Jun 15 2023

NETMANAGEIT

Intelligence Report

Android Malware Impersonates ChatGPT-Themed Applications

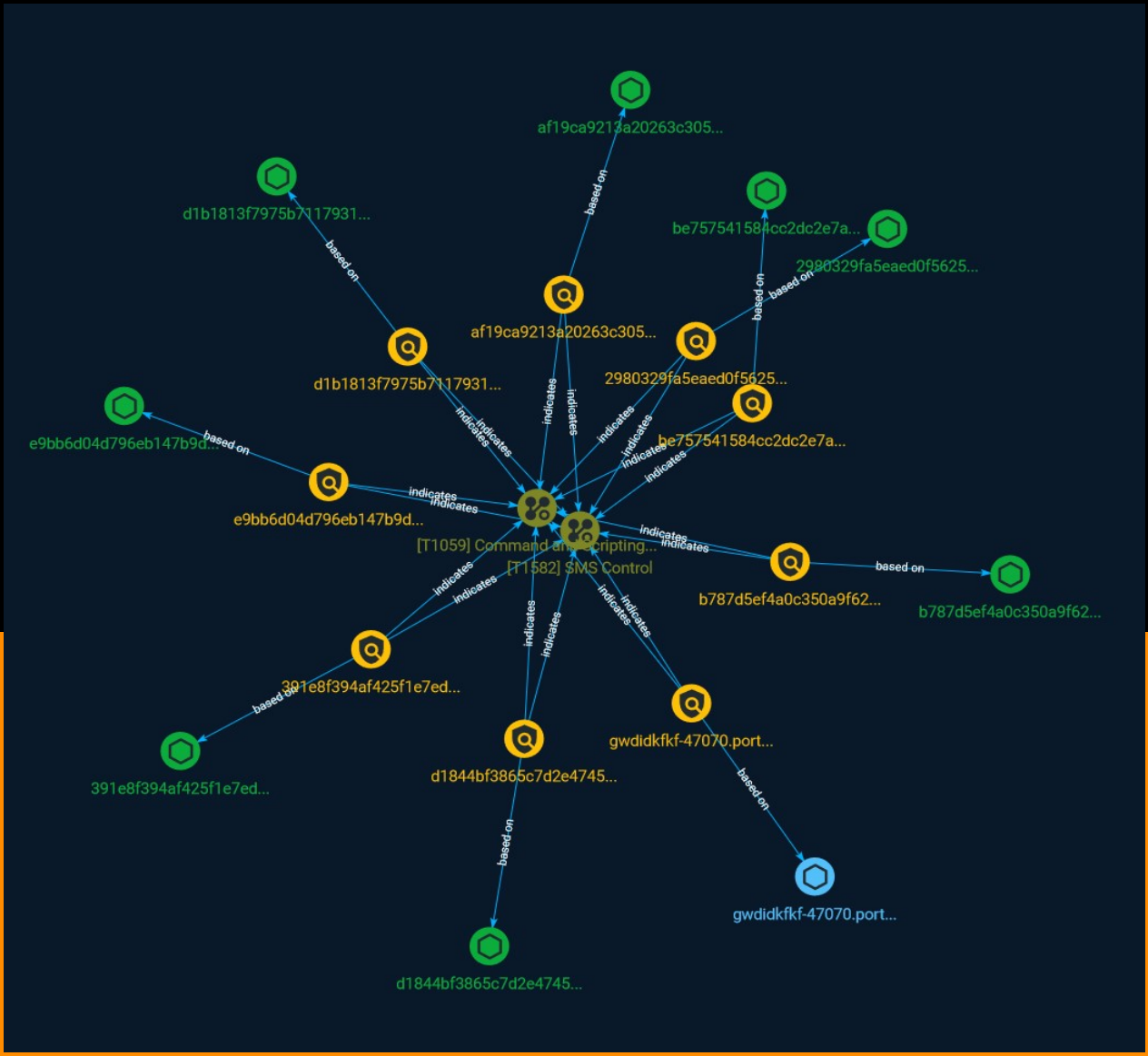

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Unit 42 researchers have observed a surge of malware written for the Android platform that is attempting to impersonate the popular ChatGPT application. These malware variants emerged along with the release by OpenAI of GPT-3.5, followed by GPT-4, infecting victims interested in using the ChatGPT tool.

