ANY.RUN Researchers Analyze a Rare Gh0stBins Variant: Static Analysis, Protocol Description, RDP Stream Recovery

DUBAI, UAE, June 26, 2023 /EINPresswire.com/ -- ANY.RUN, a cloud interactive sandbox for malware analysis, has released a malware analysis of a rare Gh0stBins variant in their blog.

□ □□□□-□□□□ □□□□ □□□□□□□□□□

Gh0stBins RAT is a little-studied malware family originating from China. At the time of the release, the DLL analysed by ANY.RUN drew 0 detectins on Virus Total.

The new study provides insights into the escalating landscape of Chinese cyber threats, through an examination of a sophisticated modular RAT. Chinese malware frequently gets less attention compared to that emerging from former USSR regions. Yet, cybercriminals from the Middle Kingdom have been markedly enhancing their skills, churning out sophisticated malware with relentless efficiency. In this analysis, researchers from ANY.RUN explore:

• In-depth analysis of the loader, RAT, and RDP module stages: both basic descriptions and protocols

• Analysis of the RAT's network traffic

• How to □□□□□□□□ □ □□□□□□ □□□□□□□ □□□ □□□□□□□ □□□□□ □□□□□□ □ □□□□□□□ □□□□□□□.

This analysis provides insight into the strategies used by adversaries from China. Apart from breaking down the arhitecture and behaviour of the RAT, the article provides:

• Suricata and YARA rules to detect Gh0stBins

• A Phython script to recover the leaked data

• Indicators of Compromise (IOCs) associated with the analyzed sample

Read more with the code and scripts examples in the article at ANY.RUN.

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