Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

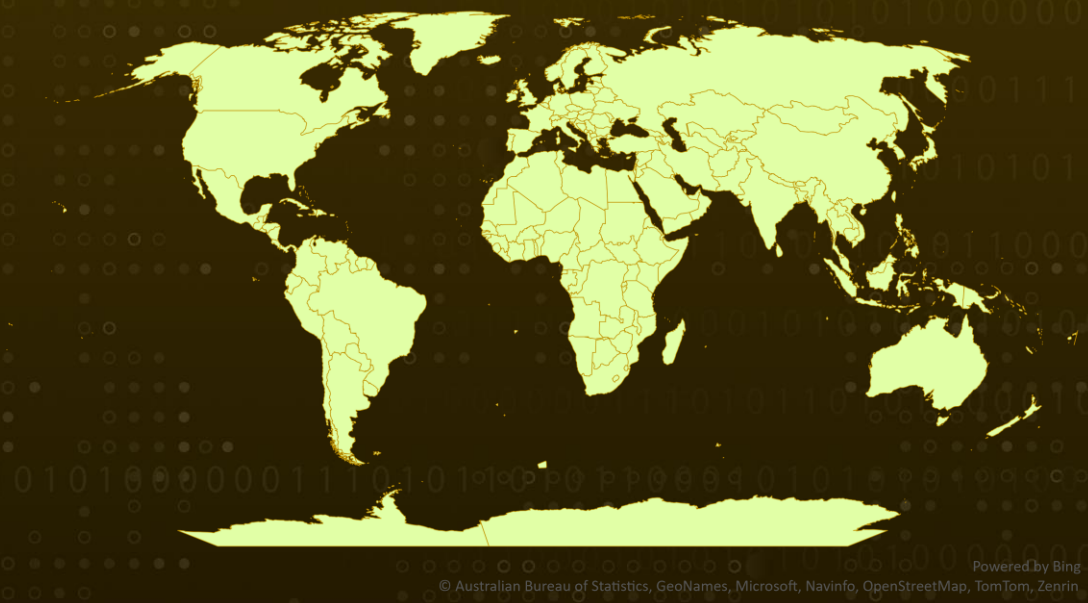
Exploiting ChatGPT's Popularity for Malware Distribution

Date of Publication	Admiralty Code	TA Number
February 24, 2023	A1	TA2023101

Summary

First appeared: February 2023
Attack Region: Worldwide
Attack: The attack on ChatGPT involved the exploitation of its widespread usage to distribute malware and carry out various cyber-attacks, including phishing and typosquatting.

Attack Regions



Attack Details

#1 A social engineering and phishing attack takes advantage of the popularity of ChatGPT, an AI tool developed by OpenAI, to distribute malware and steal sensitive information from unsuspecting users.

#2 The attackers have created fake social media pages and typosquatted domains that mimic the official ChatGPT website, which can easily mislead users into thinking they are accessing a legitimate website. These fake websites encourage users to download and install malicious files that can infect their devices with malware and steal sensitive data.

#3 To add credibility to their fake pages, the attackers mix unrelated posts, such as videos and other content, with links that lead to phishing pages. These phishing pages trick users into downloading malware by presenting them with buttons that encourage them to download and install the ChatGPT tool.

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	TA0002 Execution	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1105 Ingress Tool Transfer	T1584 Compromise Infrastructure
T1059 Command and Scripting Interpreter	T1608 Stage Capabilities	T1608.005 Link Target	T1204 User Execution
T1001 Data Obfuscation	T1011 Exfiltration Over Other Network Medium		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4e8d09ca0543a48f649fce72483777f0 174539797080a9bcbb3f32c5865700bf c8aa7a66e87a23e16ecacad6d1337dc4 94e3791e3ceec63a17ca1a52c4a35089 6a481f28affc30aef0d3ec6914d239e4 81e6a150d459642f2f3641c5a4621441 5f6f387edf4dc4382f9953bd57fa4c62
SHA256	d1b1813f7975b7117931477571a2476decff41f124b84cc7a2074dd00b5eba7c 3ec772d082aa20f4ff5cf01e0d1cac38b4f647ceb79fdd3ffd1aca455ae8f60b ae4d01a50294c9e6f555fe294aa537d7671fed9bc06450e6e2198021431003f9 46200951190736e19be7bcc9c0f97316628acce43fcf5b370faa450e74c5921e 34b88f680f93385494129bfe3188ce7a0f5934abed4bf6b8e9e78cf491b53727 53ab0aecf4f91a7ce0c391cc6507f79f669bac033c7b3be2517406426f7f37f0 60e0279b7cff89ec8bc1c892244989d73f45c6fcc3e432eaca5ae113f71f38c5

