ID: 756300
Sample Name: #U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html
Cookbook: defaultwindowshtmlcookbook.jbs
Time: 00:19:55
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report #U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
HTML 3
Sigma Signatures 3
Snort Signatures 4
Joe Sandbox Signatures 4
Phishing 4
System Summary 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted URLs 7
World Map of Contacted IPs 7
Public IPs 8
Private 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 10
Static File Info 10
General 10
Network Behavior 10
Network Port Distribution 10
TCP Packets 10
UDP Packets 12
DNS Queries 12
DNS Answers 13
HTTP Request Dependency Graph 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: chrome.exePID: 2516, Parent PID: 4704 15
General 15
File Activities 15
Registry Activities 15
Analysis Process: chrome.exePID: 5208, Parent PID: 2516 15
General 15
File Activities 16
Analysis Process: chrome.exePID: 5552, Parent PID: 4704 16
General 16
Registry Activities 16
Disassembly 16

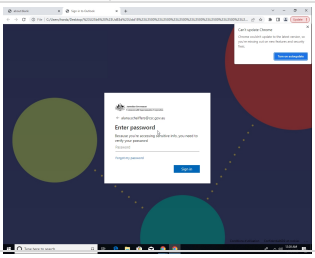
Windows Analysis Report

#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment...

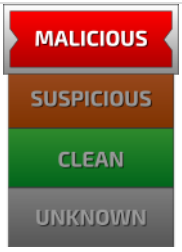
Overview

General Information

Sample Name:	#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html
Analysis ID:	756300
MD5:	c8a579e165f7b8..
SHA1:	b6c3f4b86d8658..
SHA256:	95d40b7fb897e1..
Infos:	



Detection



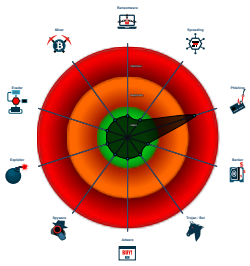
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected HtmlPhish10
- HTML document with suspicious title
- Phishing site detected (based on im…
- JA3 SSL client fingerprint seen in co…
- IP address seen in connection with …

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 2516 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5208 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1816,i,18019605785344620809,16696382858066997968,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 5552 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
61093.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

