



ID: 694551
Cookbook: urldownload.jbs
Time: 23:40:22
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading ATX.htm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 4
Snort Signatures 5
Joe Sandbox Signatures 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
Private 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\Users\user\Desktop\cmdline.out 11
C:\Users\user\Desktop\download\Downloading ATX.htm 11
Static File Info 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 12
UDP Packets 14
DNS Queries 14
DNS Answers 15
HTTP Request Dependency Graph 15
HTTPS Proxied Packets 15
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: cmd.exePID: 2668, Parent PID: 592 19
General 19
File Activities 19
Analysis Process: wget.exePID: 1568, Parent PID: 2668 20
General 20
File Activities 20
File Created 20
File Written 20
Analysis Process: chrome.exePID: 3024, Parent PID: 1136 20
General 20
File Activities 21
Registry Activities 21
Analysis Process: chrome.exePID: 2028, Parent PID: 3024 21
General 21
File Activities 21
Registry Activities 21
Disassembly 21

Copyright Joe Security LLC 2022

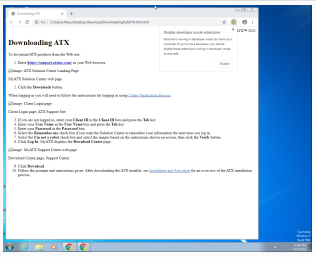
Windows Analysis Report

https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading ATX.h...

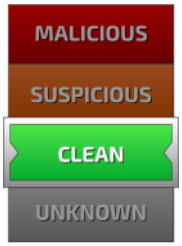
Overview

General Information

Sample URL:	http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading ATX.htm
Analysis ID:	694551
Infos:	



Detection

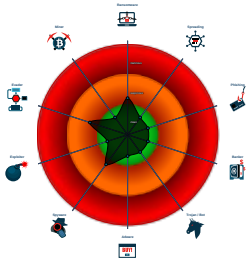


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Queries the volume information (nam…
- Very long cmdline option found, this…
- Allocates memory within range whic…
- Uses code obfuscation techniques (…
- Detected potential crypto function

Classification



Process Tree

- **System is w7x64**
- cmd.exe (PID: 2668 cmdline: C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm" > cmdline.out 2>&1 MD5: AD7B9C14083B52BC532FBA5948342B98)
  - wget.exe (PID: 1568 cmdline: wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm" MD5: 3DADB6E2ECE9C4B3E1E322E617658B60)
- chrome.exe (PID: 3024 cmdline: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized -- "C:\Users\user\Desktop\download\Downloading ATX.htm.html MD5: 6ACAE527E744C80997B25EF2A0485D5E)
  - chrome.exe (PID: 2028 cmdline: "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1008,10190009164659793 11,6662852395727443255,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1436 /prefetch:8 MD5: 6ACAE527E744C80997B25EF2A0485D5E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2022

