EINPRESSWIRE

Cybersecurity Firm ANY.RUN Releases Free Win10 VM, Suricata Search, and Other Features

DUBAI, UNITED ARAB EMIRATES, August 1, 2024 /EINPresswire.com/ -- ANY.RUN, a provider of an interactive sandbox for malware analysis and threat intelligence products, has shared its monthly updates. The new features include Suricata search, free Windows 10 VM for malware analysis, and expanded YARA and Suricata detection.

□□□□ □□□□ □□□□□□□
□□□□□□□□□□□□□□

Threat Intelligence Lookup is ANY.RUN’s searchable database of the latest threat data. It now lets users access indicators of compromise (IOCs) extracted directly from malware configurations.

These IOCs are one of the most reliable means to identify attackers' infrastructure.

Users can easily gather these indicators to enrich their investigations and detection systems to block harmful activity.

□□□□□□□□ □□□□□□

Suricata IDS is a system for detecting cyber threats' network activity. It runs on rules that contain unique details about specific threats.

Thanks to TI Lookup’s Suricata search feature, users can now find specific network threats using Suricata rule-related information.

These include parameters like SuricataClass, SuricataMessage, SuricataThreatLevel, and SuricataID. All the results are available via a special Network threats tab, making it easy to identify potential network risks.

□□□□□□□ □□ □□□ □□□□ □□□□□

ANY.RUN made Windows 10 VM available in its free Community plan.

Now more users will have access to a modern OS environment for studying and analyzing the latest malware and phishing threats.

□□□□□□□□ □□□□□□ □□□□□□□□□

ANY.RUN sandbox also updated its database of YARA and Suricata rules to cover new types of malware families: Luka and Medusa ransomware, XMRig, Grandoreiro, Metasploit, and others.

The sandbox also introduced detection of malicious use of Windows Management Instrumentation (WMI), PowerShell, and certain WinAPI calls.

See a detailed review of all July updates — visit ANY.RUN’s blog.

□□□□□ □□□.□□□

ANY.RUN is a leading provider of interactive sandbox and threat intelligence services, helping over 400,000 cybersecurity professionals worldwide. ANY.RUN’s sandbox simplifies malware analysis of threats targeting both Windows and Linux systems, while threat intelligence products: including TI Lookup, Yara Search, and Feeds, help professionals find relevant information on active threats.

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/732208424

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.