



ID: 756305
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 00:25:02
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-0f3428ae2124&acct=e9c112fa-3eae-493c-8bfc-d97737244948&er=7fde1f21-6f07-4a5d-8217-7c1e45a31ab1 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
Contacted URLs 6
World Map of Contacted IPs 6
Public IPs 6
Private 7
General Information 7
Warnings 7
Created / dropped Files 7
Static File Info 7

Copyright Joe Security LLC 2022

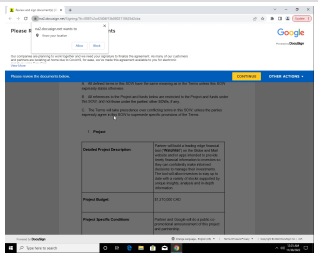
Windows Analysis Report

https://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-0f3428ae2124&acct...

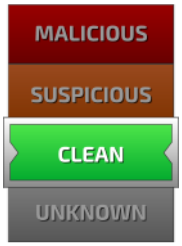
Overview

General Information

Sample URL:	https://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-...9c112fa-3eae-493c-8bfc-d97737244948&er=7fde1f21-6f07-4a5d-8217-7c1e45a31ab1
Analysis ID:	756305



Detection

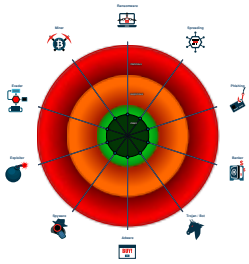


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 3652 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-0f3428ae2124&acct=e9c112fa-3eae-493c-8bfc-d97737244948&er=7fde1f21-6f07-4a5d-8217-7c1e45a31ab1 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 4072 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=2068 --field-trial-handle=1796,i,12823625518947830979,6690553971199126096,131072 --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

