SECURITY ADVISORY

CYBER STASH

March, 2024

DEEP#GOSU Malware Campaign

Context

DEEP#GOSU Malware, attributed to the North Korean state-sponsored group Kimsuky, is a highly sophisticated cyber threat utilizing PowerShell and VBScript to compromise Windows systems. It operates stealthily, with capabilities including keylogging, monitoring clipboard activities, executing dynamic payloads, and exfiltrating data.

This malware employs a Remote Access Trojan (RAT) for remote control, scheduled tasks, and self-executing PowerShell scripts. Its use of TruRat suggests a focus on data exfiltration and surveillance. Additionally, the malware utilizes cloud services for command and control communication, showcasing advanced evasion techniques and highlighting the group's intent for espionage activities.

Mitigation strategies could include employing email filtering to detect and block deceptive attachments, particularly those disguised as innocuous file types like PDFs, and, enforcing PowerShell execution policies and whitelist trusted scripts to prevent unauthorized execution.

Mitigation

Defending against the DEEP#GOSU Malware Campaign necessitates more than just patching vulnerabilities. It involves actively limiting and monitoring adversary behaviours and conducting forensic-level post-breach analysis:

Forensic-Depth Memory Analysis: Incorporate regular memory-based forensic analysis across all systems into your threat hunting strategy to unveil malicious fileless executables

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

User Security Awareness Training: Provide user awareness training to educate employees on the risks of opening attachments from unknown sources.

Technical Details

The technical steps involved in the DEEP#GOSU malware infection process are:

Email Attachment: The attack begins with a malicious email attachment containing a ZIP archive. Inside this archive is a deceptive shortcut file (.LNK) disguised as a PDF file ("IMG_20240214_0001.pdf.lnk").

Execution of PowerShell Script: Upon opening the .LNK file, a PowerShell script embedded within the file is executed. This script communicates with a Dropbox infrastructure controlled by the threat actor to retrieve and execute another PowerShell script ("ps.bin").

Second-stage PowerShell Script: The second PowerShell script fetched from Dropbox retrieves a .NET assembly file called "r_enc.bin," which is actually the TruRat remote access trojan (RAT). TruRat has the capability to record keystrokes, manage files, and facilitate remote control of the compromised system.

Execution of VBScript: Additionally, the PowerShell script retrieves a VBScript ("info_sc.txt") from Dropbox. This VBScript is designed to run arbitrary code, including another PowerShell script ("w568232.ps12x"). The VBScript utilizes Windows Management Instrumentation (WMI) to execute commands on the system and set up scheduled tasks for persistence.

Dynamic Configuration Retrieval: The VBScript dynamically retrieves configuration data for the Dropbox connection from Google Docs. This allows the threat actor to modify account information without altering the script itself.

Data Exfiltration: The PowerShell script gathers extensive system information and exfiltrates the data via a POST request to Dropbox. This script serves as a backdoor for periodic communication with a command-and-control (C2) server via Dropbox, enabling the threat actor to encrypt, exfiltrate, or download data as needed.

Surveillance and Logging: The PowerShell script continuously logs user activity, including keystrokes, clipboard content, and foreground window activity. This information is then sent to the threat actor's C2 server, allowing for comprehensive surveillance and control over compromised hosts.

Tactics, Techniques and Procedures

The notable TTPs related to the DEEP#GOSU Malware are:

T1059.001 - Command and Scripting Interpreter: DEEP#GOSU malware utilizes PowerShell and VBScript scripts for execution, enabling adversaries to execute commands and carry out malicious activities on compromised systems. These scripts are often delivered via phishing emails or embedded within malicious attachments.

T1059.003 - Scheduled Task/Job: Adversaries establish persistence on compromised systems by creating scheduled tasks or jobs that execute DEEP#GOSU malware at predefined intervals. This ensures that the malware remains active and operational, even after system reboots or security measures are applied.

T1071.001 - Application Layer Protocol: DEEP#GOSU malware communicates with command-and-control (C2) servers using application layer protocols such as HTTP or HTTPS. This allows adversaries to remotely control compromised systems, exfiltrate data, and receive commands without arousing suspicion.

T1027 - Obfuscated Files or Information: Adversaries obfuscate DEEP#GOSU malware components to evade detection by security software and analysts. This includes obfuscating code, file names, and communication channels to conceal malicious activities and hinder analysis efforts.

T1107 - File Deletion: DEEP#GOSU malware deletes files and artifacts associated with its presence on compromised systems to cover its tracks and evade detection. This includes removing logs, temporary files, and other evidence of malicious activity to maintain stealth and persistence.

Cyber Threat Intelligence

The attribution of DEEP#GOSU Malware to the North Korean state-sponsored group Kimsuky illuminates a historical trajectory of cyber espionage endeavors, targeting diverse sectors. The deployment of such intricately designed malware not only underscores the group's profound technical prowess and extensive resources but also elucidates its strategic intent to procure sensitive intelligence for espionage purposes.

The incorporation of TruRat, an openly available remote access trojan, signifies a deliberate emphasis on data exfiltration and surveillance, affording threat actors the means to clandestinely monitor compromised systems and clandestinely remove invaluable data.

References

Related IOC's & Yara Rules:

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a
- https://www.hivepro.com/wp-content/uploads/2024/03/The-Evolution-of-DEEPGOSU-Attack-Campaign-by-Kimsuky-Group_TA2024108.pdf

File Hashes:

- F262588C48D2902992FFD275D2BE6362FE7F02E2F00A44AB8C75AC1A2827C6E9
- 1617587CCDF5B0344089559ECF8FE7D39F6E07A6A64F74F2B44BFA2C8CB67983
- 46A5D54C264152CE915792AF31C75824A558AF7D7340D78B34E146D8C6249E79
- 1B75F70C226C9ADA8E79C3FDD987277B0199928800C51E5A1E55FF01246701DB
- 69C917EA96DB28DBD5B67073CA0AAC234D25651A849171B45F20979EAFA05A1C
- 60666CACDD6806ED05771F32EAA719E3EFD2F4DB55F28A447D383C3EAC1DC72E
- B72CAAB78D164637FEA0937D7A94FC470579EC6BB4FA87DADB6F0FA7826E217C
- 89CAD9A57985CC0AB3B7403A943AD0AA7B167DC7A3C38557417FEDEA67A77B87

Public Intelligence:

- https://thehackernews.com/2024/03/new-deepgosu-malware-campaign-targets.html
- https://cybersecsentinel.com/deep-gosu-malware/