

**INFORME ANÁLISIS FORENSE -**

**XXXXX EJEMPLO**

**Preparado para: EMPRESA EL WILLY S.A.C**

**Fecha: 15 de Agosto del 2017**

**El presente documento contiene información estrictamente privada y confidencial**

# ÍNDICE

ÍNDICE...................................................................................................................................2 OBJETIVO..............................................................................................................................3 ALCANCE..............................................................................................................................3

|  |  |  |  |
| --- | --- | --- | --- |
|  | Formato | Documento Nº: CYS-FOR-14 | |
| Versión : 01 | 2 de 49 |
| **ANÁLISIS DE ANÁLISIS FORENSE** | | | |

PROCESO DE IDENTIFICACIÓN Y PRESERVACIÓN........................................................4

PROCESO DE ADQUISICIÓN DE EVIDENCIA....................................................................5

PROCESO DE BÚSQUEDA Y ANÁLISIS DE LA EVIDENCIA..............................................7

Proceso de Indexación.......................................................................................................7

Búsqueda y Análisis............................................................................................................8

Registro de Eventos Relacionados.............................................................................10

CONCLUSIONES................................................................................................................46

# OBJETIVO

El presente informe técnico tiene como objetivo principal evidenciar el origen del incidente en el equipo marca XXXXX, modelo X XXXX, y con número de serie XXXXXXX proporcionada por la parte solicitante e identificar sus comportamientos y el impacto que tuvo.

# ALCANCE

De acuerdo al incidente reportado el alcance del análisis forense estuvo centrado a lo siguiente:

* Detectar el origen del ataque y si hubo un compromiso en el sistema o red.

Artefactos analizados:

* Logs de Eventos de Windows: System, Security, entre otros.
* Registro de Windows: SOFTWARE, SYSTEM, NTUSER.DAT, SAM y USRCLASS
* Ejecución de archivos: AmCache, ShimCache.
* Actividad de usuario: MFT, UserAsist.
* Registros

# PROCESO DE IDENTIFICACIÓN Y PRESERVACIÓN

Se ha realizado la identificación plena del equipo de cómputo tipo laptop, marca **XXXX**, modelo **XXXX**, y con número de serie **XXXXXX** cuya identificación se muestra a continuación:

Se ha verificado que cuenta con una única unidad de almacenamiento interno de estado sólido que es de tipo **XXXX** de marca **XXX**, modelo **XX**, número de serie **xxxxx**y de **xxxxx** capacidad de almacenamiento.

ADJUNTAR IMAGEN

# PROCESO DE ADQUISICIÓN DE EVIDENCIA

Se ha procedido a realizar la imagen forense (copia espejo /copia forense) de la unidad de almacenamiento previamente identificada, para lo cual se ha utilizado xxxxxxxx, el mismo garantiza mantener la integridad de los datos del dispositivo de almacenamiento origen, así como la generación automática de su firma HASH como elemento de seguridad digital. Durante el proceso de creación de imagen forense (Copia espejo/copia forense) se evidencio que las particiones lógicas que se encuentran en la unidad de almacenamiento están cifradas, por tal motivo no es posible identificar el sistema de archivos de las particiones tal como se puede visualizar a continuación:

Posteriormente se procedió a realizar una imagen forense (copia espejo /copia forense) a la unidad de almacenamiento previamente identificada, para lo cual se ha utilizado Duplicador Forense Tableau TX1, el mismo garantiza mantener la integridad de los datos del dispositivo de almacenamiento origen, así como la generación automática de su firma HASH como elemento de seguridad digital.

INSERTAR IMAGEN HASH

# PROCESO DE BÚSQUEDA Y ANÁLISIS DE LA EVIDENCIA

## Proceso de Indexación

En el proceso de indexación (extracción de la imagen forense) se ha utilizado un bloqueador de escritura por hardware marca Tableau para garantizar el aseguramiento de la información contenida en la imagen forense, y para el procesamiento se ha utilizado el software de análisis forense Magnet Axiom V.6.3.0.32040, que se ha configurado con el nivel más completo de decodificación, es decir, incluye la posibilidad de realizar recuperación de data eliminada

Al momento de agregar el archivo de imagen forense, se ha evidenciado que la unidad de almacenamiento cuenta con particiones:

INSERTAR IMAGEN

## Búsqueda y Análisis

### EJEMPLOS DE ARCHIVOS ANALIZADOS:

### NTUSER.DAT

El **ntuser.dat** es un archivo de configuración que guarda información de los comportamientos de Windows y de igual manera nos almacena la información del primer inicio de sesión de los usuarios creados en el sistema.

### NTUSER.DAT.LOG1

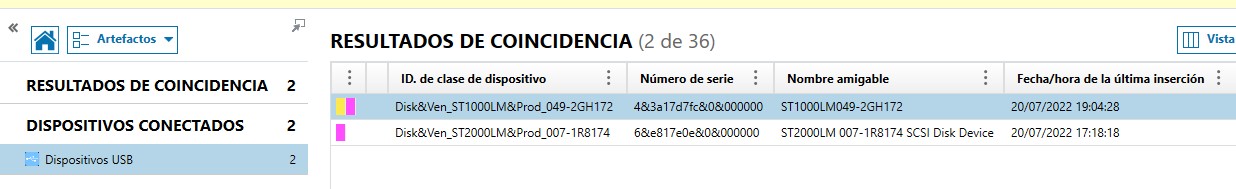
Este archivo contiene información de configuración de cuentas, carpetas y diseño de Windows, además, almacena todos los cambios durante una sesión en vivo dentro de una copia de

