ID: 756098
Cookbook: browseurl.jbs
Time: 16:33:31
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

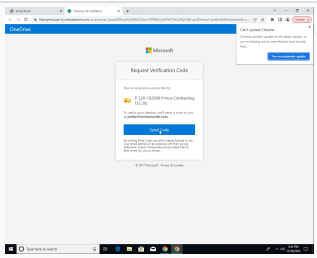
Windows Analysis Report

https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10...

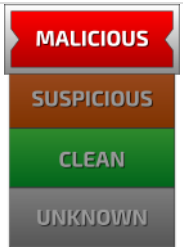
Overview

General Information

Sample URL:	https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGr...kCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb
Analysis ID:	756098
Infos:	



Detection



HTMLPhisher

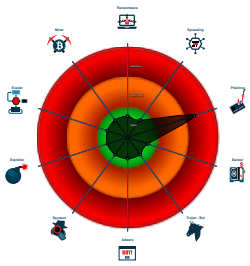
Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected HtmlPhish10

Phishing site detected (based on im...

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4916 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized "about:blank MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 5664 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-GB --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1724,i,9580845018825437107,15182149715928468815,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- chrome.exe (PID: 4688 cmdline: C:\Program Files\Google\Chrome\Application\chrome.exe" "https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
96554.0.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

