Jul 03 2023

NETMANAGEIT

Intelligence Report

Anatsa banking Trojan hits UK, US and DACH with new campaign

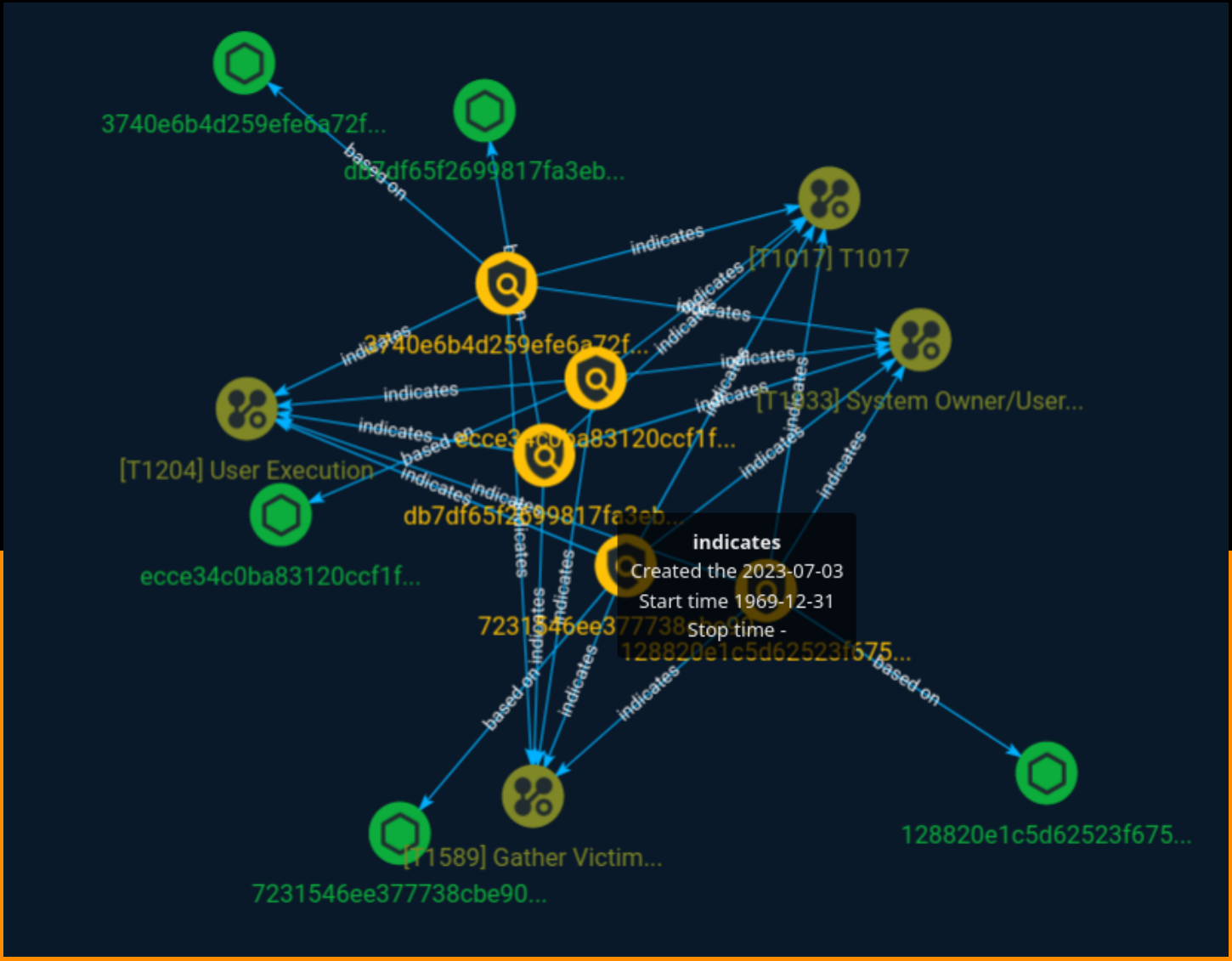

Table of contents

Overview

Entities

Observables

External References

Overview

Description

As of March 2023, ThreatFabric's cyber fraud analysts have been monitoring multiple ongoing Google Play Store dropper campaigns delivering the Android banking Trojan Anatsa, with over 30.000 installations. The threat actors behind this new wave of Anatsa showed interest in new institutions from the US, UK, and DACH region. Our fraud intelligence platform was able to confirm this dangerous malware family adding multiple Android banking apps from these regions as new targets.

Confidence

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

15 / 100

Indicator

Name
7231546ee377738cbe9075791eb6e76b7bc163c1b91831e05e81b4756fff4028
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7231546ee377738cbe9075791eb6e76b7bc163c1b91831e05e81b4756fff4028']
Name
db7df65f2699817fa3ebfb3ebef106a3801a96b9da1ba6d88e727a253ae34da6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'db7df65f2699817fa3ebfb3ebef106a3801a96b9da1ba6d88e727a253ae34da6']
Name

ecce34c0ba83120ccf1f8e1640cd867fbfeb490dbc8a41d1cf8c577d508819c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecce34c0ba83120ccf1f8e1640cd867fbfeb490dbc8a41d1cf8c577d508819c3']

Name

128820e1c5d62523f675042da9d1e11af3191217afe308bcc17e51ad8c2ece03

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '128820e1c5d62523f675042da9d1e11af3191217afe308bcc17e51ad8c2ece03']

Name

3740e6b4d259efe6a72f503429fb67db96363935a29f7428ccab5b78fa9bee73

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'3740e6b4d259efe6a72f503429fb67db96363935a29f7428ccab5b78fa9bee73']
```

Attack-Pattern

Name
T1017
ID
T1017
Name
Gather Victim Identity Information
ID
T1589
Description
Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://

attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte) (Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds) (Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts] (https://attack.mitre.org/techniques/T1078)).

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing] (https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Country

Name
Austria
Name
Switzerland
Name
United Kingdom of Great Britain and Northern Ireland
Name
Germany
Name
United States of America

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.

StixFile

Value
7231546ee377738cbe9075791eb6e76b7bc163c1b91831e05e81b4756fff4028
3740e6b4d259efe6a72f503429fb67db96363935a29f7428ccab5b78fa9bee73
128820e1c5d62523f675042da9d1e11af3191217afe308bcc17e51ad8c2ece03
ecce34c0ba83120ccf1f8e1640cd867fbfeb490dbc8a41d1cf8c577d508819c3
db7df65f2699817fa3ebfb3ebef106a3801a96b9da1ba6d88e727a253ae34da6

External References

- https://otx.alienvault.com/pulse/64a3148d9d9a6d06237d3159
- https://www.threatfabric.com/blogs/anatsa-hits-uk-and-dach-with-new-campaign