



ID: 791293
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 09:37:51
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report https://www.adobe.com/go/ConnectMac11Plus 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
World Map of Contacted IPs 6
Public IPs 6
Private 6
General Information 6
Warnings 7
Created / dropped Files 7
C:\Users\alfredo\Downloads\AdobeConnect_2022_10_42.dmg (copy) 7
C:\Users\alfredo\Downloads\AdobeConnect_2022_10_42.dmg.crdownload 7
C:\Users\alfredo\Downloads\dd33bf63-bcc2-421f-9a42-22e4888237f7.tmp 8
Static File Info 8

Copyright Joe Security LLC 2023

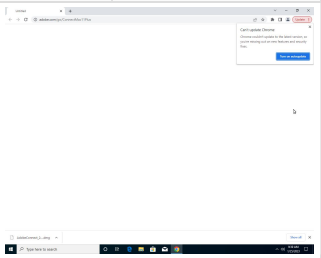
Windows Analysis Report

https://www.adobe.com/go/ConnectMac11Plus

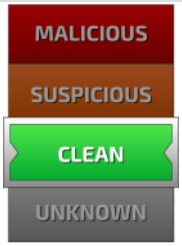
Overview

General Information

Sample URL:	https://www.adobe.com/go/ConnectMac11Plus
Analysis ID:	791293



Detection

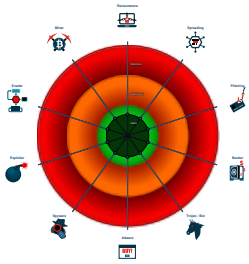


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64_ra**
- chrome.exe (PID: 2152 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument https://www.adobe.com/go/ConnectMac11Plus MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 3076 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=1792,i,15306135692962938665,157313184428459191 62,131072 --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 2023

Joe Sandbox Signatures

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

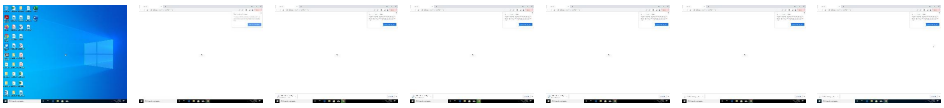
Mitre Att&ck Matrix

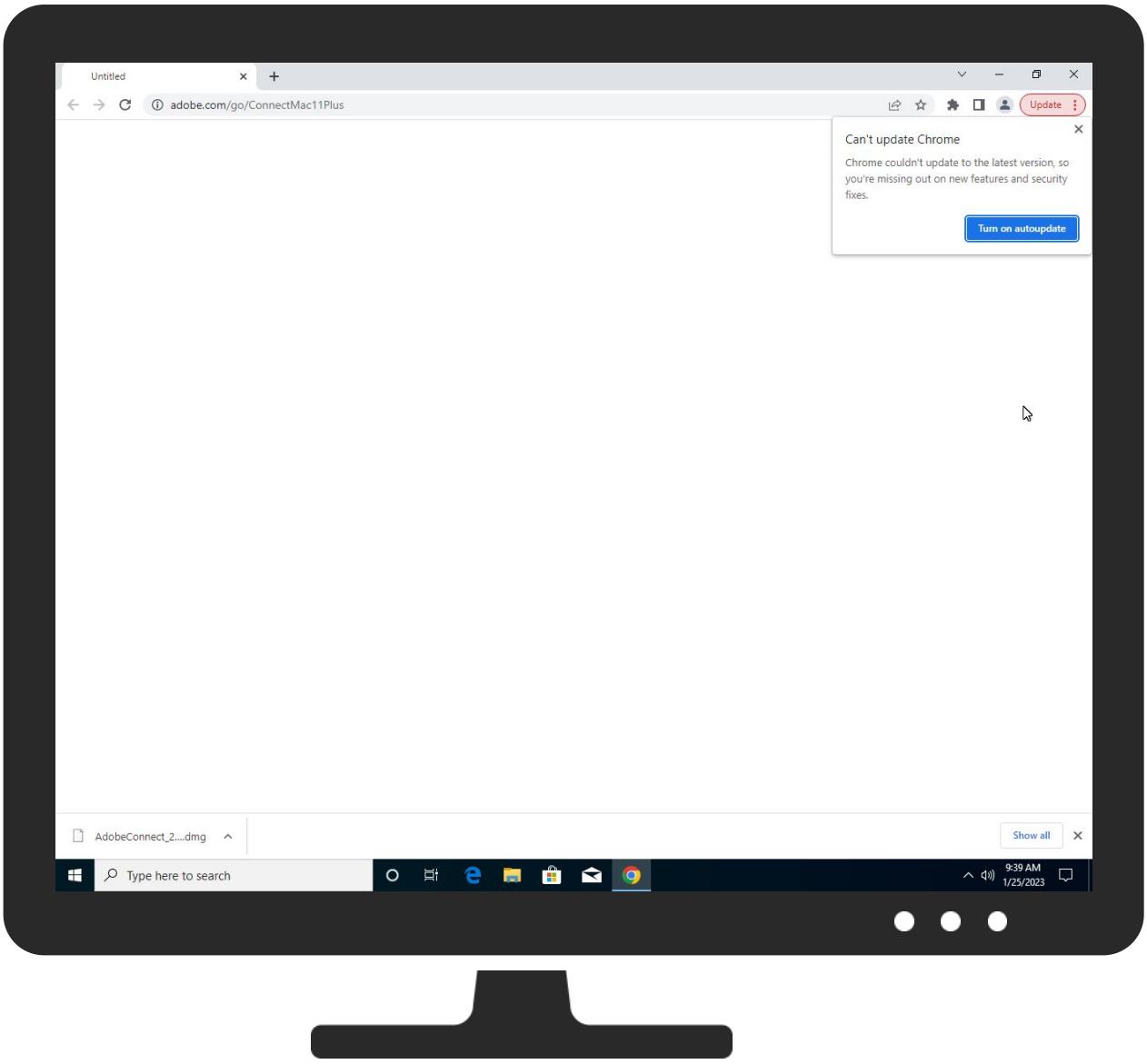
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