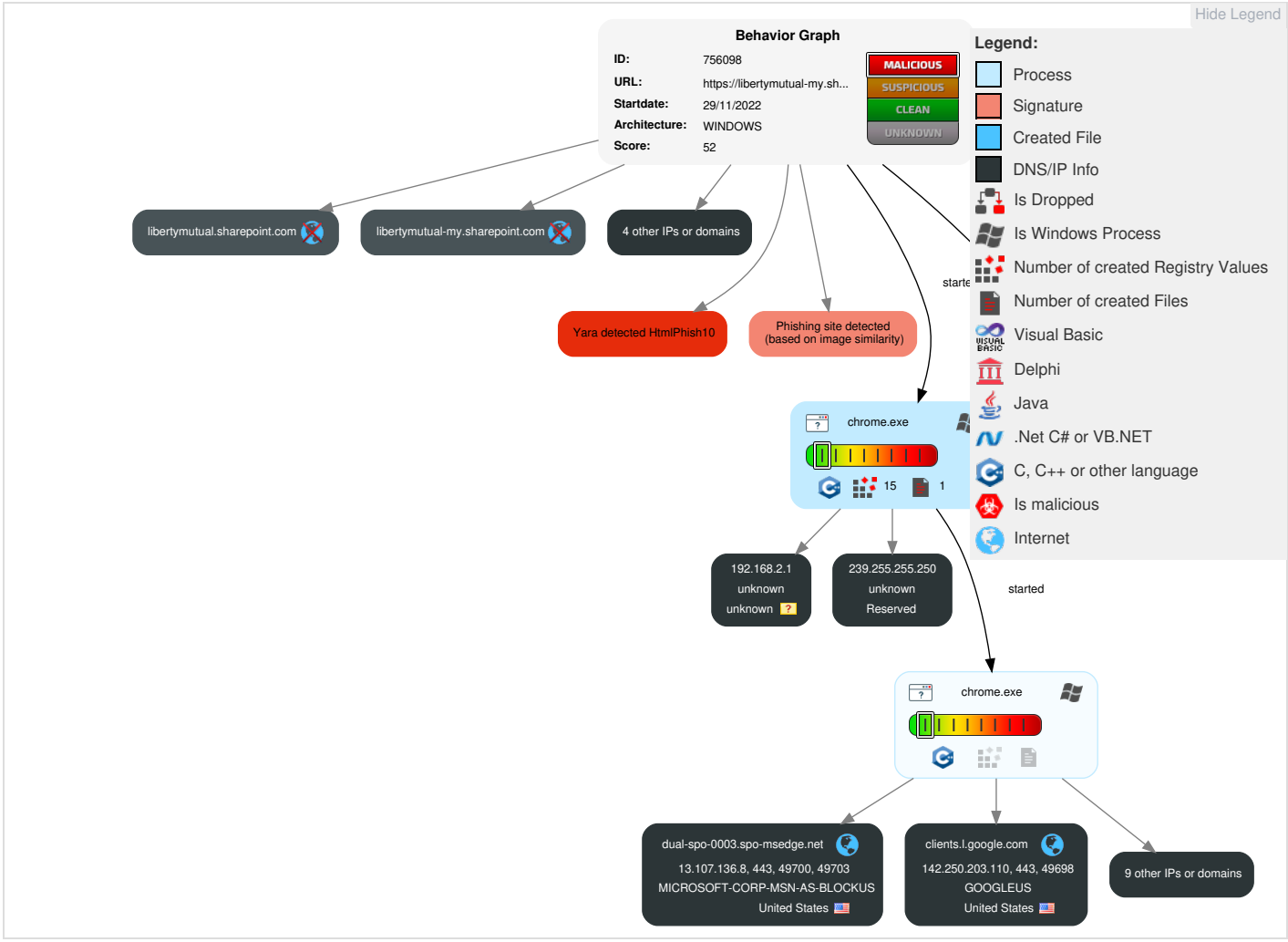
Yara detected HtmlPhish10

Phishing site detected (based on image similarity)

