Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Aurora Botnet evolves into a Stealer

Date of Publication	Admiralty Code	TA Number
November 22, 2022	A1	TA2022268

Summary

Date: April 16, 2022
Attack Region: Worldwide
Threat Actor: Cheshire
Attack: Aurora botnet a Malware-as-a-Service (MaaS) has been transformed into a stealer.

Attack Regions

Attack Details

#1 Aurora was first discovered in Russian-speaking underground forums and was capable of stealing, downloading, and gaining remote access. A threat actor by the name of Cheshire is selling this Malware-as-a-Service.

#2 Aurora was advertised on Telegram and underground forums in late August 2022 as a stealer instead of a botnet, which could steal sensitive data from browsers and cryptocurrency applications, exfiltrate data directly from disks and load additional payloads.

#3 Typically, Aurora spreads via phishing or social engineering. Aurora runs multiple commands through WMIC to collect basic host information, snap a desktop image, and send everything to the C2. Additionally, the malware targets data stored in multiple browsers, cryptocurrency browser extensions, cryptocurrency wallets, and Telegram. A single base64-encoded JSON file with all stolen data is sent to the C2 through TCP ports 8081 or 9865.

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

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1566 Phishing	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1012 Query Registry
T1047 Windows Management Instrumentation	T1027 Obfuscated Files or Information	T1140 Deobfuscate/Decode Files or Information	T1539 Steal Web Session Cookie
T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1082 System Information Discovery	T1614 System Location Discovery
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1083 File and Directory Discovery	T1005 Data from Local System
T1041 Exfiltration Over C2 Channel	T1113 Screen Capture	T1119 Automated Collection	T1071 Application Layer Protocol
T1071.001 Web Protocols			

Indicator of Compromise (IOC)

TYPE	VALUE
IPV4:Port	138.201.92[.]44:8081 146.19.24[.]118:8081 167.235.233[.]95:9865 185.173.36[.]94:8081 185.209.22[.]98:8081 193.233.48[.]15:9865 37.220.87[.]2:8081 45.137.65[.]190:8081 45.144.30[.]146:8081 45.15.156[.]115:8081 45.15.156[.]22:8081 45.15.156[.]33:8081 45.15.156[.]80:8081 45.15.156[.]97:8081 45.15.157[.]137:8081 49.12.222[.]119:8081

TYPE	VALUE
IPV4:Port	49.12.97[.]28:8081 5.9.85[.]111:8081 65.108.253[.]85:8081 65.109.25[.]109:8081 78.153.144[.]31:8081 79.137.195[.]171:8081 81.19.140[.]21:8081 82.115.223[.]218:8081 85.192.63[.]114:8081 89.208.104[.]160:8081 95.214.55[.]225:8081
Domains	alls0ft[.]cloud allsofts[.]cloud cheatcloud[.]info freesoft[.]digital onesoftware[.]site unisoft[.]store winsofts[.]cloud mividajugosa[.]com
URLs	https[:]//alls0ft.cloud/, https[:]//allsofts.cloud/, https[:]//cheatcloud.info/, https[:]//freesoft.digital/, https[:]//onesoftware.site/, https[:]//unisoft.store/, https[:]//winsofts.cloud/, https[:]//mividajugosa.com/, https[:]//cdn.discordapp.com/attachments/1028937934763720724/1038878571302756372/Adobe_Photoshop_2022_CRACK.rar, https[:]//cdn.discordapp.com/attachments/1036677135621951653/1037145460089040916/Adobe_Photoshop.zip, https[:]//cdn.discordapp.com/attachments/1036703574828269658/1037132394534281266/Adobe_Premiere_Pro.zip, https[:]//cdn.discordapp.com/attachments/1037343714319794236/1037352224650690650/Adobe_Photoshop.zip, https[:]//cdn.discordapp.com/attachments/1041004296050835459/1041454535836696656/onesoftware.site.zip, https[:]//cdn.discordapp.com/attachments/1041004296050835459/1041740296993636372/FreeSoft.zip, https[:]//www.dropbox.com/s/dl/0wzz3wsk5sy7kck/Fortnite%20Hack%20%231.zip
SHA256	a485913f71bbd74bb8a1bdce2e2c5d80c107da7d6c08bf088599c1ee62ccb109 f6b17c5c0271074fc27c849f46b70e25deafa267a060c35f1636ab08dda237d6 51a2fe0ea58a7a656bc817e91913f6d6c50e947823b96a3565e7593eea2fd785