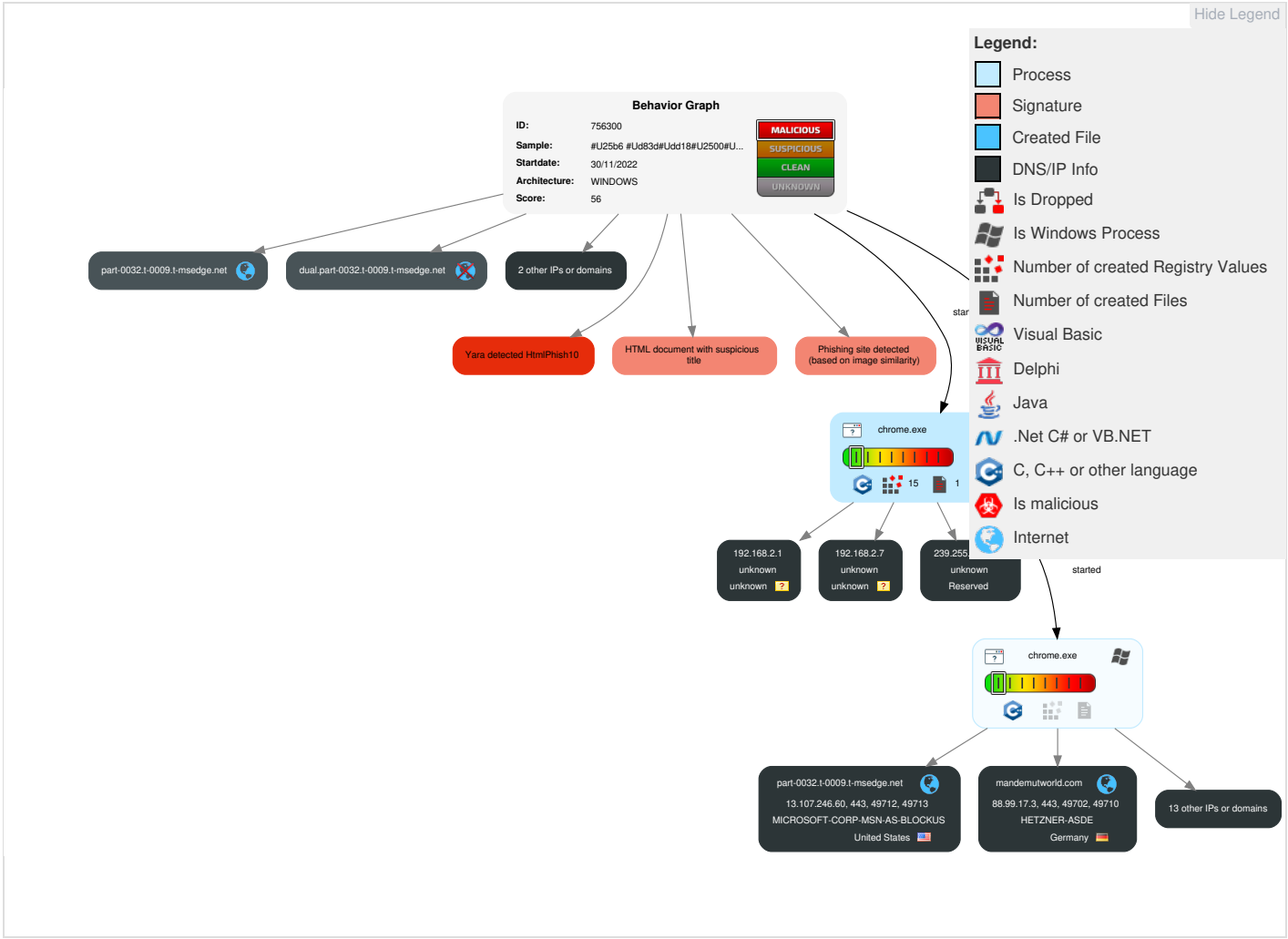
System Summary

HTML document with suspicious title

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	4 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

