ID: 694551
Cookbook: urldownload.jbs
Time: 23:48:02
Date: 31/08/2022
Version: 35.0.0 Citrine

Table of Contents

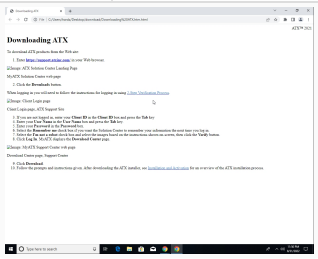
Windows Analysis Report

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

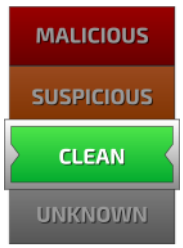
Overview

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

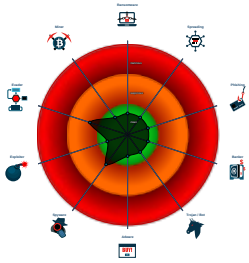


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Queries the volume information (nam...
- Very long cmdline option found, this...
- Deletes files inside the Windows fol...
- Uses code obfuscation techniques (...

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 5992 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: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 2804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wget.exe (PID: 4968 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: 5396 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\download\Downloading ATX.htm.html MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
  - chrome.exe (PID: 2080 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=1588 --field-trial-handle=1724,i,8435291165856388015,4643082473579285808,131072 /prefetch:8 MD5: 0FEC2748F363150DC54C1CAFFB1A9408)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