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

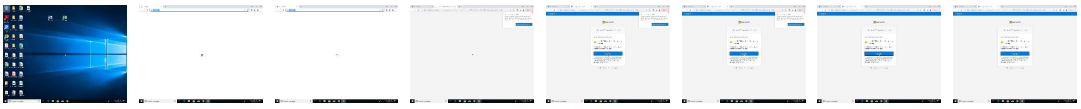
Behavior Graph

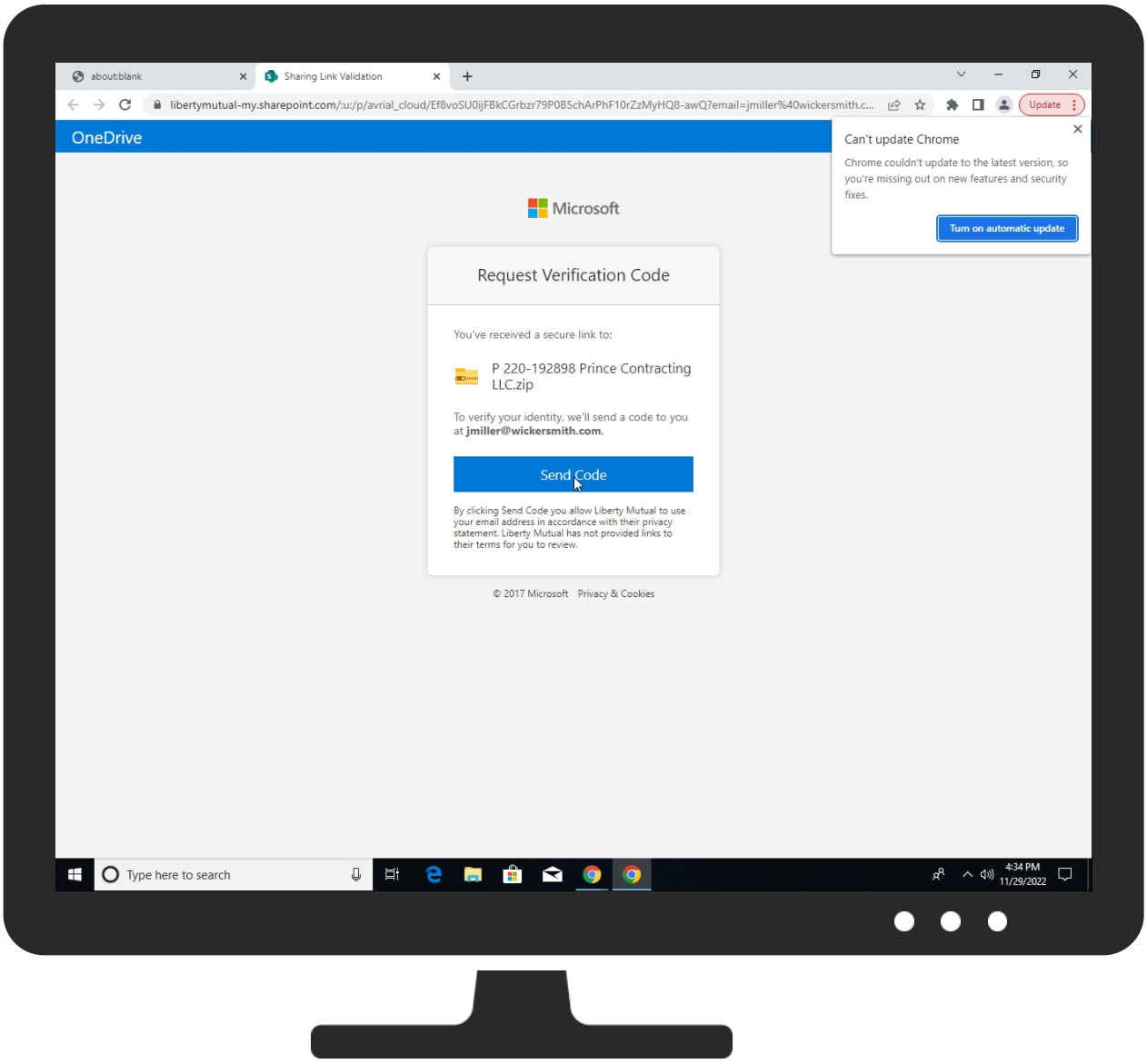


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://libertymutual-my.sharepoint.com/ScriptResource.axd?d=5mQ_iKrRt6bkxCajegfQ0Xj8aJJmvcT2782B3AdsDBISS7wRyo-fC4wefKgNp-h5aaWymGxlyV1LYhgm2wooLg31o6ucvLiM1eADoo-nRuR1SNjlAaYolMAFpSlXk7AC2eX8j-sebEShcuK_XdLz6Fy_31PEi1k1_VrDdn0RU52KP60sBxUEZ-V5a9ta0AL80&t=49337fe8	0%	Avira URL Cloud	safe	
http://https://libertymutual-my.sharepoint.com/ScriptResource.axd?d=swX6V43-4OTyPhELW84nrj2rzOlulWwdq6Ya8zvi6O1jPv9gA4yfBLI4jn6r9rvqLeBnrExnTcTJfQW8nX3VRPMzrXTilPgpPll4CDZ-CbR6uhTPIZrrf-RpKxb32eIfndFGi_x6X1S8A5lVJe7SUSrphZ3lRRW1p0_UgAEpmsEWlL-Uf2CDmvbD9cuUHOw10&t=49337fe8	0%	Avira URL Cloud	safe	
http://https://libertymutual-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	0%	Avira URL Cloud	safe	
http://https://libertymutual-my.sharepoint.com/_layouts/15/images/microsoft-logo.png	0%	Avira URL Cloud	safe	

