Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

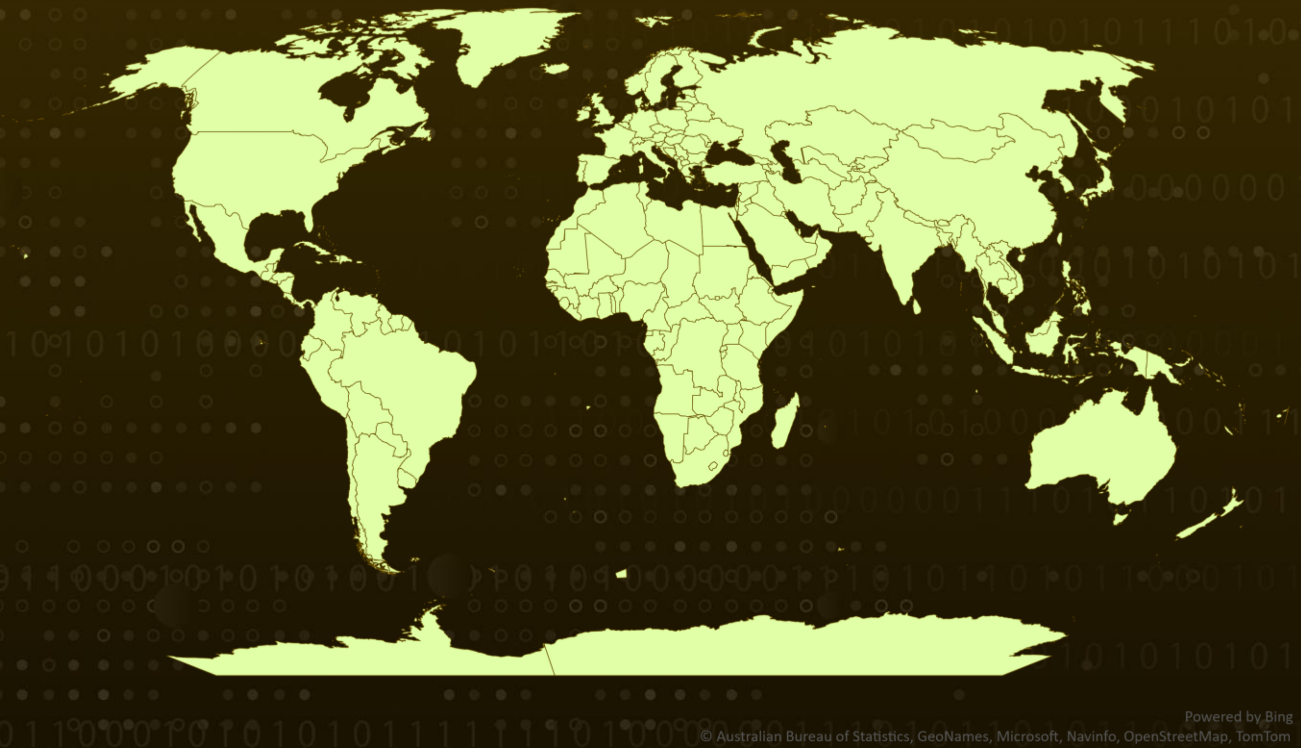
ShellBot Malware Targets Mismanaged Linux Servers

Date of Publication	Admiralty Code	TA Number
March 22, 2023	A1	TA2023152

Summary

First appeared: November 2018
Malware: ShellBot (aka PerlBot, DDoS Perl IrcBot)
Attack Region: Worldwide
Attack: Malicious actors are installing the ShellBot malware on Linux SSH servers that are poorly managed. The ShellBot malware, which is developed using Perl, is known for utilizing the IRC protocol to establish communication with its command and control (C&C) server.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 ShellBot malware strains are presumed to have been deployed after threat actors utilized account credentials obtained via scanners and SSH BruteForce malware on target systems. ShellBot malware is coded in Perl and communicates with command-and-control servers using the Internet Relay Chat (IRC) protocol.

#2 The ShellBot version, “LiGhT's Modded perlbot v2" has multiple features that can be exploited for malicious purposes, including DDoS commands like TCP, UDP, and HTTP Flooding. Additionally, it provides commands for controlling compromised systems, enabling other attacks such as log deletion, reverse shell, and scanner.