Snort Signatures

No Snort rule has matched

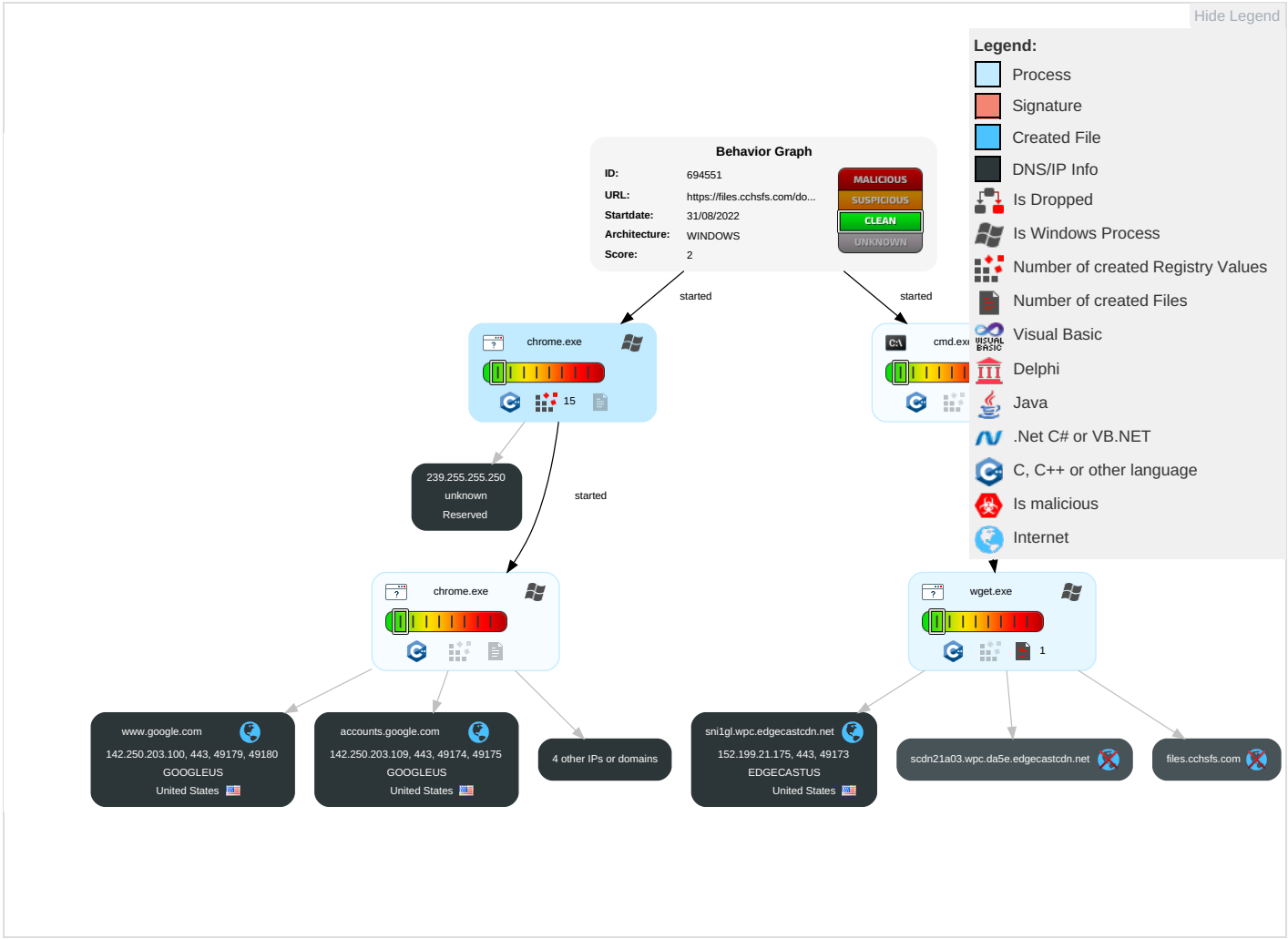
Joe Sandbox Signatures

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	1 2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 2 System Information Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 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	1 Remote System 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)	1 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

