

# **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

Type a search term... GO ADVANCED

**EVIDENCE (199)**

**ALL EVIDENCE 740,185**

**REFINED RESULTS 1,046**

- Classified 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=%			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/?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

Time zone UTC-5:00

ENG US 2:01 AM 2022-11-15

TAGS, PROFILES & MEDIA CATEGORIES

Getting Started YouTube Reddit Blackboard Google Drive Home New Tab Other Bookmarks

crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'onewe.live.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	7939298186	2022-11-09	2022-11-09	2023-11-04	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 05
	7939293951	2022-11-09	2022-11-09	2023-11-04	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 06
	7296261079	2022-08-08	2022-08-08	2023-08-08	onewe.live.com	*.onewe.live.com onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	6928292077	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6928298881	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 02
	6928274559	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6928266723	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 02
	6928246605	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6928237160	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 02
	6928207154	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6928196328	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6928159731	2022-06-13	2022-06-13	2023-06-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 02
	6928137598	2022-06-13	2022-06-13	2023-06-08	storage.live.com	soak2.test.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6889243047	2022-06-07	2022-06-02	test.onewe.live.com	soak3.test.onewe.live.com test.onewe.live.com	soak2.test.onewe.live.com test.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 06
	6723916812	2022-05-13	2022-05-13	2023-05-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6723885518	2022-05-13	2022-05-13	2023-05-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6723834399	2022-05-13	2022-05-13	2023-05-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 02
	6723822286	2022-05-13	2022-05-13	2023-05-08	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft Azure TLS Issuing CA 01
	6438113579	2022-03-30	2022-03-29	2023-03-29	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	6082438790	2022-02-01	2022-02-01	2023-02-01	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	6041696840	2022-01-24	2022-01-24	2023-01-24	storage.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	6041636590	2022-01-24	2022-01-24	2023-01-24	storage.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	6041626702	2022-01-24	2022-01-24	2023-01-24	storage.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	5297592223	2021-09-27	2021-09-27	2022-09-27	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	5219070663	2021-09-14	2021-09-14	2022-09-14	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	5219070453	2021-09-14	2021-09-14	2022-09-14	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 02
	5073921676	2021-08-19	2021-08-19	2022-08-19	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	5073910333	2021-08-19	2021-08-19	2022-08-19	storage.live.com	skyapi.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	5034606769	2021-08-13	2021-08-13	2022-08-13	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01
	4771762765	2021-06-09	2021-06-09	2022-06-07	onewe.live.com	*.onewe.live.com	C=US, O=Microsoft Corporation, CN=Microsoft RSA TLS CA 01

ENG US WiFi 14:49 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.

Magnet AXIOM Examine v6.7.1.33408 - GBC-22

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

FILTERS Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

EVIDENCE (4)

Host	Creation Date	Month	2nd Month	Hits	Artifact	Artifact Type	Source
.staggeringbeauty.com				147998	Chrome Cookies	Google Analytics First Visit Cookies	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS)
.eelslap.com				147997	Chrome Cookies	Google Analytics First Visit Cookies	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS)
.heeeeeeyy.com				148175	Chrome Cookies	Google Analytics First Visit Cookies	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS)
.oooooooooo.com				148176	Chrome Cookies	Google Analytics First Visit Cookies	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS)

ALL EVIDENCE 740,185 Refined Results 1,046

- Classified 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

Time zone UTC-5:00

ENG US WiFi 1:51 AM 2022-11-15

Subdomains (2) ⓘ

Subdomain	Detections	Type	Name
heeeeeeeeey.com	0 / 95	151.101.1.195	151.101.65.195
www.heeeeeeeeey.com	0 / 95	151.101.1.195	151.101.65.195

Communicating Files (3) ⓘ

Scanned	Detections	Type	Name
2020-09-15	48 / 66	Win32 EXE	iel
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	D3STROY3R.exe
2022-09-10	63 / 70	Win32 EXE	dcc661ff0c98b62ae63fe057be3c18ce939690ea7421e27820e7166cc75e5f7
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?UmVmboKArmdwa5leGU=?-
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	08da02846cb4cd0f1a715dc6a29e7db79b4b9f6f37336703fa7fa574280912a

Historical Whois Lookups (5) ⓘ

Last Updated	Registrar

Registerant

5:07 PM  
ENG US  
2022-11-14

Subdomains (1) ⓘ

Subdomain	Detections	Type	Name
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) ⓘ

Last Updated	Registrar

Registerant

5:08 PM  
ENG US  
2022-11-14

Screenshot of a web browser showing a search result for "hooooooooo.com" on virustotal.com. The results include:

- Subdomains (2)**: hooooooooo.com (0 / 95), www.hooooooooo.com (0 / 95).
- Communicating Files (1)**: Scanned 2020-09-15, Detections 48 / 66, Type Win32 EXE, Name lel.
- Files Referring (13)**: A list of files from various dates, including D3STR0Y3R.exe, minecract cracked by peoroy.exe, and US-2018-11-08 01-21-587DBB2B0-372D679B-BE7F2A2E-224DB1E1-2BA7C8F2E-v32.zip.
- Historical Whois Lookups (5)**: Last Updated 2022-05-29, Registrar Google LLC.

Bottom right corner shows: ENG US 5:10 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.

Screenshot of Magnet AXIOM Examine v6.7.1.33408 - GBC-22 interface showing evidence artifacts.

**EVIDENCE (120)**

Search Term	URL	Date/Time	Date
volatility standalone	https://www.google.com/search?q=volatility+stand...	2022-01-20 2:10:41 PM	
volatility standalone	https://www.google.com/search?q=volatility+stand...	2022-01-20 2:10:41 PM	
volatility standalone	https://www.google.com/search?q=volatility+stand...	2022-01-20 2:10:41 PM	
volatility standalone	https://www.google.com/search?q=volatility+stand...	2022-01-20 2:10:41 PM	
random website generator	https://www.google.com/search?q=random+websit...	2022-01-20 2:12:44 PM	
random website generator	https://www.google.com/search?q=random+websit...	2022-01-20 2:12:44 PM	
random website generator	https://www.google.com/search?q=random+websit...	2022-01-20 2:12:45 PM	
random website generator	https://www.google.com/search?q=random+websit...	2022-01-20 2:12:45 PM	
fakenamegenerator	https://www.google.com/search?q=fakenamegener...	2022-01-20 2:13:45 PM	
fakenamegenerator	https://www.google.com/search?q=fakenamegener...	2022-01-20 2:13:45 PM	
fakenamegenerator	https://www.google.com/search?q=fakenamegener...	2022-01-20 2:13:46 PM	
fakenamegenerator	https://www.google.com/search?q=fakenamegener...	2022-01-20 2:13:46 PM	
magic number list	https://www.google.com/search?q=magic+number...	2022-10-15 9:34:46 AM	
\$(CURRENT_WORD)	https://www.google.com/search?q=\$(CURRENT_WO...		
volatility standalone	https://www.google.com/search?q=volatility+stand...		
random website generator	https://www.google.com/search?q=random+websit...		
fakenamegenerator	https://www.google.com/search?q=fakenamegener...		
fakenamegenerator	https://www.google.com/search?q=fakenamegener...		
random website generator	https://www.google.com/search?q=random+websit...		
random website generator	https://www.google.com/search?q=random+websit...		
random website generator	https://www.google.com/search?q=random+websit...		

**magic number list**

**T433-Student-W10-09af4a2c.vmem**

**DETAILS**

**ARTIFACT INFORMATION**

Search Term: magic number list  
 URL: https://www.google.com/search?q=magic+number+list&rlz=1C1CHBF\_enCA989CA989&qq=magic+number+list&ll=chrome..69157j0i2213013j0i1521230j0i2130j0i1012130j0i1521230j0i3902.5081j0j7&so=urceid=chrome&ie=UTF-8  
 Date/Time: 2022-10-15 9:34:46 AM  
 Original Search Query: magic number list  
 Web Page Title: magic number list - Google Search  
 Artifact type: Google Searches  
 Item ID: 159060  
 Original artifact: WebKit Browser Web History (Carved)

**EVIDENCE INFORMATION**

Source: T433-Student-W10-09af4a2c.vmem  
 Recovery method:  
 Deleted source:  
 Location: File Offset 1639651077

Time zone: UTC-5:00

ENG US 2:06 AM 2022-11-15

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?

The screenshot shows the Magnet AXIOM Examine interface with the following details:

- Top Bar:** 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.
- EVIDENCE (49):**
  - Left Panel:** Facebook URLs (13), Google Analytics First Visit Cookies (4), Google Analytics Referral Cookies (4), Google Analytics Session Cookies (4), Google Searches (120), Identifiers - Device (70), Identifiers - People (211), Locally Accessed Files and Folders (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).
  - Table Headers:** Page Title, URL, Created Date..., Dom...
  - Table Data:** A list of 49 entries, mostly from Google, including Microsoft Edge, Google Chrome, Doubleclick.net, Google.com, Novirusthanks.org, Sumologic.com, and various Twitter and Google search results.
- Bottom Status Bar:** Time zone UTC-5:00, ENG US, 2:25 AM, 2022-11-15.

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.

