EINPRESSWIRE

ANY.RUN Analyze New Node.js Malware with Unprecedented Capabilities

DUBAI, UNITED ARAB EMIRATES, September 27, 2023 / EINPresswire.com/ -- Researchers at ANY.RUN, an interactive sandbox for malware analysis, have discovered and analyzed a new Node.js malware called Lu0Bot.

□□□□□□ □□□□□□□

Lu0Bot is more versatile and difficult to detect than most malware families because it targets a platform-agnostic runtime environment commonly used in modern web applications and employs multi-layer JavaScript obfuscation, combining traditional malware traits with web technologies.

While its activity level is currently low, Lu0Bot may be more prevalent than it seems, with many dormant samples awaiting commands from the command-and-control servers.

□□□ □□□ □□□□□□□□

Lu0Bot is capable of stealing personal information, such as passwords and credit card numbers, and taking over control of the victim's computer. It can also be used to launch DDoS attacks. However, due to the programming language in which it is written, the range of its capabilities can be expanded significantly.

□□□□□□□□ □□□□□□□

ANY.RUN’s investigation into the malware’s code revealed that:

- Lu0Bot uses a Node.js interpreter that accepts encrypted JS code as input.
- It fetches system data using WMIC, including information about processes and the execution location.
- The malware's domain is constructed from various parts, assembled into a single entity within the JS code.
- The malware copies itself to the startup folder to ensure that it remains operational after the system restarts.
- Lu0Bot's code starts with an array of encrypted strings, which are then manipulated and decrypted using a custom function that employs an alternative form of BASE64, URL encode-decode, and RC4.

Read the article to see how the ANY.RUN team successfully extracted the configuration of Lu0Bot and presented YARA, Sigma, and Suricata rules along with a comprehensive list of IOCs, which are essential for prompt detection of the malware.

Vlada Belousova
ANYRUN FZCO
2027889264
email us here
Visit us on social media:
Twitter
YouTube