ANY.RUN Releases A List of Top Malware Trends in November 2023

DUBAI, DUBAI, UNITED ARAB EMIRATES, November 30, 2023 /EINPresswire.com/ -- ANY.RUN, a leading provider of an interactive malware analysis sandbox, released its latest findings on the evolving threat landscape. The platform, trusted by top security teams worldwide, sees over 14,000 sample submissions daily from its community, providing a vast repository of malware data for identifying emerging trends.

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

ANY.RUN identified a new phishing campaign utilizing steganography, a technique that embeds data within other files, particularly, images.

As part of one of the attacks exposed by the company's team, malicious code hidden inside an image downloaded and executed additional malware, giving attackers remote access to the victim's computer.

This marks a resurgence of steganography, which had been less commonly used due to its complexity.

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

ANY.RUN analyzed the Tycoon platform, a 2FA – Adversary-in-the-Middle (AiTM) and Phishing-as-a-Service (PhaaS) platform and discovered that it uses WebSockets to communicate with victims. This allows the platform to maintain a persistent connection with compromised devices.

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

ANY.RUN observed a growing trend of attackers misusing legitimate services, such as InterPlanetary File System (IPFS), Google Translate, and page jump anchor techniques, to spread phishing scams. This tactic makes it more difficult for security solutions to detect phishing attempts.

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

ANY.RUN highlighted the case of a student who developed an academic proof-of-concept ransomware called MauriCrypt. Unfortunately, this research was exploited by malicious actors who used the code to create a real-world ransomware threat known as CryptGh0st.

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

ANY.RUN re-examined socks5systemz, a malware first spotted three years ago. The malware turns victims' devices into proxies for forwarding traffic, potentially enabling malicious activity.

Learn more about ANY.RUN's research in the company's blog.

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