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

Type a search term... GO ADVANCED

**EVIDENCE (113)**

Column view

	Site...	URL	Date/Time	Date...	Artifact
	Twitter	1/0/_dk_https://eelslap.com http://eelslap.com http://...	2022-01-20 2:13:40 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://eelslap.com http://eelslap.com https://...	2022-01-20 2:13:40 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://eelslap.com https://twitter.com https://...	2022-01-20 2:13:40 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://heeeeeee...	2022-01-20 2:14:39 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://heeeeeee...	2022-01-20 2:14:39 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:12:55 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:12:57 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:18 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:34 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:06 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:11 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:50 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:12:59 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:59 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:14 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:36 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:42 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:26 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:12:53 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:22 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:27 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:32 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:15 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:13:02 PM		Chrome Cache Records
	Twitter	1/0/_dk_https://heeeeeey.com https://twitter.com...	2022-01-20 2:14:23 PM		Chrome Cache Records

**Twitter**

T433-Student-W10.vmdk

**DETAILS**

**ARTIFACT INFORMATION**

Site Name Twitter  
URL 1/0/\_dk\_https://heeeeeey.com https://twitter.com/com/settings?  
session\_id=a15b17e1d52f6bc9aeddac65b01a4c17917d4e  
Date/Time 2022-01-20 2:14:23 PM  
Artifact type Social Media URLs  
Item ID 148726  
Original artifact Chrome Cache Records

**EVIDENCE INFORMATION**

Source T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Users\T433-COMP4071\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache\_Data\data\_1  
Recovery method  
Deleted source  
Location File Offset 346880

Time zone UTC-5:00

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

Type a search term... GO ADVANCED

**EVIDENCE (205)**

Column view

	Host	Name	Value	Accessed Date/...	Created Date/T...	Expir
	.technoratimedia.com	tads_zora		2022-01-20 2:13:54 PM	2022-01-20 2:13:54 PM	2027-C
	.360yield.com	tuuid		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2022-C
	.betweendifigital.com	tuuid		2022-01-20 2:13:52 PM	2022-01-20 2:13:52 PM	2023-C
	.bidswitch.net	tuuid		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2023-C
	.mfadsvr.com	tuuid		2022-01-20 2:13:49 PM	2022-01-20 2:13:48 PM	2024-C
	.360yield.com	tuuid_lu		2022-01-20 2:13:49 PM	2022-01-20 2:13:48 PM	2022-C
	.bidswitch.net	tuuid_lu		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2023-C
	.mfadsvr.com	tuuid_lu		2022-01-20 2:13:49 PM	2022-01-20 2:13:49 PM	2024-C
	.cnree.com	uid		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2023-C
	.turn.com	uid		2022-01-20 2:13:51 PM	2022-01-20 2:13:51 PM	2022-C
	.tyni.com	uid		2022-01-20 2:13:52 PM	2022-01-20 2:13:52 PM	2023-C
	.openx.net	univ_id		2022-01-20 2:13:51 PM	2022-01-20 2:13:51 PM	2022-C
	.betweendifigital.com	ut		2022-01-20 2:13:52 PM	2022-01-20 2:13:52 PM	2023-C
	.mathtag.com	uuid		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2023-C
	.tribalfusion.com	ANON_ID		2022-01-20 2:13:56 PM	2022-01-20 2:13:56 PM	2022-C
	.media.net	visitor-id		2022-01-20 2:13:48 PM	2022-01-20 2:13:48 PM	2023-C
	.deepintent.com	CDIUSER		2022-01-20 2:13:54 PM	2022-01-20 2:13:54 PM	2023-C
	.dotomi.com	DotomiTest		2022-01-20 2:13:57 PM	2022-01-20 2:13:57 PM	2022-C
	.pubmatic.com	PUBMDCID		2022-01-20 2:13:57 PM	2022-01-20 2:13:51 PM	2022-C
	.pubmatic.com	PugT		2022-01-20 2:13:57 PM	2022-01-20 2:13:57 PM	2022-C
	.pubmatic.com	SPugT		2022-01-20 2:13:59 PM	2022-01-20 2:13:59 PM	2022-C
	.pubmatic.com	SyncRTB3		2022-01-20 2:13:56 PM	2022-01-20 2:13:56 PM	2022-C
	.adsrvr.org	TDCPM		2022-01-20 2:13:56 PM	2022-01-20 2:13:56 PM	2023-C
	beacon.lynx.cognitivlabs.com	UID		2022-01-20 2:13:56 PM	2022-01-20 2:13:56 PM	2023-C
	.adsrvr.org	TDID		2022-01-20 2:13:56 PM	2022-01-20 2:13:48 PM	2023-C

**.technoratimedia.com**

T433-Student-W10.vmdk

**DETAILS**

**ARTIFACT INFORMATION**

Host .technoratimedia.com  
Name tads\_zora  
Accessed Date/Time 2022-01-20 2:13:54 PM  
Created Date/Time 2022-01-20 2:13:54 PM  
Expiration Date/Time 2027-01-19 2:13:54 PM  
Path /  
Artifact type Chrome Cookies  
Item ID 148079

**EVIDENCE INFORMATION**

Source T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Users\T433-COMP4071\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies  
Recovery method Parsing  
Deleted source  
Location Table: cookies(rowid: 180)  
Evidence number T433-Student-W10.vmdk

Time zone UTC-5:00

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 Type a search term... GO ADVANCED

**EVIDENCE (205)**

**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

Host	Name	Value	Accessed Date/Time	Created Date/Time	Expiration Date/Time
.aiwaysjudgeabookbyitscov...	_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
.aiwaysjudgeabookbyitscov...	_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
<b>.bidr.io</b>	<b>bito</b>		2022-01-20 2:13:54 PM	2022-01-20 2:13:54 PM	2023-02-19 9:13:54 AM
.bidr.io	bitolsSecure		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
.cappier.net	_uid		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	CMPSS		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 2:14:41 PM	2024-01-20 2:14:41 PM
.checkboxrace.com	_ga_RXJX4V8YBQ		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 .bidr.io
- Name bito
- Accessed Date/Time 2022-01-20 2:13:54 PM
- Created Date/Time 2022-01-20 2:13:54 PM
- Expiration Date/Time 2023-02-19 9:13:54 AM
- Path /
- Artifact type File
- Item ID 1480

**EVIDENCE INFORMATION**

- Source T433-Student-W10.vmdk
- Recovery method Pars
- Deleted source

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 Type a search term... GO ADVANCED

**EVIDENCE (205)**

**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

Host	Name	Value	Accessed Date/Time	Created Date/Time	Expiration Date/Time
.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
.piplio.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
.piplio.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
<b>.rubiconproject.com</b>	<b>khaos</b>		2022-01-20 2:13:54 PM	2022-01-20 2:13:52 PM	2023-01-20 2:13:54 PM
.ljjit.com	ljj_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
.piplio.com	nnls		2022-01-20 2:13:51 PM	2022-01-20 2:13:51 PM	2023-02-21 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
.piplio.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

.rubiconproject.com

**T433-Student-W10.vmdk**

**DETAILS**

**ARTIFACT INFORMATION**

- Host .rubiconproject.com
- Name khaos
- Accessed Date/Time 2022-01-20 2:13:54 PM
- Created Date/Time 2022-01-20 2:13:54 PM
- Expiration Date/Time 2022-02-19 2:13:54 PM
- Path /
- Artifact type File
- Item ID 1480

**EVIDENCE INFORMATION**

- Source T433-Student-W10.vmdk
- Recovery method Pars
- Deleted source

Time zone UTC-5:00

ENG US 3:21 AM 2022-11-15

Getting Started YouTube Reddit Blackboard Google Drive Home New Tab

bidr.io

Communicating Files (18) ⓘ

Scanned	Detections	Type	Name
2020-11-10	40 / 70	Win32 EXE	Facebook Videos Player.exe
2020-11-10	44 / 72	Win32 EXE	Facebook Videos Player.exe
2020-11-13	44 / 72	Win32 EXE	6660bb8f295fb64939275a2c8560b641a49c7ebaa72df65edef1b145db89e1d
2021-02-22	8 / 69	Win32 EXE	remote.exe
2021-02-20	37 / 60	RAR	60483801
2020-11-25	35 / 61	RAR	60483801
2022-11-15	0 / 61	Network capture	dns2 pcap
2022-01-19	51 / 69	Win32 EXE	427ad5e28dd26fea1865ca90d05ea191 virus
2022-09-26	60 / 72	Win32 EXE	0bb17ee11311301375c5c46039df5e80a08adc76
2022-11-13	0 / 63	PDF	Freelancemom_Business_Plan_Development.pdf

• • •

Files Referring (49) ⓘ

Scanned	Detections	Type	Name
2019-06-27	63 / 72	Win32 EXE	Win
2019-12-29	0 / 61	Mozilla Firefox Extension	uBlock0@raymondhill.net.xpi
2019-06-21	51 / 70	Win32 EXE	1666b5354f45bb2d64b0e42919a49277c6b7ae1bfa08ac87d3ca999d9f2e33ab
2019-06-16	56 / 70	Win32 EXE	TJproMain
2019-07-06	4 / 72	Win32 EXE	WS0AF75750.DAT
2022-10-29	5 / 63	Win32 EXE	HitmanPro37
2022-03-10	10 / 67	Win32 EXE	HitmanPro_x64.exe
2019-06-04	53 / 70	Win32 EXE	f8385c3411fd1566621ce505384bf2d virus
2022-09-13	17 / 66	Win32 EXE	wsc_x9_free.exe
2021-07-29	12 / 68	Win32 EXE	HitmanPro.exe

• • •

9:51 PM  
ENG US  
2022-11-14

Getting Started YouTube Reddit Blackboard Google Drive Home New Tab

rubiconproject.com

Historical Whois Lookups (14) ⓘ

Scanned	Detections	Type	Name
2022-07-20	1 / 59	Windows shortcut	World of Warships.lnk
2022-05-23	41 / 67	Win32 EXE	d10cd916ff4351f8e6883b14d3f78492.virus
2022-06-19	18 / 67	Win32 EXE	_cache_%SAMPLENAME%
2021-01-11	60 / 71	Win32 EXE	Downloader
2022-10-31	2 / 62	Windows shortcut	World of Warships.lnk
2022-07-05	3 / 60	Win32 EXE	EdgeIEMode_0406.exe
2021-12-14	0 / 58	Windows shortcut	MyPlayCity Games.lnk
2022-10-06	0 / 62	Windows shortcut	00544ae69c4597118c1ac7d14040b01e6248989d29df0339ce6fde115f1609
2022-07-10	0 / 58	Windows shortcut	MyPlayCity Games.lnk
2022-09-21	0 / 60	Windows shortcut	00635e8799a8ca1eca61e0db5c2cdc79c282c06239181b9af0bac9161fb1e5d9

