Apr 01 2024

NETMANAGEIT

Intelligence Report

January 2024 review of virus activity on mobile devices

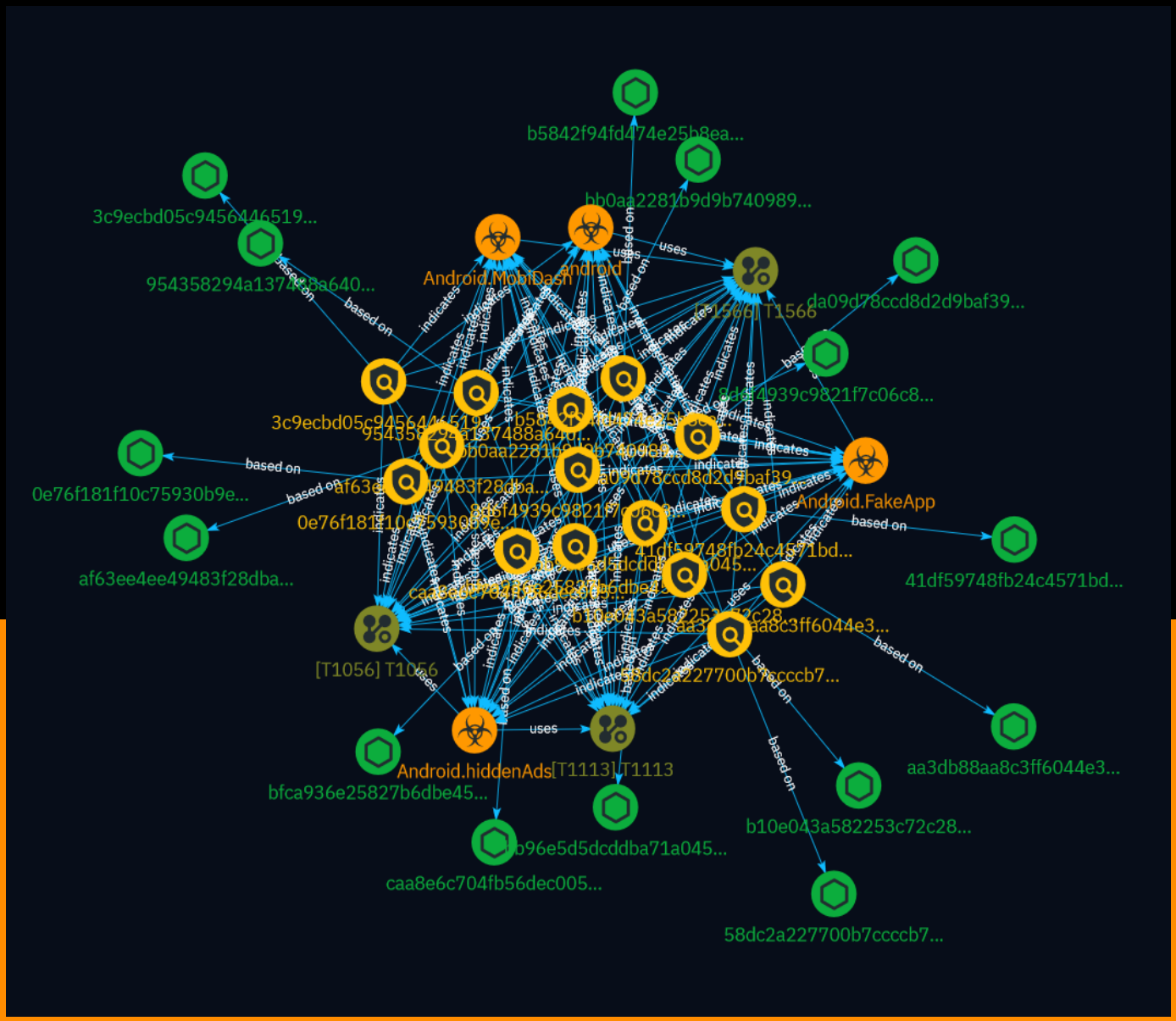

Table of contents

Overview

Entities

Observables

External References

Overview

Description

According to detection statistics collected by Dr.Web for Android anti-virus, in January 2024 adware trojans from Android.HiddenAds family maintained the lead in several detections on protected devices. Many Android malware families became more active.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

da09d78ccd8d2d9baf391ebedd03328d144beb0a4fc6374626774ba1f89170fe

Description

SHA256 of a2e5122c1660ffcf759b3ac3a74263924cf722ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da09d78ccd8d2d9baf391ebedd03328d144beb0a4fc6374626774ba1f89170fe']

Name

caa8e6c704fb56dec005da9c674670a3e3fc3e7b8f86daf379e983f31957cc4d

Description

SHA256 of e4a1485cb847f36dd6176096304901d99f231529

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'caa8e6c704fb56dec005da9c674670a3e3fc3e7b8f86daf379e983f31957cc4d']

Name

bb96e5d5dcddba71a045b3a0e5999c7f909721c2e6ce2d477b20c91fd95c0160

Description

SHA256 of 9496d9a804596dcb27290d508e46fc5a27a714a9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb96e5d5dcddba71a045b3a0e5999c7f909721c2e6ce2d477b20c91fd95c0160']

Name

bfca936e25827b6dbe457c103d1141468f96a26b2550335566a43b9594d9bf78

Description

SHA256 of e07fa9e81fe7718521ff1200ccf53f18e4f0d178

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfca936e25827b6dbe457c103d1141468f96a26b2550335566a43b9594d9bf78']