TYPE	VALUE
SHA1	cebddeb999f4809cf7fd7186e20dc0cc8b88689d c57a3bcf3f71ee1afc1a08c3a5e731df6363c047 aeb646eeb4205f55f5ba983b1810afb560265091 189a16b466bbebba57701109e92e285c2909e8a2 afa741309997ac04a63b4dd9afa9490b6c6235c1 23f50f990d4533491a76ba619c996b9213d25b49 f1a5a1187624fcf1a5804b9a15a4734d9da5aaf6
URLs	hxxps://openai-pc-pro[.]online hxxps://chat-gpt-pc[.]online hxxps://chatgpt-go[.]online hxxp://chatgpt-go.online/clip[.]exe hxxp://chatgpt-go.online/java[.]exe hxxps://rebrand[.]ly/qaltfnuChatGPTOpenAI

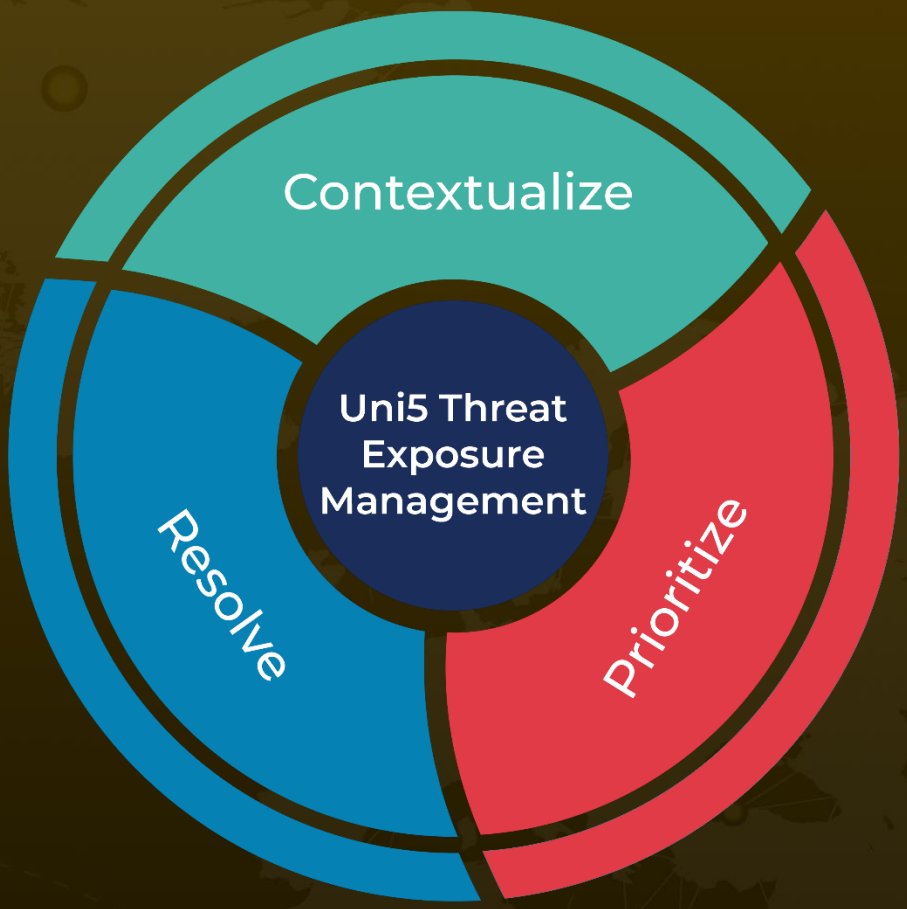
References

https://blog.cyble.com/2023/02/22/the-growing-threat-of-chatgpt-based-phishing-attacks/

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

February 24, 2023 • 12:15 AM

More at www.hivepro.com