• • •

Files Referring (200) ⓘ

Scanned	Detections	Type	Name
2022-11-11	2 / 67	Win32 EXE	Hyena.exe
2022-10-25	7 / 72	Win32 EXE	Cabri II Plus
2022-08-25	40 / 70	Win32 DLL	004989.dll
2022-07-15	5 / 59	unknown	7684673183c853fa5f5745489a00fc38207f6e1d694a3e4a994a653caf815e4
2022-07-12	1 / 59	Android	897a8ecb3ecf1e0978ec7f2ba4e8be0a7d0bcd4e516b04db12123650483518b2
2022-06-20	1 / 57	Android	c32f0c909d11002a9159b6eb4b16ec94ff6029b922fd7d74f7201c558a8f2a
2022-06-17	1 / 57	Android	e333711a30add1656047155218a8caab05f93689fba441d0ce45b0f7b0f96fd
2022-06-16	1 / 57	Android	ceb5afa86d54d51b746b6c75098107a0c68057ad941c829deb7eb6979fed2d7b
2022-06-09	1 / 56	Email	Tarki_Kankaille_pilkka_vankeustuomio_satojen_tuhansien_eurojen_huajaikista.pdf
2022-05-13	17 / 66	Win32 EXE	6384a037ecc5401f567860078978a0d18fd77339674338251fe0ea90ca80200d

• • •

9:51 PM  
ENG US  
2022-11-14

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

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 Type a search term... GO ADVANCED

**Artifacts**

**EVIDENCE (58,688)**

	URL	User...	Artifact type	Source
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://report-example.test/test			Potential Browser Activity	T433-Student-W10-09af4a2c.vmem
http://safebrowsing.googleusercontent.com/safebro...			Potential Browser Activity	T433-Student-W10-09af4a2c.vmem
<b>http://sandsprite.com</b>			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://sandsprite.com/blogs/index.php?uid=7&pid=...			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://sandsprite.com/iDef/SysAnalyzer/			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/ImageObject			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/ImageObject			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/LocalBusiness			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/LocalBusiness			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/Person			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/Person			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/Product			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/Text			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/Text			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
http://schema.org/TouristAttraction			Potential Browser Activity	T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)

**http://...**

**T433-Student-W10.vmdk**

**DETAILS**

**ARTIFACT INFORMATION**

- URL http://
- Artifact type Pot
- Item ID 8224

**EVIDENCE INFORMATION**

- Source T433-S Partition NTFS, PDFS, PDFS
- Recovery method Carving
- Deleted source
- Location File Off
- Evidence number T433-S

Time zone UTC-5:00

https://www.virustotal.com/gui/url/c14017f0c563d581619e716b0635ff7b21234fadec2a563fd0983f52f3e0c73e

Getting Started YouTube Reddit Blackboard Google Drive Home New Tab

http://sandsprite.com/

① 1 security vendor flagged this URL as malicious

http://sandsprite.com/ sand sprite.com 200 Status 2022-11-11 14:35:56 UTC 3 days ago

DETECTION DETAILS COMMUNITY

Community Score 1 / 90

Security Vendors' Analysis

Vendor	Result	Details
Heimdal Security	Malicious	Abusix Clean
Acronis	Clean	ADMINUSLabs Clean
AICC (MONITORAPP)	Clean	AlienVault Clean
alphaMountain.ai	Clean	Anty-AVL Clean
Artists Against 419	Clean	Avira Clean
BADWARE.INFO	Clean	benkow.cc Clean
Bfore Ai PreCrime	Clean	BitDefender Clean
BlockList	Clean	Blueliv Clean
Certego	Clean	Chong Lua Dao Clean
CINS Army	Clean	CMC Threat Intelligence Clean

2:56 AM 2022-11-15

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

**FILTERS**: Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists. **CLEAR FILTERS**: sandsprite **GO ADVANCED**

**Artifacts**: MATCHING RESULTS (12 of 740,185)

	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/Def/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

**DETAILS**: packages.csv  
**T433-Student-W10.vmdk**

**ARTIFACT INFORMATION**

- File Name: packages.csv
- Last Modified Date/Time: 2021-10-22 10:13:52 PM
- Size (Bytes): 26850
- SHA1 Hash: 40d154a6ec9a5f0a72e22928403b8783d87e8284
- MDS Hash: 0447193bd23c7e0f9bdbba1645a5e701f
- 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\bda187f3flare-vm-master.zip\flare-vm-master\packages.csv
- Recovery method: Parsing
- Deleted source
- Location: n/a
- Evidence number: T433-Student-W10.vmdk

Time zone: UTC-5:00

Magnet AXIOM Examine v6.7.1.33408 - GBC-22

**FILTERS**: Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists. **CLEAR FILTERS**: Type a search term... **GO ADVANCED**

**Artifacts**: MATCHING RESULTS (12 of 740,185)

	Item
	packages.csv
	http://sandsprite.com/blogs/index.php?uid=7&pid=57
	http://sandsprite.com
	http://sandsprite.com/Def/SysAnalyzer/
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	4100
	Readme.txt
	Readme.txt

**EVIDENCE INFORMATION**

```

Host Application = PowerShell\Windows\Microsoft\Windows\PowerShell\4Operational.exe
bypass -command Import-Module 'C:\ProgramData\boxstarter\Boxstarter.Bootstrapper.ps1';Invoke-Boxstarter -RebootOk -NoPassword:$True
  Engine Version = 5.1.19041.906
  Runspace ID = d36cef6-8811-4081-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-C0T433-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

Source: T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell\4Operational.evtx

Recovery method: Parsing

Time zone: UTC-5:00

The screenshot shows a Microsoft Edge browser window with the URL <https://www.myeventlog.com/search/show/976>. The page title is "MyEventlog". On the left, there is a "Event Search" form with fields for Event ID, Source, Category, and Message, and a "Search" button. On the right, the event details are displayed:

**Event submitted by Event Log Doctor**

**Event ID:** 4100  
**Source:** Microsoft-Windows-PowerShell  
**Category:** Executing Pipeline  
**Log:** Microsoft-Windows-PowerShell/Operational

**Message:**

