ID: 756227
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 20:58:15
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

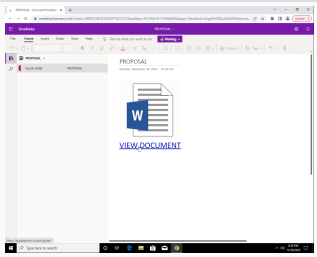
Windows Analysis Report

http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA

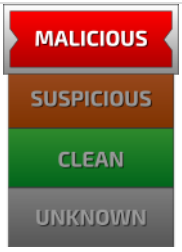
Overview

General Information

Sample URL:	http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA
Analysis ID:	756227
Infos:	



Detection



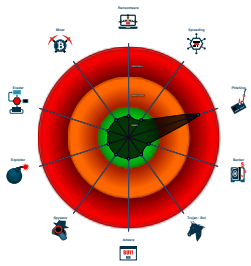
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected HtmlPhish10
- Antivirus detection for URL or domain
- Phishing site detected (based on log…
- Phishing site detected (based on im…
- HTML body contains low number of …
- Invalid T&C link found
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 6884 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 7052 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=2040 --field-trial-handle=1784,i,14432860437327741238,17742013553884360258,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
67460.4.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	
88411.6.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

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing

Yara detected HtmlPhish10

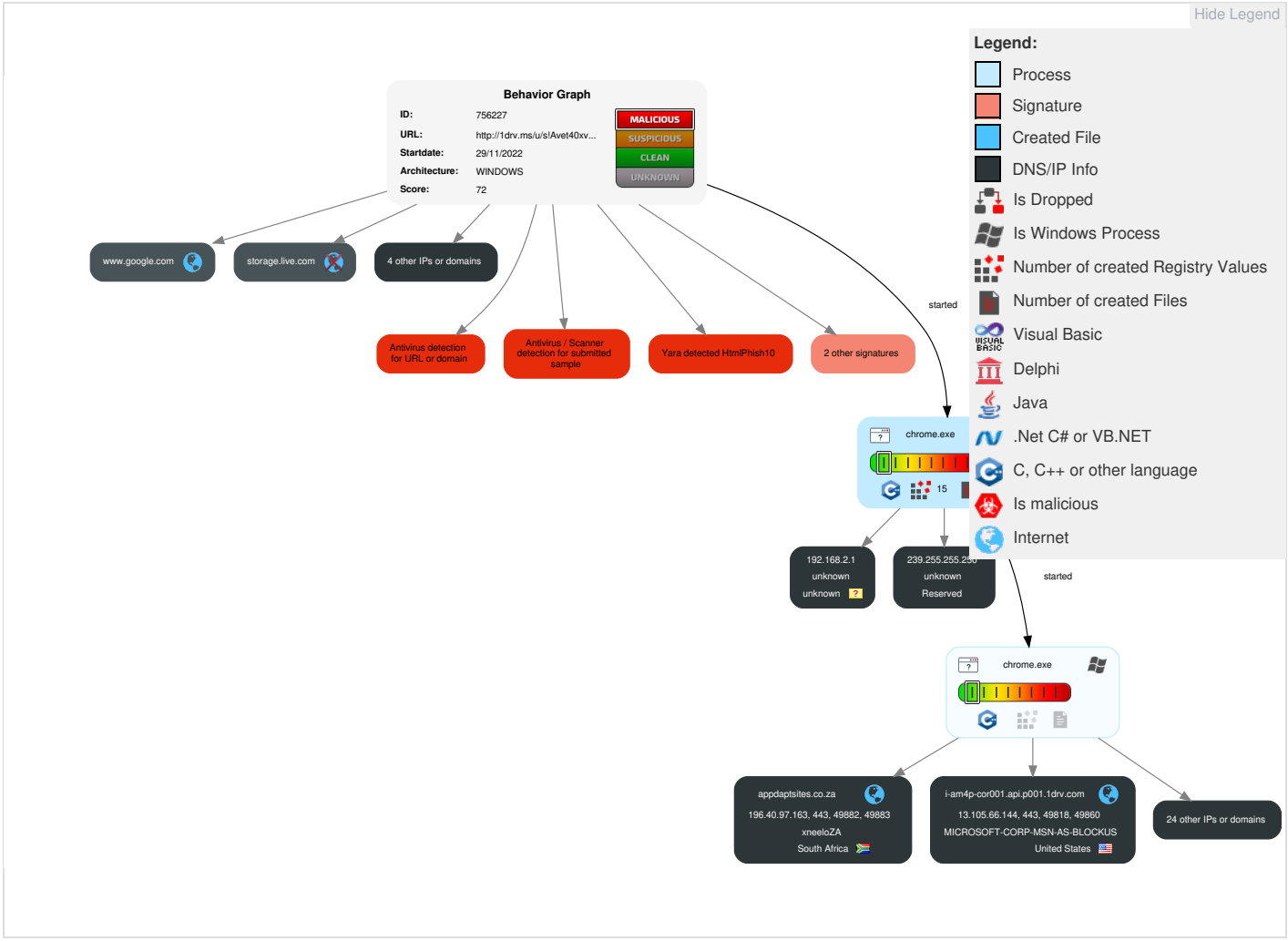
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