NTUSER.DAT denominado NTUSER.DAT.LOG1

### Registro de Eventos Relacionados

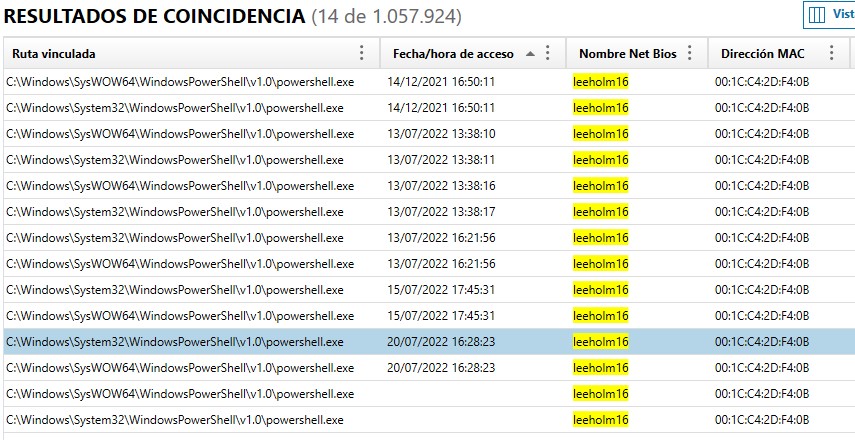
#### • DISPOSITIVOS CONECTADOS

Dentro de la categoría / **DISPOSITIVOS USB** se evidencio que en fecha 20 de julio del 2020 se realizó la conexión con dos dispositivos de almacenamiento, la primera correspondiente a las17:18 horas, y la segunda a las 19:04 horas; los detalles se presentan a continuación:

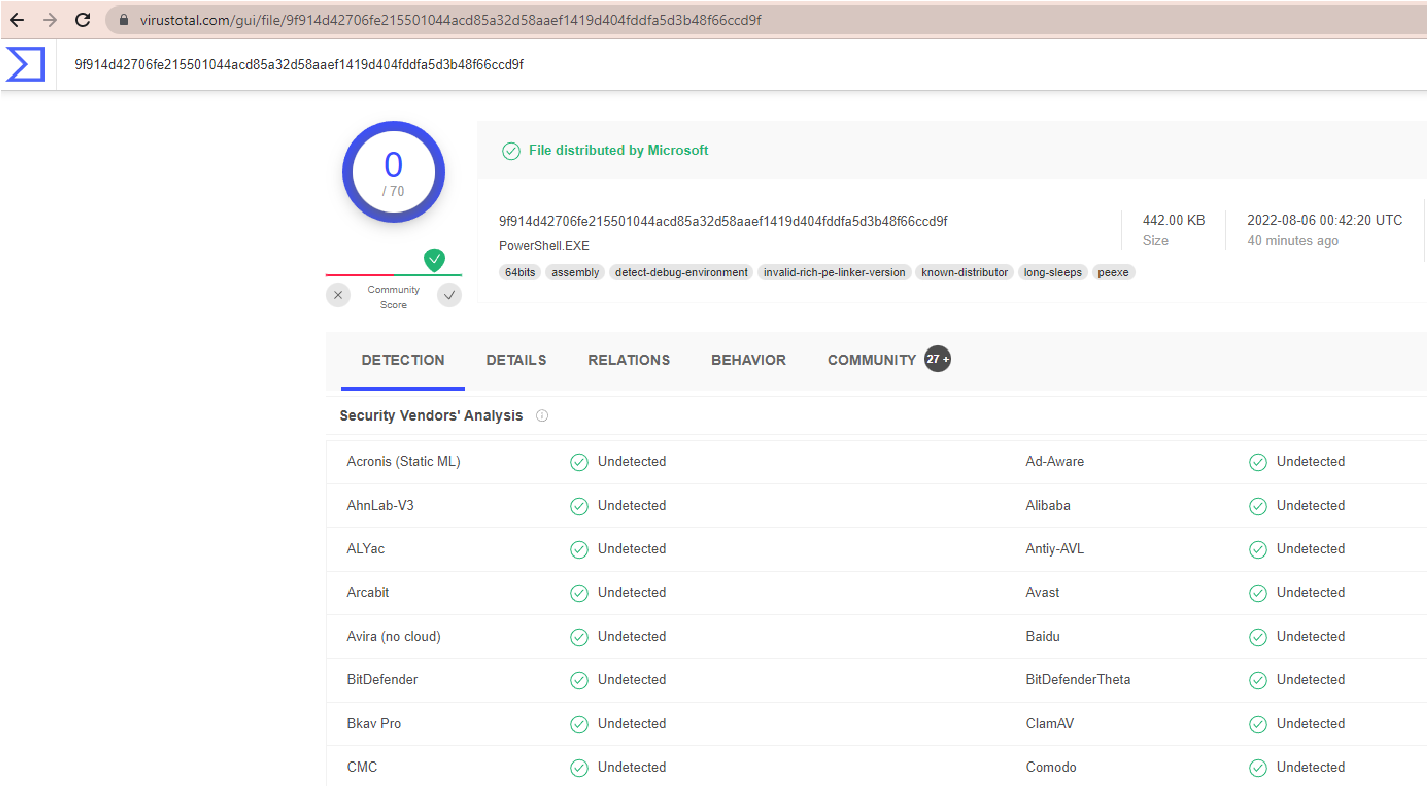


#### • REGISTROS LINK

Se ha verificado que existen catorce (14) registros de enlace (LNK) al ejecutable PowerShell.exe, inclusive, una conexión en fecha 20 de julio del 2020 a las 16:28 horas, el registro indica haberse realizado desde un equipo remoto identificado como ‘leeholm16’ que cuenta con una dirección de red MAC ‘00:1C:C4:2D:F4:08’.

