SECURITY ADVISORY

CYBER STASH

September, 2024

North Korean Linked MISTPEN Malware

Context

A recently identified cyber-espionage group associated with North Korea, designated as UNC2970 by Mandiant, has been employing job-themed phishing tactics to penetrate organizations within the energy and aerospace sectors. This group is deploying a novel backdoor malware, referred to as MISTPEN, specifically engineered to exfiltrate sensitive data.

UNC2970 is linked to the notorious Lazarus Group (also known as TEMP.Hermit or Diamond Sleet), which operates under the auspices of North Korea's Reconnaissance General Bureau (RGB). Since at least 2013, this organization has strategically targeted a range of sectors, including government, defense, telecommunications, and finance, with the intent to gather intelligence that aligns with North Korean strategic objectives.

The ongoing campaign, named "Operation Dream Job," has effectively targeted prominent organizations across multiple countries, including the United States, United Kingdom, Germany, Sweden, Singapore, and Australia. The implications of this activity underscore the need for heightened vigilance and robust cybersecurity measures within affected sectors.

Mitigation

Defending against the UNC2970 attack requires immediate and proactive measures:

Keep Software Updated: Regularly patch and update all software to address vulnerabilities and reduce the attack surface.

Restrict Unauthorized Software Installation: Limit user permissions to prevent the installation of unapproved applications, enhancing security against potential threats.

Block Access to High-Risk Infrastructure: Proactively restrict access to known high-risk IP addresses, ASNs, and TLDs to mitigate exposure to malicious activities.

Deploy Endpoint Detection and Response (EDR) Solutions: Implement EDR tools to provide real-time monitoring, threat detection, and automated response capabilities, enhancing overall incident response.

Technical Details

MISTPEN Malware Delivery

The MISTPEN malware is deployed through targeted spear-phishing attacks that exploit job-related themes to engage potential victims. This phishing campaign typically involves the distribution of malicious ZIP archive files disguised as legitimate job descriptions. Within these archives resides a trojanized version of a recognized PDF reader, specifically an outdated iteration of Sumatra PDF, accompanied by a launcher designated as BURNBOOK.

MISTPEN Analysis

MISTPEN is a lightweight backdoor, meticulously crafted in C, with the primary function of downloading and executing Portable Executable (PE) files. This backdoor is a modified derivative of the open-source Notepad++ binhex plugin (version 2.0.0.1), enhanced through the integration of a thread that activates the execution of malicious code within the DllMain function.

MISTPEN utilizes AES encryption to decrypt a token using the key EF 0D 4E A6 D8 B8 E8 73 DF 17 5C 0B 51 F6 3B 33, enabling access to a Microsoft API endpoint. Communication is established over HTTP with the following Microsoft Graph URLs:

hxxps://login.microsoftonline.com/common/oauth2/v2.0/token

hxxps://graph.microsoft.com/v1.0/me/drive/root:/path/upload/hello/

hxxps://graph.microsoft.com/v1.0/me/drive/root:/path/upload/world/

hxxps://graph.microsoft.com/v1.0/me/drive/items/

TEARPAGE Analysis

TEARPAGE functions as a loader embedded within the resource section of BURNBOOK, employing DLL search order hijacking via the legitimate BdeUISrv.exe binary. The malware copies this binary from its original location into the directory where the loader resides. Upon execution, TEARPAGE decrypts an encrypted payload stored in %APPDATA% \Thumbs.ini.

Attack Chain Overview

1. Spear-Phishing: Attackers engage victims via email or messaging platforms like WhatsApp, posing as recruiters and sharing tailored job postings aimed at high-level professionals.

2. Payload Delivery: Victims receive the job description as a ZIP file, containing a PDF that requires the included, weaponized PDF reader for access.

3. Malware Execution: Opening the PDF with the compromised Sumatra PDF reader triggers the execution of a malicious DLL via BURNBOOK, commencing the infection process.

4. MISTPEN Deployment: BURNBOOK subsequently deploys an embedded DLL file named "wtsapi32.dll," tracked as TEARPAGE. TEARPAGE decrypts and executes the MISTPEN backdoor upon system reboot.

MISTPEN, a trojanized variant of a legitimate Notepad++ plugin (binhex.dll), serves as a lightweight backdoor capable of downloading and executing PE files from a command-and-control (C2) server. It communicates with the C2 infrastructure through HTTP requests directed to Microsoft Graph URLs, facilitating remote command execution.

