Apr 19 2024

NETMANAGEIT

Intelligence Report

Analysis of the SoumniBot Android banker

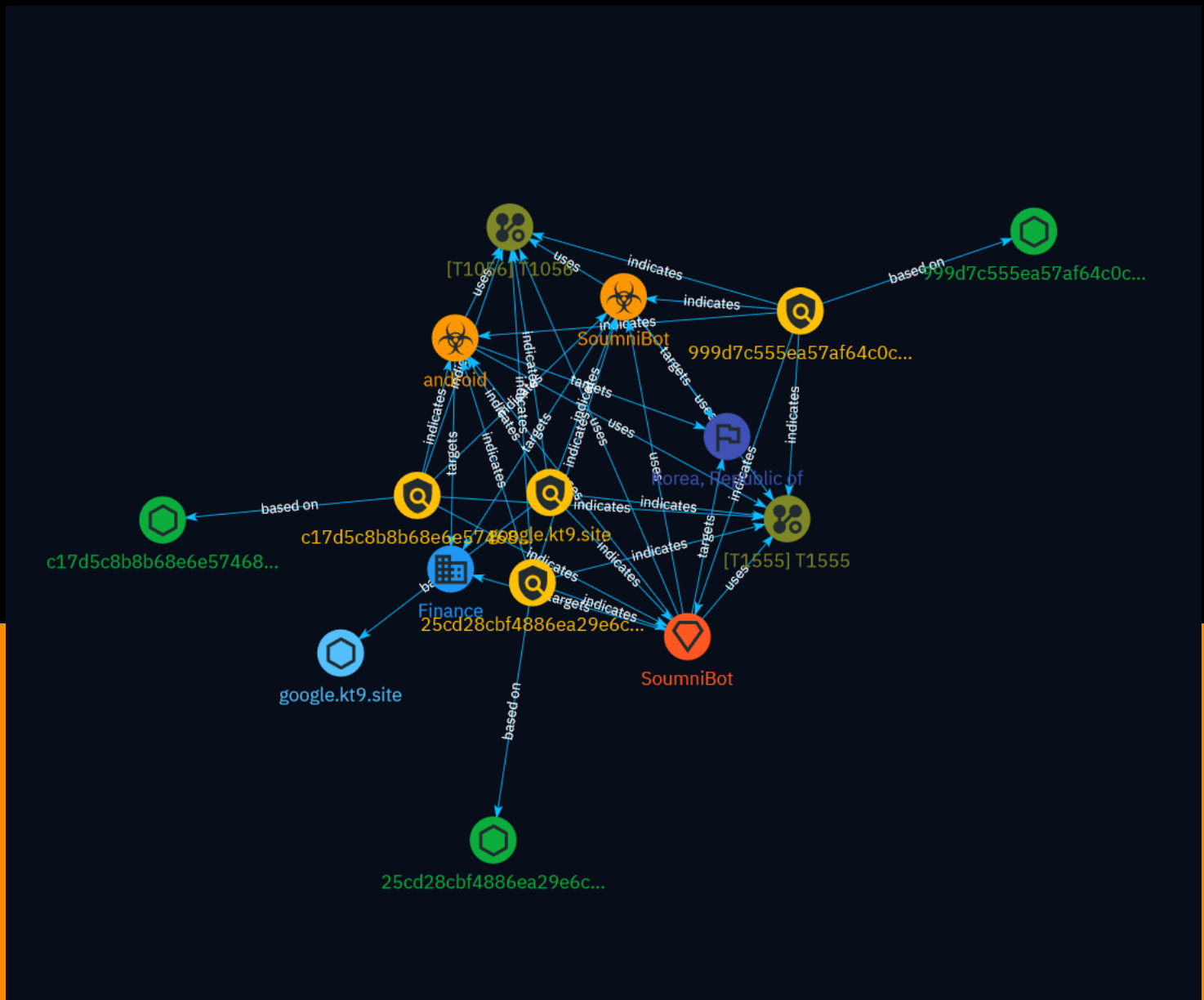

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new Android banking Trojan called SoumniBot has been discovered targeting Korean users. The malware uses unique obfuscation techniques to evade detection, including exploiting bugs in how the Android manifest file is parsed. Once installed, SoumniBot steals sensitive data like contacts, messages, and banking certificates, and can receive commands from a C2 server.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
google.kt9.site
Pattern Type
stix
Pattern
[hostname:value = 'google.kt9.site']
Name
c17d5c8b8b68e6e574688e93b9c80e4cdcb15162614f465be0baecec0f261974
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'c17d5c8b8b68e6e574688e93b9c80e4cdcb15162614f465be0baecec0f261974']
Name

999d7c555ea57af64c0cba26a27704ee5229b4151571bb9c12c6aa2089a7a61c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '999d7c555ea57af64c0cba26a27704ee5229b4151571bb9c12c6aa2089a7a61c']

Name

25cd28cbf4886ea29e6c378dbcdc3b077c2b33a8c58053bbaefb368f4df11529

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25cd28cbf4886ea29e6c378dbcdc3b077c2b33a8c58053bbaefb368f4df11529']

Malware

Name
SoumniBot

Name
android

Intrusion-Set

Name
SoumniBot

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
T1555
ID
T1555
Description

Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Country

Name
Korea, Republic of

Sector

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

Hostname

Value
google.kt9.site

StixFile

Value
c17d5c8b8b68e6e574688e93b9c80e4cdcb15162614f465be0baecec0f261974
999d7c555ea57af64c0cba26a27704ee5229b4151571bb9c12c6aa2089a7a61c
25cd28cbf4886ea29e6c378dbcdc3b077c2b33a8c58053bbaefb368f4df11529

External References

- https://securelist.com/soumnibot-android-banker-obfuscates-app-manifest/112334/
- https://otx.alienvault.com/pulse/66202dedc08e0a0473dba616