Forensics Lab

Author Name: Hui Nok Hang

Executive summary

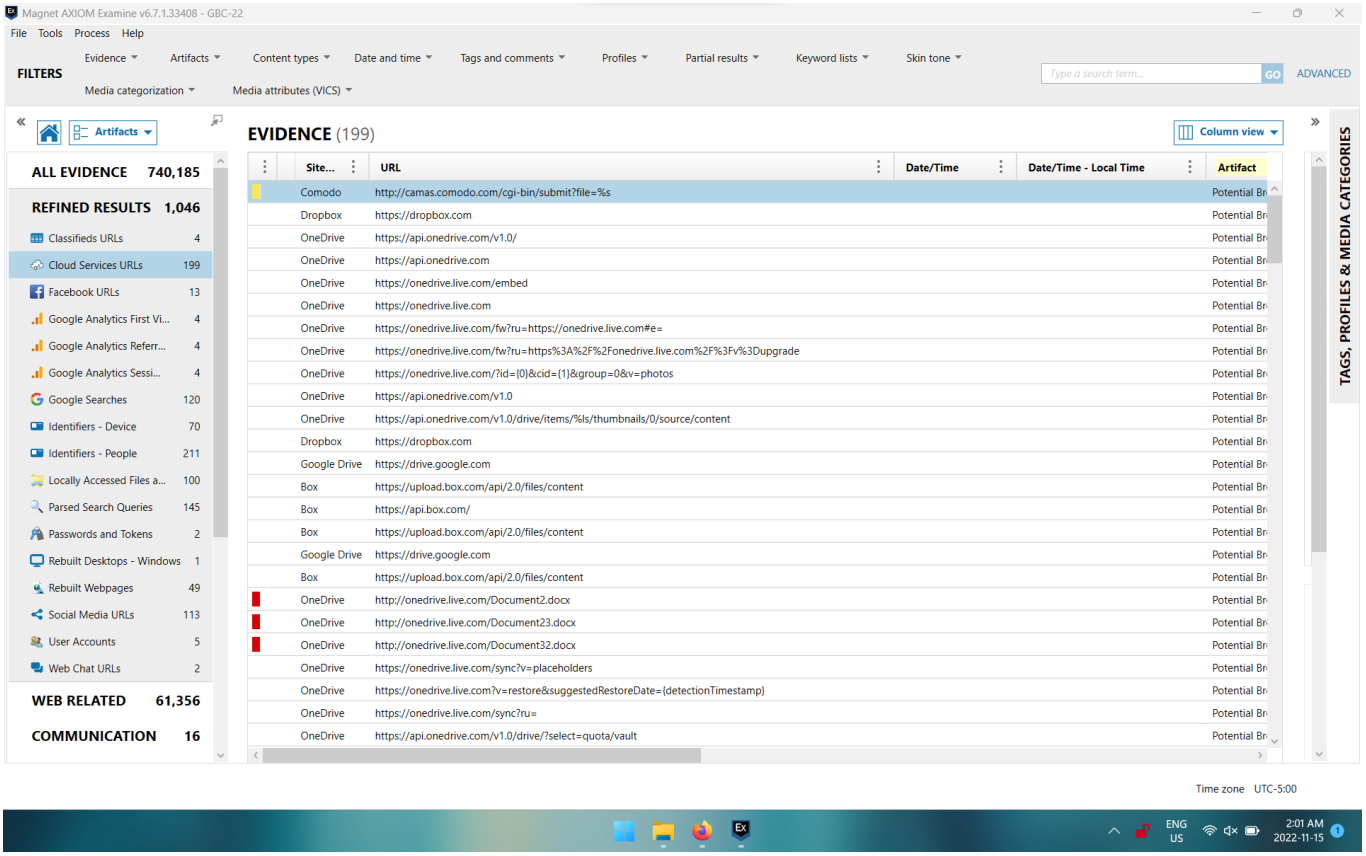
A client got their computer compromised, and subsequently I am tasked with reconstructing the story with digital forensics. Working with data that spans over 20 years, it is best to first attempt to understand the precise time frame of the attack that we are interested in, in order to narrow down the events that will contribute to the forensics operation as well as increasing the accuracy of the investigation.

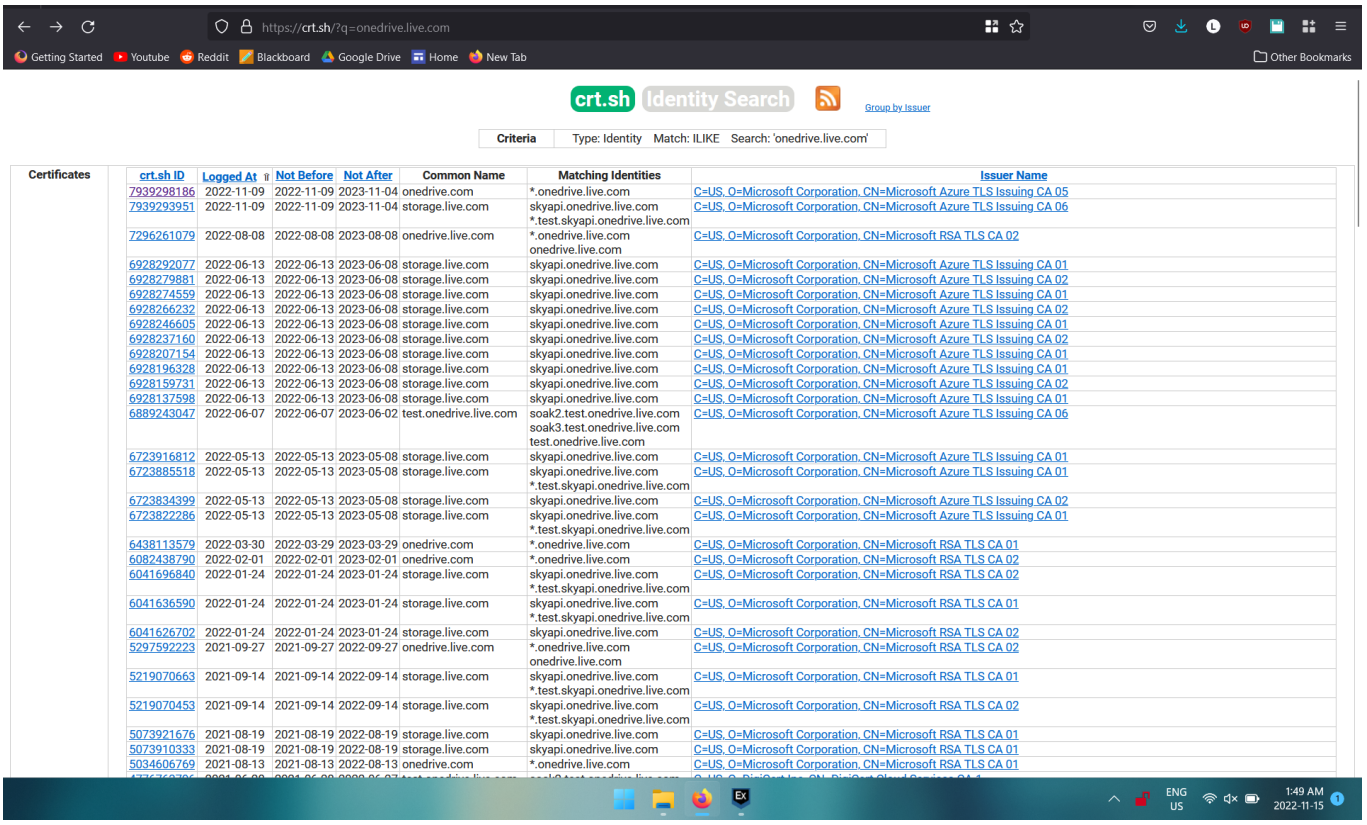
Investigation

Web related evidence

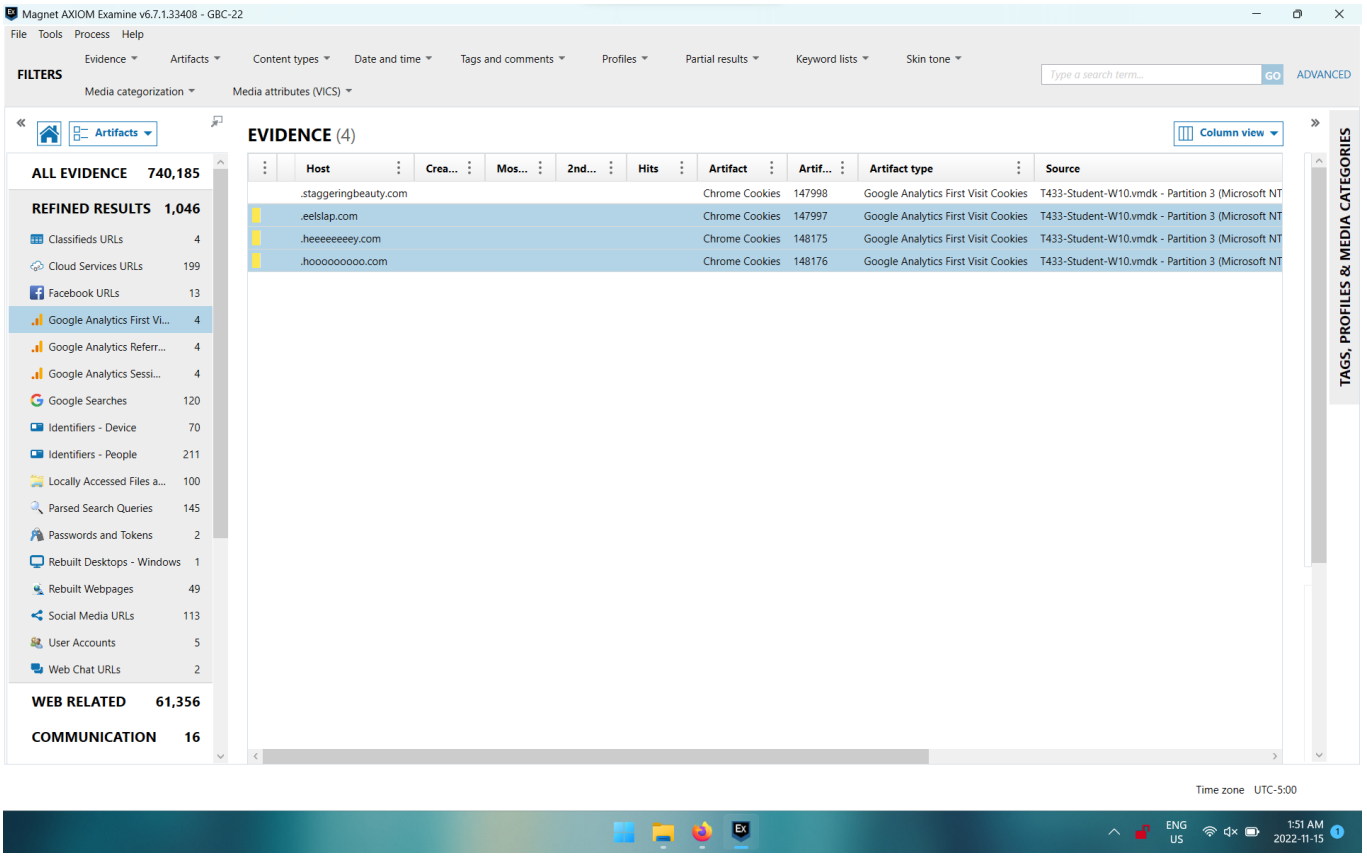
In Cloud Services URLs, there are three download links that appear to be evidence of intrusion by malware. At first glance, these links look like every other link that directs to downloads of content hosted on OneDrive cloud service. However, the strings of text after http://onedrive.live.com/ contain direct file names: Document2, Document23 and Document32 which is an unusual format for onedrive links as filenames in urls are usually dealt with in hashes. Furthermore, these links are using an insecure http rather than the proper https that onedrive uses. Proof of https certificate of the domain is shown below from crt.sh.

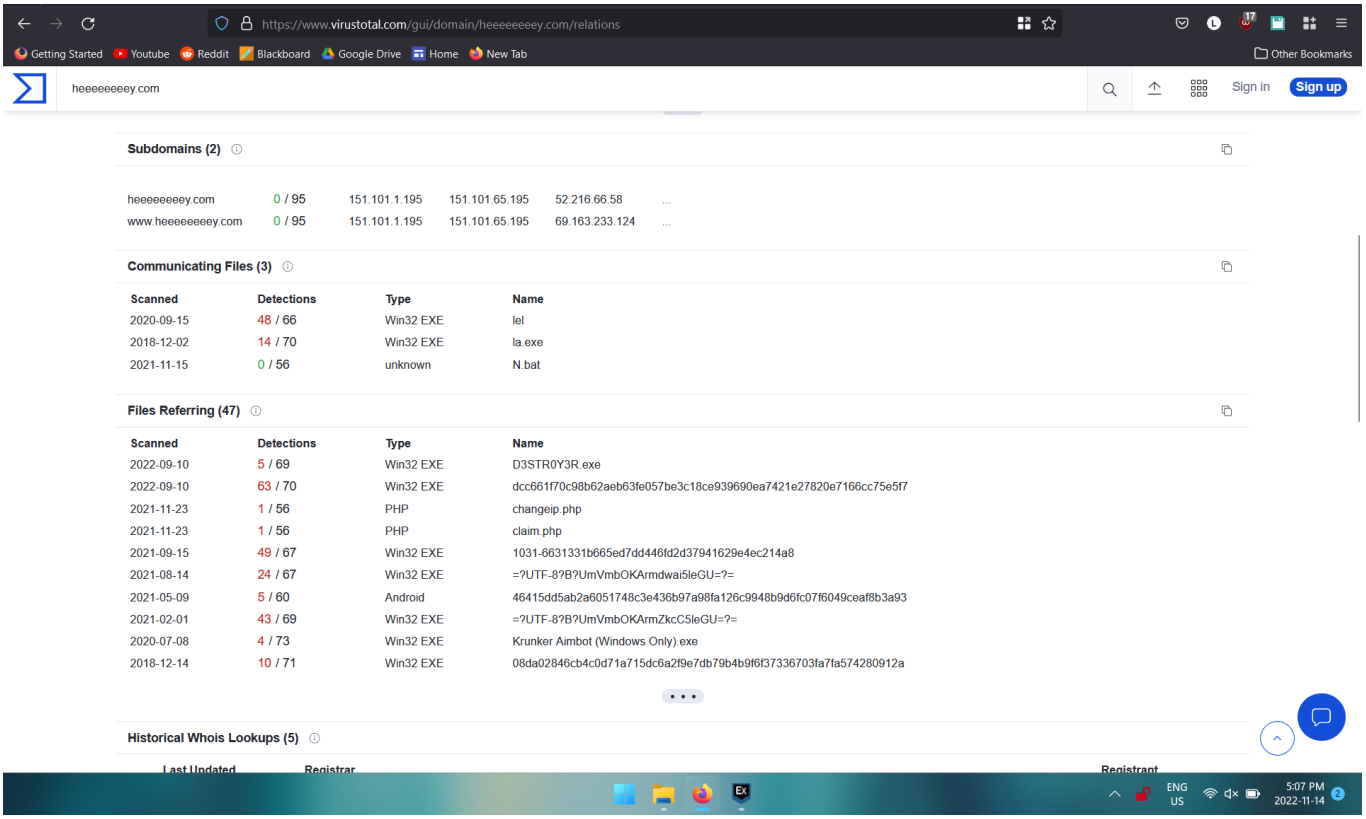
camas.comodo.com was also visited by this user. From the URL, it seems like the user was trying to submit a malware sample to the website. Although the link does not appear to be malicious, the link suggests that the user is involved with information security, which is a potential source of the malware and the compromise.

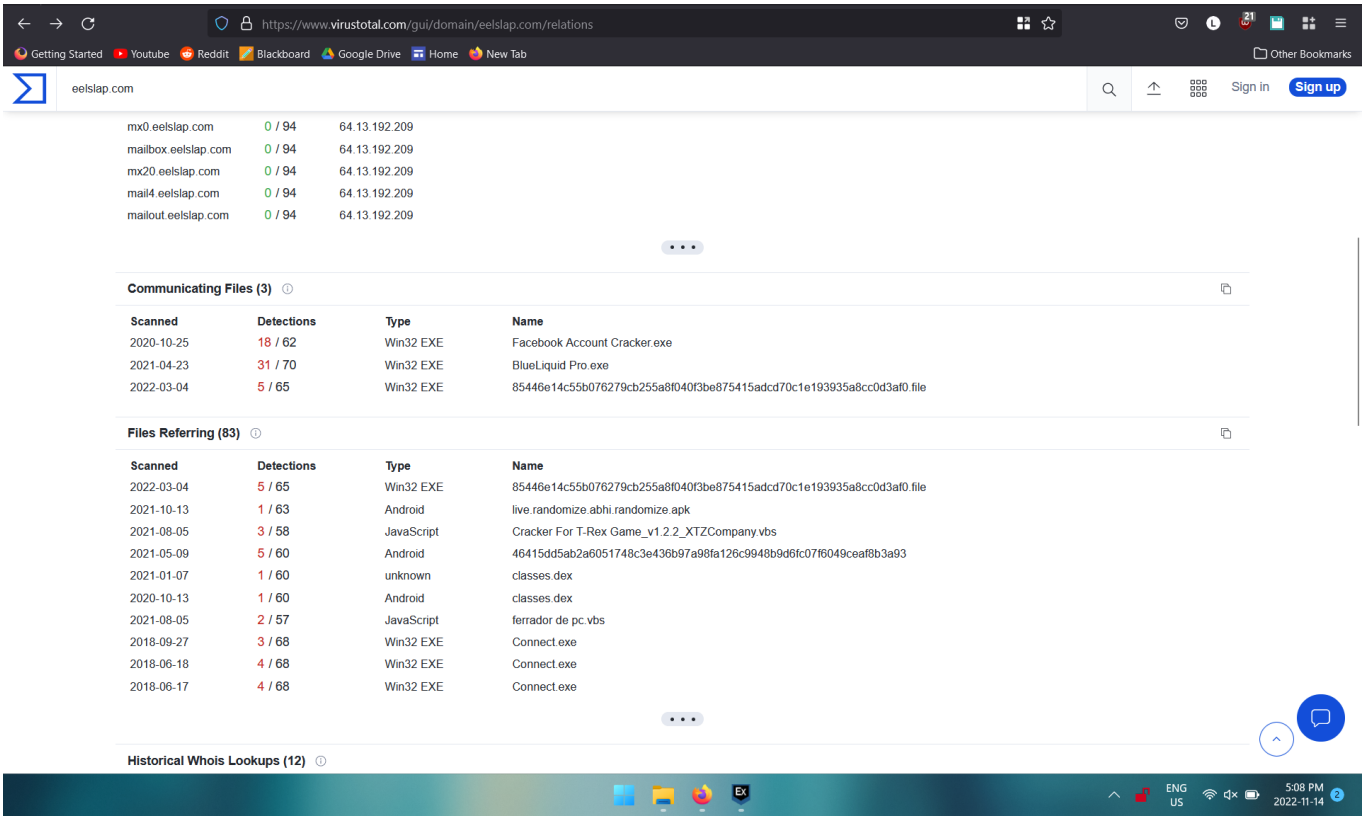

Magnet AXIOM Examine v6.7.1.33408 - GBC-22
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term...
GO
ADVANCED
Artifacts
EVIDENCE (199)
Column view
ALL EVIDENCE 740,185
REFINED RESULTS 1,046
Classifieds URLs 4
Cloud Services URLs 199
Facebook URLs 13
Google Analytics First Vi... 4
Google Analytics Referr... 4
Google Analytics Sessi... 4
Google Searches 120
Identifiers - Device 70
Identifiers - People 211
Locally Accessed Files a... 100
Parsed Search Queries 145
Passwords and Tokens 2
Rebuilt Desktops - Windows 1
Rebuilt Webpages 49
Social Media URLs 113
User Accounts 5
Web Chat URLs 2
WEB RELATED 61,356
COMMUNICATION 16
Site... URL Date/Time Date/Time - Local Time Artifact
Comodo http://camas.comodo.com/cgi-bin/submit?file=%s Potential Br
Dropbox https://dropbox.com Potential Br
OneDrive https://api.onedrive.com/v1.0/ Potential Br
OneDrive https://api.onedrive.com Potential Br
OneDrive https://onedrive.live.com/embed Potential Br
OneDrive https://onedrive.live.com Potential Br
OneDrive https://onedrive.live.com/fw?ru=https://onedrive.live.com#e= Potential Br
OneDrive https://onedrive.live.com/fw?ru=https%3A%2F%2Fonedrive.live.com%2F%3Fv%3Dupgrade Potential Br
OneDrive https://onedrive.live.com/?id={0}&cid={1}&group=0&v=photos Potential Br
OneDrive https://api.onedrive.com/v1.0 Potential Br
OneDrive https://api.onedrive.com/v1.0/drive/items/%ls/thumbnails/0/source/content Potential Br
Dropbox https://dropbox.com Potential Br
Google Drive https://drive.google.com Potential Br
Box https://upload.box.com/api/2.0/files/content Potential Br
Box https://api.box.com/ Potential Br
Box https://upload.box.com/api/2.0/files/content Potential Br
Google Drive https://drive.google.com Potential Br
Box https://upload.box.com/api/2.0/files/content Potential Br
OneDrive http://onedrive.live.com/Document2.docx Potential Br
OneDrive http://onedrive.live.com/Document23.docx Potential Br
OneDrive http://onedrive.live.com/Document32.docx Potential Br
OneDrive https://onedrive.live.com/sync?v=placeholders Potential Br
OneDrive https://onedrive.live.com?v=restore&suggestedRestoreDate={detectionTimestamp} Potential Br
OneDrive https://onedrive.live.com/sync?ru= Potential Br
OneDrive https://api.onedrive.com/v1.0/drive/?select=quota/vault Potential Br
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00
ENG US
2:01 AM 2022-11-15