Domains and IPs

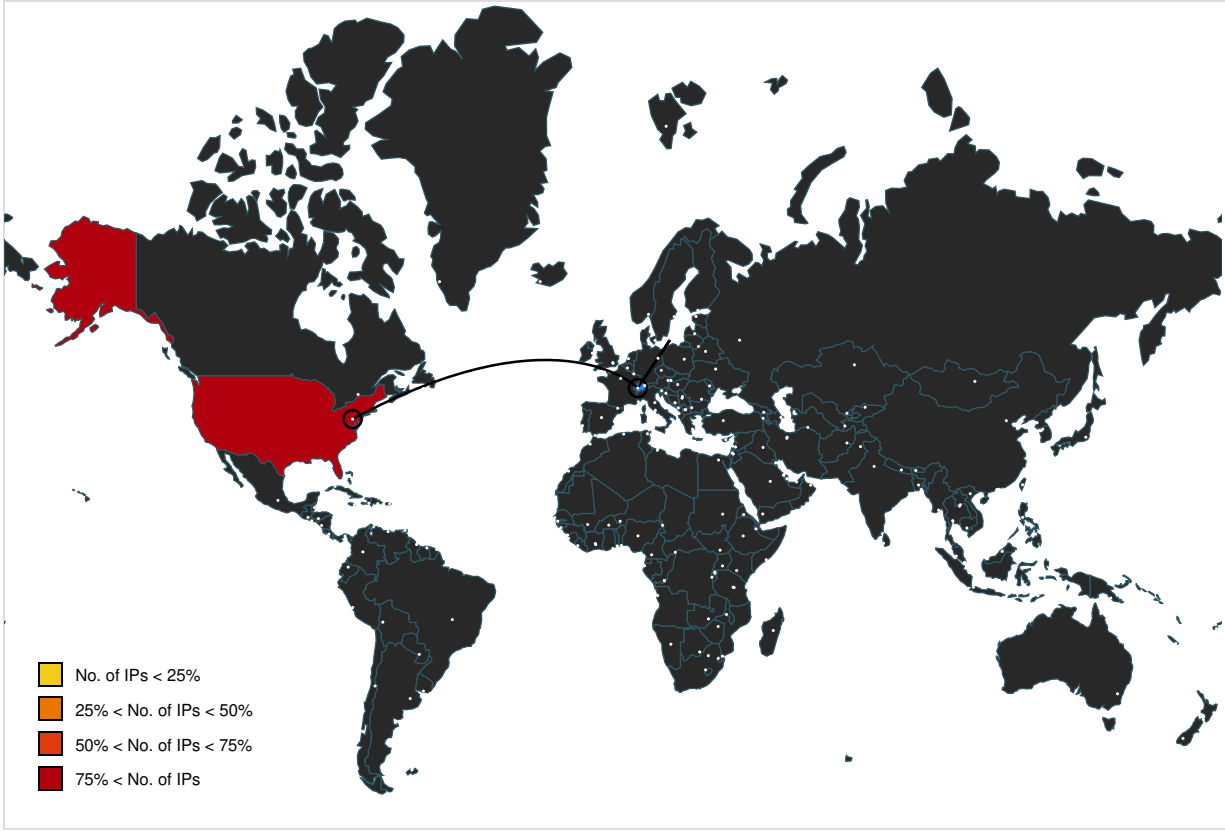
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.168.45	true	false		high
dual-spo-0003.spo-msedge.net	13.107.136.8	true	false		unknown
www.google.com	172.217.168.36	true	false		high
clients.l.google.com	142.250.203.110	true	false		high
clients2.google.com	unknown	unknown	false		high
libertymutual-my.sharepoint.com	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb	true		unknown
http://https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb	true		unknown
http://https://libertymutual-my.sharepoint.com/_layouts/15/images/microsoft-logo.png	false	• Avira URL Cloud: safe	unknown
http://https://libertymutual-my.sharepoint.com/_layouts/15/images/favicon.ico?rev=47	false	• Avira URL Cloud: safe	unknown
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-GB&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://libertymutual-my.sharepoint.com/ScriptResource.axd?d=5mQ_iKrRt6bkxCajegfQ0Xj8aJJmvcT2782B3AdsDBISS7wRyo-fC4wefKgNp-h5aaWymGxlyV1LYhgm2wooLg31o6ucvLiM1eADoo-nRuR1SNjlAaYolMAFpSlXk7AC2eX8j-sebEShcuK_XdLz6Fy_31PEi1k1_VrDdn0RU52KP60sBxUEZ-V5a9ta0AL80&t=49337fe8	false	• Avira URL Cloud: safe	unknown
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://libertymutual-my.sharepoint.com/ScriptResource.axd?d=swX6V43-4OTyPhELW84nrj2rzOlulWwdq6Ya8zvi6O1jPv9gA4yfBLI4jn6r9rvqLeBnrExnTcTJfQW8nX3VRPMzrXTilPgpPll4CDZ-CbR6uhTPIZrrf-RpKxb32eIfndFGi_x6X1S8A5lVJe7SUSrphZ3lRRW1p0_UgAEpmsEWlL-Uf2CDmvbD9cuUHOw10&t=49337fe8	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.136.8	dual-spo-0003.spo-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756098
Start date and time:	2022-11-29 16:33:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb
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:	5
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:	mal52.phis.win@24/0@6/7
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): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 172.217.168.67, 34.104.35.123, 23.11.206.33, 23.11.206.49, 2.21.22.154, 2.21.22.169, 152.199.19.161
- Excluded domains from analysis (whitelisted): spoppe-b.ec.azureedge.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net.globalredir.akadns.net, e40491.dscd.akamaiedge.net, clientservices.googleapis.com, res-1.cdn.office.net, statica.akamai.odsp.cdn.office.net-c.edgesuite.net, statica.akamai.odsp.cdn.office.net, edgedl.me.gvt1.com, spoppe-b.azureedge.net, update.googleapis.com, res-1.cdn.office.net-c.edgekey.net, 18204-ipv4v6e.farm.prod.sharepointonline.com.akadns.net, res-1.cdn.office.net-c.edgekey.net.globalredir.akadns.net, a1813.dscd.akamai.net, cs9.wpc.v0cdn.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