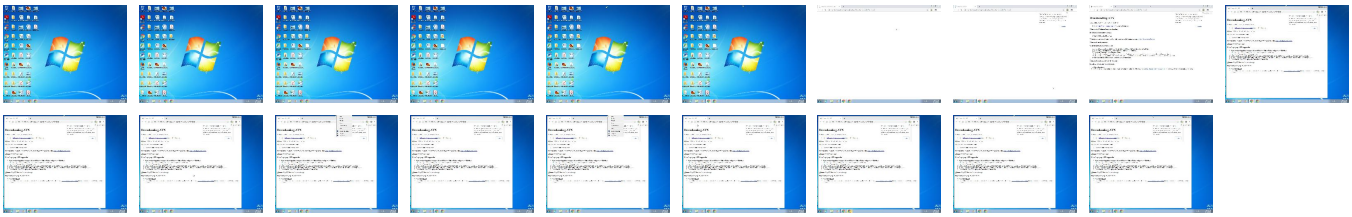
Behavior Graph

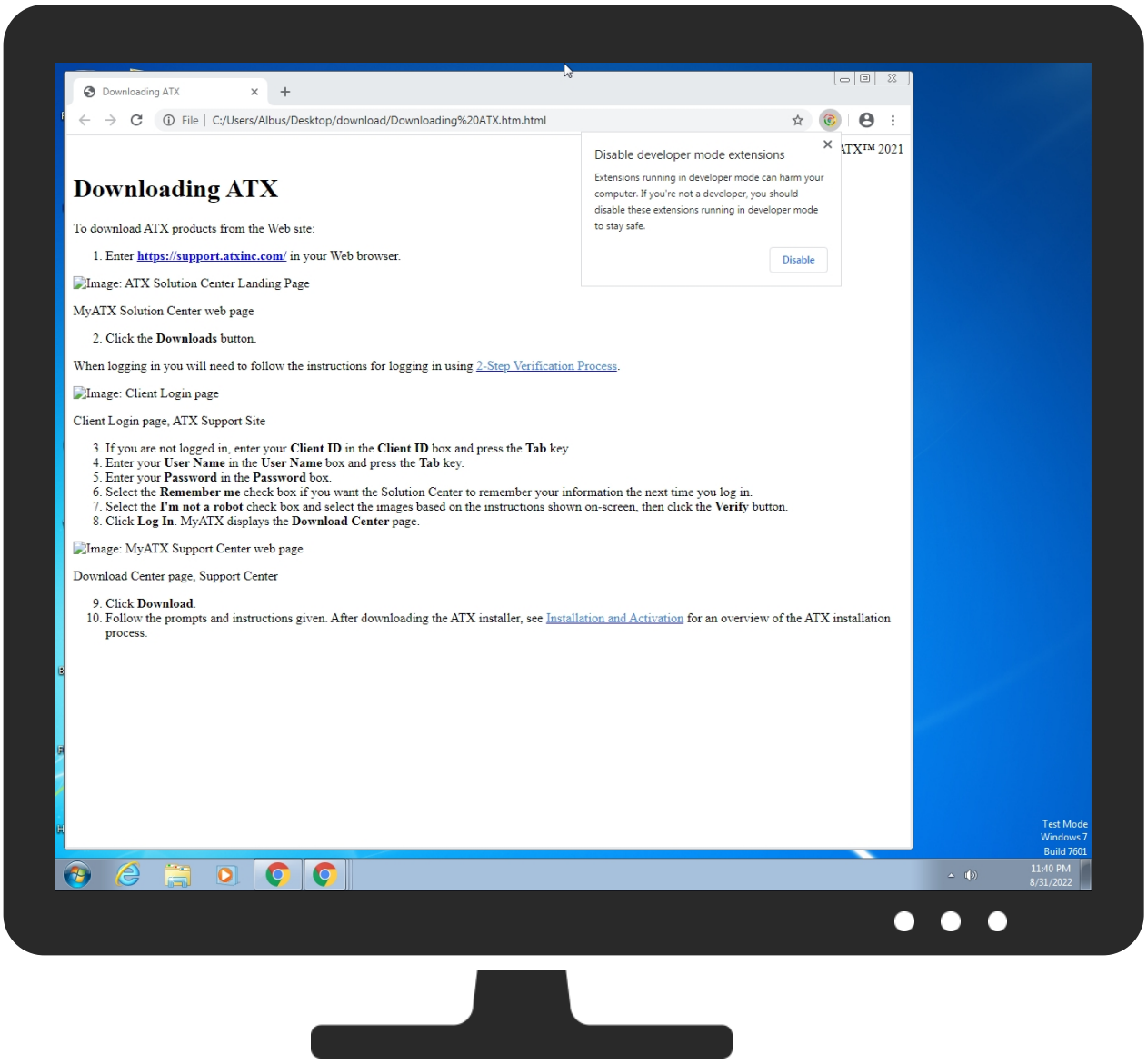


Screenshots

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://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm	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://support.atxinc.com/	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	142.250.203.109	true	false		high
www.google.com	142.250.203.100	true	false		high
clients.l.google.com	216.58.215.238	true	false		high
sni1gl.wpc.edgecastcdn.net	152.199.21.175	true	false		high
files.cchsfs.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high