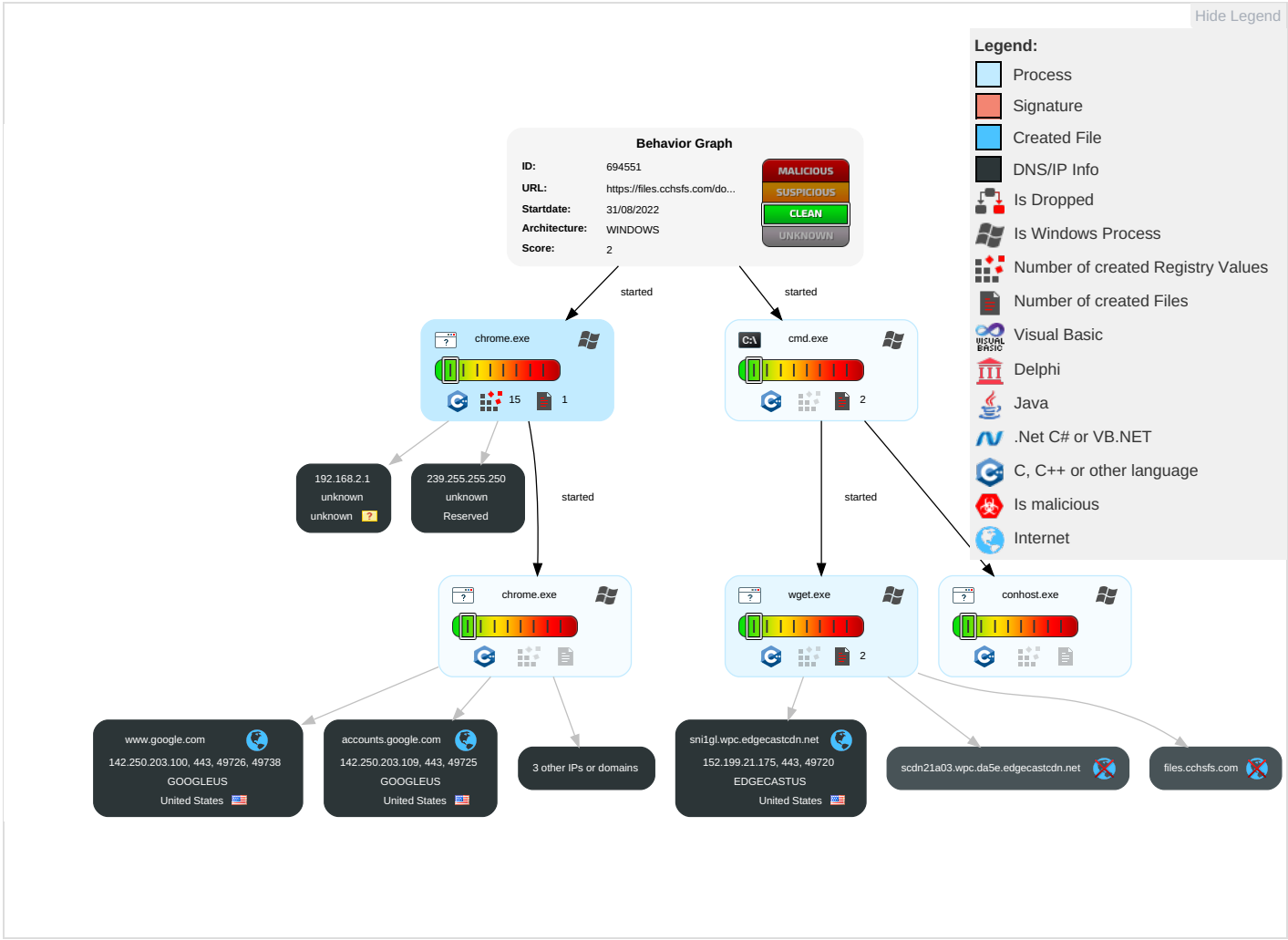
Joe Sandbox Signatures

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	1 2 Command and Scripting Interpreter	Path Interception	1 Process Injection	3 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	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 2 System Information 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	1 Remote System Discovery	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)	1 File Deletion	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