TYPE	VALUE
SHA256	73485bc0ca251edcca9e4c279cbc4876b1584fb981a5607a4bdeae156a70d082 2bdba09d02482f3016df62a205a456fc5e253f5911543bf40da14a59ad2bc566 459a8faa7924a25a15f64c34910324baed5c24d2fe68badd9a4a320628c08cb8 aa504264669e5bdbda0aac3ada1cd16964499c92d2b48d036a16ba22d79f44f6 4b5450b61a1be5531d43fe36f731c78a28447b85f2466b4389ea7bbb09ecec9c 04b2edcc9d62923a37ef620f622528d70edab52ccd3409814900046ad3aa255e5 a4a3a66aee74f3442961a860b8376d2a2dc2cf3783b0829f6973e63d6d839e5b

References

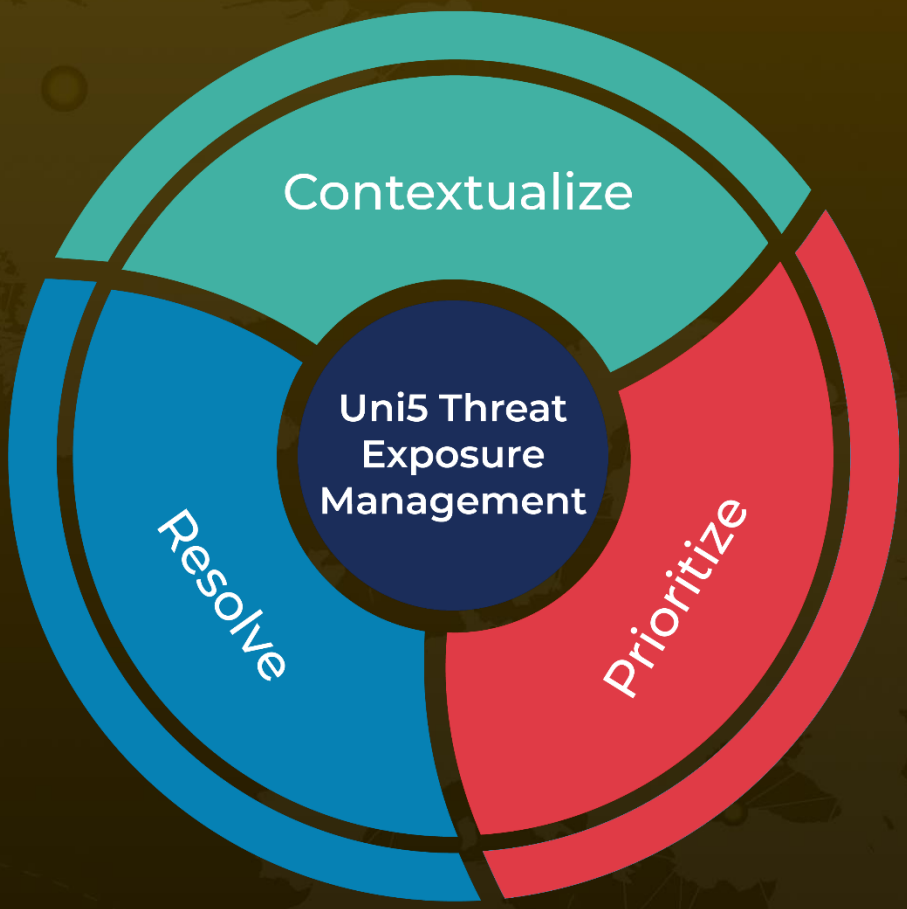
https://blog.sekoia.io/aurora-a-rising-stealer-flying-under-the-radar/

https://otx.alienvault.com/pulse/637baa6081d4bafd9cb4afec

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 22, 2022 . 3:45 AM

More at www.hivepro.com