Oct 05 2023

NETMANAGEIT

Intelligence Report

Let's dig deeper: dissecting the new Android Trojan GoldDigger

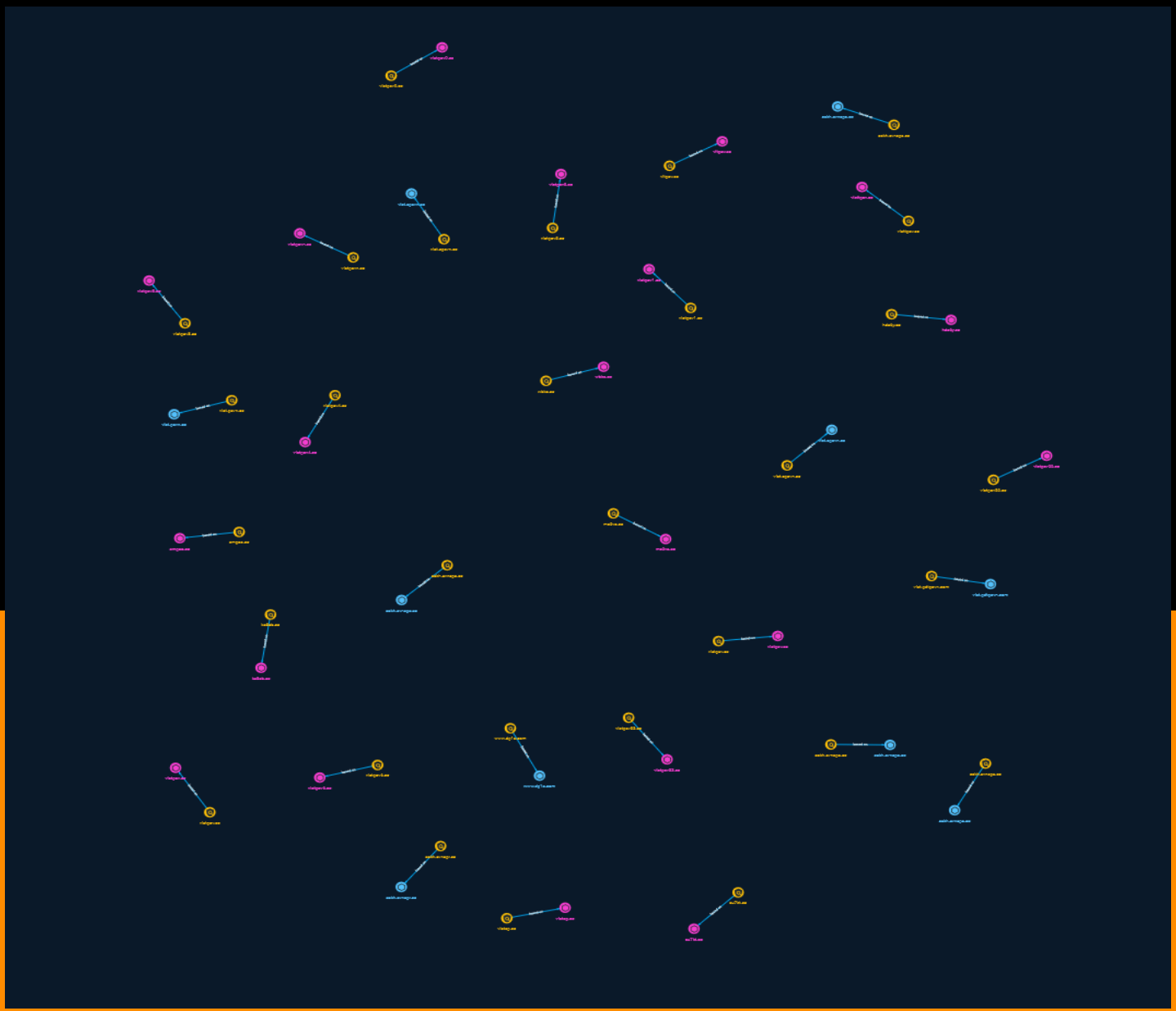

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Group-IB has published a new blog on GoldDigger, a banking trojan that exploits accessibility services or permissions to carry out fraudulent activities.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
viet.govn.cc
Pattern Type
stix
Pattern
[hostname:value = 'viet.govn.cc']
Name
smgeo.cc
Pattern Type
stix
Pattern
[domain-name:value = 'smgeo.cc']
Name
vietgov5.cc

