ID: 791286
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 09:24:03
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

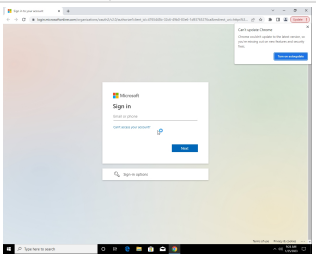
Windows Analysis Report

https://www.office.com/?auth=2&home=1

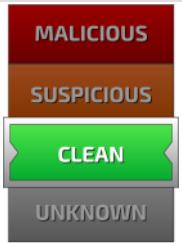
Overview

General Information

Sample URL:	https://www.office.com/?auth=2&home=1
Analysis ID:	791286



Detection

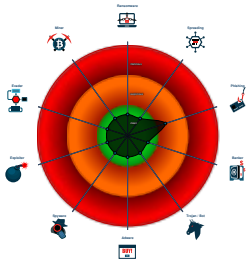


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- HTML body contains low number of …
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 1644 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://www.office.com/?auth=2&home=1 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 5328 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=2044 --field-trial-handle=1796,i,8177445550997338781,4573666773275504079,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

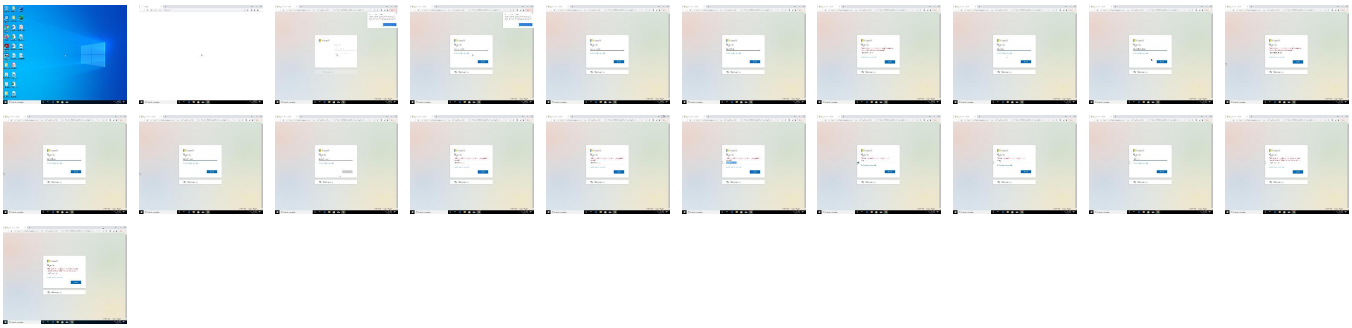
Mitre Att&ck Matrix

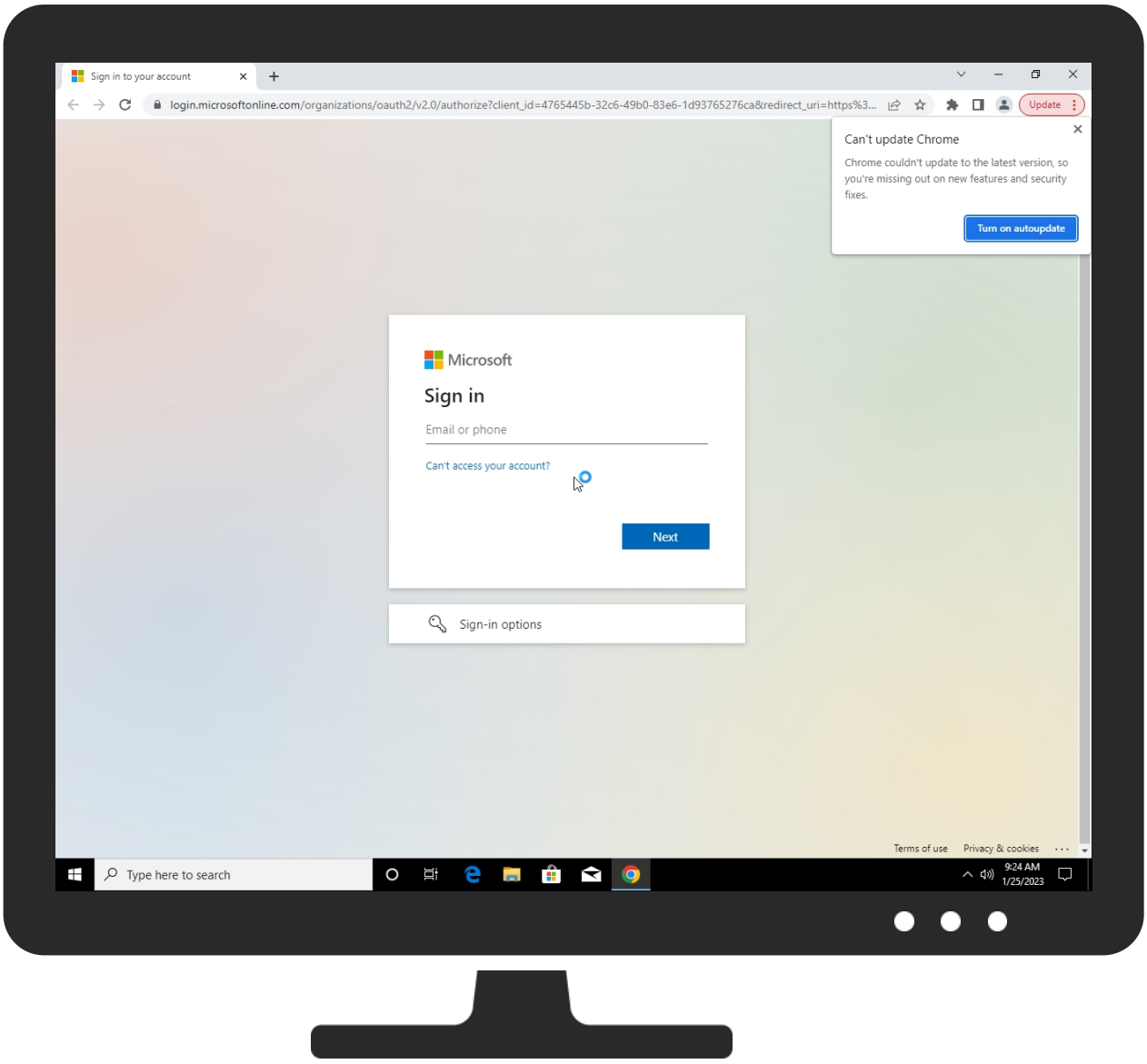
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 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	1 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	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
https://www.office.com/?auth=2&home=1	0%	Virustotal		Browse
https://www.office.com/?auth=2&home=1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

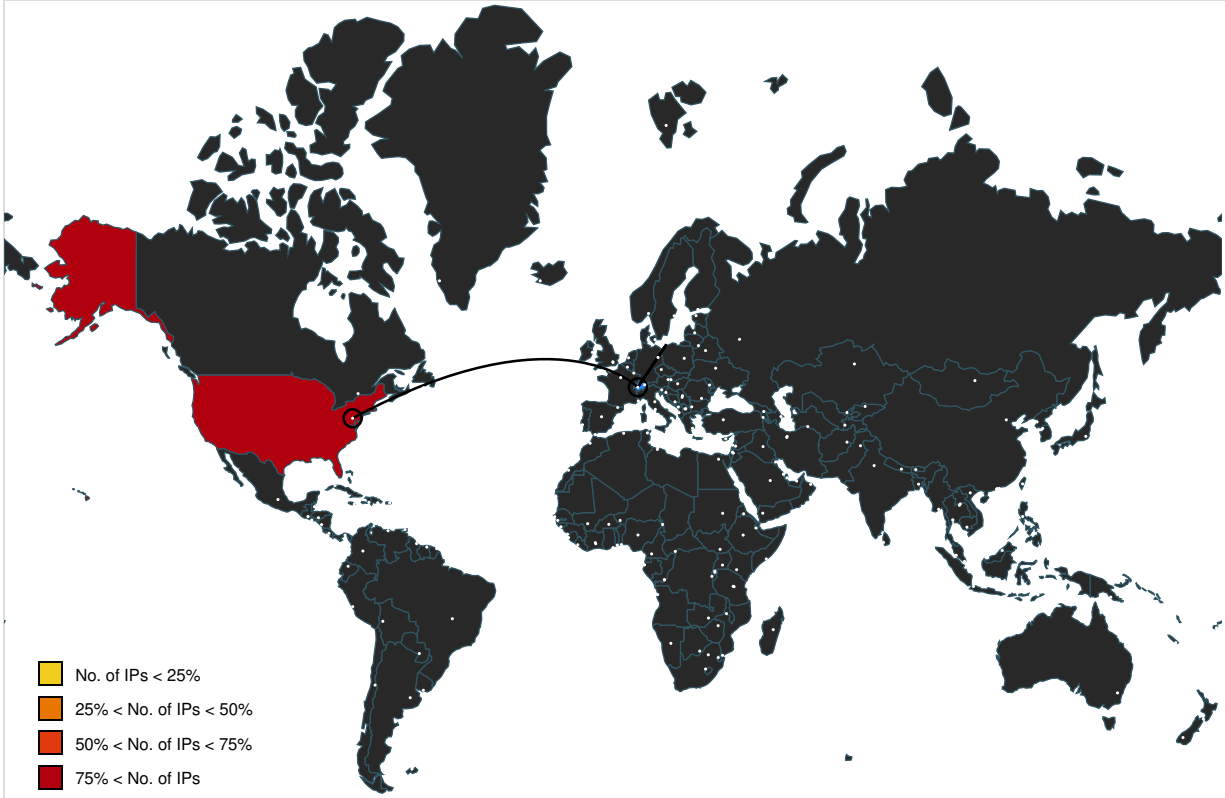
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false		unknown
accounts.google.com	142.250.186.77	true	false		high
www.google.com	142.250.181.228	true	false		high
part-0017.t-0009.fdv2-t-msedge.net	13.107.237.45	true	false		unknown
clients.l.google.com	142.250.185.238	true	false		high
www.office.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
identity.nel.measure.office.net	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false		unknown
login.microsoftonline.com	unknown	unknown	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.107.6.156	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.35	unknown	United States		15169	GOOGLEUS	false
142.250.186.67	unknown	United States		15169	GOOGLEUS	false
40.126.32.134	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
2.16.238.10	unknown	European Union		20940	AKAMAI-ASN1EU	false
142.250.185.238	clients.l.google.com	United States		15169	GOOGLEUS	false
40.126.32.72	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
40.126.32.74	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
142.250.185.164	unknown	United States		15169	GOOGLEUS	false
88.221.169.199	unknown	European Union		16625	AKAMAI-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.16.238.149	unknown	European Union		20940	AKAMAI-ASN1EU	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
142.250.186.77	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.184.202	unknown	United States		15169	GOOGLEUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791286
Start date and time:	2023-01-25 09:24:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://www.office.com/?auth=2&home=1
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:	8
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.win@27/0@10/168

