Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

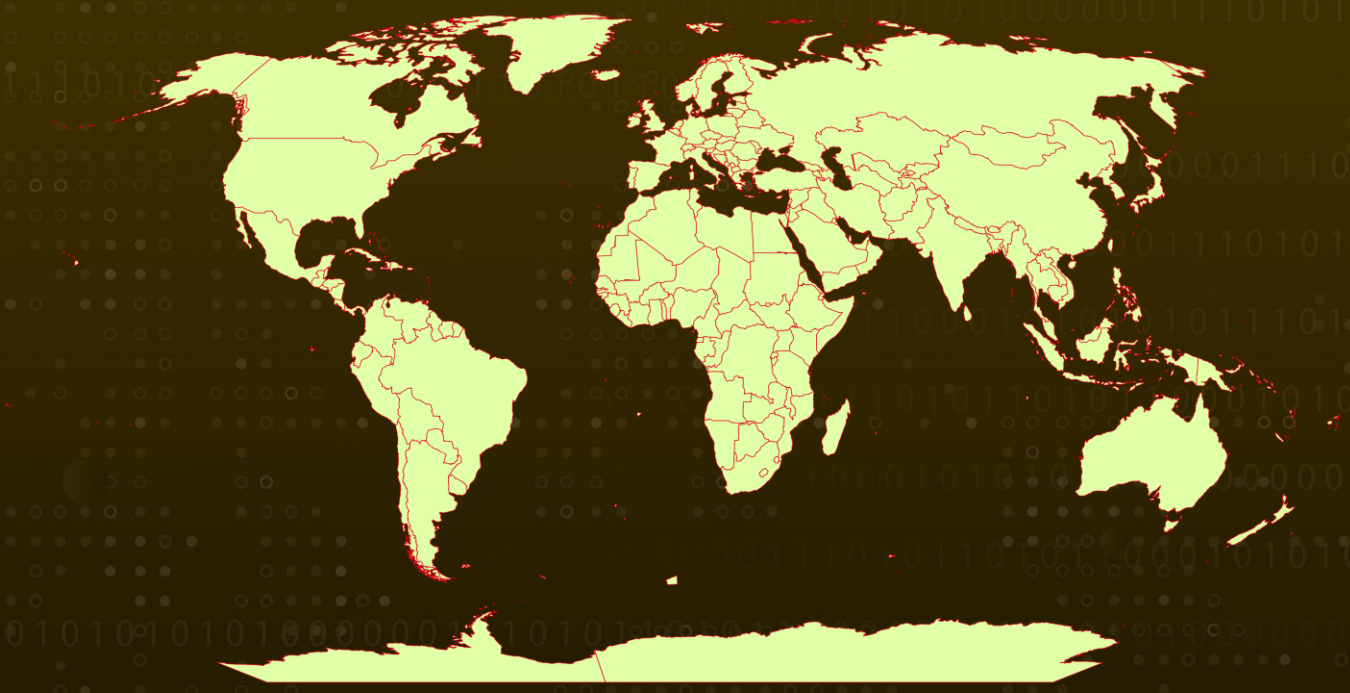
KmsdBot Cryptominer Targets the Gaming Industry

Date of Publication	Admiralty Code	TA Number
November 14, 2022	A1	TA2022255

Summary

Date: November 10, 2022
Attack Region: Worldwide
Targeted Industry: gaming industry, technology industry, and luxury car manufacturers.
Attack: KmsdBot exploits systems over an SSH connection with insecure login credentials.

Attack Regions



Attack Details

#1

KmsdBot is Golang-based malware that leverages the Secure Shell (SSH) cryptographic protocol to obtain access to targeted systems to mine cryptocurrencies and carry out distributed denial-of-service (DDoS) attacks. The malware supports several architectures, including Winx86, Arm64, and mips64, x86 64.

#2

The ksmdx binary is a downloader that sends an HTTP POST request to the C2 with the message "Bruh Started" to notify it that the system is infected. The malware takes its name from an executable called "kmsd.exe," downloaded from a remote site after a successful penetration. KmsdBot can execute scanning activities and spread itself by downloading a list of login and password combinations. It could additionally control the mining operation and update the malware.

