EINPRESSWIRE

New Redline Stealer Variant Employs Lua Bytecode and Propagates via GitHub

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 2, 2024 /EINPresswire.com/ -- A new Redline Stealer variant was discovered in the wild. This version uses Lua bytecode to hide its malicious code and propagates through Microsoft's official vcpkg repository on GitHub. Executing a sample in ANY.RUN sandbox confirms this behavior.

Lua bytecode makes it harder for security software to detect the malware, as Lua is a less common programming language, and many security tools may not be equipped to properly analyze it.

The attackers uploaded a malicious zip file named □□□□□.□□□.□.□.□.□□□ to the repository, containing an MSI installer with two executable files and a text file holding the Lua bytecode.

Analysis of the Lua bytecode is challenging due to obfuscation and the use of Lua's foreign function interface to call Windows API functions directly, further complicating detection efforts.

The malware uses GitHub to distribute the malicious package. Recently, ANY.RUN highlighted a phishing campaign using GitHub to distribute STRAAT and VCURMS. In both cases, the commercial protection of the platform makes it difficult to detect the malicious nature of the files. These are two isolated instances of GitHub being used to distribute malware.

Redline Stealer remains a widespread malware, ranking as the 5th most frequently detected family in ANY.RUN's Q1 Malware Trends report.

To protect against this threat, users are advised to exercise caution when downloading files, even from trusted sources like GitHub. Suspicious files can be analyzed using a sandbox such as ANY.RUN, which detects and highlights malicious activity using YARA and Suricata rules, as well as signatures.

For more information on the new Redline Stealer variant, visit the post in ANY.RUN blog.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
Twitter
YouTube