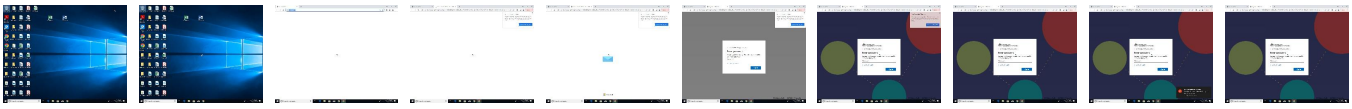
Behavior Graph

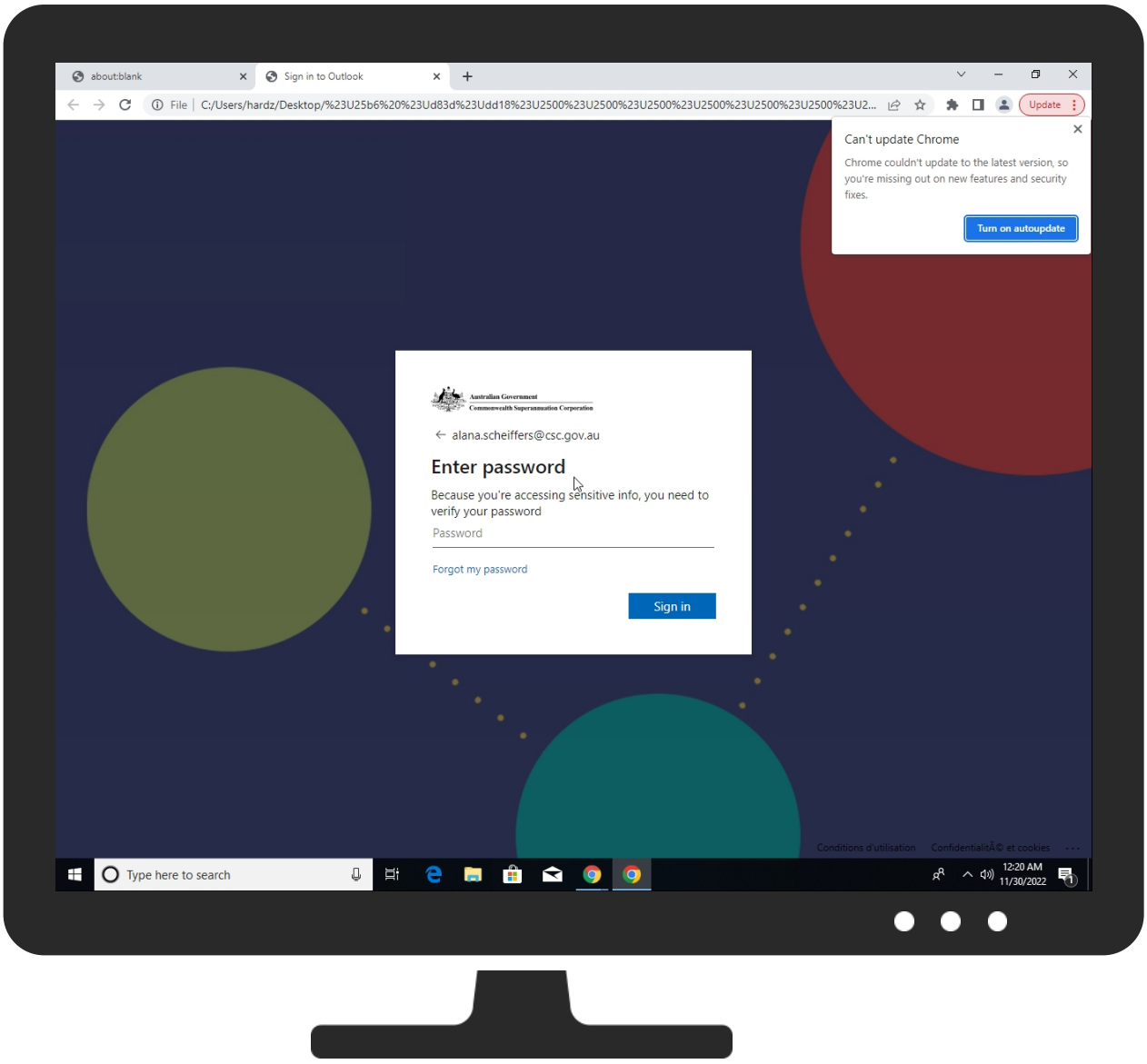


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauthimages.net/81d6b03a-itah-k4j9-s88y6um2sckipyinyzz2ai-jemkeyiq/logintenantbranding/0/bannerlogo?ts=637758174410899401	0%	Avira URL Cloud	safe	
http://https://mandemutworld.com/onlne/aa/5ac0e99.php	0%	Avira URL Cloud	safe	
http://https://mandemutworld.com/onlne/aa/admin/js/mj.php?ar=d29yZA==	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msauthimages.net/81d6b03a-itah-k4j9-s88y6um2sckipyinyzz2ai-jemkeyiq/logintenantbranding/0/illustration?ts=637758160209820938	0%	Avira URL Cloud	safe	

