ANY.RUN monthly updates: New Config Extractors, Suricata Rules, and More

DUBAI, UNITED ARAB EMIRATES, August 31, 2023 /EINPresswire.com/ -- ANY.RUN, a cloud interactive sandbox for malware analysis, has released a Monthly Updates: New Config Extractors, Suricata Rules, and More.

□□□□□□□□ □□□□□□□□

New detection logic for IP, URL, Domain. The overhauled logic enables more robust detection of malicious IPs, URLs, and domains.

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

ANY.RUN's added support for several new malware and improved detection capabilities for families that were already supported: Lu0Bot support, Strela extractor and new YARA rules, RaccoonClipper extractor and new YARA rules, Fixed extractor and rules for LummaStealer.

□□□□□□□□□□□ □□□□□□□□

• Added a rule to detect KrakenStealer
• Updated extractor and YARA for GO LaplasClipper variations
• Updated RaccoonStealer extractor and YARA
• Updated extractor and YARA for StealC
• Updated Remcos extractor and YARA
• Separated tags between StormKitty and AsyncRAT
• Added support for extracting configuration from new XWorm types.

□□□□□□□□ □□□□□□

In August, ANY.RUN focused on network rules heavily, writing 120 new Suricata rules.

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

This month, ANY.RUN continued submitting rules to the Emerging Threats community:

• Parallax RAT now detectable
• Mekotio rules boosted
• New rule for DarkCloud stealer.

The ANY.RUN team works hard to keep up with emerging threats.

Read more with examples in the article at ANY.RUN.

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