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.adobe.com/go/ConnectMac11Plus	0%	Virustotal		Browse
https://www.adobe.com/go/ConnectMac11Plus	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

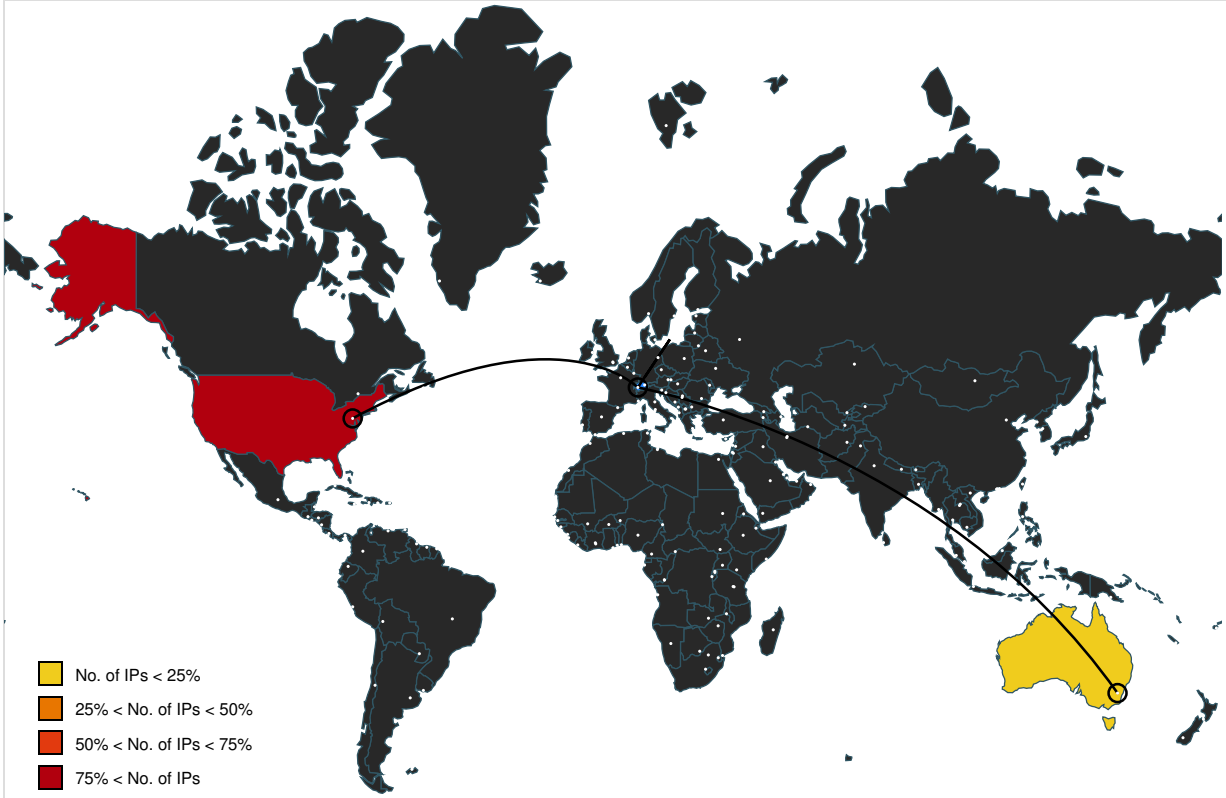
Copyright Joe Security LLC 2023

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.16.238.9	unknown	European Union		20940	AKAMAI-ASN1EU	false
2.19.126.84	unknown	European Union		16625	AKAMAI-ASUS	false
142.250.181.238	unknown	United States		15169	GOOGLEUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.212.131	unknown	United States		15169	GOOGLEUS	false
142.250.185.131	unknown	United States		15169	GOOGLEUS	false
216.58.212.132	unknown	United States		15169	GOOGLEUS	false
142.250.186.141	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:	791293
Start date and time:	2023-01-25 09:37:51 +01:00
Joe Sandbox Product:	CloudBasic

Copyright Joe Security LLC 2023

Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Sample URL:	https://www.adobe.com/go/ConnectMac11Plus
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:	12
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@26/3@0/107

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

C:\Users\alfredo\Downloads\AdobeConnect_2022_10_42.dmg (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	191610206
