Jul 26 2023

NETMANAGEIT

Intelligence Report

Android GravityRAT goes after WhatsApp backups

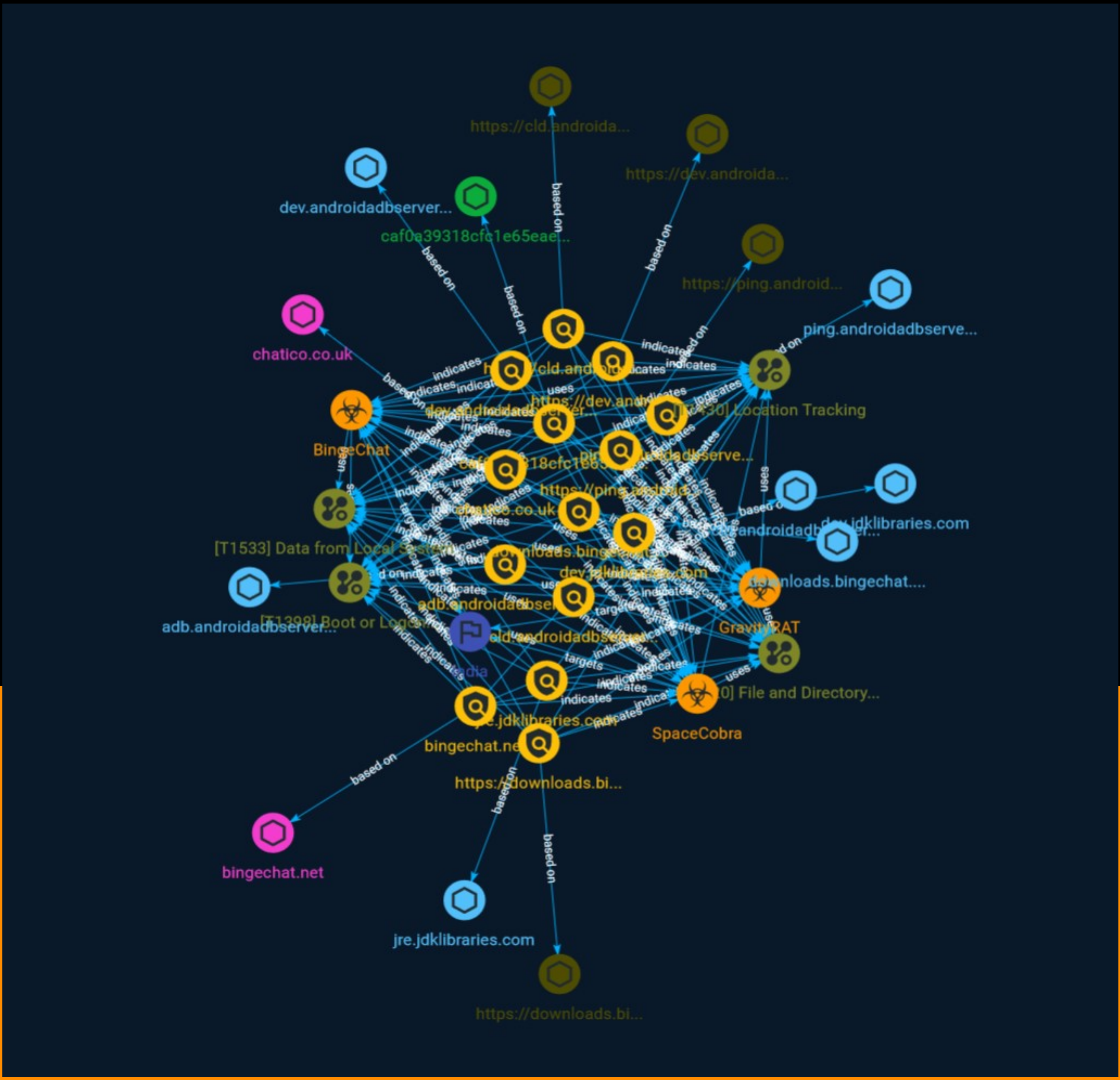

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Confidence

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

15 / 100

Indicator

Name
adb.androidadbserver.com

Pattern Type
stix

Pattern
[hostname:value = 'adb.androidadbserver.com']

Name
caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84

Description
dbgdetect_files SHA256 of 2b448233e6c9c4594e385e799cea9ee8c06923bd

Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = 'caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84']

Name

https://dev.androidadbserver.com

Pattern Type

stix

Pattern

[url:value = 'https://dev.androidadbserver.com']