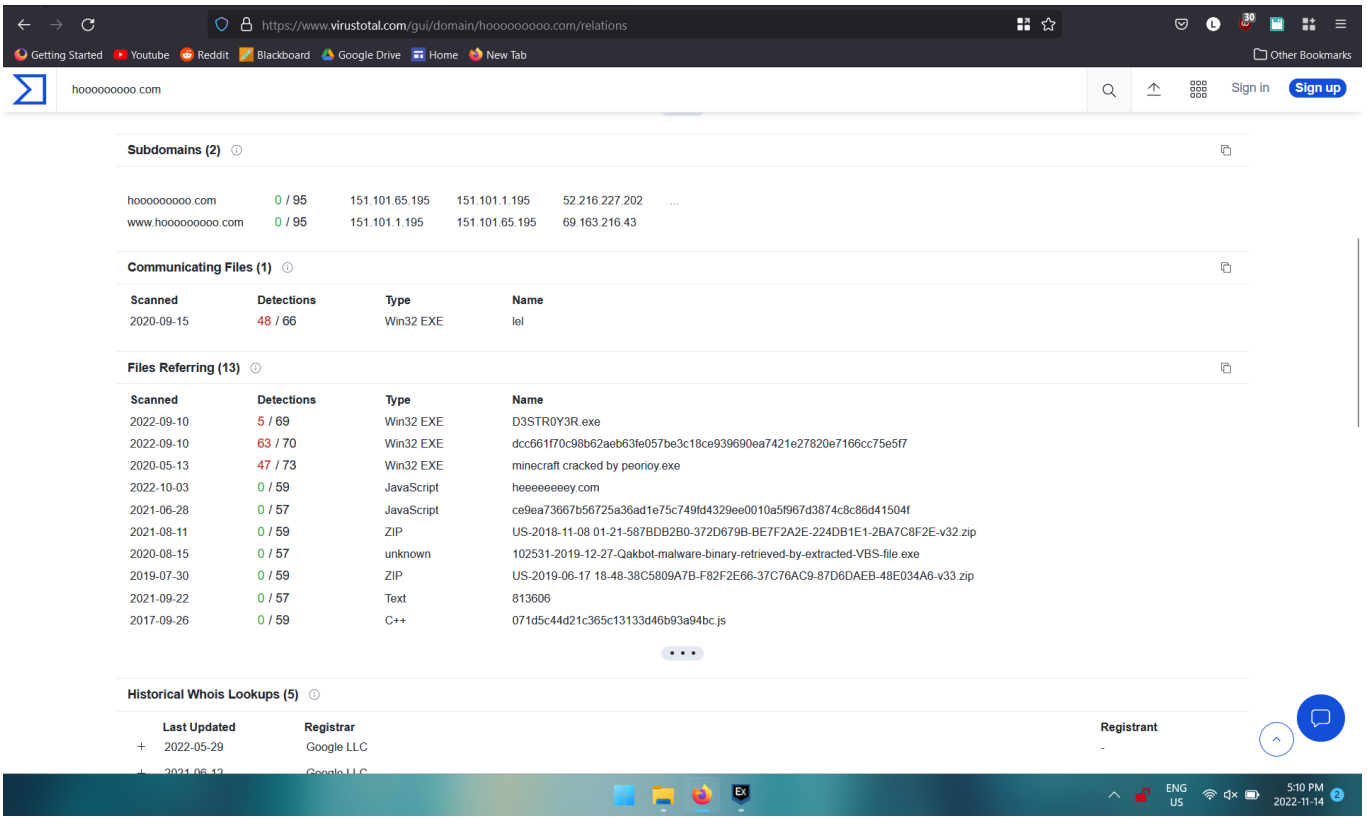


When inspecting the cookies from Google analytics, 4 funny looking domains can be seen. Upon looking these websites up on VirusTotal, they appear clean on the record. However, 3 of them are seen to be associated with malware activities in the past. Either there are quite a number of flagged and known malwares referring to these websites in their body, or they have been documented communicating with these malicious softwares.

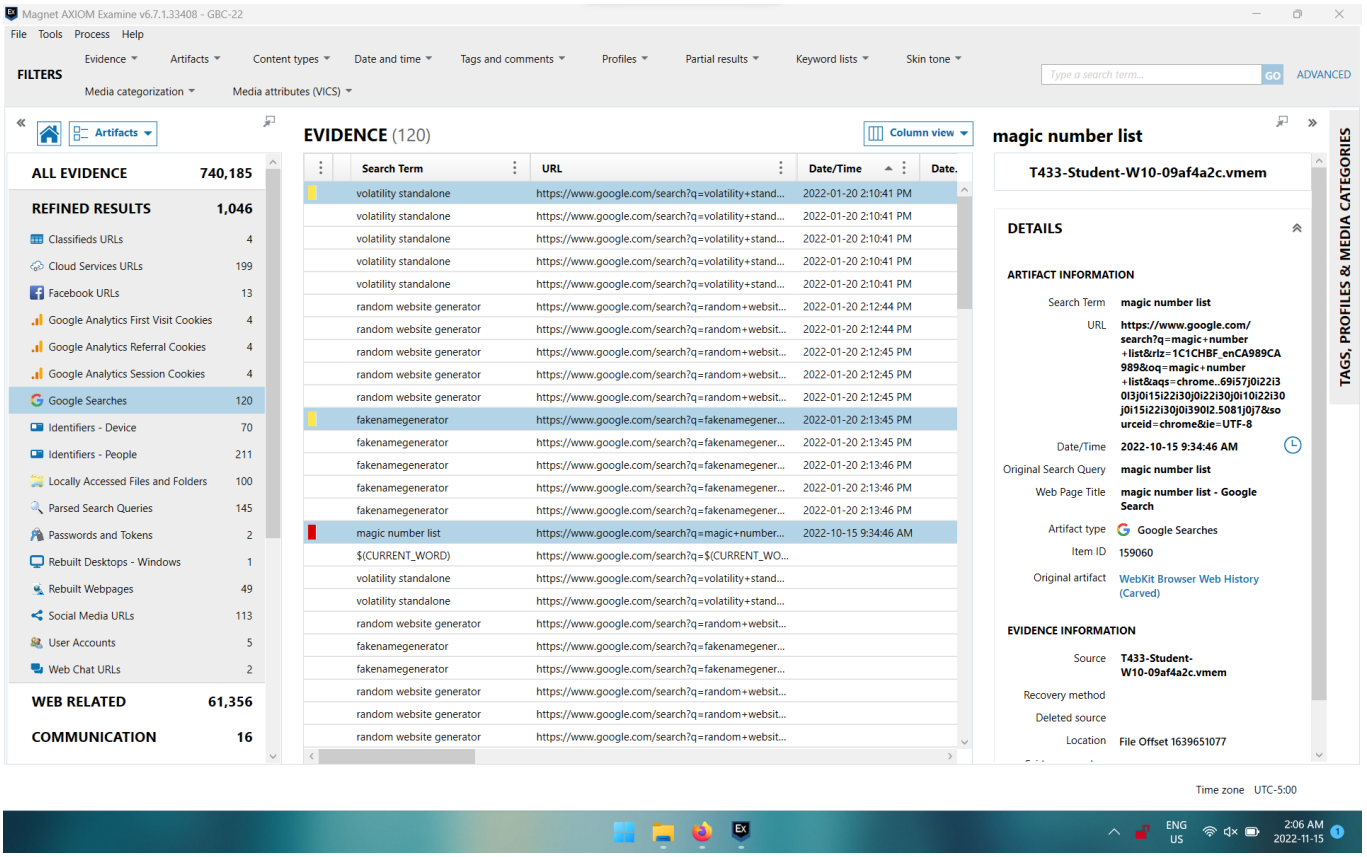



https://www.virustotal.com/gui/domain/heeeeeeey.com/relations
Getting Started
Youtube
Reddit
Blackboard
Google Drive
Home
New Tab
Other Bookmarks
heeeeeeey.com
Sign in
Sign up
Subdomains (2)
heeeeeeey.com 0 / 95 151.101.1.195 151.101.65.195 52.216.66.58 ...
www.heeeeeeey.com 0 / 95 151.101.1.195 151.101.65.195 69.163.233.124 ...
Communicating Files (3)
Scanned Detections Type Name
2020-09-15 48 / 66 Win32 EXE lel
2018-12-02 14 / 70 Win32 EXE la.exe
2021-11-15 0 / 56 unknown N.bat
Files Referring (47)
Scanned Detections Type Name
2022-09-10 5 / 69 Win32 EXE D3STR0Y3R.exe
2022-09-10 63 / 70 Win32 EXE dcc661f70c98b62aeb63fe057be3c18ce939690ea7421e27820e7166cc75e5f7
2021-11-23 1 / 56 PHP changeip.php
2021-11-23 1 / 56 PHP claim.php
2021-09-15 49 / 67 Win32 EXE 1031-6631331b665ed7dd446fd2d37941629e4ec214a8
2021-08-14 24 / 67 Win32 EXE =?UTF-8?B?UmVmbOKArmdwai5leGU=?=
2021-05-09 5 / 60 Android 46415dd5ab2a6051748c3e436b97a98fa126c9948b9d6fc07f6049ceaf8b3a93
2021-02-01 43 / 69 Win32 EXE =?UTF-8?B?UmVmbOKArmZkcC5leGU=?=
2020-07-08 4 / 73 Win32 EXE Krunker Aimbot (Windows Only).exe
2018-12-14 10 / 71 Win32 EXE 08da02846cb4c0d71a715dc6a2f9e7db79b4b9f6f37336703fa7fa574280912a
Historical Whois Lookups (5)
Last Updated Registrar Registrant
ENG US
5:07 PM 2022-11-14

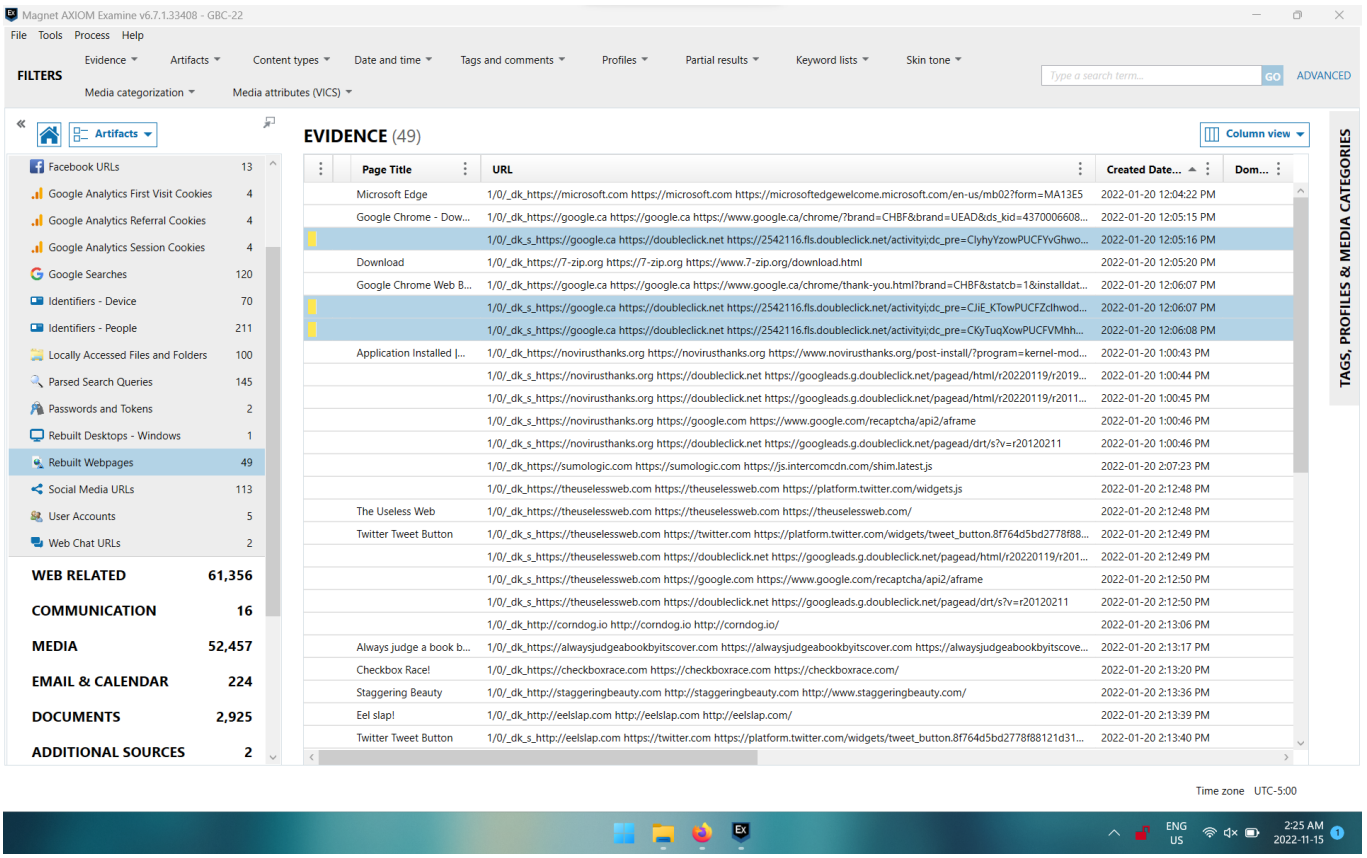

https://www.virustotal.com/gui/domain/eelslap.com/relations
Getting Started
Youtube
Reddit
Blackboard
Google Drive
Home
New Tab
Other Bookmarks
eelslap.com
Sign in
Sign up
mx0.eelslap.com 0 / 94 64.13.192.209
mailbox.eelslap.com 0 / 94 64.13.192.209
mx20.eelslap.com 0 / 94 64.13.192.209
mail4.eelslap.com 0 / 94 64.13.192.209
mailout.eelslap.com 0 / 94 64.13.192.209
Communicating Files (3)
Scanned Detections Type Name
2020-10-25 18 / 62 Win32 EXE Facebook Account Cracker.exe
2021-04-23 31 / 70 Win32 EXE BlueLiquid Pro.exe
2022-03-04 5 / 65 Win32 EXE 85446e14c55b076279cb255a8f040f3be875415adcd70c1e193935a8cc0d3af0.file
Files Referring (83)
Scanned Detections Type Name
2022-03-04 5 / 65 Win32 EXE 85446e14c55b076279cb255a8f040f3be875415adcd70c1e193935a8cc0d3af0.file
2021-10-13 1 / 63 Android live.randomize.abhi.randomize.apk
2021-08-05 3 / 58 JavaScript Cracker For T-Rex Game_v1.2.2_XTZCompany.vbs
2021-05-09 5 / 60 Android 46415dd5ab2a6051748c3e436b97a98fa126c9948b9d6fc07f6049ceaf8b3a93
2021-01-07 1 / 60 unknown classes.dex
2020-10-13 1 / 60 Android classes.dex
2021-08-05 2 / 57 JavaScript ferrador de pc.vbs
2018-09-27 3 / 68 Win32 EXE Connect.exe
2018-06-18 4 / 68 Win32 EXE Connect.exe
2018-06-17 4 / 68 Win32 EXE Connect.exe
Historical Whois Lookups (12)
ENG US
5:08 PM 2022-11-14



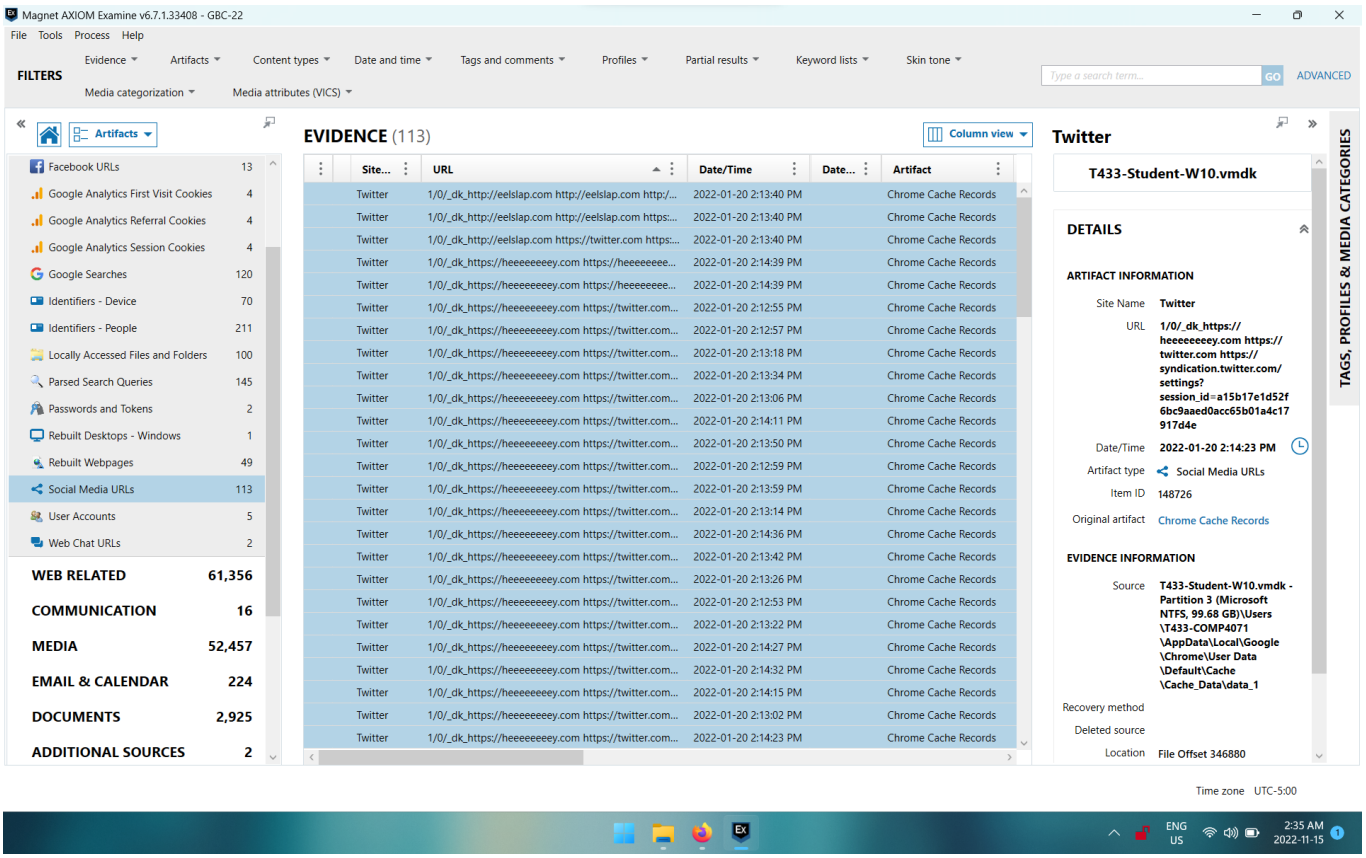
In Google searches, it appears that this user is rather computer savvy and looked up the magic number list on google. The magic number list is a list containing file signatures used to identify the content of a certain file. The two search terms “volatility standalone” and “fakenamegenerator” appear to have been done after the breach. Nonetheless, they indicate familiarity with OSINT and digital forensics. It appears that the user of this computer was somewhat involved in cyber security.