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

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

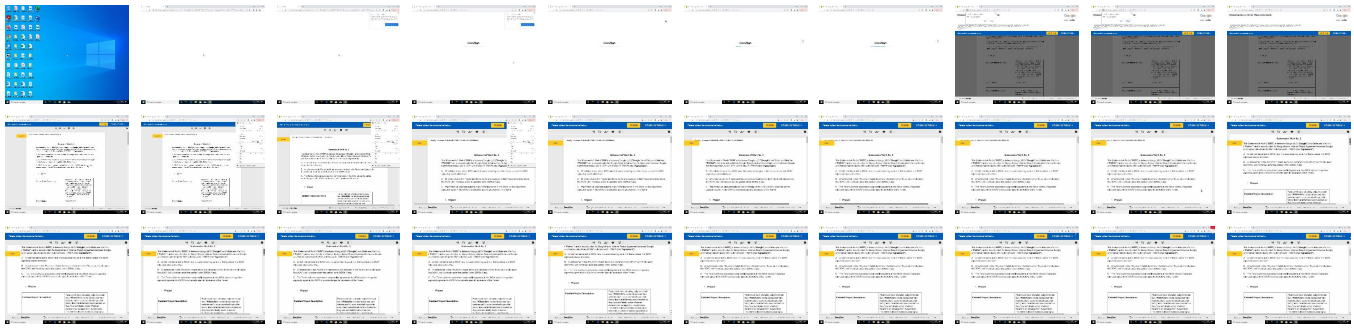
Mitre Att&ck Matrix

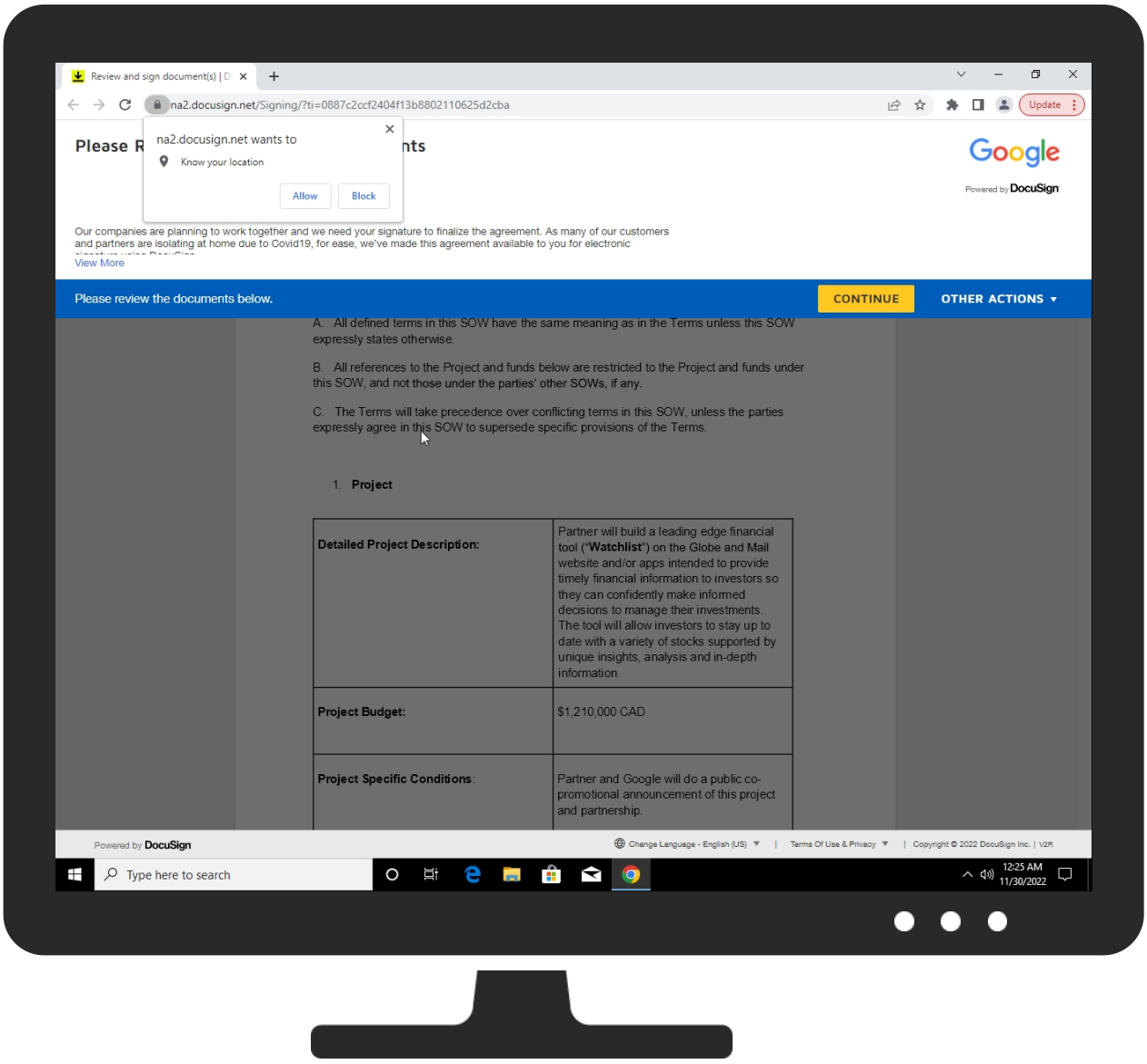
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	2 Masquerading	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://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-0f3428ae2124&act=e9c112fa-3eae-493c-8bfc-d97737244948&er=7fde1f21-6f07-4a5d-8217-7c1e45a31ab1	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2022