```
Error Message = File C:\Users\wizard\test.ps1 cannot be loaded. The file C:\Users\wizard\test.ps1 is not digitally signed. You cannot run this script on the current system. For more information about running scripts and setting execution policy, see about_Execution_Policies at http://go.microsoft.com/fwlink/?LinkId=135170.
Fully Qualified Error ID = UnauthorizedAccess
Recommended Action =
Context:
Severity = Warning
Host Name = ConsoleHost
Host Version = 5.1.14393.1944
Host ID = babd41a2-db0f-45d0-ac50-e34b71dd9ac0
Host Application = powershell .\test.ps1
Engine Version = 5.1.14393.1944
Runspace ID = 0155307c-603a-440d-a22c-85b5c9cbffff
Pipeline ID = 1
Command Name =
Command Type =
Script Name =
Command Path =
Sequence Number = 15
User = DOMAIN\user
Connected User =
Shell ID = Microsoft.PowerShell
User Data:
```

At the bottom of the browser window, the status bar shows: ENG US 3:16 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 screenshot shows a Microsoft Edge browser window with the URL <https://www.virustotal.com/gui/domain/w3.org>. The page title is "w3.org". The main content area displays:

**1 security vendor flagged this domain as malicious**

w3.org (top-1K)

Registrar: Gandi SAS | Creation Date: 28 years ago | Last Updated: 5 months ago

Community Score: 1 / 95

Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (12+). The DETECTION tab is selected, showing the "Security Vendors' Analysis" table:

Security Vendor	Analysis	Comments	
ESTsecurity	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Anti-AVL	Clean
Armis	Clean	Avira	Clean
BADWARE INFO	Clean	Baidu-International	Clean
benkow.cc	Clean	Bfore Ai PreCrime	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Luu Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean

At the bottom of the browser window, the status bar shows: ENG US 2:59 AM 2022-11-15

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.

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

Type a search term... GO ADVANCED

**EVIDENCE (18)**

	URL	Date Visited Dat...	Title	Type...
Edge Chromium Cookies	63	https://go.microsoft.com/fwlink/?linkid=2132465	2022-01-20 12:04:22 PM	Microsoft Edge
Edge Chromium Downloads	2	https://microsofetedgewelcome.microsoft.com/en-us...	2022-01-20 12:04:22 PM	Microsoft Edge
Edge Chromium Favicons	34	https://microsofetedgewelcome.microsoft.com/mb02	2022-01-20 12:04:22 PM	Microsoft Edge
Edge Chromium Keywo...	2	https://microsofetedgewelcome.microsoft.com/en-us...	2022-01-20 12:04:23 PM	Microsoft Edge
Edge Chromium Shortcuts	1	https://microsofetedgewelcome.microsoft.com/en-us...	2022-01-20 12:04:23 PM	Microsoft Edge
Edge Chromium Web History	14	https://microsofetedgewelcome.microsoft.com/en-us...	2022-01-20 12:04:23 PM	Microsoft Edge
Edge Chromium Web Visits	18	https://www.bing.com/search?query=chrome&cvid=4fd...	2022-01-20 12:05:11 PM	https://www.bing.com/aclick?id=e8kRgfdqjEvBxrkWV...
Edge/Internet Explor...	141	https://www.bing.com/aclick?id=e8kRgfdqjEvBxrkWV...	2022-01-20 12:05:14 PM	https://www.bing.com/aclick?id=e8kRgfdqjEvBxrkWV...
Edge/Internet Explorer 10...	18	https://clickserve.dartsearch.net/link/click?lid=43700...	2022-01-20 12:05:15 PM	Google Chrome - Download the Fast, Secure Browse...
Edge/Internet Explorer 10...	65	https://ad.doubleclick.net/ddm/clk/297066946;1241...	2022-01-20 12:05:15 PM	Google Chrome - Download the Fast, Secure Browse...
Edge/Internet Explorer 10...	3	https://www.google.ca/chrome/?brand=CHBF&bran...	2022-01-20 12:05:15 PM	Google Chrome - Download the Fast, Secure Browse...
Edge/Internet Explorer 10...	63	https://www.bing.com/search?q=7zip&qs=n&form...	2022-01-20 12:05:18 PM	https://www.bing.com/newtabredir?url=https%3A%
Internet Explorer Favorites	26	https://www.bing.com/search?query=chrome&cvid=4fd...	2022-01-20 12:05:20 PM	0
Internet Explorer Typed URLs	4	https://www.bing.com/search?query=7zip&qs=n&form...	2022-01-20 12:05:20 PM	0
Potential Brows...	58,688	https://www.bing.com/newtabredir?url=https%3A%	2022-01-20 12:05:20 PM	0
Safari History	8	http://www.novirusthanks.org/post-install/?program...	2022-01-20 1:00:43 PM	Application Installed   NoVirusThanks
WebKit Browser W...	155	https://www.novirusthanks.org/post-install/?program...	2022-01-20 1:00:43 PM	Application Installed   NoVirusThanks

**COMMUNICATION 16**

**MEDIA 52,457**

**EMAIL & CALENDAR 224**

**DOCUMENTS 2,925**

**ARTIFACT INFORMATION**

URL https://clickserve.dartsearch.net/link/click?lid=437000660893132111&ds\_a\_kwrid=58700007349494178&ds\_a\_cid=405525800&ds\_a\_caid=14353474773&ds\_a\_agid=12919022323&ds\_a\_id=kwd-11095292051&ds\_x\_axid=83700007063098147&ds\_x\_adxtype=18&ds\_a\_cid=4055258000&ds\_a\_fld=1225476951178&ds\_e\_agid=80333188998504&ds\_e\_target\_id=kwd-8033315603538&loc=32&rd=8&e\_network=o&ds\_url.v=2&ds\_dest.url=https://www.google.ca/chrome/?brand=CHBF&brand=UEA&dgclid=5f53fd4083d128fe549c3d9e7bab8&gclid=rc-3p.ds&ds\_id=4370006089311211&utm\_source=bing&utm\_medium=cpc&utm\_campaign=1011197%20%7C20Chrome%20Win10%20%7C20DR%20%7C20ES501%20%7C%20NA%20%7C20CA%20%7C20en%20%7C20desk%20%7C20SEM%20%7C20BKWS%20-%20%7C20KWS%20-%20%7C20%

Time zone UTC-5:00

ENG US 9:54 PM 2022-11-14

clickserve.dartsearch.net

Communicating Files (1.01 K) ○

Scanned	Detections	Type	Name
2019-08-18	17 / 58	Android	181_com.streaming.sexymen.hot.video.hd.watch.free.movies.hdv boy man.tv.online.music.workout_release.apk
2021-11-17	0 / 51	Android	com.beidentity.shop30.apk
2022-07-14	0 / 60	PDF	Kawasaki-Boss-175-Engine-Parts-Catalog.pdf
2020-11-06	53 / 71	Win32 EXE	0044d6350b632842aa1a02dcba962a3720e60278d05e918be607164277c3f9e09
2022-03-26	19 / 62	Android	fd15ed8c38659093c5ddd2471dbc9921edf7bbe510ac851a55666a96b6a397_adv.apk
2022-08-12	0 / 64	Android	01587adeb921d03c46fb605cdfc8d8ed912d151baa7c5bb30e060a00e9277bb
2019-08-06	0 / 61	Android	0195ecc897ed79611b9b53cc9b8a08225ce8f28f75709c241c7b27116122cf40 vir
2021-02-16	0 / 56	Android	22E29DB65BA135498D35298FE2AF02BD
2021-01-13	30 / 61	Android	bd2ebbb32c557d774b1005058d9ec3f9f.apk
2019-03-31	0 / 58	Android	com.cindylarm.apk

Files Referring (200) ○

Scanned	Detections	Type	Name
2022-11-12	6 / 72	Win32 EXE	be14a2fd952fa400570695737bd138bc.virus
2022-10-05	61 / 71	Win32 EXE	c5a6cd8bf5890551a7f40398179aece.virus
2022-10-02	8 / 59	Win32 EXE	PDF To Word
2022-09-24	2 / 62	ZIP	US_2019_01_18_02_51_402C50D67_7E544B57.zip
2022-09-14	1 / 54	Email	method.rar dosyasini indir - download
2022-09-12	50 / 70	Win32 EXE	f78de1fabbb141ad229f4275d3e1d9314.virus
2022-08-30	2 / 68	Win32 DLL	RAM_CARVING022996.dll4
2022-08-29	2 / 59	unknown	148a11534f957df947b49da486c09c6ae98d1e604a7c8787fc74c7132bf9e9
2022-08-25	53 / 71	Win32 EXE	Lentract0.exe
2022-08-16	1 / 60	Email	Asphalt 8 Airborne mod by 0880.zip - Safefileku

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.

Magnet AXIOM Examine v6.7.1.33408 - GBC-22

**FILTERS**

- Evidence
- Artifacts
- Content types
- Date and time
- Tags and comments
- Profiles
- Partial results
- Keyword lists

**CLEAR FILTERS** Type a search term... GO ADVANCED

**Artifacts**

**MATCHING RESULTS (10 of 740,185)**

Item ID	Item	Artifact type
123114	Mail Delivery Subsystem <MAILER-DAEMON@zinfandel.lacita.com>	Identifiers - People
123117	Mail Delivery Subsystem <MAILER-DAEMON@zinfandel.lacita.com>	Identifiers - People
123958	linuxuser@www.linux.org.uk	EML(X) Files
123112	<linuxuser-admin@www.linux.org.uk>	EML(X) Files
123116	linuxuser@www.linux.org.uk	EML(X) Files
123949	<linuxuser-admin@www.linux.org.uk>	EML(X) Files
123111	<linuxuser-admin@www.linux.org.uk>	MBOX Emails
123946	<linuxuser-admin@www.linux.org.uk>	MBOX Emails
123011	msg_25.txt	Text Documents
123864	msg_25.txt	Text Documents

**linuxuser@www.linux.org.uk**

**T433-Student-W10.vmdk**

**PREVIEW**

**FIND**

**From:** Daniel James <daniel@linuxuser.co.uk>  
**Sent:** 2001-04-06 11:03:39 AM  
**To:** linuxuser@www.linux.org.uk  
**Subject:** [LinuxUser] bulletin no. 45

--JAB03225.986577786/zinfandel.lacita.com--

**DETAILS**

**ARTIFACT INFORMATION**

To linuxuser@www.linux.org.uk  
From Daniel James <daniel@linuxuser.co.uk>  
Date/Time 2001-04-06 11:03:39 AM  
Subject [LinuxUser] bulletin no. 45  
Body --JAB03225.986577786/zinfandel.lacita.com--

Time zone UTC-5:00

https://www.virustotal.com/gui/domain/zinfandel.lacita.com/relations

Getting Started YouTube Reddit Blackboard Google Drive Home New Tab

zinfandel.lacita.com

www.lacita.com 0 / 94 104.28.18.89 104.28.19.89

Communicating Files (158.82 K)

Scanned	Detections	Type	Name
2022-10-10	68 / 71	Win32 EXE	lsass.exe
2019-06-03	60 / 74	Win32 EXE	000031163d35bc67a473901b1c2bfd52d43ea012f9119e9fc92cb4930027be7a
2022-10-13	66 / 72	Win32 EXE	sys32.exe
2019-10-19	51 / 68	Win32 EXE	.
2022-10-13	66 / 72	Win32 EXE	sys32.exe
2022-07-29	63 / 71	Win32 EXE	Harry Potter ShareReactor.com
2022-05-23	55 / 68	Win32 EXE	tserv.exe
2022-05-21	60 / 68	Win32 EXE	sys32.exe
2022-05-21	61 / 67	Win32 EXE	sys32.exe
2019-11-15	60 / 71	Win32 EXE	40748e65abec590f018c4f5ea28d594.virus
2019-05-01	59 / 71	Win32 EXE	c00edfa57d8b328ed190bf0956e4fa31.virus
