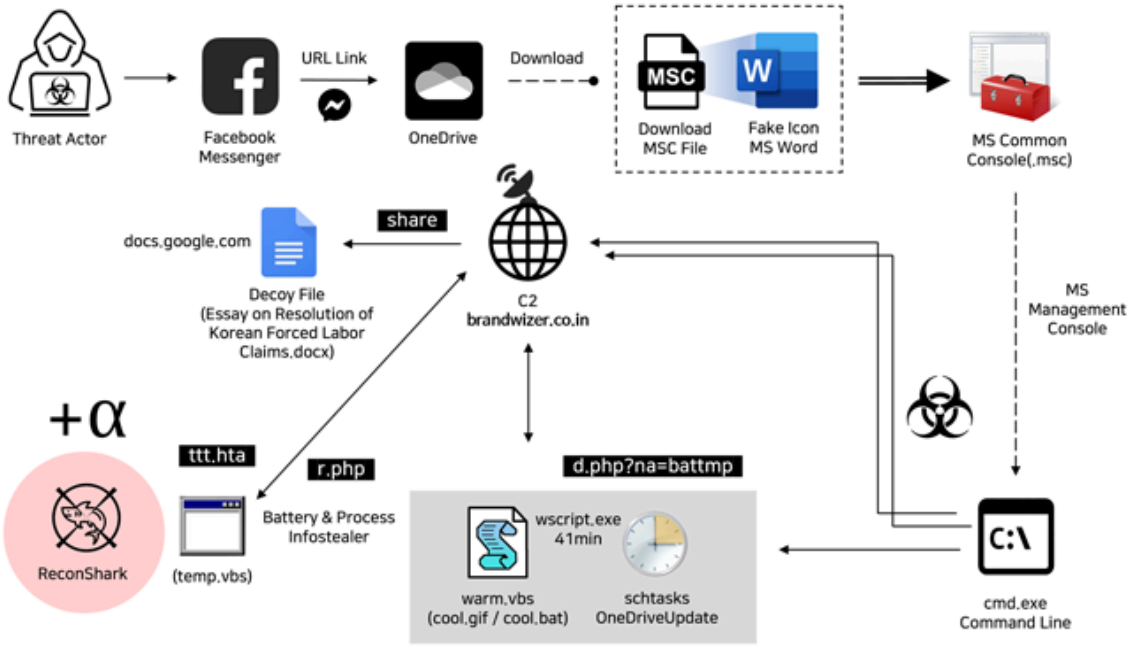
North Korean Hackers Exploit Facebook Messenger in Targeted Malware Campaign

By The Hacker News

Published: 2024-05-16 · Archived: 2026-04-05 23:04:01 UTC



The North Korea-linked Kimsuky hacking group has been attributed to a new social engineering attack that employs fictitious Facebook accounts to targets via Messenger and ultimately delivers malware.

"The threat actor created a Facebook account with a fake identity disguised as a public official working in the North Korean human rights field," South Korean cybersecurity company Genians said in a report published last week.

The multi-stage attack campaign, which impersonates a legitimate individual, is designed to target activists in the North Korean human rights and anti-North Korea sectors, it noted.

The approach is a departure from the typical email-based spear-phishing strategy in that it leverages the social media platform to approach targets through Facebook Messenger and trick them into opening seemingly private documents written by the persona.

The decoy documents, hosted on OneDrive, is a Microsoft Common Console document that masquerades as an essay or content related to a trilateral summit between Japan, South Korea, and the U.S. -- "My_Essay(prof).msc" or "NZZ_Interview_Kohei Yamamoto.msc" -- with the latter uploaded to the VirusTotal platform on April 5, 2024, from Japan.

This raises the possibility that the campaign may be oriented toward targeting specific people in Japan and South Korea.

The use of MSC files to pull off the attack is a sign that Kimsuky is utilizing uncommon document types to fly under the radar. In a further attempt to increase the likelihood of success of the infection, the document is disguised as an innocuous Word file using the word processor's icon.

Should a victim launch the MSC file and consent to opening it using Microsoft Management Console (MMC), they are displayed a console screen containing a Word document that, when launched, activates the attack sequence.

This involves running a command to establish a connection with an adversary-controlled server ("brandwizer.co[.]in") to display a document hosted on Google Drive ("Essay on Resolution of Korean Forced Labor Claims.docx"), while additional instructions are executed in the background to set up persistence as well as collect battery and process information.

The gathered information is then exfiltrated to the command-and-control (C2) server, which is also capable of harvesting IP addresses, User-Agent strings, and timestamp information from the HTTP requests, and delivering relevant payloads as necessary.

Genians said that some of the tactics, techniques, and procedures (TTPs) adopted in the campaign overlap with prior Kimsuky activity disseminating malware such as ReconShark, which was detailed by SentinelOne in May 2023.

"In the first quarter of this year, spear-phishing attacks were the most common method of APT attacks reported in South Korea," the company noted. "Although not commonly reported, covert attacks via social media are also occurring."

"Due to their one-on-one, personalized nature, they are not easily detected by security monitoring and are rarely reported externally, even if the victim is aware of them. Therefore, it is very important to detect these personalized threats at an early stage."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/05/north-korean-hackers-exploit-facebook.html