Jun 11 2023

NETMANAGEIT

Intelligence Report

ChatGPT-Themed Scam Attacks Are on the Rise

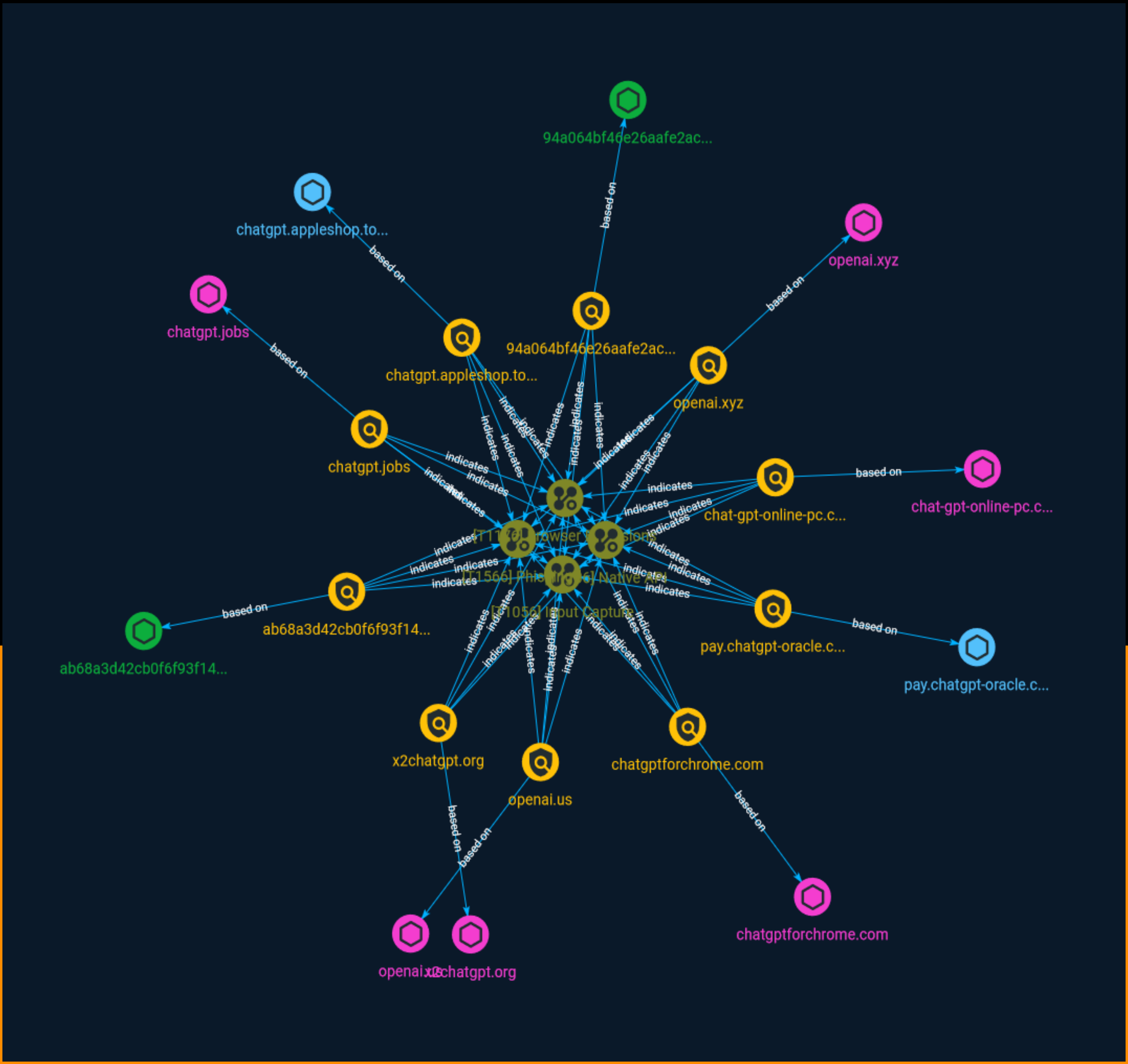

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Attack-Pattern 5
- Indicator 9

Observables

- Domain-Name 13
- StixFile 14
- Hostname 15

External References

- External References 16

Overview

Description

Unit 42 researchers are monitoring the trending topics, newly registered domains and squatting domains related to ChatGPT, as it is one of the fastest-growing consumer applications in history. The dark side of this popularity is that ChatGPT is also attracting the attention of scammers seeking to benefit from using wording and domain names that appear related to the site. Between November 2022 through early April 2023, we noticed a 910% increase in monthly registrations for domains related to ChatGPT. In this same time frame, we observed a 17,818% growth of related squatting domains from DNS Security logs. We also saw up to 118 daily detections of ChatGPT-related malicious URLs captured from the traffic seen in our Advanced URL Filtering system.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence.(Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Native API

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.(Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC)(Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. While invoking API functions, adversaries may also attempt to bypass defensive tools (ex: unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001)).

Indicator

Name
openai.us
Pattern Type
stix
Pattern
[domain-name:value = 'openai.us']
Name
chatgpt.appleshop.top
Pattern Type
stix
Pattern
[hostname:value = 'chatgpt.appleshop.top']
Name
pay.chatgpt-oracle.com

Pattern Type

stix

Pattern

[hostname:value = 'pay.chatgpt-oracle.com']

Name

ab68a3d42cb0f6f93f14e2551cac7fb1451a49bc876d3c1204ad53357ebf745f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ab68a3d42cb0f6f93f14e2551cac7fb1451a49bc876d3c1204ad53357ebf745f']

Name

openai.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'openai.xyz']

Name

chatgptforchrome.com

Pattern Type

stix

Pattern

[domain-name:value = 'chatgptforchrome.com']

Name

chatgpt.jobs

Pattern Type

stix

Pattern

[domain-name:value = 'chatgpt.jobs']

Name

chat-gpt-online-pc.com

Pattern Type

stix

Pattern

[domain-name:value = 'chat-gpt-online-pc.com']

Name

x2chatgpt.org

Pattern Type

stix

Pattern

[domain-name:value = 'x2chatgpt.org']

Name

94a064bf46e26aafe2accb2bf490916a27eba5ba49e253d1afd1257188b05600

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '94a064bf46e26aafe2accb2bf490916a27eba5ba49e253d1afd1257188b05600']

Domain-Name

Value
chat-gpt-online-pc.com
openai.us
x2chatgpt.org
openai.xyz
chatgpt.jobs
chatgptforchrome.com

StixFile

Value
ab68a3d42cb0f6f93f14e2551cac7fb1451a49bc876d3c1204ad53357ebf745f
94a064bf46e26aafe2accb2bf490916a27eba5ba49e253d1afd1257188b05600

Hostname

Value
chatgpt.appleshop.top
pay.chatgpt-oracle.com

External References

- https://unit42.paloaltonetworks.com/chatgpt-scam-attacks-increasing/
- https://otx.alienvault.com/pulse/64417ea3fd9afae377286978