2022-05-23	62 / 68	Win32 EXE	0b61f55ad6506737d00b23470bd75c19e.virus
2022-05-22	62 / 67	Win32 EXE	lsass.exe
2014-09-12	51 / 55	Win32 EXE	0002CAB9B478E0579F21D8857099346441DE1ABB3F8A3818E1989E87BC9DFE0
2022-05-22	61 / 68	Win32 EXE	Winamp 5.0 (en).Crack.com
2020-03-22	66 / 72	Win32 EXE	d16e89c3ef0ca5acc31360f9b01590.virus
2021-05-17	55 / 69	Win32 EXE	84cc677811f77b68de1b1854dd2ef034.virus
2021-10-09	58 / 67	Win32 EXE	lsass.exe
2020-06-05	60 / 72	Win32 EXE	0003d224374db291101b9da57e8287fd4f52388a2db0c19e81b89620ec93a920
2020-04-12	67 / 73	Win32 EXE	000410852b05b745c557894fa9ea8a3f986852c6d22c8a3a74a7ec4a4d8c80
2022-06-17	56 / 66	Win32 EXE	00054c8949e17df0b084b1612259b8b7156e9c5bc81c1563d9864de8483ccfce
2020-04-21	59 / 70	Win32 EXE	b03663e3e93d563890fc79f7198c7dcc.virus
2022-02-09	52 / 65	Win32 EXE	myfile.exe
2019-02-27	50 / 69	Win32 EXE	b51200b8072b3dfc1b03632c14a4039e.virus
2019-04-20	54 / 69	Win32 EXE	00063728a77af0c4493452dce72a81bc466ff8e73fa206fa3757a338e8f14f3

8:01 PM ENG US 2022-11-14 2

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.

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 Type a search term... GO ADVANCED

**EVIDENCE (10)**

	From
James Sumners <james.sumners@gmail.com>	
luxuser-admin@www.linux.org.uk>	Mail Delivery Subsystem <MAILER-DAEMON@zinfra...
ebmaster@python.org>	MAILER DAEMON <>
luxuser-admin@www.linux.org.uk>	Mail Delivery Subsystem <MAILER-DAEMON@zinfra...
ebmaster@python.org>	MAILER DAEMON <>
> <bob@gov>	Alice <alice@edu>
> <bob@gov>	Ted <ted@com>
e <alice@edu>	Bob <bob@gov>
<ted@com>	Bob <bob@gov>
> <bob@gov>, Carol <carol@gov>, Alice <alice...	Ted <ted@com>

**PREVIEW**

**FIND**

Subject: Banned file: auto\_mail.python.bat in mail from you

**BANNED FILENAME ALERT**

Your message to: xxxxxxxx@dot.ca.gov,xxxxxxxxxxxxxx@dot.ca.gov,xxxxxxxxxxxx@dot.ca.gov,xxx@dot.ca.gov,

**DETAILS**

**ARTIFACT INFORMATION**

To <webmaster@python.org>  
 From MAILER DAEMON <>  
 Date/Time 2004-11-26 10:41:44 PM  
 Subject Banned file: auto\_mail.python.bat in mail from you  
 Body BANNED FILENAME ALERT

Time zone UTC-5:00

Two instances of attachment zips were also found in emails.

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 Type a search term... GO ADVANCED

**EVIDENCE (12)**

	File N...	Artif...	Artif...	Subject	File...	File...
text.gz	EML(X) Files	27305		Sample message	.gz	60
text.gz	EML(X) Files	28697		Sample message	.gz	60
dingusfish.gif	EML(X) Files	123088		Here is your dingus fish	.gif	3512
dingusfish.gif	EML(X) Files	123090		Here is your dingus fish	.gif	3512
wibble.JPG	EML(X) Files	123102			JPG	272
wibble2.JPG	EML(X) Files	123102			JPG	317
clock.bmp,69c	EML(X) Files	123122		IMAP file test	.bmp,69c	630
dingusfish.gif	EML(X) Files	123943		Here is your dingus fish	.gif	3512
clock.bmp,69c	EML(X) Files	123940		IMAP file test	.bmp,69c	630
dingusfish.gif	EML(X) Files	123959		Here is your dingus fish	.gif	3512
wibble.JPG	EML(X) Files	123963			JPG	272
wibble2.JPG	EML(X) Files	123963			JPG	317

**text.gz**

**T433-Student-W10.vmdk**

**DETAILS**

**ARTIFACT INFORMATION**

File Name text.gz  
 Subject Sample message  
 File Extension .gz  
 File Size (Bytes) 60  
 MD5 Hash be840549c9d20a1d0c0d4cc94ab8daa3  
 SHA1 Hash bb8699fd1ce6874a0f9aeab3acb887fb8d8f3bbff  
 To Address(es) gkj@gregorykjohnson.com  
 From Address "Gregory K. Johnson"  
 <gkj@gregorykjohnson.com>  
 Email Timestamp Date/Time 2005-07-13 5:23:11 PM  
 Artifact type Email Attachments  
 Item ID 27348  
 Original artifact EML(X) Files

**EVIDENCE INFORMATION**

Source T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB)\Python27\Lib\test\test\_mailbox.py  
 Recovery method  
 Deleted source  
 Location File Offset 85974  
 Evidence number T433-Student-W10.vmdk

Time zone UTC-5:00

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.

The screenshot shows the Magnet AXIOM interface with the following details:

- File menu:** File, Tools, Process, Help.
- Toolbar:** Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists, Skin tone.
- Search Bar:** Type a search term... GO ADVANCED.
- FILTERS:** Media categorization, Media attributes (VICS).
- EVIDENCE (70):**
  - ALL EVIDENCE:** 740,185
  - REFINED RESULTS:** 1,046
  - WEB RELATED:** 61,356
  - COMMUNICATION:** 16
- Table Headers:** Identifier, Column Name, Artifact, Artif..., Artifact type, Source, Rec.
- Table Data:** Numerous rows of data, including:
  - 192.168.175.128, DHCP IPv4 Address, Network Interfaces (Registry), 38685, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 192.168.152.128, DHCP IPv4 Address, Network Interfaces (Registry), 38698, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - T433-Faculty/Desk-COMP4071, Displayed Computer Name, Operating System Information, 47888, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - VMware Virtual NVMe Disk, Friendly Name, USB Devices, 43612, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - NECMVMWar VMware SATA CD01, Friendly Name, USB Devices, 43605, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - DA4ECC7C4EEC52B5, Full Volume Serial Number, File System Information, 5, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 00:0C:29:A1:2A:7B, MAC Address, LNK Files, 8056, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 00:11:09:07:7E:DD, MAC Address, LNK Files, 11015, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 00:1C:C4:2D:F4:0B, MAC Address, LNK Files, 51896, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 00:0C:29:A1:2A:7B, MAC Address, LNK Files, 155726, Identifiers - Device, T433-Student-W10-09af4a2c.vmem
  - 00:0C:29:91:27:AB, MAC Address, LNK Files, 158994, Identifiers - Device, T433-Student-W10-09af4a2c.vmem
  - 00:11:09:07:7E:DD, MAC Address, LNK Files, 164126, Identifiers - Device, T433-Student-W10-09af4a2c.vmem
  - 00:0C:29:A1:2A:7B, MAC Address, LNK Files, 628276, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 00:11:09:07:7E:DD, MAC Address, LNK Files, 630022, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 00:00:00:00:00:00, MAC Address, LNK Files, 640411, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 45:00:49:00:58:00, MAC Address, LNK Files, 643584, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 90:00:00:00:FF:15, MAC Address, LNK Files, 643598, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 00:1C:C4:2D:F4:0B, MAC Address, LNK Files, 643624, Identifiers - Device, T433-Student-W10-Snapshot1.vmem
  - 7&1ffda586&08:0000, Serial Number, USB Devices, 43609, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 582d152678&08:000000, Serial Number, USB Devices, 43612, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 68:30:c8:a5:f8:08:5, Serial Number, USB Devices, 43608, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 4&1ebe8d07&0:0:00C0, Serial Number, USB Devices, 43610, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 58:2edfd08d8&08:010000, Serial Number, USB Devices, 43605, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 58:2891968b:&0, Serial Number, USB Devices, 43618, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)
  - 58:20be2f2fa8:08:0, Serial Number, USB Devices, 43607, Identifiers - Device, T433-Student-W10.vmdk - Partition 3 (Microsoft NT...)

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.

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 Type a search term... GO ADVANCED

**Artifacts**

**EVIDENCE (70)**

Identifier	Column Name	Artifact	Artif...
DESKTOP-E3Q9F72	Computer	Windows Event Logs	69349
WIN-G5FDGL40A8P	Computer	Windows Event Logs	69347
T433-Student-COMP4071	Computer	Windows Event Logs	69345
T433-FacultyDesk-COMP4071	Computer	Windows Event Logs	69455
T433-FacultyDesk-COMP4071	Computer	Windows Event Logs	155296
DESKTOP-E3Q9F72	Computer	Windows Event Logs	155360
T433-Student-COMP4071	Computer	Windows Event Logs	157126
WIN-G5FDGL40A8P	Computer	Windows Event Logs	157290
T433-FACULTYDES	Computer	Windows Event Logs	162827
WIN-G5FDGL40A8P	Computer	Windows Event Logs	628056
T433-FacultyDesk-COMP4071	Computer	Windows Event Logs	628516
DESKTOP-E3Q9F72	Computer	Windows Event Logs	629753
T433-Student-COMP4071	Computer	Windows Event Logs	631043
T433-FACULTYDES	Computer Name	Operating System Information	47888
DESKTOP-E3Q9F72	Computer Name	Windows Event Logs - Script Events	80995
T433-STUDENT-CO	Computer Name	Windows Event Logs - Script Events	81202
T433-FACULTYDES	Computer Name	Windows Event Logs - Script Events	84424
00:50:56:FF:7A:CF	Default Gateway MAC	Network Profiles	47637
00:50:56:E1:D0:C6	Default Gateway MAC	Network Profiles	47642
0.0.0	DHCP IPv4 Address	Network Interfaces (Registry)	38669
192.168.175.128	DHCP IPv4 Address	Network Interfaces (Registry)	38685
192.168.152.128	DHCP IPv4 Address	Network Interfaces (Registry)	38698
T433-FacultyDesk-COMP4071	Displayed Computer Name	Operating System Information	47888
VMware Virtual NVMe Disk	Friendly Name	USB Devices	43612
NECVMWar VMware SATA CD01	Friendly Name	USB Devices	43605

Time zone UTC-5:00

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 Type a search term... GO ADVANCED

**Artifacts**

**EVIDENCE (476)**

Event ID	Created Date/Ti...	Even...	Event Description Summary	User
