New Variant of RisePro Malware: Enhanced Communication Protocol and Remote Access Capabilities

DUBAI, UNITED ARAB EMIRATES, November 28, 2023 / EINPresswire.com/ -- Researchers at ANY.RUN, a leading malware sandbox provider, have analyzed a new variant of the RisePro malware that features a significantly overhauled communication protocol and remote access capabilities. The malware, which has two versions written in C# and C++, has been observed targeting victims worldwide.

□□□ □□□□□□□□□

• The new variant employs a custom protocol over TCP for communication, marking a departure from the previous HTTP-based method.

• The malware has expanded data exfiltration capabilities, now stealing passwords, browsing history, and sensitive documents from a broader range of applications.

• The malware collects information about the user's IP address, locale, system details, and other computer specifications.

• The malware exfiltrates stolen data in a .zip archive named with the country code, IP address, and .zip extension.

□□□ □□□ □□ □□□□

The malware optionally deploys remote control functionality via Hidden Virtual Network Computing (HVNC), allowing attackers to take complete control of infected systems.

□□□□□□□□□□ □□ □□□ □□□ □□□□□□□□ □□□□□□□□

The analysis results enabled the team to update the detection capabilities of the ANY.RUN sandbox to identify any malicious files or links related to RisePro attacks.

Learn more in ANY.RUN’s blog

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