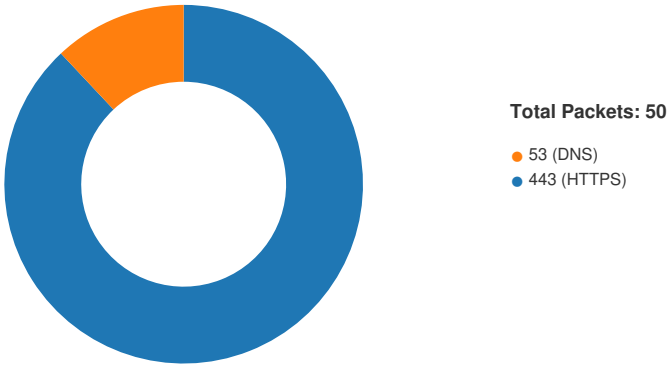
No created / dropped files found

Static File Info

No static file info

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:34:36.602917910 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:36.602982044 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:36.603066921 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:36.603607893 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:36.603630066 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:36.605094910 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.605150938 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.605249882 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.605688095 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.605711937 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.677752018 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.679575920 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:36.681091070 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:36.681133032 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:36.681379080 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.681413889 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.681869984 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.681971073 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.683208942 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:36.683304071 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:36.684669018 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:36.684750080 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.243598938 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:37.243639946 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.243817091 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.244359970 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:37.244379044 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.250080109 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.250108957 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.250241041 CET	443	49697	172.217.168.45	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:34:37.250401974 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.250415087 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.261284113 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.261344910 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.261475086 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.261986017 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.262006044 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.278415918 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.278497934 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:37.278527975 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.280052900 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.280229092 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:37.281644106 CET	49698	443	192.168.2.4	142.250.203.110
Nov 29, 2022 16:34:37.281666994 CET	443	49698	142.250.203.110	192.168.2.4
Nov 29, 2022 16:34:37.290790081 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.290807009 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.305408001 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.305515051 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.305531025 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.305562973 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.305608034 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.371381998 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.379755020 CET	49697	443	192.168.2.4	172.217.168.45
Nov 29, 2022 16:34:37.379803896 CET	443	49697	172.217.168.45	192.168.2.4
Nov 29, 2022 16:34:37.380893946 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.380914927 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.382375956 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.382477999 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.513562918 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.513586998 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.513766050 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.514971972 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.514986992 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:37.655860901 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:37.802654028 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.802699089 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.802804947 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.803174019 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.803193092 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.862715960 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.885215998 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.885273933 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.886660099 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.886799097 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.898997068 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.899027109 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.899218082 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:37.990910053 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:37.990966082 CET	443	49701	172.217.168.36	192.168.2.4
Nov 29, 2022 16:34:38.090908051 CET	49701	443	192.168.2.4	172.217.168.36
Nov 29, 2022 16:34:38.336935043 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.336977005 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337068081 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337080956 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337093115 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:38.337116957 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337140083 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:38.337147951 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337162971 CET	49700	443	192.168.2.4	13.107.136.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:34:38.337184906 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337197065 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337215900 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.337275028 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:38.337275028 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:38.337275028 CET	49700	443	192.168.2.4	13.107.136.8
Nov 29, 2022 16:34:38.337290049 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.363943100 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.363965034 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.364062071 CET	443	49700	13.107.136.8	192.168.2.4
Nov 29, 2022 16:34:38.364072084 CET	443	49700	13.107.136.8	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:34:35.831396103 CET	64167	53	192.168.2.4	8.8.8.8
Nov 29, 2022 16:34:35.833471060 CET	58565	53	192.168.2.4	8.8.8.8
Nov 29, 2022 16:34:35.859225035 CET	53	64167	8.8.8.8	192.168.2.4
Nov 29, 2022 16:34:35.861438990 CET	53	58565	8.8.8.8	192.168.2.4
Nov 29, 2022 16:34:36.507632017 CET	61007	53	192.168.2.4	8.8.8.8
Nov 29, 2022 16:34:37.462059975 CET	61124	53	192.168.2.4	8.8.8.8
Nov 29, 2022 16:34:37.487755060 CET	53	61124	8.8.8.8	192.168.2.4
Nov 29, 2022 16:34:37.578932047 CET	59444	53	192.168.2.4	8.8.8.8
Nov 29, 2022 16:34:37.604933023 CET	53	59444	8.8.8.8	192.168.2.4
Nov 29, 2022 16:34:41.866458893 CET	56022	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:34:35.831396103 CET	192.168.2.4	8.8.8.8	0x965c	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:35.833471060 CET	192.168.2.4	8.8.8.8	0xc902	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:36.507632017 CET	192.168.2.4	8.8.8.8	0xff84	Standard query (0)	libertymutual-my.sharepoint.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:37.462059975 CET	192.168.2.4	8.8.8.8	0xddce	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:37.578932047 CET	192.168.2.4	8.8.8.8	0xf962	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:41.866458893 CET	192.168.2.4	8.8.8.8	0x1996	Standard query (0)	libertymutual-my.sharepoint.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 16:34:35.859225035 CET	8.8.8.8	192.168.2.4	0x965c	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:35.861438990 CET	8.8.8.8	192.168.2.4	0xc902	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:35.861438990 CET	8.8.8.8	192.168.2.4	0xc902	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	libertymutual-my.sharepoint.com	libertymutual.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	libertymutual.sharepoint.com	2462-ipv4v6e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false