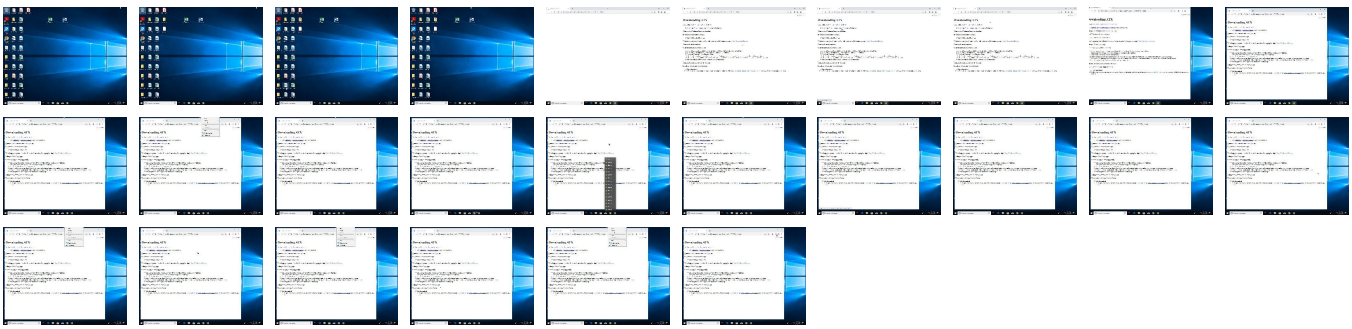
Behavior Graph

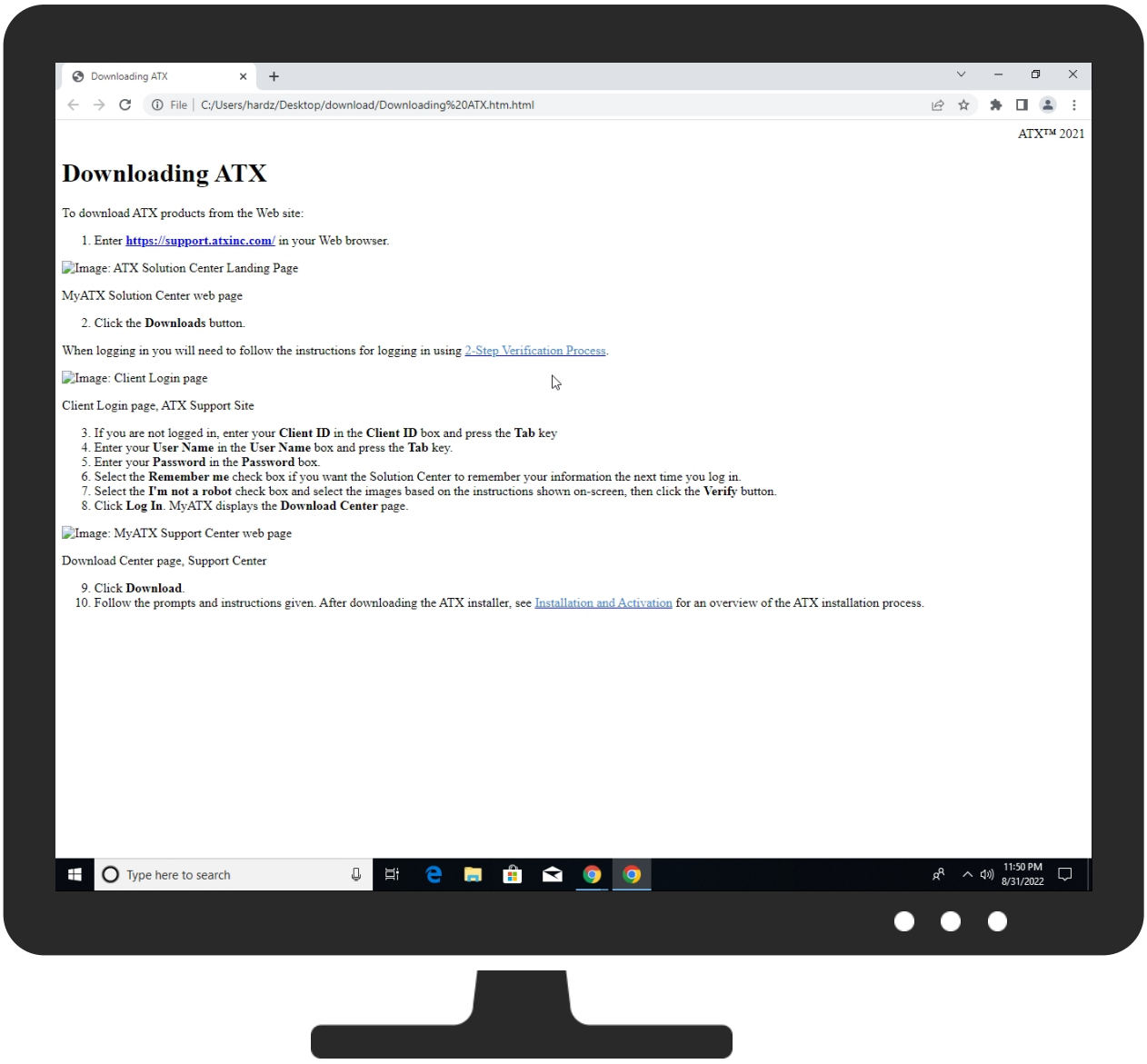


Screenshots

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%	Virustotal		Browse
http://https://support.atxinc.com/	0%	Avira URL Cloud	safe	