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	4 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	5 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	3 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

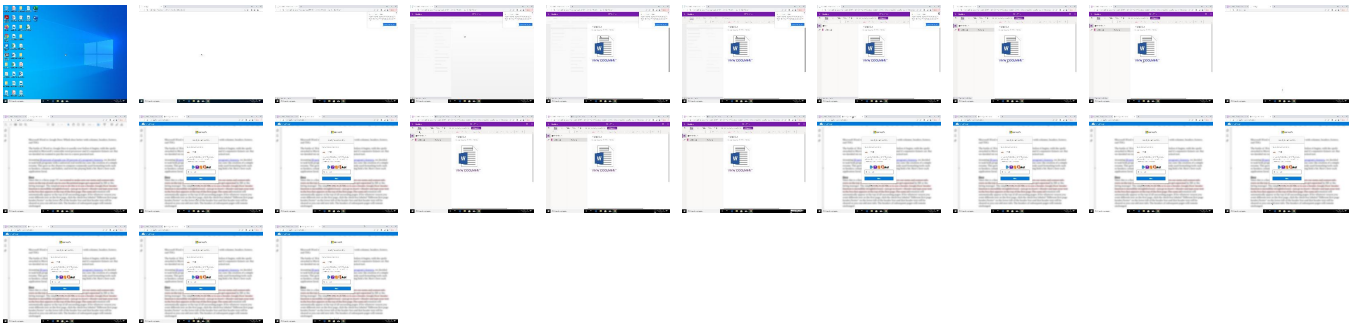
Behavior Graph

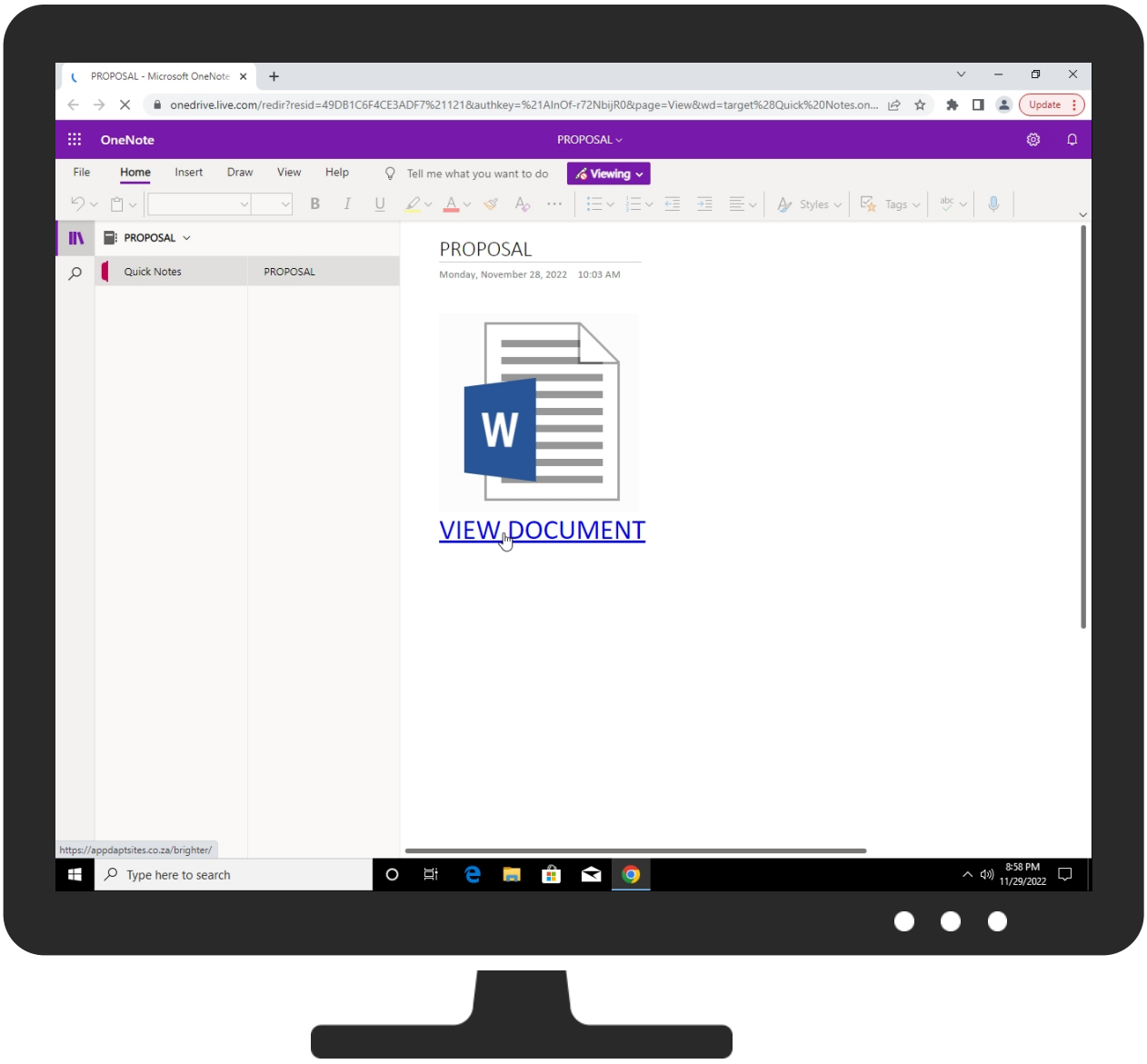


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA	0%	Avira URL Cloud	safe	
http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
http://https://onedrive.live.com/view.aspx?resid=49DB1C6F4CE3ADF7!121&authkey=!AInOf-r72NbijR0	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://onedrive.live.com/redir?resid=49DB1C6F4CE3ADF7%21121&authkey=%21AInOf-r72NbijR0&page=View&wd=target%28Quick%20Notes.one%7C09c202ac-b53c-486e-b917-feeea66d027e%2FPROPOSAL%7C2fb3d88b-1f2f-42b6-8f97-4520dc81c8f2%2F%29&wdorigin=NavigationUrl	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	
http://https://appdaptsites.co.za/brighter/	100%	SlashNext	Credential Stealing type: Phishing & Social Engineering	

