Oct 31 2023

NETMANAGEIT

Intelligence Report

Malvertising via Dynamic Search Ads delivers malware bonanza

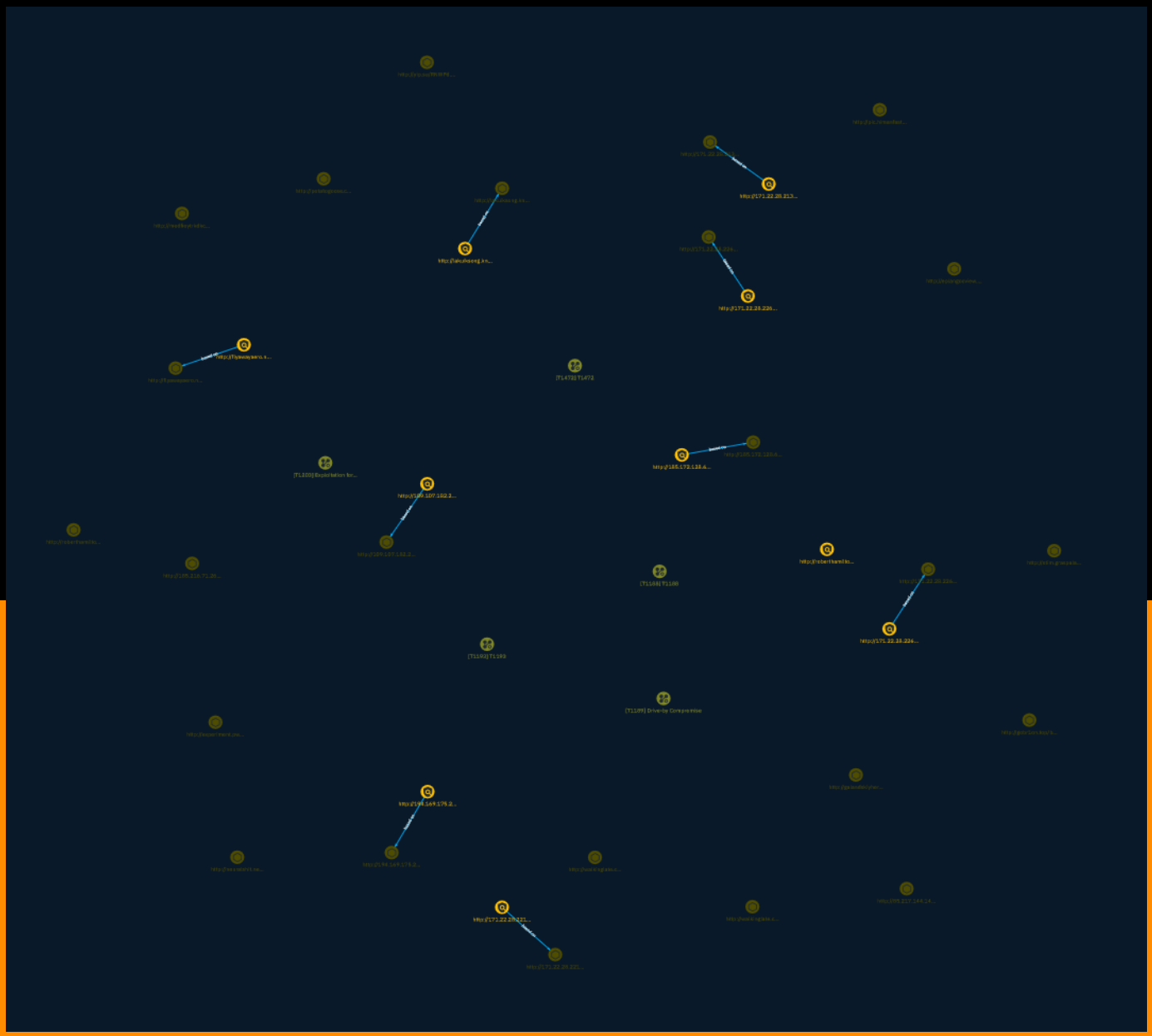

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Most, if not all malvertising incidents result from a threat actor either injecting code within an existing ad, or intentionally creating one.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
T1188
ID
T1188
Name
T1193
ID
T1193
Name
T1472
ID
T1472
Name
Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Exploitation for Client Execution

ID

T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Indicator

Name

http://171.22.28.226/download/WWW14_64.exe

Description

Threat: malware_download - Reporter: zbetcheckin - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://171.22.28.226/download/WWW14_64.exe']

Name

http://194.169.175.233/setup.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://194.169.175.233/setup.exe']

Name

http://lakuiksong.known.co.ke/netTimer.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://lakuiksong.known.co.ke/netTimer.exe']

Name

http://roberthamilton.top/timeSync.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://roberthamilton.top/timeSync.exe']

Name

http://185.172.128.69/newumma.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://185.172.128.69/newumma.exe']

Name

http://109.107.182.2/race/bus50.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://109.107.182.2/race/bus50.exe']

Name

http://171.22.28.226/download/Services.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type

stix

Pattern

[url:value = 'http://171.22.28.226/download/Services.exe']

Name

http://flyawayaero.net/baf14778c246e15550645e30ba78ce1c.exe

Description

Threat: malware_download - Reporter: zbetcheckin - Status: offline

Pattern Type

stix

Pattern

[url:value = 'http://flyawayaero.net/baf14778c246e15550645e30ba78ce1c.exe']

Name

http://171.22.28.213/3.exe

Description

Threat: malware_download - Reporter: andretavare5 - Status: online

Pattern Type
stix
Pattern
[url:value = 'http://171.22.28.213/3.exe']
Name
http://171.22.28.221/files/Ads.exe
Description
Threat: malware_download - Reporter: andretavare5 - Status: online
Pattern Type
stix
Pattern
[url:value = 'http://171.22.28.221/files/Ads.exe']

Url

Value
http://lakuiksong.known.co.ke/netTimer.exe
http://galandskiyher5.com/downloads/toolspub1.exe
http://185.216.71.26/download/k/KL.exe
http://eplangocview.com/wp-download/File.7z
http://walkinglate.com/watchdog/watchdog.exe
http://potatogoose.com/1298d7c8d865df39937f1b0eb46c0e3f/baf14778c246e15550645e30ba78ce1c.exe
http://stim.graspalace.com/order/tuc19.exe
http://experiment.pw/setup294.exe
http://171.22.28.226/download/WWW14_64.exe
http://walkinglate.com/uninstall.exe
http://flyawayaero.net/baf14778c246e15550645e30ba78ce1c.exe
http://185.172.128.69/newumma.exe

http://194.169.175.233/setup.exe

http://yip.su/RNWPd.exe

http://gobr1on.top/build.exe

http://109.107.182.2/race/bus50.exe

http://pic.himanfast.com/order/tuc15.exe

http://171.22.28.221/files/Ads.exe

http://medfioytrkdkcodlskeej.net/987123.exe

http://171.22.28.226/download/Services.exe

http://neuralshit.net/1298d7c8d865df39937f1b0eb46c0e3f/7725eaa6592c80f8124e769b4e8a07f7.exe

http://171.22.28.213/3.exe

http://85.217.144.143/files/My2.exe

http://roberthamilton.top/timeSync.exe

External References

- https://otx.alienvault.com/pulse/6540ba5fa326e950af31893b
- https://www.malwarebytes.com/blog/threat-intelligence/2023/10/malvertising-via-dynamic-search-ads-delivers-malware-bonanza