Researcher Exposes XWorm Malware’s C2 Communication

DUBAI, UNITED ARAB EMIRATES, November 27, 2023 / EINPresswire.com/ -- ANY.RUN, a leading malware analysis sandbox provider, has published a research article by Igal Lytzki (0xToxin on Twitter) in its blog, detailing the inner workings of the XWorm malware, a Remote Access Trojan (RAT) targeting Windows systems. The analysis delves into the communication between the XWorm server and infected clients, revealing the malware's data theft and remote-control capabilities.

□□□□□□□□□□ □□□□□'□ □□□□□□□ □□□□□□□□□□□□□

The research found that XWorm uses AES-ECB encryption to communicate with its command-and-control (C2) server.

By decrypting this data, Lytzki was able to analyze the information exchanged between the malware and its server. This revealed that the malware collects sensitive information such as username, machine name, OS version, webcam presence, CPU and GPU details, installed antivirus software, and more.

□□□□□□□□□□ □□□□□'□ □□□□□□ □□□□□□□ □□□□□□□□

The researcher also discovered two plugins that can be activated through remote control of infected systems:

• Info stealer plugin: This plugin steals sensitive data, including credit card information, Chromium cookies, Discord tokens, FileZilla credentials, browser data, browser history, WiFi

passwords, MetaMask data, and Telegram data.

• Commands plugin: This plugin enables attackers to execute various malicious actions, such as disabling or terminating Windows Defender, excluding paths from Windows Defender scans, installing the .NET framework, and blanking the screen.

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

The information gathered during the research has been integrated into the ANY.RUN sandbox, improving its detection capabilities.

Learn more in ANY.RUN's blog.

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