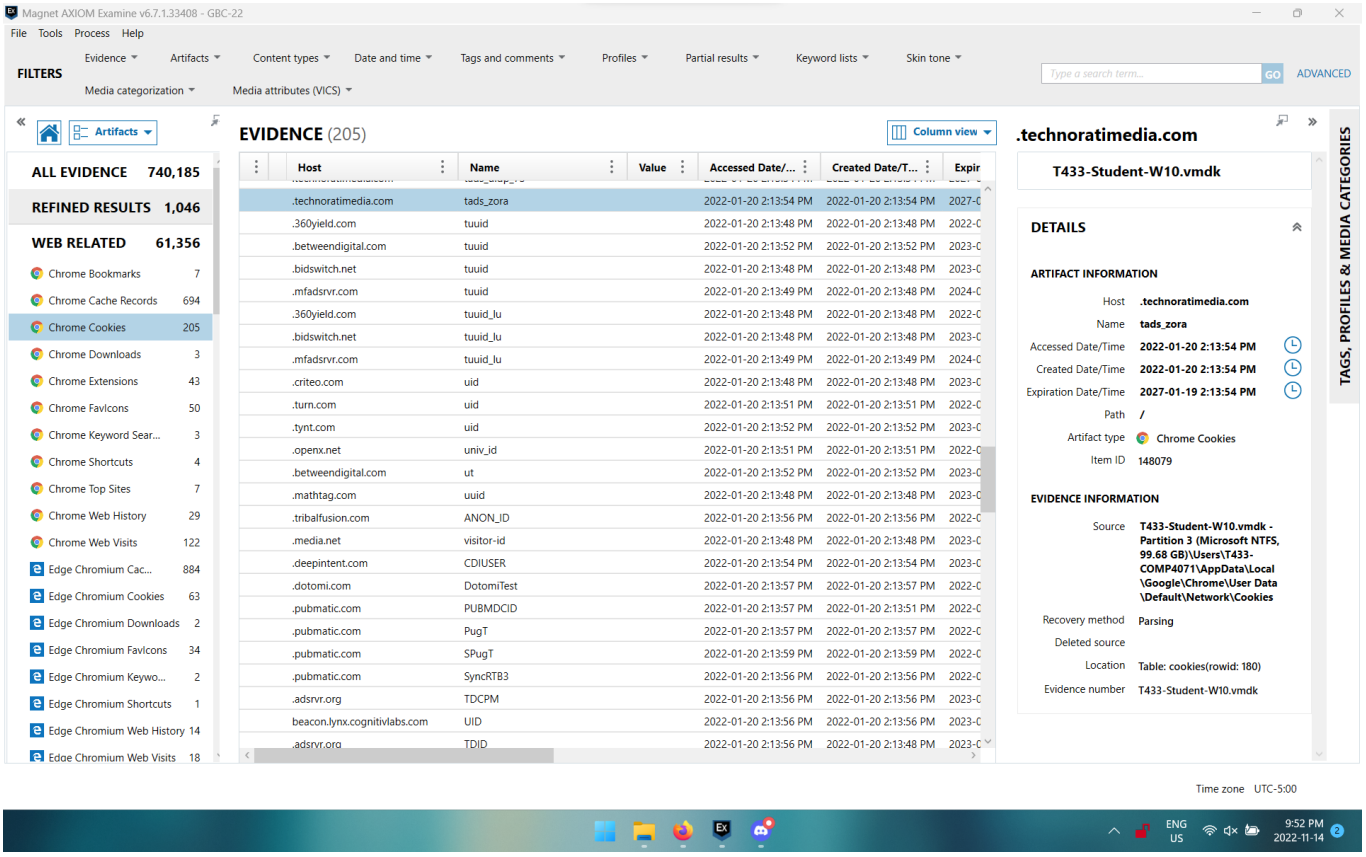
It seems like at the time of the event, the user got redirected to multiple ad pages on google. Although these ads websites are not directly flagged, it is worth looking into as a potential source of unwanted softwares. Also, if we look at the timestamps of these webpages rebuilt, the user had been searching for IT related softwares/domains before 1pm. However, after 2:07pm, there was suddenly an influx of the funny sounding domains that we flagged earlier and the user appeared to be tweeting about them. Despite not being direct evidence, this is somewhat of an erratic behavior. Did the malware have something to do with this?

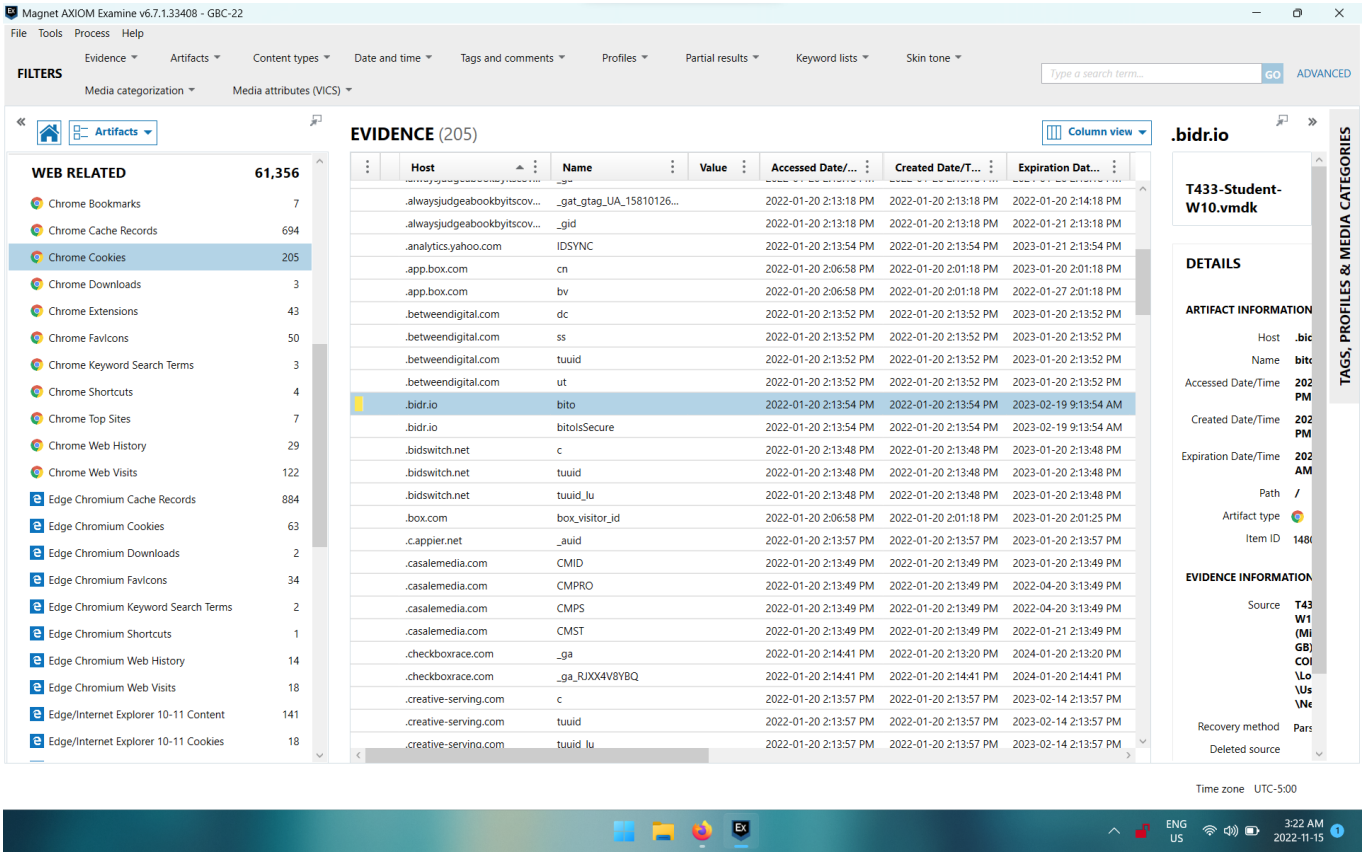


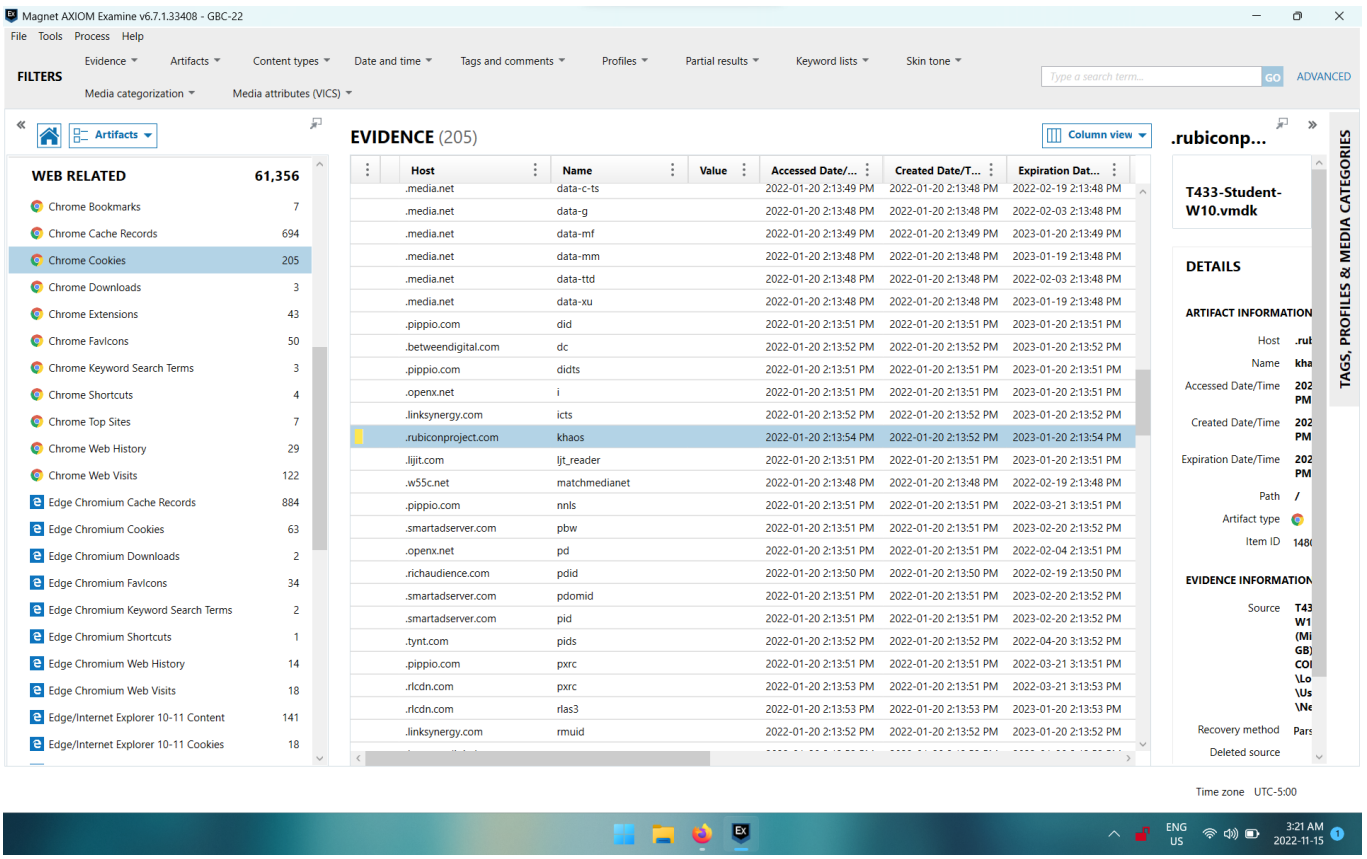
In social media URLs, the tweets containing these potentially malicious websites are in a great quantity. The tweets were also occurring so fast at extremely short intervals.

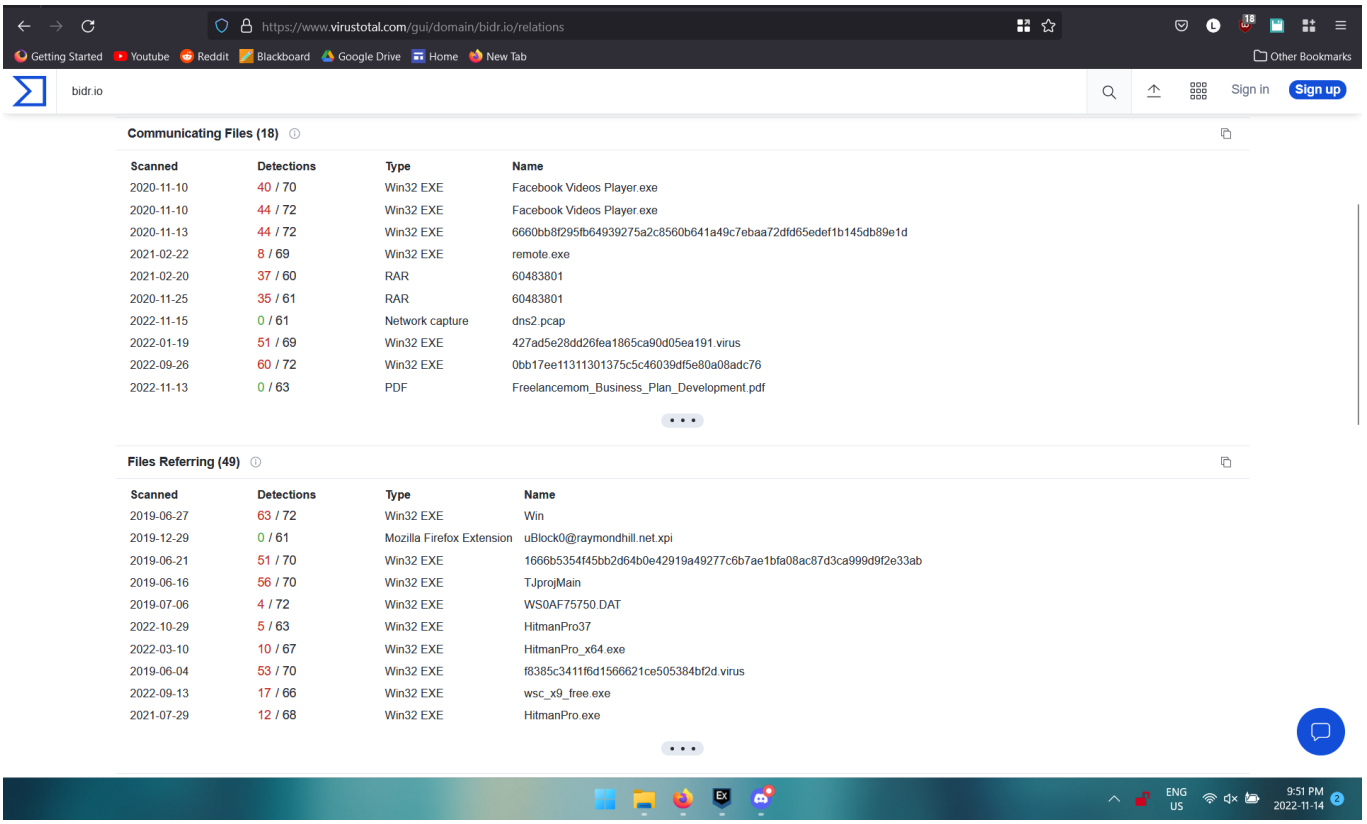


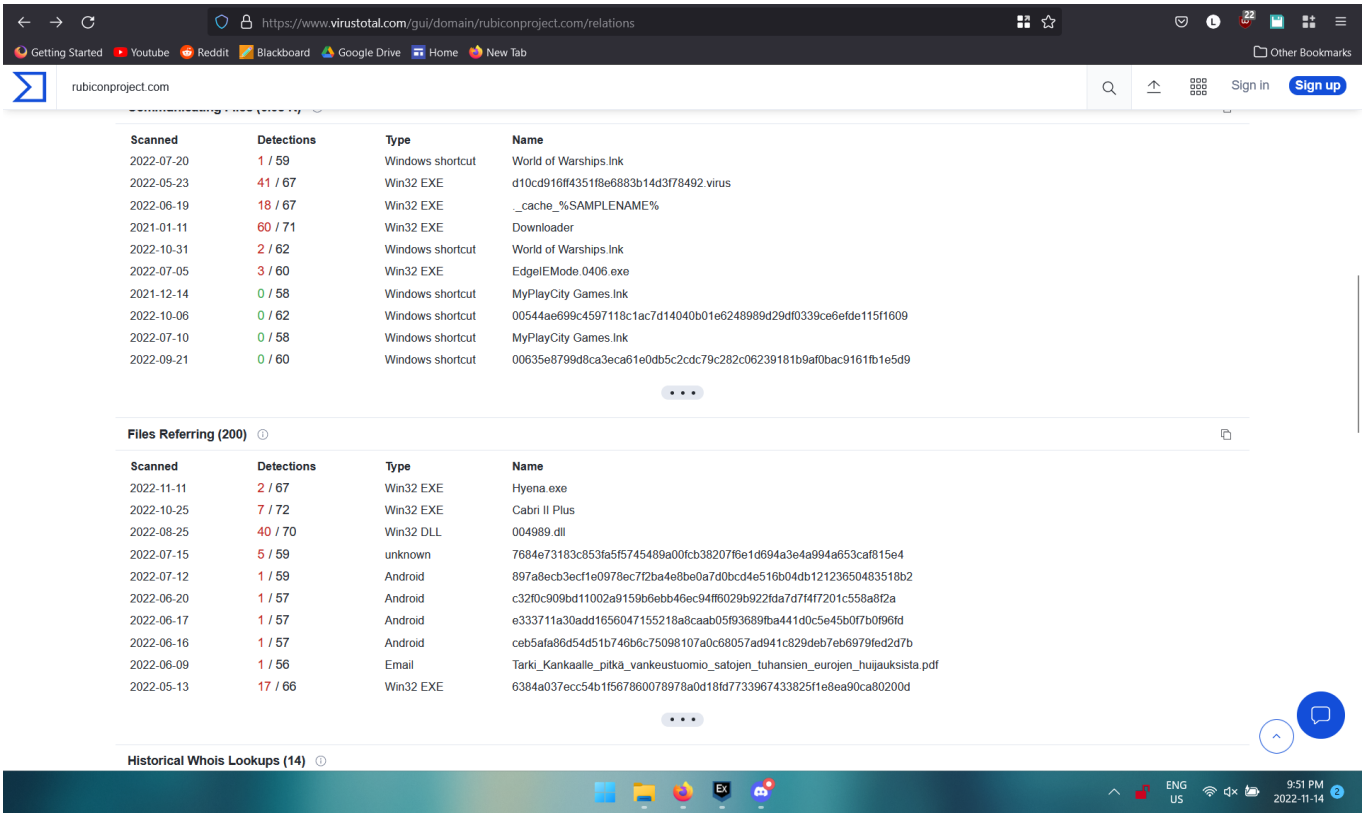
In the Chrome browser cookies, there are a multitude of suspicious looking domain names, seemingly short and random in nature. I found two samples that are associated with malicious activity - bidr.io and rubiconproject.com - but I am sure there are much more. Almost all of these cookies are also created at the likely time of the compromise event.