Pattern Type
stix
Pattern
[domain-name:value = 'vietgov5.cc']
Name
viet.gdtgovn.com
Pattern Type
stix
Pattern
[hostname:value = 'viet.gdtgovn.com']
Name
www.dg1e.com
Pattern Type
stix
Pattern
[hostname:value = 'www.dg1e.com']
Name
viet.cgovn.cc

Pattern Type
stix
Pattern
[hostname:value = 'viet.cgovn.cc']
Name
viet.egovn.cc
Pattern Type
stix
Pattern
[hostname:value = 'viet.egovn.cc']
Name
vitgov.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vitgov.cc']
Name
cskh.evnspc.cc

Pattern Type
stix
Pattern
[hostname:value = 'cskh.evnspc.cc']
Name
vietgov33.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov33.cc']
Name
vietgovn.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgovn.cc']
Name
cskh.evnspo.cc

Pattern Type
stix
Pattern
[hostname:value = 'cskh.evnspo.cc']
Name
ks8cb.cc
Pattern Type
stix
Pattern
[domain-name:value = 'ks8cb.cc']
Name
vietgov1.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov1.cc']
Name
vietcp.cc

Pattern Type
stix
Pattern
[domain-name:value = 'vietcp.cc']
Name
vietgov4.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov4.cc']
Name
zu7kt.cc
Pattern Type
stix
Pattern
[domain-name:value = 'zu7kt.cc']
Name
vietgov3.cc

Pattern Type
stix
Pattern
[domain-name:value = 'vietgov3.cc']
Name
viettgov.cc
Pattern Type
stix
Pattern
[domain-name:value = 'viettgov.cc']
Name
vietgov6.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov6.cc']
Name
ms2ve.cc

Pattern Type
stix
Pattern
[domain-name:value = 'ms2ve.cc']
Name
vietgov22.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov22.cc']
Name
vietgav.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgav.cc']
Name
hds6y.cc

Pattern Type
stix
Pattern
[domain-name:value = 'hds6y.cc']
Name
cskh.evnspr.cc
Pattern Type
stix
Pattern
[hostname:value = 'cskh.evnspr.cc']
Name
wbke.cc
Pattern Type
stix
Pattern
[domain-name:value = 'wbke.cc']
Name
cskh.evnspa.cc

Pattern Type
stix
Pattern
[hostname:value = 'cskh.evnspa.cc']
Name
vietgov.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov.cc']
Name
vietgov0.cc
Pattern Type
stix
Pattern
[domain-name:value = 'vietgov0.cc']
Name
cskh.evnspe.cc

Pattern Type
stix
Pattern
[hostname:value = 'cskh.evnspe.cc']

Domain-Name

Value
vietgov4.cc
vitgov.cc
vietcp.cc
vietgov3.cc
vietgov22.cc
vietgov6.cc
vietgov5.cc
ms2ve.cc
smgeo.cc
wbke.cc
zu7kt.cc
vietgov1.cc
vietgav.cc

vietgov.cc

viettgov.cc

vietgov33.cc

vietgovn.cc

hds6y.cc

ks8cb.cc

vietgov0.cc

Hostname

Value
cskh.evnspo.cc
cskh.evnspc.cc
viet.egovn.cc
www.dg1e.com
viet.cgovn.cc
viet.gdtgovn.com
cskh.evnspr.cc
cskh.evnspa.cc
cskh.evnspe.cc
viet.govn.cc

External References

- https://otx.alienvault.com/pulse/651ec229a61c1166a2a3f456
- https://www.group-ib.com/blog/golddigger-fraud-matrix/