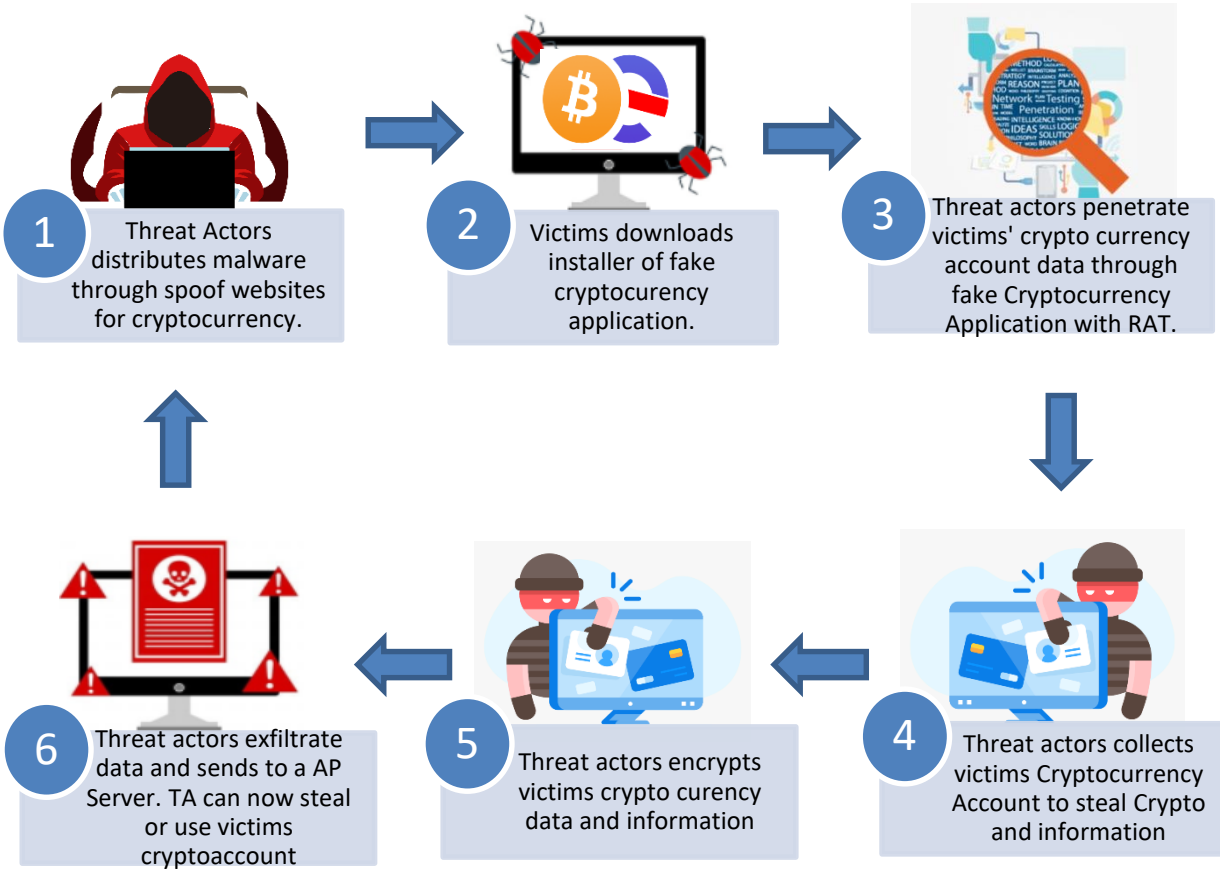
Applejeus Malware
(CSB21-06)
May 14, 2021

Applejeus malware, initially discovered in 2018, is a variant used by the North Korean government-sponsored cyber threat actor HIDDEN COBRA, also known as Lazarus Group. The said group target individuals and companies, including cryptocurrency exchanges and financial service companies and has targeted organizations for cryptocurrency theft in over 30 countries during 2020 alone.

Applejeus malware threat actors used fake websites disguised as legitimate cryptocurrency trading platform to spread the malware. Seen on both Windows and Linux operating systems, Applejeus malware trick individuals into downloading said malware infecting their computer and network. HIDDEN COBRA actors also use additional initial infection vectors, such as phishing, social networking, and social engineering techniques to lure users into downloading the malware.

HOW IT WORKS



IMPACT

- Interfere with the normal functions of the computer system or prevent its utilization.
- Give threat actor control of the system and resources available.
- Maybe used to gather personal information or data from infected computer.
- May spread throughout the network infecting other computer.

MITIGATIONS

- Remove infected computer within the network.
- Coordinate with IT Project Officer assigned in your office/unit.
- Perform a full system scan in safe mode to remove any infections.
- Change all passwords to any accounts associated from the infected computer.

PREVENTION

- Install anti-malware and anti-virus software.
- Don't click on suspicious links or download attachments from unknown sources.
- Keep computer and application software up to date.
- Back up data regularly.
- Regularly perform security scan.
- Ensure all software and hardware is up to date, and all patches have been installed.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa21-048a
- https://support.google.com/google-ads/answer/2375413?hl=en