Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

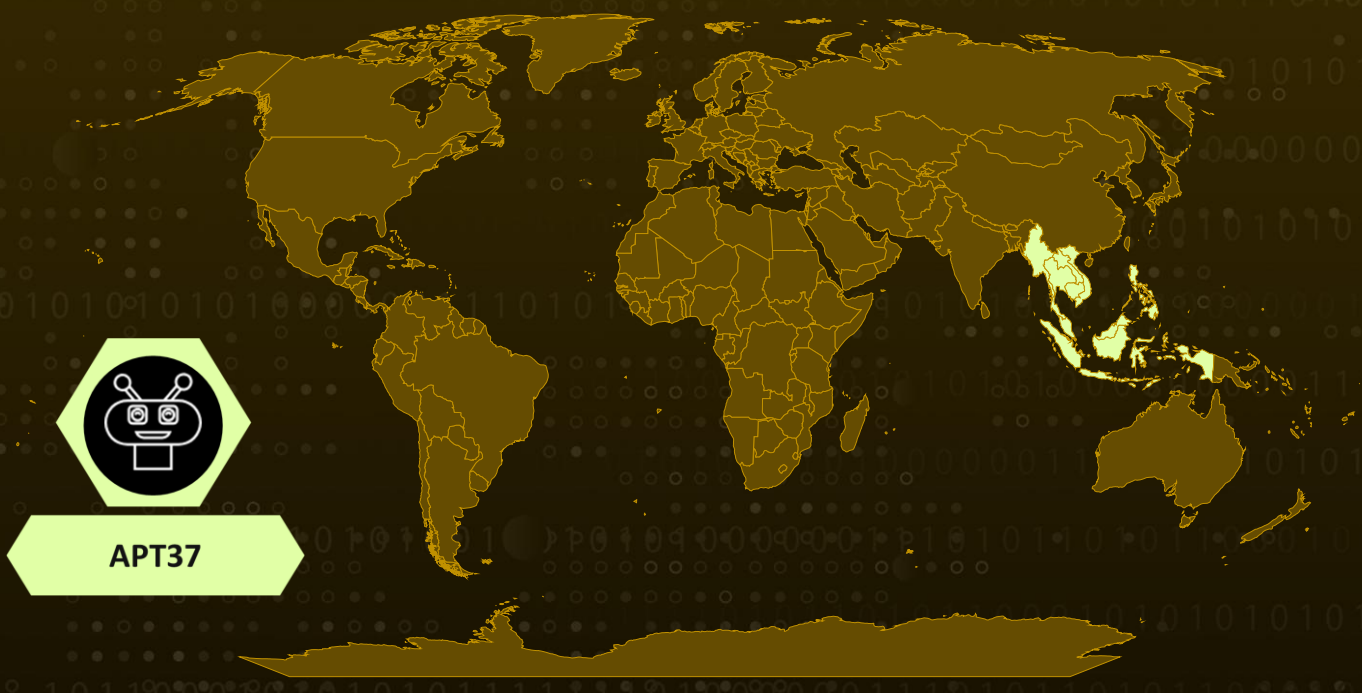
SHROUDED#SLEEP: North Korea's Silent Cyber Assault on Southeast Asia

Date of Publication	Admiralty Code	TA Number
October 7, 2024	A2	TA2024381

Summary

Attack Discovered: October 2024
Targeted Countries: Southeast Asia
Malware: VeilShell
Campaign Name: SHROUDED#SLEEP
Actor: APT37 (aka Reaper, TEMP.Reaper, Ricochet Chollima, ScarCruft, Cerium, Group 123, Red Eyes, Geumseong121, Venus 121, Hermit, InkySquid, ATK 4, ITG10, Ruby Sleet, Crooked Pisces, Moldy Pisces, Osmium, Opal Sleet)
Attack: An ongoing cyber espionage campaign, dubbed SHROUDED#SLEEP, has been attributed to North Korea's APT37, a well-known advanced persistent threat group. This group has been actively targeting countries across Southeast Asia, with Cambodia emerging as the primary focus. The campaign employs a sophisticated, multi-stage attack sequence that culminates in the deployment of a custom VeilShell PowerShell backdoor, which offers a broad range of Remote Access Trojan (RAT) functionalities.