Entropy (8bit):	**7.9940299949210205**
Encrypted:	**true**
SSDEEP:	
MD5:	DE2BD886093C1561CF269AFE61C0E251
SHA1:	CEA8D88F741E0A5670135A922553AEB72C975FFC
SHA-256:	FE4ECAA3823E50A7A4443439982B27737AA636622FF42D7D3E8DB645F64A2766
SHA-512:	AA117968F7B6DE77E04E1B6F75D82CC7F00972B066D57FE22A0C0F2CEF392090D9EAF96020349125A4037015216B80D4B8CDCA80EB25F493563C069568C46CD
Malicious:	false
Reputation:	low
Preview:	x.su.T.p..a``d.a``..|S.H.y..2...P.....{.V5...#...o.. .1.....<...4..x.c`..C8.....^H..G.GBW...*..x....A.....%.M."...&...I..y...x....4o`6...]E..._..v.....IUTEz..q.....u..o.....vS.`..~u..:.t>..4 .?.B..... @..... @..... @..... @..... @..... @...../...p.Sx.su.T.p..a``d.a``..(..H1....Q@Q.P...P.....{.V5...#...o.....?..(..I...B...x.....0..... ..".... @..... @`]..... @..... @....)p...x....xTE.....A.Dd.....%...iH.m..."..eT.O.q.[q..;Q...22*....3`..`:..T.....%.&A.....%...=...h...:u.:u..(.....[..d..q%..3....x.e."Y..m\nZ..a.3\.?.).a6.1G.....~I...c m..5S..?.O6.W7.....5;....:b{.$...7L..S..[.....U.S{;O.w....|.`}{..z|WJK.N..JjT.?.2>...4..Ax..]...[.....%??....y.e..-..H.A...:...._...iq.....z.3...Hk%5..Om.#.....N.:.I.....|.H../.m8 .H.T.N...R|..%5...].W.T..O..m.y.T[7,.I.5..u.Vq...B.,.9.....7.....I.V....z].uE.K.F...J...!.n..9.k.4s.4.3..@...n..1.^xL6.....dHs.5.4.U...W..ztC.....#..".....6...}.r....p|.).K.