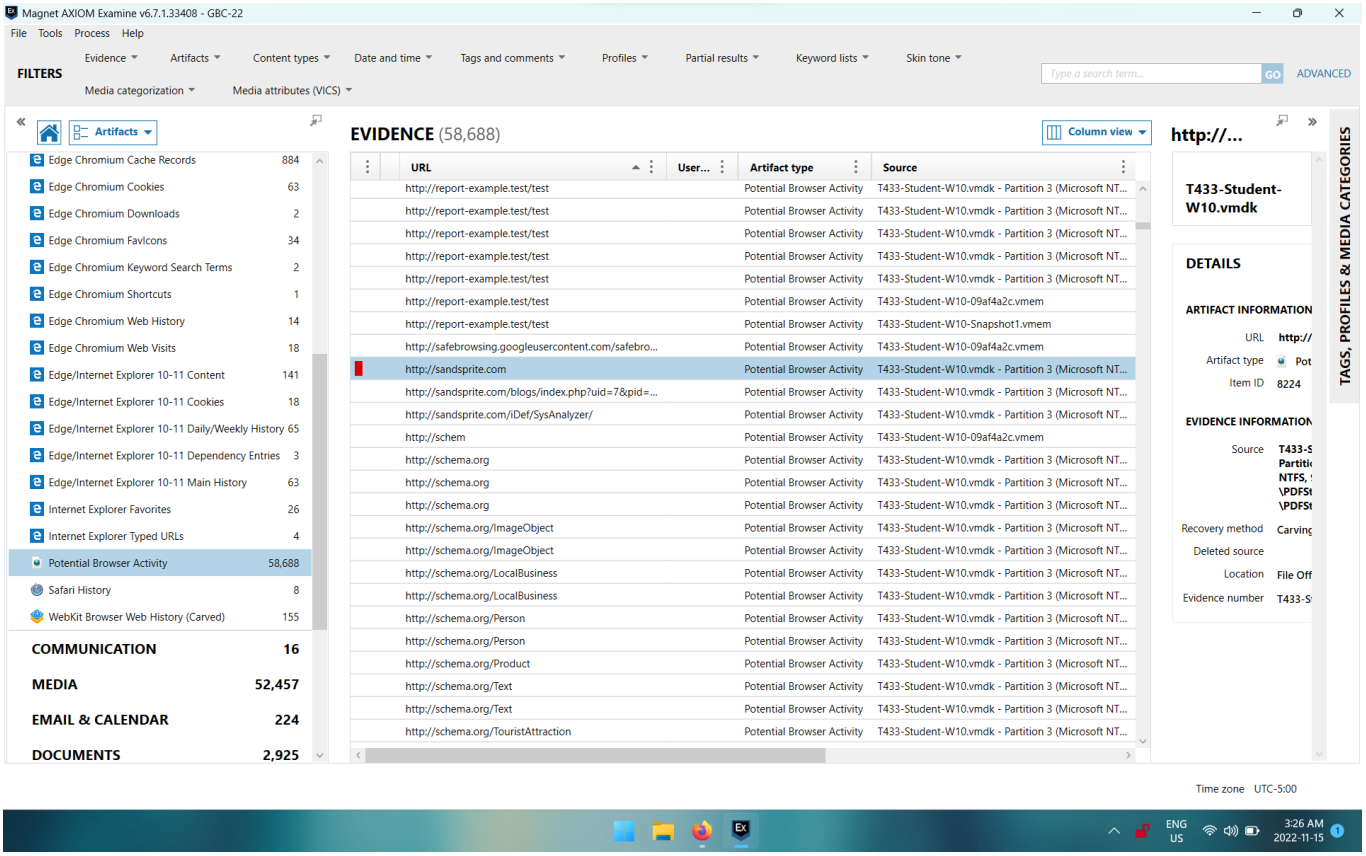

Magnet AXIOM Examine v6.7.1.33408 - GBC-22
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term... GO ADVANCED
Artifacts
WEB RELATED 61,356
Chrome Bookmarks 7
Chrome Cache Records 694
Chrome Cookies 205
Chrome Downloads 3
Chrome Extensions 43
Chrome Favicons 50
Chrome Keyword Search Terms 3
Chrome Shortcuts 4
Chrome Top Sites 7
Chrome Web History 29
Chrome Web Visits 122
Edge Chromium Cache Records 884
Edge Chromium Cookies 63
Edge Chromium Downloads 2
Edge Chromium Favicons 34
Edge Chromium Keyword Search Terms 2
Edge Chromium Shortcuts 1
Edge Chromium Web History 14
Edge Chromium Web Visits 18
Edge/Internet Explorer 10-11 Content 141
Edge/Internet Explorer 10-11 Cookies 18
EVIDENCE (205)
Column view
Host Name Value Accessed Date/... Created Date/T... Expiration Dat...
.always judgeabookbyitscov... _gat_gtag_UA_15810126... 2022-01-20 2:13:18 PM 2022-01-20 2:13:18 PM 2022-01-20 2:14:18 PM
.always judgeabookbyitscov... _gid 2022-01-20 2:13:18 PM 2022-01-20 2:13:18 PM 2022-01-21 2:13:18 PM
.analytics.yahoo.com IDSYNC 2022-01-20 2:13:54 PM 2022-01-20 2:13:54 PM 2023-01-21 2:13:54 PM
.app.box.com cn 2022-01-20 2:06:58 PM 2022-01-20 2:01:18 PM 2023-01-20 2:01:18 PM
.app.box.com bv 2022-01-20 2:06:58 PM 2022-01-20 2:01:18 PM 2022-01-27 2:01:18 PM
.betweendigital.com dc 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.betweendigital.com ss 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.betweendigital.com tuuid 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.betweendigital.com ut 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.bidr.io bito 2022-01-20 2:13:54 PM 2022-01-20 2:13:54 PM 2023-02-19 9:13:54 AM
.bidr.io bitoIsSecure 2022-01-20 2:13:54 PM 2022-01-20 2:13:54 PM 2023-02-19 9:13:54 AM
.bidswitch.net c 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2023-01-20 2:13:48 PM
.bidswitch.net tuuid 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2023-01-20 2:13:48 PM
.bidswitch.net tuuid_lu 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2023-01-20 2:13:48 PM
.box.com box_visitor_id 2022-01-20 2:06:58 PM 2022-01-20 2:01:18 PM 2023-01-20 2:01:25 PM
.c.appier.net _auid 2022-01-20 2:13:57 PM 2022-01-20 2:13:57 PM 2023-01-20 2:13:57 PM
.casalemedia.com CMID 2022-01-20 2:13:49 PM 2022-01-20 2:13:49 PM 2023-01-20 2:13:49 PM
.casalemedia.com CMPRO 2022-01-20 2:13:49 PM 2022-01-20 2:13:49 PM 2022-04-20 3:13:49 PM
.casalemedia.com CMPS 2022-01-20 2:13:49 PM 2022-01-20 2:13:49 PM 2022-04-20 3:13:49 PM
.casalemedia.com CMST 2022-01-20 2:13:49 PM 2022-01-20 2:13:49 PM 2022-01-21 2:13:49 PM
.checkboxrace.com _ga 2022-01-20 2:14:41 PM 2022-01-20 2:13:20 PM 2024-01-20 2:13:20 PM
.checkboxrace.com _ga_RJXX4V8YBQ 2022-01-20 2:14:41 PM 2022-01-20 2:14:41 PM 2024-01-20 2:14:41 PM
.creative-serving.com c 2022-01-20 2:13:57 PM 2022-01-20 2:13:57 PM 2023-02-14 2:13:57 PM
.creative-serving.com tuuid 2022-01-20 2:13:57 PM 2022-01-20 2:13:57 PM 2023-02-14 2:13:57 PM
.creative-serving.com tuuid_lu 2022-01-20 2:13:57 PM 2022-01-20 2:13:57 PM 2023-02-14 2:13:57 PM
.bidr.io
T433-Student-W10.vmdk
DETAILS
ARTIFACT INFORMATION
Host .bic
Name bito
Accessed Date/Time 202 PM
Created Date/Time 202 PM
Expiration Date/Time 202 AM
Path /
Artifact type
Item ID 148
EVIDENCE INFORMATION
Source T43 W1 (Mi GB) CO \Lo \Us \Ne
Recovery method Pars
Deleted source
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00
ENG US
3:22 AM 2022-11-15

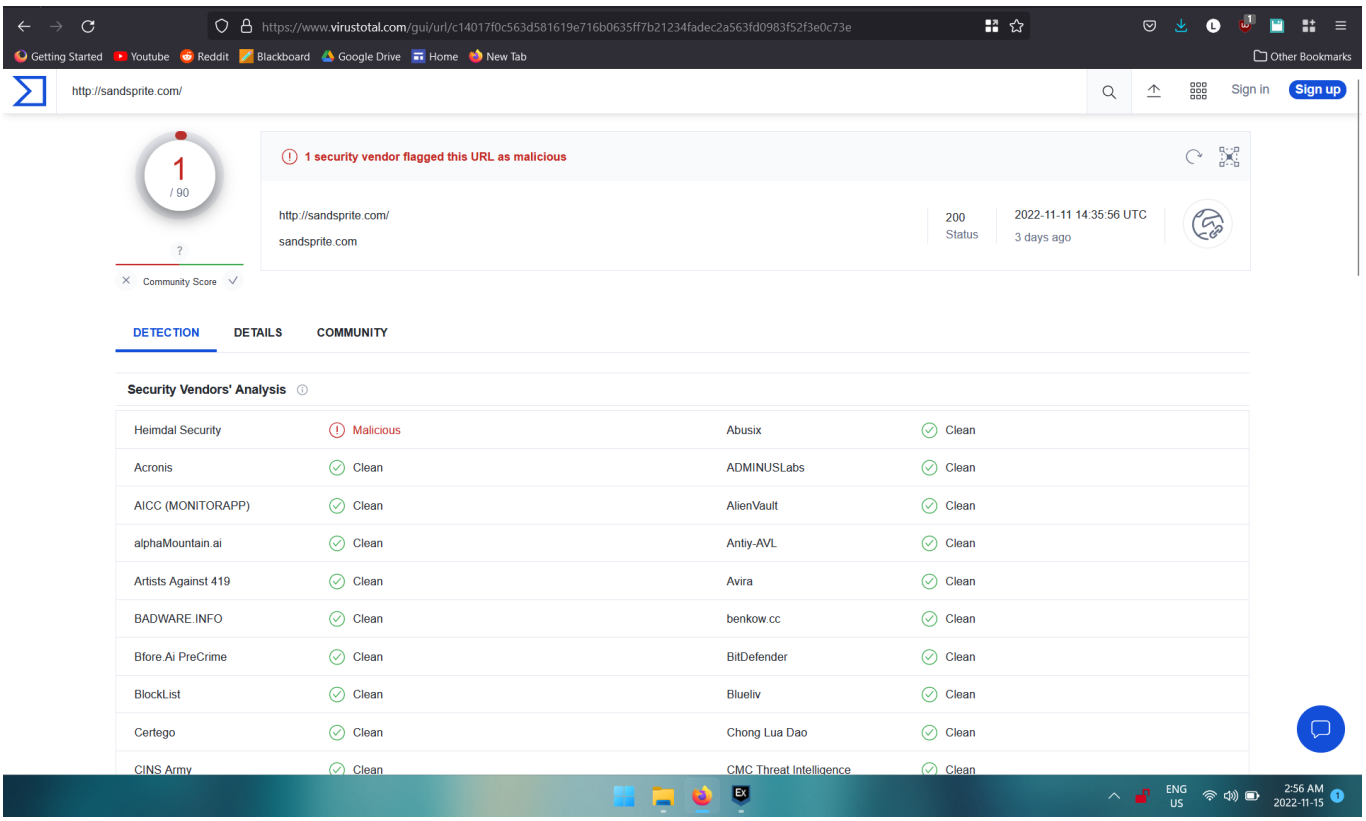

Magnet AXIOM Examine v6.7.1.33408 - GBC-22
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone
Media categorization Media attributes (VICS)
Type a search term... GO ADVANCED
Artifacts
WEB RELATED 61,356
Chrome Bookmarks 7
Chrome Cache Records 694
Chrome Cookies 205
Chrome Downloads 3
Chrome Extensions 43
Chrome Favicons 50
Chrome Keyword Search Terms 3
Chrome Shortcuts 4
Chrome Top Sites 7
Chrome Web History 29
Chrome Web Visits 122
Edge Chromium Cache Records 884
Edge Chromium Cookies 63
Edge Chromium Downloads 2
Edge Chromium Favicons 34
Edge Chromium Keyword Search Terms 2
Edge Chromium Shortcuts 1
Edge Chromium Web History 14
Edge Chromium Web Visits 18
Edge/Internet Explorer 10-11 Content 141
Edge/Internet Explorer 10-11 Cookies 18
EVIDENCE (205)
Column view
Host Name Value Accessed Date/... Created Date/T... Expiration Dat...
.media.net data-c-ts 2022-01-20 2:13:49 PM 2022-01-20 2:13:48 PM 2022-02-19 2:13:48 PM
.media.net data-g 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2022-02-03 2:13:48 PM
.media.net data-mf 2022-01-20 2:13:49 PM 2022-01-20 2:13:49 PM 2023-01-20 2:13:49 PM
.media.net data-mm 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2023-01-19 2:13:48 PM
.media.net data-ttd 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2022-02-03 2:13:48 PM
.media.net data-xu 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2023-01-19 2:13:48 PM
.pippio.com did 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-01-20 2:13:51 PM
.betweendigital.com dc 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.pippio.com didts 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-01-20 2:13:51 PM
.openx.net i 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-01-20 2:13:51 PM
.linksynergy.com icts 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.rubiconproject.com khaos 2022-01-20 2:13:54 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:54 PM
.lijit.com lijt_reader 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-01-20 2:13:51 PM
.w55c.net matchmedianet 2022-01-20 2:13:48 PM 2022-01-20 2:13:48 PM 2022-02-19 2:13:48 PM
.pippio.com nnls 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2022-03-21 3:13:51 PM
.smartadserver.com pbw 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-02-20 2:13:52 PM
.openx.net pd 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2022-02-04 2:13:51 PM
.richaudience.com pdid 2022-01-20 2:13:50 PM 2022-01-20 2:13:50 PM 2022-02-19 2:13:50 PM
.smartadserver.com pdomid 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-02-20 2:13:52 PM
.smartadserver.com pid 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2023-02-20 2:13:52 PM
.tynt.com pids 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2022-04-20 3:13:52 PM
.pippio.com pxrc 2022-01-20 2:13:51 PM 2022-01-20 2:13:51 PM 2022-03-21 3:13:51 PM
.rlcdn.com pxrc 2022-01-20 2:13:53 PM 2022-01-20 2:13:51 PM 2022-03-21 3:13:53 PM
.rlcdn.com rlas3 2022-01-20 2:13:53 PM 2022-01-20 2:13:53 PM 2023-01-20 2:13:53 PM
.linksynergy.com rmuid 2022-01-20 2:13:52 PM 2022-01-20 2:13:52 PM 2023-01-20 2:13:52 PM
.rubiconp...
T433-Student-W10.vmdk
DETAILS
ARTIFACT INFORMATION
Host .rub
Name kha
Accessed Date/Time 202 PM
Created Date/Time 202 PM
Expiration Date/Time 202 PM
Path /
Artifact type
Item ID 148
EVIDENCE INFORMATION
Source T43 W1 (Mi GB) CO \Lo \Us \Ne
Recovery method Pars
Deleted source
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00
ENG US
3:21 AM 2022-11-15



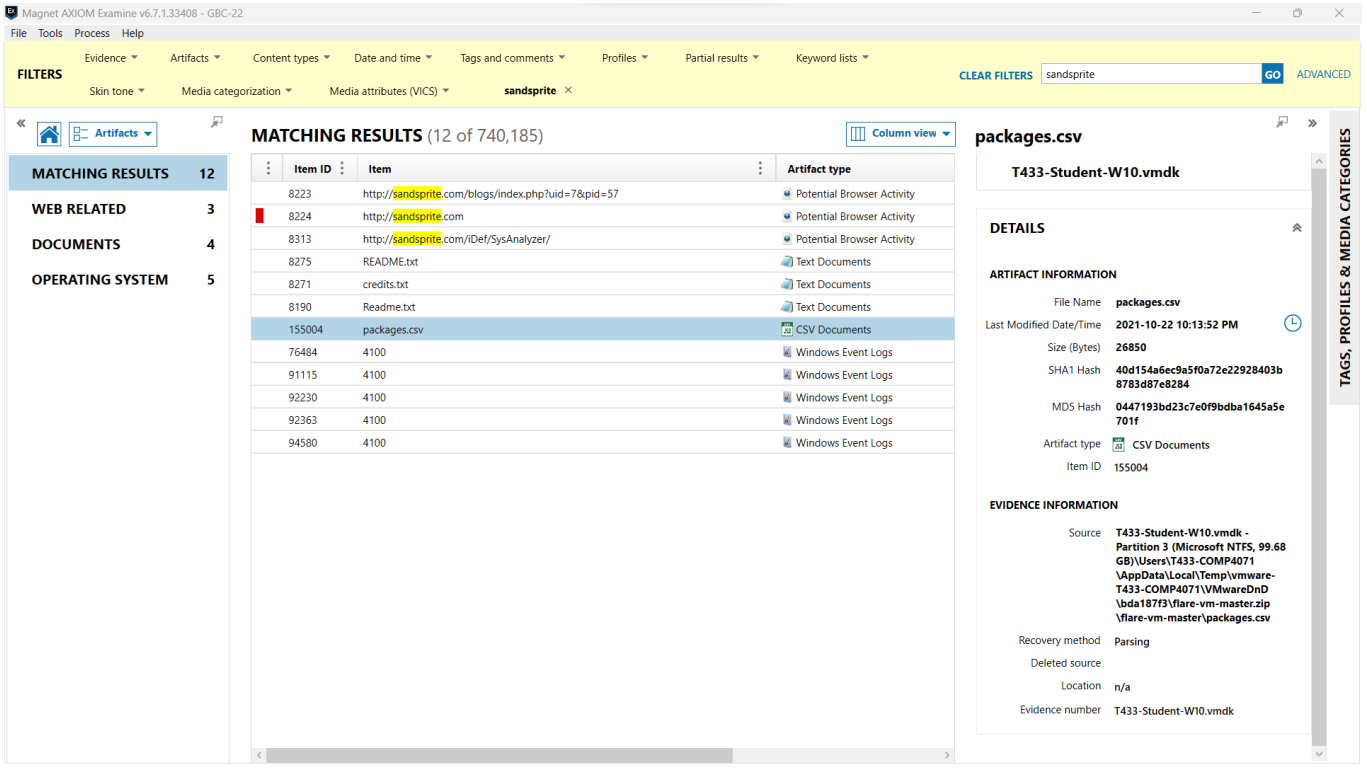


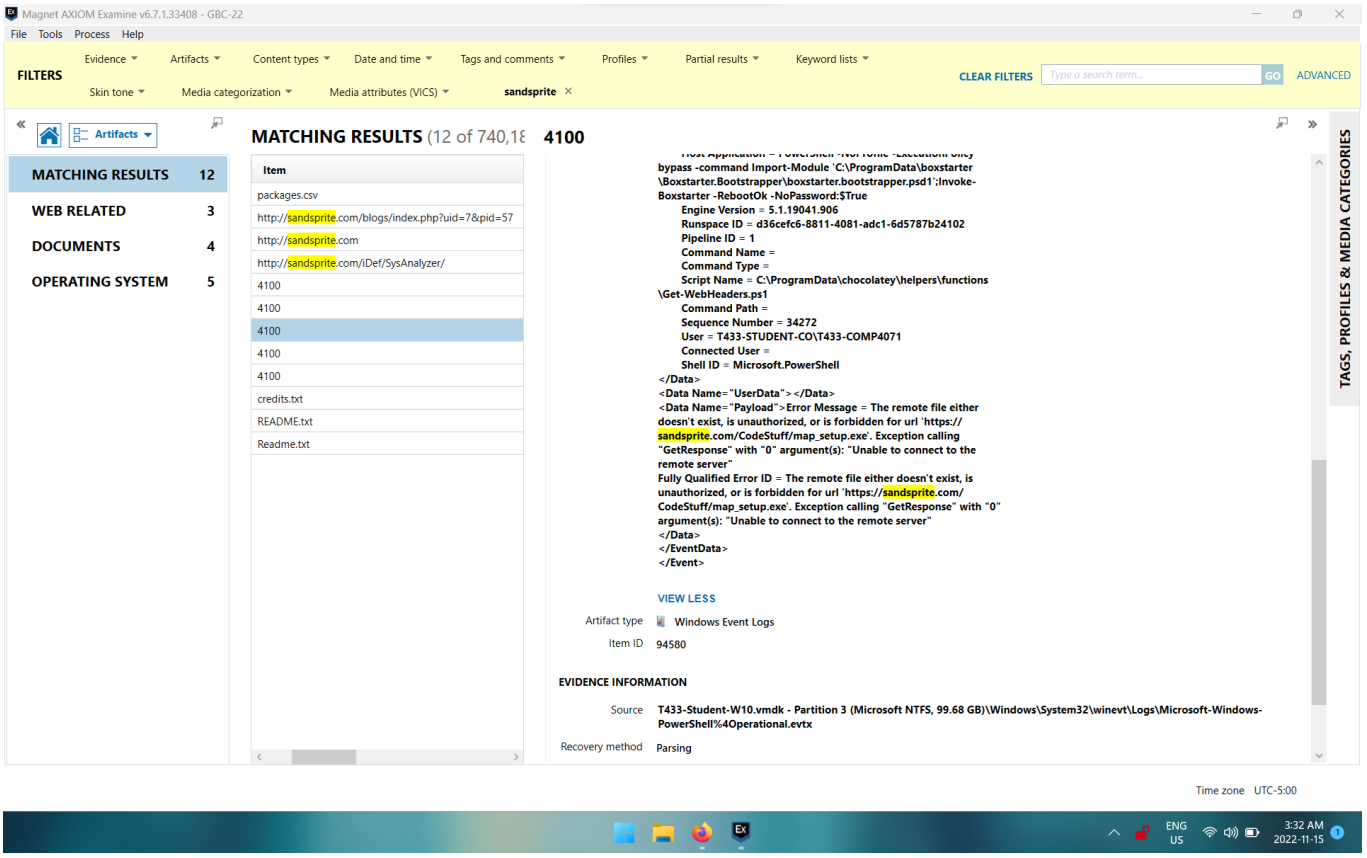
In potential browser activity, one of the domains out of 50k appear to be malicious - sandsprite.com. Aside from being flagged on virustotal, upon searching the keyword in Axiom, the domain is also appearing in other suspicious looking documents.

