Mar 29 2024

NETMANAGEIT

Intelligence Report

Android Malware Vultur Expands Its Wingspan

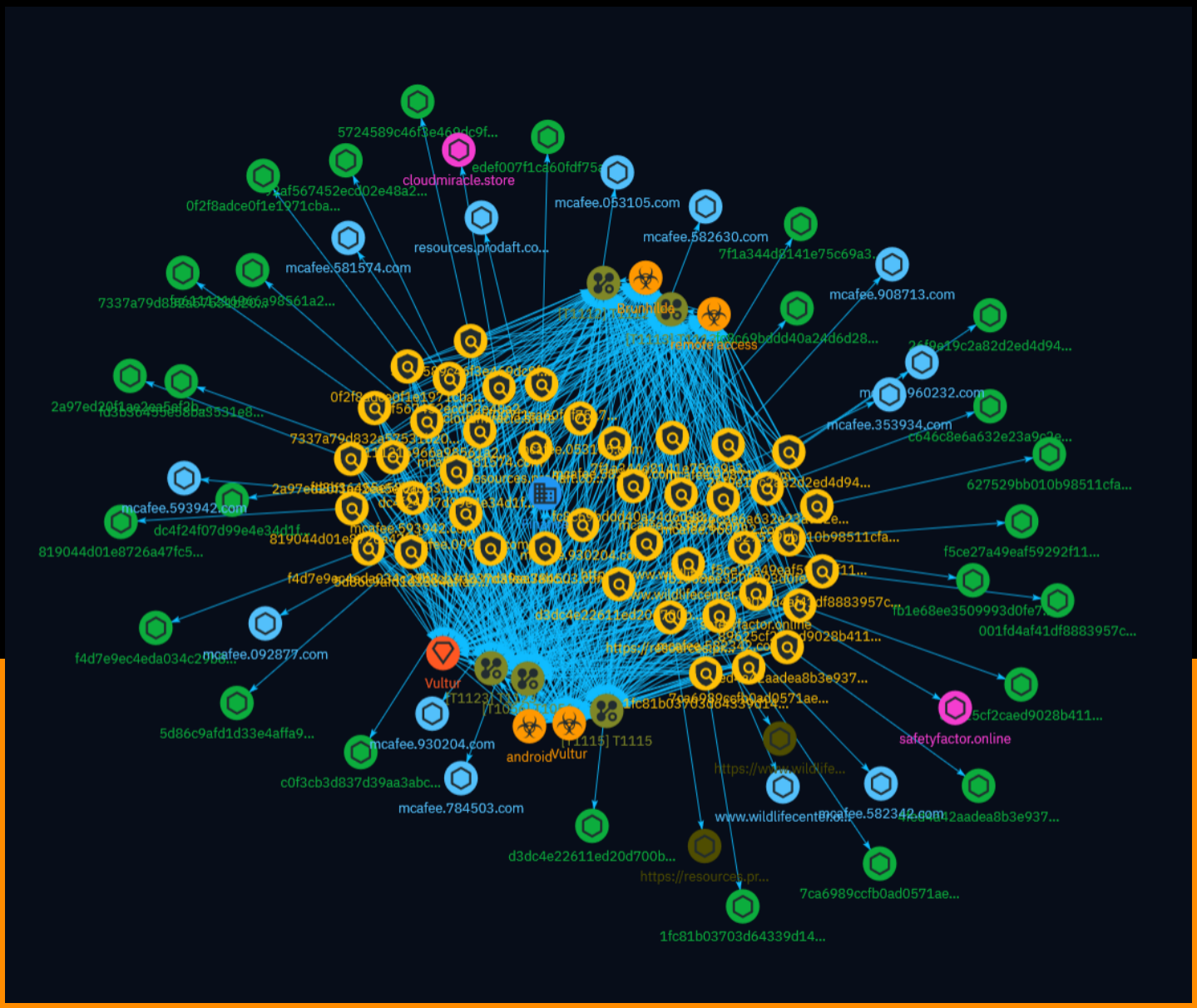

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The authors behind Android banking malware Vultur have added new features allowing more remote interaction with victim devices. Vultur encrypts C2 communication, uses multiple encrypted payloads, and disguises as legitimate apps. New features include file management, blocking apps, custom notifications, disabling lock screen. Vultur correlates to Android dropper Brunhilda.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
www.wildlifecenter.org
Pattern Type
stix
Pattern
[hostname:value = 'www.wildlifecenter.org']
Name
resources.prodaft.com
Pattern Type
stix
Pattern
[hostname:value = 'resources.prodaft.com']
Name
mcafee.960232.com

Pattern Type
stix
Pattern
[hostname:value = 'mcafee.960232.com']
Name
mcafee.930204.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.930204.com']
Name
mcafee.784503.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.784503.com']
Name
mcafee.908713.com

Pattern Type
stix
Pattern
[hostname:value = 'mcafee.908713.com']
Name
mcafee.593942.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.593942.com']
Name
mcafee.582630.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.582630.com']
Name
mcafee.582342.com

Pattern Type
stix
Pattern
[hostname:value = 'mcafee.582342.com']
Name
mcafee.581574.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.581574.com']
Name
mcafee.353934.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.353934.com']
Name
mcafee.092877.com

Pattern Type
stix
Pattern
[hostname:value = 'mcafee.092877.com']
Name
mcafee.053105.com
Pattern Type
stix
Pattern
[hostname:value = 'mcafee.053105.com']
Name
safetyfactor.online
Pattern Type
stix
Pattern
[domain-name:value = 'safetyfactor.online']
Name
https://www.wildlifecenter.org/vulture-facts

Pattern Type
stix
Pattern
[url:value = 'https://www.wildlifecenter.org/vulture-facts']
Name
cloudmiracle.store
Pattern Type
stix
Pattern
[domain-name:value = 'cloudmiracle.store']
Name
https://resources.prodaft.com/brunhilda-daas-malware-report
Pattern Type
stix
Pattern
[url:value = 'https://resources.prodaft.com/brunhilda-daas-malware-report']
Name
fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160']
Name
fb1e68ee3509993d0fe767b0372752d2fec8f5b0bf03d5c10a30b042a830ae1a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fb1e68ee3509993d0fe767b0372752d2fec8f5b0bf03d5c10a30b042a830ae1a']
Name
fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b']

Name

fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607']

Name

f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af']

