Forbes Middle East

Apple Mac Hack Warning: North Korea Uses Fake Cryptocurrency Companies To Break Into macOS

Hackers said to be sponsored by North Korea have found a novel way to attack Apple Macs, according to research published on Sunday.

The so-called Lazarus Group, considered by the U.S. government and numerous cybersecurity companies to be sponsored by North Korea, are trying to get into Macs via some fake cryptocurrency software created by a front company.

Here's how it worked, according to Apple Mac security specialist and principal security researcher at Jamf Patrick Wardle: The hackers created a fake company complete with an official-looking website. In this latest case, the North Koreans set up the front company, JMT Trading.

They then wrote an open-source cryptocurrency trading app and put it up on the code-sharing site GitHub. Hidden within that code, though, was malware that, when downloaded onto a target Apple PC, would give the hacker the ability to do anything they wanted on the Mac. As Wardle put it in a blog post: "The ability to remotely execute commands clearly gives a remote attacker full and extensible control over the infected macOS system."

The hackers may then go a step further by contacting administrators and users of cryptocurrency exchanges, asking them to test and review their new app, Wardle told *Forbes*. If they get lucky, they get a bit of leverage in an official cryptocurrency vendor and start infecting targets.

North Korea has repeatedly tried to find a way into cryptocurrency coffers, with a good degree of success. In August, reports indicated it had made as much as $2 billion by hacking into a mix of traditional banks and cryptocurrency companies. Some of that money appears to be going into helping the state develop weapons of mass destruction.

This latest attack on macOS follows a *modus operandi* similar to a previous campaign detected by Russin cybersecurity firm Kaspersky in August 2018. Again, a front company—Celas LLC—was created to target the cryptocurrency sector.

"Do you have to worry about getting infected? Probably not, unless you're an employee working at a cryptocurrency exchange," said Wardle.

http://staging.forbesmiddleeast.com/apple-mac-hack-warning-north-korea-uses-fake-cryptocurrency-companies-to-break-into-macos