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

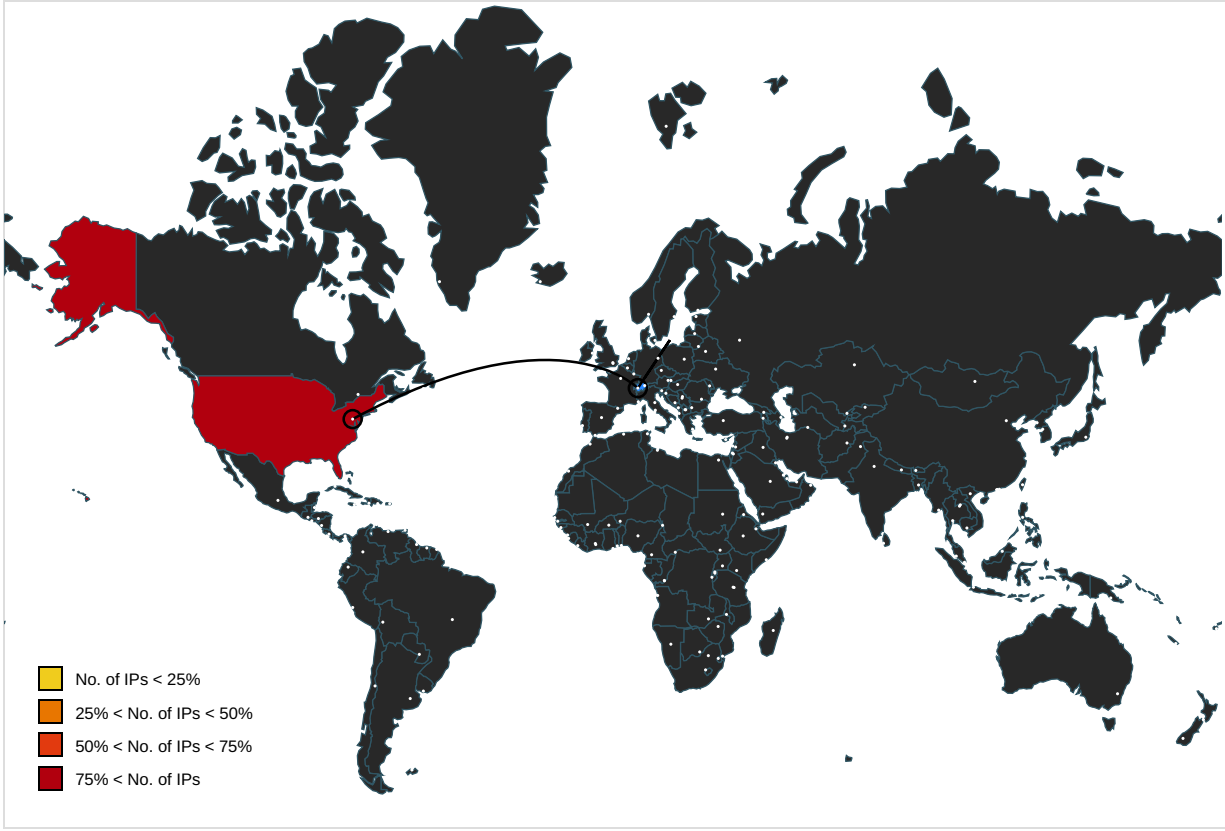
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
file:///C:/Users/user/Desktop/download/Downloading%20ATX.htm.html	false		low
http://https://www.google.com/jsapi	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	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.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Do	wget.exe	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/DoP:	wget.exe, 00000002.00000002.260168945.0000000000B88000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htmf	wget.exe, 00000002.00000002.260362958.0000000001470000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.madcapsoftware.com/Schemas/MadCap.xsd	Downloading ATX.htm.2.dr	false		high
http://https://files.cchsfs.com/doc/atx/2021/Help/Content/Both-SSource/Installation/Downloading%20ATX.htmj	wget.exe, 00000002.00000002.260574088.00000002E1D000.00000004.00000800.00020000.00000000.sdmp, wget.exe, 00000002.00000002.260362958.0000000001470000.00000004.00000020.00020000.00000000.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
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694551
Start date and time:	2022-08-31 23:48:02 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
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 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	21
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.win@36/2@5/7
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.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, 172.217.168.42
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, az393887.vo.msecnd.net, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, clientservices.googleapis.com, arc.msn.com, ris.api.iris.microsoft.com, edgedl.me.gvt1.com, update.googleapis.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.gstatic.com, www.google-analytics.com, optimizationguide-pa.googleapis.com
- Execution Graph export aborted for target wget.exe, PID 4968 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey 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):	5.188843004194417
Encrypted:	false
SSDEEP:	12:Hu4FpdftToi4dENVCrWXCrwtT1De5RhKj1DbBKb3nzVE3viBKb3RRa:OKpRtTJ4d7rZrOxePgj1pcDa3vEcLa
MD5:	9C2DFB8ECF331B98DCE6F1AF4D42817A
SHA1:	A291ED3673619047383FD832E841274DD90D250D
SHA-256:	35975DAB63A532E0434BA22DBD40E7679EF350CD6626382AD61E4DFD7445BD38
SHA-512:	DECD34EB7DAC8A0A3273D9EADDED6629049E5E22DD70B80BCEDB54D8597F927719F59DF7E582D0C01F0D5875D2E4C7988295F2D02D82E78DB7A519B44EB9E666
Malicious:	false
Reputation:	low
Preview:	--2022-08-31 23:50:03-- 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% 109K=0.08s....2022-08-31 23:50:05 (109 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

