Rewterz Threat Alert –North Korean APT Kimsuky Aka Black Banshee - Active IOCs - Rewterz

Published: 2024-01-23 · Archived: 2026-04-02 10:37:17 UTC

Severity

High

Analysis Summary

Kimsuky is a North Korean advanced persistent threat (APT) group, also known as “Black Banshee”. The group has been active since at least 2012 and is believed to be state-sponsored. Kimsuky is known for conducting cyber espionage operations and targeting organizations and individuals in various countries, including South Korea, Japan, and the United States. The group has been observed using various techniques to compromise its targets, such as phishing attacks, malware infections, and supply chain attacks. The group’s ultimate goals and motivations are not well understood, but they are generally believed to be focused on intelligence gathering and political or economic gain. The tactics, techniques, and procedures (TTPs) used by the Kimsuky APT group are constantly evolving, but some of their most commonly used methods include:

- Phishing attacks: The group has been known to send phishing emails that contain malicious attachments or links to compromised websites.
- Malware infections: Kimsuky has been observed using various types of malware, including remote access trojans (RATs), backdoors, and wiper malware.
- Supply chain attacks: The group has been known to compromise legitimate software or websites to distribute malware to a wider audience.
- Lateral movement: Once the group has compromised a target, they use techniques such as network scanning, password cracking, and privilege escalation to move laterally within the victim’s network.
- Data exfiltration: Kimsuky has been observed using various methods to steal data from its targets, including command-and-control servers, cloud storage services, and removable media.

In October 2022, Kimsuky was observed using mobile malware to target Android devices. Researchers gave the malicious APKs the names FastFire, FastViewer, and FastSpy by including the word Fast in the package name and describing each one’s characteristics. This group has been conducting constant attacks on mobile devices to steal the target’s information. Their sophisticated technique is Firebase, a standard service employed as the C&C server in FastFire. Furthermore, some attempts are being made to avoid detection by modifying Androspy, an open-source RAT. Sophisticated attack vectors, similar to FastViewer, are utilized to attack specified targets, and existing open sources are being leveraged to produce high-performance variations such as FastSpy. FastViewer and FastSpy were employed to attack South Koreans and all three APKs. The mobile targeting approach of the Kimsuky group is becoming more advanced, thus it is important to be cautious about sophisticated attacks aimed at Android smartphones or devices.

In May 2023, the Kimsuky group was observed using a new version of its reconnaissance malware, called ReconShark (an evolution of the threat actor's BabyShark malware toolset), in a global cyberespionage campaign. The malware is designed to gather information on targeted systems and exfiltrate that data back to the attackers. It is believed that the group uses this information to gain access to sensitive networks and steal valuable intellectual property.

Impact

- Data Theft and Espionage
- Sensitive Data Exposure

Indicators of Compromise

Domain Name

lfpa.website

MD5

- 97ba3c7b95aac463c4c561c5f940bbf8

SHA-256

- 35ddb63c0729a7e3019c026865ea195607a51943d8867607a26c006f0df6e594

SHA-1

- 13c2c93022576a173226f10e35c64c83b495f868

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Emails from unknown senders should always be treated with caution.
- Never trust or open links and attachments received from unknown sources/senders.
- It is also recommended that individuals and organizations use secure and encrypted communication channels, such as VPNs and encrypted email when transmitting sensitive information.
- Additionally, the use of multi-factor authentication can help to reduce the risk of sensitive information being stolen by attackers.
