ID: 708230
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 07:46:45
Date: 23/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

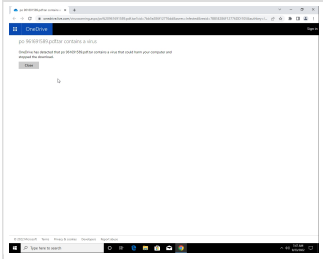
Windows Analysis Report

http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD!105&authkey...

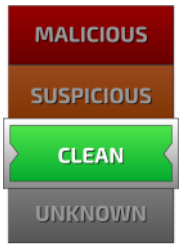
Overview

General Information

Sample URL:	http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD!105&authkey=AMOExoSCD2ywjes
Analysis ID:	708230



Detection

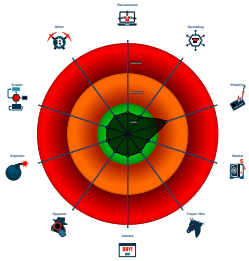


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Found iframes
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 2436 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD%21105&authkey=AMOExoSCD2ywjes MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 964 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=1912 --field-trial-handle=1800,i,18321044787883545475,3443962279196911152,131072 --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.

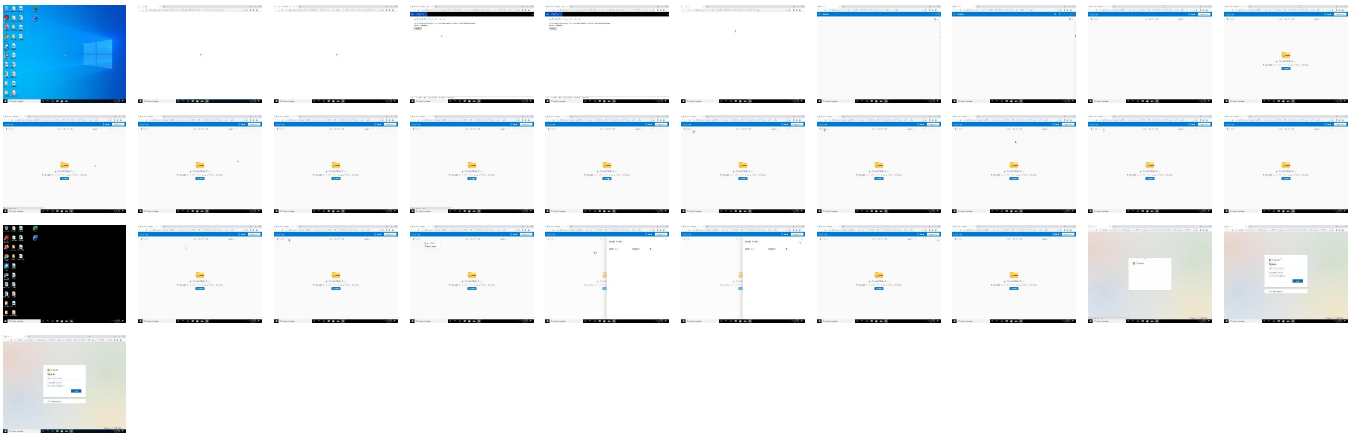
Mitre Att&ck Matrix

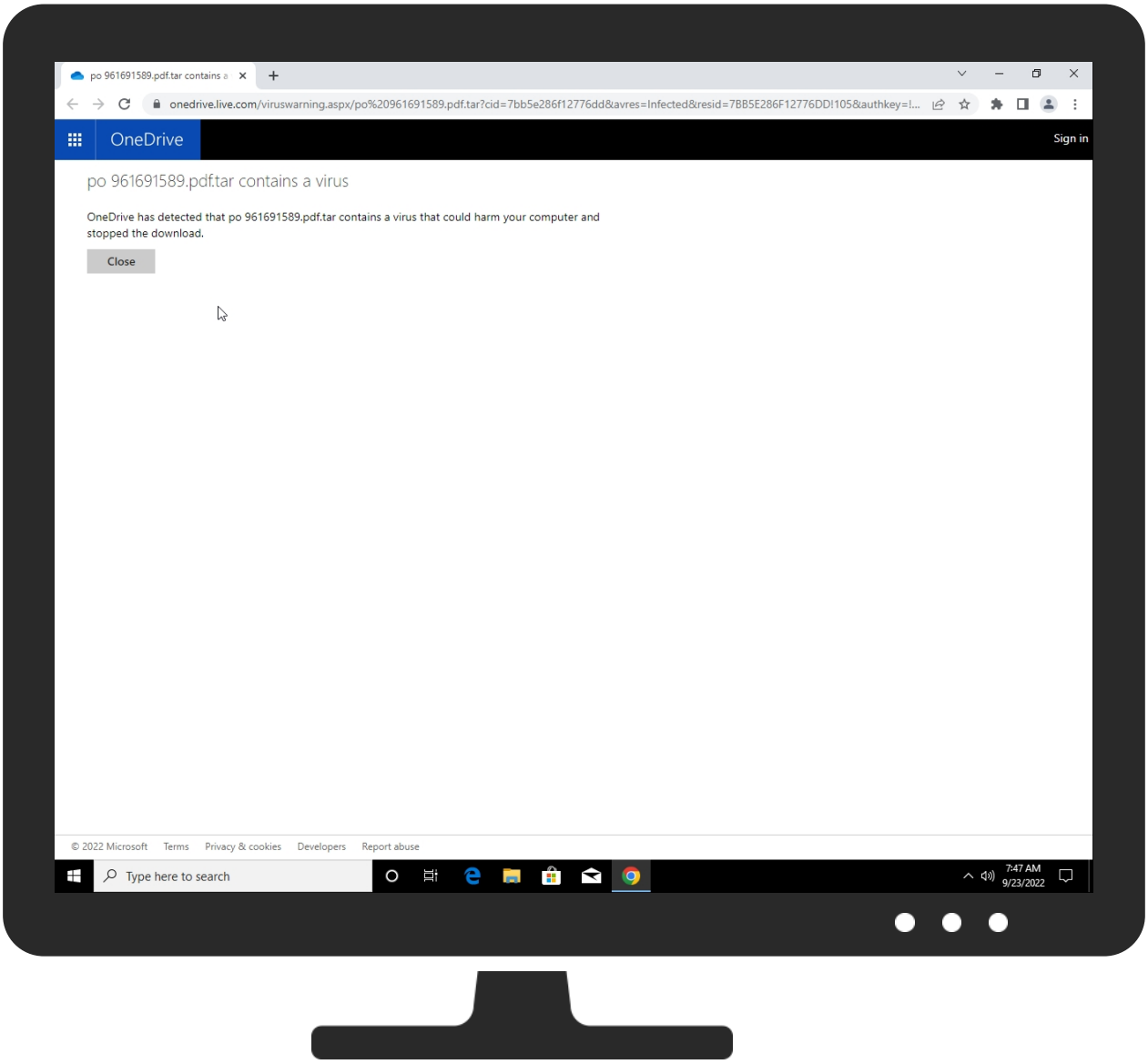
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Drive-by Compromise	Windows Management Instrumentation	Path Interception	1 Process Injection	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	1 Extra Window Memory Injection	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)	1 Extra Window Memory Injection	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
http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD%21105&authkey=AMOExoSCD2ywjes	0%	Avira URL Cloud	safe	
http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD%21105&authkey=AMOExoSCD2ywjes	1%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