Domains and IPs

Contacted Domains

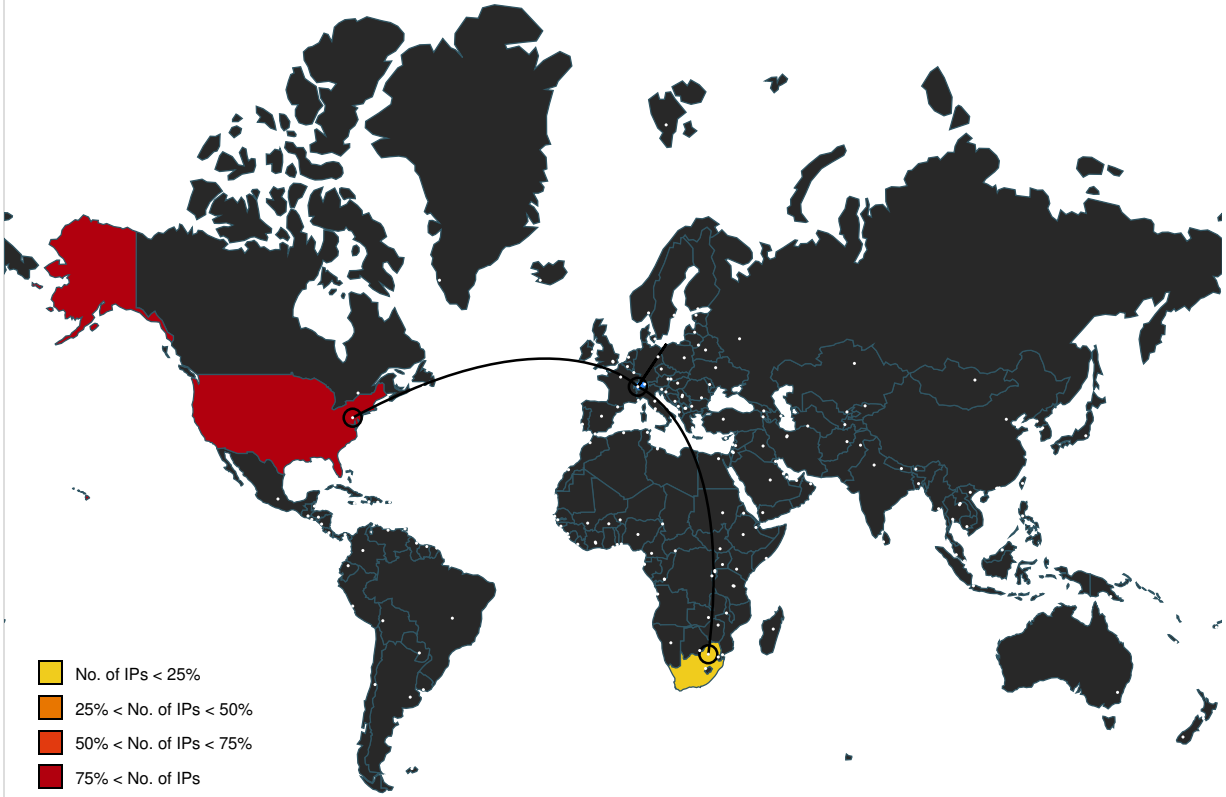
Name	IP	Active	Malicious	Antivirus Detection	Reputation
b-0016.b-msedge.net	13.107.6.171	true	false		unknown
i-am4p-cor001.api.p001.1drv.com	13.105.66.144	true	false		high
i-dub06p-cor001.api.p001.1drv.com	20.135.20.1	true	false		high
accounts.google.com	142.250.184.205	true	false		high
dual-a-0001.a-msedge.net	204.79.197.200	true	false		unknown
appdaptsites.co.za	196.40.97.163	true	false		high
www.google.com	172.217.18.100	true	false		high
clients.l.google.com	142.250.185.206	true	false		high
1drv.ms	13.107.42.12	true	false		high
onenoteonlinesync.onenote.com	unknown	unknown	false		high
augloop.office.com	unknown	unknown	false		high
c.live.com	unknown	unknown	false		high
storage.live.com	unknown	unknown	false		high
ajax.aspnetcdn.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
p.sfx.ms	unknown	unknown	false		high
spoprod-a.akamaihd.net	unknown	unknown	false		high
www.onenote.com	unknown	unknown	false		high
messaging.engagement.office.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/redir?resid=49DB1C6F4CE3ADF7%21121&authkey=%21AInOf-r72NbijR0&page=View&wd=target%28Quick%20Notes.one%7C09c202ac-b53c-486e-b917-feeea66d027e%2FPROPOSAL%7C2fb3d88b-1f2f-42b6-8f97-4520dc81c8f2%2F%29&wdorigin=NavigationUrl	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://appdaptsites.co.za/brighter/	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/bootstrap.js	false		high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/css.css	false		high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/bootstrap_002.js	false		high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/jquery.js	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://appdaptsites.co.za/favicon.ico	false		high
http://https://appdaptsites.co.za/brighter/	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/bootstrap.css	false		high
http://https://onedrive.live.com/view.aspx?resid=49DB1C6F4CE3ADF7!121&authkey=!AInOf-r72NbijR0	false	• SlashNext: Credential Stealing type: Phishing & Social Engineering	high
http://https://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/jquery-3.js	false		high
http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA	false		high

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=104.0.5112.102&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://appdaptsites.co.za/brighter/Sharing%20Link%20Validation_files/popper.js	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
196.40.97.163	appdaptsites.co.za	South Africa		37153	xneeloZA	false
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