Name

f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd2']

Name

edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21']

Name

d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a']

Name

dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e']

Name

c646c8e6a632e23a9c2e60590f012c7b5cb40340194cb0a597161676961b4de0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c646c8e6a632e23a9c2e60590f012c7b5cb40340194cb0a597161676961b4de0']

Name

c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d']

Name

92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d']

Name

89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2']

Name

819044d01e8726a47fc5970efc80ceddea0ac9bf7c1c5d08b293f0ae571369a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '819044d01e8726a47fc5970efc80ceddea0ac9bf7c1c5d08b293f0ae571369a9']

Name

7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c']

Name

7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd74']

Name

7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06']

Name

627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3']

Name

5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c']

Name

5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d']

Name

4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5']

Name

2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f']

Name

26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400']

Name

1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3']

Name

0f2f8adce0f1e1971cba5851e383846b68e5504679d916d7dad10133cc965851

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f2f8adce0f1e1971cba5851e383846b68e5504679d916d7dad10133cc965851']

Name

001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc']

Malware

Name
Brunhilda
Name
Vultur
Name
remote access
Name
android

Intrusion-Set

Name
Vultur

Attack-Pattern

Name
T1056
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
T1112
ID
T1112
Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Name

T1115

ID

T1115

Description

Adversaries may collect data stored in the clipboard from users copying information within or between applications. For example, on Windows adversaries can access clipboard data by using `clip.exe` or `Get-Clipboard`.(Citation: MSDN Clipboard)(Citation: clip_win_server)(Citation: CISA_AA21_200B) Additionally, adversaries may monitor then replace users' clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining_ruby_reversinglabs) macOS and Linux also have commands, such as `pbpaste`, to grab clipboard contents.(Citation: Operating with EmPyre)

Name

T1123

ID

T1123

Description

An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.