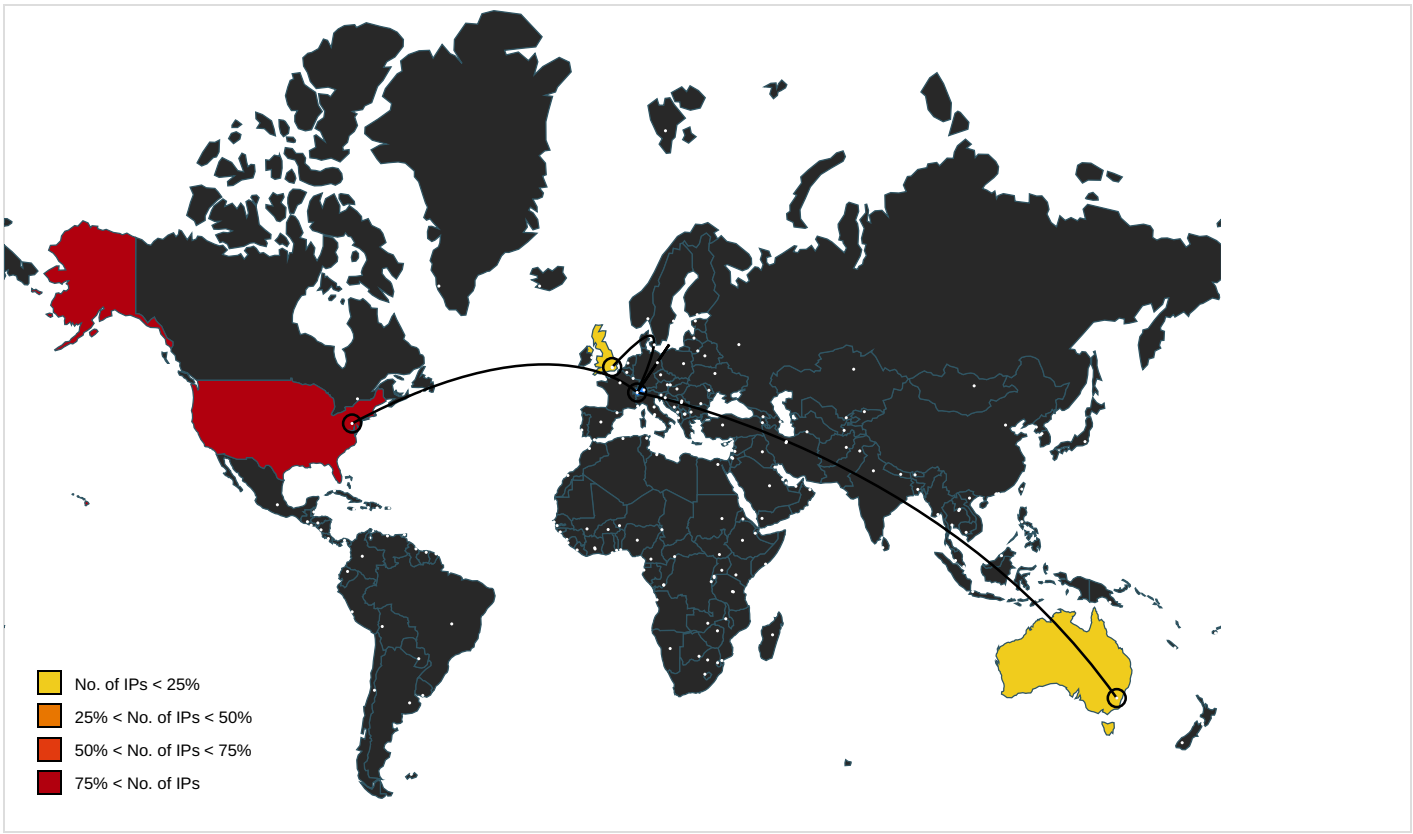
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.185.173	true	false		high
dual-a-0001.a-msedge.net	204.79.197.200	true	false		unknown
l-0003.l-dc-msedge.net	13.107.43.12	true	false		unknown
part-0017.t-0009.fbs1-t-msedge.net	13.107.219.45	true	false		unknown
i-am3p-cor006.api.p001.1drv.com	13.104.158.180	true	false		high
www.google.com	142.250.186.164	true	false		high
clients.l.google.com	142.250.185.206	true	false		high
c.live.com	unknown	unknown	false		high
shellprod.msocdn.com	unknown	unknown	false		unknown
storage.live.com	unknown	unknown	false		high
skyapi.onedrive.live.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
onedrive.live.com	unknown	unknown	false		high
wf6uzq.db.files.1drv.com	unknown	unknown	false		high
skydrive.live.com	unknown	unknown	false		high
api.onedrive.com	unknown	unknown	false		high
p.sfx.ms	unknown	unknown	false		high
amcdn.msftauth.net	unknown	unknown	false		unknown
dub01pap002files.storage.live.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://onedrive.live.com/?cid=7bb5e286f12776dd&id=7BB5E286F12776DD%21105&authkey=%21AMOExoSCD2ywjes	false		high
https://onedrive.live.com/viruswarning.aspx/po%20961691589.pdf.tar?cid=7bb5e286f12776dd&avres=Infected&resid=7BB5E286F12776DD!105&authkey=!AMOExoSCD2ywjes	false		high
https://onedrive.live.com/?authkey=%21AMOExoSCD2ywjes&cid=7BB5E286F12776DD&id=7BB5E286F12776DD%21105&parId=root&o=OneUp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
52.228.36.228	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
204.79.197.200	dual-a-0001.a-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.219.45	part-0017.t-0009.fbs1-t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.16.107.90	unknown	European Union		20940	AKAMAI-ASN1EU	false
13.95.147.73	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
51.11.192.49	unknown	United Kingdom		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.20.9.204	unknown	European Union		20940	AKAMAI-ASN1EU	false