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.64, 40.126.31.73, 20.190.159.73, 20.190.159.75, 20.190.159.4, 40.126.31.67, 20.190.159.71, 20.190.159.23, 13.107.6.156, 142.250.186.35, 40.126.32.134, 40.126.32.74, 40.126.32.133, 20.190.160.22, 20.190.160.20, 40.126.32.136, 40.126.32.68, 40.126.32.76, 34.104.35.123, 40.126.32.138, 40.126.32.72, 40.126.32.140, 2.16.238.149, 2.16.238.152, 20.190.160.14, 20.190.160.17, 88.221.169.152, 142.250.184.202, 142.250.186.170, 216.58.212.170, 216.58.212.138, 172.217.18.10, 142.250.186.138, 142.250.186.74, 142.250.186.106, 172.217.16.202, 142.250.184.234, 172.217.18.106, 142.250.185.202, 142.250.185.234, 142.250.185.138, 172.217.23.106, 142.250.186.42, 88.221.169.199
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, www.tm.lg.prod.aadmsa.akadns.net, e13678.dscb.akamaiedge.net, home-office365-com.b-0004.b-msedge.net, clientservices.googleapis.com, ak.privatelink.msidentity.com, a1894.dscb.akamai.net, www.tm.a.prd.aadg.trafficmanager.net, officehome.cdn.office.net-c.edgekey.net, www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net, www.microsoft.com-c-3.edgekey.net, prda.aadg.msidentity.com, officehome.cdn.office.net, login.live.com, login.msa.msidentity.com, www.tm.ak.prd.aadg.trafficmanager.net, fs.microsoft.com, content-autofill.googleapis.com, aadcdnoriginwus2.azureedge.net, b-0004.b-msedge.net, settings-win.data.microsoft.com, aadcdn.msauth.net, e19254.dscg.akamaiedge.net, login.msa.msidentity.com, firstparty-azurefd-prod.trafficmanager.net, edgedl.me.gvt1.com, nel.measure.office.net.edgesuite.net, privacy.microsoft.com, officehome.cdn.office.net-c.edgekey.net.globalredir.akadns.net, aadcdnoriginwus2.afd.azureedge.net, privacy.microsoft.com.
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteVirtualMemory calls found.

Created / dropped Files

No created / dropped files found

Static File Info

No static file info