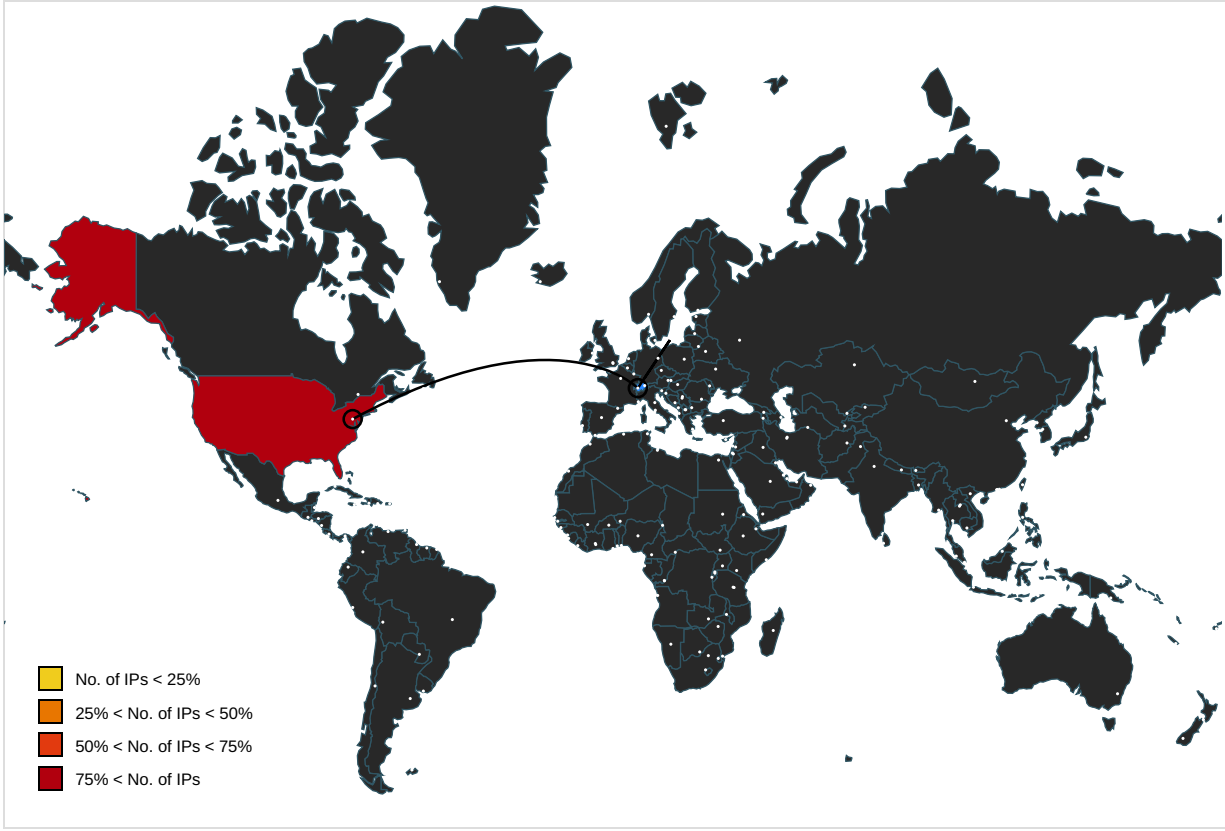
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
file:///C:/Users/user/Desktop/download/Downloading%20ATX.htm.html	false		low
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.google.com/jsapi	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc	false		high
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.atxinc.com/	Downloading ATX.htm.3.dr	false	• Avira URL Cloud: safe	unknown
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htmS	wget.exe, 00000003.00000002.913115920.000000007ED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.madcapsoftware.com/Schemas/MadCap.xsd	Downloading ATX.htm.3.dr	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm(	wget.exe, 00000003.00000002.913115920.000000007ED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htmJ	wget.exe, 00000003.00000002.912995632.000000000020000.00000004.00000020.00040000.00000000.sdmp	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htmW	wget.exe, 00000003.00000002.913203014.000000000910000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm:	wget.exe, 00000003.00000002.913115920.000000007ED000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.215.238	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
152.199.21.175	sni1gl.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
142.250.203.109	accounts.google.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.255
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694551
Start date and time:	2022-08-31 23:40:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	urldownload.jbs
Sample URL:	http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading ATX.htm
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@29/2@4/7
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, vga.dll, conhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 142.250.203.99, 34.104.35.123, 172.217.168.78
- Excluded domains from analysis (whitelisted): az393887.vo.msecnd.net, edgedl.me.gvt1.com, update.googleapis.com, clientservices.googleapis.com, www.gstatic.com, www.google-analytics.com
- Execution Graph export aborted for target wget.exe, PID 1568 because there are no executed function
- 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.

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

C:\Users\user\Desktop\cmdline.out	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	614
Entropy (8bit):	5.208818046642858
Encrypted:	false
SSDEEP:	12:HgFpdftToi4dENVCrWXCrwtT1De5RhKj1DbpbKb3ni1VmyRipbKb3RRa:SpRtTJ4d7rZrOxePgj1BbcEJRsbcLa
MD5:	886CD67138B262F20D4FEFDDE2C9D030
SHA1:	8DE41B7CCC15A8B4ADFAA1E21EB0F33A1ABF4B9F
SHA-256:	2ADB51673672E55B64534D773E5581F69B0C2B709BB74C5BC5AD164B57028D8E
SHA-512:	93A5052CA654C6B09890048D7FDE1035D0903312F204A9CD6431F64A71224418013BCA3E8C0723BBC1C8935FCA31535DD3115442B46156FD9CA2AD13AD3D466
Malicious:	false
Reputation:	low
Preview:	--2022-08-31 23:40:21-- https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm..Resolving files.cchsfs.com (files.cchsfs.com)... 152.199.21.175..Connecting to files.cchsfs.com (files.cchsfs.com)|152.199.21.175|:443... connected...HTTP request sent, awaiting response... 200 OK..Length: 8577 (8.4K) [text/html]..Saving to: 'C:/Users/user/Desktop/download/Downloading ATX.htm'.... 0K ..... 100% 86.4K=0.1s ....2022-08-31 23:40:23 (86.4 KB/s) - 'C:/Users/user/Desktop/download/Downloading ATX.htm' saved [8577/8577]....

