

Lazarus Group Deploys Its First Mac Malware in Cryptocurrency Exchange Hack

By Catalin Cimpanu

Published: 2018-08-23 · Archived: 2026-04-05 13:11:08 UTC



Lazarus Group, the North Korean hackers who hacked Sony Films a few years back, have deployed their first Mac malware ever, according to Russian antivirus vendor Kaspersky Lab.

In a report shared with Bleeping Computer in advance, Kaspersky researchers reveal that Lazarus Group penetrated the IT systems of an Asia-based cryptocurrency exchange platform.

The hack of this platform was not reported in the media as of yet, a Kaspersky spokesperson told Bleeping Computer.



Visit Advertiser website [GO TO PAGE](#)

"The company was breached successfully, but we are not aware of any financial loss," Vitaly Kamluk, Head of GReAT APAC at Kaspersky Lab told Bleeping Computer via email today. "We assume the threat was contained based on our notification."

Exchange hacked after employee downloads trojanized app

The hack, which Kaspersky Lab analyzed under the codename of Operation AppleJeus, took place after one of the exchange's employees downloaded an app from a legitimate-looking website that claimed to be from a company that develops cryptocurrency trading software.

But the app was a fake and infected with malware. On Windows, the app downloaded and infected users with [Fallchill](#), a remote access trojan (RAT) known to be associated with the Lazarus Group since at least 2016, when it was deployed for the first time in live campaigns.

But unlike previous Lazarus operations, the hackers also deployed a Mac malware strain, something they have not done before. The malware was hidden inside the Mac version of the same cryptocurrency trading software.

Experts say that both the Windows and Mac malware wasn't visible inside the tainted app. Lazarus operators did not embed the malware inside the third-party app directly but merely modified its update component to download the malware at a later date.

The mystery of the malware's certificate

Furthermore, the trojanized cryptocurrency trading software was also signed by a valid digital certificate, allowing it to bypass security scans.

The big mystery surrounding this certificate is that it was issued by a company that Kaspersky experts said they weren't able to prove it ever existed at the address in the certificate's information.

"The fact that they developed malware to infect macOS users in addition to Windows users and – most likely – even created an entirely fake software company and software product in order to be able to deliver this malware undetected by security solutions, means that they see potentially big profits in the whole operation, and we should definitely expect more such cases in the near future," Kamluk says.

Kaspersky didn't name the hacked cryptocurrency exchange

Several cyber-security firms have pointed out many times this year that since the start of 2017, North Korean hackers have shown great interest in penetrating cryptocurrency exchanges and financial institutions, from where they steal funds that they later bring back into North Korea.

In the past year, several Asian cryptocurrency exchange platforms suffered security incidents, primarily exchange platforms located in South Korea. Hacks have been reported at [Bithumb](#), [Yapizon](#), [YouBit](#), [Coinrail](#), and [Bithumb again](#).

Kaspersky did not reveal the name of the cryptocurrency exchange at the center of its report, but told Bleeping Computer

This week, US cyber-security firm Trend Micro reported a [supply-chain attack on South Korean organizations](#), but did not attribute the hack to North Korea, nor did it specify that the hack targeted a cryptocurrency exchange platform.

"We are aware of waves of attacks on supply chains in South Korea this year, but AppleJeus is unrelated to these attacks," Kamluk told Bleeping Computer. "The victim was not located in South Korea."

Article updated post-publication with additional comments from Kaspersky.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/lazarus-group-deploys-its-first-mac-malware-in-cryptocurrency-exchange-hack/>