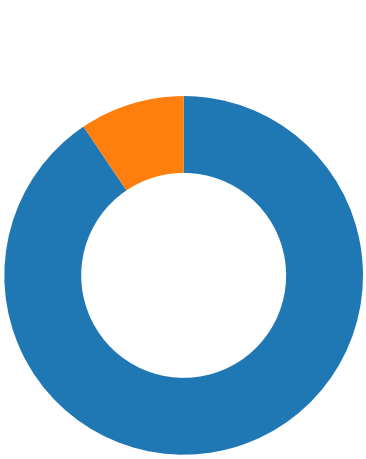
No static file info

Network Behavior

Network Port Distribution

Total Packets: 53

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:04.352344036 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.352401018 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.352613926 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.355834961 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.355881929 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.419096947 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.419192076 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.435869932 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.435920954 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.436273098 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.440810919 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.487370968 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.816746950 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.816947937 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.817008972 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:04.817039967 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.817084074 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.902312994 CEST	49720	443	192.168.2.3	152.199.21.175
Aug 31, 2022 23:50:04.902391911 CEST	443	49720	152.199.21.175	192.168.2.3
Aug 31, 2022 23:50:12.495328903 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.495378971 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.495441914 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.495848894 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.495876074 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.495934963 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.496475935 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.496526957 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.496594906 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.496958971 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.496968031 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.497222900 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.497232914 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.497554064 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.497571945 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.552290916 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.553348064 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.553373098 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.554888010 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.554953098 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.556191921 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.559505939 CEST	49726	443	192.168.2.3	142.250.203.100