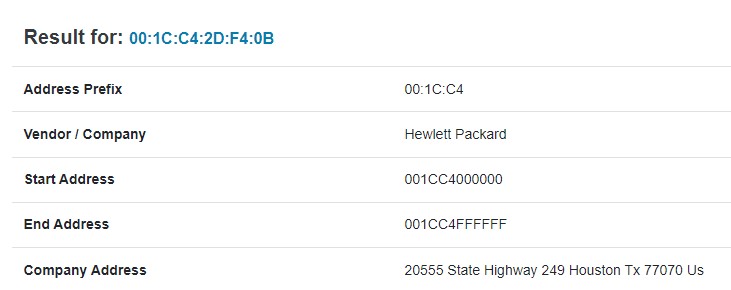


Se ha extraído el archivo correspondiente al ejecutable PowerShell.exe, para verificar si se encuentra o no con algún tipo de infección maliciosa (malware), del resultado del análisis realizado en la plataforma ‘virustotal.com’ se ha obtenido como resultado que no tiene ningún tipo de infección maliciosa.



Se ha realizado la búsqueda de relación de fabricante al adaptador de red con dirección

MAC ‘00:1C:C4:2D:F4:08’, el cual se ha obtenido como respuesta que el fabricante es ‘Hewlett Packard’



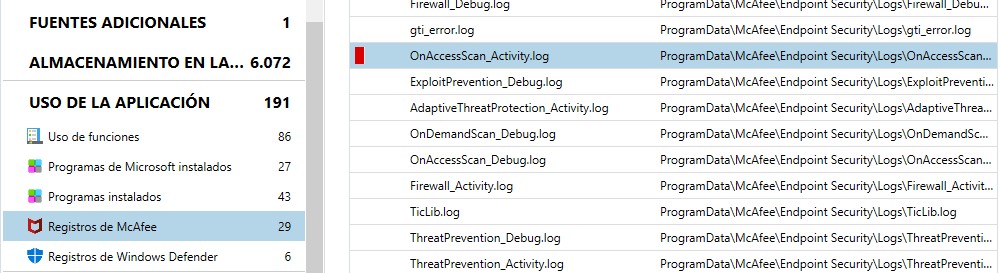
#### • EVENTOS PREVIOS AL PRIMER REGISTRO ALMACENADO EN EL LOG DE LA APLICACION XXXXX

Se ha verificado que en la categoría CUENTAS DE USUARIO – WINDOWS existe un inicio de sesión por el usuario “**XXXXX**” (perteneciente al grupo de administradores) en fecha XX de XX del XX a las 03:20:59 horas, el cual accedió minutos antes del primer registro de actividades de la aplicación XXXX como se puede visualizar en la siguiente imagen.

INSERTAR IMAGEN

#### • REGISTROS DE XXXX Y EVENTOS RELACIONADOS

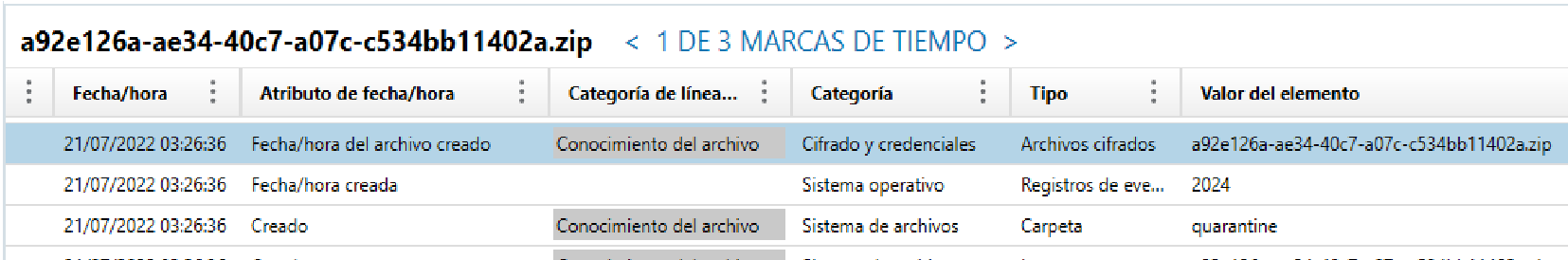
De la categoría **USO DE LA APLICACIÓN / REGISTRO DE XXXX** se obtuvo el archivo del registro de actividades de la aplicación McAfee



