DPRK hackers dupe targets into typing PowerShell commands as admin

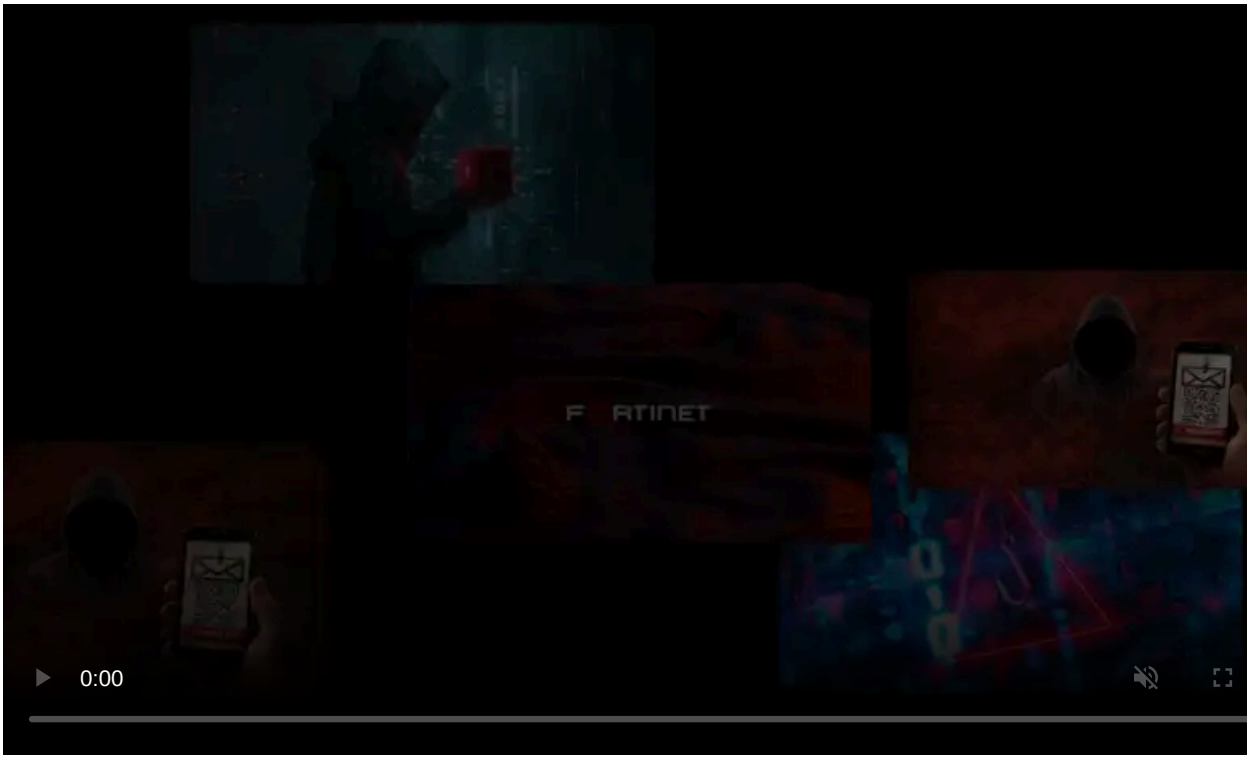
By Bill Toulas

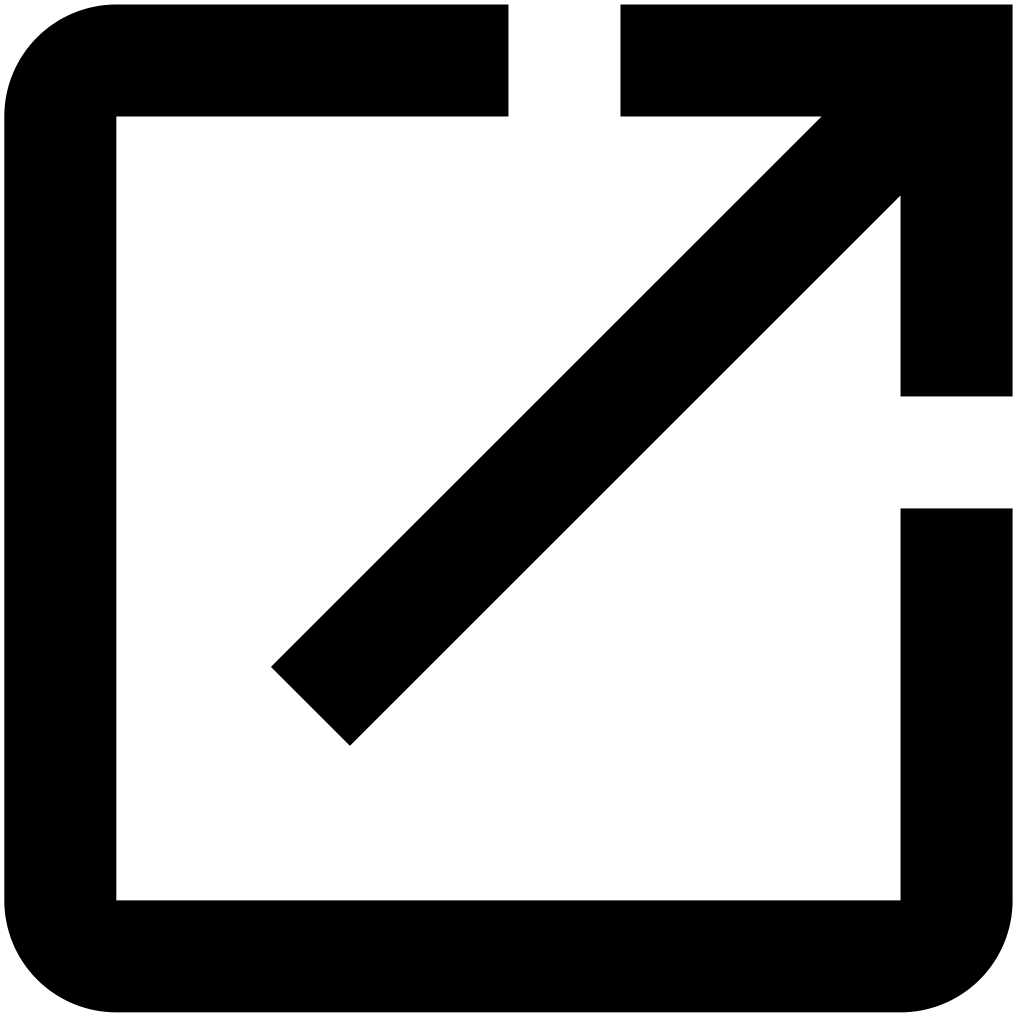
Published: 2025-02-12 · Archived: 2026-04-06 00:33:24 UTC

