Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

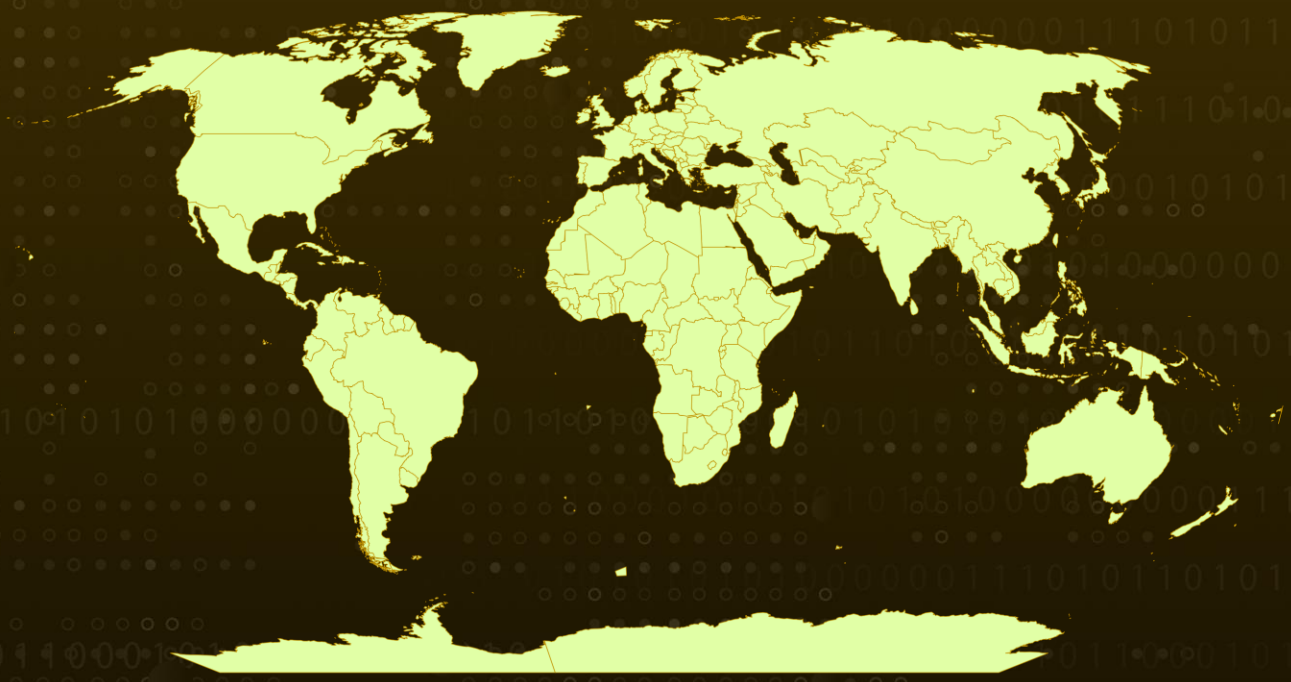
Tsunami Botnet Preying on Insufficiently Shielded Linux SSH Servers

Date of Publication	Admiralty Code	TA Number
June 22, 2023	A1	TA2023274

Summary

Attack Began: February 2023
Malware: Tsunami botnet (aka Kaiten), ShellBot, and an XMRig coin miner
Attack Region: Worldwide
Attack: An ongoing hacking campaign has been targeting inadequately secured Linux SSH servers. The objective of this campaign is to deploy the Tsunami DDoS botnet. Furthermore, the threat actors responsible for these attacks have been observed installing various other malware families.

Attack Regions



Attack Details

#1 An unidentified malicious actor is employing brute-force techniques to compromise Linux SSH servers, installing a diverse array of malware variants. These include the Tsunami DDoS bot, ShellBot, log cleansing utilities, privilege escalation tools, and XMRig, a Monero cryptocurrency mining program.

#2 The targeted attacks primarily focus on inadequately managed Linux SSH servers, with a predominant emphasis on the deployment of DDoS bots and CoinMiners. Tsunami, also called Kaiten, is a notable DDoS bot that consistently accompanies Mirai and Gafgyt during exploits directed at susceptible IoT devices.