40.126.31.71	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.43.12	l-0003.l-dc-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.43.13	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.189.173.14	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
104.91.71.141	unknown	United States		16625	AKAMAI-ASUS	false
13.104.208.162	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
184.51.105.213	unknown	United States		3257	GTT-BACKBONEGTTDE	false
23.54.139.180	unknown	United States		20940	AKAMAI-ASN1EU	false
142.250.186.163	unknown	United States		15169	GOOGLEUS	false
13.107.42.13	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
13.107.42.12	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
20.234.93.27	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
23.45.102.249	unknown	United States		20940	AKAMAI-ASN1EU	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.190.159.2	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.185	unknown	United States		15133	EDGECASTUS	false
2.20.8.220	unknown	European Union		20940	AKAMAI-ASN1EU	false
142.250.185.173	accounts.google.com	United States		15169	GOOGLEUS	false
40.90.128.17	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.221.169.199	unknown	European Union		16625	AKAMAI-ASUS	false
142.250.186.164	www.google.com	United States		15169	GOOGLEUS	false
152.199.21.175	unknown	United States		15133	EDGECASTUS	false
23.213.164.142	unknown	United States		16625	AKAMAI-ASUS	false
172.217.16.195	unknown	United States		15169	GOOGLEUS	false
142.250.185.74	unknown	United States		15169	GOOGLEUS	false
20.44.10.123	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.221.168.218	unknown	European Union		16625	AKAMAI-ASUS	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	708230
Start date and time:	2022-09-23 07:46:45 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	http://onedrive.live.com/download?cid=7BB5E286F12776DD&resid=7BB5E286F12776DD!105&authkey=AMOExoSCD2ywjes
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:	13
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@29/0@18/372

