Pentesting Technical Report

4Geeks
Ph: +1 786 345 5555

0. Índice

0. Índice **2**

1. Introducción **3**

2. Herramientas utilizadas **3**

3. Evidencias relevantes **3**

3.1 Archivos manipulados 3

3.2 Compresión 3

3.3 Navegación sospechosa 4

3.4 Eliminación de rastros 4

3.5 Prefetch y artefactos 4

4. Linea del tiempo **4**

5. Conclusión **5**

6. Anexo **5**

1. Introducción

El principal objetivo de esta práctica sería actuar como un forense para ver qué ha ocurrido en la organización que ha sido atacada y ver qué datos han sido filtrados,movidos,eliminados…

2. Herramientas utilizadas

Las principales herramientas que han sido usadas para esta práctica han sido:

- autopsy: es una herramienta de código abierto que se utiliza para poder hacer un análisis de los discos duros o cualquier otra unidad de almacenamiento.

3. Evidencias relevantes

3.1 Archivos manipulados

Como podemos ver gracias a la herramienta autopsy,existen varios archivos manipulados como podrían ser:

- MpdCmdRun.exe -> el cual es un ejecutable que podemos ver la fecha de modificación y/o ejecución que es reciente
- mpenginedb.db -> un archivo de la base datos que podemos ver que también ha sido modificado muy recientemente
- msedge_installer.log -> este archivo que se encuentra en los archivos temporales también ha sido manipulado.Puede que el atacante haya podido borrar alguna evidencia de algún log del navegador edge
- NTUSER.DAT -> que se encuentra en la carpeta del usuario afectado también ha sido alterada recientemente,posiblemente el atacante haya editado algo del perfil del usuario.

Hay muchos más archivos afectados la gran mayoría son relacionados con la base de datos,log y ejecutables

3.2 Compresión

Podemos ver como existen varios comprimidos que han sido modificados y/o ejecutados como podrían ser:

- msedge.7z: podemos ver como ha sido modificado

- Windows10.0-KB5055169-x64.cab:tanto este como muchos otros archivos de windows han sido manipulado según podemos ver en la fecha de edición

Hay más archivos modificados como por ejemplo todos los relacionados con Server,sls..

3.3 Navegación sospechosa

Gracias a autopsy podemos observar que en la carpeta Searches del volumen 3 se han intentado enviar datos mediante querys,esta información nos la los log existentes que podemos ver en formato xml que se llaman Indeed location y everywhere.search.

3.4 Eliminación de rastros

Podemos ver que hay muchísimos archivos eliminados,logs,base de datos etc…

Los que yo más destacaría serían los que son del perfil del usuario John Doe,archivo temporal tmp.edb y muchos archivos eliminados de la base de datos

3.5 Prefetch y artefactos

Gracias a la existencia de archivos prefetch se puede confirmar que ha habido ejecuciones tanto en el navegador edge como apps para descomprimir 7-zip

4. Linea del tiempo

El orden en que ha podido ocurrir el ataque ha podido ser el siguiente:

