[Kimsuky] Operation Covert Stalker - ASEC

By ATCP

Published: 2023-10-31 · Archived: 2026-04-05 16:25:03 UTC

On May 3rd, 2022, AhnLab posted an analysis on the ASEC blog under the title **“Distribution of Malicious Word File Related to North Korea’s April 25th Military Parade”**.

[+] Analysis of Malware Disguised with Military Parade Content: https://asec.ahnlab.com/en/33936/

This report is based on 17 months of tracking and analysis of the Kimsuky group’s hacking activities (C2 operations, management, sending hacking emails, distributing malware, etc.) that share similar patterns with the major characteristics (C2, web shells, etc.) explained in the analysis above. The Kimsuky group’s hacking activities included sending phishing emails and hacking emails with malware attachments to certain individuals or organizations involved in the field of North Korea, politics, diplomacy, and security with the purpose of stealing email accounts and important materials. The group carried out covert and persistent hacking to achieve its purpose, which is why we named this operation **“Operation Covert Stalker”**. The report also explains why we believe the Kimsuky group is behind the hacking activities.

[+] Report Summary

– **Phishing emails** disguised with legitimate URLs **or hacking emails** with malware attachments have been sent **to certain individuals or organizations involved in the field of North Korea, politics, diplomacy, and security.**

– The **RDP vulnerability (CVE-2019-0708)** was exploited in Windows systems, and **unidentified vulnerabilities** were exploited in vulnerable websites for hacking.
– An account for accessing RDP has been created to **gain persistence in connection** and **installed additional remote control programs** such as RDP Wrapper, Quasar RAT, Ammy RAT, AnyDesk, and TeamViewer.
– **Various malicious behaviors** have been carried out, such as searching for targets for hacking, sending hacking emails, scanning for the RDP vulnerability (CVE-2019-0708), and testing malware.
– Targets have been infected with the **BlackBit ransomware** and victims have been led to pay the ransom for recovery.
– C2 have been **configured, managed, and operated** via web shells (Green Dinosaur, WebadminPHP, and other unknown web shells).
– Some malware included **North Korean expressions such as "련동"** ("ryeondong", integration)**, "봉사기"** ("bongsagi", server)**, and "대명부"** ("daemyeonbu", interface).

[+] Download Report: 20231101_Kimsuky_OP. Covert Stalker (This report supports Korean only for now.)

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/58654/