Botnet Encyclopedia

guardicore.com/botnet-encyclopedia/

Get in-depth analyses of attack campaigns captured by Guardicore Global Sensors Network (GGSN).
Learn about each botnet's scope, its associated indicators of compromise (IOCs), and the attack flow.

MoneroSsh

MoneroSsh

Read More

911

911

A long-running campaign in which a Mirai-variant named "Sora" is deployed. The malware scans for additional victims over Telnet port 23.

Read More

GhOul

GhOul

This Telnet DDoS campaign is targeting SSH servers and has been active since February 2020.

Read More

PLEASE_READ_ME_VVV

PLEASE_READ_ME_VVV

This campaign, unlike many others, is not a cryptomining botnet. Here, the attackers compromise victim machines using MySQL brute force

Read More

Smominru

Smominru

The Smominru botnet and its variants MyKings and Hexmen managed to infect thousands of MS-SQL machines on a daily basis

Read More

PLEASE_READ_ME

PLEASE_READ_ME

PLEASE_READ_ME_VVV is a mass-scale ransom attack, in which the attackers choose to leave the ransom note within MySQL database tables.

Read More

We strive for cooperation with the cyber threat intelligence community and welcome any contribution, question and suggestion.

Contact Us