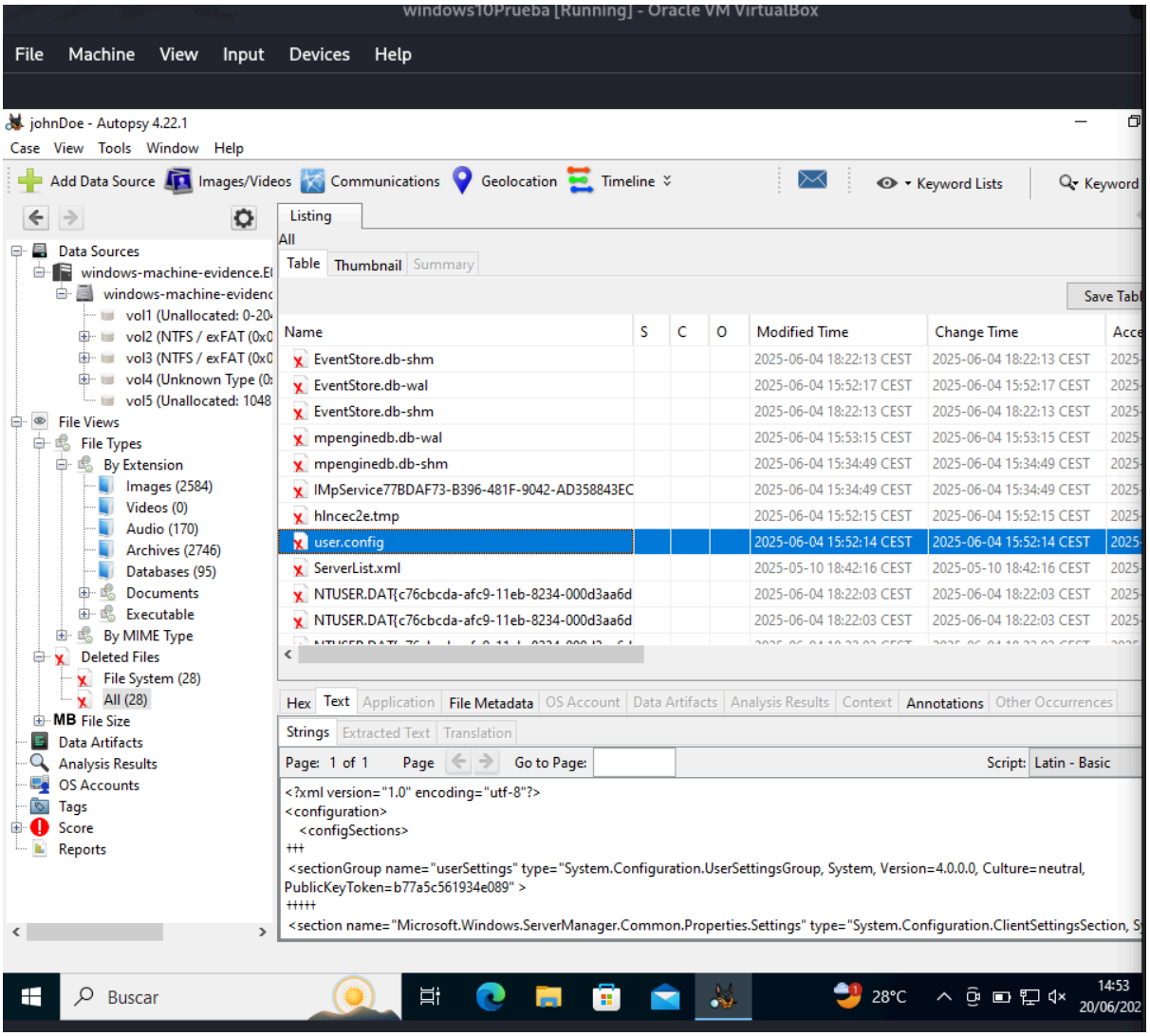
1. El atacante vía web ha llegado a un endpoint vulnerable
2. A través de este endpoint ha podido obtener credenciales del usuario,máquina y servidor,todo esto lo ha hecho a base de unas queries maliciosas.
3. Una vez el atacante ya ha obtenido los datos que necesitaba ha borrado las evidencias que le podían delatar.

5. Conclusión

Las principales conclusiones que podemos sacar de esta práctica podría llegar a ser lo bastante útil que resulta ser una herramienta como autopsy la cuál sabiendo en qué archivos debes de mirar la cantidad de información que puedes llegar a sacar con tan solo conocimientos básicos de gestor de archivos y dicha herramienta forense.

