Google: North Korean hackers have targeted security researchers via social media

By Catalin Cimpanu

Published: 2021-01-26 · Archived: 2026-04-05 21:33:08 UTC

Group of hooded hackers shining through a digital north korean flag cybersecurity concept

Michael Borgers, Getty Images/iStockphoto

Google said today that a North Korean government hacking group has targeted members of the cyber-security community engaging in vulnerability research.

The attacks have been spotted by the Google Threat Analysis Group (TAG), a Google security team specialized in hunting advanced persistent threat (APT) groups.

In a report published earlier today, Google said North Korean hackers used multiple profiles on various social networks, such as Twitter, LinkedIn, Telegram, Discord, and Keybase, to reach out to security researchers using fake personas.

Email was also used in some instances, Google said.

"After establishing initial communications, the actors would ask the targeted researcher if they wanted to collaborate on vulnerability research together, and then provide the researcher with a Visual Studio Project," said

Adam Weidemann, a security researcher with Google TAG.

The Visual Studio project contained malicious code that installed malware on the targeted researcher's operating system. The malware acted as a backdoor, contacting a remote command and control server and waiting for commands.

This malware was later linked to the Lazarus Group, a well-known North Korean state-sponsored operation.

> KTAE code similarity analysis for the malware used to target security researchers involved in 0day analysis and development. "Manuscrypt" (also known as FALLCHILL) is typically used by the Lazarus APT. 👉 pic.twitter.com/hXxuJIj9Lc
>
> — Costin Raiu (@craiu) January 26, 2021

New mysterious browser attack also discovered

But Wiedemann said that the attackers didn't always distribute malicious files to their targets. In some other cases, they asked security researchers to visit a blog they had hosted at **blog[.]br0vvnn[.]io** (*do not access*).

Google said the blog hosted malicious code that infected the security researcher's computer after accessing the site.

"A malicious service was installed on the researcher's system and an in-memory backdoor would begin beaconing to an actor-owned command and control server," Weidemann said.

But Google TAG also added that many victims who accessed the site were also running "fully patched and up-to-date Windows 10 and Chrome browser versions" and still got infected.

Details about the browser-based attacks are still scant, but some security researchers believe the North Korean group most likely used a combination of Chrome and Windows 10 zero-day vulnerabilities to deploy their malicious code.

As a result, the Google TAG team is currently asking the cyber-security community to share more details about the attacks, if any security researchers believe they were infected.

The Google TAG report includes a list of links for the fake social media profiles that the North Korean actor used to lure and trick members of the infosec community.

Security researchers are advised to review their browsing histories and see if they interacted with any of these profiles or if they accessed the malicious blog.br0vvnn.io domain.


nk-apt-twitter-profiles.png
Image: Google

In case they did, they are most likely to have been infected, and certain steps need to be taken to investigate their own systems.

The reason for targeting security researchers is pretty obvious as it could allow the North Korean group to steal exploits for vulnerabilities discovered by the infected researchers, vulnerabilities that the threat group could deploy in its own attacks with little to no development costs.

In the meantime, several security researchers have already disclosed on social media that they received messages from the attackers' accounts, although, none have admitted to having systems compromised.

> WARNING! I can confirm this is true and I got hit by @z0x55g who sent me a Windows kernel PoC trigger. The vulnerability was real and complex to trigger. Fortunately I only ran it in VM.. in the end the VMDK I was using was actually corrupted and non-bootable, so it self-imploded https://t.co/dvdCWsZyne
>
> — Richard Johnson (@richinseattle) January 26, 2021