4104	2022-01-20 12:39:19 PM	870	Creating Scriptblock text.	
4104	2022-01-20 12:39:35 PM	877	Creating Scriptblock text.	
4104	2022-01-20 12:39:44 PM	885	Creating Scriptblock text.	
5861	2022-01-20 11:58:13 AM	121	WMI Registration of Permanent Event Consumer.	
5860	2022-01-20 11:58:20 AM	123	Remote Desktop Services: Session logoff succeeded. NT AUTHORITY\SYSTEM	
4104	2022-01-20 12:40:07 PM	895	Creating Scriptblock text.	
5861	2022-01-20 12:01:31 PM	131	WMI Registration of Permanent Event Consumer.	
5860	2022-01-20 12:01:38 PM	133	Remote Desktop Services: Session logoff succeeded. NT AUTHORITY\SYSTEM	
4104	2022-01-20 12:40:42 PM	902	Creating Scriptblock text.	
4104	2022-01-20 12:40:44 PM	904	Creating Scriptblock text.	
5861	2022-01-20 12:20:25 PM	167	WMI Registration of Permanent Event Consumer.	
5860	2022-01-20 12:20:44 PM	170	Remote Desktop Services: Session logoff succeeded. NT AUTHORITY\SYSTEM	
4104	2022-01-20 12:40:46 PM	911	Creating Scriptblock text.	
4104	2022-01-20 12:41:55 PM	919	Creating Scriptblock text.	
5861	2022-01-20 12:25:24 PM	185	WMI Registration of Permanent Event Consumer.	
5860	2022-01-20 12:25:31 PM	188	Remote Desktop Services: Session logoff succeeded. NT AUTHORITY\SYSTEM	
4104	2022-01-20 12:42:02 PM	926	Creating Scriptblock text.	
4104	2022-01-20 12:42:08 PM	933	Creating Scriptblock text.	
4104	2022-01-20 12:42:24 PM	940	Creating Scriptblock text.	
4104	2022-01-20 12:42:26 PM	942	Creating Scriptblock text.	
4104	2022-01-20 12:42:27 PM	949	Creating Scriptblock text.	
4104	2022-01-20 12:42:38 PM	958	Creating Scriptblock text.	
4104	2022-01-20 12:42:40 PM	965	Creating Scriptblock text.	
5861	2022-01-20 1:35:01 PM	235	WMI Registration of Permanent Event Consumer.	
5860	2022-01-20 1:35:58 PM	237	Remote Desktop Services: Session logoff succeeded. NT AUTHORITY\SYSTEM	

Time zone UTC-5:00

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.

The screenshot shows the Magnet AXIOM Examine v6.7.1.33408 - GBC-22 interface. The main window displays the 'EVIDENCE (100)' table. The table has columns for Path, Path..., Accessed Date/T..., and Accessed Da.... The data in the table shows numerous entries for files like 'New Text Document.txt' located at 'C:\Users\T433-COMP4071\Desktop'. These files were accessed on 2022-01-20 at various times between 12:09:28 PM and 13:59:41 PM. The sidebar on the left lists categories such as Evidence, Artifacts, Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists, Skin tone, Filters, and Media categorization. The right sidebar shows 'TAGS, PROFILES & MEDIA CATEGORIES'. The bottom status bar indicates Time zone: UTC-5:00, ENG US, 4:18 AM, and 2022-11-15.

Path	Path...	Accessed Date/T...	Accessed Da...
C:\	Drive	2022-01-20 12:09:28 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 13:59:41	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41	2022-01-20 13:59:41
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 1:59:41 PM	
C:\Users\T433-COMP4071\Desktop\New Text Document.txt	Drive	2022-01-20 13:59:41	
C:\Users\T433-COMP4071\Desktop\Oct 15 Process	Drive		
C:\Users\T433-COMP4071\Desktop\Oct 15 Process Hacker Processes.txt	Drive		
C:\Users\T433-COMP4071\Desktop\Oct 15 Process Hacker Processes.txt	Drive	2022-10-15 10:18:56 AM	
C:\Users\T433-COMP4071\Desktop\Oct15	Drive	2022-10-15 10:18:56	
C:\Users\T433-COMP4071\Desktop\Oct15	Drive	2022-10-15 10:11:30	
C:\Users\T433-COMP4071\Desktop\Oct15	Drive		
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 1:38:56 PM	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 13:38:56	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 13:38:56	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 1:38:56 PM	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 1:38:56 PM	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 1:38:56 PM	
C:\Users\T433-COMP4071\Desktop\README.txt	Drive	2022-01-20 13:38:56	
C:\Users\T433-COMP4071\Desktop\Sumo Install Token.txt	Drive	2022-01-20 1:59:54 PM	

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.

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 Type a search term... GO ADVANCED

**EVIDENCE (100)**

Path	Path...	Accessed Date/T...	Accessed Da...
L:\Users\1433-COMP4U\Downloads	Drive	2022-10-15 9:35:57 AM	2022-10-15 10:30:47
C:\Users\T433-COMP4071\Downloads\8124b9a07865df313625b6e19f3912567df267cf132ff37e5a22474386a56913.docx	Drive		
C:\Users\T433-COMP4071\Downloads\8128046452\f824b9a07865df13625b6e19f3912567df267cf132ff37e5a22474386a56913.docx	Drive		
C:\Users\T433-COMP4071\Downloads\8124b9a07865df313625b6e19f3912567df267cf132ff37e5a22474386a56913.docx	Drive		2022-10-15 09:35:57
C:\Users\T433-COMP4071\Downloads\8132966359\72bcab518a250017c3865a19e26fbcdce367e7a713ba60682f2a66c49710797f.docx	Drive	2022-10-15 9:29:35 AM	
C:\Users\T433-COMP4071\Downloads\8132966359\72bcab518a250017c3865a19e26fbcdce367e7a713ba60682f2a66c49710797f.docx	Drive		2022-10-15 09:29:35
C:\Users\T433-COMP4071\Downloads\8132966359\72bcab518a250017c3865a19e26fbcdce367e7a713ba60682f2a66c49710797f.docx	Drive		
C:\Users\T433-COMP4071\Downloads\8132966359\72bcab518a250017c3865a19e26fbcdce367e7a713ba60682f2a66c49710797f.docx	Drive		
C:\Users\T433-COMP4071\Downloads\8138576281\7bee5c2c37e206380e6f2cc13587a11a43fc574c9399bf2638b159c6397d3ec.pdf	Drive	2022-10-15 9:32:04 AM	
C:\Users\T433-COMP4071\Downloads\8138576281\7bee5c2c37e206380e6f2cc13587a11a43fc574c9399bf2638b159c6397d3ec.pdf	Drive		2022-10-15 09:32:04
C:\Users\T433-COMP4071\Downloads\8138576281\7bee5c2c37e206380e6f2cc13587a11a43fc574c9399bf2638b159c6397d3ec.pdf	Drive		
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive	2022-01-20 1:30:47 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive		2022-01-20 13:30:47
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive		
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive	2022-01-20 1:30:47 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive		2022-01-20 1:30:47 PM
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive		
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive	2022-01-20 1:30:47 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers	Drive		2022-01-20 13:30:47
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive	2022-01-20 1:31:23 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		2022-01-20 13:31:23
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive	2022-01-20 1:31:23 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		2022-01-20 1:31:23 PM
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive	2022-01-20 1:31:23 PM	
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		2022-01-20 13:31:23
C:\Users\T433-COMP4071\Downloads\Wallpapers\29409404431_8a95313b1d_o.jpg	Drive		
Time zone UTC-5:00	ENG US	4:22 AM	2022-11-15

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.

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 Type a search term... GO ADVANCED

**EVIDENCE (47)**

Application Name	Company	Created...	Key Last Update...	Insta...	Version	Potential Location
Python 3.7.9 Documentation (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:17 PM	7980	3.7.9150.0	
Autopsy	The Sleuth Kit	2022-01-20	2022-01-20 12:41:53 PM	2372209	4.18.0	
Node.js	Node.js Foundation	2022-01-20	2022-01-20 11:52:44 PM	83878	13.14.0	
Python 3.7.9 Test Suite (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:17 PM	21352	3.7.9150.0	
Python 3.7.9 Tcl/Tk Support (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:22 PM	16540	3.7.9150.0	
VMware Tools	VMware, Inc.	2022-01-20	2022-01-20 11:54:49 AM	99748	11.2.6.17901274	
Python 3.7.9 Core Interpreter (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:11 PM	3708	3.7.9150.0	
Python 3.7.9 Add to Path (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:26 PM	40	3.7.9150.0	
Python 3.7.9 Standard Library (64-bit)	Python Software Foundation	2022-01-20	2022-01-20 12:25:14 PM	26232	3.7.9150.0	
FileInsight - File analysis tool	McAfee Inc.	2022-01-20	2022-01-20 12:42:14 PM			
Google Chrome	Google LLC	2022-01-20	2022-01-20 12:07:21 PM	97.0.4692.99	C:\Program Files\Google\Chrome\Appli...	
Graphviz	Graphviz	2022-01-20	2022-01-20 10:36:36 PM	2.49.3	C:\Program Files\Graphviz	
HashCalc 2.02	SlavaSoft Inc.	2022-01-20	2022-01-20 12:59:15 PM			
Maltego	Paterva	2022-01-20	2022-01-20 11:55:25 PM	4	C:\Program Files (x86)\Paterva\Maltego	
Microsoft Edge Update		2022-01-20	2022-01-20 9:26:38 AM	1.3.167.21		
Nmap 7.70	Nmap Project	2022-01-20	2022-01-20 12:55:11 PM	7.70	C:\Program Files (x86)\Nmap	
Npcap 0.99-r2	Nmap Project	2022-01-20	2022-01-20 12:55:20 PM	0.99-r2	C:\Program Files\Npcap	
PDFStreamDumper 0.9.5xx		2022-01-20	2022-01-20 10:07:01 PM		c:\PDFStreamDumper	
SysAnalyzer 2.x		2022-01-20	2022-01-20 11:02:21 PM			
WinPcap 4.1.3	Riverbed Technology, Inc.	2022-01-20	2022-01-20 12:54:48 PM	4.1.0.2980	C:\Program Files (x86)\WinPcap	
Wireshark 3.6.1 64-bit	The Wireshark developer co...	2022-01-20	2022-01-20 12:55:00 PM	200396	3.6.1	C:\Program Files\Wireshark
Python 2.7.15	Python Software Foundation	2022-01-20	2022-01-20 12:24:40 PM	27843	2.7.15150	C:\Python27.x86
