Lazarus Group financial targeting

Threat Memo - TM 20-004 - Date: 14/01/2020 - Version: 1.0

TLP:WHITE

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cybercrime, Cyberespionage	Theft of funds Information gathering	World	Financial, cryptocurrency	A1

Key Points

- North Korean threat actor Lazarus Group continues to target financial institutions and cryptocurrencies.
- The goal is likely collecting funds for North Korea.
- Lazarus Group continues to be an important asset for the North Korean regime for both revenue generation, but also technological cyberespionage.

Summary

Since its hack on Sony Pictures in 2014, the Bangladesh Central Bank US$ 81M hack and the global Wannacry ransomware infection in 2017, Lazarus Group, the North Korean state-sponsored hacker group known for cyberespionage, has matured its capabilities. Lately, Kaspersky Labs has issued reports[1,2] on the AppleJeus campaigns targeting cryptocurrency trading platform users and their systems. These platforms serve as a marketplace where cryptocurrency traders can buy and sell this digital money with the goal of speculation. Often, these software packages allow the user to automate trading orders, much like algorithmic trading in conventional securities trading.

In the first wave of AppleJeus attacks, existing open-source trading platforms were repacked with malware and published on fake trading platform sites intended to lure the user, possibly via social engineering. In the second wave, a fake company was used to deliver highly targeted malware to victims by adopting a multi-stage procedure to avoid detection. Only systems displaying specific characteristics would be infected with the final malware. In both waves, Lazarus Group wrote its malware for macOS as well as Windows. The last wave included a fileless variant, indicating the group has broken through that technical threshold.

Besides cyberespionage activities, Lazarus Group continues to target financial institutions and networks, including cryptocurrency, as a means of procuring funds for North Korea. Recent events include:

- Hacking an Indian nuclear power plant and space research organisation (November 2019),
- Compromising a cryptocurrency trading app targeting exchange administrators (October 2019),
- Attacking ATMs and banks in India (September 2019),
- Targeting Android users in South Korea through trojanised apps in the Google Play Store (August 2019).

Comments

In this current wave of cryptocurrency trading platform attacks, Lazarus Group targets financial institutions and individuals using high frequency cryptocurrency trading. Although the goal of these attacks is likely to embezzle funds, this current attack wave is not limited to stealing private cryptocurrency keys (such as in the attacks described in CERT-EU Memo [191126-1]) but rather serves to gain access to financial institutions and traders in order to conduct much larger theft operations.

Recent attacks by Lazarus Group confirm that this threat actor is an important asset for the North Korean regime for both revenue generation, but also technological cyberespionage.

Beyond their technical expertise (multiplatform malware variants, fileless persistence, etc.), the group continues to exhibit that they master multiple variants of supply chain compromise:

- setting up a fake company,
- setting up a fake trading platform,
- compromising trading app,
- targeting exchange administrators.

[1] https://securelist.com/operation-applejeus/87553/

[2] https://securelist.com/operation-applejeus-sequel/95596/