Confidence

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

15 / 100

Attack-Pattern

Name
SMS Control
ID
T1582
Description
Adversaries may delete, alter, or send SMS messages without user authorization. This could be used to hide C2 SMS messages, spread malware, or various external effects. This can be accomplished by requesting the `RECEIVE_SMS` or `SEND_SMS` permissions depending on what the malware is attempting to do. If the app is set as the default SMS handler on the device, the `SMS_DELIVER` broadcast intent can be registered, which allows the app to write to the SMS content provider. The content provider directly modifies the messaging database on the device, which could allow malicious applications with this ability to insert, modify, or delete arbitrary messages on the device.(Citation: SMS KitKat) (Citation: Android SmsProvider)
Name
Command and Scripting Interpreter
ID
T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Indicator

Name
2980329fa5eaed0f5625e961572f7ae8136ca7df30cca9e9c8783c827627b692
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2980329fa5eaed0f5625e961572f7ae8136ca7df30cca9e9c8783c827627b692']
Name
d1844bf3865c7d2e4745baa2496297937821171d7a3ad4412b0a4e767bc32b5e
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd1844bf3865c7d2e4745baa2496297937821171d7a3ad4412b0a4e767bc32b5e']
Name

d1b1813f7975b7117931477571a2476decff41f124b84cc7a2074dd00b5eba7c

Description

SHA256 of cebddeb999f4809cf7fd7186e20dc0cc8b88689d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd1b1813f7975b7117931477571a2476decff41f124b84cc7a2074dd00b5eba7c']

Name

b787d5ef4a0c350a9f62f55907c8ef6d92bf7699b8544fabff5a263e52a2d0d1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b787d5ef4a0c350a9f62f55907c8ef6d92bf7699b8544fabff5a263e52a2d0d1']

Name

391e8f394af425f1e7edff6aea1605aa89f2fb0233c44e70cff265fc60ec3b1b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '391e8f394af425f1e7edff6aea1605aa89f2fb0233c44e70cff265fc60ec3b1b']

Name

af19ca9213a20263c30584a2bf260dcdb3b4eafa4f43af10824af781573a2314

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af19ca9213a20263c30584a2bf260dcdb3b4eafa4f43af10824af781573a2314']

Name

gwdidkfkf-47070.portmap.io

Pattern Type

stix

Pattern

[hostname:value = 'gwdidkfkf-47070.portmap.io']

Name

e9bb6d04d796eb147b9d73a7df91fb9e6a99e0be8a41a61329d600a9dfe8b1ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9bb6d04d796eb147b9d73a7df91fb9e6a99e0be8a41a61329d600a9dfe8b1ae']

Name

be757541584cc2dc2e7adacf7a5186be07d474f06c8698a938589f86ce56ea34

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'be757541584cc2dc2e7adacf7a5186be07d474f06c8698a938589f86ce56ea34']

StixFile

Value
e9bb6d04d796eb147b9d73a7df91fb9e6a99e0be8a41a61329d600a9dfe8b1ae
af19ca9213a20263c30584a2bf260dcdb3b4eafa4f43af10824af781573a2314
be757541584cc2dc2e7adacf7a5186be07d474f06c8698a938589f86ce56ea34
2980329fa5eaed0f5625e961572f7ae8136ca7df30cca9e9c8783c827627b692
d1844bf3865c7d2e4745baa2496297937821171d7a3ad4412b0a4e767bc32b5e
d1b1813f7975b7117931477571a2476decff41f124b84cc7a2074dd00b5eba7c
b787d5ef4a0c350a9f62f55907c8ef6d92bf7699b8544fabff5a263e52a2d0d1
391e8f394af425f1e7edff6aea1605aa89f2fb0233c44e70cff265fc60ec3b1b

Hostname

Value
gwdidkfkf-47070.portmap.io

External References

- https://otx.alienvault.com/pulse/648b79387967f2109520998e