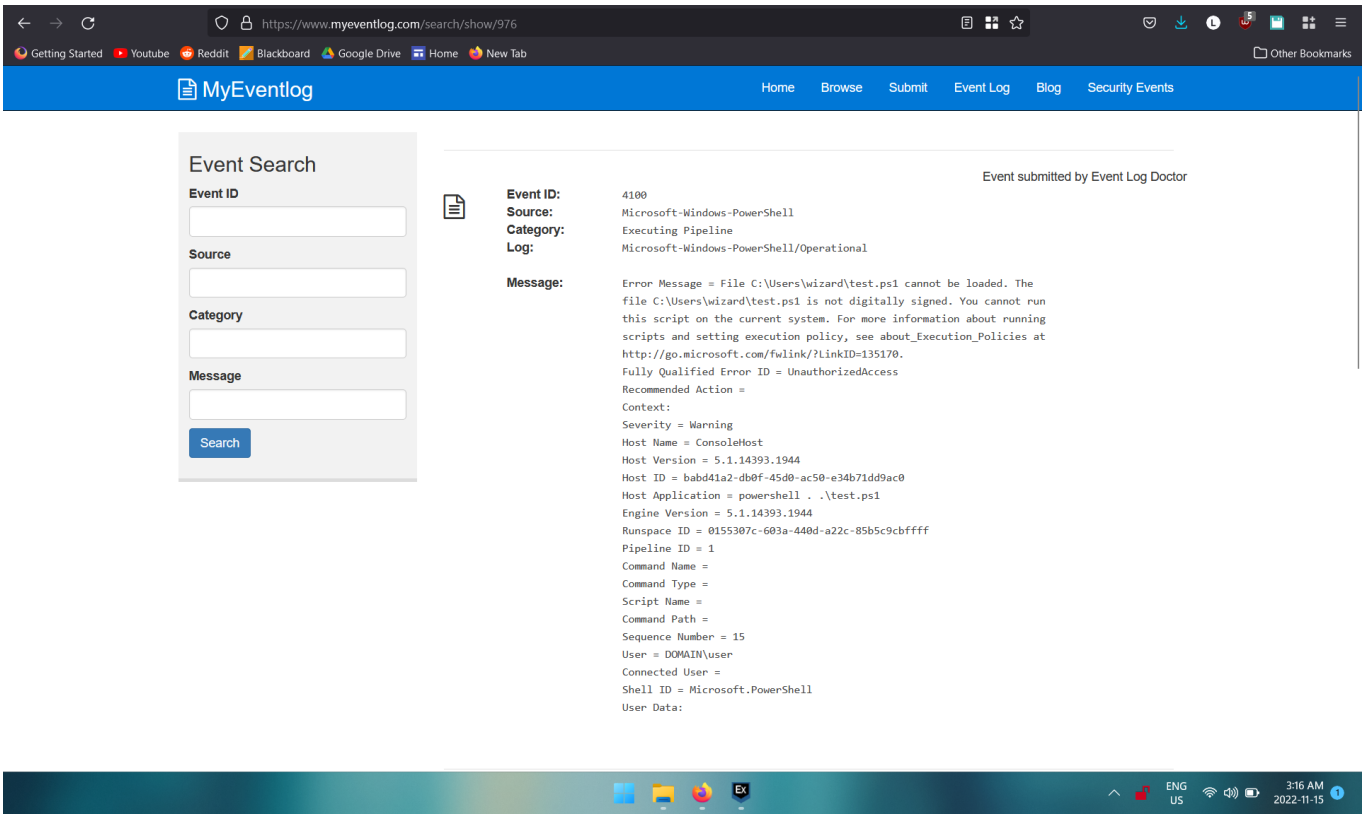




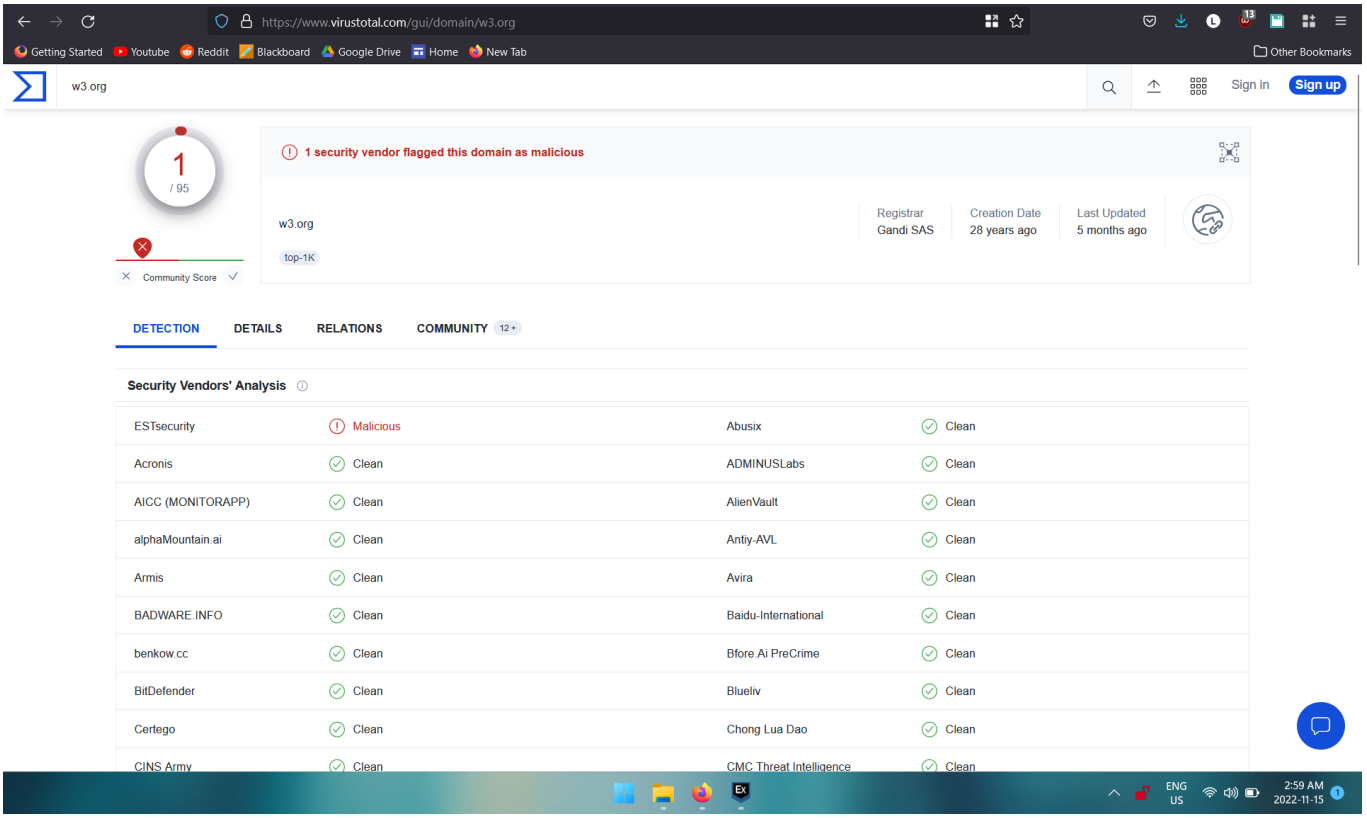
Furthermore, 5 windows security logs were triggered involving event ID 4100, which indicates that some application that contains the domain was trying to run a remote download script on the system without the proper privileges. It is fair to say that this domain is associated with malicious activities.


Magnet AXIOM Examine v6.7.1.33408 - GBC-22
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists
Skin tone Media categorization Media attributes (VICS) sandsprite
CLEAR FILTERS sandsprite GO ADVANCED
Artifacts
MATCHING RESULTS 12
WEB RELATED 3
DOCUMENTS 4
OPERATING SYSTEM 5
MATCHING RESULTS (12 of 740,185)
Column view
Item ID Item Artifact type
8223 http://sandsprite.com/blogs/index.php?uid=7&pid=57 Potential Browser Activity
8224 http://sandsprite.com Potential Browser Activity
8313 http://sandsprite.com/iDef/SysAnalyzer/ Potential Browser Activity
8275 README.txt Text Documents
8271 credits.txt Text Documents
8190 Readme.txt Text Documents
155004 packages.csv CSV Documents
76484 4100 Windows Event Logs
91115 4100 Windows Event Logs
92230 4100 Windows Event Logs
92363 4100 Windows Event Logs
94580 4100 Windows Event Logs
packages.csv
T433-Student-W10.vmdk
DETAILS
ARTIFACT INFORMATION
File Name packages.csv
Last Modified Date/Time 2021-10-22 10:13:52 PM
Size (Bytes) 26850
SHA1 Hash 40d154a6ec9a5f0a72e22928403b8783d87e8284
MD5 Hash 0447193bd23c7e0f9bdba1645a5e701f
Artifact type CSV Documents
Item ID 155004
EVIDENCE INFORMATION
Source T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Users\T433-COMP4071\AppData\Local\Temp\vmware-T433-COMP4071\VMwareDnD\bda187f3\flare-vm-master.zip\flare-vm-master\packages.csv
Recovery method Parsing
Deleted source
Location n/a
Evidence number T433-Student-W10.vmdk
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00
ENG US
3:15 AM 2022-11-15

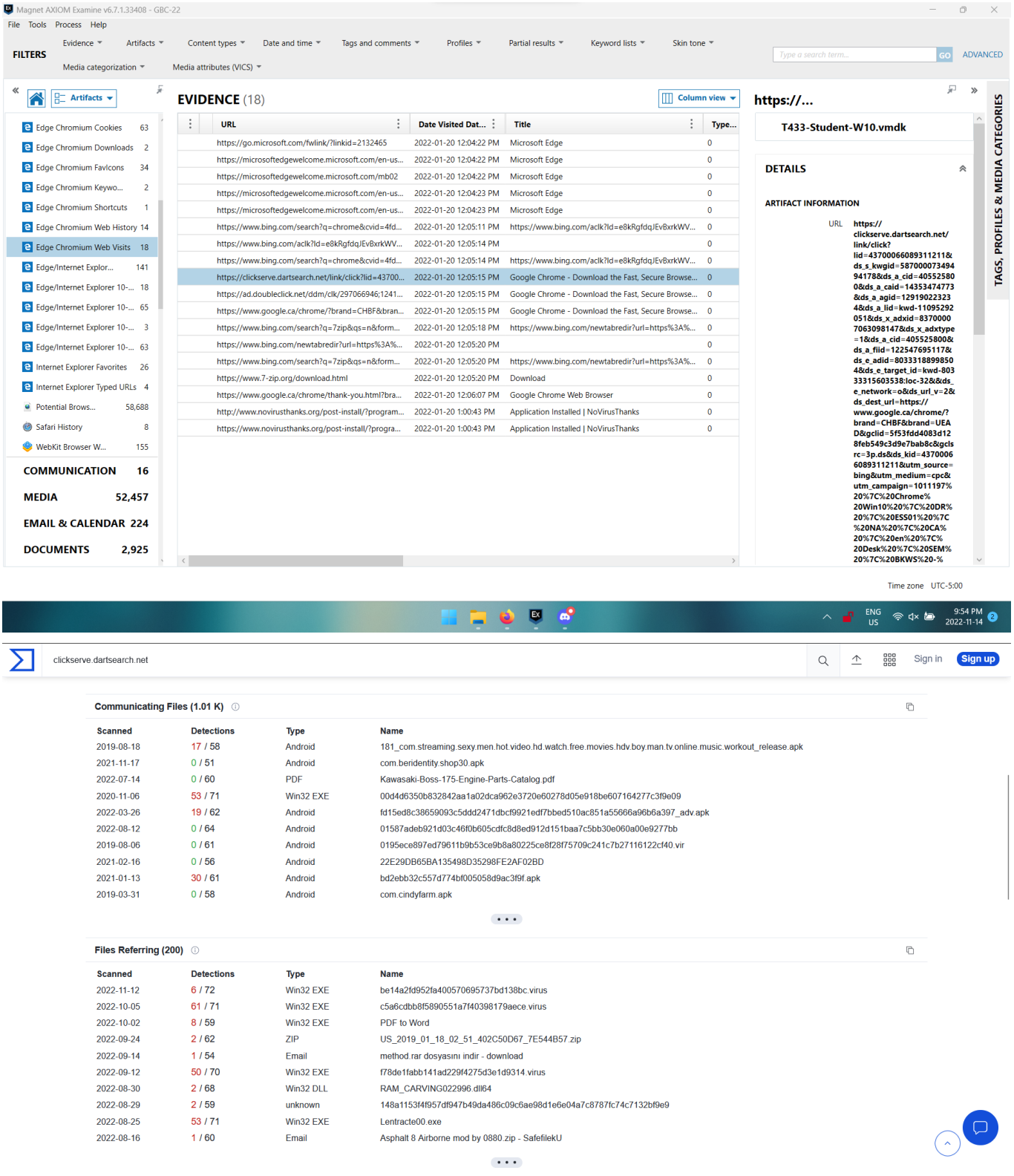

Magnet AXIOM Examine v6.7.1.33408 - GBC-22
File Tools Process Help
FILTERS
Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists
Skin tone Media categorization Media attributes (VICS) sandsprite
CLEAR FILTERS Type a search term... GO ADVANCED
Artifacts
MATCHING RESULTS 12
WEB RELATED 3
DOCUMENTS 4
OPERATING SYSTEM 5
MATCHING RESULTS (12 of 740,18
Item
packages.csv
http://sandsprite.com/blogs/index.php?uid=7&pid=57
http://sandsprite.com
http://sandsprite.com/iDef/SysAnalyzer/
4100
4100
4100
4100
4100
credits.txt
README.txt
Readme.txt
4100
bypass -command Import-Module 'C:\ProgramData\boxstarter\Boxstarter.Bootstrapper\boxstarter.bootstrapper.psd1';Invoke-Boxstarter -RebootOk -NoPassword:$True
Engine Version = 5.1.19041.906
Runspace ID = d36cefc6-8811-4081-adc1-6d5787b24102
Pipeline ID = 1
Command Name =
Command Type =
Script Name = C:\ProgramData\chocolatey\helpers\functions\Get-WebHeaders.ps1
Command Path =
Sequence Number = 34272
User = T433-STUDENT-CO\T433-COMP4071
Connected User =
Shell ID = Microsoft.PowerShell
</Data>
<Data Name="UserData"> </Data>
<Data Name="Payload">Error Message = The remote file either doesn't exist, is unauthorized, or is forbidden for url 'https://sandsprite.com/CodeStuff/map_setup.exe'. Exception calling "GetResponse" with "0" argument(s): "Unable to connect to the remote server"
Fully Qualified Error ID = The remote file either doesn't exist, is unauthorized, or is forbidden for url 'https://sandsprite.com/CodeStuff/map_setup.exe'. Exception calling "GetResponse" with "0" argument(s): "Unable to connect to the remote server"
</Data>
</EventData>
</Event>
VIEW LESS
Artifact type Windows Event Logs
Item ID 94580
EVIDENCE INFORMATION
Source T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx
Recovery method Parsing
TAGS, PROFILES & MEDIA CATEGORIES
Time zone UTC-5:00
ENG US
3:32 AM 2022-11-15



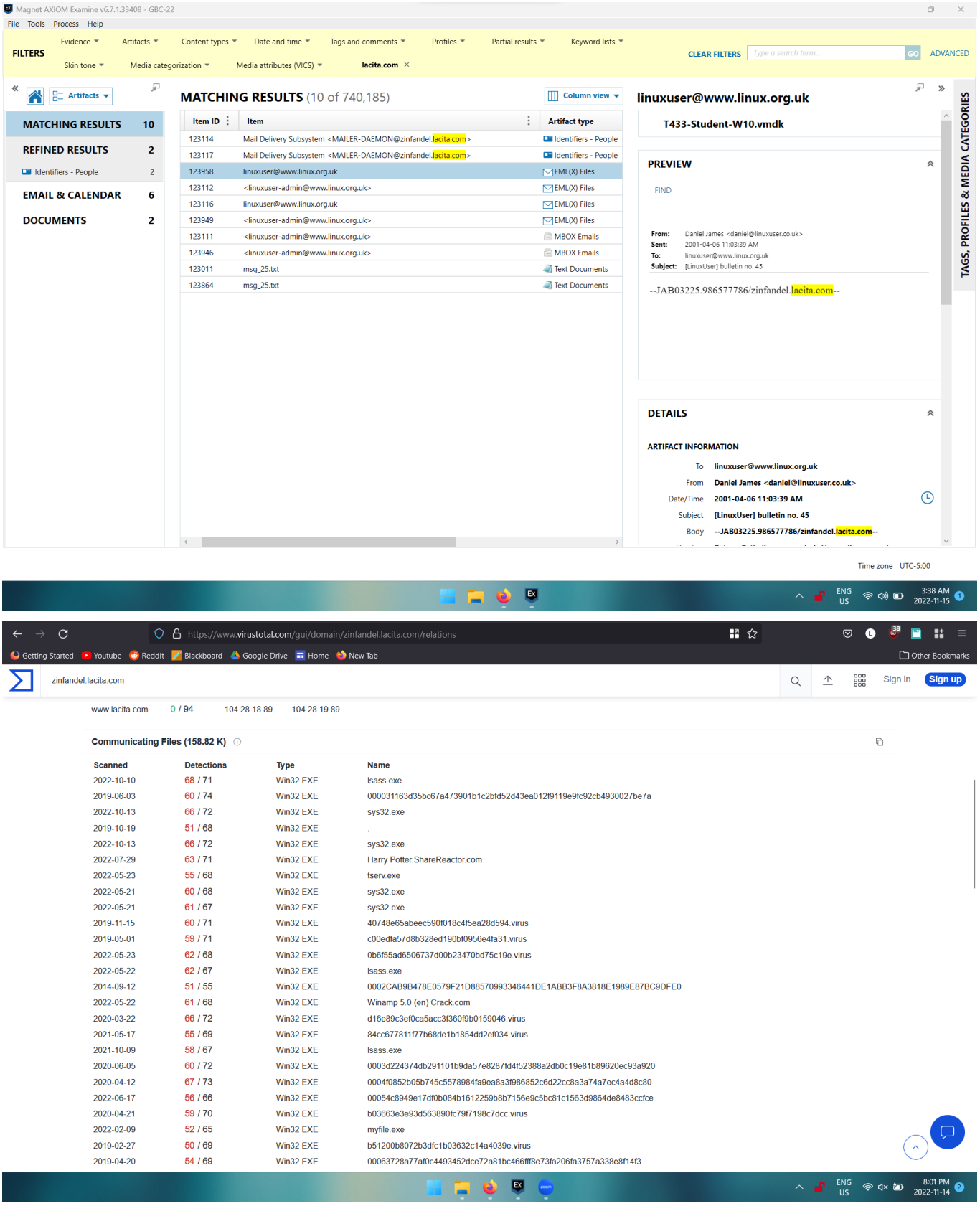
Due to the sheer number of domains in web related activities, I could not possibly check whether every website is malicious. I have a few examples below of domains that are flagged on virustotal.