Name

bb0aa2281b9d9b7409893e1704fddf341ca50bf12b03b55349b9120c11162a44

Description

SHA256 of 9c97f4010f2b10bf00951216141b8aa5e67c86bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb0aa2281b9d9b7409893e1704fddf341ca50bf12b03b55349b9120c11162a44']

Name

b5842f94fd474e25b8ea59abe90f787ee40febfc89372cb9b1518a4bc0747dc8

Description

SHA256 of e9213c8e5327622d7cebc0232d1a6b751c53a54d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b5842f94fd474e25b8ea59abe90f787ee40febfc89372cb9b1518a4bc0747dc8']

Name

b10e043a582253c72c28f59966cc9dc96de47309ce844b20556b995b0cb99f2e

Description

SHA256 of 4e164cd0a8ad4e00102717957ee85320234bc7d3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b10e043a582253c72c28f59966cc9dc96de47309ce844b20556b995b0cb99f2e']

Name

af63ee4ee49483f28dba784be9d6522e24e470f059e3965ed268f146996ec66c

Description

SHA256 of 0f244a35f16ef045bb389a07c520d222e683561d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af63ee4ee49483f28dba784be9d6522e24e470f059e3965ed268f146996ec66c']

Name

aa3db88aa8c3ff6044e3461cf41b46d97be98229a023a147e5830b5ded85c627

Description

SHA256 of 48dd9d4b9c69c5c5f0fa387864d8ce1f68dea50f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aa3db88aa8c3ff6044e3461cf41b46d97be98229a023a147e5830b5ded85c627']

Name

8d6f4939c9821f7c06c834dc83bab53e48f400e8238803ff0c5c87cd767744e9

Description

SHA256 of c4a767a1cdc0e904f664b301ecfb279de2793c40

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8d6f4939c9821f7c06c834dc83bab53e48f400e8238803ff0c5c87cd767744e9']

Name

954358294a137488a64021141f5f01d7fb88d0df0149cb1bde504c4756f99390

Description

SHA256 of 25f6988e1a46566ac85463fd3f66d314b4441263

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '954358294a137488a64021141f5f01d7fb88d0df0149cb1bde504c4756f99390']

Name

58dc2a227700b7ccccb73bf643e4efb8c9212387401683929b6c62b7dfabc9b0

Description

SHA256 of e1b517dfacaa735014331dca8dfe8099ea74c8e5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '58dc2a227700b7ccccb73bf643e4efb8c9212387401683929b6c62b7dfabc9b0']

Name

3c9ecbd05c94564465190cd717c94dbfaea7183b955cdb90cbc95c800d68ba7a

Description

SHA256 of decd232709a4878f0b6b1cb5cfb28d3b8b471d3e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c9ecbd05c94564465190cd717c94dbfaea7183b955cdb90cbc95c800d68ba7a']

Name

41df59748fb24c4571bddf2541a8fe7738eee82b4f4f48f8190f2dffb92f1c0f

Description

SHA256 of b176d98d97df68855ca8fba1b2f2ac2274b03397

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41df59748fb24c4571bddf2541a8fe7738eee82b4f4f48f8190f2dffb92f1c0f']

Name

0e76f181f10c75930b9ebe9aec5e418a2fbc668295c4919de1d8aad9cb79e522

Description

ALF:AndroidOSSuspiciousPerms.A SHA256 of 6ca09dd7292d2ea97325c1aa4217dc3232e84ca7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0e76f181f10c75930b9ebe9aec5e418a2fbc668295c4919de1d8aad9cb79e522']

Malware

Name
Android.MobiDash
Name
Android.FakeApp
Name
Android.hiddenAds
Name
android

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
T1566
ID
T1566
Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

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)

StixFile

Value
da09d78ccd8d2d9baf391ebedd03328d144beb0a4fc6374626774ba1f89170fe
caa8e6c704fb56dec005da9c674670a3e3fc3e7b8f86daf379e983f31957cc4d
bfca936e25827b6dbe457c103d1141468f96a26b2550335566a43b9594d9bf78
bb0aa2281b9d9b7409893e1704fddf341ca50bf12b03b55349b9120c11162a44
bb96e5d5dcddba71a045b3a0e5999c7f909721c2e6ce2d477b20c91fd95c0160
b5842f94fd474e25b8ea59abe90f787ee40febfc89372cb9b1518a4bc0747dc8
b10e043a582253c72c28f59966cc9dc96de47309ce844b20556b995b0cb99f2e
af63ee4ee49483f28dba784be9d6522e24e470f059e3965ed268f146996ec66c
3c9ecbd05c94564465190cd717c94dbfaea7183b955cdb90cbc95c800d68ba7a
aa3db88aa8c3ff6044e3461cf41b46d97be98229a023a147e5830b5ded85c627
954358294a137488a64021141f5f01d7fb88d0df0149cb1bde504c4756f99390
8d6f4939c9821f7c06c834dc83bab53e48f400e8238803ff0c5c87cd767744e9
58dc2a227700b7ccccb73bf643e4efb8c9212387401683929b6c62b7dfabc9b0

0e76f181f10c75930b9ebe9aec5e418a2fbc668295c4919de1d8aad9cb79e522

41df59748fb24c4571bddf2541a8fe7738eee82b4f4f48f8190f2dffb92f1c0f

External References

- https://otx.alienvault.com/pulse/660a7b2d9f45d7a70b1a8fc1