RUBYCARP hackers linked to 10-year-old crypto mining botnet

Date: 12th April 2024 | Severity: High

Summary

A Romanian botnet group named 'RUBYCARP' is leveraging known vulnerabilities and performing brute force attacks to breach corporate networks and compromise servers for financial gain. RUBYCARP currently operates a botnet managed via private IRC channels comprising over 600 compromised servers.

RUBYCARP has been observed maintaining a long-running botnet for carrying out crypto mining, distributed denial-of-service (DDoS), and phishing attacks.

The researchers have noted some associations with the Outlaw APT threat group, though the link is loose and based on common tactics used across botnets.

Attack Vectors

- RUBYCARP gains initial access by leveraging public exploits for known vulnerabilities (for example, CVE-2021-3129 in the Laravel Framework) or through SSH brute-force attacks. Once inside the system, the threat actors install ShellBot, and then use the compromised server to launch distributed denial of service (DDoS) attacks and to mine cryptocurrency. To evade detection, RUBYCARP rotates its malicious infrastructure, frequently updating its IP addresses and domains.
- RUBYCARP was also observed sending phishing email messages that impersonate legitimate entities (for example, Swiss Bank, Nets Bank, and Bring Logistics) to steal financial information, such as credit card numbers.
- RUBYCARP uses multiple IRC networks for general communications, but also to manage its botnets and coordinate cryptomining campaigns.
- In one of the logs we acquired, RUBYCARP tends to share the tools it is using, which include many of the tools we have been able to collect through our honeypot, such as: Banner Masscan X (kernel module) Brute
- The most recurring IRC admins we found within the Shellbot configuration files are "juice," "MUIE," and "Smecher," who also each have their own respective channels for malicious operations. "juice" has been the most prolific in setting up new malicious Shellbot configurations, new servers, and new victim channels.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• run.psybnc[.]org • juicessh[.]space • sshd.baselinux[.]net • juice.baselinux[.]net • sshd[.]run • physics.uctm[.]edu • chat.juicessh[.]pro • download.c3bash[.]org
IPs	• 91[.]208.206.118 • 80[.]83.124.150 • 194[.]163.141.243

Recommendation

- Employee Training and Awareness.
- Stay up to date with known vulnerabilities.
- Use strong passwords on all the devices on your network and change them regularly.
- Do not open suspicious email attachments.
- While good access control, risk management, and design will limit the impact of a known vulnerability, it's better to just ensure you have few known vulnerabilities and mitigate them as needed.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.bleepingcomputer.com/news/security/rubycarp-hackers-linked-to-10-year-old-cryptomining-botnet/
- https://sysdig.com/blog/rubycarp-romanian-botnet-group/