Lazarus enhances capabilities in AppleJeus cryptocurrency attack, Kaspersky reveals

In 2018 Kaspersky's Global Research and Analysis Team (GReAT) published findings on AppleJeus – an operation aimed at stealing cryptocurrency carried out by prolific threat actor the Lazarus group. Now, new findings show that the operation continues with more careful steps from the infamous threat actor, improved tactics and procedures and the use of Telegram as one of its new attack vectors. Victims in the UK, Poland, Russia and China, including several connected to cryptocurrency business entities, were affected during the operation.

The Lazarus group is one of the most active and prolific advanced persistent threat (APT) actors, which carried out a number of campaigns targeting cryptocurrency-related organizations. During its initial 2018 AppleJeus operation, the threat actor created a fake cryptocurrency company in order to deliver their manipulated application and exploit a high level of trust among potential victims. This operation was marked by Lazarus building its first macOS malware. The application was downloaded by users from third-party websites and the malicious payload was delivered via what was disguised as a regular application update. The payload enabled the attacker to gain full control of the users' device and steal cryptocurrency.
Kaspersky researchers identified significant changes to the group's attack tactics in the 'sequel' operation. The attack vector in the 2019 attack mimicked the one from the previous year, but with some improvements. This time, Lazarus created fake cryptocurrency-related websites, which hosted links to fake organization Telegram channels and delivered malware via the messenger.

Just as in the initial AppleJeus operation, the attack consisted of two phases. Users would first download an application, and the associated downloader would fetch the next payload from a remote server, finally enabling the attacker to fully control the infected device with a permanent backdoor. However, this time the payload was delivered carefully in order to evade detection by behavior-based detection solutions. In attacks against macOS-based targets an authentication mechanism was added to the macOS downloader and the development framework was changed, in addition, a file-less infection technique was adopted this time. When targeting Windows users, the attackers avoided the use of Fallchill malware (which was employed in the first AppleJeus operation) and created a malware that only ran on specific systems after checking them against a set of given values. These changes demonstrate that the threat actor has become more careful in their attacks,

employing new methods to avoid being detected.

Lazarus also made significant modifications in the macOS malware and expanded the number of versions. Unlike in the previous attack, during which Lazarus used open source QtBitcoinTrader to build a crafted macOS installer, during the AppleJeus Sequel the threat actor started to use their homemade code to build a malicious installer. These developments signify that the threat actor will continue to create modifications of the macOS malware and our most recent detection was an intermediate result of these changes.

“The sequel AppleJeus operation demonstrates that despite significant stagnation in the cryptocurrency markets, Lazarus continues to invest in cryptocurrency-related attacks, making them more sophisticated. Further changes and diversification of their malware demonstrates that there is no reason to believe that these attacks will not grow in numbers and become a more serious threat,” – comments Seongsu Park, Kaspersky security researcher.

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

To protect from this and similar attacks, we recommend crypto businesses apply the following measures:
• Introduce basic security awareness training for all employees so that they can better distinguish phishing attempts
• Conduct an application security assessment. It may help you to showcase your reliability to potential investors
• Monitor for emerging vulnerabilities in smart contract execution environments

For consumers already exploring cryptocurrencies, or planning to, Kaspersky recommends the following advice:

• Only use reliable and proven cryptocurrency platforms
• Do not click on links that lure you to an online bank or a web wallet
• Use a reliable security solution for comprehensive protection from a wide range of threats such as Kaspersky Security Cloud

Read more about the AppleJeus Sequel on https://securelist.com/operation-applejeus-sequel/95596/