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

TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence	TA0011 Command and Control
T1584 Compromise Infrastructure	T1584.005 Botnet	T1078 Valid Accounts	T1554 Compromise Client Software Binary
T1001 Data Obfuscation			

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	701b874a56a9a0ed4101a88621441afec936c4210e18d9a3e20f9a95c454ce40,8d1df3c5357adbab988c62682c85b51582649ff8a3b5c21fca3780fe220e5b11e83a61c538f11e4fc9dd9d0f414a9e74d0d585ffe3302e4d3741be6a3523bd1e,714eeba5b6e4610946cd07c1ddadddc94052bfe450a8a9b1c23495721082884d,8775bdd7a33f136d31b2840dab68505ac0ab8eaa0bcb58713fae36552b8a1f95,b927e0fe58219305d86df8b3e44493a7c854a6ea4f76d1ebe531a7bfd4365b54,75569874dadb814ce51d121c108ead006b0f39c27057945b649837563f635f51,09761d69bd5b00b2e767a1105dd3e80ce17b795cd817676c737a1e83c5b96f1b,8d1df3c5357adbab988c62682c85b51582649ff8a3b5c21fca3780fe220e5b11,3928c5874249cc71b2d88e5c0c00989ac394238747bb7638897fc210531b4aab,e83a61c538f11e4fc9dd9d0f414a9e74d0d585ffe3302e4d3741be6a3523bd1e,01b4d10e08d10c36d0c50f00d017fd6b3da8ebdd194ecafd12b0335c07f9ae10,74075b2bdfaf52d9e5984a28ec7765ae489077a69dd696718e724a455a6f7910

Recent Breaches

https://fivem.net/

References

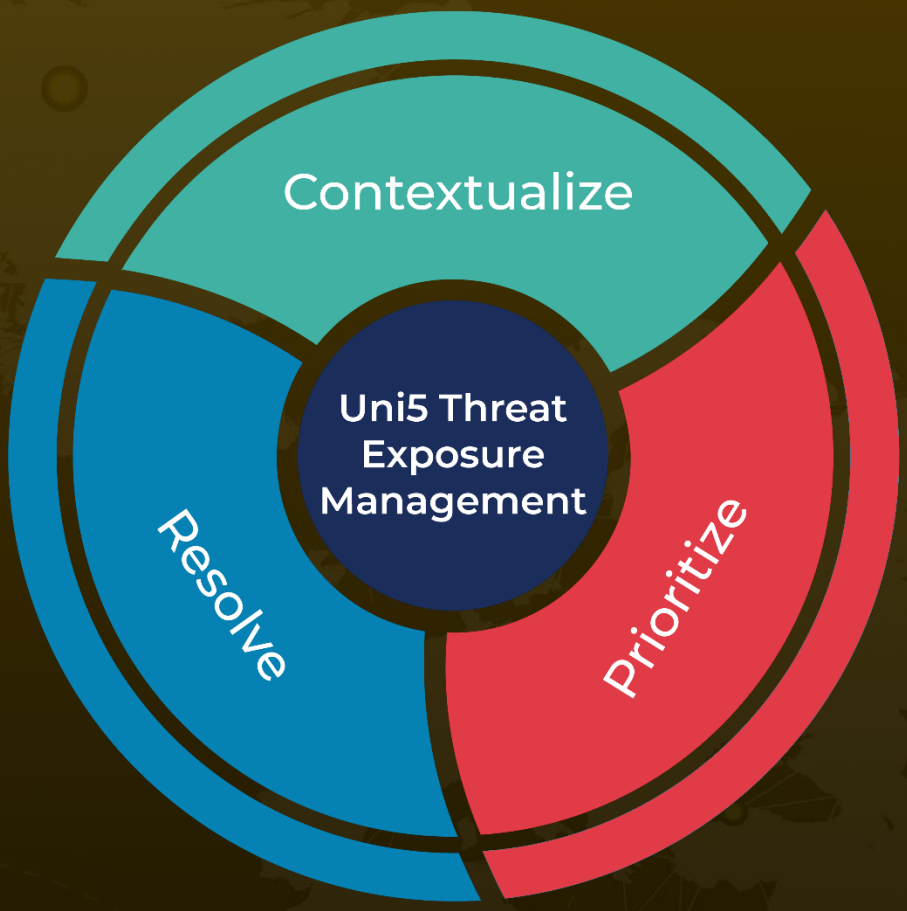
https://www.akamai.com/blog/security-research/kmdsbot-the-attack-and-mine-malware

https://thehackernews.com/2022/11/new-kmsdbot-malware-hijacking-systems.html

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 14, 2022 . 5:55 AM

More at www.hivepro.com