204.79.197.200	dual-a-0001.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.6.171	b-0016.b-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.184.205	accounts.google.com	United States		15169	GOOGLEUS	false
13.105.66.144	i-am4p-cor001.api.p001.1drv.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.42.12	1drv.ms	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.196	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756227
Start date and time:	2022-11-29 20:58:15 +01:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	10
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:	mal72.phis.win@29/0@23/11
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 40.126.32.136, 40.126.32.72, 20.190.160.17, 40.126.32.74, 20.190.160.22, 20.190.160.20, 40.126.32.138, 40.126.32.68, 40.126.32.133, 40.126.32.134, 20.190.160.14, 142.250.186.67, 13.107.42.13, 34.104.35.123, 2.16.241.80, 2.16.241.83, 13.95.147.73, 88.221.169.199, 52.109.89.78, 13.69.116.104, 20.234.93.27, 172.217.18.106, 142.250.74.202, 142.250.186.74, 142.250.185.170, 142.250.185.138, 172.217.23.106, 142.250.185.202, 142.250.185.74, 142.250.185.234, 216.58.212.170, 142.250.184.234, 142.250.186.170, 172.217.16.202, 142.250.185.106, 142.250.186.106, 142.250.184.202, 20.50.73.9, 52.111.240.16, 152.199.19.161, 2.16.238.159, 2.16.238.138, 52.109.76.126, 52.111.243.14, 40.126.32.140, 40.126.32.76, 184.24.2.183, 184.24.3.163, 152.199.19.160, 142.250.185.227, 52.111.243.19
- Excluded domains from analysis (whitelisted): odwebp.trafficmanager.net, e2682.g.akamaiedge.net, slscr.update.microsoft.com, c1-wildcard.cdn.office.net-c.edgekey.net.globalredir.akadns.net, www.tm.lg.prod.aadmsa.akadns.net, clientservices.googleapis.com, res-1.cdn.office.net, browser.events.data.trafficmanager.net, appsforoffice.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, cdn.onenote.net.edgekey.net, augloop-prod-pd00.westeurope.cloudapp.azure.com, prod-campaignaggregator.omexexternallfb.office.net.akadns.net, login.live.com, update.googleapis.com, eu-office.events.data.microsoft.com, onenoteonlinesync.onenote.trafficmanager.net, www.bing.com, onedscolprdweu06.westeurope.cloudapp.azure.com, fs.microsoft.com, spoppe-b.ec.azureedge.net, content-autofill.googleapis.com, westeurope1-odwebp.cloudapp.net, osiprod-neu-celadon-000.northeurope.cloudapp.azure.com, reverseproxy.onenote.trafficmanager.net, www.tm.a.prd.aadg.akadns.net, e19254.dscg.akamaiedge.net, onedscolprdneu01.northeurope.cloudapp
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtWriteFile calls found.
- 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

