Contents

[**Kimsuky (G0094)** 2](#_Toc179362249)

[**I. Introduction** 2](#_Toc179362250)

[**II. Tactics** 2](#_Toc179362251)

[**III. Techniques** 2](#_Toc179362252)

[**IV. Procedures** 3](#_Toc179362253)

[**V. Summary** 4](#_Toc179362254)

[**References** 6](#_Toc179362255)

## **Kimsuky (G0094)**

## **I. Introduction**

Kimsuky, which is also known as Velvet Chollima, Black Banshee, and Thallium, is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group is primarily known for its focus on intelligence gathering operations targeting South Korean entities, including government agencies, think tanks, and individuals involved in Korean reunification efforts. In recent years, Kimsuky has expanded its targeting to include other countries, particularly those involved in North Korean policy-making and nuclear issues.

## **II. Tactics**

Kimsuky's tactical approach is characterized by

1. **Social Engineering**

Heavy reliance on sophisticated social engineering techniques to manipulate targets into compromising their security.

1. ***Persistent Intelligence Gathering***

Continuous efforts to collect sensitive information related to Korean peninsula affairs and international relations.

1. ***Credential Harvesting***

Focused campaigns to obtain login credentials for various services, particularly email accounts of high-value targets.

1. ***Mobile Device Targeting***

Increasing focus on compromising mobile devices to gather intelligence and track targets.

1. ***Adaptive Toolset***

Regular updates and modifications to their malware and tools to evade detection and improve efficacy.

## **III. Techniques**

Kimsuky employs a range of techniques in their operations.

|  |  |
| --- | --- |
| Technique | Description |
| Spear-phishing Campaigns (T1566) | Use of highly targeted emails with malicious attachments (T1566.001).  Employment of spear-phishing links leading to credential harvesting pages (T1566.002). |
| Watering Hole Attacks (T1189) | Compromise of websites frequented by targets to distribute malware or gather intelligence. |
| Malware Deployment | Use of custom malware families such as BabyShark, KimskyMiner, and AppleSeed.  Deployment of Android malware for mobile device compromise. |
| Command and Control (C2) Infrastructure | Use of compromised websites for C2 communication (T1102.002).  Implementation of social media platforms for C2, including Twitter and GitHub (T1102.002). |
| Credential Access | Development of convincing phishing pages mimicking legitimate login portals (T1056.003).  Use of keyloggers to capture user credentials (T1056.001). |
| Persistence | Creation of scheduled tasks for periodic malware execution (T1053.005).  Use of Windows Registry run keys for persistence (T1547.001). |
| Defense Evasion | Obfuscation of malicious PowerShell scripts (T1027.009). |

## **IV. Procedures**

Kimsuky's typical attack chain follows this sequence

1. ***Initial Access***

a. Highly targeted spear-phishing emails are sent, often impersonating trusted entities or individuals.

b. Emails contain either malicious attachments (often .hwp files) or links to credential harvesting sites.

1. ***Execution***

a. If a malicious attachment is opened, it typically exploits vulnerabilities in the Hangul Word Processor (HWP) software.

b. For credential harvesting, victims are directed to convincing phishing sites that mimic legitimate login pages.

1. ***Persistence and Privilege Escalation***

a. Once executed, malware establishes persistence through scheduled tasks or registry modifications.

b. The group attempts to elevate privileges, often through social engineering or by exploiting local vulnerabilities.

1. ***Discovery and Lateral Movement***

a. Kimsuky conducts network reconnaissance to identify high-value targets and sensitive data.

b. Lateral movement is achieved using stolen credentials and exploiting misconfigurations.

1. ***Collection and Exfiltration***

a. Sensitive documents and emails are identified and collected.

b. Data is exfiltrated through various channels, often disguised as legitimate traffic to cloud services.

1. ***Ongoing Operations***

a. Kimsuky maintains long-term access to compromised networks for continuous intelligence gathering.

b. They regularly update their tools and techniques to evade detection and maintain persistence.

## **V. Summary**

This group’s operations offer a compelling look into North Korea's cyber espionage priorities and methods. Their targeting aligns closely with North Korean state interests, which focus on South Korean government activities, reunification efforts, and international policy towards North Korea.

What stands out about Kimsuky is their sophisticated social engineering. They excel at creating convincing lures that appeal to their targets' professional interests. They often impersonate journalists or researchers who are seeking expert opinions on Korean peninsula affairs. This approach has proven particularly effective against think tanks and policy experts. Kimsuky's shift towards mobile device compromise is equally noteworthy, because it reflects the broader trend of sensitive communications moving to mobile platforms. Their development of Android malware that is capable of monitoring device activity and exfiltrating data highlights the need for comprehensive security measures across all devices.

Another intriguing tactic is that Kimsuky's uses social media platforms and public code repositories for command and control. This clever approach allows them to hide their malicious traffic in plain sight, by blending in with normal network activities. As geopolitical dynamics on the Korean peninsula continue to evolve, Kimsuky's operations serve as a digital indicator of North Korean intelligence priorities. Their targeting choices often reveal which issues and individuals in the North Korean regime considers most crucial at any given time, making their activities valuable not just for cybersecurity professionals, but also for those involved in international relations and policy-making related to North Korea.

## **References**

1. CISA. (2020). "North Korean State-Sponsored Advanced Persistent Threat Group Activities." <https://www.cisa.gov/uscert/ncas/alerts/aa20-301a>
2. Falcone, R., & Lee, B. (2018). "New BabyShark Malware Targets U.S. National Security Think Tanks." Palo Alto Networks. <https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/>
3. MITRE ATT&CK. (2024). "Kimsuky, G0094." <https://attack.mitre.org/groups/G0094/>