C:\Users\user\Desktop\download\Downloading ATX.htm	
Process:	C:\Windows\SysWOW64\wget.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8577
Entropy (8bit):	4.948305470120674
Encrypted:	false
SSDEEP:	96:NGJK7LLipGgyNE10YE1oxSqeQKqxEYkY02Xusc:NGJK7u9115QQKJvR
MD5:	9F844B6827EF34B8BE5E6D3FDBADB6E9
SHA1:	3806E376AF067E23F25FA610EEEDB67858EF6695
SHA-256:	78D2CF034E63796F3B7B2281CDD4B5741AE3E260A9FD1D7C7BE4A41E796F75BF
SHA-512:	CAAB3D5AAF960C1220DC1542D752CF04FEE50926BF0E6DF930D4D6C253FB062D699D4886F2F7BB2DA7426C0AB502CA35C8F8D18BBE16C4E247F0B3EAC45AE1D0
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>..<html xmlns:MadCap="http://www.madcapsoftware.com/Schemas/MadCap.xsd" lang="en-us" xml:lang="en-us" data-mc-search-type="Stem" data-mc-help-system-file-name="Default.xml" data-mc-path-to-help-system="../../../" data-mc-toc-path="Installation and Activation" data-mc-target-type="WebHelp2" data-mc-runtime-file-type="Topic" data-mc-preload-images="false" data-mc-in-preview-mode="false">.. saved from url=(0016)http://localhost -->.. <head>.. <meta name="viewport" content="width=device-width, initial-scale=1.0" />.. <meta charset="utf-8" />.. <meta http-equiv="X-UA-Compatible" content="IE=edge" />.. <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />.. <meta name="msapplication-config" content="../../../Skins/Favicons/browserconfig.xml" />.. <link rel="shortcut icon" href="../../../Skins/Favicons/WK_F_Pos@x2.png" />.. <link rel="icon" sizes="32x32" href="../../../Skins/Favicons/WK_F_Pos@x2.png" />

Static File Info

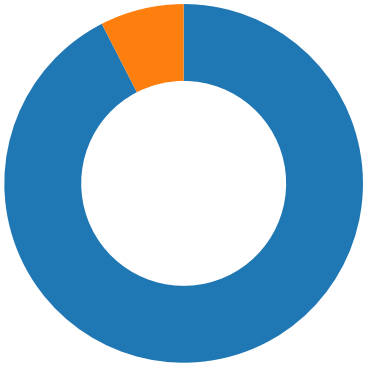
No static file info

Network Behavior

Network Port Distribution

Total Packets: 53

- 53 (DNS)
- 443 (HTTPS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:41:19.106123924 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.106163025 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.106218100 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.110198021 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.110217094 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.179549932 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.179743052 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.198069096 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.198112965 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.198365927 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.201191902 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.243365049 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.581839085 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.581958055 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.582048893 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.582050085 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:19.582094908 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.750538111 CEST	49173	443	192.168.2.22	152.199.21.175
Aug 31, 2022 23:41:19.750575066 CEST	443	49173	152.199.21.175	192.168.2.22
Aug 31, 2022 23:41:28.537720919 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.537770033 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.537839890 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.602472067 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.602543116 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.602699995 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.611823082 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.611857891 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.612135887 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.612179041 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.613923073 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:28.613965034 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.614036083 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:28.614372015 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:28.614387035 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.666033983 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.668195009 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.673752069 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.716207981 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.716249943 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.716799974 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.716856003 CEST	443	49175	142.250.203.109	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:41:28.717058897 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:28.717108965 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.717453957 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.717536926 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.718559027 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:28.718647003 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:28.719094038 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.719172955 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:28.719909906 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:28.719971895 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:29.508254051 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:29.508462906 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:29.508631945 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:29.508654118 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:29.508657932 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.508789062 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.509161949 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:29.509191990 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.509243965 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:29.509269953 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:29.543838024 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:29.543910027 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:29.543920040 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:29.543934107 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:29.543976068 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:29.586033106 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.586292028 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.586524963 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:29.587258101 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:29.719418049 CEST	443	49174	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:29.719526052 CEST	49174	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:30.180073977 CEST	49176	443	192.168.2.22	216.58.215.238
Aug 31, 2022 23:41:30.180113077 CEST	443	49176	216.58.215.238	192.168.2.22
Aug 31, 2022 23:41:30.180613041 CEST	49175	443	192.168.2.22	142.250.203.109
Aug 31, 2022 23:41:30.180650949 CEST	443	49175	142.250.203.109	192.168.2.22
Aug 31, 2022 23:41:30.784313917 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.784372091 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.784447908 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.785588026 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.785653114 CEST	443	49180	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.785727024 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.793322086 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.793380976 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.793853998 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.793900967 CEST	443	49180	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.850653887 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.855654001 CEST	443	49180	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.893690109 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.893723011 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.895031929 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.895117998 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.905047894 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:30.905132055 CEST	443	49180	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.907831907 CEST	443	49180	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:30.907919884 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:31.997870922 CEST	49179	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:31.998112917 CEST	49180	443	192.168.2.22	142.250.203.100
Aug 31, 2022 23:41:31.998135090 CEST	443	49179	142.250.203.100	192.168.2.22
Aug 31, 2022 23:41:31.998294115 CEST	443	49180	142.250.203.100	192.168.2.22

