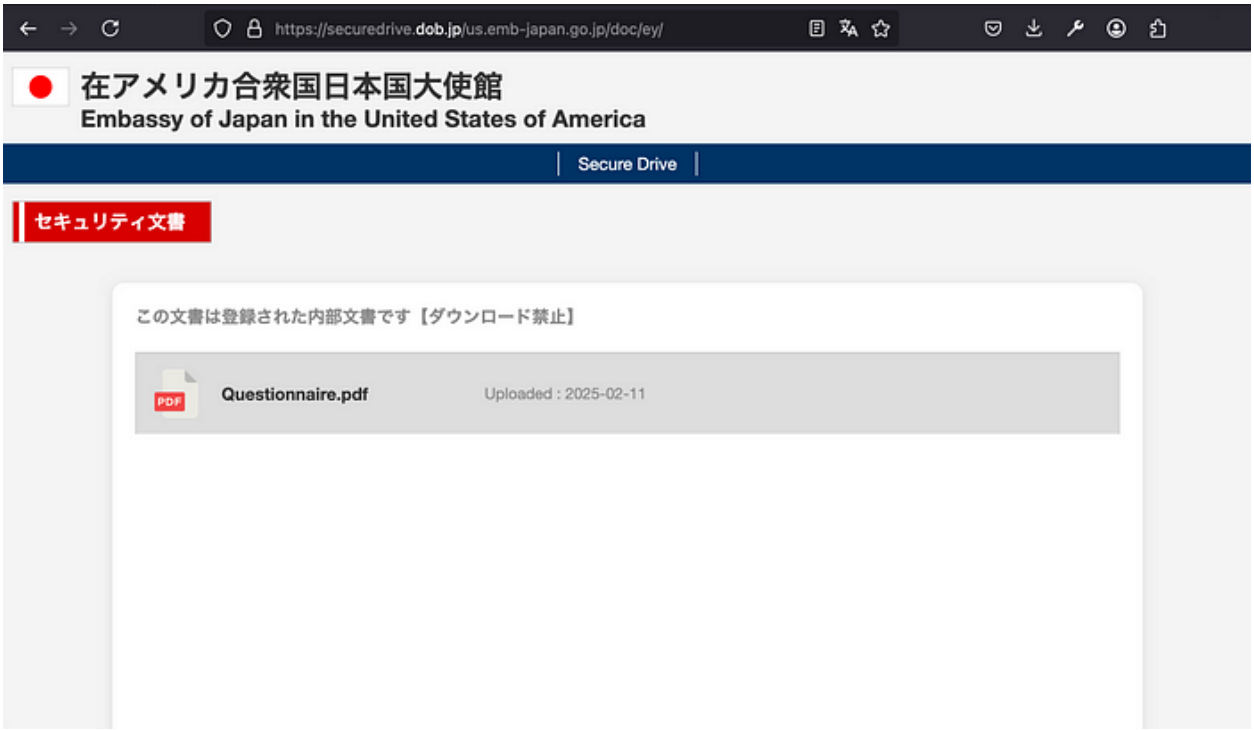
Kimsuky Impersonates the Embassy of Japan in the United States

2025-02-19
By Alec Dhuse

The North Korean threat actor known as Kimsuky, also identified as APT43 and Emerald Sleet, has initiated a new campaign impersonating the Embassy of Japan in the United States. Their primary targets are individuals involved in North Korean-related research at think tanks and research institutions in the United States.

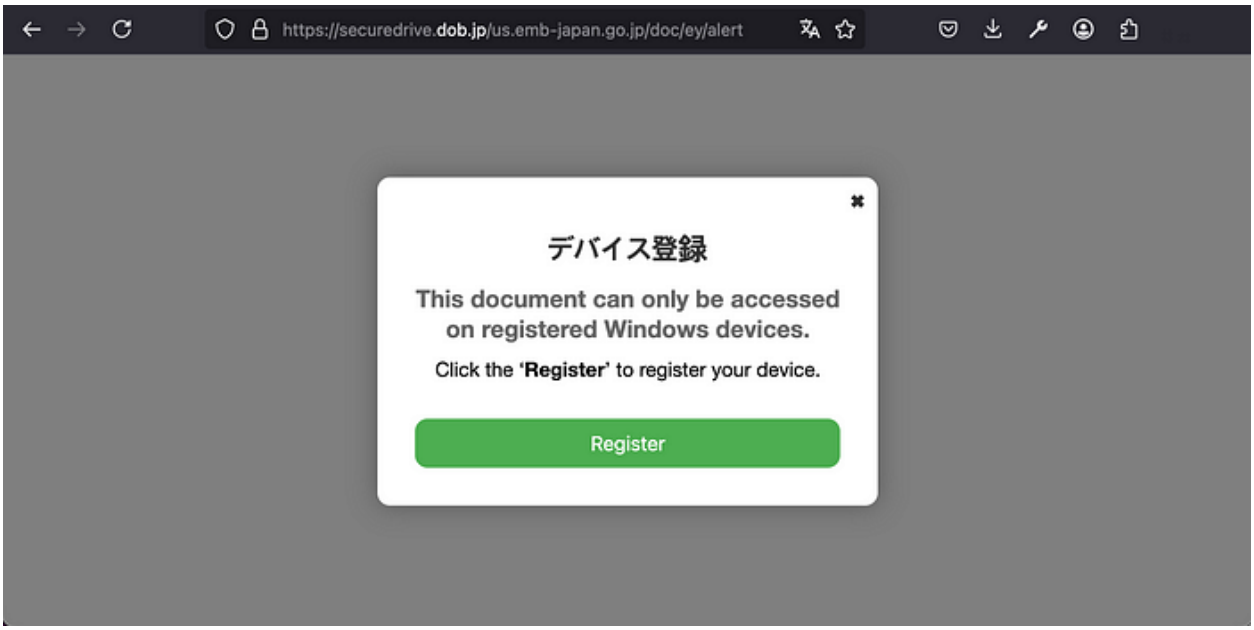
In this campaign, Kimsuky impersonates a representative from the Japanese embassy using a free ProtonMail account. The initial email sent by the attacker is an invitation to a meeting with the Japanese ambassador. Subsequent emails provide details about the meeting and a formal-looking PDF attachment outlining the event's agenda. This PDF contains a malicious link leading to a fake questionnaire on the topics to be discussed.

When the victim clicks the link, they are redirected to a fraudulent secure drive disguised as the official Embassy of Japan portal.



The secure drive website impersonating the Embassy of Japan.

If the victim attempts to access the questionnaire, the phishing site displays a deceptive message: "This document can only be accessed on registered Windows devices."



The fraudulent device registration message.

The site then instructs the victim to open the Windows Run prompt and paste a provided confirmation code. A pop-up message conveniently includes a copy button, which places malicious Windows Command Shell code onto the clipboard. When the user pastes the "confirmation code" into the Run prompt and presses enter, the malicious script is executed.

Fake access code and instructions to paste the code into the Windows Run prompt.

The Windows Command Shell does the following:

- Opens a benign decoy document.

- Creates a hidden system directory named tempcaches in the root of the c drive.
- Creates a scheduled task named Update-out-of-date-20240324001883765674.
- Executes a malicious script c:\tempcaches\temp.vbs via Windows Script Host.
- Schedules the task to run 19 minutes later.
- Uses curl to download a file from:
  - hXXps://bit-albania.com/yron/demo.php?ccs=cin to c:\tempcaches\config.sys.
  - At the time of analysis, this file was unavailable — it may have been removed or required server-side validation that could not be satisfied during analysis.
- Executes the downloaded script.
- Downloads another script file from the bit-albania[.] domain. This file's name is specified in the first line of the previously downloaded file.
- Executes the newly downloaded second script.
- Creates a second scheduled task named Update-out-of-date-20240324001883765675 set to run 20 minutes later.
- Collects system data by running:
  - tasklist.exe (to list running processes)
  - whoami (to identify the logged-in user)
- Exfiltrates the collected data via hXXps://bit-albania.com/yron/updemo.php.

Conclusion

Kimsuky continues to impersonate well-known individuals using free email providers. Their strategy involves building trust through multiple benign emails before delivering a malicious payload — a tactic that has proven highly effective over several years.

To mitigate this threat, organizations should:

- **Educate users** on phishing techniques and email security best practices.
- **Disable the Windows Run prompt** for users who do not require it.
- **Encourage reporting of suspicious emails** to security teams.

Additionally, Kimsuky has adopted a newer tactic that involves using social engineering to trick victims into running a malicious Windows Command Shell script, and this strategy is proving effective. To protect potential victims, organizations should consider turning off the Windows Run prompt for users who do not need it.

With the increased political instability in the U.S., the North Korean government is likely to ramp up its intelligence-gathering efforts against research institutions in Western countries. Security professionals should prepare by collaborating with individuals in their organizations who are likely to be targeted. They should educate these individuals about the tactics and techniques used by this threat actor. Furthermore, organizations should establish a straightforward method for reporting suspicious email messages, which a security professional can review.

Indicators of Compromise (IoCs)

- Kimsuky has extensively used the compromised domain: bit-albania[.]com.

URLs

- hXXps://securedrive.dob.jp/us.emb-japan.go.jp/doc/ey
- hXXps://securedrive.dob.jp/us.emb-japan.go.jp/doc/ey/src/resp.php
- hXXps://bit-albania.com/yron/demo.php?ccs=cin
- hXXps://bit-albania.com/yron/demo.php?ccs=cout
- hXXps://bit-albania.com/yron/updemo.php

Tactics, Techniques, and Procedures (TTPs)

Resource Development

- T1584.003 Compromise Infrastructure: Virtual Private Server
- T1585.002 Establish Accounts: Email Accounts

Initial Access

- T1566.001 Phishing: Spearphishing Attachment

Execution

- T1059.003 Command and Scripting Interpreter: Windows Command Shell
- T1059.001 Command and Scripting Interpreter: PowerShell
- T1053.005 Scheduled Task/Job: Scheduled Task

Defense Evasion

- T1564.001 Hide Artifacts: Hidden Files and Directories
- T1656 Impersonation

Discovery

- T1033 System Owner/User Discovery
- T1057 Process Discovery

Exfiltration

- T1020 Automated Exfiltration

Tags

- Cybersecurity
- Kimsuky
- North Korea
- Phishing