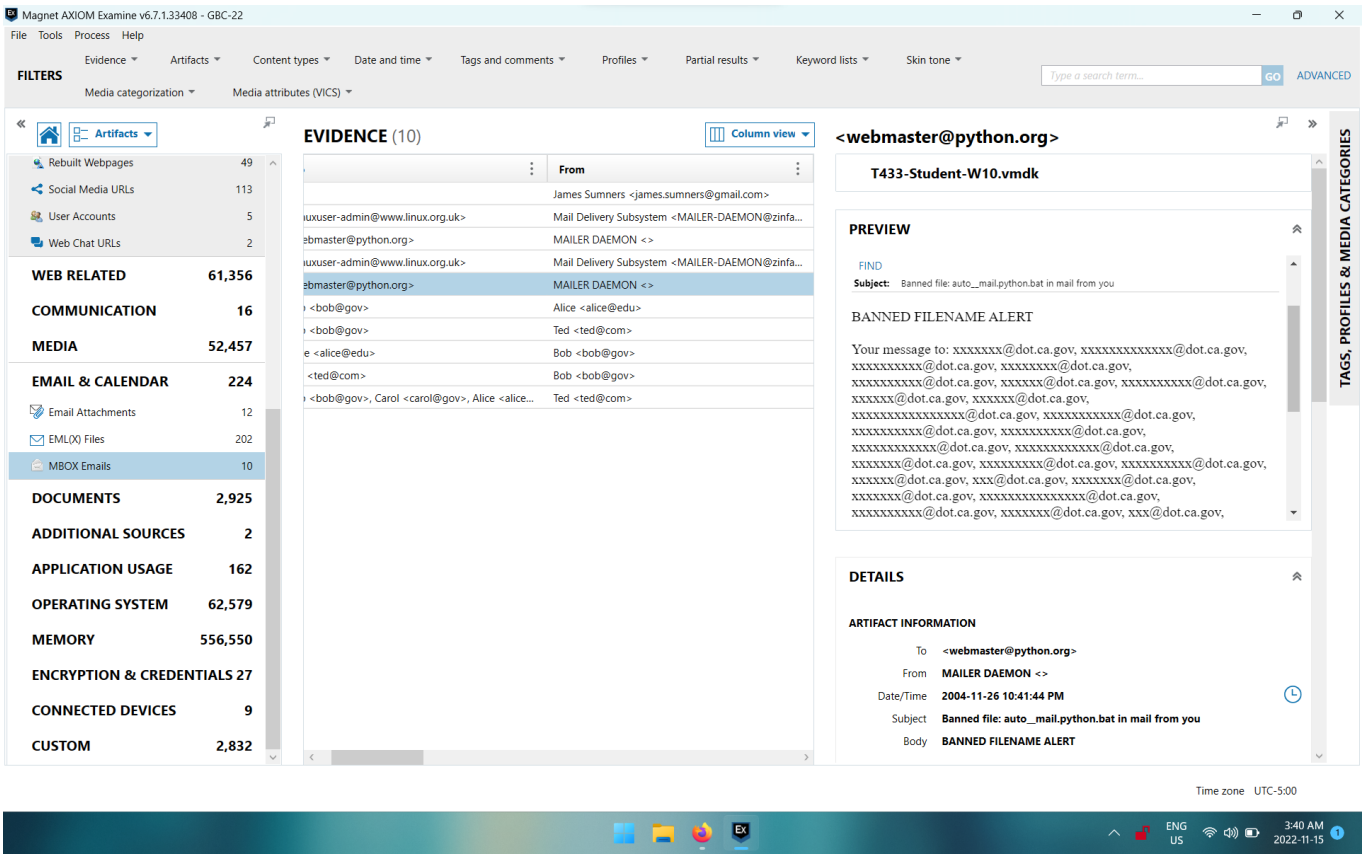
The observation that there are a number of suspicious web activities on the host is also true for other browsers like Edge. Here is one example.



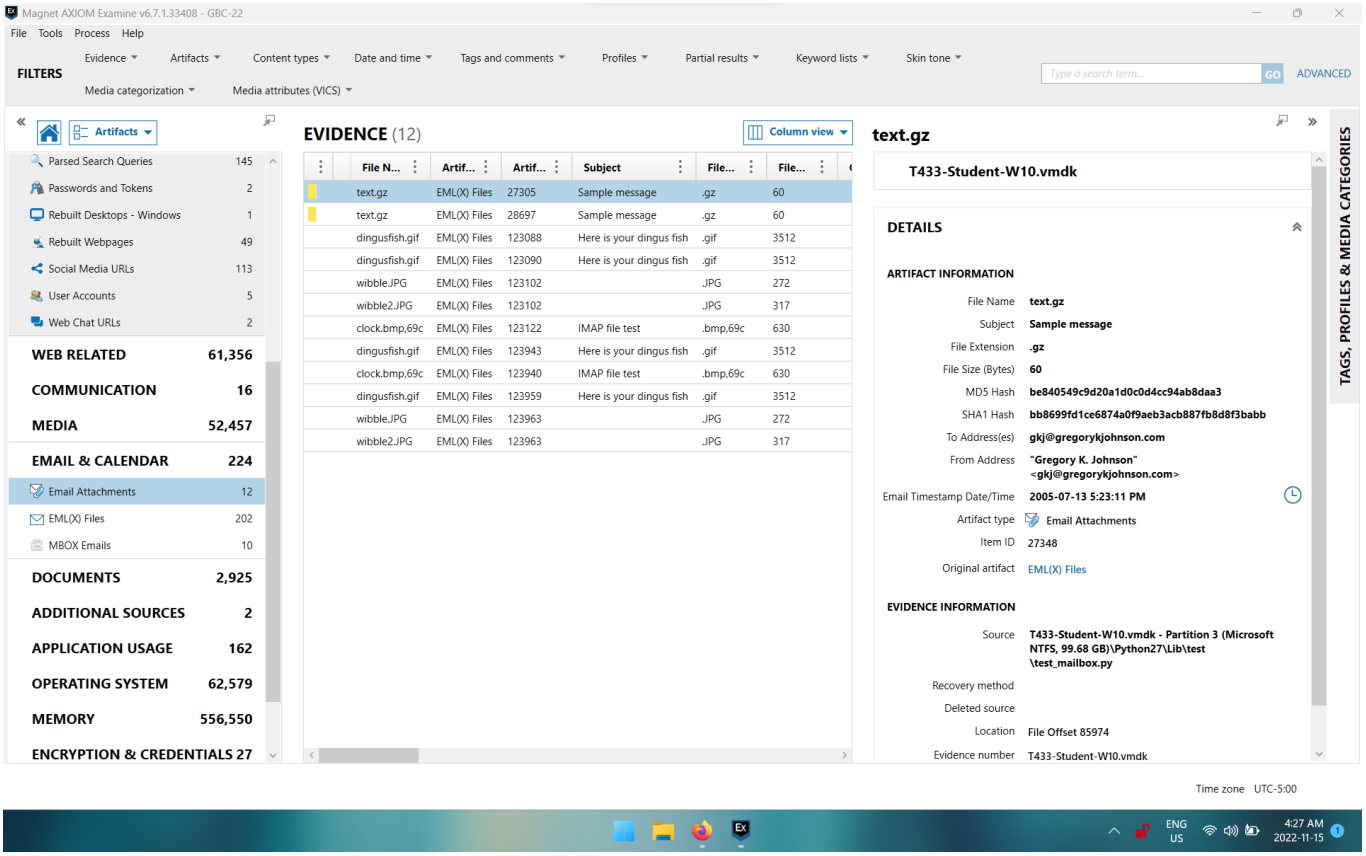
In the emails, domain names that appear suspicious are seen in the bodies. Although the time frame does not match the attack, I thought it is worth noting.



The user was also found trying to send a .bat script called auto__mail.python.bat to some email addresses, but was sent back by the system due to triggering a defense alert.

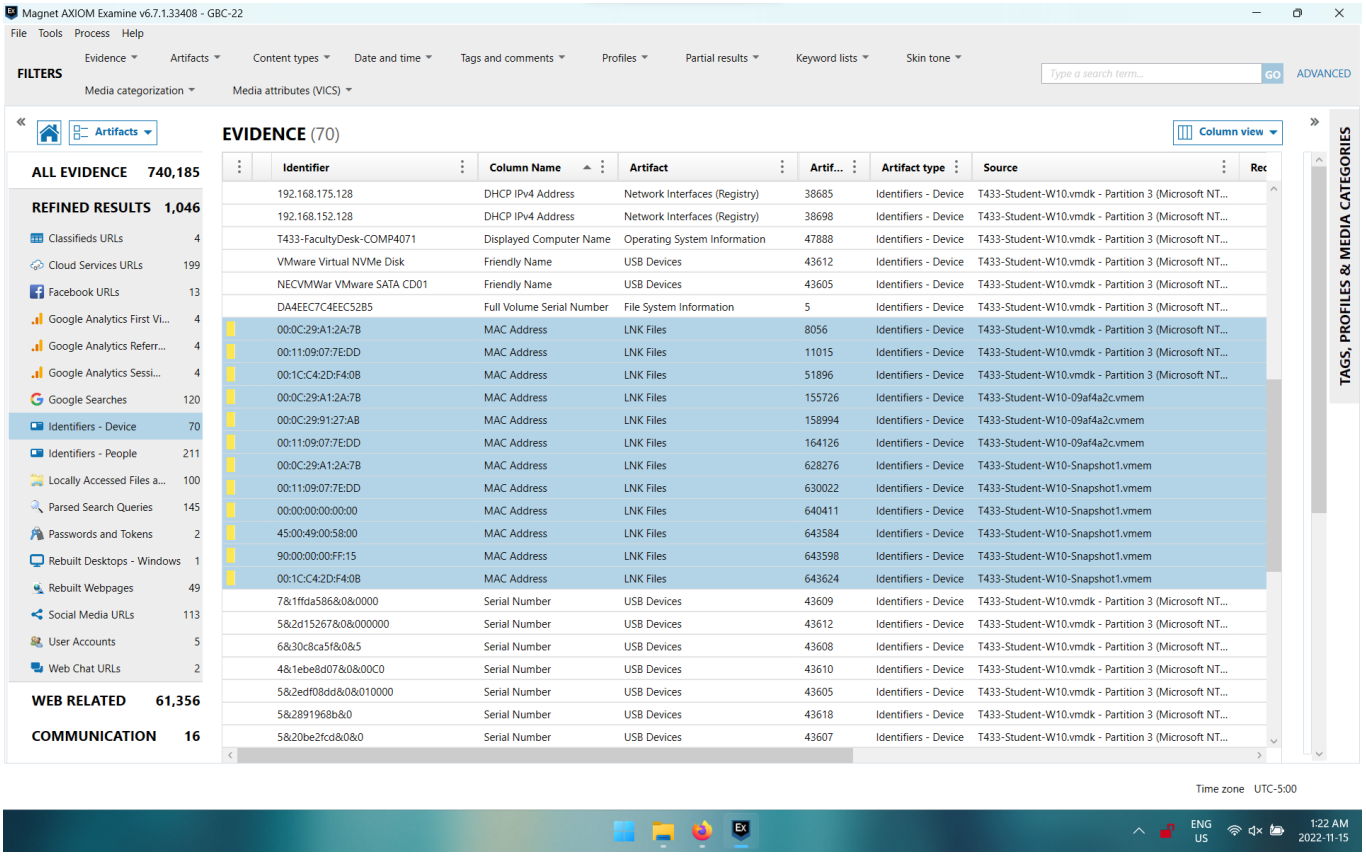


Two instances of attachment zips were also found in emails.

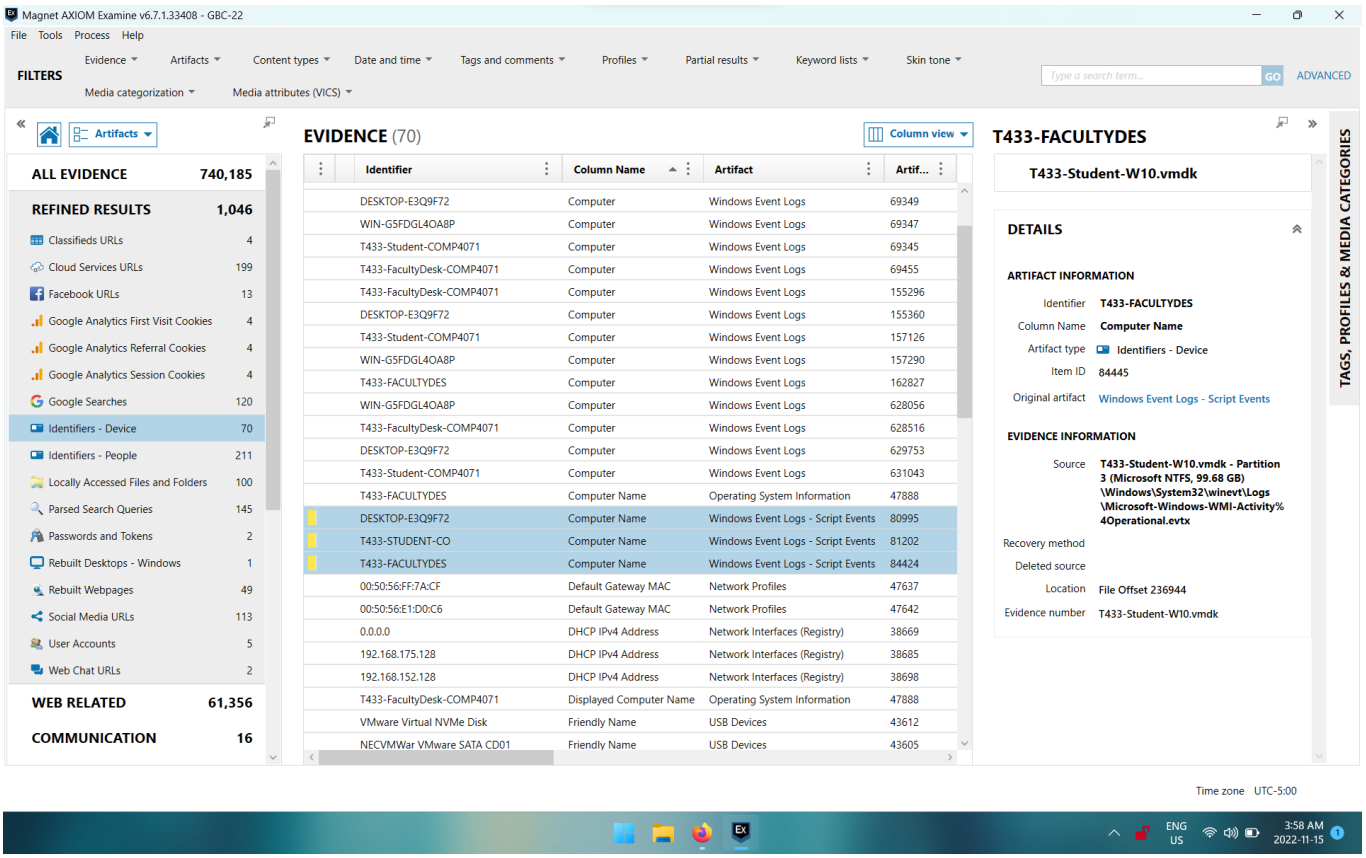


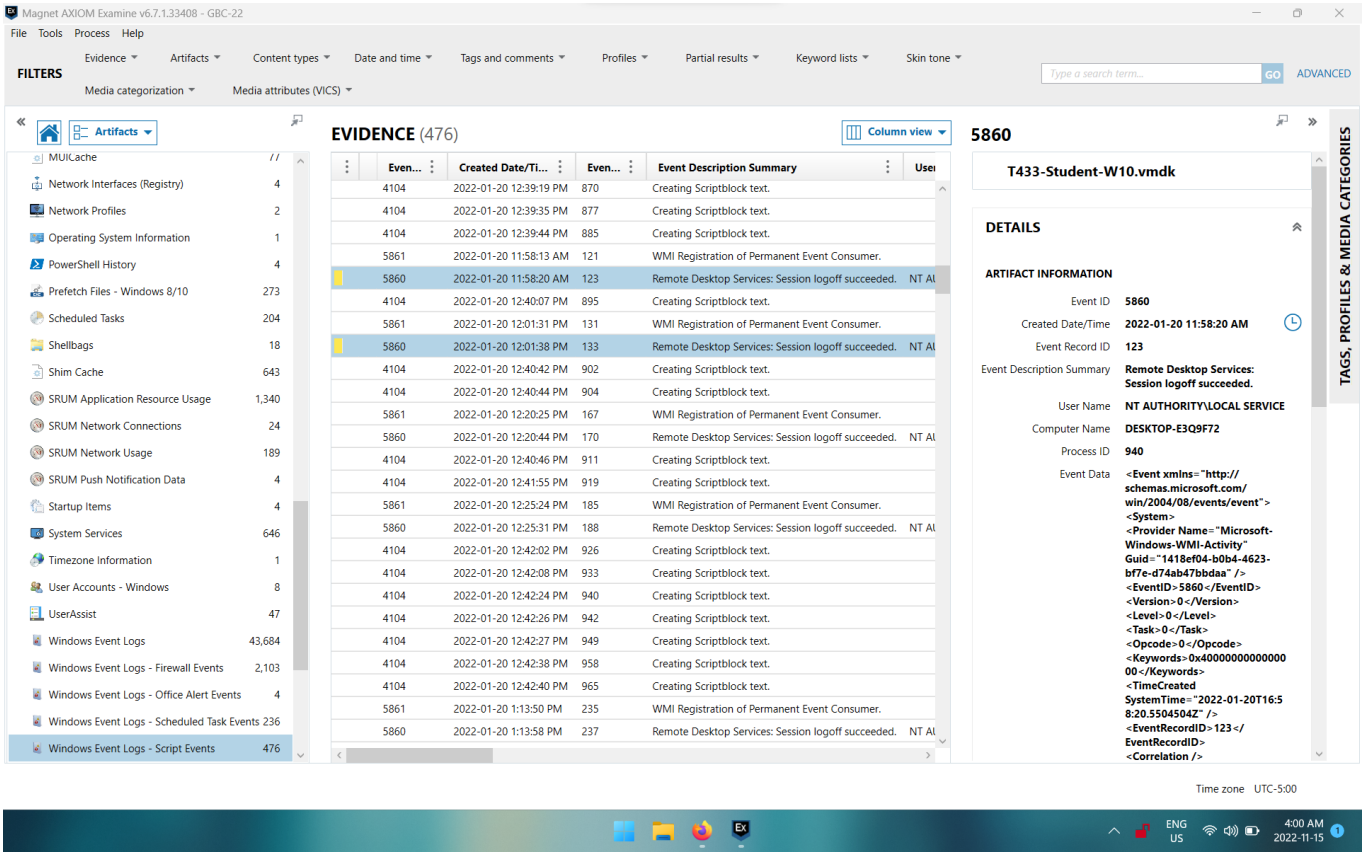
Local data evidence

First, the MAC address of the host might have been spoofed as potential changes are observed. Multiple LNK files related to Mac addresses are present.



