EINPRESSWIRE

ANY.RUN Publishes In-Depth Technical Analysis of GorillaBot, a Mirai-Based Botnet Targeting Over 100 Countries

DUBAI, DUBAI, UNITED ARAB EMIRATES, March 25, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has published a comprehensive technical breakdown of GorillaBot, a newly discovered botnet based on the infamous Mirai source code. The botnet has already launched over 300,000 attacks globally and is actively targeting sectors including telecommunications, finance, and education.

□ □□□ □□□□ □□ □□ □□□ □□□□□□

GorillaBot reuses significant portions of Mirai's original code but introduces its own enhancements, including custom encryption schemes, raw TCP communication, and advanced anti-analysis techniques.

It stands out for its ability to evade detection in containerized environments and honeypots, making it a more elusive threat than its predecessors.

□□□ □□□□□□□□□ □□□□ □□□ □□□□□□□□

· □□□□□ □□ □□□□□ □□□□: GorillaBot heavily reuses core logic from Mirai while introducing its own improvements.

· □□□□□□□□ □□ □□□□□□□□□□□□□: Utilizes raw TCP sockets and a custom XTEA-like cipher for encrypting server addresses and communication.

· □□□□□□□□□□□□□□ □□□□□□□□□: Combines a decrypted hardcoded array and a server-provided magic value, then hashes it with SHA-256 for authentication.

· □□□□□□□ □□□□□□□□□□: Performs environment checks to avoid honeypots and Kubernetes containers, exiting immediately if detected.

· □□□□-□□□□□□□□□ □□□□□□□□: Uses TracerPid checks and SIGTRAP handling to avoid analysis tools.

· □□□□□□□□□□□ □□□□□□□: Encrypts internal configuration using a Caesar cipher and a custom block cipher.

To explore the full technical breakdown of GorillaBot, including behavior analysis, code insights, and relevant IOCs visit the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN is a cloud-based cybersecurity platform used by over 500,000 professionals worldwide. It offers an interactive malware sandbox along with powerful threat intelligence capabilities, enabling real-time behavioral analysis across Windows, Linux, and Android environments. From dynamic analysis to uncovering IOCs and tracking threat actors, ANY.RUN helps security teams investigate threats faster, collaborate more effectively, and stay ahead of emerging malware.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/796923754