#3 Due to the publicly accessible source code of the Tsunami botnet, it is widely utilized by numerous threat actors. SSH is a secure and encrypted network communication protocol used by network administrators to remotely manage Linux devices. It enables tasks such as executing commands, altering configurations, updating software, and resolving issues.

#4 However, if servers are inadequately secured, attackers scour the Internet for publicly accessible Linux SSH servers and employ brute-force techniques to gain unauthorized access. The compromised hosts are infected with ShellBot, a Perl-based DDoS bot that utilizes the IRC protocol for communication. Tsunami, another malware variant, communicates with command and control (C&C) servers through the IRC protocol.

#5 Additionally, the attackers employ MIG Logcleaner and Shadow Log Cleaner tools to eliminate traces of intrusion on compromised systems, reducing the likelihood of prompt detection. The privilege escalation malware takes the form of an ELF file, enabling the attackers to elevate their privileges to that of a root user. Finally, the threat actors activate an XMRig coin miner to hijack the server's computational resources and mine Monero on a designated pool.

Recommendations

To bolster the security of Linux servers, it is highly advisable to switch to key-based authentication, Key-based authentication offers a higher level of security through the utilization of cryptographic keys. Furthermore, it is vital to minimize the exposure of Linux SSH service to reduce the risk of unauthorized access.

Additionally, deploy robust intrusion detection systems and monitoring tools to promptly identify and respond to any signs of compromise, such as the presence of privilege escalation malware or unauthorized coin mining activities.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control
TA0040 Impact	**T1498** Network Denial of Service	**T1070** Indicator Removal	**T1176** Browser Extensions
T1140 Deobfuscate/Decode Files or Information	**T1059** Command and Scripting Interpreter	**T1546** Event Triggered Execution	**T1110** Brute Force
T1071 Application Layer Protocol	**T1552** Unsecured Credentials	**T1021** Remote Services	**T1525** Implant Internal Image
T1059.004 Unix Shell	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**T1095** Non-Application Layer Protocol

Indicators of Compromise (IOCs)

TYPE	VALUE
Hostname	ircxx[.]us[.]to ircx[.]us[.]to
URLs	hxxp://ircxx[.]us[.]to:53 hxxp://ircx[.]us[.]to:6667 hxxp://ircx[.]us[.]to:53 hxxp://ircx[.]us[.]to:20 hxxp://irc[.]dal[.]net:6667 hxxp://ddoser[.]org/top;tar hxxp://ddoser[.]org/top hxxp://ddoser[.]org/siwen/ping6 hxxp://ddoser[.]org/siwen/cls hxxp://ddoser[.]org/siwen/clean hxxp://ddoser[.]org/siwen/bot hxxp://ddoser[.]org/siwen/a hxxp://ddoser[.]org/logo;perl hxxp://ddoser[.]org/logo hxxp://ddoser[.]org/key|bash;cd hxxp://ddoser[.]org/key: hxxp://ddoser[.]org/key hxxp://ddoser[.]org/a;chmod hxxp://ddoser[.]org/a
SHA256	f72babf978d8b86a75e3b34f59d4fc6464dc988720d1574a781347896c2989c7 dcbcade6487fed9909749e98f9c126f79ca1e52f64912a9e7121265c9b97cc20 d5c7c78f6620717ca1aa834483fb662b26d48c8ee5f162ce9c904620352be48b a4399b5cb3fcddb7968dae9c929862a60512ecb50060eaf6a3b7c565b51b57e3 993a5ee854f2fc84facc54fe495dc6ee46b3702dc9c02d2ca315fdf1e33d3e02 8a3808d549c6fe4560153558fe20fd47f8089b392b984dfbde4c20b92044e358 5785b3e2de8814b81c8a6902b4961cbc5e2e80a82899ed7f74d12006e3f46144 4853fa813d500d103cfcb3f5199317c1a82b83300d5493ab65710d4bf8bcfe63
SHA1	b5da30e5e62fd8efba68b5949ef3f67c38949d18 82ba6edd28b4985d102c472d233dcff28a2511f8 7929af55b83e9d10bf8c408081d56fe7cbfc9ec0