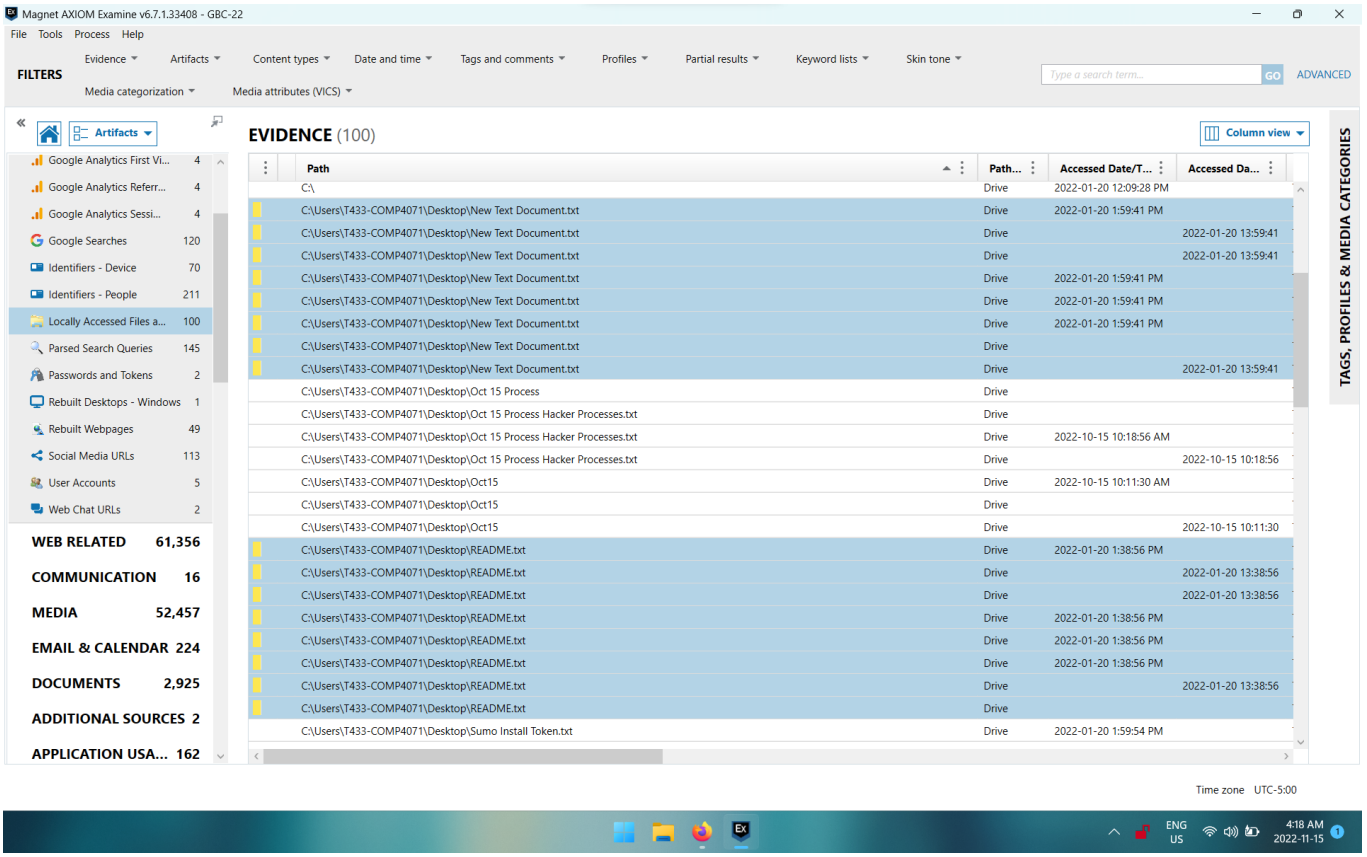
Furthermore in the device section, some devices have been recorded in Axiom from Windows Script event logs. These event logs indicate a remote desktop service logging off. While this is not conclusive of an intrusion, the log was recorded in the timeframe that the attack happened so this is suspicious.



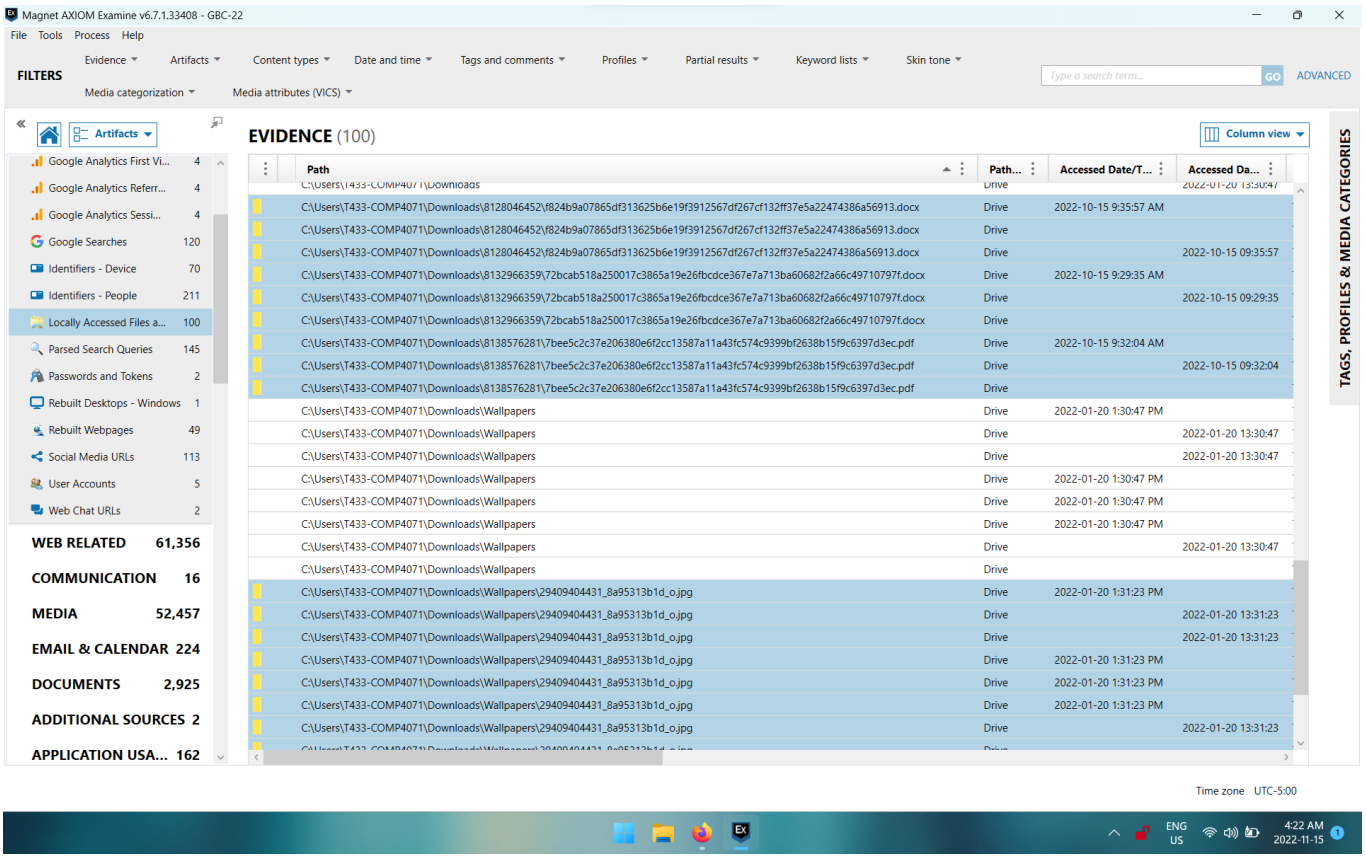


In locally accessed files, some text files have been created on the desktop during the attack time frame. As you can see in the screenshots, not only were the files “New Text Document.txt” and “README.txt”

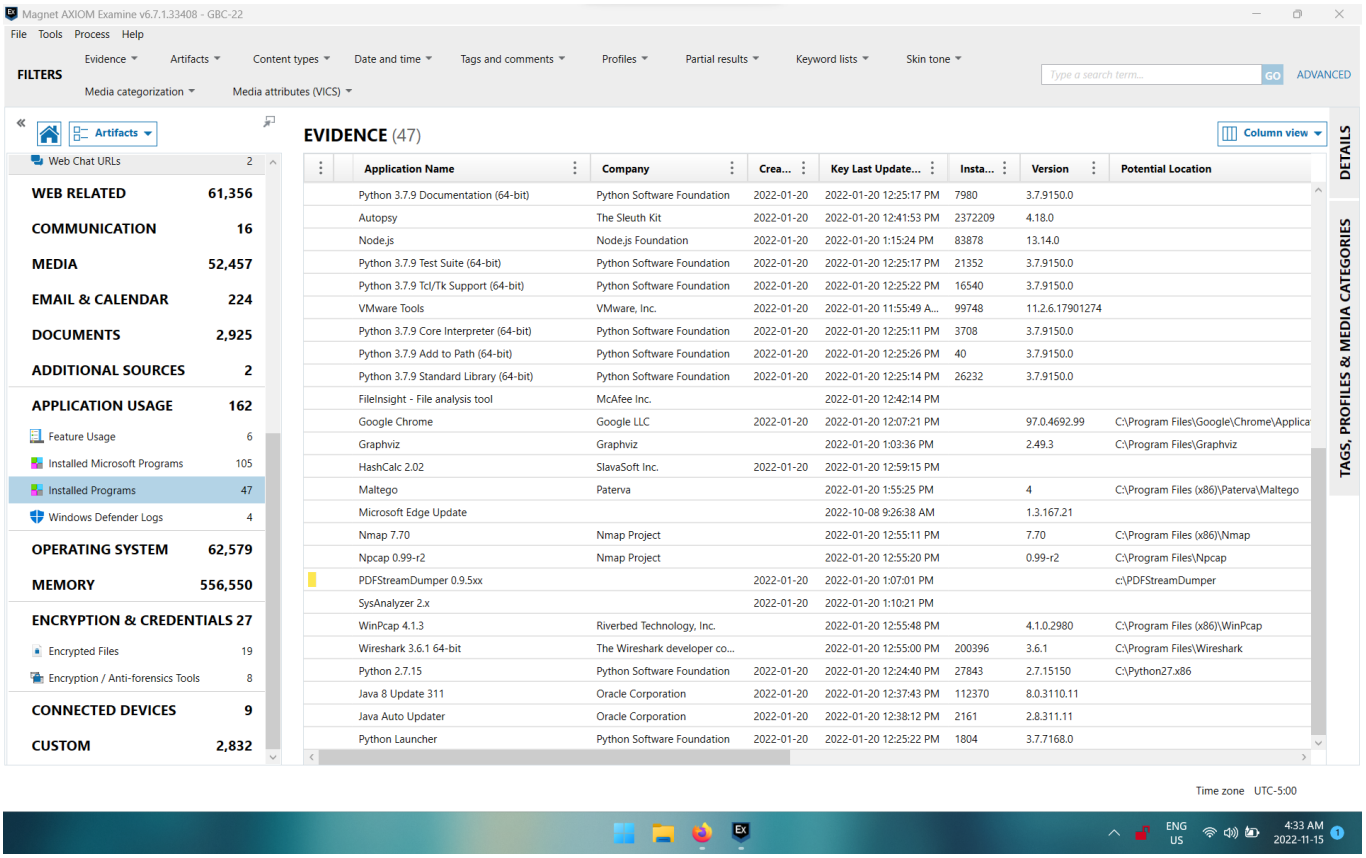
created, they were also being accessed multiple times, microseconds apart which potentially indicate automated activities.



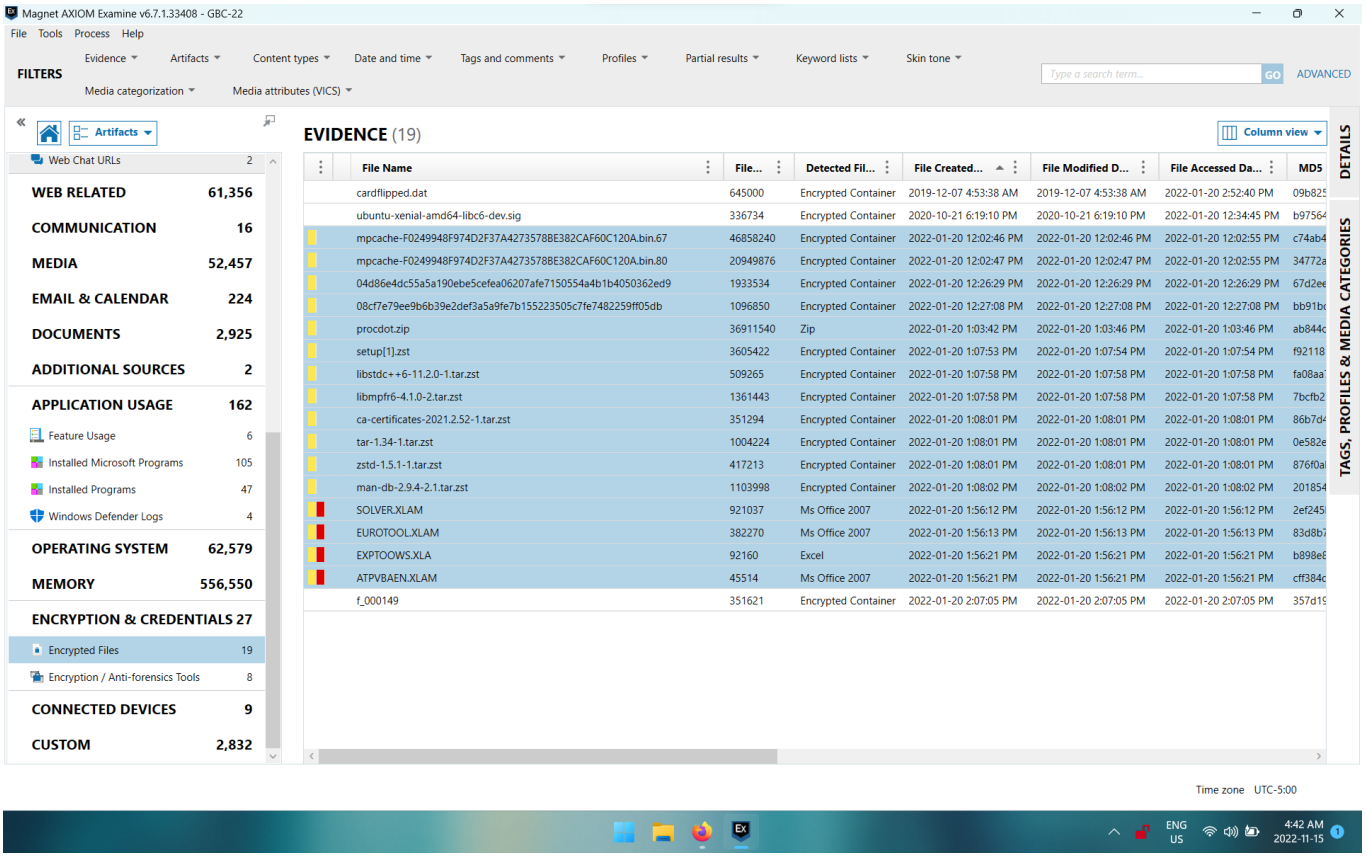
In the Downloads folder, some pdfs and docx with hash-like file names are found to be accessed. At the time of the incident, wallpaper jpgs were also accessed milliseconds apart. These files might all be malicious.



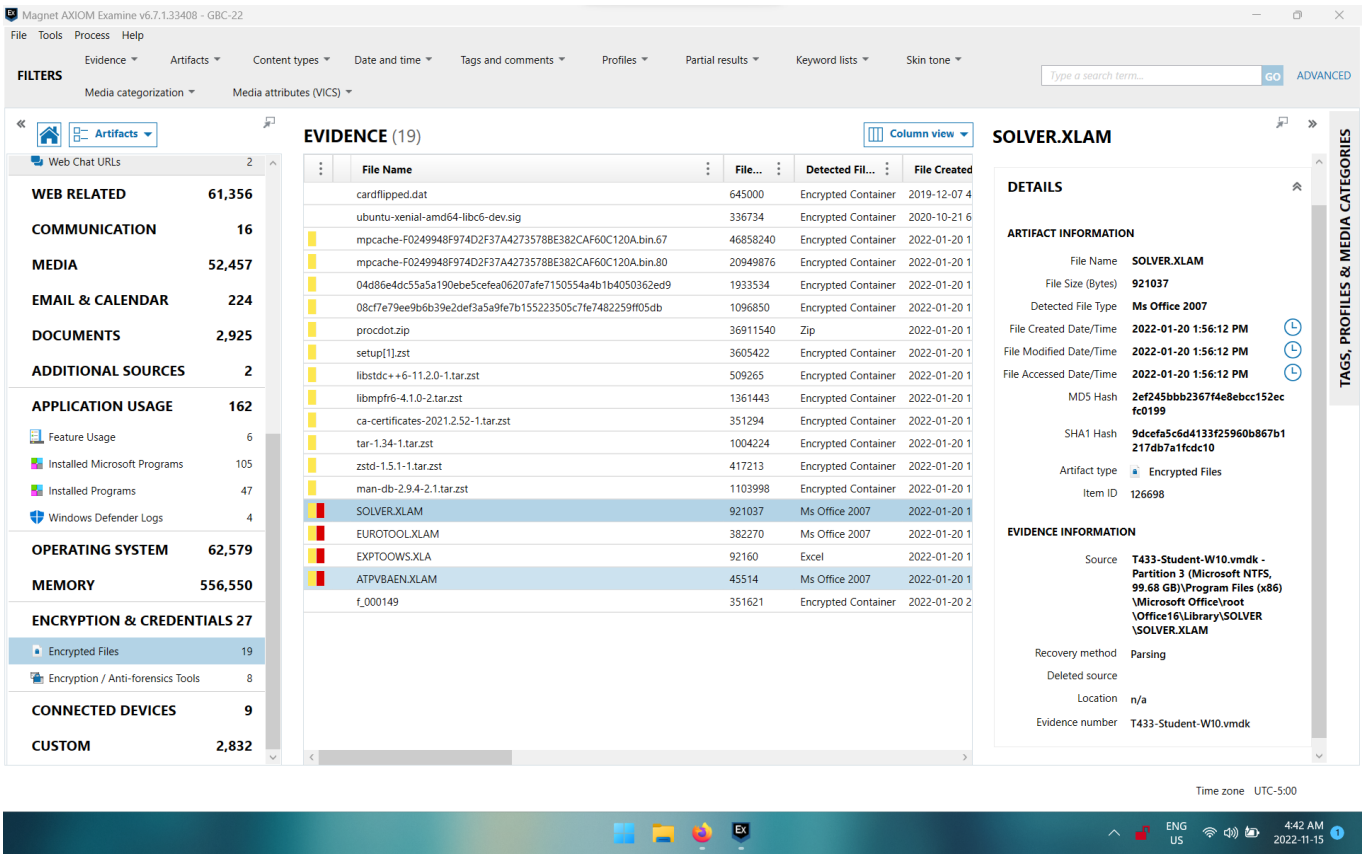
In the list of installed programs, PDFStreamDumper was seen associated with the previously identified malicious domains. Also, its installation location is rather unorthodox as it does not follow the convention of installing programs in C:/Program Files.



