Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

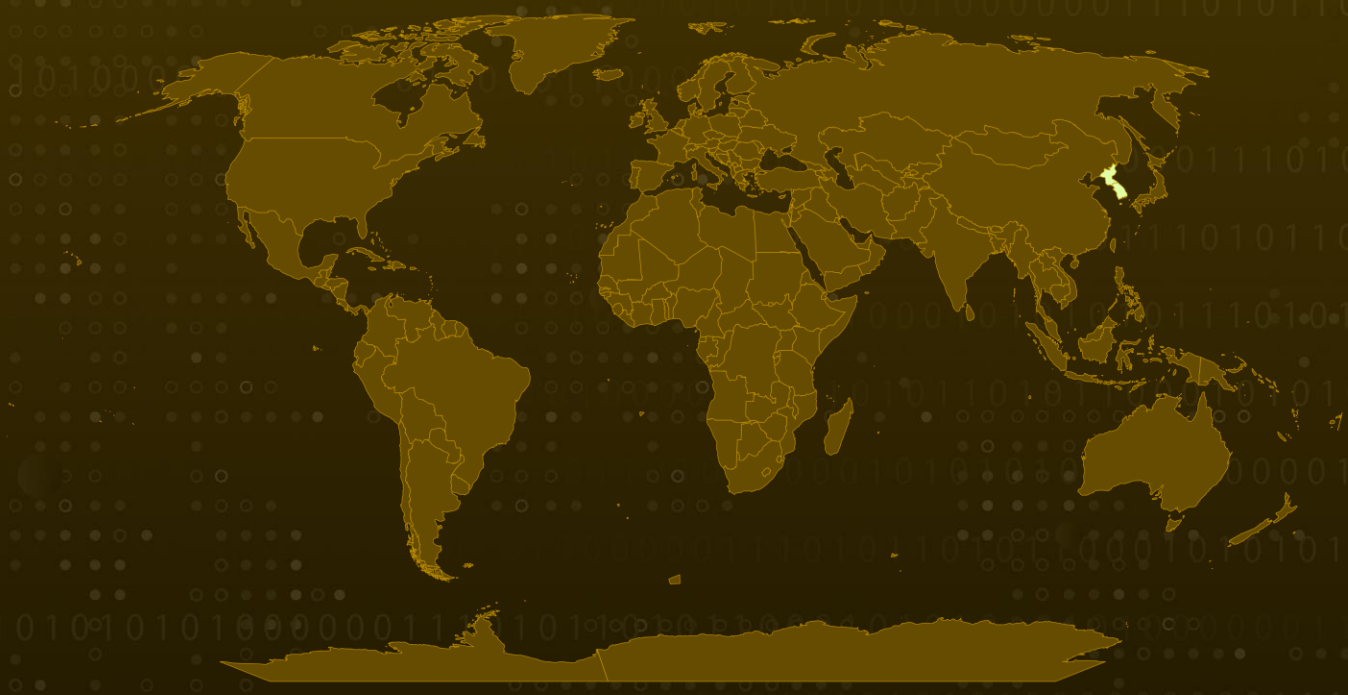
Linux Malware Using SHC Compiler Installs CoinMiner and DDoS Bots

Date of Publication	Admiralty Code	TA Number
January 5, 2023	A1	TA2023007

Summary

First appeared: 2019
Attack Region: Korea
Attack: There is a new SHC-compiled Linux malware that installs CoinMiner and DDoS bots

Attack Regions



Attack Details

#1

A new strain of Linux malware, developed using the Shc compiler, has been found to install a CoinMiner on infected systems. It is believed that this malware is being spread through dictionary attacks on inadequately secured Linux SSH servers. Once it gains access to a system, it installs several different types of malware, including the Shc downloader, XMRig CoinMiner, and a DDoS IRC Bot developed with Perl.

#2

These DDoS bots have been continuously installed on Linux servers with weak credentials for many years and remain a threat today. To prevent these types of attacks, Linux server administrators should use strong, regularly-changed passwords for their accounts and keep their systems up to date with the latest patches to prevent vulnerabilities from being exploited.