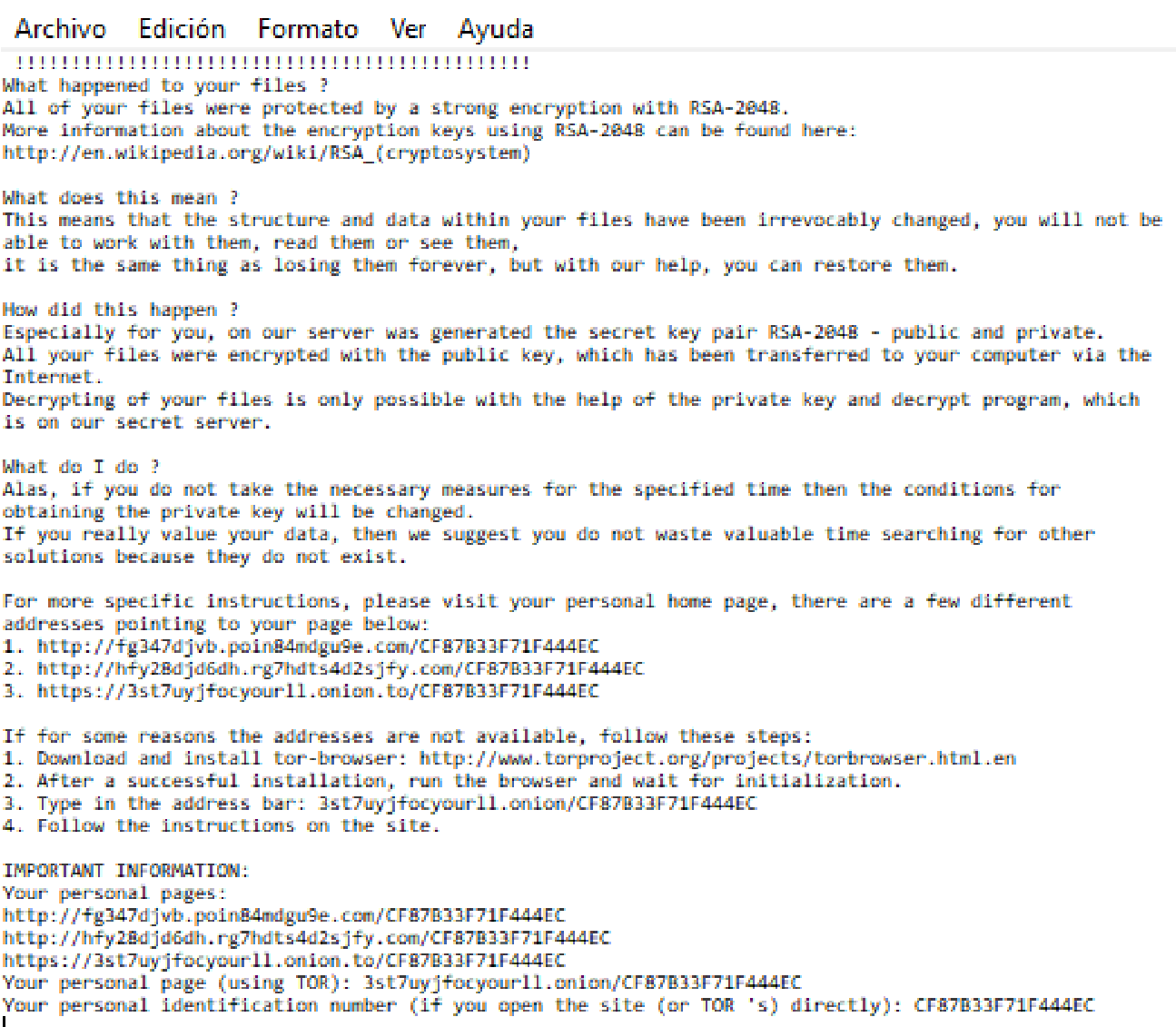
#### ◦ REGISTRO : 21-0XX7-XX – 03:26:XX

Al ejecutarse la primera actividad del archivo de texto “howto\_recover\_file\_suuao.txt” se creó un archivo en C:\Quarantine/quarantine/a92e126a-ae34-40c7-a07cc534bb11402a.zip, dentro de esta ruta se encuentra el archivo de texto detectado como infectado: “howto\_recover\_file\_suuao.txt”, este registro se crea a partir del acceso al directorio D:\DISCO D\DISCO D\Mis Documentos\howto\_recover\_file\_suuao.txt.

◦ En la categoría línea de tiempo se identificó la fecha y hora de la creación del archivo a92e126a-ae34-40c7-a07c-c534bb11402a.zip almacenado en la carpeta “QUARANTINE”.



A continuación, se presenta los detalles del archivo **a92e126a-ae34-40c7-a07cc534bb11402a.zip,** así como el contenido del archivo “.txt”.



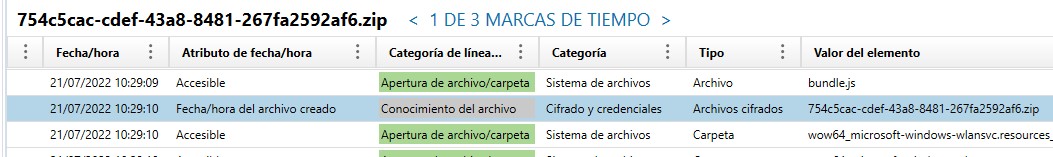
#### ◦ REGISTRO : 2020-07-21 - 10:29:12

Al ejecutarse la segunda actividad del archivo de texto “howto\_recover\_file\_suuao.txt” se creó un archivo en C:\Quarantine/quarantine/754c5cac-cdef-43a8-8481267fa2592af6.zip, , dentro de esta ruta se encuentra el archivo de texto detectado como infectado: “howto\_recover\_file\_suuao.txt”, este registro se crea a partir del acceso al directorio D:\DISCO D\DISCO D\MI CARPETA\howto\_recover\_file\_suuao.txt