Copyright Joe Security LLC 2022

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:41:18.937033892 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 31, 2022 23:41:27.871912956 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:28.023561954 CEST	50108	53	192.168.2.22	8.8.8.8
Aug 31, 2022 23:41:28.043100119 CEST	53	50108	8.8.8.8	192.168.2.22
Aug 31, 2022 23:41:28.113667965 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:28.225126982 CEST	54723	53	192.168.2.22	8.8.8.8
Aug 31, 2022 23:41:28.244508982 CEST	53	54723	8.8.8.8	192.168.2.22
Aug 31, 2022 23:41:28.618118048 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:28.863960028 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:28.933747053 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:29.368880033 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:29.614661932 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:29.683285952 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:30.433396101 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:30.756593943 CEST	55244	53	192.168.2.22	8.8.8.8
Aug 31, 2022 23:41:30.775914907 CEST	53	55244	8.8.8.8	192.168.2.22
Aug 31, 2022 23:41:34.031162024 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:34.032438040 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:34.373091936 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:34.781018972 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:34.781955957 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:35.125859022 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:35.531505108 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:35.547050953 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:35.890403986 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:36.328377962 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:36.329225063 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:37.089637995 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:37.089874029 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:37.854212046 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:37.854537010 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:38.463912010 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:39.212840080 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:39.379249096 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:39.380043983 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:39.380413055 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:39.963140965 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.123166084 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.123651028 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.123667002 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.880435944 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.880568981 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:40.880574942 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:41:47.565970898 CEST	138	138	192.168.2.22	192.168.2.255
Aug 31, 2022 23:42:27.999362946 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:42:28.757688046 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:42:29.522181034 CEST	137	137	192.168.2.22	192.168.2.255
Aug 31, 2022 23:43:17.124361992 CEST	138	138	192.168.2.22	192.168.2.255

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:41:18.937033892 CEST	192.168.2.22	8.8.8.8	0x5f2b	Standard query (0)	files.cchsfs.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:41:28.023561954 CEST	192.168.2.22	8.8.8.8	0x6d1	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:41:28.225126982 CEST	192.168.2.22	8.8.8.8	0xabf0	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:41:30.756593943 CEST	192.168.2.22	8.8.8.8	0x77e8	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:41:19.084029913 CEST	8.8.8.8	192.168.2.22	0x5f2b	No error (0)	files.cchsfs.com	az393887.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:41:19.084029913 CEST	8.8.8.8	192.168.2.22	0x5f2b	No error (0)	scdn21a03.wpc.da5e.edgecastcdn.net	sni1gl.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:41:19.084029913 CEST	8.8.8.8	192.168.2.22	0x5f2b	No error (0)	sni1gl.wpc.edgecastcdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 31, 2022 23:41:28.043100119 CEST	8.8.8.8	192.168.2.22	0x6d1	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:41:28.043100119 CEST	8.8.8.8	192.168.2.22	0x6d1	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 31, 2022 23:41:28.244508982 CEST	8.8.8.8	192.168.2.22	0xabf0	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
Aug 31, 2022 23:41:30.775914907 CEST	8.8.8.8	192.168.2.22	0x77e8	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- files.cchsfs.com
- accounts.google.com
- clients2.google.com
- www.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49173	152.199.21.175	443	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:19 UTC	0	OUT	GET /doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko Accept: */* Accept-Encoding: identity Host: files.cchsfs.com Connection: Keep-Alive
2022-08-31 21:41:19 UTC	0	IN	HTTP/1.1 200 OK Cache-Control: public, max-age=60 Content-MD5: n4RLaCfvNLi+Xm0/26226Q== Content-Type: text/html Date: Wed, 31 Aug 2022 21:41:19 GMT Etag: 0x8DA5EB947286FBB Last-Modified: Tue, 05 Jul 2022 19:05:08 GMT Server: Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0 x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5945c6da-201e-004b-5282-bdbe5e000000 x-ms-version: 2009-09-19 Content-Length: 8577 Connection: close

