North Korean Hackers Exploit PowerShell Trick to Hijack Devices in New Cyberattack

thehackernews.com/2025/02/north-korean-hackers-exploit-powershell.html

February 12, 2025

The North Korea-linked threat actor known as Kimsuky has been observed using a new tactic that involves deceiving targets into running PowerShell as an administrator and then instructing them to paste and run malicious code provided by them.

"To execute this tactic, the threat actor masquerades as a South Korean government official and over time builds rapport with a target before sending a spear-phishing email with an [sic] PDF attachment," the Microsoft Threat Intelligence team said in a series of posts shared on X.

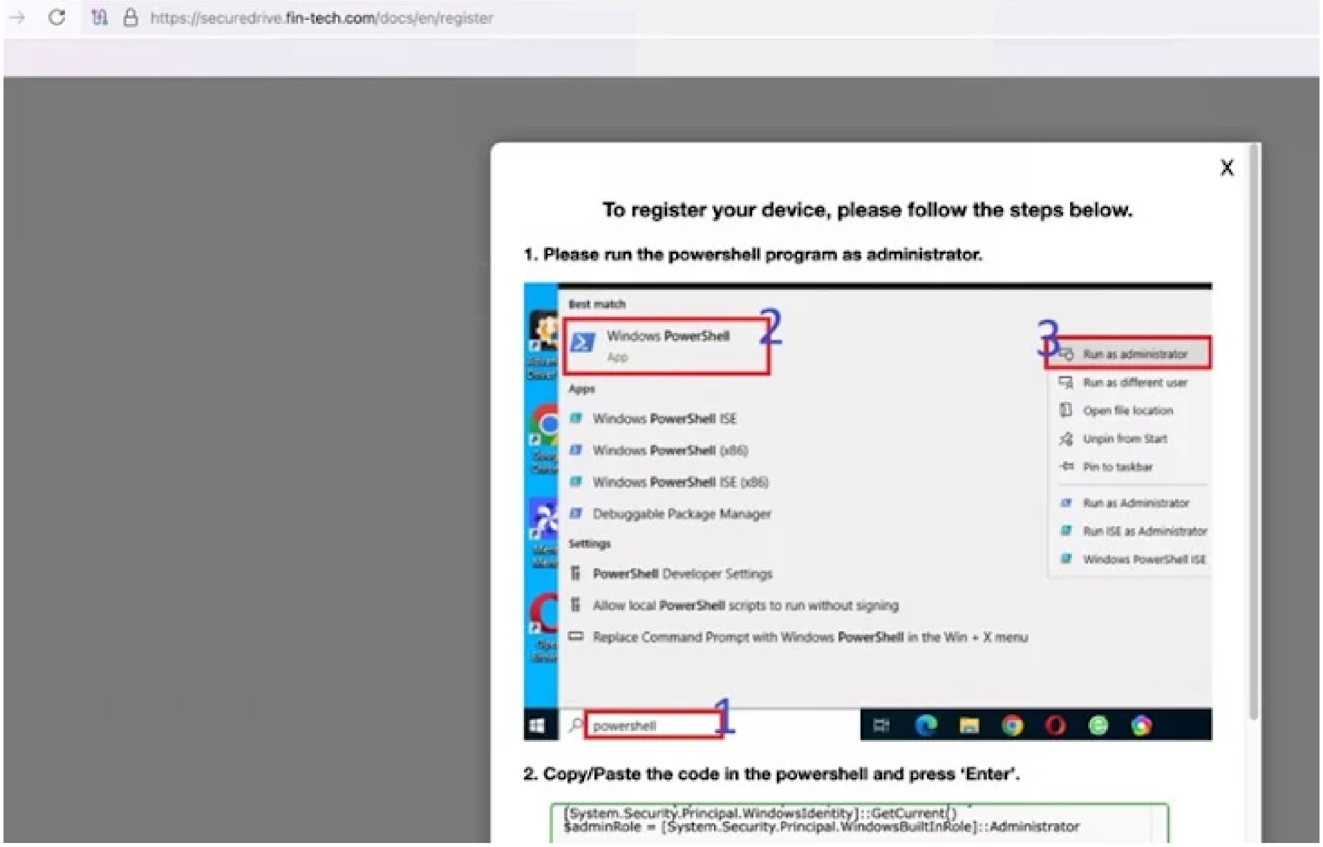
To read the purported PDF document, victims are persuaded to click a URL containing a list of steps to register their Windows system. The registration link urges them to launch PowerShell as an administrator and copy/paste the displayed code snippet into the terminal, and execute it.