Warnings

- Exclude process from analysis (whitelisted): svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.4, 20.190.159.75, 20.190.159.23, 20.190.159.2, 20.190.159.68, 20.190.159.71, 20.190.159.64, 40.126.31.71, 172.217.16.195, 13.107.42.13, 34.104.35.123, 13.107.42.12, 52.228.36.228, 23.213.164.142, 13.95.147.73, 20.234.93.27, 2.16.107.90, 2.16.107.82, 20.189.173.14, 13.104.208.162, 23.54.139.180
- Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, odwebp.trafficmanager.net, c-msn-com-nsatc.trafficmanager.net, clientservices.googleapis.com, res-1.cdn.office.net, odc-commonafdrk-geo.onedrive.akadns.net, browser.events.data.trafficmanager.net, canadacentral1-odwebpl.cloudapp.net, l-0004.l-msedge.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, prda.aadg.msidentity.com, l-0003.l-msedge.net, login.live.com, common.be.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, modernb.akamai.odsp.cdn.office.net-c.edgesuite.net, a1883.dscd.akamai.net, common-emea.onedrive.akadns.net, odc-db-files-geo.onedrive.akadns.net, odwebpl.trafficmanager.net, odc-db-files-brs.onedrive.akadns.net, odc-commonafdrk-brs.onedrive.akadns.net, res-1.cdn.office.net-c.edgekey.net.globalredir.akadns.net, e7695.dscg.akamaiedge.net, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, onedscolprdwus13.westus.cloudapp.azure.com, westeurope1-odwebp.cloudapp.net, ctldl.windowsupdate.com, www.t
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

No created / dropped files found

Static File Info

No static file info