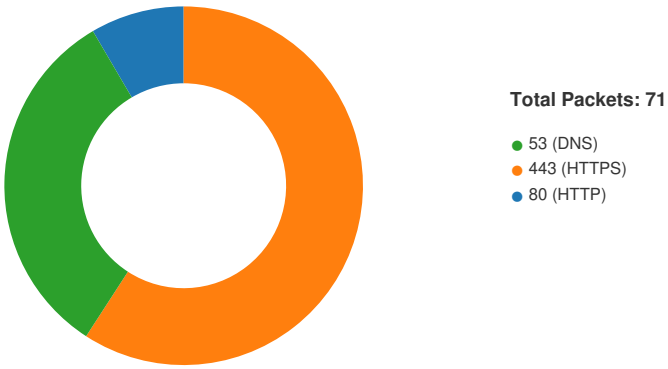
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:58:42.716931105 CET	49692	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:42.717200994 CET	49693	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:42.718436003 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:42.718493938 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:42.718576908 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:42.720043898 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:42.720081091 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:42.720396996 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:42.720455885 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.720549107 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:42.720777988 CET	49695	443	192.168.2.3	142.250.185.206

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:58:42.720807076 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.736819983 CET	80	49692	13.107.42.12	192.168.2.3
Nov 29, 2022 20:58:42.736911058 CET	49692	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:42.736982107 CET	80	49693	13.107.42.12	192.168.2.3
Nov 29, 2022 20:58:42.737036943 CET	49693	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:42.737582922 CET	49692	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:42.757195950 CET	80	49692	13.107.42.12	192.168.2.3
Nov 29, 2022 20:58:42.794739008 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:42.796108007 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:42.796153069 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:42.797441006 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:42.797539949 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:42.802316904 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.802685976 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:42.802706003 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.803184986 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.803262949 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:42.803646088 CET	80	49692	13.107.42.12	192.168.2.3
Nov 29, 2022 20:58:42.804027081 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:42.804120064 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:42.843658924 CET	49692	80	192.168.2.3	13.107.42.12
Nov 29, 2022 20:58:43.087194920 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.087284088 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.087441921 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.087460041 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.087629080 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.087730885 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:43.087794065 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.087850094 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:43.087862968 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.088193893 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.120177984 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.120347023 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:43.120392084 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.120443106 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.120526075 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:43.121881008 CET	49695	443	192.168.2.3	142.250.185.206
Nov 29, 2022 20:58:43.121926069 CET	443	49695	142.250.185.206	192.168.2.3
Nov 29, 2022 20:58:43.128674984 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.128720999 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.140055895 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.140235901 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.140279055 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.140547991 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:43.140621901 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.144618034 CET	49694	443	192.168.2.3	142.250.184.205
Nov 29, 2022 20:58:43.144654036 CET	443	49694	142.250.184.205	192.168.2.3
Nov 29, 2022 20:58:45.697762012 CET	49708	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.697854996 CET	443	49708	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.697968006 CET	49708	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.698157072 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.698211908 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.698301077 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.698476076 CET	49708	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.698504925 CET	443	49708	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.698668957 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.698703051 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.712171078 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.712260962 CET	443	49711	13.107.6.171	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:58:45.712362051 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.712574005 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.712605000 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.845626116 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.846018076 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.846060991 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.847258091 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.847362041 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.849375963 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.849392891 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.849514961 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.849625111 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.849684000 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.849714994 CET	49711	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.849725008 CET	443	49711	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.862226963 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.863667011 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.863713026 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.866172075 CET	443	49708	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.866457939 CET	49708	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.866503000 CET	443	49708	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.866559029 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.866664886 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.867027044 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.867043018 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.867192984 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.867525101 CET	49709	443	192.168.2.3	13.107.6.171
Nov 29, 2022 20:58:45.867544889 CET	443	49709	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.869709015 CET	443	49708	13.107.6.171	192.168.2.3
Nov 29, 2022 20:58:45.869837046 CET	49708	443	192.168.2.3	13.107.6.171