Domains and IPs

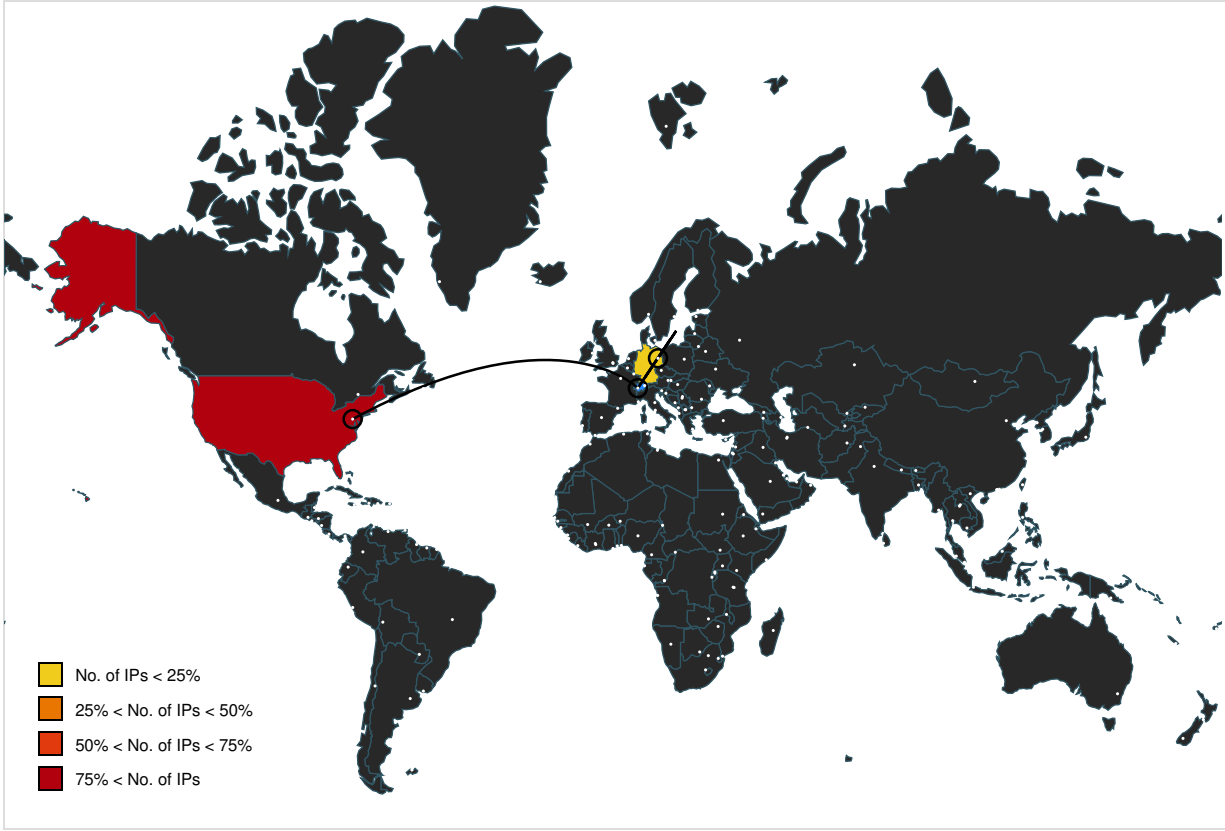
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
mandemutworld.com	88.99.17.3	true	false		unknown
cdnjs.cloudflare.com	104.17.24.14	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high
part-0032.t-0009.t-msedge.net	13.107.246.60	true	false		unknown
cs1227.wpc.alphacdn.net	192.229.221.185	true	false		unknown
www.google.com	172.217.168.68	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
cs1025.wpc.upsiloncdn.net	152.199.23.72	true	false		unknown
aadcdn.msauthimages.net	unknown	unknown	false		unknown
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
cdn.jsdelivr.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/css/font-awesome.min.css	false		high
http://https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.css	false		high
file:///C:/Users/user/Desktop/%23U25b6%20%23Ud83d%23Udd18%23U2500%23U2500%23U2500%23U2500%23U2500%23U2500%23U2500%20126%20Voice-Attchment.919-340-XX.html	true		low
http://https://mandemutworld.com/onlne/aa/5ac0e99.php	false	• Avira URL Cloud: safe	unknown
http://https://maxcdn.bootstrapcdn.com/font-awesome/4.7.0/fonts/fontawesome-webfont.woff2?v=4.7.0	false		high
http://https://mandemutworld.com/onlne/aa/admin/js/mj.php?ar=d29yZA==	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauthimages.net/81d6b03a-itah-k4j9-s88y6um2sckipyinyzz2ai-jemkeyiq/logintenantbranding/0/bannerlogo?ts=637758174410899401	false	• Avira URL Cloud: safe	unknown
http://https://aadcdn.msauthimages.net/81d6b03a-itah-k4j9-s88y6um2sckipyinyzz2ai-jemkeyiq/logintenantbranding/0/illustration?ts=637758160209820938	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.17.24.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
152.199.23.72	cs1025.wpc.upsiloncdn.net	United States		15133	EDGECASTUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
13.107.246.60	part-0032.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.99.17.3	mandemutworld.com	Germany		24940	HETZNER-ASDE	false
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
192.229.221.185	cs1227.wpc.alphacdn.net	United States		15133	EDGECASTUS	false

