AppleJeus: Lazarus group hunts cryptocurrency exchanges using macOS malware

Researchers in Kaspersky Lab's Global Research and Analysis Team (GReAT) have discovered AppleJeus – a new malicious operation by the infamous Lazarus group. The attackers penetrated the network of a cryptocurrency exchange in Asia using Trojanized cryptocurrency trading software. The goal of the attack was to steal cryptocurrency from their victims. In addition to Windows-based malware, researchers were able to identify a previously unknown version targeting the macOS platform.
This is the first case where Kaspersky Lab researchers have observed the notorious Lazarus group distributing malware that targets macOS users, and it represents a wakeup call for everyone who uses this OS for cryptocurrency-related activity.

Based on the analysis by GReAT, the penetration of the stock exchange's infrastructure began when an unsuspecting company employee downloaded a third-party application from the legitimate looking website of a company that develops software for cryptocurrency trading.

The application's code is not suspicious, with the exception of one component – an updater. In legitimate software such components are used to download new versions of programs. In the case of AppleJeus, it acts like a reconnaissance module: first it collects basic information about the computer it has been installed on, then it sends this information back to the command and control server and, if the attackers decide that the computer is worth attacking, the malicious code comes back in the form of a software update. The malicious update installs a Trojan known as Fallchill, an old tool that the Lazarus group has recently switched back to. This fact provided the researchers with a base for attribution. Upon installation, the Fallchill Trojan provides the attackers with almost unlimited access to the attacked computer, allowing them to steal valuable financial information or to deploy additional tools for that purpose.

The situation was exacerbated by the fact that the criminals have developed software for both the Windows and macOS platform. The latter is generally far less exposed to cyberthreats than Windows. The functionality of both platform versions of the malware is exactly the same.

Another unusual thing about the AppleJeus operation is that while it looks like a supply-chain attack, in reality this may not be the case. The vendor of the cryptocurrency trading software that was used to deliver the malicious payload to the victims' computers has a valid digital certificate for signing its software and legitimate looking registration records for the domain. However – at least based on publicly available information – Kaspersky Lab researchers could not identify any legitimate organization located at the address used in the certificate's information.

"We noticed a growing interest of the Lazarus Group in cryptocurrency markets at the beginning of 2017, when Monero mining software was installed on one of their servers by a Lazarus operator. Since then, they have been spotted several times targeting cryptocurrency exchanges alongside regular financial organizations. 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. For macOS users this case is a wakeup call, especially if they use their Macs to perform operations with cryptocurrencies," notes Vitaly Kamluk, Head of GReAT APAC team at Kaspersky Lab.

The Lazarus group, known for its sophisticated operations and links to North Korea is noted not only for its cyberespionage and cybersabotage attacks, but also for financially motivated attacks. A number of researchers, including at Kaspersky Lab, have previously reported on this group targeting banks and other large financial enterprises.

In order to protect yourself and your company from sophisticated cyberattacks from groups like Lazarus, Kaspersky Lab security experts advise the following:

• Do not automatically trust the code running on your systems. Neither an authentic looking website, nor a solid company profile, nor digital certificates guarantee the absence of backdoors.
• Use a robust security solution, equipped with malicious-behavior detection technologies that enable even previously unknown threats to be caught.
• Subscribe your organization's security team to a high quality threat intelligence reporting service in order to get early access to information on the most recent developments in the tactics, techniques and procedures of sophisticated threat actors.
• Use multi-factor authentication and hardware wallets if you are dealing with significant financial transactions. For this purpose, preferably use a standalone, isolated computer that you do not use to browse the internet or read email.

Read the full version of the report on https://securelist.com/operation-applejeus/87553/