Microsoft: BlueNoroff hackers plan new crypto-theft attacks

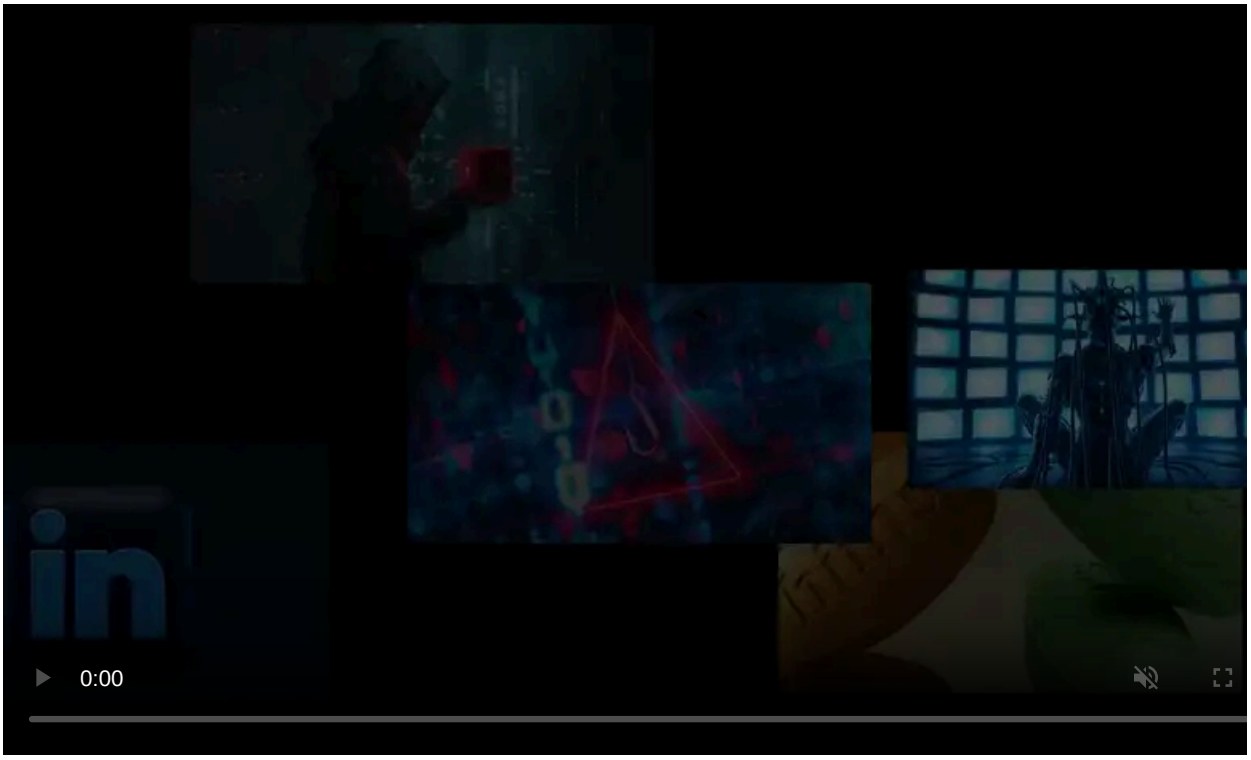
By Sergiu Gatlan

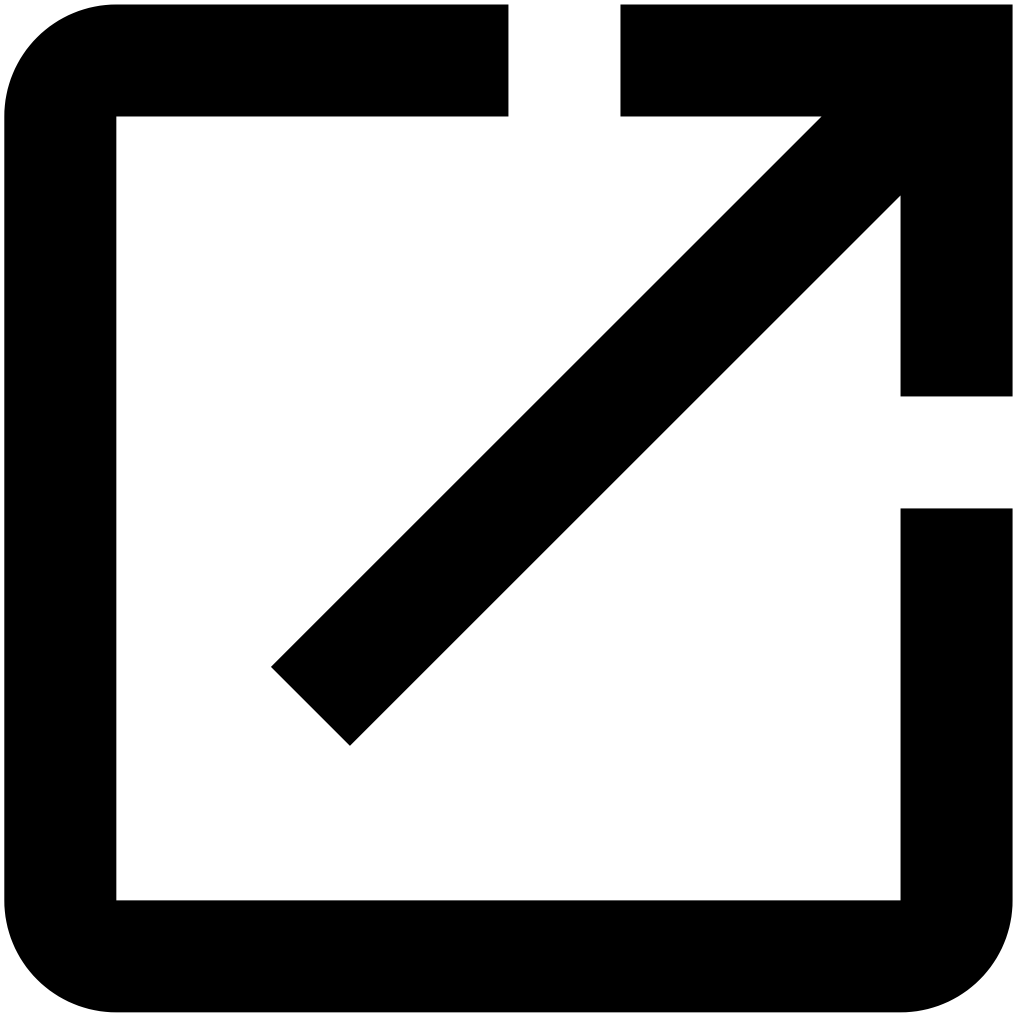
Published: 2023-11-10 · Archived: 2026-04-05 18:43:41 UTC

Microsoft warns that the BlueNoroff North Korean hacking group is setting up new attack infrastructure for upcoming social engineering campaigns on LinkedIn.

This financially motivated threat group (tracked by Redmond as Sapphire Sleet) also has a documented history of cryptocurrency theft attacks targeting employees within cryptocurrency companies.

After picking their targets following initial contact on LinkedIn, the BlueNoroff hackers backdoor their systems by deploying malware hidden in malicious documents pushed via private messages on various social networks.


0:00



"The threat actor that Microsoft tracks as Sapphire Sleet, known for cryptocurrency theft via social engineering, has in the past few weeks created new websites masquerading as skills assessment portals, marking a shift in the persistent actor's tactics," according to Microsoft Threat Intelligence security experts.

"Sapphire Sleet typically finds targets on platforms like LinkedIn and uses lures related to skills assessment. The threat actor then moves successful communications with targets to other platforms."

Previously, the North Korean state hackers were seen distributing malicious attachments directly or using links to pages hosted on legitimate websites like GitHub.

However, Microsoft believes that swift detection and removal of the attackers' malicious files from legitimate online services prompted the BlueNoroff hackers to create their own websites capable of hosting malicious payloads.