Attack Regions



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

Attack Details

#1 The SHROUDED#SLEEP campaign, attributed to North Korea's **APT37** (also known as Reaper or Group123), is targeting countries in Southeast Asia, with a primary focus on Cambodia. APT37, a well-known advanced persistent threat (APT) group, has shifted its focus beyond South Korea and is now expanding its reach to other regions. Victims in this campaign are likely being tricked via phishing emails, which contain malicious zip files as the initial payload. These emails serve as the starting point for a complex attack chain that delivers sophisticated malware designed for espionage and remote access.

#2 The campaign employs .lnk shortcut files, which are manipulated to appear legitimate while hiding malicious code. These shortcuts are linked to PowerShell commands that decode and extract payloads directly from the file itself. The commands specifically target and extract three encoded payloads, which include an Excel lure document, a configuration file, and a malicious DLL file. These files are then deposited into the Windows Startup folder, ensuring persistence by executing on the next system reboot. The decoy lure documents serve to distract the user while the malware operates in the background.

#3 One of the key techniques used in this attack is AppDomainManager hijacking, where attackers manipulate the .NET AppDomainManager class to inject malicious code into applications early in the execution process. The malicious DomainManager.dll is loaded during startup, allowing the attackers to execute code from a remote server. The malware communicates with the attackers' command-and-control (C2) infrastructure, utilizing techniques such as JavaScript execution and PowerShell scripting to remotely control the victim's system.

#4 The ultimate goal of the campaign appears to be long-term remote access and espionage. The attackers employ a custom VeilShell PowerShell backdoor, which grants them full control over the compromised machines. This backdoor allows them to execute arbitrary commands, manipulate system settings, and exfiltrate sensitive data. The SHROUDED#SLEEP campaign's use of stealthy techniques, persistence mechanisms, and legitimate tools makes it a potent and dangerous threat in Southeast Asia's cyber landscape.

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. Limit user permissions to only what is necessary for their role, reducing the potential impact of a compromised account.

Monitor Windows Startup Directory: Regularly audit the startup directory at %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup for unauthorized or suspicious entries, as seen in this campaign where threat actors staged their malware for persistence. Additionally, monitor critical autorun locations in the Windows Registry for any changes and implement automated alerts for modifications in key registry paths often targeted by malware.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.001 Spearphishing Attachment	T1560 Archive Collected Data
T1132 Data Encoding	T1003 OS Credential Dumping	T1555 Credentials from Password Stores	T1027 Obfuscated Files or Information
T1070 Indicator Removal	T1070.004 File Deletion	T1112 Modify Registry	T1574 Hijack Execution Flow

T1574.014 AppDomainManager	**T1033** System Owner/User Discovery	**T1057** Process Discovery	**T1069** Permission Groups Discovery
T1082 System Information Discovery	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.007** JavaScript
T1204 User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File	**T1053** Scheduled Task/Job
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1041** Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	172[.]93[.]181[.]249, 208[.]85[.]16[.]88
Domains	hxxps[:]//jumpshare[.]com/view/load/crjl6ovj7HVGtuhdQrF1, hxxps[:]//jumpshare[.]com/viewer/load/zB564bxDA3yG8PnFR90I
SHA256	BEAF36022CE0BD16CAAEE0EBFA2823DE4C46E32D7F35E793AF4E1538E705379F, 913830666DD46E96E5ECBECC71E686E3C78D257EC7F5A0D0A451663251715800, 9D0807210B0615870545A18AB8EAE8CECF324E89AB8D3B39A461D45CAB9EF957, CFBD704CAB3A8EDD64F8BF89DA7E352ADF92BD187B3A7E4D0634A2DC764262B5, 55235BC9B0CB8A1BEA32E0A8E816E9E7F5150B9E2EEB564EF4E18BE23CA58434, 106C513F44D10E6540E61AB98891AEE7CE1A9861F401EEE2389894D5A9CA96EF, 6B95BC32843A55DA1F8186AEC06C0D872CAC13D9DF6D87114C5F8B7277C72A4F, 4E8B6DECCDFC259B2F77573AEF391953ED587930077B4EDB276DBBB679EF350B, 50BF6FDBFF9BFC1702632EAC919DC14C09AF440F5978A162E17B468081AFBB43, AF74D416B65217D0B15163E7B3FD5D0702D65F88B260C269C128739E7E7A4C4D, 7E9F91F0CFE3769DF30608A88091EE19BC4CF52E8136157E4E0A5B6530D510EC