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:58:42.648577929 CET	59183	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:42.650408983 CET	64581	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:42.652430058 CET	52752	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:42.666460037 CET	53	59183	1.1.1.1	192.168.2.3
Nov 29, 2022 20:58:42.667942047 CET	53	64581	1.1.1.1	192.168.2.3
Nov 29, 2022 20:58:42.670615911 CET	53	52752	1.1.1.1	192.168.2.3
Nov 29, 2022 20:58:42.813381910 CET	63995	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:43.709613085 CET	59889	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:44.795058012 CET	62323	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:46.365263939 CET	61730	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:46.382596970 CET	53	61730	1.1.1.1	192.168.2.3
Nov 29, 2022 20:58:46.435731888 CET	54306	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:46.454617977 CET	53	54306	1.1.1.1	192.168.2.3
Nov 29, 2022 20:58:46.532649040 CET	64287	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:50.168251991 CET	60633	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:54.819307089 CET	61153	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:55.119458914 CET	62641	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:55.922353029 CET	64782	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:56.093806982 CET	52230	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:56.217138052 CET	56943	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:56.611047983 CET	49392	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:58:57.895622015 CET	57673	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:59:01.870812893 CET	54044	53	192.168.2.3	1.1.1.1
Nov 29, 2022 20:59:02.447354078 CET	53	54044	1.1.1.1	192.168.2.3
Nov 29, 2022 20:59:02.495793104 CET	53372	53	192.168.2.3	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 20:59:57.739254951 CET	54439	53	192.168.2.3	1.1.1.1
Nov 29, 2022 21:00:19.740616083 CET	53082	53	192.168.2.3	1.1.1.1
Nov 29, 2022 21:00:46.463978052 CET	60575	53	192.168.2.3	1.1.1.1
Nov 29, 2022 21:00:46.483812094 CET	53	60575	1.1.1.1	192.168.2.3
Nov 29, 2022 21:00:46.485804081 CET	49826	53	192.168.2.3	1.1.1.1
Nov 29, 2022 21:00:46.504244089 CET	53	49826	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 20:58:42.648577929 CET	192.168.2.3	1.1.1.1	0x4966	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:42.650408983 CET	192.168.2.3	1.1.1.1	0xef28	Standard query (0)	1drv.ms	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:42.652430058 CET	192.168.2.3	1.1.1.1	0xfc87	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:42.813381910 CET	192.168.2.3	1.1.1.1	0xacf6	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:43.709613085 CET	192.168.2.3	1.1.1.1	0x1d67	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:44.795058012 CET	192.168.2.3	1.1.1.1	0xa435	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.365263939 CET	192.168.2.3	1.1.1.1	0x739d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.435731888 CET	192.168.2.3	1.1.1.1	0xc46	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.532649040 CET	192.168.2.3	1.1.1.1	0xcbbe	Standard query (0)	onenoteonlinesync.onenote.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:50.168251991 CET	192.168.2.3	1.1.1.1	0x3c1b	Standard query (0)	c.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:54.819307089 CET	192.168.2.3	1.1.1.1	0x7179	Standard query (0)	messaging.engagement.office.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:55.119458914 CET	192.168.2.3	1.1.1.1	0x90c8	Standard query (0)	spoprod-a.akamaihd.net	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:55.922353029 CET	192.168.2.3	1.1.1.1	0xb585	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:56.093806982 CET	192.168.2.3	1.1.1.1	0xa70e	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:56.217138052 CET	192.168.2.3	1.1.1.1	0x160c	Standard query (0)	augloop.office.