Copyright Joe Security LLC 2022

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:19 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3a 4d 61 64 43 61 70 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 61 64 63 61 70 73 6f 66 74 77 61 72 65 2e 63 6f 6d 2f 53 63 68 65 6d 61 73 2f 4d 61 64 43 61 70 2e 78 73 64 22 20 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 64 61 74 61 2d 6d 63 2d 73 65 61 72 63 68 2d 74 79 70 65 3d 22 53 74 65 6d 22 20 64 61 74 61 2d 6d 63 2d 68 65 6c 70 2d 73 79 73 74 65 6d 2d 66 69 6c 65 2d 6e 61 6d 65 3d 22 44 65 66 61 75 6c 74 2e 78 6d 6c 22 20 64 61 74 61 2d 6d 63 2d 70 61 74 68 2d 74 6f 2d 68 65 6c 70 2d 73 79 73 74 65 6d 3d 22 2e 2e 2f 2e 2e 2f 2e 2e 2f 22 20 64 61 74 61 2d 6d 63 2d 74 6f 63 2d 70 61 74 68 3d 22 49 6e 73 74 61 6c 6c 61 74 Data Ascii: <!DOCTYPE html><html xmlns:MadCap="http://www.madcapsoftware.com/Schemas/MadCap.xsd" lang="en-us" xml:lang="en-us" data-mc-search-type="Stem" data-mc-help-system-file-name="Default.xml" data-mc-path-to-help-system="../../../" data-mc-toc-path="Installat

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	142.250.203.109	443	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:29 UTC	9	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=WP.289365
2022-08-31 21:41:29 UTC	9	OUT	Data Raw: 20 Data Ascii:
2022-08-31 21:41:29 UTC	12	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 31 Aug 2022 21:41:29 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*, ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-platform=*, ch-ua-platform-version=* Accept-CH: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version, Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Content-Security-Policy: script-src 'report-sample' 'nonce-gGY1VIbByA5xUy7uhQDiww' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'unsafe-inline' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport/allowlist Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-31 21:41:29 UTC	13	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2022-08-31 21:41:29 UTC	13	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49176	216.58.215.238	443	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:29 UTC	9	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-84.0.4147.135 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-31 21:41:29 UTC	10	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-_am273qQR5n9K-DIEGfhdQ' 'unsafe-inline' 'strict-dynamic' https: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 31 Aug 2022 21:41:29 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5721 X-Daystart: 52889 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-31 21:41:29 UTC	11	IN	Data Raw: 33 31 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 32 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 32 38 38 39 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" protocol="2.0" server="prod"><daystart elapsed_days="5721" elapsed_seconds="52889"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-08-31 21:41:29 UTC	11	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-08-31 21:41:29 UTC	12	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49179	142.250.203.100	443	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:32 UTC	13	OUT	GET /jsapi HTTP/1.1 Host: www.google.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36 Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=WP.289365

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:32 UTC	14	IN	HTTP/1.1 301 Moved Permanently Location: https://www.gstatic.com/charts/loader.js X-Content-Type-Options: nosniff Server: sffe Content-Length: 237 X-XSS-Protection: 0 Date: Wed, 31 Aug 2022 21:26:40 GMT Expires: Wed, 31 Aug 2022 21:56:40 GMT Cache-Control: public, max-age=1800 Content-Type: text/html; charset=UTF-8 Age: 892 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-08-31 21:41:32 UTC	14	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 31 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 63 68 61 72 74 73 2f 6c 6f 61 64 65 72 2e 6a 73 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>301 Moved</TI TLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://www.gstatic.com/charts/loa der.js">here</A>.</BODY></HTML>

