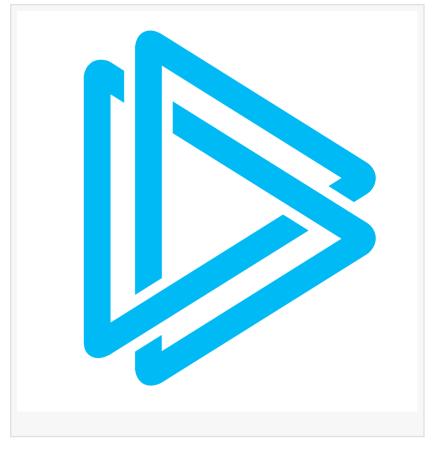


ANY.RUN Shares Analysis of AsyncRAT's Infection Tactics via Open Directories

DUBAI, DUBAI, UNITED ARAB EMIRATES, November 7, 2024 /EINPresswire.com/ -- ANY.RUN, a leader in interactive malware analysis and threat intelligence, has released a technical analysis of new techniques used in multi-stage attacks involving AsyncRAT. The report details how attackers exploit open directories to distribute AsyncRAT, examines the infection mechanisms, and offers indicators of compromise (IOCs) for identifying and mitigating this persistent threat.

Known for its ability to grant remote access to threat actors, AsyncRAT has been one of the most pervasive



Remote Access Trojans (RATs) since its launch in 2019. The malware has been observed to engage in data theft, stealing sensitive information of victims, as well as delivery of other malicious programs on to the compromised systems.

The AsyncRAT attacks presented in the report leverage open directories exposed to the internet to initiate the infection process. The attacks involve a series of obfuscated scripts and disguised files designed to evade detection and ensure the persistence of the malware on the infected system.

· Attacks start with malicious VBS and PowerShell scripts that are disguised as text and JPG files and hosted on open directories controlled by threat actors. The scripts are then used to facilitate the infection process.

- · To ensure persistence on the infected system, the attackers employ scheduled tasks that run every two minutes.
- The final stage of the attacks involves executing the main payload, which includes malicious DLL and EXE files (AsyncRAT). These files establish communication with the attacker's Command and Control (C2) server.

The report also provides security professionals with actionable IOCs to safeguard their environments against AsyncRAT. The full analysis is available on <u>ANY.RUN's blog</u>.

00000 000.000

ANY.RUN serves over 500,000 cybersecurity professionals globally, offering an interactive platform for malware analysis targeting Windows and Linux environments. With advanced threat intelligence tools such as TI Lookup, YARA Search, and Feeds, ANY.RUN enhances incident response and provides analysts with essential data to counter cyber threats effectively.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X

This press release can be viewed online at: https://www.einpresswire.com/article/758566147

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.