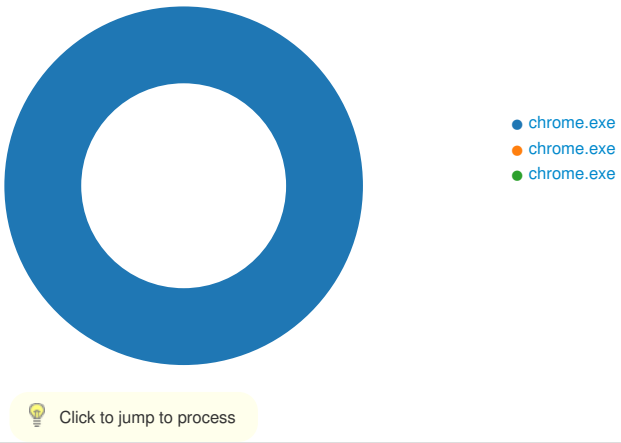
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	2462-ipv4v6e.clump.prod.aa-rt.sharepoint.com	18204-ipv4v6e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	18204-ipv4v6e.farm.prod.aa-rt.sharepoint.com	18204-ipv4v6e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	18204-ipv4v6.farm.prod.aa-rt.sharepoint.com.dual-spo-0003.spo-msedge.net	dual-spo-0003.spo-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	dual-spo-0003.spo-msedge.net		13.107.136.8	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:36.614840031 CET	8.8.8.8	192.168.2.4	0xff84	No error (0)	dual-spo-0003.spo-msedge.net		13.107.138.8	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:37.487755060 CET	8.8.8.8	192.168.2.4	0xddce	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:37.604933023 CET	8.8.8.8	192.168.2.4	0xf962	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	libertymutual-my.sharepoint.com	libertymutual.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	libertymutual.sharepoint.com	2462-ipv4v6e.clump.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	2462-ipv4v6e.clump.prod.aa-rt.sharepoint.com	18204-ipv4v6e.farm.prod.aa-rt.sharepoint.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	18204-ipv4v6e.farm.prod.aa-rt.sharepoint.com	18204-ipv4v6e.farm.prod.sharepointonline.com.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	18204-ipv4v6.farm.prod.aa-rt.sharepoint.com.dual-spo-0003.spo-msedge.net	dual-spo-0003.spo-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	dual-spo-0003.spo-msedge.net		13.107.136.8	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:34:41.974684954 CET	8.8.8.8	192.168.2.4	0x1996	No error (0)	dual-spo-0003.spo-msedge.net		13.107.138.8	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- clients2.google.com
- accounts.google.com
- libertymutual-my.sharepoint.com
- https:

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: **4916**, Parent PID: **2344**

General

Target ID:	0
Start time:	16:34:29
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 "about:blank
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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

Analysis Process: chrome.exe PID: **5664**, Parent PID: **4916**

General

Target ID:	1

Start time:	16:34:31
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-GB --service-sandbox-type=none --mojo-platform-channel-handle=1956 --field-trial-handle=1724,i,9580845018825437107,15182149715928468815,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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

Analysis Process: chrome.exe PID: **4688**, Parent PID: **2344**

General

Target ID:	2
Start time:	16:34:31
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" "https://libertymutual-my.sharepoint.com/:u:/p/avrial_cloud/Ef8voSU0ijFBkCGrbzr79P0B5chArPhF10rZzMyHQ8-awQ?email=jmiller%40wickersmith.com&e=nYNYdb
Imagebase:	0x7ff683680000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

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