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:12.559521914 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.560632944 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.560722113 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.563977003 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.571305990 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.571358919 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.572031021 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.572105885 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.572824955 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.572941065 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.899305105 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.899504900 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.899672031 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.899688005 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.900058985 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.900208950 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.900648117 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.900660992 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.901287079 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.901413918 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.901427031 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.919208050 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.919694901 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.930172920 CEST	49726	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:12.930208921 CEST	443	49726	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:12.937011003 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.937073946 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.937097073 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.937114000 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.937161922 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.946063042 CEST	49728	443	192.168.2.3	216.58.215.238
Aug 31, 2022 23:50:12.946091890 CEST	443	49728	216.58.215.238	192.168.2.3
Aug 31, 2022 23:50:12.976200104 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.976262093 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.976274967 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.976397991 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:12.976443052 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.978661060 CEST	49725	443	192.168.2.3	142.250.203.109
Aug 31, 2022 23:50:12.978676081 CEST	443	49725	142.250.203.109	192.168.2.3
Aug 31, 2022 23:50:15.027177095 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:15.027255058 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.027343988 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:15.027714014 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:15.027729034 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.079718113 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.080216885 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:15.080245972 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.081099987 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.081830025 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:15.081962109 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.287369013 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:15.287466049 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:25.103704929 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:25.103821993 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:50:25.103940010 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:25.529244900 CEST	49738	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:50:25.529298067 CEST	443	49738	142.250.203.100	192.168.2.3
Aug 31, 2022 23:51:15.113287926 CEST	49790	443	192.168.2.3	142.250.203.100
Aug 31, 2022 23:51:15.113342047 CEST	443	49790	142.250.203.100	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:50:04.166330099 CEST	51139	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:50:12.449203014 CEST	62050	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:50:12.450372934 CEST	56042	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:50:12.450449944 CEST	59636	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:50:12.468522072 CEST	53	59636	8.8.8.8	192.168.2.3
Aug 31, 2022 23:50:12.470225096 CEST	53	56042	8.8.8.8	192.168.2.3
Aug 31, 2022 23:50:12.487296104 CEST	53	62050	8.8.8.8	192.168.2.3
Aug 31, 2022 23:51:15.090920925 CEST	63446	53	192.168.2.3	8.8.8.8
Aug 31, 2022 23:51:15.110852003 CEST	53	63446	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:50:04.166330099 CEST	192.168.2.3	8.8.8.8	0xf131	Standard query (0)	files.cchsfs.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.449203014 CEST	192.168.2.3	8.8.8.8	0x1fe0	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.450372934 CEST	192.168.2.3	8.8.8.8	0xff42	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.450449944 CEST	192.168.2.3	8.8.8.8	0xf14b	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:51:15.090920925 CEST	192.168.2.3	8.8.8.8	0x1512	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 23:50:04.332082033 CEST	8.8.8.8	192.168.2.3	0xf131	No error (0)	files.cchsfs.com	az393887.vo.msecnd.net		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:50:04.332082033 CEST	8.8.8.8	192.168.2.3	0xf131	No error (0)	scdn21a03.wpc.da5e.edgecastcdn.net	sni1gl.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:50:04.332082033 CEST	8.8.8.8	192.168.2.3	0xf131	No error (0)	sni1gl.wpc.edgecastcdn.net		152.199.21.175	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.468522072 CEST	8.8.8.8	192.168.2.3	0xf14b	No error (0)	accounts.google.com		142.250.203.109	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.470225096 CEST	8.8.8.8	192.168.2.3	0xff42	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Aug 31, 2022 23:50:12.487296104 CEST	8.8.8.8	192.168.2.3	0x1fe0	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 31, 2022 23:50:12.487296104 CEST	8.8.8.8	192.168.2.3	0x1fe0	No error (0)	clients.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 31, 2022 23:51:15.110852003 CEST	8.8.8.8	192.168.2.3	0x1512	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
- www.google.com
- clients2.google.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49720	152.199.21.175	443	C:\Windows\SysWOW64\wget.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:04 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 21:50:04 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 21:50:03 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: 24dba4f7-001e-0011-4783-bdd8b9000000 x-ms-version: 2009-09-19 Content-Length: 8577 Connection: close
2022-08-31 21:50:04 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	192.168.2.3	49725	142.250.203.109	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:12 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 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: CONSENT=PENDING+904; AEC=AakniGO7HqlHWlnoY-P22_SwwnNSfVGxlF1NgK5nuj5WLe313NyJi16g7z4; SOCS=CAISHAgCEhJnd3NfMjAyMjA4MDgtMF9SQzEaAmVuIAEaBgiAvOuXBg; NID=511=nUT82hOv6CVwMNqDg-sTtCMJJ6SQ1v_cCpfCpf5nt8EolEbal01GWFyjG01tqWQgh9ciRU880J6nLd2gdbhAJs44PsHAZaVQAFIbrqe2FmF gjrAAK7W9Z8u5LDvwsuZRng98jP6E23SJ4fsPIs326YmnuCwa92dRRCcB6MNeI_o
2022-08-31 21:50:12 UTC	9	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:12 UTC	13	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 21:50:12 GMT Strict-Transport-Security: max-age=31536000; includeSubDomains Content-Security-Policy: script-src 'report-sample' 'nonce-asaZcK1JwHHJMkWGlO4ffQ' '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 Content-Security-Policy: require-trusted-types-for 'script';report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Opener-Policy: same-origin; report-to="IdentityListAccountsHttp" 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 Report-To: {"group":"IdentityListAccountsHttp","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external"}]} 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=* 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 21:50:12 UTC	15	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 21:50:12 UTC	15	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49726	142.250.203.100	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:12 UTC	9	OUT	GET /jsapi HTTP/1.1 Host: www.google.com Connection: keep-alive sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104" sec-ch-ua-mobile: ?0 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 sec-ch-ua-platform: "Windows" Accept: */* X-Client-Data: CI22yQEIpbbJAQjBtskBCKmdygEIk6HLAQj8qswBCLy8zAEIiL3MAQiywcwBCMTBzAEI18HMAQ== 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: NID=511=nUT82hOv6CVwMNqDg-sTtCMJJ6SQ1v_cCpfCpf5nt8EolEbal01GWFyjG01tqWQgh9ciRU880J6nLd2gdbhAJs44PsHAZaVQAFIbrqe2FmFgjrAAK7W9Z8u5LDvwsuZRng98jP6E23SJ4fsPIs326YmnuCwa92dRRCcB6MNeI_o
2022-08-31 21:50:12 UTC	11	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: 1412 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" Connection: close