Name

jre.jdklibraries.com

Pattern Type

stix

Pattern

[hostname:value = 'jre.jdklibraries.com']

Name

https://cld.androidadbserver.com

Pattern Type

stix

Pattern

[url:value = 'https://cld.androidadbserver.com']

Name

downloads.bingechat.net

Pattern Type

stix

Pattern

[hostname:value = 'downloads.bingechat.net']

Name

https://downloads.bingechat.net/uploadA/c1d8bad13c5359c97cab280f7b561389153/BingeChat.zip

Pattern Type

stix

Pattern

[url:value = 'https://downloads.bingechat.net/uploadA/c1d8bad13c5359c97cab280f7b561389153/BingeChat.zip']

Name

dev.androidadbserver.com

Pattern Type

stix

Pattern

[hostname:value = 'dev.androidadbserver.com']

Name

dev.jdklibraries.com

Pattern Type

stix

Pattern

[hostname:value = 'dev.jdklibraries.com']

Name

bingechat.net

Pattern Type

stix

Pattern

[domain-name:value = 'bingechat.net']

Name

ping.androidadbserver.com

Pattern Type

stix

Pattern

[hostname:value = 'ping.androidadbserver.com']

Name

cld.androidadbserver.com

Pattern Type

stix

Pattern

[hostname:value = 'cld.androidadbserver.com']

Name

chatico.co.uk

Pattern Type

stix

Pattern

[domain-name:value = 'chatico.co.uk']

Name

https://ping.androidadbserver.com

Description

HTML document, ASCII text, with CRLF line terminators
25fb23868ebf48348f9e438e00cb9b9d9b3a054f32482a781c762cc4f9cc6393

Pattern Type
stix

Pattern
[url:value = 'https://ping.androidadbserver.com']

Malware

Name
SpaceCobra

Name
BingeChat

Name
GravityRAT

Description
[GravityRAT](https://attack.mitre.org/software/S0237) is a remote access tool (RAT) and has been in ongoing development since 2016. The actor behind the tool remains unknown, but two usernames have been recovered that link to the author, which are "TheMartian" and "The Invincible." According to the National Computer Emergency Response Team (CERT) of India, the malware has been identified in attacks against organization and entities in India. (Citation: Talos GravityRAT)

Attack-Pattern

Name

Boot or Logon Initialization Scripts

ID

T1398

Description

Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence. Initialization scripts are part of the underlying operating system and are not accessible to the user unless the device has been rooted or jailbroken.

Name

File and Directory Discovery

ID

T1420

Description

Adversaries may enumerate files and directories or search in specific device locations for desired information within a filesystem. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) during automated discovery to shape follow-on behaviors, including deciding if the adversary should fully infect the target and/or attempt specific actions. On Android, Linux file permissions and

SELinux policies typically stringently restrict what can be accessed by apps without taking advantage of a privilege escalation exploit. The contents of the external storage directory are generally visible, which could present concerns if sensitive data is inappropriately stored there. iOS's security architecture generally restricts the ability to perform any type of [File and Directory Discovery](https://attack.mitre.org/techniques/T1420) without use of escalated privileges.

Name

Data from Local System

ID

T1533

Description

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration. Access to local system data, which includes information stored by the operating system, often requires escalated privileges. Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos. On Android, adversaries may also attempt to access files from external storage which may require additional storage-related permissions.

Name

Location Tracking

ID

T1430

Description

Adversaries may track a device’s physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. On Android, applications holding the `ACCESS_COAURSE_LOCATION` or

`ACCESS_FINE_LOCATION` permissions provide access to the device’s physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application’s manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox) On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

Country

Name
India

Domain-Name

Value
bingechat.net
chatico.co.uk

StixFile

Value
caf0a39318cfc1e65eae773a28de62ce08b7cf1b9d4264e843576165411e2a84

Hostname

Value
ping.androidadbserver.com
dev.androidadbserver.com
dev.jdklibraries.com
jre.jdklibraries.com
cld.androidadbserver.com
downloads.bingechat.net
adb.androidadbserver.com

Url

Value
https://cld.androidadbserver.com
https://downloads.bingechat.net/uploadA/c1d8bad13c5359c97cab280f7b561389153/BingeChat.zip
https://ping.androidadbserver.com
https://dev.androidadbserver.com

External References

- https://otx.alienvault.com/pulse/64c123829391edbf7dbf062c
- https://www.welivesecurity.com/2023/06/15/android-gravityrat-goes-after-whatsapp-backups/