Severity

High

Analysis Summary

Kimsuky is a North Korean nation-state actor that has been active since 2012. It primarily targets South Korean government agencies and conducts espionage activities against targets in the United States and Japan. Kimsuky has dropped a custom backdoor which they are calling Gold Dragon. Kimsuky deploys Gold Dragon, a second-stage backdoor, after a file-less PowerShell-deploying first-stage attack is dropped.

This group has the ability to put up phishing infrastructure that can effectively imitate well-known websites and fool users into entering their passwords. Kimsuky APT is also known by the names Thallium, Black Banshee, and Velvet Chollima. KISA (Korean Internet & Security Agency) published a full investigation of Kimsuky's phishing infrastructure and TTPs used to attack South Korea in December 2020. To get Initial Access to victim networks, Kimsuky's threat actors use a variety of spear phishing and social engineering techniques. This group is responsible for the 2014 Korea Hydro & Nuclear Power Co. compromise, and other major campaigns like Operation Kabar Cobra(2019).

Impact

- Information theft and espionage
- Exposure of sensitive data

Indicators of Compromise

MD5

- 9f2235f0d07bd903c947b17caa82ded4

SHA-256

- db7be1ef9f7656af75b3f3e47393d90e6f92f836cc09b31f6a5290655e5f8db7

SHA-1

- 55f1d9551a2ef583c248439fa545d183987bc941

URL

- https[:]//beastmodser[.]club/sil/0304/r[.]php

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.
- Always be suspicious about emails sent by unknown senders.