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	TA0011 Command and Control	TA0006 Credential Access	TA0009 Collection
TA0040 Impact	T1059 Command and Scripting Interpreter	T1560 Archive Collected Data	T1110 Brute Force
T1498 Network Denial of Service	T1132 Data Encoding	T1496 Resource Hijacking	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c13e7e87e800a970df4d113d60e75ab4 1f0e5f4736a567a631946a0d9878fad7 6fa237ce385dc9495246bc4498b64c2d 7650957bf7d798b284ea01a732ad07a5 077279a2ae5b1bc89540a1293fa807f1 497bec45d865b2a9165699433c64816c c1e65d481af4e6d4bad74cca4e8737cb 48e5ce77980d52c68a7bbfd091756036 16b7ef9cbc89ccc08f5fcd80e473c169 a2fd0f3e18259d0bba9ebbf910e925c4 a2c7c9e3b468e7e02e882066b05c55c3 c15ed837bd367fd4f66562b57b8fb57c
URL	hxxp://172.105.211[.]21/ hxxp://172.105.211[.]21/xmrig hxxp://172.105.211[.]21/snunewa.tar hxxp://167.172.103[.]111/ hxxp://172.104.170[.]240/ hxxp://172.104.170[.]240/snunewa.tar hxxp://wget.hostname[.]help/ hxxp://wget.hostname[.]help/driver.zip hxxp://pateu.freevar[.]com/xmrminer2.tgz
IPV4:PORT	64.227.112[.]247:80 157.230.116[.]194:80

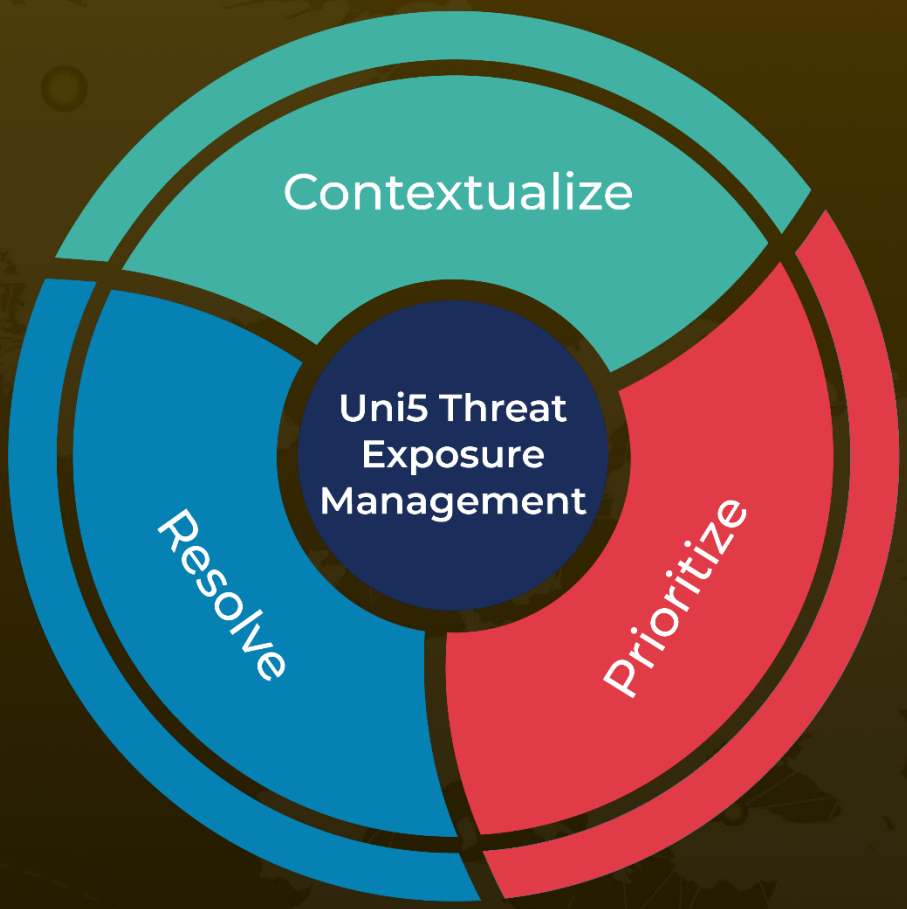
References

https://asec.ahnlab.com/en/45182/

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

January 5, 2023 • 2:30 AM

More at www.hivepro.com