TYPE	VALUE
SHA1	4898e80e81129ab9f75be89a3e4fc004039c257e 33f911983769be608b69582b283768fb991cb5a1 1fea4a56ffb7756d9b6a549dcd17be6657b31682 17ed45daa29d402d0dcf3e2cee67db1612a19334 0d4e06b0b9461df809c2ba5b80a309ae1d949bf2
MD5	e2f08f163d81f79c1f94bd34b22d3191 c5142b41947f5d1853785020d9350de4 ad04aab3e732ce5220db0b0fc9bc8a19 98b8cd5ccd6f7177007976aeb675ec38 822b6f619e642cc76881ae90fb1f8e8e 725ac5754b123923490c79191fdf4f76 6187ec1eee4b0fb381dd27f30dd352c9 421ffee8a223210b2c8f2384ee6a88b4 32eb33cdfa763b012cd8bcad97d560f0 2cd8157ba0171ca5d8b50499f4440d96 125951260a0cb473ce9b7acc406e83e1 0014403121eeaebaeede796e4b6e5dbe
Domain	ddoser[.]org

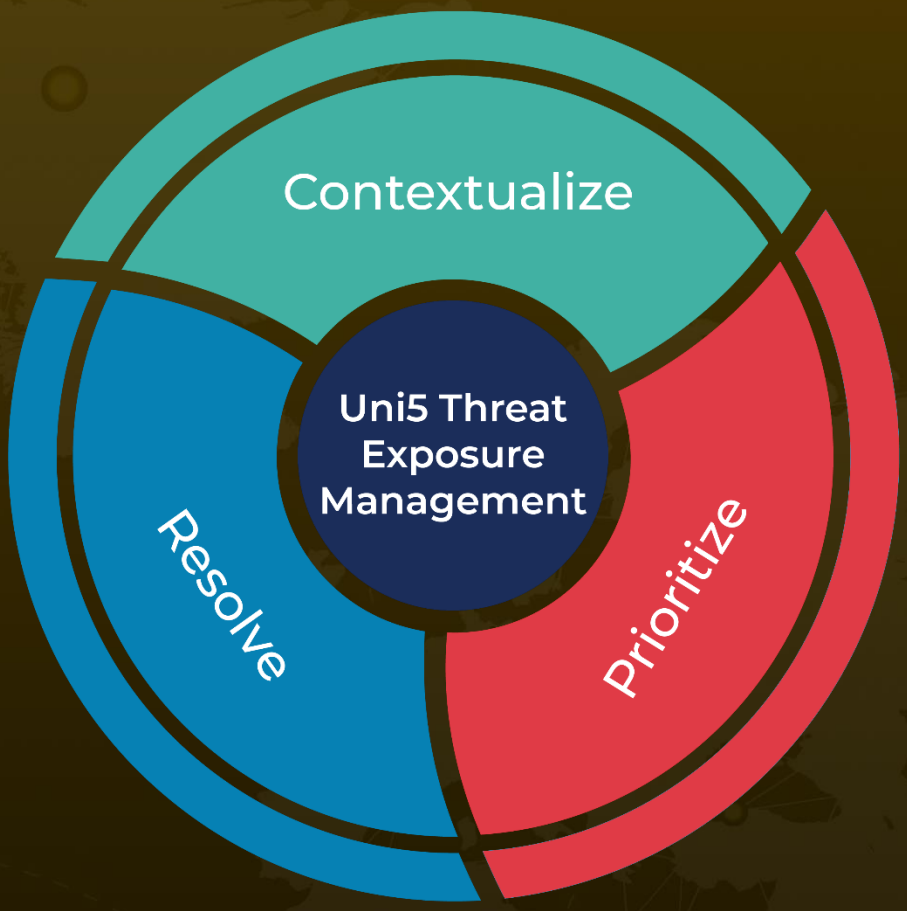
References

https://asec.ahnlab.com/en/54647/

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

June 22, 2023 • 6:51 AM

More at www.hivepro.com