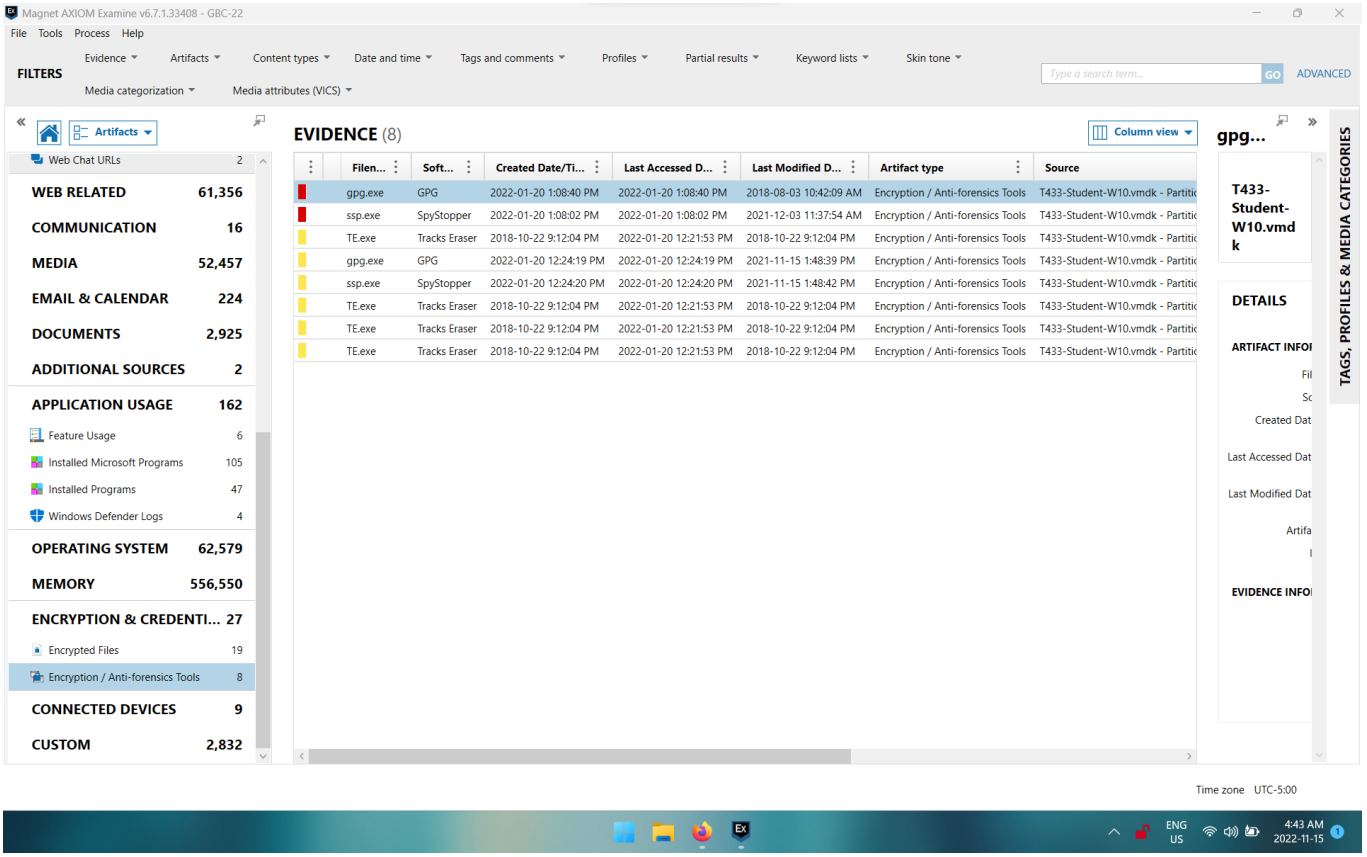
In the encrypted file section, multiple files that are created in the attack time frame are encrypted. Notably, there are 4 excel macros .XLAMs present.



If we dig into their installation location, they are installed in Program Files (x86)\Microsoft Office\root. Running XLAMs from the root directory does not require explicit permission from the logged in user. This has a good chance to be malicious.

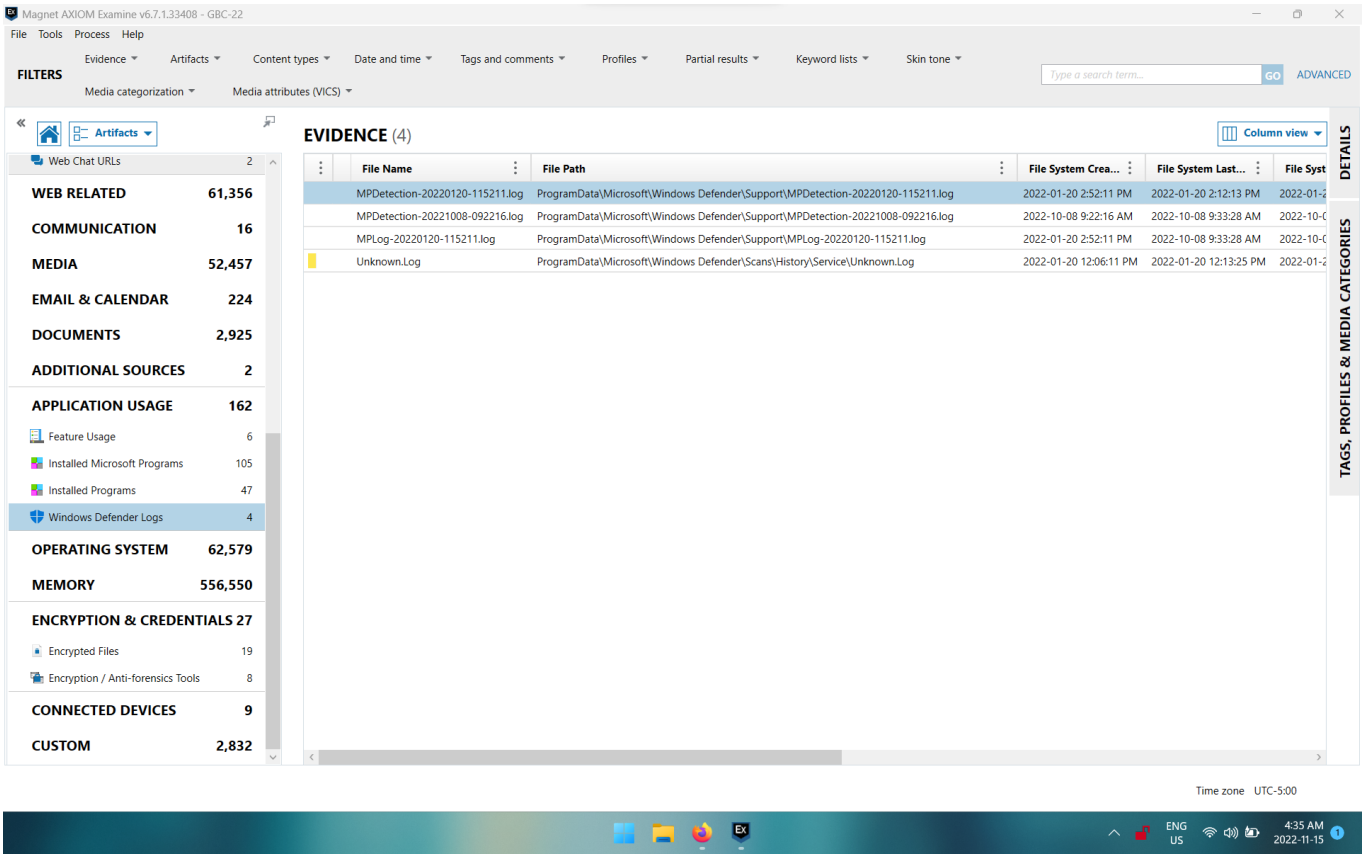


All of the files in the encryption/anti-forensics tools section were accessed during the time of attack. It is likely that they were used in conjunction with the malware for encryption and obfuscation purposes.

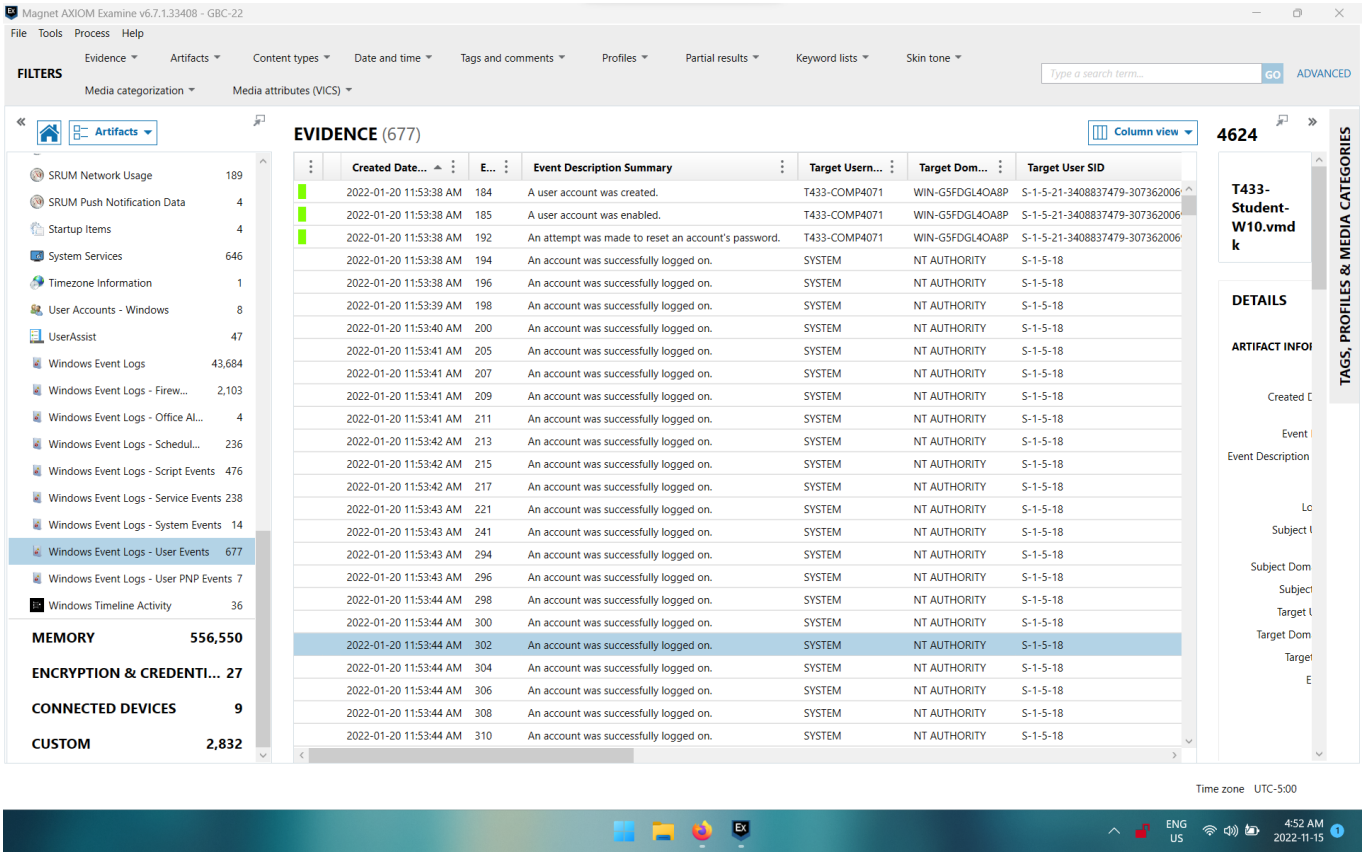


Log events evidence

In the Windows Defender Log section, Unknown.Log does not appear to follow the same naming convention as the other detection or scan logs. The File location is also different. The log file is of interest.



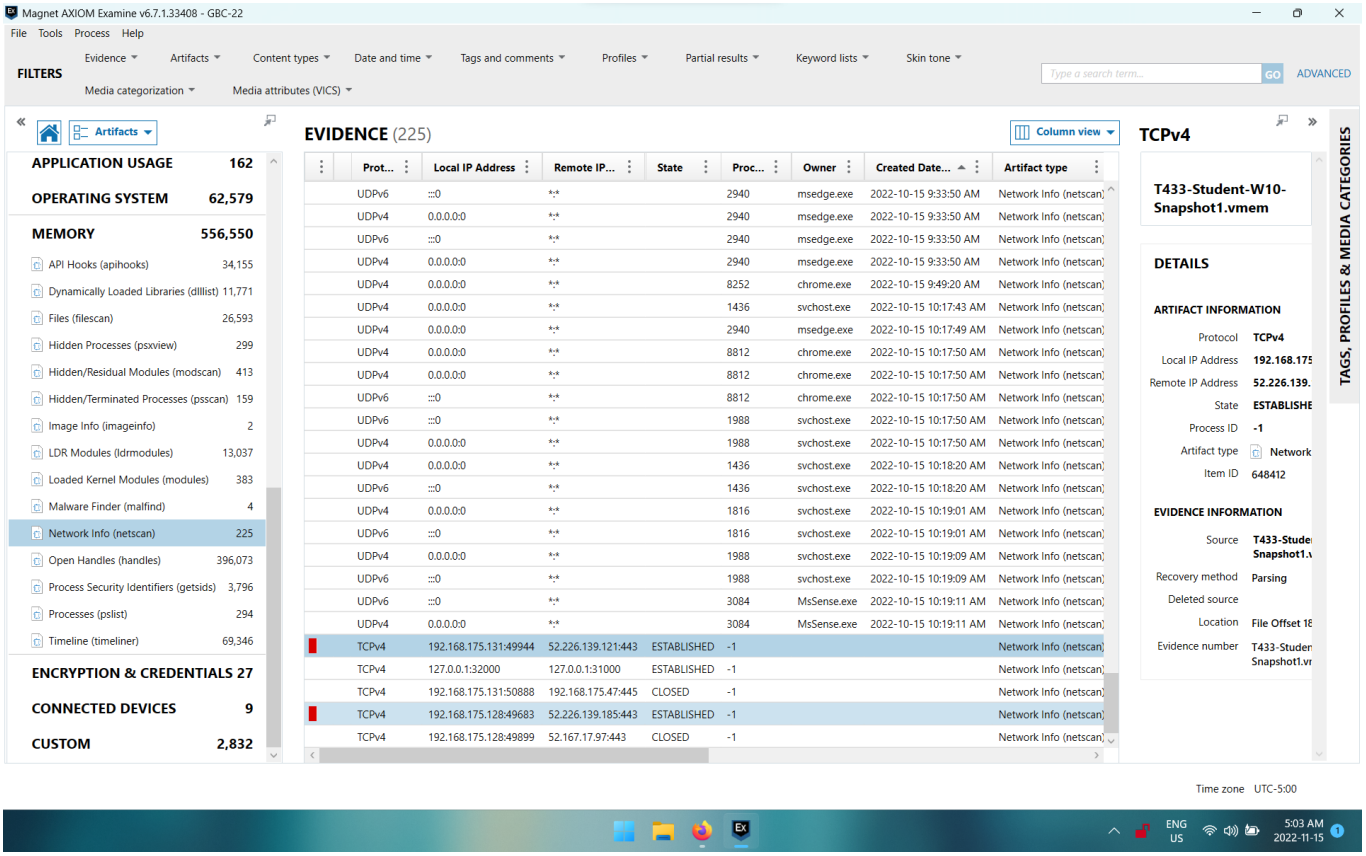
Moving on to investigate Windows event logs, first we take a look at user events. At 11:53AM, three consecutive event logs show that an attempt was first made to reset a local account's password, then the user was enabled and created. All 3 logs targeted the same user: T433-COMP4071. Most other logs are service related so these 3 stand out particularly.



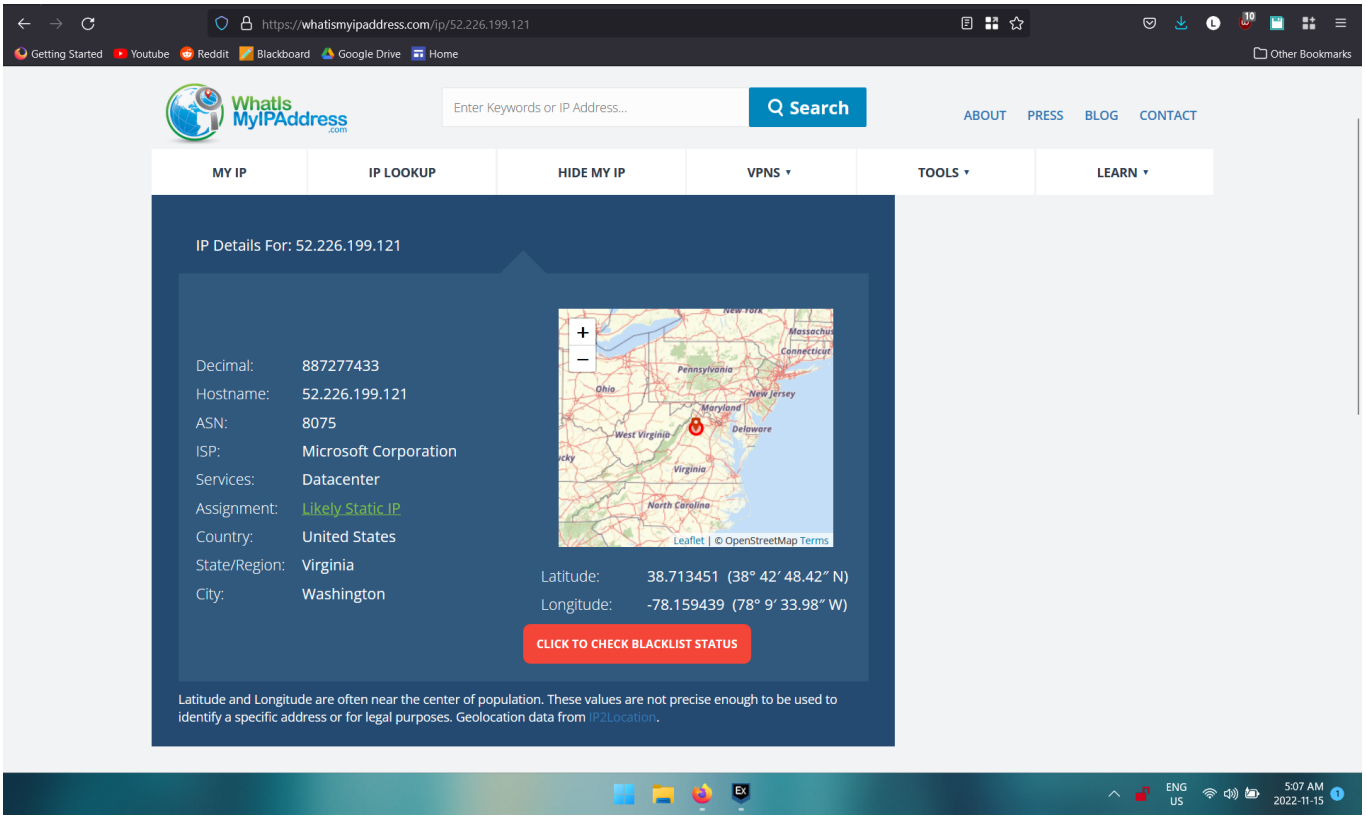
Memory evidence

We understand that the memory dump in this file case was not created right after the event. Instead, it is captured roughly 9 months after the compromise happened. While we might not see the malwares in action in the dumps, we could bank on the malwares establishing persistence within the system which leaves traces for us to investigate even until now.

First, we use netscan to check if there is any persistent connection established. There are 2 TCP/IP connections that are shown “established”. The destination addresses here are likely within the same area, with the IP being 52.226.139.121/185.



An IP lookup yields no meaningful results.



Now, let’s try to identify malicious processes with pslist.

The first thing that stands out as unusual is how there are so many chrome.exe instances running. With the previous investigation putting so much focus on web related evidence, I cannot help but suspect there is something wrong with all these instances of chrome.

Turns out they all come from the same Parent ID 8252, which is another chrome.exe instance. Tracing it back, this parent chrome.exe is launched by explorer.exe with ID 4284.

Explorer.exe ID 4284 also launched other children applications that might be malicious, such as notepad.exe and 19075-NYPD.exe.