Recommendations

Security Leaders
Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5’s Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the ’Potential MITRE ATT&CK TTPs’ & ‘Indicators of Compromise (IoC)’ on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1543 Create or Modify System Process	T1543.002 Systemd Service
T1070 Indicator Removal	T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1082 System Information Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1071 Application Layer Protocol	T1571 Non-Standard Port

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	bef1a9a49e201095da0bb26642f65a78 3eef28005943fee77f48ac6ba633740d 55e5bfa75d72e9b579e59c00eaeb6922 6d2c754760ccd6e078de931f472c0f72 7ca3f23f54e8c027a7e8b517995ae433 2cf90bf5b61d605c116ce4715551b7a3 7bc4c22b0f34ef28b69d83a23a6c88c5 176ebfc431daa903ef83e69934759212
URLs	x-x-x[.]online/ak 193.233.202[.]219/mperl 193.233.202[.]219/niko1 hxxp://34.225.57[.]146/futai/perl 80.94.92[.]241/bash hxxp://185.161.208[.]234/test.jpg hxxp://39.165.53[.]17:8088/iposzz/dred hxxp://80.68.196[.]6/ff
IPV4:PORT	164.90.240[.]68:6667 206.189.139[.]152:6667 176.123.2[.]3:6667 164.132.224[.]207:80 51.195.42[.]59:8080 192.3.141[.]163:6667 49.212.234[.]206:3303

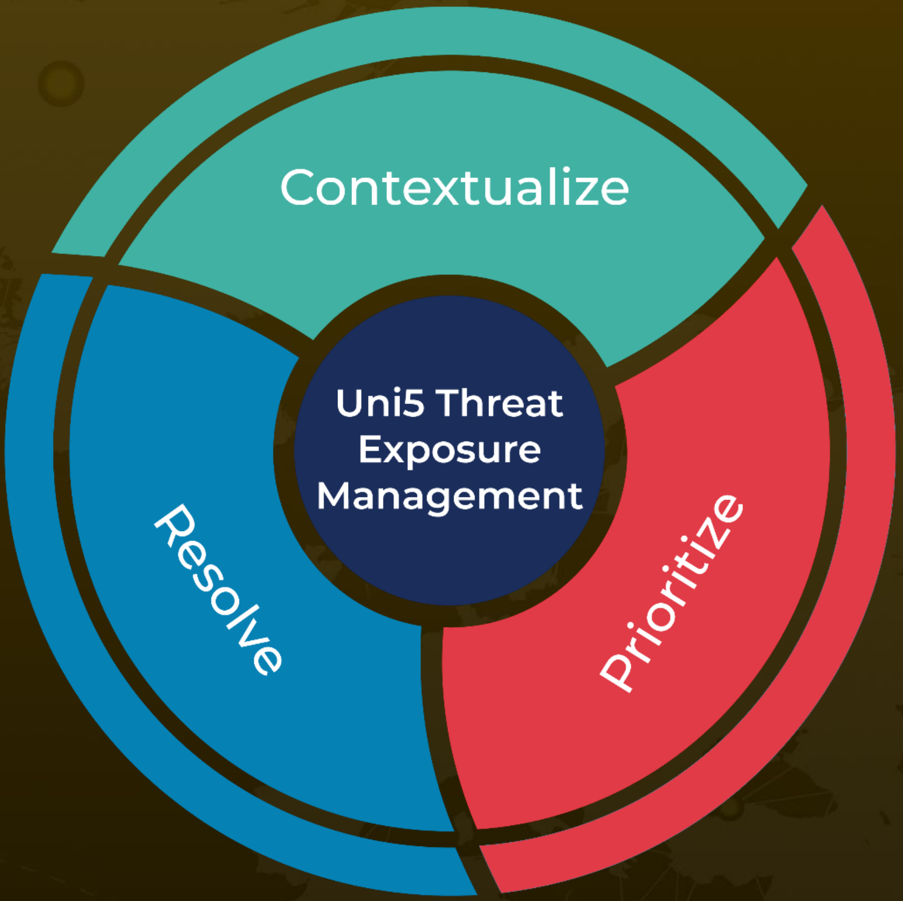
References

https://asec.ahnlab.com/en/49769/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 22, 2023 • 3:03 AM

More at www.hivepro.com