Backdoor Command Functions

The MISTPEN backdoor supports the following command functionalities:

d: This command instructs the backdoor to parse, load into memory, and execute the received PE payload, subsequently sending a message to its C2 server with the result of the execution or a confirmation string indicating the loading address.

e: Issuing this command prompts the backdoor to transmit the message "DEAD" to its C2 server, followed by termination of the process.

f: This command allows the backdoor to send a "Sleep Success" message to its C2 server, after which it enters a sleep state for a specified duration. Upon awakening, it communicates "Hi, I'm just woke up!" to the C2 server.

g: Through this command, the backdoor reports "Hiber Success" to its C2 server, updates its sleep duration in configuration, saves this to setup.bin, and subsequently enters a sleep state based on the revised timing.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to UNC2970 :

Tactic: Initial Access | Technique: Spear Phishing via Service (T1566.002)

Job-themed spear-phishing lures are used to engage victims via email and messaging apps like WhatsApp.

Tactic: Execution | Technique: User Execution (T1204)

Malicious ZIP files disguised as job descriptions trigger malware execution when opened by the user.

Tactic: Persistence | Technique: Boot or Logon Autostart Execution (T1547)

TEARPAGE ensures MISTPEN is executed after the system reboots, maintaining persistence on the compromised machine.

Tactic: Defense Evasion | Technique: Masquerading (T1036)

The attackers use a repurposed legitimate PDF reader, Sumatra PDF, and the Notepad++ plugin to evade detection.

Tactic: C&C | Technique: Application Layer Protocol (T1071.001)

MISTPEN communicates with its C2 server over HTTP via Microsoft Graph URLs to maintain control over infected machines.

Tactic: Exfiltration | Technique: Exfiltration Over C2 Channel (T1041)

The backdoor exfiltrates data through established C2 channels.

Cyber Threat Intelligence

Cicada33 UNC2970, also identified as APT 38 or the “Lazarus Group,” has orchestrated a series of targeted attacks against critical sectors, notably energy, aerospace, and defense. This group employs advanced tactics that prominently feature social engineering and job-themed phishing campaigns, designed specifically to penetrate high-level corporate environments. Their focus on senior management and personnel with access to sensitive information underscores a deliberate strategy to gather intelligence that aligns with North Korean strategic interests.

Since 2022, the group has utilized the MISTPEN malware in conjunction with its launcher, BURNBOOK. Both components have evolved through iterative enhancements, allowing the threat actors to evade detection mechanisms while deploying increasingly sophisticated capabilities. Notably, MISTPEN facilitates communication with command-and-control (C2) servers, often hosted on compromised WordPress sites, thereby enabling remote management of infected systems from diverse geographical locations.

CyberStash anticipates that the tactics employed by UNC2970 may extend beyond their current targets, posing a significant threat to a broader array of industries. As this group refines its methodologies, other sectors must remain vigilant against the possibility of similar attack vectors being leveraged against them. The implications of these developments call for enhanced awareness and robust cybersecurity measures across all critical industries to mitigate the risk posed by such advanced persistent threats.

References

IOCs:

- https://github.com/eset/malware-ioc/blob/master/nukesped_lazarus/README.adoc
- https://github.com/BRANDEFENSE/IoC/blob/main/IoC-YARA-SIGMA-Rules-%20APT38.txt
- https://github.com/halilozturkci/APT38-Lazarus-Threat-Analysis-Report-from-ADEO

Malicious URLs:

- https(://)dstvdtt.co.za/wp-content/plugins/social-pug/assets/lib(.)php
- https(://)cmasedu.com/wp-content/plugins/kirki/inc/script(.)php
- https(://)bmtpakistan.com/solution/wp-content/plugins/one-click-demo-import/assets/asset(.)php
- https(://)verisoftsystems.com/wp-content/plugins/optinmonster/views/upgrade-link-style(.)php
- https(://)www.clinicabaru.co/wp-content/plugins/caldera-forms/ui/viewer-two/viewer-2(.)php

Public Intelligence:

- https://cloud.google.com/blog/topics/threat-intelligence/unc2970-backdoor-trojanized-pdf-reader
- https://cybersecsentinel.com/unc2970-launches-mistpen-against-critical-infrastructure/
- https://medium.com/@rtate_91319/apt-38-lazarus-group-b6145ee28822
- https://industrialcyber.co/ransomware/google-details-unc2970-north-korea-linked-espionage-hackers-targeting-us-energy-aerospace-sectors/
- https://thehackernews.com/2023/03/north-korean-unc2970-hackers-expands.html