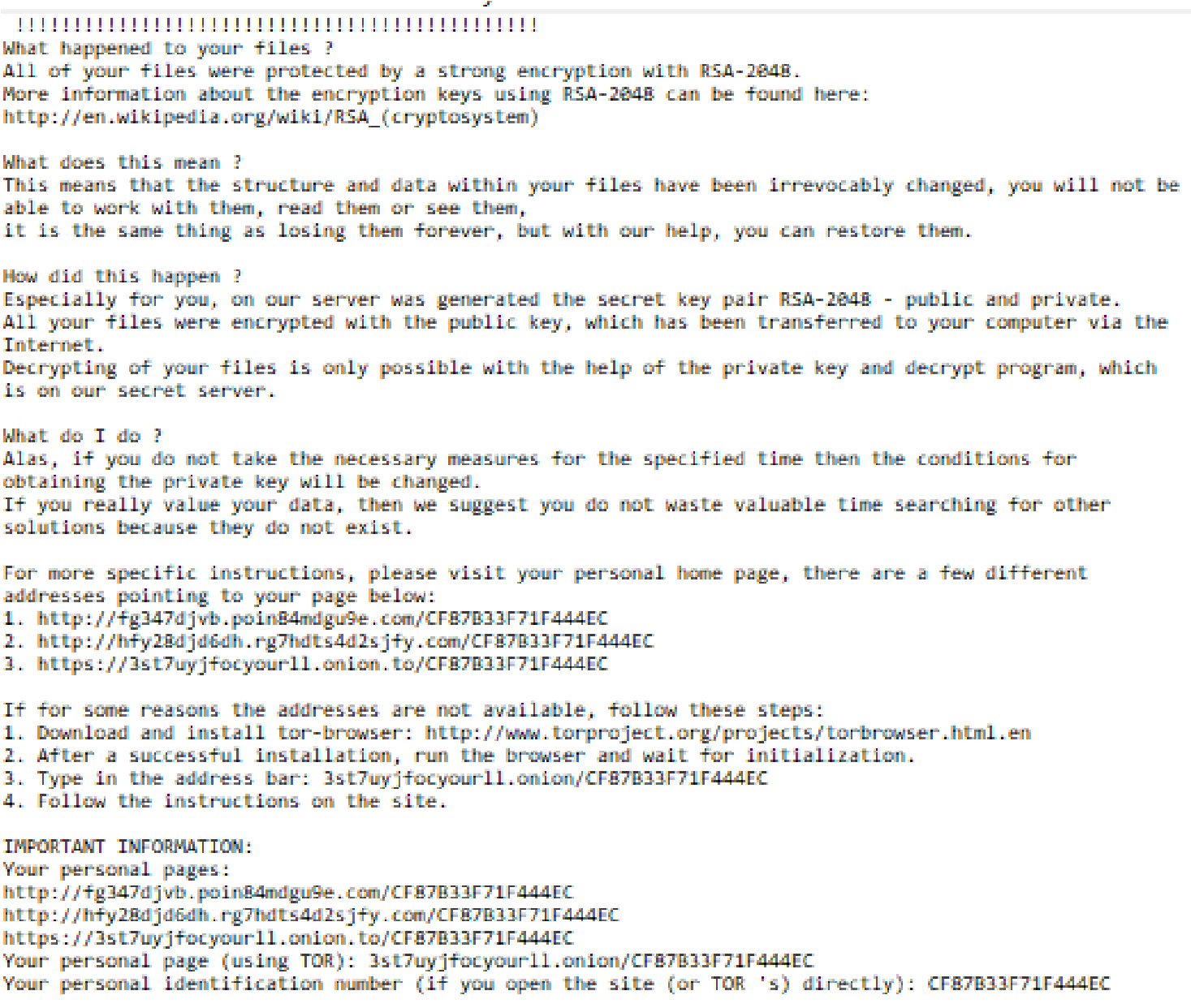
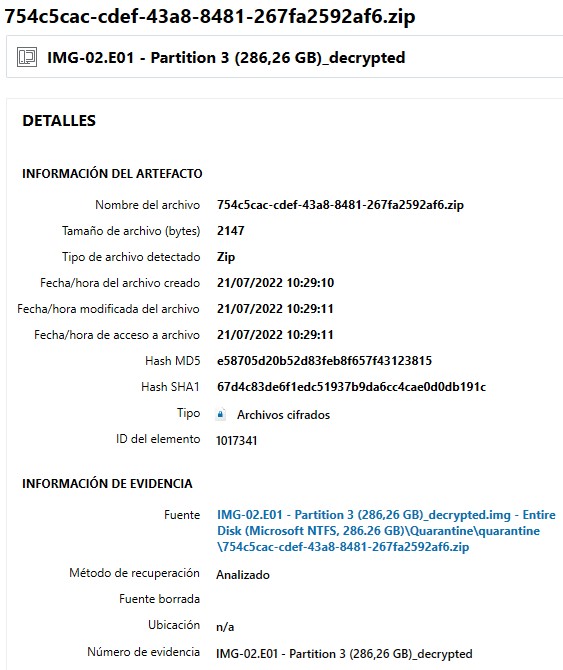
En la categoría línea de tiempo se identificó la fecha y hora de la creación del archivo

754c5cac-cdef-43a8-8481-267fa2592af6.zip almacenado en la carpeta

“QUARANTINE”.



A continuación, se presenta los detalles del archivo 754c5cac-cdef-43a8-8481267fa2592af6.zip, así como el contenido del archivo “.txt”.

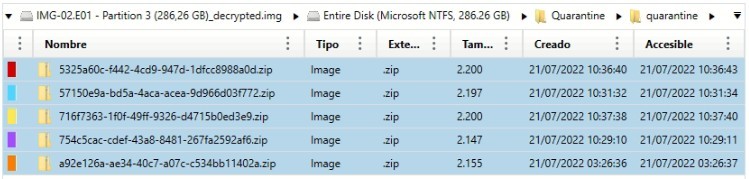
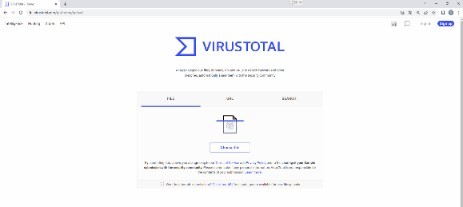


#### ◦

#### ◦ ANALISIS DE MALWARE

De los cinco (05)archivos comprimidos de tipo “Zip” almacenados en el directorio “**C:\ Quarantine\ quarantine**” se exportaron todos los archivos para un respectivo análisis de malware en el servicio web “**VirusTotal**” de dominio

“**https://www.virustotal.com/gui/home/upload**”, tal como se puede apreciar a continuación:

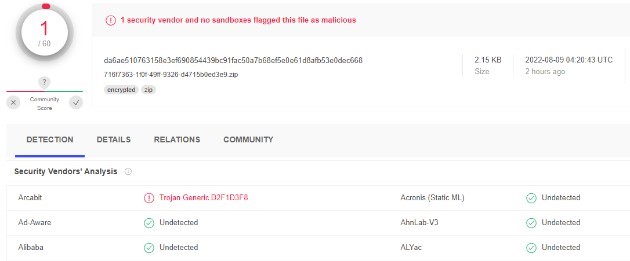


#### ▪ ANALISIS DE MALWARE “716f7363-1f0f-49ff-9326-d4715b0ed3e9.zip”

Al analizar el archivo comprimido de etiqueta “**716f7363-1f0f-49ff-9326d4715b0ed3e9.zip**” se evidencio que el servicio web “**VirusTotal**” reconoció una