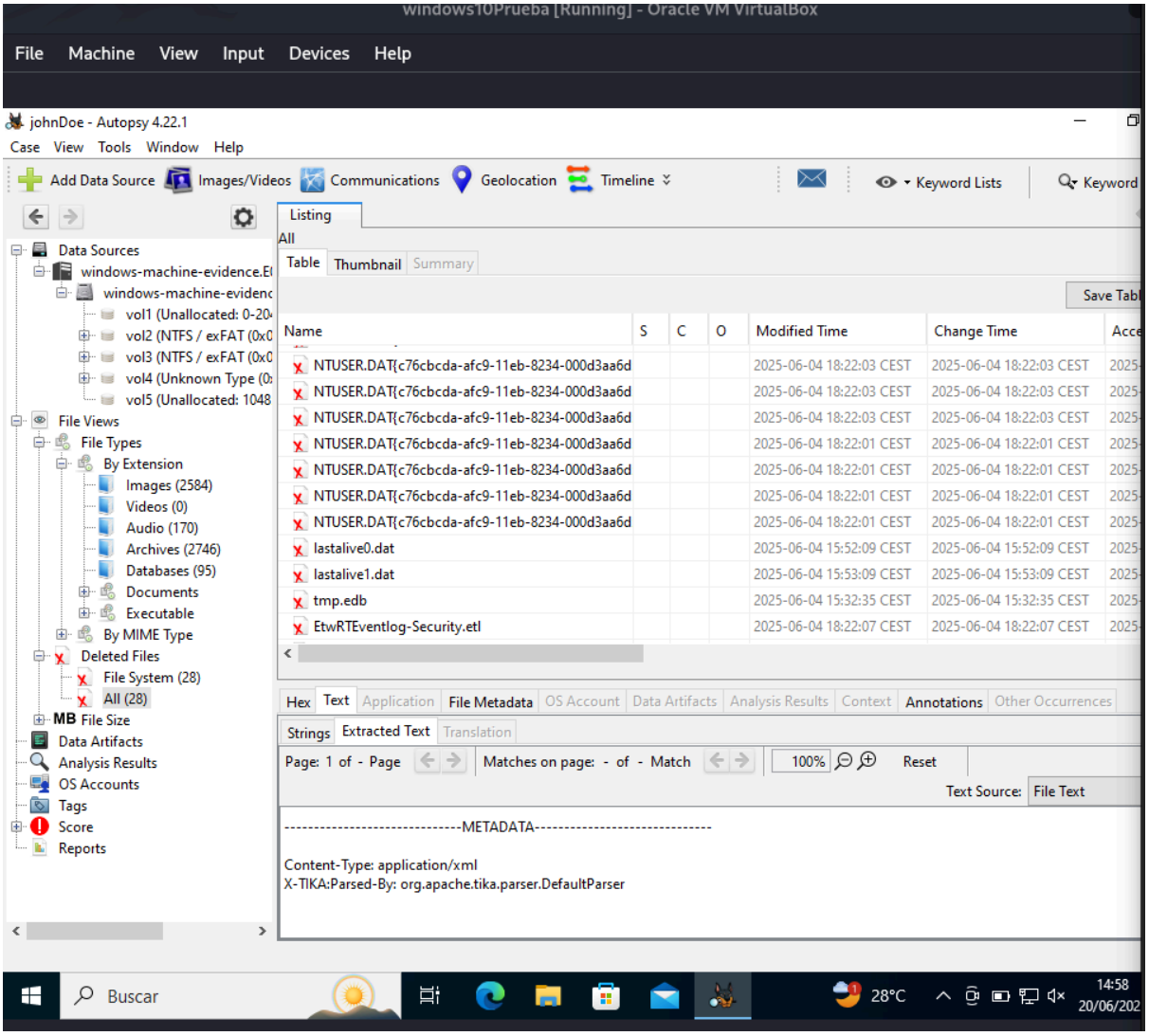
6. Anexo

Adjunto las evidencias que he encontrado con la herramienta autopsy:
Eliminación de archivos:

