Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Cinoshi A Novel Malware-as-a-Service Platform

Date of Publication	Admiralty Code	TA Number
March 24, 2023	A1	TA2023159

Summary

First appeared: March 2023
Malware: Cinoshi
Attack Region: Worldwide
Targeted Industry: Gaming
Attack: Cinoshi is a novel Malware-as-a-Service (MaaS) platform. Cinoshi's toolkit includes a stealer, botnet, clipper, and cryptominer. This MaaS platform is promoting stealer and web panel for free, which is unusual.

Attack Regions

Attack Details

#1

In March 2023, a new MaaS platform called "Cinoshi" emerged on a cybercrime forum. It offers a stealer, botnet, clipper, and cryptominer. The platform offers free stealer and web panel, while the monthly subscription for Botnet and Clipper is 1000 rubles or 15 dollars. A lifetime subscription for cryptominer is available for 2000 rubles or 30 dollars.

#2

Cinoshi's 32-bit .Net binary stealer payload uses heavy obfuscation and empty methods to avoid tampering. It modifies its code at runtime and generates errors when de-obfuscation tools are used. The stealer acquires .NET dependencies files from a decoded URL and saves them with hidden attributes. Once the data is exfiltrated, the stealer deletes the zip archive.

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	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
TA0040 Impact	T1204 User Execution	T1547 Boot or Logon Autostart Execution	T1053 Scheduled Task/Job
T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1027 Obfuscated Files or Information	T1555 Credentials from Password Stores
T1539 Steal Web Session Cookie	T1552 Unsecured Credentials	T1528 Steal Application Access Token	T1113 Screen Capture
T1087 Account Discovery	T1518 Software Discovery	T1057 Process Discovery	T1124 System Time Discovery
T1007 System Service Discovery	T1614 System Location Discovery	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel
T1567 Exfiltration Over Web Service	T1489 Service Stop		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1798e35f14a67741f3425ba67373667d 40a85e9ac222d66a0f5cf526868ef2a9 29f3e408da86aafe535e179767fb2345
SHA1	b929ed50142b9b43fb85c5b1ddb87ec00ca09f24 b4553412217971d814650995ce9d98c78660fdab 783303902cafad79efc585fd25705853b4150338
SHA256	e3aafd9f478b82cbb53ec020cdc2e00e0c4de60a7f66a1166e54ab75b6a9e8c3 ,cf1705c39dc3dbf65856ac6f5462027d9a290ab2d38da08f76aabd684b8a9944,9b7d799895932d8359d7eb5da378b67a481331fa1a912075339d972496d122d6
URLs	hxxps[:]//tryno.ru/robots hxxps[:]//anaida[.]evisyn[.]lol

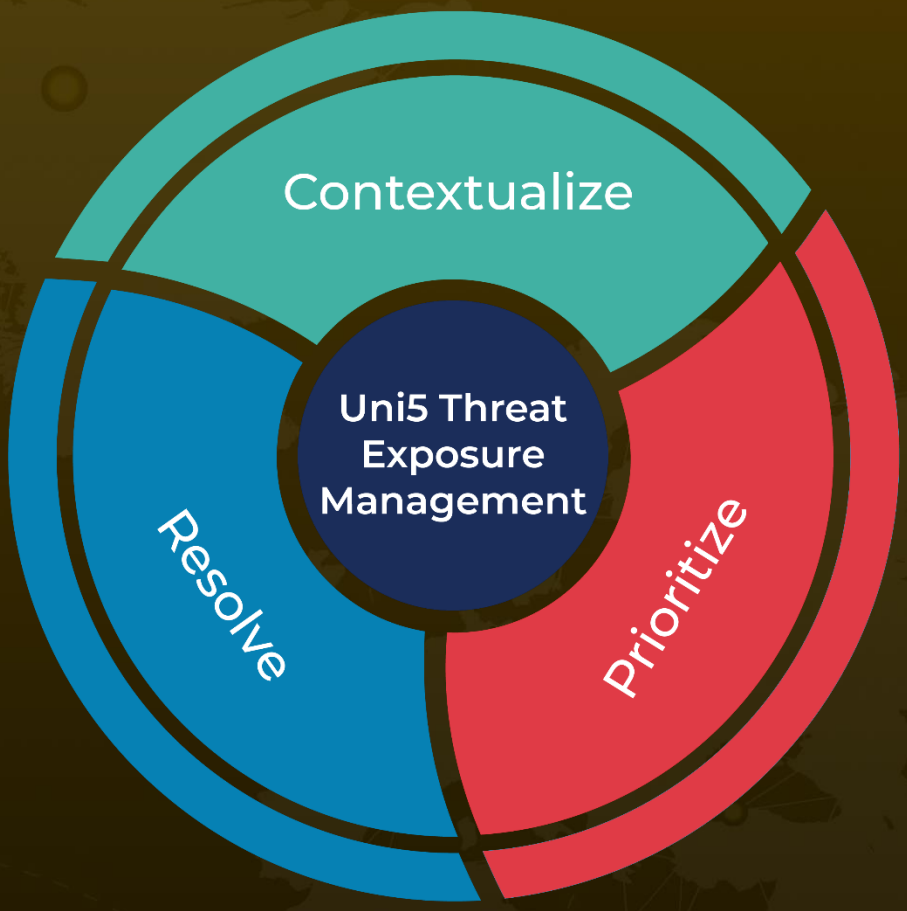
References

https://blog.cyble.com/2023/03/23/cinoshi-project-and-the-dark-side-of-free-maas/

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 24, 2023 • 3:15 AM

More at www.hivepro.com