Domains and IPs

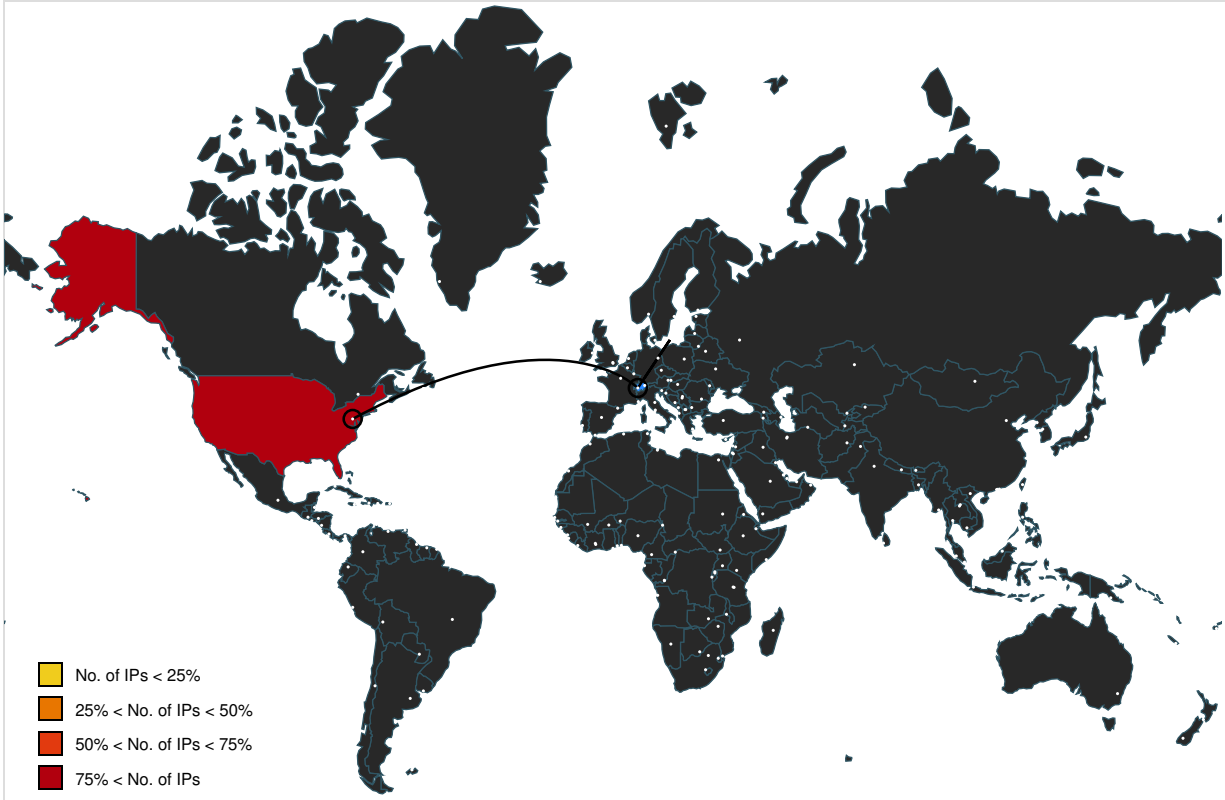
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	172.217.16.205	true	false		high
www.google.com	142.250.186.36	true	false		high
api.mixpanel.com	107.178.240.159	true	false		high
clients.l.google.com	142.250.185.206	true	false		high
arya-1323461286.us-west-2.elb.amazonaws.com	52.89.240.141	true	false		high
clients2.google.com	unknown	unknown	false		high
a.docusign.com	unknown	unknown	false		high
docucdn-a.akamaihd.net	unknown	unknown	false		high
na2.docusign.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://na2.docusign.net/Signing/?ti=0887c2ccf2404f13b8802110625d2cba	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.213.161.134	unknown	United States		20940	AKAMAI-ASN1EU	false
142.250.186.67	unknown	United States		15169	GOOGLEUS	false
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
142.250.186.36	www.google.com	United States		15169	GOOGLEUS	false
172.217.16.205	accounts.google.com	United States		15169	GOOGLEUS	false
52.89.240.141	arya-1323461286.us-west-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false
142.250.186.106	unknown	United States		15169	GOOGLEUS	false
107.178.240.159	api.mixpanel.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.99	unknown	United States		15169	GOOGLEUS	false
162.248.185.47	unknown	United States		62856	DOCUS-6-PRODUS	false
142.250.186.100	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:	756305
Start date and time:	2022-11-30 00:25:02 +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://na2.docusign.net/Signing/EmailStart.aspx?a=91c094aa-160d-4756-b8b7-0f3428ae2124&acct=e9c112fa-3eae-493c-8bfc-d97737244948&er=7fde1f21-6f07-4a5d-8217-7c1e45a31ab1
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:	clean0.win@25/0@10/139

Warnings

- Exclude process from analysis (whitelisted): svchost.exe
- Excluded IPs from analysis (whitelisted): 172.217.23.99, 162.248.185.47, 34.104.35.123, 23.213.161.134, 23.213.161.145, 142.250.186.106, 142.250.184.202, 142.250.186.138, 142.250.184.234, 172.217.18.10, 142.250.74.202, 142.250.186.170, 172.217.16.202, 216.58.212.170, 142.250.185.170, 142.250.186.42, 172.217.18.106, 172.217.23.106, 142.250.186.74, 142.250.181.234, 142.250.185.234
- Excluded domains from analysis (whitelisted): na2-west.docusign.net.akadns.net, a1737.b.akamai.net, fs.microsoft.com, edgedl.me.gvt1.com, content-autofill.googleapis.com, login.live.com, clientservices.googleapis.com, na2-geo.docusign.net.akadns.net, docucdn-a.akamaihd.net.edgesuite.net
- Not all processes where analyzed, report is missing behavior information
- 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