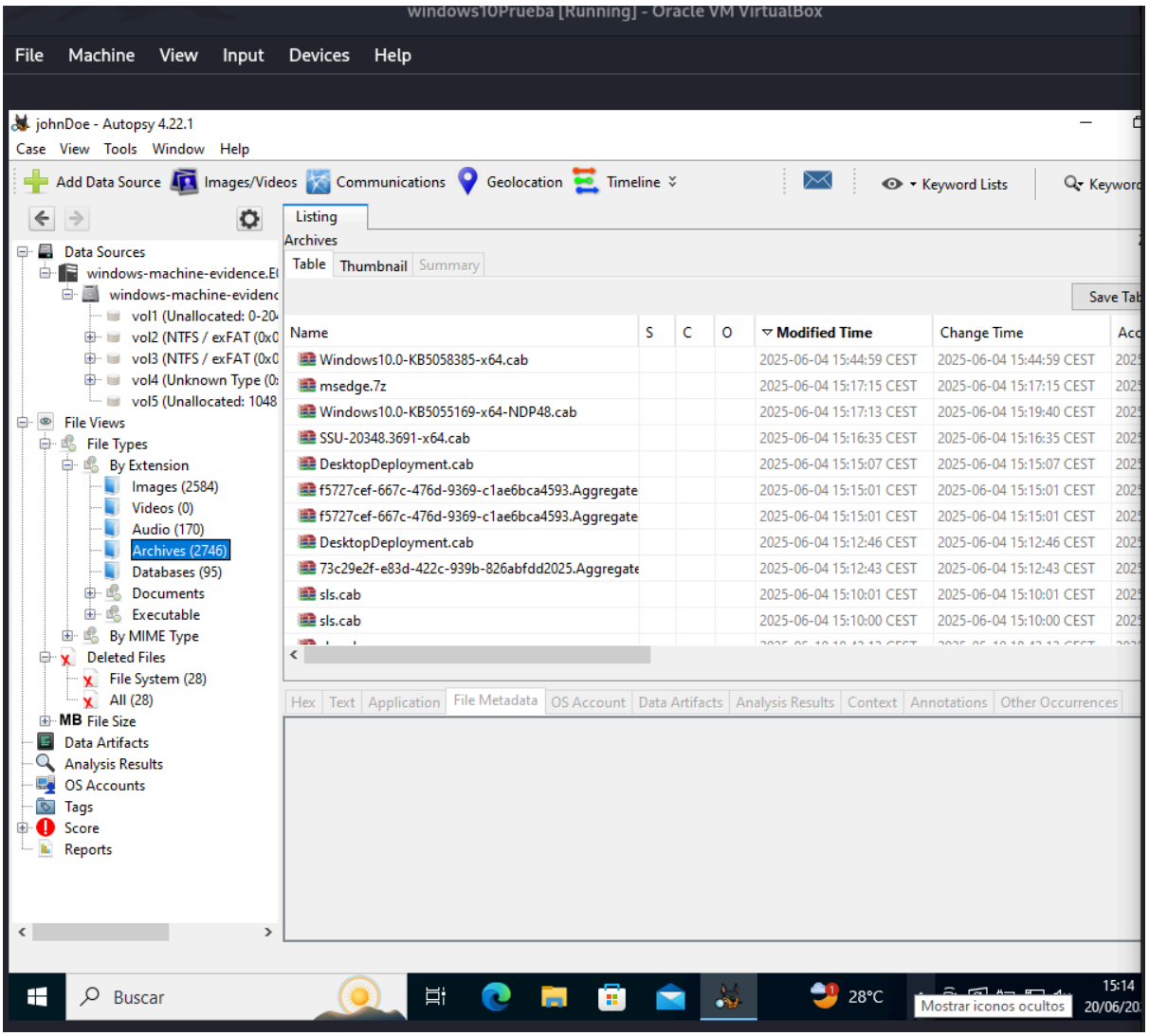


Como podemos ver existen 28 archivos eliminado,entre ellos está user.config,que es uno de los más llamativos ya que podemos ver como contiene publickeytoken referentes a una posible base de datos,archivos

borrados perteneciente a perfiles de usuarios,archivos como tmp.edb o .dat:

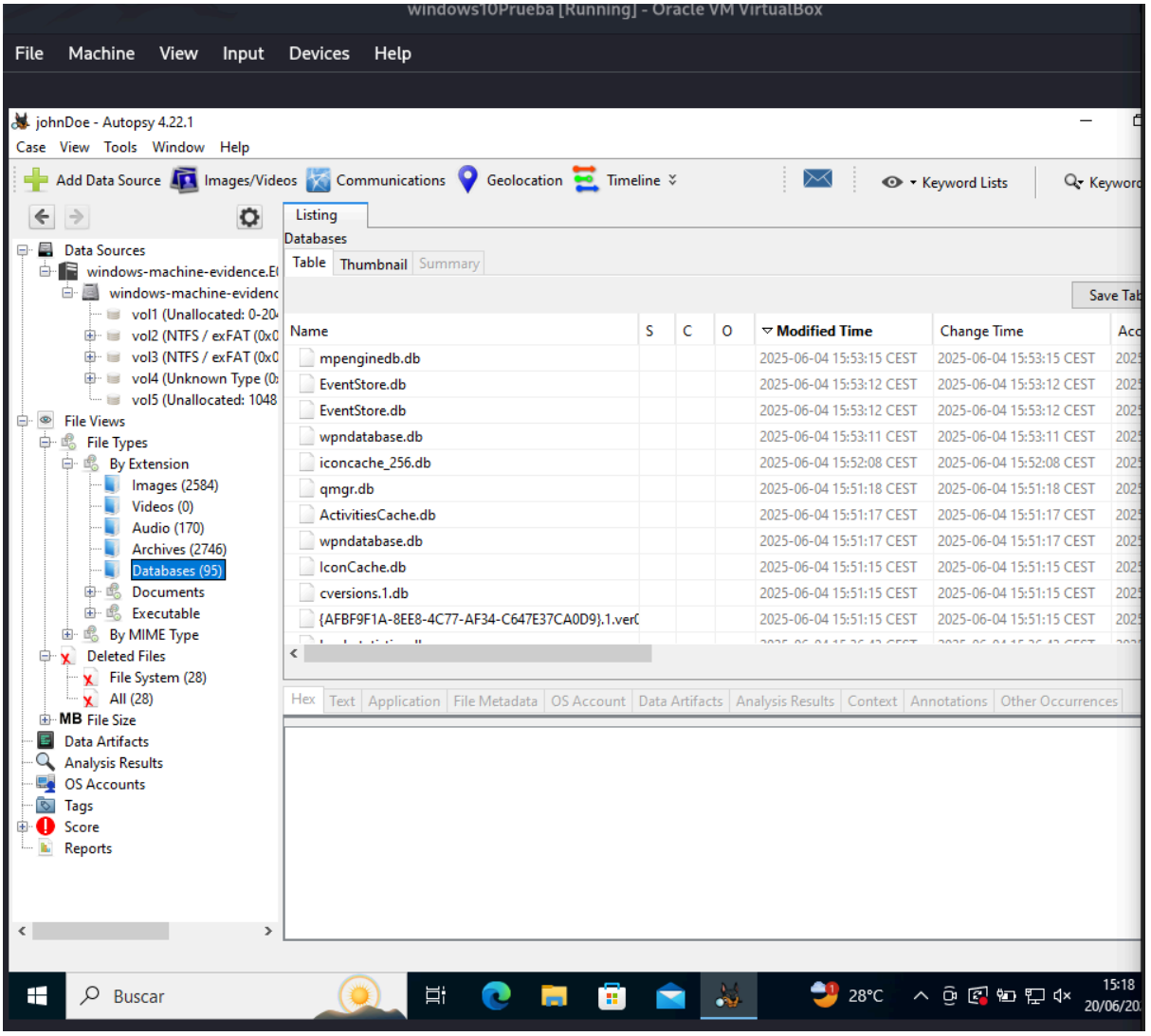


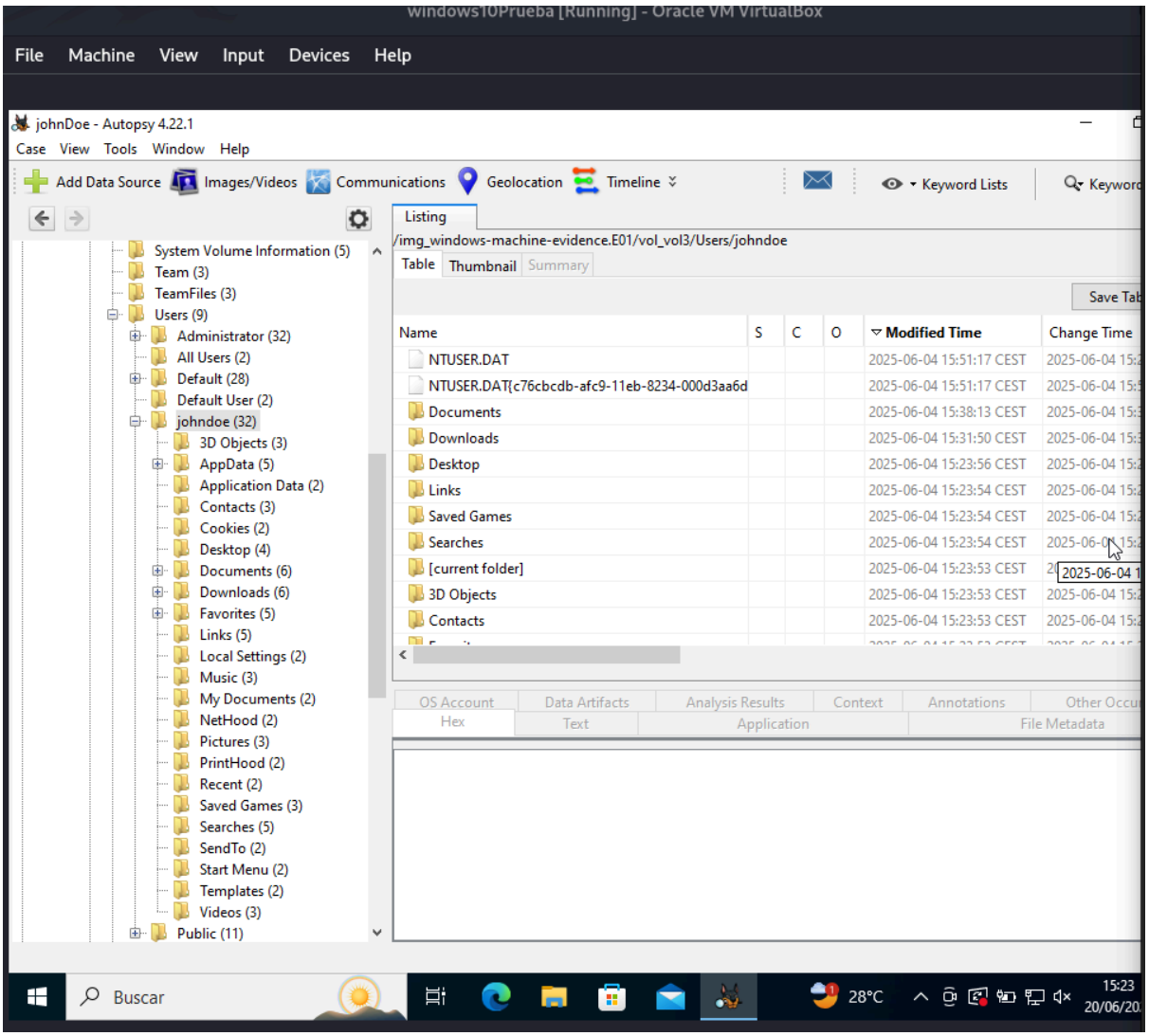
También encontramos archivos que han sido manipulados y ejecutados como podrían ser:

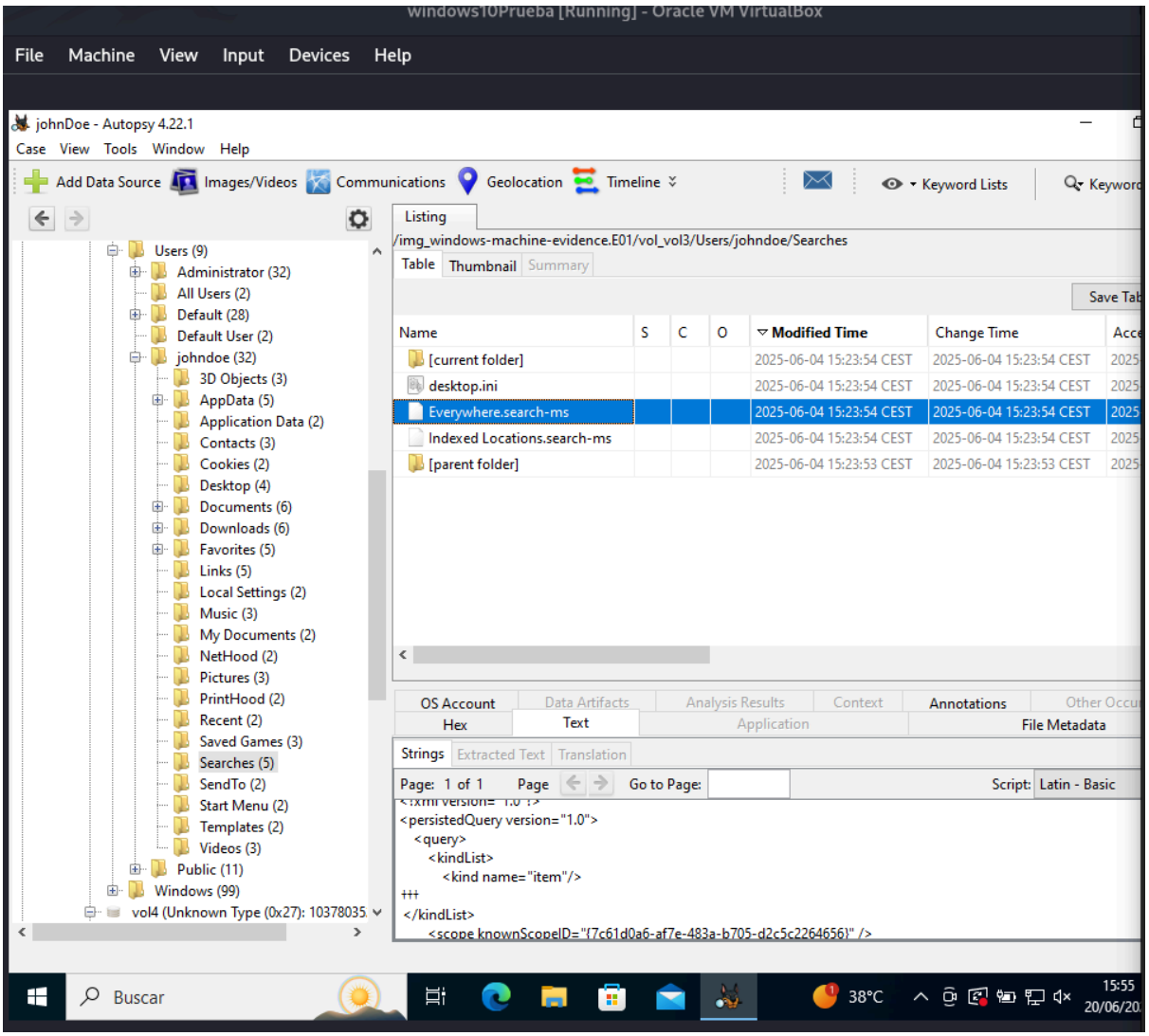


esto también es prueba de que se ha usado 7zip y el navegador edge,entre otros para el ataque