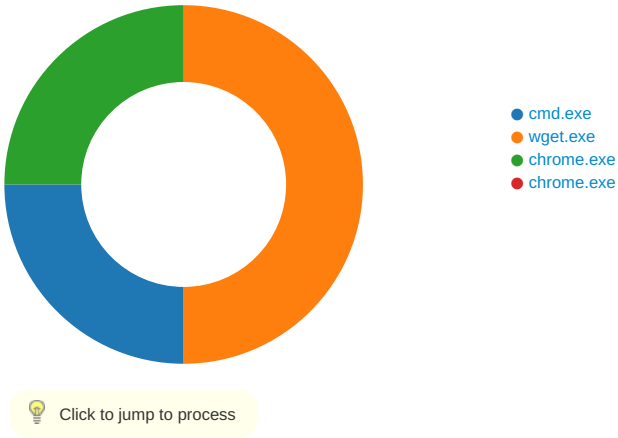
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49198	216.58.215.238	443	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:42 UTC	14	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel= &prodversion=84.0.4147.135&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: bg X-Goog-Update-AppId: nmmhkkegccagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-84.0.4147.135 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.135 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-31 21:41:42 UTC	15	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-YkIoTAhSSDf2hRsRLYKwdA' 'unsafe-inline' 'strict-dynamic' http s: http:;object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 31 Aug 2022 21:41:42 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5721 X-Daystart: 52902 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-08-31 21:41:42 UTC	16	IN	Data Raw: 33 31 61 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 37 32 31 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 35 32 39 30 32 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 31a<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5721" elapsed_seconds="52902"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:41:42 UTC	16	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2022-08-31 21:41:42 UTC	17	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **2668**, Parent PID: **592**

General

Target ID:	0
Start time:	23:40:18
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm" > cmdline.out 2>&1
Imagebase:	0x4a0b0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: wget.exe PID: **1568**, Parent PID: **2668**

General

Target ID:	3
Start time:	23:40:20
Start date:	31/08/2022
Path:	C:\Windows\SysWOW64\wget.exe
Wow64 process (32bit):	true
Commandline:	wget -t 2 -v -T 60 -P "C:\Users\user\Desktop\download" --no-check-certificate --content-disposition --user-agent="Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; AS; rv:11.0) like Gecko" "https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htm"
Imagebase:	0x400000
File size:	3895184 bytes
MD5 hash:	3DADB6E2ECE9C4B3E1E322E617658B60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\Downloading ATX.htm	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	46596C	fopen

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\download\Downloading ATX.htm	0	4096	3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3a 4d 61 64 43 61 70 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6d 61 64 63 61 70 73 6f 66 74 77 61 72 65 2e 63 6f 6d 2f 53 63 68 65 6d 61 73 2f 4d 61 64 43 61 70 2e 78 73 64 22 20 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 64 61 74 61 2d 6d 63 2d 73 65 61 72 63 68 2d 74 79 70 65 3d 22 53 74 65 6d 22 20 64 61 74 61 2d 6d 63 2d 68 65 6c 70 2d 73 79 73 74 65 6d 2d 66 69 6c 65 2d 6e 61 6d 65 3d 22 44 65 66 61 75 6c 74 2e 78 6d 6c 22 20 64 61 74 61 2d 6d 63 2d 70 61 74 68 2d 74 6f 2d 68 65 6c 70 2d 73 79 73 74 65 6d 3d 22 2e 2e 2f 2e 2e 2f 2e 2e 2f 22 20 64 61 74 61 2d 6d 63 2d 74 6f 63 2d 70 61 74 68 3d 22 49 6e 73 74 61 6c 6c 61 74	<!DOCTYPE html><html xmlns:MadCap="http://www.madcapsoftware.com/Schemas/MadCap.xsd" lang="en-us" xml:lang="en-us" data-mc-search-type="Stem" data-mc-help-system-file-name="Default.xml" data-mc-path-to-help-system="../../../" data-mc-toc-path="Installat	success or wait	1	47F21C	fwrite

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: chrome.exe PID: **3024**, Parent PID: **1136**

General

Target ID:	4
Start time:	23:40:25
Start date:	31/08/2022
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --start-maximized -- "C:\Users\user\Desktop\download\Downloading ATX.htm.html
Imagebase:	0x13f4f0000
File size:	1820656 bytes
MD5 hash:	6ACAE527E744C80997B25EF2A0485D5E
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

Registry Activities

Analysis Process: chrome.exe PID: **2028**, Parent PID: **3024**

General

Target ID:	5
Start time:	23:40:27
Start date:	31/08/2022
Path:	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1008 ,1019000916465979311,6662852395727443255,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1436 /prefetch:8
Imagebase:	0x13f4f0000
File size:	1820656 bytes
MD5 hash:	6ACAE527E744C80997B25EF2A0485D5E
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

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