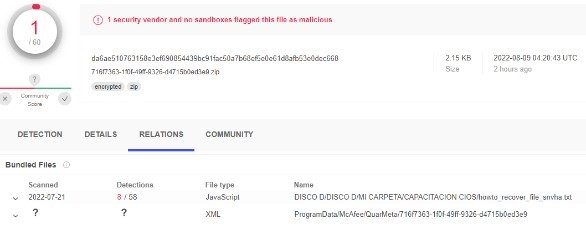
(01) coincidencia de malware en su base de datos con el nombre

“**Trojan.Generic.D2F1D3F8**”, tal como se puede apreciar a continuación:



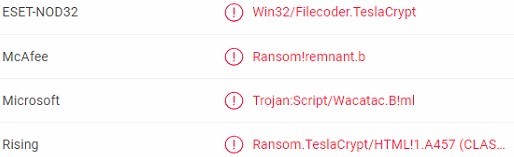
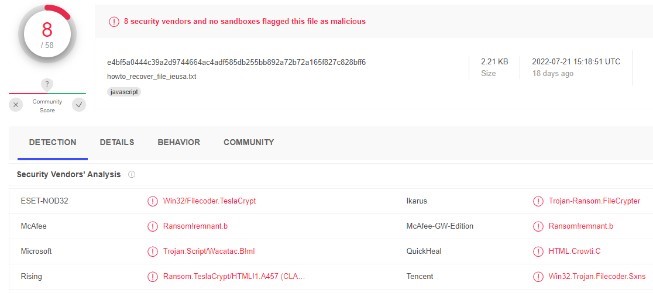
Al analizar el contenido almacenado en el archivo comprimido de etiqueta “**716f7363-1f0f-49ff-9326-d4715b0ed3e9.zip**” con el servicio web "**VirusTotal**", se constató la existencia del archivo “**DISCO D/DISCO D/MI**

**CARPETA/CAPACITACION CIOS/howto\_recover\_file\_snvha.txt**”, tal como se puede apreciar a continuación:



Se evidencio que cuenta con ocho (08) coincidencias de malware en la base de datos del servicio web “**VirusTotal**”. A continuación, se detallan las coincidencias en relación con las firmas de virus identificadas:

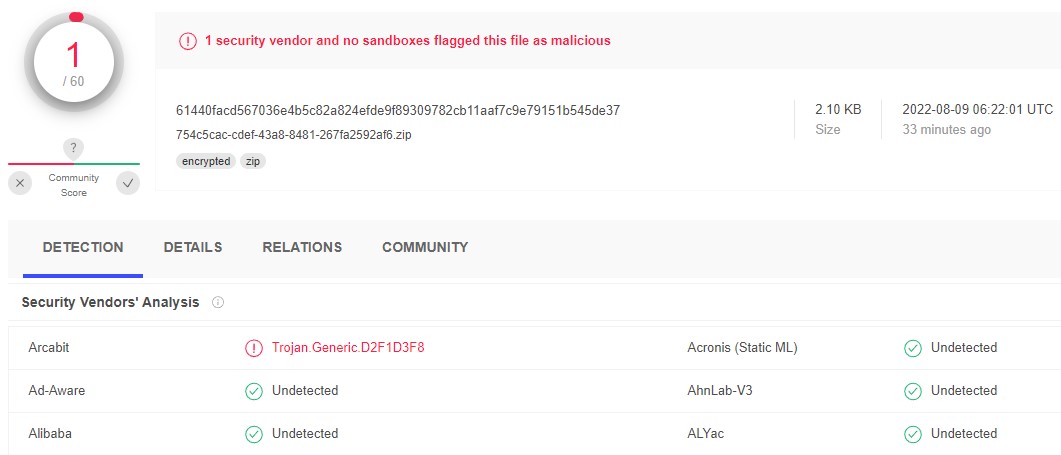
|  |  |
| --- | --- |
| **ANTIVIRUS** | **FIRMAS DE VIRUS COINCIDENTES** |
| ESET-NOD32 | Win32/Filecoder.TeslaCrypt |
| McAfee | Ransom!remnant.b |
| Microsoft | Trojan:Script/Wacatac.B!ml |
| Rising | Ransom.TeslaCrypt/HTML!1.A457 (CLASSIC) |
| Ikaru | Trojan-Ransom.FileCrypter |
| McAfee-GW-Edition | Ransom!remnant.b |
| QuickHeal | HTML.Crowti.C |
| Tencent | Win32.Trojan.Filecoder.Sxns |



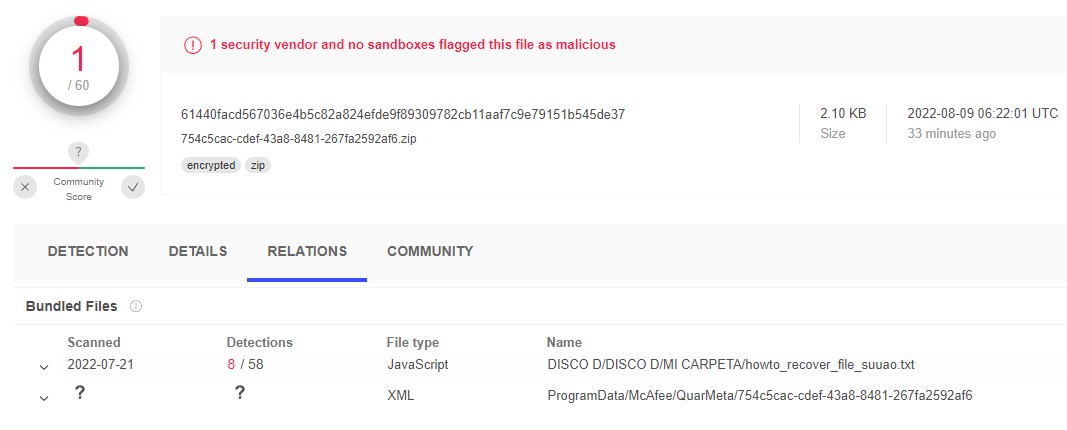
#### ▪ ANALISIS DE MALWARE “754c5cac-cdef-43a8-8481-267fa2592af6.zip”

