence and monitoring capabilities through background scripts. Notably, all command and control (C2) communication is routed through legitimate services like Dropbox or Google Docs, allowing the malware to evade detection by blending into regular network traffic.

#3 The attack begins with the distribution of malicious email attachments containing disguised files. The first stage involves executing PowerShell code embedded within shortcut files, leading to the download and execution of subsequent payloads.

#4 Stage two involves invoking code from Dropbox, dynamically loading and executing .NET assembly code. Stage three introduces the use of a C# RAT called TutClient, which offers various capabilities such as keylogging, remote desktop access, and DDoS attacks. Stage four entails executing VBScript code fetched from Dropbox, contributing to persistence and stealth.

#5 In stage five, additional VBScript execution occurs, including Windows Management Instrumentation (WMI) activity and scheduled tasks for persistence. Stage six involves PowerShell execution for system enumeration, with data encrypted and uploaded to Dropbox.

#6 Stage seven ensures persistence and stealth through PowerShell scripts, maintaining communication with a command and control server. Stage eight focuses on keylogging and clipboard monitoring, capturing user activity on compromised systems. The campaign's sophistication lies in its multi-layered approach, utilizing PowerShell and VBScript alongside legitimate services to evade detection.

Recommendations

Exercise Caution with External Sources: Avoid downloading files or attachments from external sources, especially if they are unsolicited or come unexpectedly. Encourage employees to verify the legitimacy of emails and attachments before interacting with them.

Monitor Malware Staging Directories: Pay close attention to activity in common malware staging directories, particularly related to script execution in writable directories. In this campaign, threat actors utilized subdirectories in %APPDATA%, so monitoring this location specifically could be beneficial.

Enhance Endpoint Logging: Deploy robust endpoint logging capabilities, including additional process-level logging such as Sysmon and PowerShell logging. This expanded logging coverage can help detect malicious activities associated with multi-stage attacks like DEEP#GOSU.

Implement Network Traffic Analysis: Given that the DEEP#GOSU campaign utilizes encrypted communication through legitimate services like Dropbox and Google Docs, it's crucial to deploy network traffic analysis tools capable of detecting anomalous patterns within encrypted traffic.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0005 Defense Evasion	TA0002 Execution	TA0003 Persistence
TA0010 Exfiltration	TA0011 Command and Control	TA0009 Collection	T1132 Data Encoding
T1027 Obfuscated Files or Information	T1027.010 Command Obfuscation	T1070.004 File Deletion	T1140 Deobfuscate/Decode Files or Information
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1059 Command and Scripting Interpreter

T1567 Exfiltration Over Web Service	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1102 Web Service
T1132.001 Standard Encoding	T1219 Remote Access Software	T1573 Encrypted Channel	T1115 Clipboard Data
T1056.001 Keylogging	T1056 Input Capture	T1204 User Execution	T1070 Indicator Removal
T1059.001 PowerShell	T1059.005 Visual Basic	T1204.001 Malicious Link	T1567.002 Exfiltration to Cloud Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps://content[.]dropboxapi[.]com/2/files/download/step2/ps[.]bin, hxxps://content[.]dropboxapi[.]com/2/files/download/step2/r_enc[.]bin, hxxps://content[.]dropboxapi[.]com/2/files/download/step2/info_sc[.]txt, hxxps://content[.]dropboxapi[.]com/2/files/download/step2/info_ps[.]bin, hxxps://content[.]dropboxapi[.]com/2/files/download/step2/ad_ps[.]bin, hxxps://content[.]dropboxapi[.]com/2/files/download/step2/info_sc[.]txt,
Domain	gbionet[.]com
SHA256	F262588C48D2902992FFD275D2BE6362FE7F02E2F00A44AB8C75AC1A2827C6E9, 1617587CCDF5B0344089559ECF8FE7D39F6E07A6A64F74F2B44BFA2C8CB67983, 46A5D54C264152CE915792AF31C75824A558AF7D7340D78B34E146D8C6249E79, 1B75F70C226C9ADA8E79C3FDD987277B0199928800C51E5A1E55FF01246701DB, 69C917EA96DB28DBD5B67073CA0AAC234D25651A849171B45F20979EAFA05A1C,

TYPE	VALUE
SHA256	60666CACDD6806ED05771F32EAA719E3EFD2F4DB55F28A447D383C3EAC1DC72E, B72CAAB78D164637FEA0937D7A94FC470579EC6BB4FA87DADB6F0FA7826E217C, 89CAD9A57985CC0AB3B7403A943AD0AA7B167DC7A3C38557417FEDEA67A77B87

References

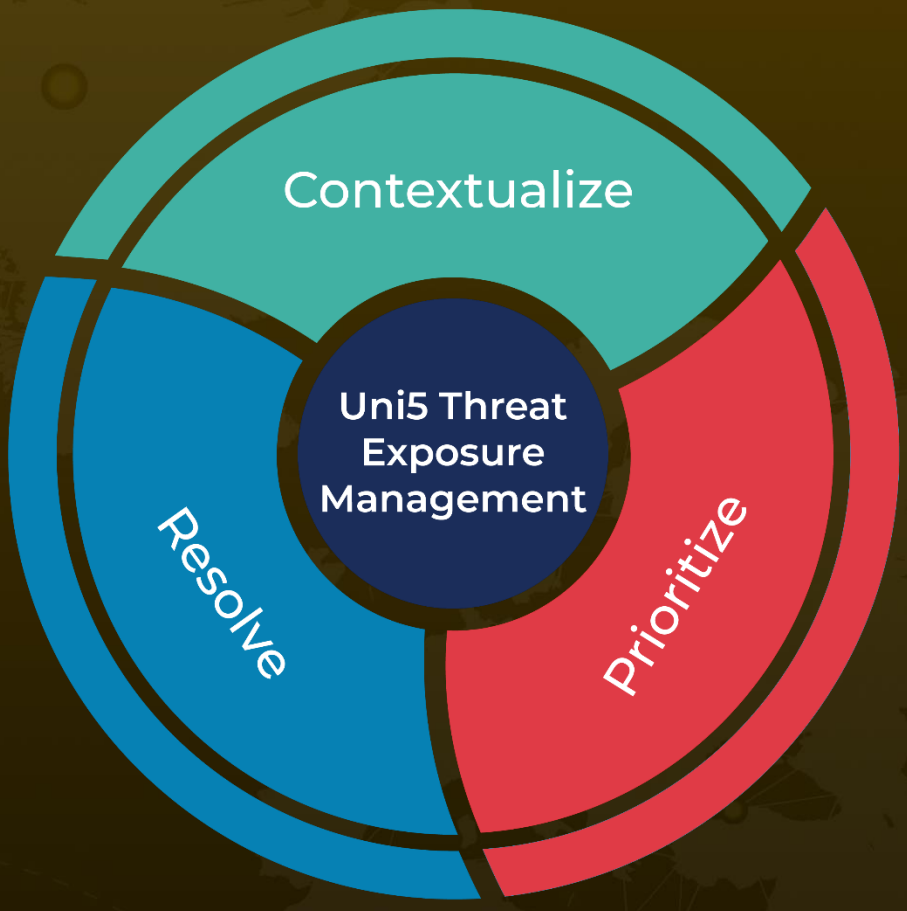
https://www.securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/

https://www.hivepro.com/threat-advisory/kimsuky-exploits-legitimate-certificate-to-disseminate-trollagent/

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 20, 2024 • 5:30 AM

More at www.hivepro.com