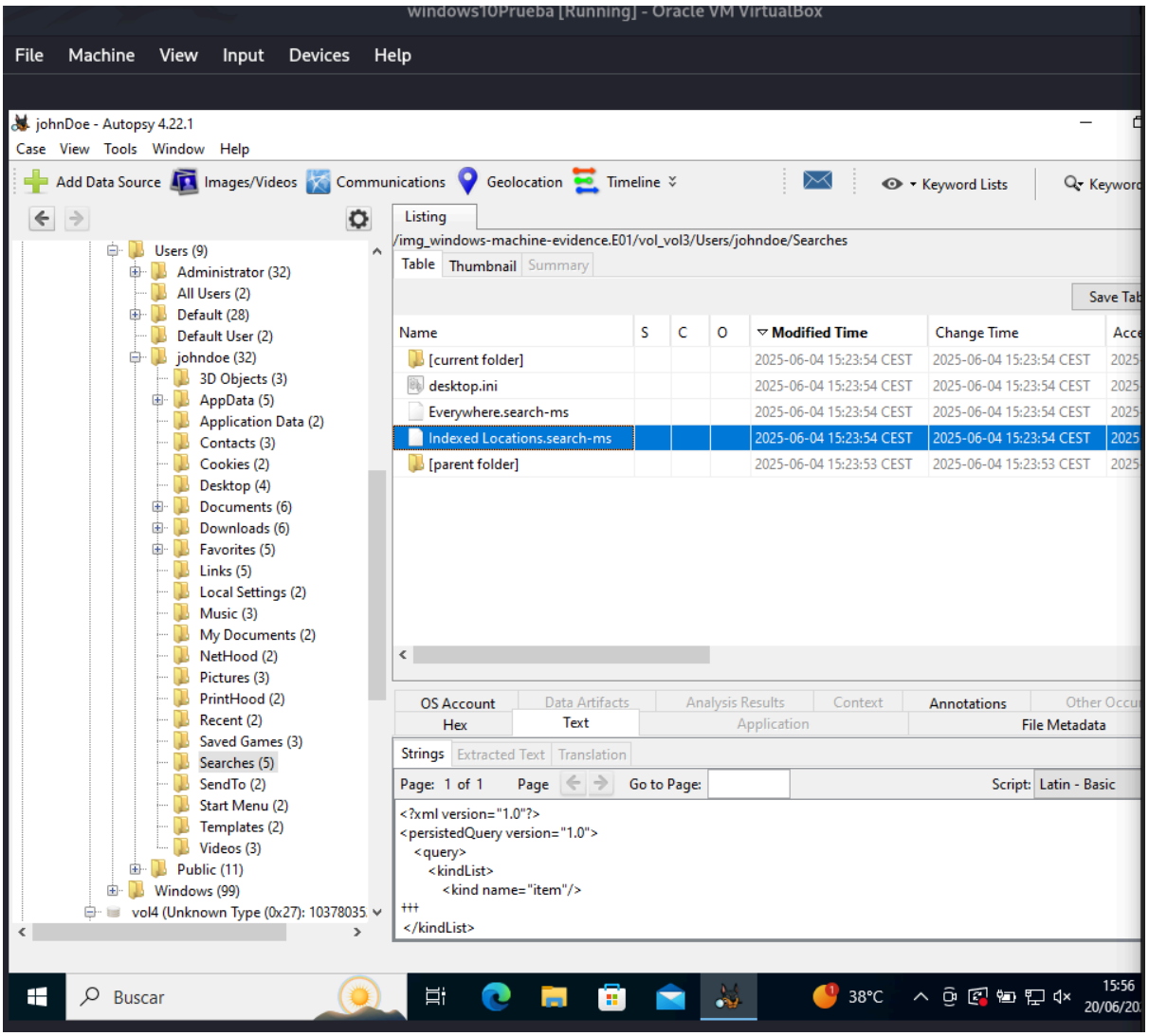
y también:


windows10Prueba [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
johnDoe - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Listing
Databases
Table Thumbnail Summary
Save Tab
Name S C O Modified Time Change Time
mpenginedb.db 2025-06-04 15:53:15 CEST 2025-06-04 15:53:15 CEST
EventStore.db 2025-06-04 15:53:12 CEST 2025-06-04 15:53:12 CEST
EventStore.db 2025-06-04 15:53:12 CEST 2025-06-04 15:53:12 CEST
wpndatabase.db 2025-06-04 15:53:11 CEST 2025-06-04 15:53:11 CEST
iconcache_256.db 2025-06-04 15:52:08 CEST 2025-06-04 15:52:08 CEST
qmgr.db 2025-06-04 15:51:18 CEST 2025-06-04 15:51:18 CEST
ActivitiesCache.db 2025-06-04 15:51:17 CEST 2025-06-04 15:51:17 CEST
wpndatabase.db 2025-06-04 15:51:17 CEST 2025-06-04 15:51:17 CEST
IconCache.db 2025-06-04 15:51:15 CEST 2025-06-04 15:51:15 CEST
cversions.1.db 2025-06-04 15:51:15 CEST 2025-06-04 15:51:15 CEST
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver 2025-06-04 15:51:15 CEST 2025-06-04 15:51:15 CEST
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Data Sources
File Views
File Types
By Extension
Images (2584)
Videos (0)
Audio (170)
Archives (2746)
Databases (95)
Documents
Executable
By MIME Type
Deleted Files
File System (28)
All (28)
File Size
Data Artifacts
Analysis Results
OS Accounts
Tags
Score
Reports
Buscar
28°C
15:18


windows10Prueba [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
johnDoe - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Listing
/img_windows-machine-evidence.E01/vol_vol3/Users/johndoe
Table Thumbnail Summary
Save Tab
Name S C O Modified Time Change Time
NTUSER.DAT 2025-06-04 15:51:17 CEST
NTUSER.DAT{c76cbcdb-afc9-11eb-8234-000d3aa6d 2025-06-04 15:51:17 CEST
Documents 2025-06-04 15:38:13 CEST
Downloads 2025-06-04 15:31:50 CEST
Desktop 2025-06-04 15:23:56 CEST
Links 2025-06-04 15:23:54 CEST
Saved Games 2025-06-04 15:23:54 CEST
Searches 2025-06-04 15:23:54 CEST
[current folder] 2025-06-04 15:23:53 CEST
3D Objects 2025-06-04 15:23:53 CEST
Contacts 2025-06-04 15:23:53 CEST
2025-06-04 1
OS Account Data Artifacts Analysis Results Context Annotations
Hex Text Application File Metadata
System Volume Information (5)
Team (3)
TeamFiles (3)
Users (9)
Administrator (32)
All Users (2)
Default (28)
Default User (2)
johndoe (32)
3D Objects (3)
AppData (5)
Application Data (2)
Contacts (3)
Cookies (2)
Desktop (4)
Documents (6)
Downloads (6)
Favorites (5)
Links (5)
Local Settings (2)
Music (3)
My Documents (2)
NetHood (2)
Pictures (3)
PrintHood (2)
Recent (2)
Saved Games (3)
Searches (5)
SendTo (2)
Start Menu (2)
Templates (2)
Videos (3)
Public (11)
Buscar
28°C
15:23



En esta imagen es donde se encuentran las evidencias que el ataque se ha realizado por web.


windows10Prueba [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
johnDoe - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Users (9)
Administrator (32)
All Users (2)
Default (28)
Default User (2)
johndoe (32)
3D Objects (3)
AppData (5)
Application Data (2)
Contacts (3)
Cookies (2)
Desktop (4)
Documents (6)
Downloads (6)
Favorites (5)
Links (5)
Local Settings (2)
Music (3)
My Documents (2)
NetHood (2)
Pictures (3)
PrintHood (2)
Recent (2)
Saved Games (3)
Searches (5)
SendTo (2)
Start Menu (2)
Templates (2)
Videos (3)
Public (11)
Windows (99)
vol4 (Unknown Type (0x27): 10378035
Listing
/img_windows-machine-evidence.E01/vol_vol3/Users/johndoe/Searches
Table Thumbnail Summary
Save Tab
Name S C O Modified Time Change Time
[current folder] 2025-06-04 15:23:54 CEST 2025-06-04 15:23:54 CEST
desktop.ini 2025-06-04 15:23:54 CEST 2025-06-04 15:23:54 CEST
Everywhere.search-ms 2025-06-04 15:23:54 CEST 2025-06-04 15:23:54 CEST
Indexed Locations.search-ms 2025-06-04 15:23:54 CEST 2025-06-04 15:23:54 CEST
[parent folder] 2025-06-04 15:23:53 CEST 2025-06-04 15:23:53 CEST
OS Account Data Artifacts Analysis Results Context Annotations
Hex Text Application File Metadata
Strings Extracted Text Translation
Page: 1 of 1 Page Go to Page: Script: Latin - Basic
<?xml version="1.0"?>
<persistedQuery version="1.0">
<query>
<kindList>
<kind name="item"/>
</kindList>
Buscar
38°C
15:56