Nov 02 2023

NETMANAGEIT

Intelligence Report

WhatsApp spy mod spreads through Telegram, attacks Arabic-speaking users

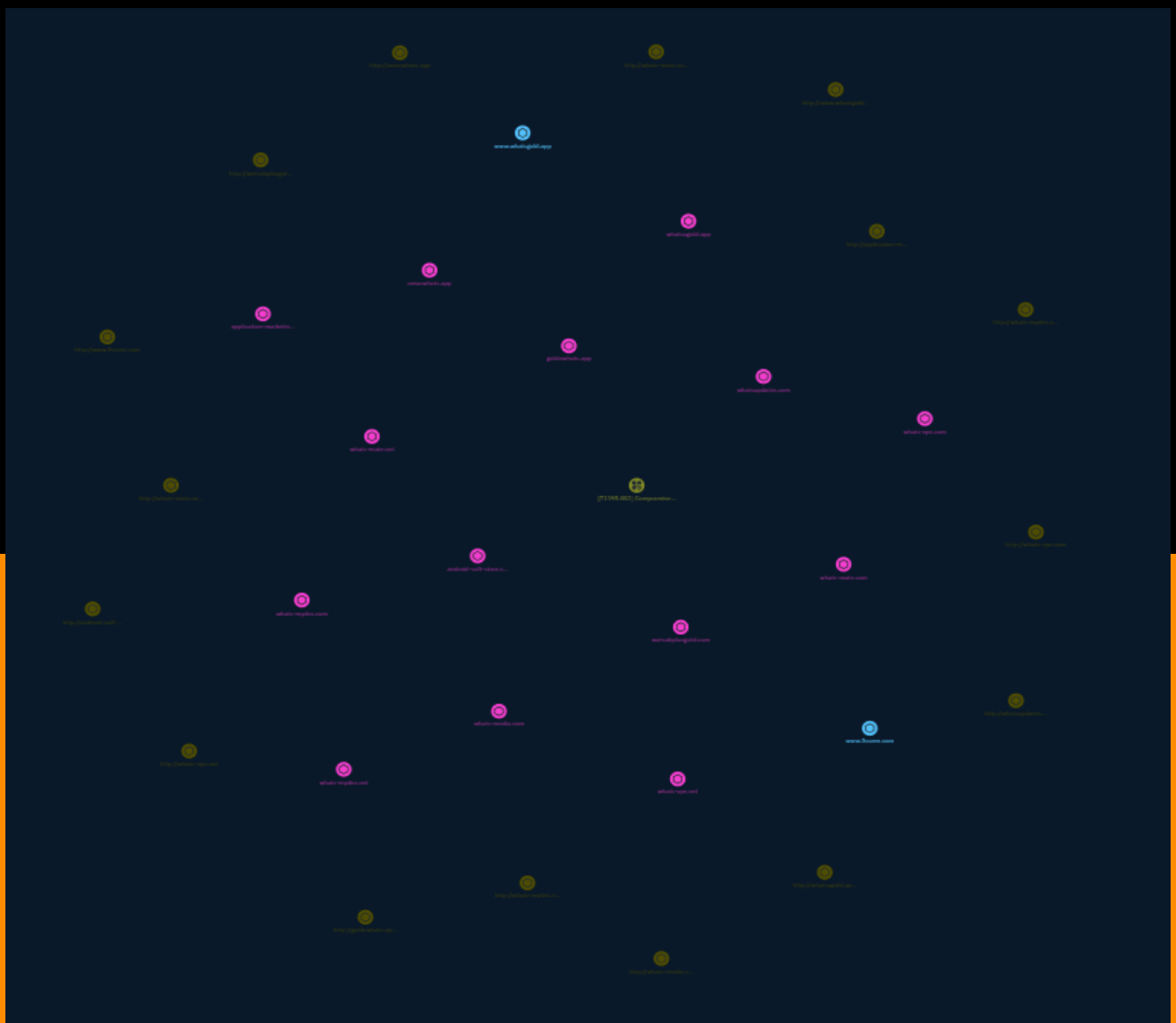

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6

Observables

- Domain-Name 7
- Hostname 9
- Url 10

External References

- External References 12

Overview

Description

It is not rare that users of popular instant messaging services find the official client apps to be lacking in functionality. To address that problem, third-party developers come up with mods that offer sought-after features besides aesthetic upgrades. Unfortunately, some of these mods contain malware alongside legitimate enhancements.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Compromise Software Supply Chain
ID
T1195.002
Description
Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the update/distribution mechanism for that software, or replacing compiled releases with a modified version. Targeting may be specific to a desired victim set or may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011)

Domain-Name

Value
android-soft-store.com
goldnwhats.app
watsabplusgold.com
whats-mate.net
whatsupdates.com
whats-media.com
omarwhats.app
whats-mate.com
whats-mydns.com
whatsagold.app
whats-vpn.net
application-marketing.com
whats-vpn.com

whats-mydns.net

Hostname

Value
www.whatsgold.app
www.3ssem.com

Url

Value
http://whats-mate.net
http://application-marketing.com
http://whats-mydns.net
http://watsabplusgold.com
http://whats-vpn.com
http://whats-vpn.net
http://whats-mate.com
http://whatsagold.app
http://www.3ssem.com
http://whats-mydns.com
http://goldnwhats.app
http://omarwhats.app
http://whatsupdates.com/api/v1/AllRequest

http://android-soft-store.com

http://www.whatsgold.app

http://whats-media.com

External References

- https://otx.alienvault.com/pulse/654399829d3f7b084090405b
- https://securelist.com/spyware-whatsapp-mod/110984/