North Korean state actor ‘Kimsuky’ (aka ‘Emerald Sleet’ or ‘Velvet Chollima’) has been observed using a new tactic inspired from the now widespread ClickFix campaigns.

ClickFix is a social engineering tactic that has gained traction in the cybercrime community, especially for distributing infostealer malware.

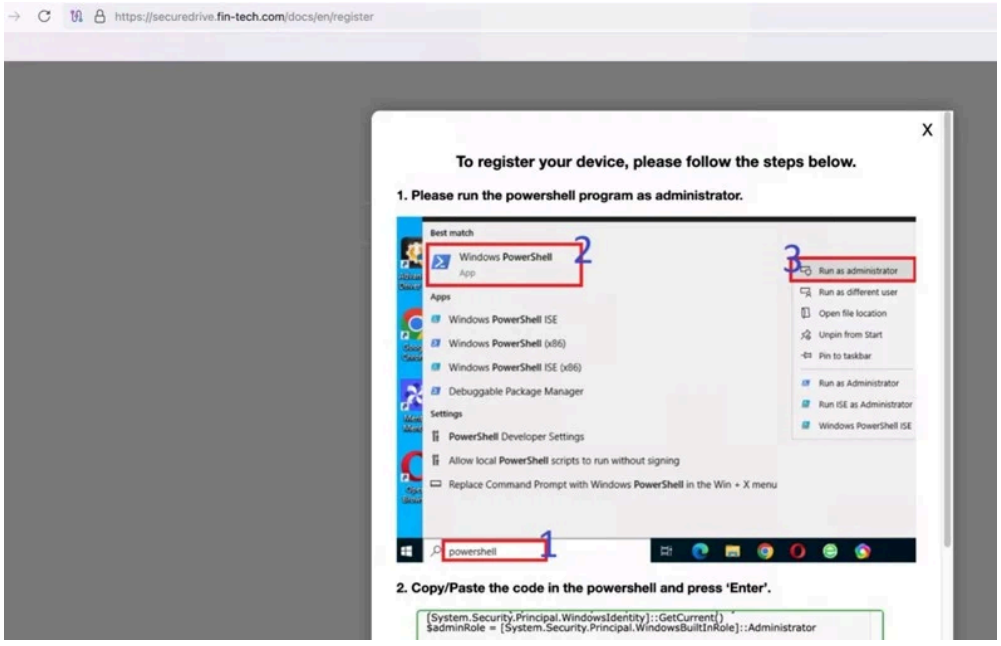
It involves deceptive error messages or prompts that direct victims to execute malicious code themselves, often via PowerShell commands. These actions typically lead to malware infections.


F RTINET
0:00



According to the information from Microsoft's Threat Intelligence team, the attacker masquerades as a South Korean government official and gradually builds a connection with the victim.

Once a certain level of trust is established, the attacker sends a spear-phishing email with a PDF attachment. However, targets that want to read the document are directed to a fake device registration link that instructs them to run PowerShell as an administrator and paste attacker-provided code.



Instructions for performing the device registration

Source: Microsoft

When executed, the code installs a browser-based remote desktop tool, downloads a certificate using a hardcoded PIN, and registers the victim's device with a remote server, giving the attacker direct access for data exfiltration.

Microsoft says it observed this tactic in limited-scope attacks starting January 2025, targeting individuals that work in international affairs organizations, NGOs, government agencies, and media companies across North America, South America, Europe, and East Asia.

Microsoft notified customers targeted by this activity, and urges others to take note of the new tactic and treat all unsolicited communications with extreme caution.

"While we have only observed the use of this tactic in limited attacks since January 2025, this shift is indicative of a new approach to compromising their traditional espionage targets," warns Microsoft.

The adoption of ClickFix tactics by nation-state actors like Kimsuky is a testament to the attack's effectiveness in actual operations.

Users should show caution when encountering requests to execute on their computers code they copy online, especially when doing so with administrator privileges.

Source: https://www.bleepingcomputer.com/news/security/dprk-hackers-dupe-targets-into-typing-powershell-commands-as-admin/