Private

IP
192.168.2.1
192.168.2.7
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756300
Start date and time:	2022-11-30 00:19:55 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.phis.winHTML@29/0@11/13
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .html • Browse: https://privacy.microsoft.com/fr/privacystatement

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.220.29, 93.184.221.240, 209.197.3.8, 67.27.158.254, 8.248.113.254, 8.238.190.126, 8.238.191.126, 67.27.157.126, 172.217.168.67, 69.16.175.10, 69.16.175.42, 104.16.88.20, 104.16.86.20, 104.16.89.20, 104.16.87.20, 104.16.85.20, 34.104.35.123
- Excluded domains from analysis (whitelisted): logincdn.msauth.net, fg.download.windowsupdate.com.c.footprint.net, cds.s5x3j6q5.hwcdn.net, cdn.jsdelivr.net.cdn.cloudflare.net, cs9.wac.phicdn.net, clientservices.googleapis.com, wu.azureedge.net, ocsp.digicert.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, aadcdn.azureedge.net, aadcdn.ec.azureedge.net, hlb.apr-52dd2-0.edgecastdns.net, update.googleapis.com, fs.microsoft.com, aadcdnoriginwus2.azureedge.net, wu.ec.azureedge.net, lgincdnvzeuno.ec.azureedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, aadcdn.msauth.net, wu-bg-shim.trafficmanager.net, firstparty-azurefd-prod.trafficmanager.net, lgincdnvzeuno.azureedge.net, edgedl.me.gvt1.com, lgincdn.trafficmanager.net, aadcdnoriginwus2.afd.azureedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

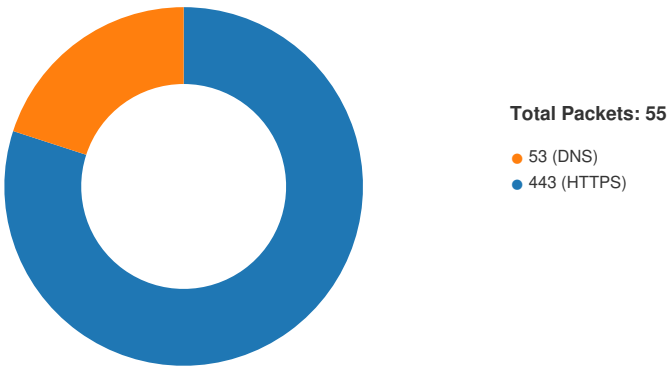
Static File Info

General

File type:	HTML document, ASCII text, with very long lines (1617), with no line terminators
Entropy (8bit):	5.344750225083175
TrID:	• HyperText Markup Language (12001/1) 66.65% • HyperText Markup Language (6006/1) 33.35%
File name:	#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html
File size:	1617
MD5:	c8a579e165f7b8c76b71f56a5766a4d0
SHA1:	b6c3f4b86d8658333c7a3e3c99c2608e1d9b0cc0
SHA256:	95d40b7fb897e11d1a5974e62ff659c3665cb7078cac051aac2d9155c8072c04
SHA512:	4bc7c18cdab4828f0a659fd22322ca9402b9a54c5ad1f710166cdf66d9749d11b9d6c5d88f8626366b890806b456901e83114eecc80d236483ac50a8bc190228
SSDEEP:	24:kVP/IwkMPtNcz4rMR5dFkS01VaODNXKCQrJdxEkLW31kSoeeyZxkw1vVI:n3MPt2ErgCaODxtQPLyppkqvW
TLSH:	5D3170749472DD31C5536CE8F1C96F0E309D815EDB16580927E888990BDBD8A4235FF9
File Content Preview:	<html><head></head><body> <form method="post" action=""><input type="hidden" name="_token" value="t1wUS8AKQFFQS9WT5UHdbIuzMtyBZXaZyYti0PMp"><input type="text" name="product_id" value="9" hidden=""><div class="form-group row mt-5"

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:20:51.580408096 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.580440044 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.580509901 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.587924004 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.587985039 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.588085890 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.589639902 CET	49698	443	192.168.2.3	142.250.203.110

