Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

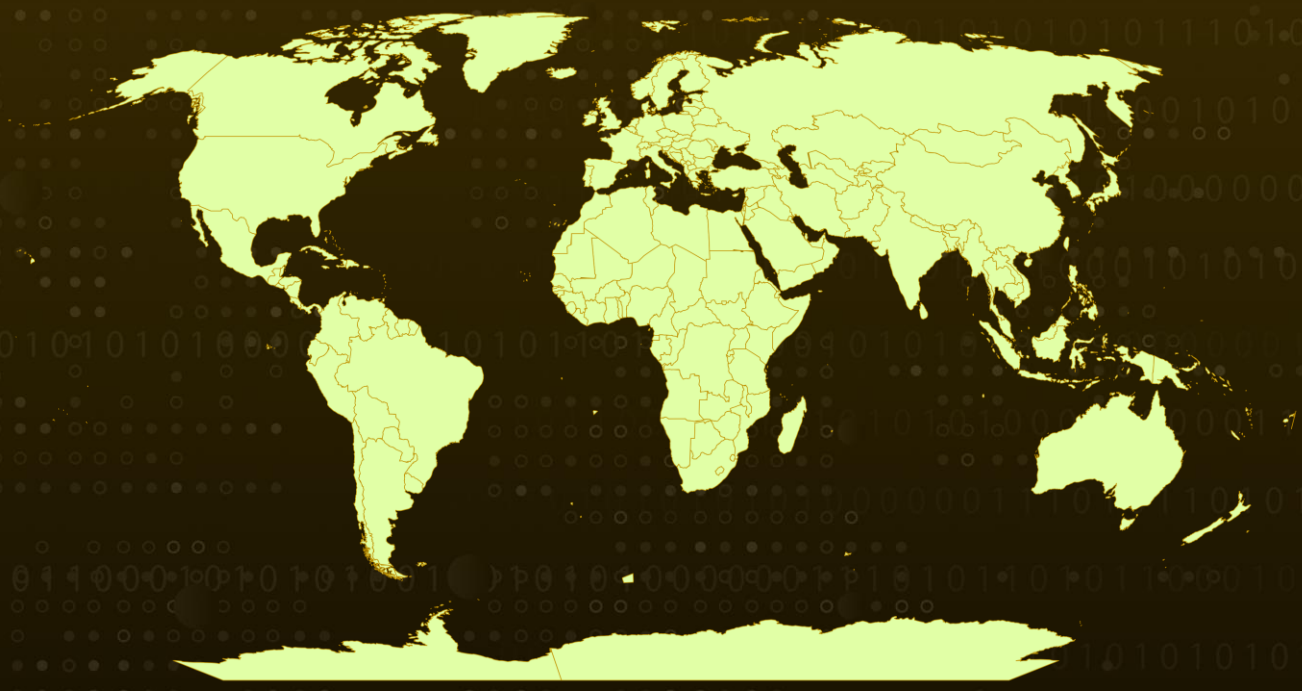
ShellBot Malware Evades Detection Using Hexadecimal IP Addresses

Date of Publication	Admiralty Code	TA Number
October 13, 2023	A1	TA2023414

Summary

First appeared: November 2018
Attack Region: Worldwide
Affected Platform: Linux SSH servers
Malware: ShellBot (aka PerlBot, DDoS Perl IrcBot)
Attack: ShellBot malware, targeting poorly managed Linux SSH servers, now employs hexadecimal IP addresses in its download URLs to evade detection. This change highlights the need for strong security measures and regular updates for administrators to protect against ShellBot attacks on Linux servers.

Attack Regions



Attack Details

#1 ShellBot, also known as PerlBot, is a notorious DDoS Bot malware developed using Perl. It primarily targets Linux systems and is infamous for its use of the IRC protocol to establish communication with its command and control (C&C) server.

#2 ShellBot is notorious for exploiting servers with weak SSH credentials through dictionary attacks, making them susceptible to various malicious activities. These activities include using compromised servers as staging grounds for DDoS attacks and deploying cryptocurrency miners. Notably, one specific variant, "DDoS PBot v2.0," is associated with the consistent use of the name "dred" during the installation of the malware.

#3 Recently, a significant change was observed in the distribution method of the ShellBot malware, which specifically targets poorly managed Linux SSH servers. The threat actor behind ShellBot shifted from using regular IP addresses to hexadecimal values in their download URLs as an evasion tactic to avoid URL detection.

#4 This shift in distribution method is in line with previous instances where threat actors employed various techniques to avoid URL detection, such as using non-standard IP address notations. For instance, a previous case involved a phishing PDF malware that used a decimal IP address notation to evade detection.

#5 ShellBot remains an ongoing and evolving threat, having been in use for an extended period. Its operators continue to adapt and modify the malware to bypass security measures and enhance its capabilities.

