ANY.RUN Unveils Automated Interactivity and Updated YARA Rules

DUBAI, UNITED ARAB EMIRATES, December 28, 2023 / EINPresswire.com/ -- ANY.RUN, a cloud-based malware analysis sandbox, today announced the release of new features and updates for December 2023. The most notable addition is Automated Interactivity (AI), which employs machine learning to automate repetitive tasks and enhance malware analysis operations.

□□□ □□□□□□□□□

□□□□□□□□□□ □□□□□□□□□□□□□□□ (□□)
ANY.RUN's new AI capability mimics human actions during malware analysis. It automatically navigates through setup forms, CAPTCHAs, installation windows, and other scenarios requiring human intervention, allowing users to reduce their involvement in the analysis process. The feature is enabled by default for API tasks and can be turned on or off for web-based tasks.

□□□□□□□□□ □□□□□□□□□ □□□□□□
ANY.RUN's Suricata rules have been expanded, providing users with more granular information when a detection occurs. This includes identifying the affected traffic segment, detailing the relevant fields, and often viewing the rule itself within the interface.

This enhanced transparency allows users to better understand each detection and apply the rules in their own incident investigations.

□□□ □□□□□ □□□□□□

ANY.RUN has added new signatures to detect various activities within the task. These rules cover the following malware families:

- W4SP Stealer
- Klippr
- OriginBotnet
- DarkGate
- IcedId

□□□ □□□□□□□□□ □□□□□□ □□□□ □□□□□□□□

In addition to the new YARA rules, ANY.RUN has also added multiple new Suricata signatures. Here's a breakdown of the additions:

- Stealers: Detection for AxileStealer, an updated version of Vidar, and AlbumStealer.
- Backdoors: Detection for Gh0stRat's encrypted DLL, which can be hidden within JPEG files.
- Loaders: Updated signature for DarkGate, which altered its activities following ANY.RUN's Twitter post on its new techniques. Additionally, signatures for Pikabot and QakBot have been added.
- Proxy: Detection for GoProxy.
- Ransomware: Detection for DirCrypt.

Learn more details in ANY.RUN's blog post.

Veronika Trifonova
ANYRUN FZCO
+1 2027889264
email us here
Visit us on social media:
Twitter
YouTube
