Feb 15 2024

NETMANAGEIT

Intelligence Report

Face Off

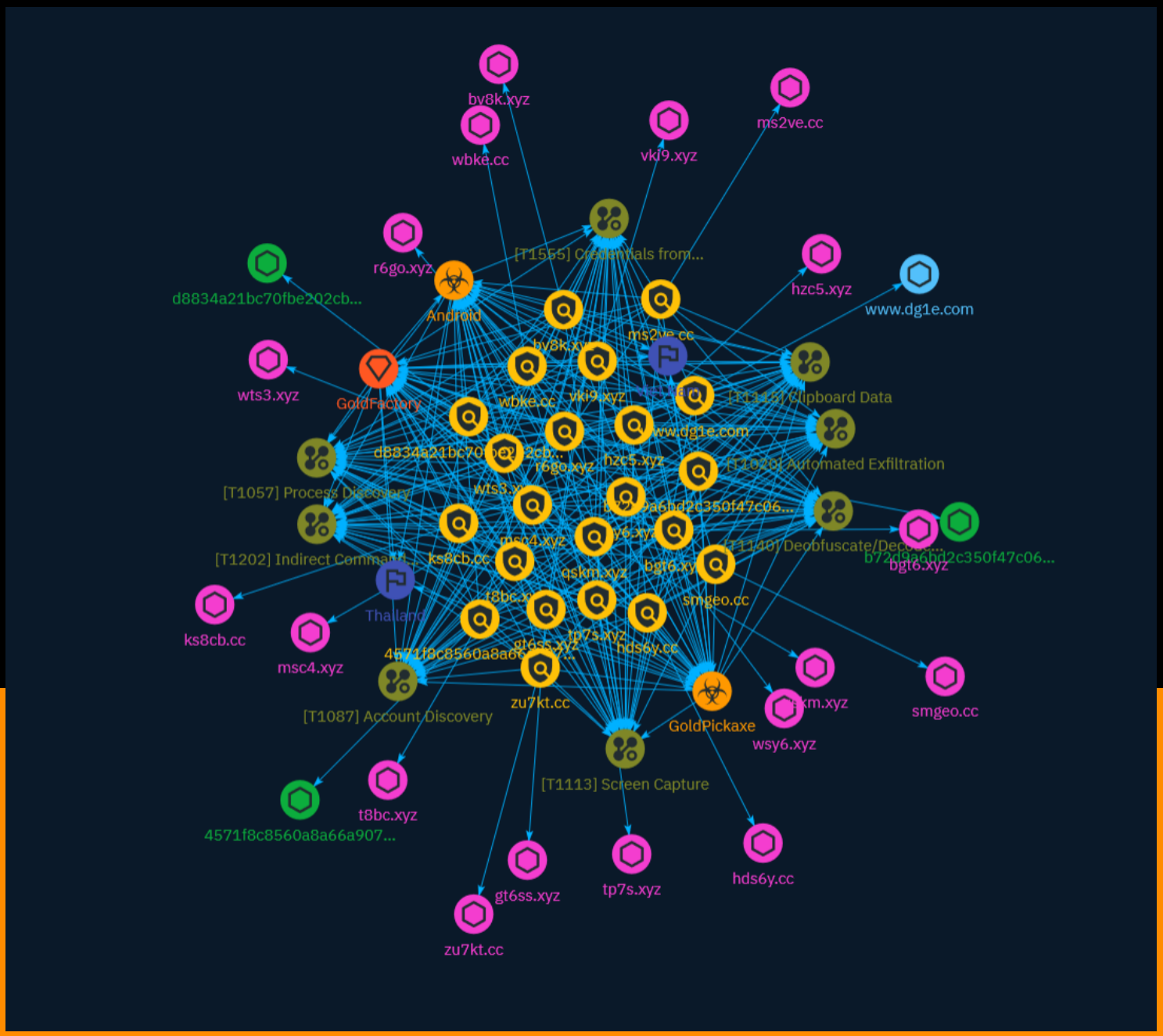

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In October 2023, Group-IB researchers released a report about a previously unknown Android Trojan specifically targeting more than 50 financial institutions in Vietnam. We named it GoldDigger as there was an activity named GoldActivity contained within the APK. Following the initial discovery of the Trojan, Group-IB's Threat Intelligence unit has been constantly monitoring this evolving threat and unearthed an entire cluster of aggressive banking Trojans actively targeting the Asia-Pacific (APAC) region.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
wts3.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'wts3.xyz']
Name
wsy6.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'wsy6.xyz']
Name
vki9.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'vki9.xyz']
Name
tp7s.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'tp7s.xyz']
Name
t8bc.xyz
Pattern Type
stix
Pattern
[domain-name:value = 't8bc.xyz']
Name
r6go.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'r6go.xyz']
Name
qskm.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'qskm.xyz']
Name
msc4.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'msc4.xyz']
Name
hzc5.xyz

Pattern Type
stix
Pattern
[domain-name:value = 'hzc5.xyz']
Name
gt6ss.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'gt6ss.xyz']
Name
bv8k.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'bv8k.xyz']
Name
bgt6.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'bgt6.xyz']

Name

d8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b7276b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b7276b']

Name

b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad6631875

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad6631875']

Name

4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3df']

Name

www.dg1e.com

Pattern Type

stix

Pattern

[hostname:value = 'www.dg1e.com']

Name

zu7kt.cc

Pattern Type

stix

Pattern

[domain-name:value = 'zu7kt.cc']

Name
wbke.cc
Pattern Type
stix
Pattern
[domain-name:value = 'wbke.cc']
Name
smgeo.cc
Pattern Type
stix
Pattern
[domain-name:value = 'smgeo.cc']
Name
ks8cb.cc
Pattern Type
stix
Pattern
[domain-name:value = 'ks8cb.cc']

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

Malware

Name
GoldPickaxe

Name
Android

Intrusion-Set

Name
GoldFactory

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

Automated Exfiltration

ID

T1020

Description

Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection. When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) and [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).

Name

Account Discovery

ID

T1087

Description

Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment. This information can help adversaries determine which accounts exist, which can aid in follow-on behavior such as brute-forcing, spear-phishing attacks, or account takeovers (e.g., [Valid Accounts](https://attack.mitre.org/techniques/T1078)). Adversaries may use several methods to enumerate accounts, including abuse of existing tools, built-in commands, and potential misconfigurations that leak account names and roles or permissions in the targeted environment. For examples, cloud environments typically provide easily accessible interfaces to obtain user lists. On hosts, adversaries can use default [PowerShell](https://attack.mitre.org/techniques/T1059/001) and other command line functionality to identify accounts. Information about email addresses and accounts may also be extracted by searching an infected system's files.

Name

Credentials from Password Stores

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.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/

encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Indirect Command Execution

ID

T1202

Description

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking [cmd](https://attack.mitre.org/software/S0106). For example, [Forfiles](https://attack.mitre.org/software/S0193), the Program Compatibility Assistant (pcalua.exe), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), Run window, or via scripts. (Citation: VectorSec ForFiles Aug 2017) (Citation: Evi1cg Forfiles Nov 2017) Adversaries may abuse these features for [Defense Evasion](https://attack.mitre.org/tactics/TA0005), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of [cmd](https://attack.mitre.org/software/S0106) or file extensions more commonly associated with malicious payloads.

Name

Clipboard Data

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

Screen Capture

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)

Country

Name
Viet Nam

Name
Thailand

Domain-Name

Value
wts3.xyz
wsy6.xyz
tp7s.xyz
vki9.xyz
t8bc.xyz
r6go.xyz
qskm.xyz
msc4.xyz
hzc5.xyz
gt6ss.xyz
bv8k.xyz
bgt6.xyz
zu7kt.cc

wbke.cc

smgeo.cc

ks8cb.cc

ms2ve.cc

hds6y.cc

StixFile

Value
d8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b7276b
b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad6631875
4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3df

Hostname

Value
www.dg1e.com

External References

- https://otx.alienvault.com/pulse/65ce2fbf2d10c7204d57dec2