ANY.RUN Discovers STRRAT and VCURMS Trojans on GitHub and AWS Servers

DUBAI, DUBAI, UNITED ARAB EMIRATES, March 26, 2024 /EINPresswire.com/ -- ANY.RUN, a cloud-based malware sandbox, discovers a new phishing campaign that deploys STRRAT and VCURMS Remote Access Trojans through a malicious Java-based downloader. A unique aspect of this campaign is the storage of malware files on AWS and Github platforms, utilizing commercial protection to obscure their malicious nature — and researchers can observe this behaviour in ANY.RUN interactive malware sandbox.

STRRAT, a Java-based RAT, acts as a keylogger primarily targeting browser and application credentials. Meanwhile, VCURMS, potentially linked to the Rude Stealer malware, extracts system data and credentials from various applications including Discord and Steam, and has the capability to upload additional modules for enhanced information theft.

The attack chain starts with phishing emails, where hackers urge recipients to verify payment information in a maldoc. Victims unwittingly download a malicious JAR file masked as a payment invoice. This JAR file further deploys the VCURMS and STRRAT trojans, initiating a potentially devastating breach.

Cybersecurity professionals can find samples of this campaing in ANY.RUN's Threat Intelligence Lookup portal, using the following query: 'RuleName:"strrat" AND DomainName:"github.com"'. Then, analysts can analyze samples of the campaign, confirm reported behavior, and extract IOCs and malware configurations from memory in ANY.RUN sandbox.

More information and examples in ANY.RUN's article.

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