Java 8 Update 311	Oracle Corporation	2022-01-20	2022-01-20 12:37:43 PM	112370	8.0.3110.11	
Java Auto Updater	Oracle Corporation	2022-01-20	2022-01-20 12:38:12 PM	2161	2.8.311.11	
Python Launcher	Python Software Foundation	2022-01-20	2022-01-20 12:25:22 PM	1804	3.7.7168.0	
Time zone UTC-5:00	ENG US	4:33 AM	2022-11-15			

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.

The screenshot shows the Magnet AXIOM Examine v6.7.1.33408 - GBC-22 interface. The main window displays the 'EVIDENCE (19)' section, which lists various files with their details such as File Name, File Type, and Date Created. A large portion of the table is filled with entries related to Microsoft Office containers, including several .XLAM files. On the left, a sidebar shows category counts: WEB RELATED (61,356), COMMUNICATION (16), MEDIA (52,457), EMAIL & CALENDAR (224), DOCUMENTS (2,925), ADDITIONAL SOURCES (2), APPLICATION USAGE (162), OPERATING SYSTEM (62,579), MEMORY (556,550), ENCRYPTION & CREDENTIALS (27), and CUSTOM (2,832). The bottom right corner shows system status: ENG US, 4:42 AM, 2022-11-15.

EVIDENCE (19)								
	File Name	File...	Detected Fil...	File Created...	File Modified D...	File Accessed Da...	MDS	DETAILS
	cardflipped.dat	645000	Encrypted Container	2019-12-07 4:53:38 AM	2019-12-07 4:53:38 AM	2022-01-20 2:52:40 PM	09b82c	
	ubuntu-xenial-amd64-libc6-dev.sig	336734	Encrypted Container	2020-10-21 6:19:10 PM	2020-10-21 6:19:10 PM	2022-01-20 12:34:45 PM	b97564	
	mpcache-F0249948F974D2F37A4273578BE382CAF60C120A.bin.67	46858240	Encrypted Container	2022-01-20 12:02:46 PM	2022-01-20 12:02:46 PM	2022-01-20 12:02:55 PM	c74ab4	
	mpcache-F0249948F974D2F37A4273578BE382CAF60C120A.bin.80	20949876	Encrypted Container	2022-01-20 12:02:47 PM	2022-01-20 12:02:47 PM	2022-01-20 12:02:55 PM	34772a	
	04d8664dc55a5a190ebec5cefa06207afe7150554a4b104050362ed9	1933534	Encrypted Container	2022-01-20 12:26:29 PM	2022-01-20 12:26:29 PM	2022-01-20 12:26:29 PM	67d2e6	
	08cf7e79ee9b6b39e2def3a5a9fe7b155223505c7fe7482259ff05db	1096850	Encrypted Container	2022-01-20 12:27:08 PM	2022-01-20 12:27:08 PM	2022-01-20 12:27:08 PM	bb91b1	
	prodot.zip	36911540	Zip	2022-01-20 1:03:42 PM	2022-01-20 1:03:46 PM	2022-01-20 1:03:46 PM	ab844c	
	setup[1].zst	3605422	Encrypted Container	2022-01-20 1:07:53 PM	2022-01-20 1:07:54 PM	2022-01-20 1:07:54 PM	f92118	
	libstdc++-6-11.2.0-1.tar.zst	509265	Encrypted Container	2022-01-20 1:07:58 PM	2022-01-20 1:07:58 PM	2022-01-20 1:07:58 PM	fa08aa	
	libmpfr6-4.1.0-2.tar.zst	1361443	Encrypted Container	2022-01-20 1:07:58 PM	2022-01-20 1:07:58 PM	2022-01-20 1:07:58 PM	7bcfb2	
	ca-certificates-2021.2.52-1.tar.zst	351294	Encrypted Container	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	8667d4	
	tar-1.34-1.tar.zst	1004224	Encrypted Container	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	0e582e	
	zstd-1.5.1-1.tar.zst	417213	Encrypted Container	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	2022-01-20 1:08:01 PM	876f0a	
	man-db-2.9.4-2.1.tar.zst	1103998	Encrypted Container	2022-01-20 1:08:02 PM	2022-01-20 1:08:02 PM	2022-01-20 1:08:02 PM	201854	
	SOLVER.XLAM	921037	Ms Office 2007	2022-01-20 1:56:12 PM	2022-01-20 1:56:12 PM	2022-01-20 1:56:12 PM	2ef245	
	EUROTOOL.XLAM	382270	Ms Office 2007	2022-01-20 1:56:13 PM	2022-01-20 1:56:13 PM	2022-01-20 1:56:13 PM	83d8b7	
	EXPTOOLS.XLA	92160	Excel	2022-01-20 1:56:21 PM	2022-01-20 1:56:21 PM	2022-01-20 1:56:21 PM	b898e8	
	ATPVBAEN.XLAM	45514	Ms Office 2007	2022-01-20 1:56:21 PM	2022-01-20 1:56:21 PM	2022-01-20 1:56:21 PM	cff384c	
	f_000149	351621	Encrypted Container	2022-01-20 2:07:05 PM	2022-01-20 2:07:05 PM	2022-01-20 2:07:05 PM	357d19	

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.

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 Type a search term... GO ADVANCED

**EVIDENCE (19)**

	File Name	File...	Detected Fil...	File Created
	cardflipped.dat	645000	Encrypted Container	2019-12-07 4
	ubuntu-xenial-amd64-libc6-dev.sig	336734	Encrypted Container	2020-10-21 6
	mpcache-F0249948F974D2F37A4273578E382CAF60C120A.bin.67	46858240	Encrypted Container	2022-01-20 1
	mpcache-F0249948F974D2F37A4273578E382CAF60C120A.bin.80	20949876	Encrypted Container	2022-01-20 1
	04d86e4dc5a5a190ebec5ceef06207afe7150554a4b1b4050362ed9	1933534	Encrypted Container	2022-01-20 1
	08cf7e79ee9b6b39e2def3a5a9fe7b155223505c7fe7482259f05db	1096850	Encrypted Container	2022-01-20 1
	prodot.zip	36911540	Zip	2022-01-20 1
	setup[1].zst	3605422	Encrypted Container	2022-01-20 1
	libstdc++-6-11.2.0-1.tar.zst	509265	Encrypted Container	2022-01-20 1
	libmpfr6-4.1.0-2.tar.zst	1361443	Encrypted Container	2022-01-20 1
	ca-certificates-2021.2.52-1.tar.zst	351294	Encrypted Container	2022-01-20 1
	tar-1.34-1.tar.zst	1004224	Encrypted Container	2022-01-20 1
	zstd-1.5.1-1.tar.zst	417213	Encrypted Container	2022-01-20 1
	man-db-2.9.4-2.1.tar.zst	1103998	Encrypted Container	2022-01-20 1
	SOLVER.XLAM	921037	Ms Office 2007	2022-01-20 1
	EUROTOOL.XLAM	382270	Ms Office 2007	2022-01-20 1
	EXPTOOLS.XLA	92160	Excel	2022-01-20 1
	ATPVBAEN.XLAM	45514	Ms Office 2007	2022-01-20 1
	f_000149	351621	Encrypted Container	2022-01-20 2

**SOLVER.XLAM**

**DETAILS**

**ARTIFACT INFORMATION**

File Name	SOLVER.XLAM
File Size (bytes)	921037
Detected File Type	Ms Office 2007
File Created Date/Time	2022-01-20 1:56:12 PM
File Modified Date/Time	2022-01-20 1:56:12 PM
File Accessed Date/Time	2022-01-20 1:56:12 PM
MD5 Hash	2ef245bbb2367f4e8ebcc152ecfc0199
SHA1 Hash	9dcdfa5c6d4133f25960b867b1217db7afcd10
Artifact type	Encrypted Files
Item ID	126698

**EVIDENCE INFORMATION**

Source	T433-Student-W10.vmdk
Partition	3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\SOLVER\
Location	n/a
Evidence number	T433-Student-W10.vmdk

Recovery method: Parsing  
Deleted source  
Location: n/a  
Evidence number: T433-Student-W10.vmdk

Time zone: UTC-5:00

ENG US 4:42 AM 2022-11-15

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.

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 Type a search term... GO ADVANCED

**EVIDENCE (8)**

	File...	Soft...	Created Date/Ti...	Last Accessed D...	Last Modified D...	Artifact type	Source
	gpg.exe	GPG	2022-01-20 1:08:40 PM	2022-01-20 1:08:40 PM	2018-08-03 10:42:09 AM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	ssp.exe	SpyStopper	2022-01-20 1:08:02 PM	2022-01-20 1:08:02 PM	2021-12-03 11:37:54 AM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	TE.exe	Tracks Eraser	2018-10-22 9:12:04 PM	2022-01-20 12:21:53 PM	2018-10-22 9:12:04 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	gpg.exe	GPG	2022-01-20 12:24:19 PM	2022-01-20 12:24:19 PM	2021-11-15 1:48:39 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	ssp.exe	SpyStopper	2022-01-20 12:24:20 PM	2022-01-20 12:24:20 PM	2021-11-15 1:48:42 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	TE.exe	Tracks Eraser	2018-10-22 9:12:04 PM	2022-01-20 12:21:53 PM	2018-10-22 9:12:04 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	TE.exe	Tracks Eraser	2018-10-22 9:12:04 PM	2022-01-20 12:21:53 PM	2018-10-22 9:12:04 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...
	TE.exe	Tracks Eraser	2018-10-22 9:12:04 PM	2022-01-20 12:21:53 PM	2018-10-22 9:12:04 PM	Encryption / Anti-forensics Tools	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...

**gpg...**

**T433-Student-W10.vmdk**

**DETAILS**

**ARTIFACT INFO**

File Name	gpg...
Created Date	2022-01-20 1:08:40 PM
Last Accessed Date	2018-08-03 10:42:09 AM
Last Modified Date	2018-08-03 11:37:54 AM
Artifact type	Encryption / Anti-forensics Tools
Source	T433-Student-W10.vmdk - Partition 3 (Microsoft NTFS, 99.68 GB) \Program Files (x86)\Microsoft Office\root\Office16\Library\gpg...

**EVIDENCE INFO**

Time zone: UTC-5:00

ENG US 4:43 AM 2022-11-15

## 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.

The screenshot shows the Magnet AXIOM Examine v6.7.1.33408 - GBC-22 interface. The left sidebar lists various evidence categories with their counts: WEB RELATED (61,356), COMMUNICATION (16), MEDIA (52,457), EMAIL & CALENDAR (224), DOCUMENTS (2,925), ADDITIONAL SOURCES (2), APPLICATION USAGE (162), OPERATING SYSTEM (62,579), MEMORY (556,550), ENCRYPTION & CREDENTIALS (27), and CONNECTED DEVICES (9). The CUSTOM category has 2,832 entries. The right side displays the 'EVIDENCE (4)' section with a table:

File Name	File Path	File System Create...	File System Last...	File System
MPDetection-20220120-115211.log	ProgramData\Microsoft\Windows Defender\Support\MPDetection-20220120-115211.log	2022-01-20 2:52:11 PM	2022-01-20 2:12:13 PM	2022-01-20 2:12:13 PM
MPDetection-20221008-092216.log	ProgramData\Microsoft\Windows Defender\Support\MPDetection-20221008-092216.log	2022-10-08 9:22:16 AM	2022-10-08 9:33:28 AM	2022-10-08 9:33:28 AM
MPLog-20220120-115211.log	ProgramData\Microsoft\Windows Defender\Support\MPLog-20220120-115211.log	2022-01-20 2:52:11 PM	2022-10-08 9:33:28 AM	2022-10-08 9:33:28 AM
Unknown.Log	ProgramData\Microsoft\Windows Defender\Scans\History\Service\Unknown.Log	2022-01-20 12:06:11 PM	2022-01-20 12:13:25 PM	2022-01-20 12:13:25 PM

At the bottom, the status bar shows Time zone: UTC-5:00, ENG US, 4:35 AM, and 2022-11-15.

