Jul 03 2023

NETMANAGEIT

Intelligence Report

Malvertising Used as Entry Vector for BlackCat, Actors Also Leverage SpyBoy Terminator

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Advertising platforms like Google Ads enable businesses to display advertisements to target audiences to boost traffic and increase sales. Malware distributors abuse the same functionality in a technique known as malvertising, where chosen keywords are hijacked to display malicious ads that lure unsuspecting search engine users into downloading certain types of malware.

Confidence

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

15 / 100

Attack-Pattern

Name
TA0029
ID
TA0029
Name
TA0028
ID
TA0028
Name
Masquerade as Legitimate Application
ID
T1444
Description
An adversary could distribute developed malware by masquerading the malware as a legitimate application. This can be done in two different ways: by embedding the malware

in a legitimate application, or by pretending to be a legitimate application. Embedding the malware in a legitimate application is done by downloading the application, disassembling it, adding the malicious code, and then re-assembling it.(Citation: Zhou) The app would appear to be the original app, but would contain additional malicious functionality. The adversary could then publish the malicious application to app stores or use another delivery method. Pretending to be a legitimate application relies heavily on lack of scrutinization by the user. Typically, a malicious app pretending to be a legitimate one will have many similar details as the legitimate one, such as name, icon, and description. (Citation: Palo Alto HenBox) Malicious applications may also masquerade as legitimate applications when requesting access to the accessibility service in order to appear as legitimate to the user, increasing the likelihood that the access will be granted.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Remote System Discovery

ID

T1018

Description

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order

to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Indicator

Name
13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe']
Name
25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c']
Name

3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce']

Name

21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839']

Name

bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef']

Name

8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5']

Name

c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe']

Name

9e5205865a23c4b8a60935a3fdf1f203286b3e240940bfbeaf0101b00cfc68d6

Description
SHA256 of aae1b17891ec215a0e238f881be862b4f598e46c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9e5205865a23c4b8a60935a3fdf1f203286b3e240940bfbeaf0101b00cfc68d6']
Name
4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a']

StixFile

Value
3ce4ed3c7bd97b84045bdcfc84d3772b4c3a29392a9a2eee9cc17d8a5e5403ce
c7a5a4fb4f680974f3334f14e0349522502b9d5018ec9be42beec5fa8c1597fe
8859a09fdc94d7048289d2481ede4c98dc342c0a0629cbcef2b91af32d52acb5
25467df66778077cc387f4004f25aa20b1f9caec2e73b9928ec4fe57b6a2f63c
bacbe893b668a63490d2ad045a69b66c96dcacb500803c68a9de6cca944affef
13090722ba985bafcccfb83795ee19fd4ab9490af1368f0e7ea5565315c067fe
21e7bcc03c607e69740a99d0e9ae8223486c73af50f4c399c8d30cce4d41e839
4a4d20d107ee8e23ce1ebe387854a4bfe766fc99f359ed18b71d3e01cb158f4a
9e5205865a23c4b8a60935a3fdf1f203286b3e240940bfbeaf0101b00cfc68d6

External References

- https://otx.alienvault.com/pulse/64a31b647e34ec2626fc3c26
- https://www.trendmicro.com/en_us/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html
- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-leverage-spyboy-terminator-/Malvertising_IOCs.txt