Name

T1113

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Sector

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

Hostname

Value
www.wildlifecenter.org
resources.prodaft.com
mcafee.960232.com
mcafee.930204.com
mcafee.908713.com
mcafee.784503.com
mcafee.593942.com
mcafee.582630.com
mcafee.582342.com
mcafee.581574.com
mcafee.353934.com
mcafee.092877.com
mcafee.053105.com

Domain-Name

Value
safetyfactor.online
cloudmiracle.store

Url

Value
https://www.wildlifecenter.org/vulture-facts
https://resources.prodaft.com/brunhilda-daas-malware-report

StixFile

Value
fd3b36455e58ba3531e8cce0326cce782723cc5d1cc0998b775e07e6c2622160
fc8c69bddd40a24d6d28fbf0c0d43a1a57067b19e6c3cc07e2664ef4879c221b
fb1e68ee3509993d0fe767b0372752d2fec8f5b0bf03d5c10a30b042a830ae1a
fa6111216966a98561a2af9e4ac97db036bcd551635be5b230995faad40b7607
f5ce27a49eaf59292f11af07851383e7d721a4d60019f3aceb8ca914259056af
f4d7e9ec4eda034c29b8d73d479084658858f56e67909c2ffedf9223d7ca9bd2
edef007f1ca60fdf75a7d5c5ffe09f1fc3fb560153633ec18c5ddb46cc75ea21
dc4f24f07d99e4e34d1f50de0535f88ea52cc62bfb520452bdd730b94d6d8c0e
d3dc4e22611ed20d700b6dd292ffddbc595c42453f18879f2ae4693a4d4d925a
c646c8e6a632e23a9c2e60590f012c7b5cb40340194cb0a597161676961b4de0
c0f3cb3d837d39aa3abccada0b4ecdb840621a8539519c104b27e2a646d7d50d
92af567452ecd02e48a2ebc762a318ce526ab28e192e89407cac9df3c317e78d
89625cf2caed9028b41121c4589d9e35fa7981a2381aa293d4979b36cf5c8ff2

819044d01e8726a47fc5970efc80ceddea0ac9bf7c1c5d08b293f0ae571369a9

7f1a344d8141e75c69a3c5cf61197f1d4b5038053fd777a68589ecdb29168e0c

7ca6989ccfb0ad0571aef7b263125410a5037976f41e17ee7c022097f827bd74

7337a79d832a57531b20b09c2fc17b4257a6d4e93fcaeb961eb7c6a95b071a06

627529bb010b98511cfa1ad1aaa08760b158f4733e2bbccfd54050838c7b7fa3

5d86c9afd1d33e4affa9ba61225aded26ecaeb01755eeb861bb4db9bbb39191c

5724589c46f3e469dc9f048e1e2601b8d7d1bafcc54e3d9460bc0adeeada022d

4fed4a42aadea8b3e937856318f9fbd056e2f46c19a6316df0660921dd5ba6c5

2a97ed20f1ae2ea5ef2b162d61279b2f9b68eba7cf27920e2a82a115fd68e31f

26f9e19c2a82d2ed4d940c2ec535ff2aba8583ae3867502899a7790fe3628400

1fc81b03703d64339d1417a079720bf0480fece3d017c303d88d18c70c7aabc3

0f2f8adce0f1e1971cba5851e383846b68e5504679d916d7dad10133cc965851

001fd4af41df8883957c515703e9b6b08e36fde3fd1d127b283ee75a32d575fc

External References

- https://blog.fox-it.com/2024/03/28/android-malware-vultur-expands-its-wingspan/
- https://otx.alienvault.com/pulse/6606b6e1722ebefb11263f04