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.

Magnet AXIOM Examine v6.7.1.33408 - GBC-22

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

**FILTERS**

Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

**EVIDENCE (677)**

	Created Date...	E...	Event Description Summary	Target User...	Target Dom...	Target User SID
	2022-01-20 11:53:38 AM	184	A user account was created.	T433-COMP4071	WIN-G5FDGL4OABP	S-1-5-21-3408837479-307362006
	2022-01-20 11:53:38 AM	185	A user account was enabled.	T433-COMP4071	WIN-G5FDGL4OABP	S-1-5-21-3408837479-307362006
	2022-01-20 11:53:38 AM	192	An attempt was made to reset an account's password.	T433-COMP4071	WIN-G5FDGL4OABP	S-1-5-21-3408837479-307362006
	2022-01-20 11:53:38 AM	194	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:38 AM	196	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:39 AM	198	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:40 AM	200	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:41 AM	205	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:41 AM	207	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:41 AM	209	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:41 AM	211	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:42 AM	213	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:42 AM	215	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:42 AM	217	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:43 AM	221	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:43 AM	241	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:43 AM	294	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:43 AM	296	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	298	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	300	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	302	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	304	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	306	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	308	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18
	2022-01-20 11:53:44 AM	310	An account was successfully logged on.	SYSTEM	NT AUTHORITY	S-1-5-18

**4624**

**T433-Student-W10.vmdk**

**DETAILS**

**ARTIFACT INFO**

Created Date Event Description Lc Subject L Subject Dom Target L Target Dom Target E

Time zone UTC-5:00

ENG US 4:52 AM 2022-11-15

## 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.

Magnet AXIOM Examine v6.7.1.33408 - GBC-22

File Tools Process Help

Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

**FILTERS**

Media categorization Media attributes (VICS)

Type a search term... GO ADVANCED

**EVIDENCE (225)**

**APPLICATION USAGE** 162

**OPERATING SYSTEM** 62,579

**MEMORY** 556,550

- API Hooks (apihooks) 34,155
- Dynamically Loaded Libraries (dllist) 11,771
- Files (filescan) 26,593
- Hidden Processes (psview) 299
- Hidden/Residual Modules (modscan) 413
- Hidden/Terminated Processes (psscan) 159
- Image Info (imageinfo) 2
- LDR Modules (ldrmodules) 13,037
- Loaded Kernel Modules (modules) 383
- Malware Finder (malfind) 4
- Network Info (netscan) 225
- Open Handles (handles) 396,073
- Process Security Identifiers (getsids) 3,796
- Processes (pslist) 294
- Timeline (timeliner) 69,346

**ENCRYPTION & CREDENTIALS** 27

**CONNECTED DEVICES** 9

**CUSTOM** 2,832

**TCPv4**

Protocol	Local IP Address	Remote IP Address	State	Process ID	Owner	Created Date...	Artifact type
UDPV6	::0	*.*	2940	msedge.exe	2022-10-15 9:33:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	2940	msedge.exe	2022-10-15 9:33:50 AM	Network Info (netscan)	
UDPV6	::0	*.*	2940	msedge.exe	2022-10-15 9:33:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	2940	msedge.exe	2022-10-15 9:33:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	8252	chrome.exe	2022-10-15 9:49:20 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1436	svchost.exe	2022-10-15 10:17:43 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	2940	msedge.exe	2022-10-15 10:17:49 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	8812	chrome.exe	2022-10-15 10:17:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	8812	chrome.exe	2022-10-15 10:17:50 AM	Network Info (netscan)	
UDPV6	::0	*.*	8812	chrome.exe	2022-10-15 10:17:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1988	svchost.exe	2022-10-15 10:17:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1988	svchost.exe	2022-10-15 10:17:50 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1436	svchost.exe	2022-10-15 10:18:20 AM	Network Info (netscan)	
UDPV6	::0	*.*	1436	svchost.exe	2022-10-15 10:18:20 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1816	svchost.exe	2022-10-15 10:19:01 AM	Network Info (netscan)	
UDPV6	::0	*.*	1816	svchost.exe	2022-10-15 10:19:01 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	1988	svchost.exe	2022-10-15 10:19:09 AM	Network Info (netscan)	
UDPV6	::0	*.*	1988	svchost.exe	2022-10-15 10:19:09 AM	Network Info (netscan)	
UDPV6	::0	*.*	3084	MsSense.exe	2022-10-15 10:19:11 AM	Network Info (netscan)	
UDPV4	0.0.0.0	*.*	3084	MsSense.exe	2022-10-15 10:19:11 AM	Network Info (netscan)	
TCPv4	192.168.175.131:49944	52.226.139.121:443	ESTABLISHED	-1			Network Info (netscan)
TCPv4	127.0.0.1:32000	127.0.0.1:31000	ESTABLISHED	-1			Network Info (netscan)
TCPv4	192.168.175.131:50888	192.168.175.47:445	CLOSED	-1			Network Info (netscan)
TCPv4	192.168.175.128:49683	52.226.139.185:443	ESTABLISHED	-1			Network Info (netscan)
TCPv4	192.168.175.128:49899	52.167.17.97:443	CLOSED	-1			Network Info (netscan)

Time zone UTC-5:00

ENG US 5:03 AM 2022-11-15

An IP lookup yields no meaningful results.

https://whatismyipaddress.com/ip/52.226.199.121

Getting Started YouTube Reddit Blackboard Google Drive Home Other Bookmarks

**What's MyIPAddress.com**

Enter Keywords or IP Address... Q Search

ABOUT PRESS BLOG CONTACT

MY IP IP LOOKUP HIDE MY IP VPNs TOOLS LEARN

IP Details For: 52.226.199.121

Decimal: 887277433 Hostname: 52.226.199.121 ASN: 8075 ISP: Microsoft Corporation Services: Datacenter Assignment: Likely Static IP Country: United States State/Region: Virginia City: Washington

Latitude: 38.713451 (38° 42' 48.42" N) Longitude: -78.159439 (78° 9' 33.98" W)

CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address or for legal purposes. Geolocation data from IP2Location.

ENG US 5:07 AM 2022-11-15

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.

Screenshot of Magnet AXIOM Examine v6.7.1.33408 - GBC-22 showing Process list details.

**EVIDENCE (294)**

APPLICATION USAGE	162
OPERATING SYSTEM	62,579
MEMORY	556,550
API Hooks (apihooks)	34,155
Dynamically Loaded Libraries (dllist)	11,771
Files (flescan)	26,593
Hidden Processes (psxview)	299
Hidden/Residual Modules (modscan)	413
Hidden/Terminated Processes (psscan)	159
Image Info (imageinfo)	2
LDR Modules (ldrmodules)	13,037
Loaded Kernel Modules (modules)	383
Malware Finder (malfind)	4
Network Info (netscan)	225
Open Handles (handles)	396,073
Process Security Identifiers (getsids)	3,796
Processes (plist)	294
Timeline (timeliner)	69,346
ENCRYPTION & CREDENTIALS	27
CONNECTED DEVICES	9
CUSTOM	2,832

**Process List Details:**

Process Name	Process ID	Parent Process ID	Handle Count	Session ID	Working Set	Process Start Date/Time	Process Exit Date/Time	Artifact Type
explorer.exe	4284	4228	0	1	0	2022-10-08 9:28:03 AM		Processes (plist)
notepad.exe	8836	4284	0	1	0	2022-10-15 9:03:59 AM		Processes (plist)
chrome.exe	8252	4284	0	1	0	2022-10-15 9:05:02 AM		Processes (plist)
chrome.exe	8796	8252	0	1	0	2022-10-15 9:05:12 AM		Processes (plist)
chrome.exe	7844	8252	0	1	0	2022-10-15 9:05:03 AM		Processes (plist)
chrome.exe	3448	8252	0	1	0	2022-10-15 9:05:15 AM		Processes (plist)
chrome.exe	8812	8252	0	1	0	2022-10-15 9:05:13 AM		Processes (plist)
chrome.exe	8944	8252	0	1	0	2022-10-15 9:05:24 AM		Processes (plist)
chrome.exe	1100	8252	0	1	0	2022-10-15 9:07:44 AM		Processes (plist)
chrome.exe	8060	8252	0	1	0	2022-10-15 9:10:40 AM		Processes (plist)
chrome.exe	3980	8252	0	1	0	2022-10-15 9:34:44 AM		Processes (plist)
chrome.exe	7384	8252	0	1	0	2022-10-15 9:34:47 AM		Processes (plist)
19075-NYPD.exe	6028	4284	0	1	1	2022-10-15 9:47:59 AM		Processes (plist)
chrome.exe	469296	8252	0	1	0	2022-10-15 10:01:32 AM		Processes (plist)
explorer.exe	4284	4228	0	1	0	2022-10-08 9:28:03 AM		Processes (plist)
System	4	0	0	-1	0	2022-10-08 9:27:57 AM		Processes (plist)
Registry	92	4	0	-1	0	2022-10-08 9:27:53 AM		Processes (plist)
smss.exe	316	4	0	-1	0	2022-10-08 9:27:57 AM		Processes (plist)
csrss.exe	428	416	0	0	0	2022-10-08 9:27:58 AM		Processes (plist)
wininit.exe	504	416	0	0	0	2022-10-08 9:27:58 AM		Processes (plist)
csrss.exe	512	496	0	1	0	2022-10-08 9:27:58 AM		Processes (plist)
winlogon.exe	600	496	0	1	0	2022-10-08 9:27:58 AM		Processes (plist)
services.exe	640	504	0	0	0	2022-10-08 9:27:58 AM		Processes (plist)
lsass.exe	656	504	0	0	0	2022-10-08 9:27:58 AM		Processes (plist)
svchost.exe	760	640	0	0	0	2022-10-08 9:27:58 AM		Processes (plist)

Time zone: UTC-5:00

Icons at bottom: Windows, Taskbar, Firefox, Explorer, ENG US, WiFi, Battery, 5:37 AM, 2022-11-15