ANY.RUN Simplifies Analysis of Malicious PowerShell Scripts

DUBAI, DUBAI, UNITED ARAB EMIRATES, April 18, 2024 /EINPresswire.com/ -- [ANY.RUN](#), the leading provider of an interactive malware analysis sandbox, now lets users analyze PowerShell scripts, a common component in many malware attacks.

⬜⬜⬜ ⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜ ⬜⬜ ⬜⬜⬜⬜ ⬜⬜ ⬜⬜⬜⬜⬜ ⬜⬜⬜⬜⬜⬜⬜

PowerShell is a versatile command-line shell and scripting language employed by system administrators. Its flexibility has made it a favorite among many threat actors.

Attackers use PowerShell scripts to:

⬜ Download and execute malicious binaries
⬜ Bypass antivirus software
⬜ Execute malicious scripts
⬜ Collect and exfiltrate system data
⬜ Remotely control infected systems

⬜⬜⬜ ⬜⬜⬜.⬜⬜⬜ ⬜⬜⬜⬜⬜ ⬜⬜⬜⬜⬜⬜⬜⬜⬜ ⬜⬜⬜⬜⬜⬜⬜⬜⬜⬜ ⬜⬜⬜⬜⬜⬜⬜ ⬜⬜⬜⬜⬜⬜

ANY.RUN's Script Tracer tool now provides a detailed breakdown of every function in a PowerShell script, showing the entry point, parameters, and exit point.

It also connects related functions' inputs and outputs, making it easier to trace the flow of data through a script.

The tool automatically detects PowerShell scripts and provides an easy-to-use detail view for

inspecting specific parameter data in binary, hexadecimal, and plaintext formats.

Key features of ANY.RUN's PowerShell Tracer tool:

 Automatic detection of PowerShell scripts
 Detailed breakdown of every function
 Connection of related functions' inputs and outputs
 Easy-to-use interface for inspecting specific parameter data
Learn more and see an example of a malicious PowerShell script analysis on [ANY.RUN's blog](#).

 .
ANY.RUN facilitates the analysis of threats targeting both Windows and Linux systems, providing analysts with an advanced tool for investigations. The service detects malware in under 40 seconds, identifies prevalent malware families using YARA and Suricata rules, and uses behavioral signatures to track malicious actions when you encounter a new threat.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
Twitter
YouTube