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:56.611047983 CET	192.168.2.3	1.1.1.1	0x2d20	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:57.895622015 CET	192.168.2.3	1.1.1.1	0x1d75	Standard query (0)	p.sfx.ms	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:01.870812893 CET	192.168.2.3	1.1.1.1	0x141d	Standard query (0)	appdaptsites.co.za	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:02.495793104 CET	192.168.2.3	1.1.1.1	0xe79a	Standard query (0)	storage.live.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:57.739254951 CET	192.168.2.3	1.1.1.1	0x7379	Standard query (0)	www.onenote.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:00:19.740616083 CET	192.168.2.3	1.1.1.1	0xd585	Standard query (0)	augloop.office.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:00:46.463978052 CET	192.168.2.3	1.1.1.1	0x4948	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:00:46.485804081 CET	192.168.2.3	1.1.1.1	0x185f	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 29, 2022 20:58:42.666460037 CET	1.1.1.1	192.168.2.3	0x4966	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:42.666460037 CET	1.1.1.1	192.168.2.3	0x4966	No error (0)	clients.l.google.com		142.250.185.206	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 20:58:42.667942047 CET	1.1.1.1	192.168.2.3	0xef28	No error (0)	1drv.ms		13.107.42.12	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:42.670615911 CET	1.1.1.1	192.168.2.3	0xfc87	No error (0)	accounts.google.com		142.250.184.205	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:42.831137896 CET	1.1.1.1	192.168.2.3	0xacf6	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:43.727652073 CET	1.1.1.1	192.168.2.3	0x1d67	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:44.815952063 CET	1.1.1.1	192.168.2.3	0xa435	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:45.655867100 CET	1.1.1.1	192.168.2.3	0xde3e	No error (0)	onenote.wac.trafficmanager.net.b-0016.b-dc-msedge.net.b-0016.b-msedge.net	b-0016.b-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:45.655867100 CET	1.1.1.1	192.168.2.3	0xde3e	No error (0)	b-0016.b-msedge.net		13.107.6.171	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.382596970 CET	1.1.1.1	192.168.2.3	0x739d	No error (0)	www.google.com		172.217.18.100	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.454617977 CET	1.1.1.1	192.168.2.3	0xc46	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:46.551220894 CET	1.1.1.1	192.168.2.3	0xcbbe	No error (0)	onenoteonlinesync.onenote.com	onenoteonlinesync.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:50.189974070 CET	1.1.1.1	192.168.2.3	0x3c1b	No error (0)	c.live.com	c.msn.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:50.189974070 CET	1.1.1.1	192.168.2.3	0x3c1b	No error (0)	c.msn.com	c-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:50.586435080 CET	1.1.1.1	192.168.2.3	0x9f0	No error (0)	c-bing-com.a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:50.586435080 CET	1.1.1.1	192.168.2.3	0x9f0	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:50.586435080 CET	1.1.1.1	192.168.2.3	0x9f0	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:54.839752913 CET	1.1.1.1	192.168.2.3	0x7179	No error (0)	messaging.engagement.office.com	prod-campaignaggregator.omexexternallfb.office.net.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:55.141391993 CET	1.1.1.1	192.168.2.3	0x90c8	No error (0)	spoprod-a.akamaihd.net	spoprod-a.akamaihd.net.edgesuite.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:55.941742897 CET	1.1.1.1	192.168.2.3	0xb585	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:55.941742897 CET	1.1.1.1	192.168.2.3	0xb585	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:55.941742897 CET	1.1.1.1	192.168.2.3	0xb585	No error (0)	am4pcor001-com.be.1drv.com	i-am4p-cor001.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:55.941742897 CET	1.1.1.1	192.168.2.3	0xb585	No error (0)	i-am4p-cor001.api.p001.1drv.com		13.105.66.144	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:58:56.112489939 CET	1.1.1.1	192.168.2.3	0xa70e	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false

