Malware Analysis Digest from ANY.RUN: March 2023

DUBAI, UAE, April 6, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the March 2023 edition of the Malware Analysis Digest. Here are some highlights from the Malware Analysis Digest:

Emotet Malware Targets US Taxpayers with Fake W-9 Forms

Once installed, Emotet steals victims' emails for future reply-chain attacks, sends spam emails, and installs other malware that grants initial access to threat actors, such as ransomware gangs.

Outlook Vulnerability (CVE-2023-23397) and Mitigation Steps

This vulnerability enables threat actors to steal user account credentials, including the NTLM hash value, upon receiving an email and triggering a notification. Attackers can exploit this information for internal propagation and further system compromise.

New IcedID Variants Focus on Malware Delivery Instead of Bank Fraud

Recent IcedID malware variants have shifted focus from online banking fraud to installing further malware on compromised systems. Proofpoint predicts the use of new IcedID variants will likely grow, with more variants possibly emerging later in 2023.

CatB: a new Ransomware Strain Discovered

CatB searches for user-specific files to encrypt, but unlike other ransomware families, it prepends the ransom note to each encrypted file instead of dropping it in separate files in various locations. The malware uses anti-VM techniques to hide its behavior from analysis environments, making it more challenging for security researchers to study its operations.

Kimsuky Group Distributes Malware via Fake Profile Template on GitHub

A malicious Word file distributed by the Kimsuky Group, disguised as a profile template was found in the wild. The malware collects information saved on browsers, similar to the one found in a previously discovered Malicious Word Document.

New ‘HinataBot’ Botnet Could Launch Massive 3.3 Tbps DDoS Attacks

A new botnet named HinataBot has been discovered targeting Realtek SDK, Huawei routers, and Hadoop YARN servers to recruit devices for massive DDoS (distributed denial of service) attacks.

At ANY.RUN we understand the importance of cybersecurity in today's digital landscape. Our team of experts is dedicated to providing cutting-edge cybersecurity solutions to help organizations stay protected against evolving threats.

Read our article for more information on the most significant security events and emerging threats.

Vlada Belousova
ANYRUN FZCO
v.belousova@any.run
Visit us on social media:
Twitter
YouTube