C:\Users\alfredo\Downloads\AdobeConnect_2022_10_42.dmg.crdownload

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	191610206
Entropy (8bit):	**7.9940299949210205**
Encrypted:	**true**
SSDEEP:	
MD5:	DE2BD886093C1561CF269AFE61C0E251
SHA1:	CEA8D88F741E0A5670135A922553AEB72C975FFC
SHA-256:	FE4ECAA3823E50A7A4443439982B27737AA636622FF42D7D3E8DB645F64A2766
SHA-512:	AA117968F7B6DE77E04E1B6F75D82CC7F00972B066D57FE22A0C0F2CEF392090D9EAF96020349125A4037015216B80D4B8CDCA80EB25F493563C069568C46CD
Malicious:	false
Reputation:	low

Preview:	x.su.T.p..a``d.a``..|S.H.y..2...P.....{.V5...#...o.. .1.....<...4..x.c`..C8.....^H..G.GBW...*..x....A.....%.M."...&...I..y...x....4o`6...]E..._..v.....IUTEz..q.....u..o.....vS.`..~u..:t>..4 .?.B..... @..... @..... @..... @..... @..... @...../...p.Sx.su.T.p..a``d.a``..(..H1....Q@Q.P...P.....{.V5...#...o.....?..(..!...B...x.....0..... ..."..... @..... @`]..... @..... @....)p...x....xTE.....A.Dd.....%...iH.m..."..eT.O.q.[q..;Q...22*....3`...`:..T.....%.&A.....%...=...h...:u.:u..(.....[..d..q%..3....x.e."Y..m\nZ..a.3\.?.).a6.1G.....~I...c m..5S..?.O6.W7.....5;....:b{.$...7L..S..[.....U.S{;O.w....|.`}{..z|WJK.N..JjT.?.2>...4..Ax..]...[.....%??....y.e..-..H.A...:..._...iq.....z.3...Hk%5..Om.#.....N..:|.....|.H../.m8 .H.T.N...R|..%5...].W.T..O..m.y.T[7,.|.5..u.Vq...B.,.9.....7.....I.V....z].uE.K.F...J...!.n..9.k.4s.4.3..@...n..1.^xL6.....dHs.5.4.U...W..ztC.....#.."......6...}.r....p|.).K.

C:\Users\alfredo\Downloads\dd33bf63-bcc2-421f-9a42-22e4888237f7.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	zlib compressed data
Category:	dropped
Size (bytes):	528128
Entropy (8bit):	**7.99793820227339**
Encrypted:	**true**
SSDEEP:	
MD5:	A3DE29AAFD4269236B3AF012BBDB15FC
SHA1:	3C257C12D4F8A386A4B3CFB732A8D918B7AA868B
SHA-256:	7DA974156BF40CBD5222CE6A20DED9F377F839ED33D785A83F7896F683ED456E
SHA-512:	0571581D32828695196936BAD3196D109736D4045FDEF47848D82428C4B79ACE6CBB71B13021D57C3207FFC708050CED809CC70FCD48B73DEFA13DE0E6C9360
Malicious:	false
Reputation:	low
Preview:	x.su.T.p..a``d.a``..|S.H.y..2...P.....{.V5...#...o.. .1.....<...4..x.c`..C8.....^H..G.GBW...*..x....A.....%.M."...&...I..y...x....4o`6...]E..._..v.....IUTEz..q.....u..o.....vS.`..~u..:t>..4 .?.B..... @..... @..... @..... @..... @..... @...../...p.Sx.su.T.p..a``d.a``..(..H1....Q@Q.P...P.....{.V5...#...o.....?..(..!...B...x.....0..... ..."..... @..... @`]..... @..... @....)p...x....xTE.....A.Dd.....%...iH.m..."..eT.O.q.[q..;Q...22*....3`...`:..T.....%.&A.....%...=...h...:u.:u..(.....[..d..q%..3....x.e."Y..m\nZ..a.3\.?.).a6.1G.....~I...c m..5S..?.O6.W7.....5;....:b{.$...7L..S..[.....U.S{;O.w....|.`}{..z|WJK.N..JjT.?.2>...4..Ax..]...[.....%??....y.e..-..H.A...:..._...iq.....z.3...Hk%5..Om.#.....N..:|.....|.H../.m8 .H.T.N...R|..%5...].W.T..O..m.y.T[7,.|.5..u.Vq...B.,.9.....7.....I.V....z].uE.K.F...J...!.n..9.k.4s.4.3..@...n..1.^xL6.....dHs.5.4.U...W..ztC.....#.."......6...}.r....p|.).K.

Static File Info

No static file info