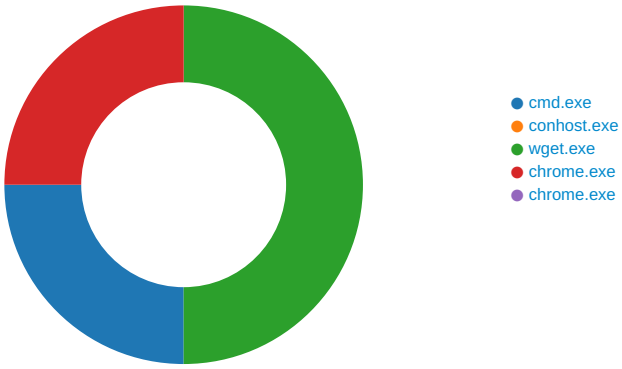
Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:12 UTC	11	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 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</TITLE></HEAD><BODY><H1>301 Moved</H1>The document has moved<A HREF="https://www.gstatic.com/charts/loader.js">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49728	216.58.215.238	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:50:12 UTC	10	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=104.0.5112.81&lang=en-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccmgmieda%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 X-Goog-Update-Updater: chromecrx-104.0.5112.81 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2022-08-31 21:50:12 UTC	12	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-nzNUD2qctefgBadpFJw-GQ' '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 21:50:12 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5721 X-Daystart: 53412 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 21:50:12 UTC	12	IN	Data Raw: 32 63 39 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 33 34 31 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: 2c9<?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="53412"/><app appid="nmmhkkegccagdldgiimedpiccmgmieda" cohort="1::" cohortname=""
2022-08-31 21:50:12 UTC	13	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 2f 67 Data Ascii: mhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" protected="0" size="248531" status="ok" version="1.0.0.6"/></app></g
2022-08-31 21:50:12 UTC	13	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **5992**, Parent PID: **1652**

General

Target ID:	0
Start time:	23:50:02
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:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: conhost.exe PID: **2804**, Parent PID: **5992**

General

Target ID:	1
Start time:	23:50:02
Start date:	31/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: wget.exe PID: 4968, Parent PID: 5992

General

Target ID:	2
Start time:	23:50:03
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	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: 5396, Parent PID: 5324

General

Target ID:	5
Start time:	23:50:07
Start date:	31/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\user\Desktop\download\Downloading ATX.htm.html
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}	dr	unicode	0	1	success or wait	1	7FF6146AA143	RegSetValueExW

Analysis Process: chrome.exe PID: **2080**, Parent PID: **5396**

General

Target ID:	6
Start time:	23:50:09
Start date:	31/08/2022
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	"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=1588 --field-trial-handle=1724,i,8435291165856388015,4643082473579285808,131072 /prefetch:8
Imagebase:	0x7ff614650000
File size:	2851656 bytes
MD5 hash:	0FEC2748F363150DC54C1CAFFB1A9408
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

Disassembly

No disassembly