Should the victim follow through, the malicious code downloads and installs a browser-based remote desktop tool, along with a certificate file with a hardcoded PIN from a remote server.

"The code then sends a web request to a remote server to register the victim device using the downloaded certificate and PIN. This allows the threat actor to access the device and carry out data exfiltration," Microsoft said.

The tech giant said it observed the use of this approach in limited attacks since January 2025, describing it as a departure from the threat actor's usual tradecraft.

It's worth noting that the Kimsuky is not the only North Korean hacking crew to adopt the compromise strategy. In December 2024, it was revealed that threat actors linked to the Contagious Interview campaign are tricking users into copying and executing a malicious command on their Apple macOS systems via the Terminal app so as to address a supposed problem with accessing the camera and microphone through the web browser.



https://securedrive.fin-tech.com/docs/en/register

To register your device, please follow the steps below.

1. Please run the powershell program as administrator.

2. Copy/Paste the code in the powershell and press 'Enter'.

```
[System.Security.Principal.WindowsIdentity]::GetCurrent()
$adminRole = [System.Security.Principal.WindowsBuiltInRole]::Administrator
```

Such attacks, along with those that have embraced the so-called ClickFix method, have taken off in a big way in recent months, in part driven by the fact that they rely on the targets to infect their own machines, thereby bypassing security protections.

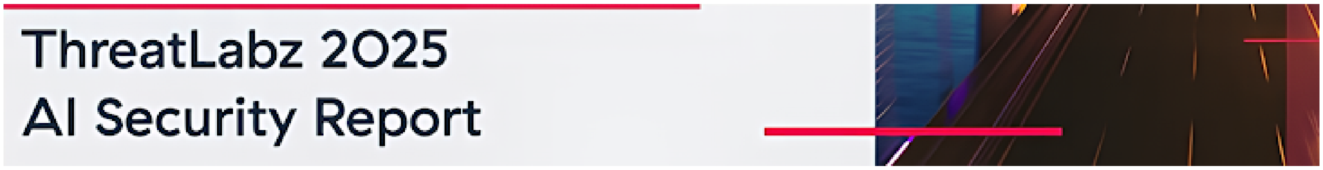
Arizona woman pleads guilty to running laptop farm for N. Korean IT workers

The development comes as the U.S. Department of Justice (DoJ) said a 48-year-old woman from the state of Arizona pleaded guilty for her role in the fraudulent IT worker scheme that allowed North Korean threat actors to obtain remote jobs in more than 300 U.S. companies by posing as U.S. citizens and residents.

The activity generated over $17.1 million in illicit revenue for Christina Marie Chapman and for North Korea in violation of international sanctions between October 2020 and October 2023, the department said.

"Chapman, an American citizen, conspired with overseas IT workers from October 2020 to October 2023 to steal the identities of U.S. nationals and used those identities to apply for remote IT jobs and, in furtherance of the scheme, transmitted false documents to the Department of Homeland Security," the DoJ said.

"Chapman and her coconspirators obtained jobs at hundreds of U.S. companies, including Fortune 500 corporations, often through temporary staffing companies or other contracting organizations."



The defendant, who was arrested in May 2024, has also been accused of running a laptop farm by hosting multiple laptops at her residence to give the impression that the North Korean workers were working from within the country, when, in reality, they were based in China and Russia and remotely connected to the companies' internal systems.

"As a result of the conduct of Chapman and her conspirators, more than 300 U.S. companies were impacted, more than 70 identities of U.S. person were compromised, on more than 100 occasions false information was conveyed to DHS, and more than 70 U.S. individuals had false tax liabilities created in their name," the DoJ added.

The increased law enforcement scrutiny has led to an escalation of the IT worker scheme, with reports emerging of data exfiltration and extortion.

"After being discovered on company networks, North Korean IT workers have extorted victims by holding stolen proprietary data and code hostage until the companies meet ransom demands," the U.S. Federal Bureau of Investigation (FBI) said in an advisory last month. "In some instances, North Korean IT workers have publicly released victim companies' proprietary code."

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