These websites are password-protected to thwart analysis efforts and are camouflaged as skills assessment portals, urging recruiters to register for an account.

Who is BlueNoroff?

Earlier this week, Jamf Threat Labs' security researchers linked BlueNoroff to new ObjCShellz macOS malware used to backdoor targeted Macs by opening remote shells on compromised devices.

In recent years, Kaspersky linked BlueNoroff to a series of attacks against cryptocurrency startups and financial organizations worldwide, including in the U.S., Russia, China, India, the U.K., Ukraine, Poland, Czech Republic, UAE, Singapore, Estonia, Vietnam, Malta, Germany, and Hong Kong.

Additionally, the FBI attributed the largest crypto hack in history—the breach of Axie Infinity's Ronin network bridge—to the Lazarus and BlueNoroff hacking groups. The attackers stole 173,600 Ethereum and 25.5 million USDC tokens, amounting to over $617 million.

Four years ago, a United Nations report estimated that North Korean state hackers, including BlueNoroff, had already stolen around $2 billion in at least 35 cyberattacks targeting banks and cryptocurrency exchanges across more than a dozen countries.

In 2019, the U.S. Treasury also sanctioned BlueNoroff and two other North Korean hacking groups (Lazarus Group and Andariel) for channeling stolen financial assets to the North Korean government.

Source: https://www.bleepingcomputer.com/news/security/microsoft-bluenoroff-hackers-plan-new-crypto-theft-attacks/