EINPRESSWIRE

ANY.RUN Exposes the Use of Brute Ratel C4 for Loading Latrodectus Malware

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 24, 2024 /EINPresswire.com/ -- ANY.RUN, a leader in cybersecurity solutions, has published a detailed analysis on the use of the Brute Ratel C4 (BRC4) framework to deploy the recently discovered Latrodectus malware loader.

□□□□□□ □□□□□□ □□ □□ □□□□□□□□□□□□□□□
Brute Ratel C4, first introduced in December 2020, is a commercial Command and Control (C2) framework designed for adversarial attack simulations, red-team engagements, and penetration testing. It stands out from other C2 frameworks due to its ability to bypass and avoid EDR solutions.

□□□ □□□□□□□□□□□□ □□□□□□□□ □□□□□□□□□□□
Latrodectus, believed to be the successor of the notorious ICEDID malware, has been linked to the same threat actor group. This new loader is used in multi-stage attacks, typically initiated through phishing emails containing malicious JavaScript or PDF files.

□□-□□□□□ □□□□□□□□□ □□ □□□□□□□□□□□□ □□ □□□.□□□
ANY.RUN's guest expert, Mohamed Talaat, conducted comprehensive research on a complex multi-stage attack involving the Brute Ratel C2 framework and the Latrodectus malware.

The team started by analyzing a malicious MSI file. Using reverse engineering, they uncovered how the badger loaded the Latrodectus loader into memory. Key steps included identifying a hidden DLL, decrypting a payload, and tracing advanced evasion techniques.

□□□□□□□□□□□□ □□□ □□□□□□□□□□□□□ □□□□□□□□□□□□□
The analysis reveals all the steps in how the Brute Ratel C4 framework's badger component was employed to deploy the Latrodectus malware loader into the victim's system.

Learn more details about the research on ANY.RUN’s blog.

□□□□□ □□□.□□□
ANY.RUN offers a suite of cybersecurity products, including an interactive sandbox and a Threat Intelligence portal. Trusted by over 400,000 professionals globally, the sandbox provides an efficient and user-friendly platform for analyzing malware targeting both Windows and Linux systems. In addition, ANY.RUN's Threat Intelligence services, comprising Lookup, Feeds, and YARA Search, allow users to gather critical information about threats and respond to incidents with enhanced speed and accuracy.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/730099027