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:20:51.589658976 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.589828968 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.589863062 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.645701885 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:51.645747900 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.645848036 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:51.656306982 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:51.656346083 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.664351940 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:51.664397955 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:51.664473057 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:51.664977074 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:51.665004015 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:51.682297945 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.682796955 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.682857037 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.683593988 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.683711052 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.684911013 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.684988022 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.738284111 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.738959074 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.768210888 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:51.792342901 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:51.792398930 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.792643070 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.792714119 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.793606043 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.793617010 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:51.793637037 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.793642044 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:51.793697119 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.794492960 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.794519901 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:51.794589043 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:51.795229912 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.795310020 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:51.795352936 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:51.795850039 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:51.795912981 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:51.917767048 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.228665113 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.228708982 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.228904009 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.229000092 CET	49699	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.229074001 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.229320049 CET	443	49699	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.229429960 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:52.229470968 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.229624033 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.229727983 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.229759932 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.229943991 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.229964972 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.230084896 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.230529070 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:52.230551958 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.230659962 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.230670929 CET	443	49702	88.99.17.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:20:52.275619030 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.275754929 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.275758028 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.275810957 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.277087927 CET	49698	443	192.168.2.3	142.250.203.110
Nov 30, 2022 00:20:52.277116060 CET	443	49698	142.250.203.110	192.168.2.3
Nov 30, 2022 00:20:52.283499002 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.283524036 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.283612013 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.283644915 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.283662081 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.283713102 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.306258917 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.306454897 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:52.306482077 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.306627989 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.306683064 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:52.307744980 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.307773113 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.307828903 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.307882071 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.307921886 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.307924986 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.307938099 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.307974100 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.307971954 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.308029890 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.308037043 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.316368103 CET	49701	443	192.168.2.3	172.217.168.45
Nov 30, 2022 00:20:52.316411018 CET	443	49701	172.217.168.45	192.168.2.3
Nov 30, 2022 00:20:52.333547115 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.333578110 CET	443	49702	88.99.17.3	192.168.2.3
Nov 30, 2022 00:20:52.333789110 CET	49702	443	192.168.2.3	88.99.17.3
Nov 30, 2022 00:20:52.333816051 CET	443	49702	88.99.17.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:20:51.253921986 CET	57990	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:51.281322956 CET	53	57990	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:51.368350029 CET	52387	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:51.395328045 CET	53	52387	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:51.586791992 CET	60625	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:51.615792036 CET	53	60625	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:52.469736099 CET	49302	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:52.475405931 CET	53975	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:52.476200104 CET	51139	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:52.492763996 CET	53	49302	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:52.498127937 CET	60582	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:52.517107010 CET	53	60582	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:53.837598085 CET	59636	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:20:53.857350111 CET	53	59636	8.8.8.8	192.168.2.3
Nov 30, 2022 00:20:55.704586029 CET	65320	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:21:07.316586971 CET	59433	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:21:52.566946030 CET	65511	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:21:52.585711956 CET	53	65511	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:20:51.253921986 CET	192.168.2.3	8.8.8.8	0x3f99	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:51.368350029 CET	192.168.2.3	8.8.8.8	0xedc6	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:51.586791992 CET	192.168.2.3	8.8.8.8	0xf934	Standard query (0)	mandemutworld.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.469736099 CET	192.168.2.3	8.8.8.8	0x53c3	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.475405931 CET	192.168.2.3	8.8.8.8	0x6243	Standard query (0)	cdn.jsdelivr.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.476200104 CET	192.168.2.3	8.8.8.8	0xc736	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.498127937 CET	192.168.2.3	8.8.8.8	0xb775	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:53.837598085 CET	192.168.2.3	8.8.8.8	0xd609	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:55.704586029 CET	192.168.2.3	8.8.8.8	0x43b	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:07.316586971 CET	192.168.2.3	8.8.8.8	0xfc48	Standard query (0)	aadcdn.msauthimages.net	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:52.566946030 CET	192.168.2.3	8.8.8.8	0x290d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:20:51.281322956 CET	8.8.8.8	192.168.2.3	0x3f99	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:20:51.281322956 CET	8.8.8.8	192.168.2.3	0x3f99	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:51.395328045 CET	8.8.8.8	192.168.2.3	0xedc6	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:51.615792036 CET	8.8.8.8	192.168.2.3	0xf934	No error (0)	mandemutworld.com		88.99.17.3	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.492763996 CET	8.8.8.8	192.168.2.3	0x53c3	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.492763996 CET	8.8.8.8	192.168.2.3	0x53c3	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.497066975 CET	8.8.8.8	192.168.2.3	0xc736	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:20:52.500051022 CET	8.8.8.8	192.168.2.3	0x6243	No error (0)	cdn.jsdelivr.net	cdn.jsdelivr.net.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:20:52.502990961 CET	8.8.8.8	192.168.2.3	0xba5f	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:52.517107010 CET	8.8.8.8	192.168.2.3	0xb775	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:53.857350111 CET	8.8.8.8	192.168.2.3	0xd609	No error (0)	cdnjs.cloudflare.com		104.17.24.14	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:53.857350111 CET	8.8.8.8	192.168.2.3	0xd609	No error (0)	cdnjs.cloudflare.com		104.17.25.14	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:53.858860970 CET	8.8.8.8	192.168.2.3	0xe9df	No error (0)	dual.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:20:53.858860970 CET	8.8.8.8	192.168.2.3	0xe9df	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:53.858860970 CET	8.8.8.8	192.168.2.3	0xe9df	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)	false