References

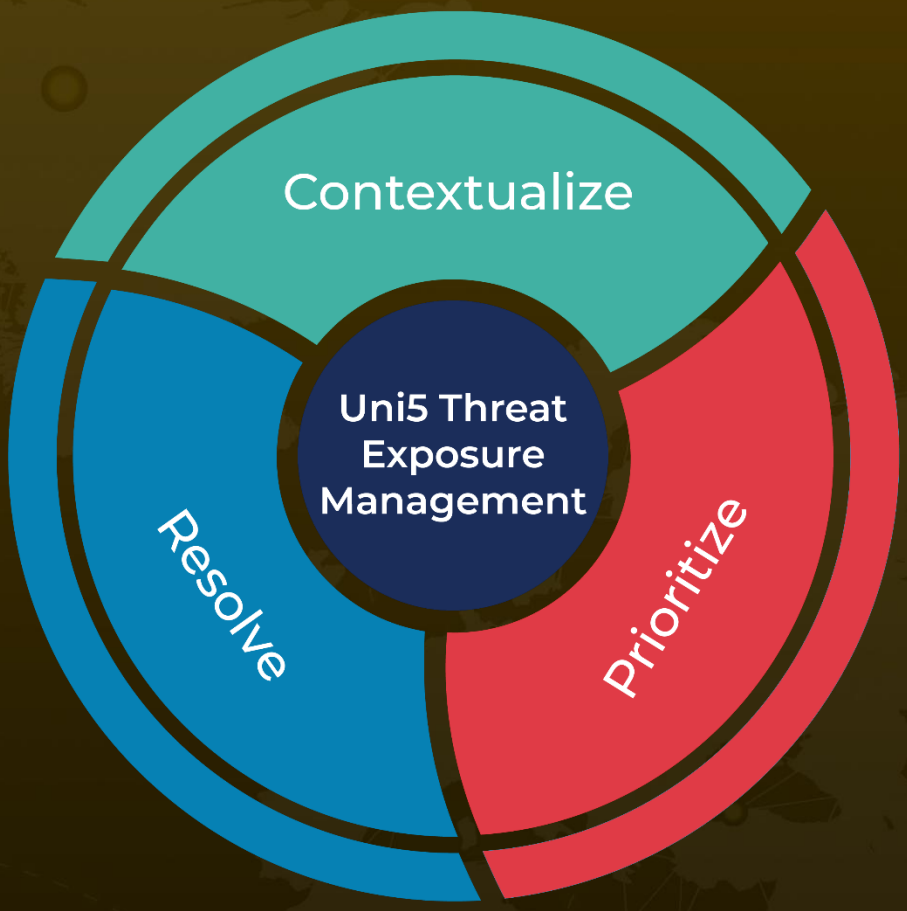
https://www.securonix.com/blog/shroudedsleep-a-deep-dive-into-north-koreas-ongoing-campaign-against-southeast-asia/

https://hivepro.com/threat-advisory/reaper-north-korean-hacking-group-targets-defectors/

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

October 7, 2024 • 7:00 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com