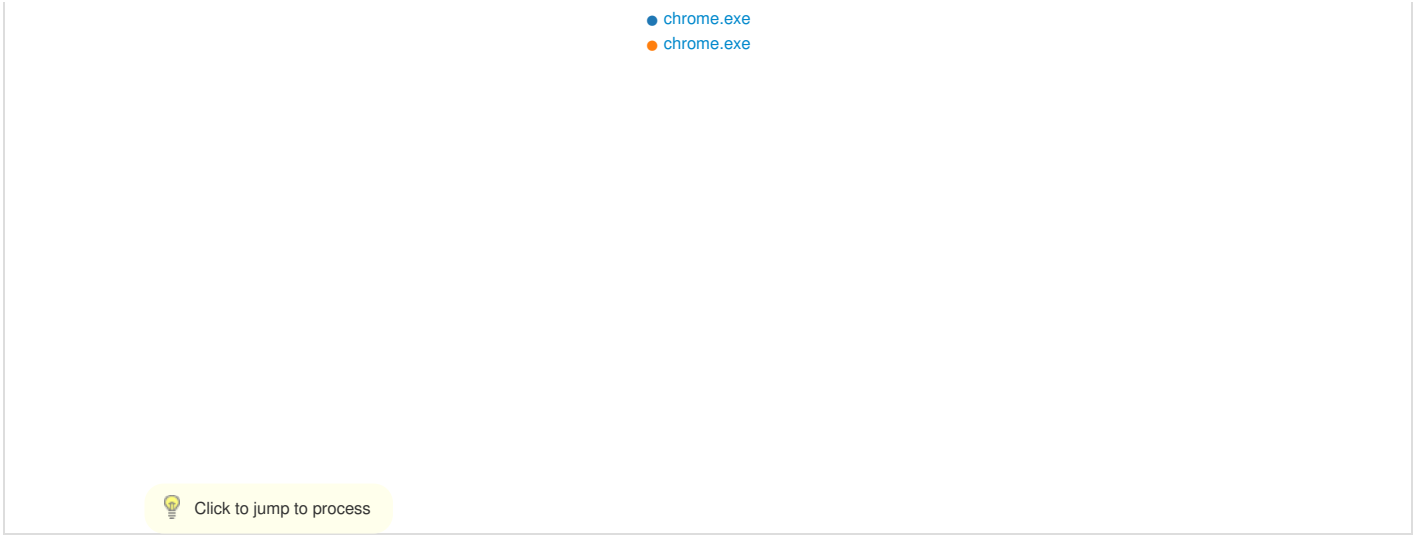
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 20:58:56.237684011 CET	1.1.1.1	192.168.2.3	0x160c	No error (0)	augloop.office.com	augloop-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:56.629834890 CET	1.1.1.1	192.168.2.3	0x2d20	No error (0)	ajax.aspnetcdn.com	mscomajax.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:58:57.918621063 CET	1.1.1.1	192.168.2.3	0x1d75	No error (0)	p.sfx.ms	odwebp.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:02.447354078 CET	1.1.1.1	192.168.2.3	0x141d	No error (0)	appdaptsites.co.za		196.40.97.163	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:02.514467955 CET	1.1.1.1	192.168.2.3	0xe79a	No error (0)	storage.live.com	common-geo.ha.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:02.514467955 CET	1.1.1.1	192.168.2.3	0xe79a	No error (0)	common-geo.ha.1drv.com	common-geo.onedrive.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:02.514467955 CET	1.1.1.1	192.168.2.3	0xe79a	No error (0)	dub06pcor001-com.be.1drv.com	i-dub06p-cor001.api.p001.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:02.514467955 CET	1.1.1.1	192.168.2.3	0xe79a	No error (0)	i-dub06p-cor001.api.p001.1drv.com		20.135.20.1	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:48.863146067 CET	1.1.1.1	192.168.2.3	0xfc3d	No error (0)	onenote.wac.trafficmanager.net.b-0016.b-dc-msedge.net.b-0016.b-msedge.net	b-0016.b-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 20:59:48.863146067 CET	1.1.1.1	192.168.2.3	0xfc3d	No error (0)	b-0016.b-msedge.net		13.107.6.171	A (IP address)	IN (0x0001)	false
Nov 29, 2022 20:59:57.758727074 CET	1.1.1.1	192.168.2.3	0x7379	No error (0)	www.onenote.com	reverseproxy.onenote.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:00:19.760790110 CET	1.1.1.1	192.168.2.3	0xd585	No error (0)	augloop.office.com	augloop-prod.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:00:46.483812094 CET	1.1.1.1	192.168.2.3	0x4948	No error (0)	www.google.com		142.250.186.68	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:00:46.504244089 CET	1.1.1.1	192.168.2.3	0x185f	No error (0)	www.google.com		172.217.16.196	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- accounts.google.com
- clients2.google.com
- https:
  - onenote.officeapps.live.com
  - c.bing.com
  - storage.live.com
  - appdaptsites.co.za
  - www.bing.com
- 1drv.ms

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **6884**, Parent PID: **2528**

General

Target ID:	0
Start time:	20:58:38
Start date:	29/11/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://1drv.ms/u/s!Avet40xvHNtJeYnOf-r72NbijR0?e=jLZzfA
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: chrome.exe PID: **7052**, Parent PID: **6884**

General

Target ID:	1
Start time:	20:58:40
Start date:	29/11/2022
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=2040 --field-trial-handle=1784,i,14432860437327741238,17742013553884360258,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff6566b0000
File size:	2852640 bytes
MD5 hash:	7BC7B4AEDC055BB02BCB52710132E9E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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

Disassembly

No disassembly