Recommendations

Strong Access Controls: Ensure that SSH access to your servers is well-protected. Use strong, complex passwords, or better yet, implement key-based authentication. Limit the number of login attempts to prevent brute force attacks.

Regular Password Updates: Encourage regular password updates for all users. Stale or unchanged passwords can become vulnerable points of entry for attackers.

Software and System Updates: Keep your server's software, including the operating system and all applications, up-to-date with the latest security patches. Vulnerabilities in outdated software can be exploited by malware like ShellBot.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0011 Command and Control	TA0040 Impact
TA0005 Defense Evasion	T1027.010 Command Obfuscation	T1027 Obfuscated Files or Information	T1498 Network Denial of Service
T1566 Phishing	T1598.003 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File
T1204.001 Malicious Link	T1132 Data Encoding	T1071.001 Web Protocols	T1071 Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	39[.]99[.]218[.]78, 116[.]204[.]84[.]189, 123[.]6[.]5[.]229, 124[.]222[.]211[.]66, 135[.]125[.]240[.]201, 175[.]178[.]157[.]198, 31[.]145[.]142[.]206, 39[.]107[.]61[.]230, 39[.]165[.]53[.]17, 61[.]242[.]178[.]220, 94[.]250[.]254[.]43
MD5	7bc4c22b0f34ef28b69d83a23a6c88c5, 8853bb0aef4a3dfe69b7393ac19ddf7f, a92559ddace1f9fa159232c1d72096b2
SHA1	5daf348ae3ca2c13ff7983c5771e9436ca540695, 620a4ef784f6bbc8c9fd08c7590b691de546049f, a10262346ce669b28914570415a223ec09c234c8

TYPE	VALUE
SHA256	8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a, 9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97, c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140
URLs	Hxxp[:]//Ox2763da4e/dred, Hxxp[:]//Ox74cc54bd/static/home/dred/dred

References

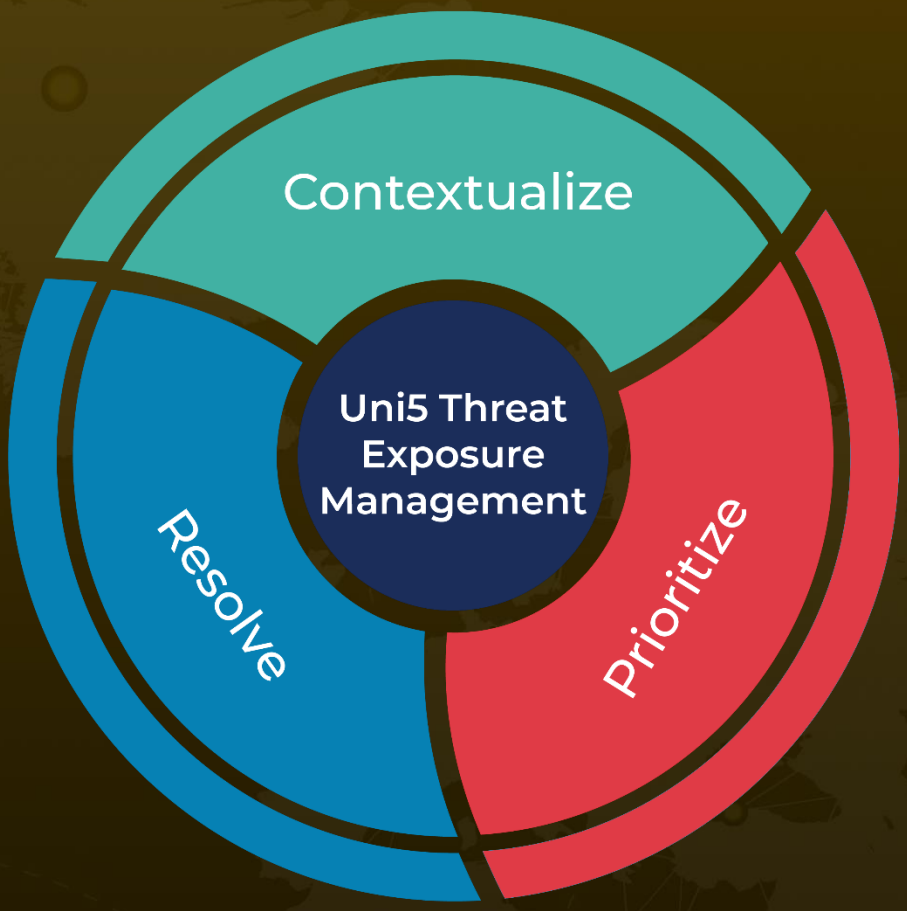
https://asec.ahnlab.com/en/57635/

https://www.hivepro.com/shellbot-malware-targets-mismanaged-linux-servers/

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

October 13, 2023 . 5:00 AM

More at www.hivepro.com