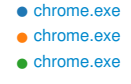
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:20:55.724462032 CET	8.8.8.8	192.168.2.3	0x43b	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:20:55.724462032 CET	8.8.8.8	192.168.2.3	0x43b	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:20:58.302872896 CET	8.8.8.8	192.168.2.3	0x2320	No error (0)	cs1227.wpc.alphacdn.net		192.229.221.185	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:07.340468884 CET	8.8.8.8	192.168.2.3	0xfc48	No error (0)	aadcdn.msauthimages.net	aadcdn.azureedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:21:07.340468884 CET	8.8.8.8	192.168.2.3	0xfc48	No error (0)	cs1025.wpc.upsiloncdn.net		152.199.23.72	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:07.558468103 CET	8.8.8.8	192.168.2.3	0x754e	No error (0)	dual.part-0032.t-0009.t-msedge.net	part-0032.t-0009.t-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:21:07.558468103 CET	8.8.8.8	192.168.2.3	0x754e	No error (0)	part-0032.t-0009.t-msedge.net		13.107.246.60	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:07.558468103 CET	8.8.8.8	192.168.2.3	0x754e	No error (0)	part-0032.t-0009.t-msedge.net		13.107.213.60	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:21:52.585711956 CET	8.8.8.8	192.168.2.3	0x290d	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)	false

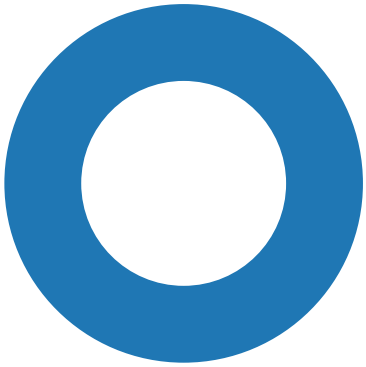
HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- mandemutworld.com
- maxcdn.bootstrapcdn.com
- logincdn.msauth.net
- https:
- cdnjs.cloudflare.com
- aadcdn.msauth.net
- aadcdn.msauthimages.net

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: **2516**, Parent PID: **4704**

General

Target ID:	0
Start time:	00:20:45
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: chrome.exe PID: **5208**, Parent PID: **2516**

General

Target ID:	1
Start time:	00:20:46
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false

Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=1964 --field-trial-handle=1816,i,18019605785344620809,16696382858066997968,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **5552**, Parent PID: **4704**

General

Target ID:	2
Start time:	00:20:47
Start date:	30/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" "C:\Users\user\Desktop\#U25b6 #Ud83d#Udd18#U2500#U2500#U2500#U2500#U2500#U2500#U2500#U2500 126 Voice-Attchment.919-340-XX.html
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly