Kimsuky’s Use of GitHub for Malware Delivery and Exfiltration

Archived: 2026-04-05 20:45:52 UTC

✅ Executive Summary:

- S2W’s Threat Intelligence Center, TALON, has recently identified ongoing activity by the North Korea–backed APT group Kimsuky involving the abuse of GitHub repositories. A detailed analysis was conducted on the latest observed tactics.

- The threat actor leveraged a malicious LNK file to download and execute additional PowerShell-based scripts from a GitHub repository.

- To access the repository, the attacker embedded a hardcoded GitHub Private Token directly within the script.

- The PowerShell script retrieved from the repository collects system metadata including last boot time, system configuration, and running processes, writes the information into a log file, and uploads it to the attacker-controlled repository.

📌 Detailed Analysis

1) NTS_Attach.zip

- The ZIP archive contains an LNK file masquerading as an electronic tax invoice.

2) 전자세금계산서.pdf.lnk

- Executing the shortcut file disguised as a PDF launches a PowerShell command that downloads and runs an additional malicious script.

3) main.ps1

- The dropped main.ps1 script downloads a decoy document and an additional malicious payload from a private GitHub repository operated by the threat actor. The script includes a hardcoded GitHub Private Token to access the repository.
  - GitHub Repository: hxxps://github[.]com/God0808RAMA/group_0721/

- The decoy document impersonates an electronic tax invoice and is displayed upon execution.

- The script then downloads a file named real.txt from the group_0721 repository. It replaces the string $upFolder with a timestamped value (ntxBill_{MMdd_HHmm}), then re-uploads the modified script back to the attacker’s

repository using the filename real.txt_{MMdd_HHmm}.txt. This allows the attacker to dynamically manage scripts based on infection time.

- To establish persistence, the script creates a file named MicrosoftEdgeUpdate.ps1 under the %AppData% path and writes a PowerShell code block defined in main.ps1.

- This block downloads the previously uploaded real.txt_{MMdd_HHmm}.txt file, saves it as temporary.ps1 under %AppData%, and executes it.

- A scheduled task is then created to repeatedly run temporary.ps1 at 30-minute intervals:
  - Task Name: BitLocker MDM policy Refresh{DBHDFE12-496SDF-Q48D-SDEF-1865BCAD7E00}
  - Trigger: One-time execution after 5 minutes, then every 30 minutes

- This mechanism allows the attacker to automatically fetch and execute updated PowerShell scripts over time.

- Additionally, a file named first.txt is downloaded from the repository, with folder names similarly modified to ntxBill_{MMdd_HHmm}. It is saved as %AppData% emporary.ps1 and appears to be executed immediately after initial infection, prior to the scheduled task being activated.

4) temporary.ps1: Info-Stealer

- The first downloaded first.txt (saved as temporary.ps1) functions as an info-stealer. It collects:
  - IP address (first NIC, first IP)
  - Current time (MMdd_HHmm)
  - Last boot time
  - OS information (Caption/Version/Build/Architecture)
  - Hardware information (Manufacturer/Model/Domain/Memory from Win32_ComputerSystem)
  - Device type: Notebook (Mobile) or Desktop
  - OS installation date
  - List of running processes

- All collected data is written to a log file and uploaded to the attacker's repository under a folder named ntxBill_{MMdd_HHmm}.

5) temporary.ps1: Time Logger

- The later-downloaded real.txt_{MMdd_HHmm}.txt file is also saved as temporary.ps1 and executed via the task scheduler. It creates a log file and records the last boot time, which is uploaded to the same folder (ntxBill_{MMdd_HHmm}).

📌 GitHub Repositories used by Kimsuky

- By analyzing the hardcoded token, investigators identified nine private repositories associated with the attacker as of August 20, 2025:
  - group_0717/
  - group_0721/

- test/
- hometax/
- group_0803/
- group_0805/
- group_0811/
- fsc_doc/
- repayment/

- Commit history from these repositories revealed the email address used by the attacker during GitHub account creation:
  - Email: sahiwalsuzuki4[@]gmail.com

- These repositories contained logs exfiltrated from infected systems, decoy documents used in the campaign, and files resembling payment reminders, business reports, and audit-related documents.

- Notably, one test log generated by the info-stealer included the process names xeno_rat_server and rdpclip, indicating the presence of remote administration tools and clipboard monitoring.

✅ Recommended Threat Detection and Mitigation Actions:

- Given the group’s continued abuse of trusted infrastructure (such as GitHub) and the use of PowerShell-based malware for information theft, the following actions are strongly recommended:
  - Monitor traffic to api.github.com, especially PUT /repos/*/contents/ requests
  - Detect the creation of scheduled tasks indicative of malware persistence mechanisms

👩‍💻 Report Author: S2W TALON

👉 Contact us: https://s2w.inc/en/contact

*The full report is available upon request and for QUAXAR subscribers.