Al analizar el archivo comprimido de etiqueta “**754c5cac-cdef-43a8-8481267fa2592af6.zip**” se evidencio que el servicio web “**VirusTotal**” reconoció una (01) coincidencia de malware en su base de datos con el nombre

“**Trojan.Generic.D2F1D3F8**”, tal como se puede apreciar a continuación:

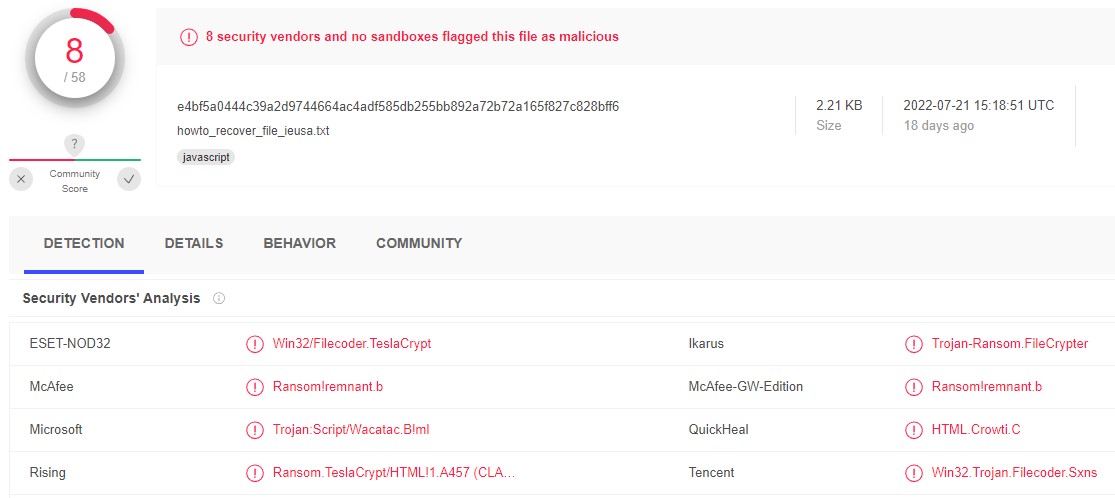


Al analizar el contenido almacenado en el archivo comprimido de etiqueta “**754c5cac-cdef-43a8-8481-267fa2592af6.zip**” con el servicio web "**VirusTotal**", se constató la existencia del archivo “**DISCO D/DISCO D/MI CARPETA/howto\_recover\_file\_suuao.txt**”, tal como se puede apreciar a continuación:



Se evidencio que cuenta con ocho (08) coincidencias de malware en la base de datos del servicio web “**VirusTotal**”. A continuación, se detallan las coincidencias en relación con las firmas de virus identificadas:

|  |  |
| --- | --- |
| **ANTIVIRUS** | **FIRMAS DE VIRUS COINCIDENTES** |
| ESET-NOD32 | Win32/Filecoder.TeslaCrypt |
| McAfee | Ransom!remnant.b |
| Microsoft | Trojan:Script/Wacatac.B!ml |
| Rising | Ransom.TeslaCrypt/HTML!1.A457 (CLASSIC) |
| Ikaru | Trojan-Ransom.FileCrypter |
| McAfee-GW-Edition | Ransom!remnant.b |
| QuickHeal | HTML.Crowti.C |
| Tencent | Win32.Trojan.Filecoder.Sxns |



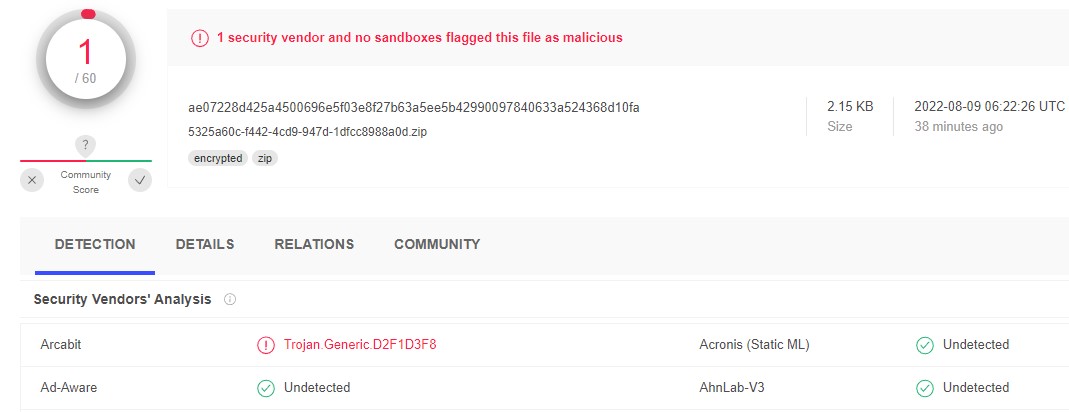
#### ▪ ANALISIS DE MALWARE “5325a60c-f442-4cd9-947d-1dfcc8988a0d.zip”

Al analizar el archivo comprimido de etiqueta “**5325a60c-f442-4cd9-947d-**

**1dfcc8988a0d.zip**” se evidencio que el servicio web “**VirusTotal**” reconoció una

(01) coincidencia de malware en su base de datos con el nombre

“**Trojan.Generic.D2F1D3F8**”, tal como se puede apreciar a continuación:



Al analizar el contenido almacenado en el archivo comprimido de etiqueta “**5325a60c-f442-4cd9-947d-1dfcc8988a0d.zip**” con el servicio web "**VirusTotal**", se constató la existencia del archivo “**DISCO D/DISCO D/MI CARPETA/CAPACITACION CIOS/howto\_recover\_file\_ieusa.txt**”, tal como se puede apreciar a continuación:

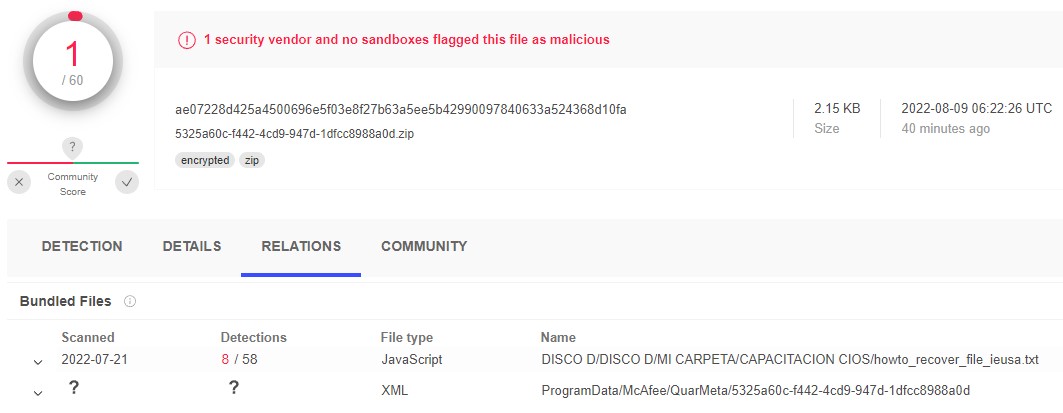
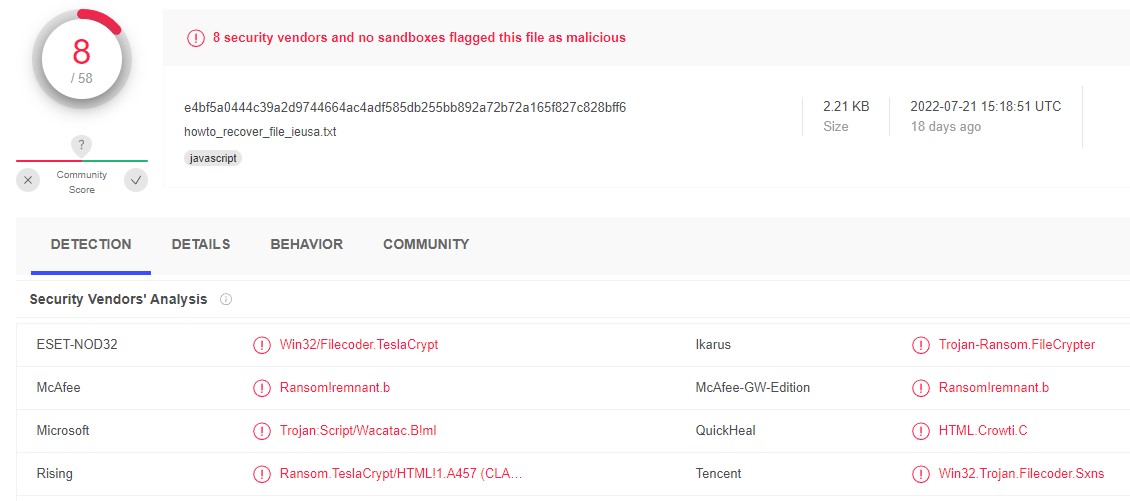


Imagen Contenido almacenado en archivo comprimido " 5325a60c-f442-4cd9-947d1dfcc8988a0d.zip"

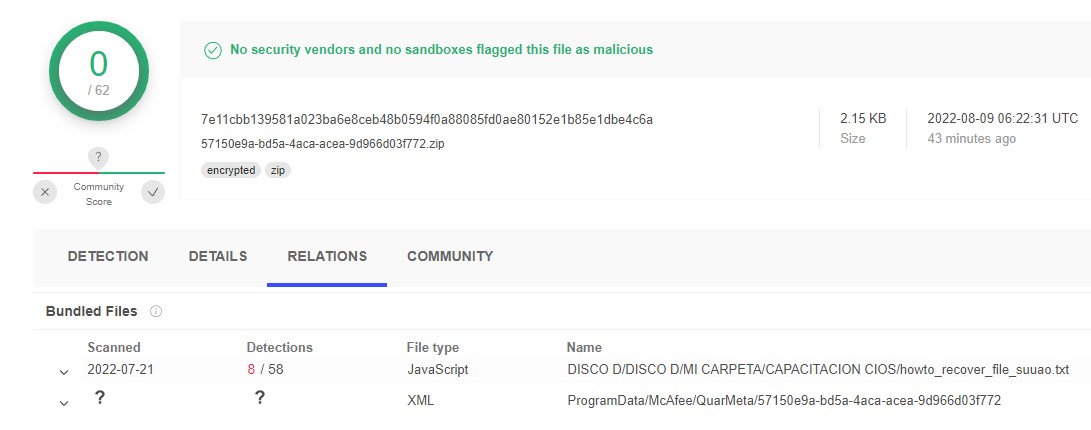
Se evidencio que cuenta con ocho (08) coincidencias de malware en la base de datos del servicio web “**VirusTotal**”. A continuación, se detallan las coincidencias en relación con las firmas de virus identificadas:

|  |  |
| --- | --- |
| **ANTIVIRUS** | **FIRMAS DE VIRUS COINCIDENTES** |
| ESET-NOD32 | Win32/Filecoder.TeslaCrypt |
| McAfee | Ransom!remnant.b |
| Microsoft | Trojan:Script/Wacatac.B!ml |
| Rising | Ransom.TeslaCrypt/HTML!1.A457 (CLASSIC) |
| Ikaru | Trojan-Ransom.FileCrypter |
| McAfee-GW-Edition | Ransom!remnant.b |
| QuickHeal | HTML.Crowti.C |
| Tencent | Win32.Trojan.Filecoder.Sxns |



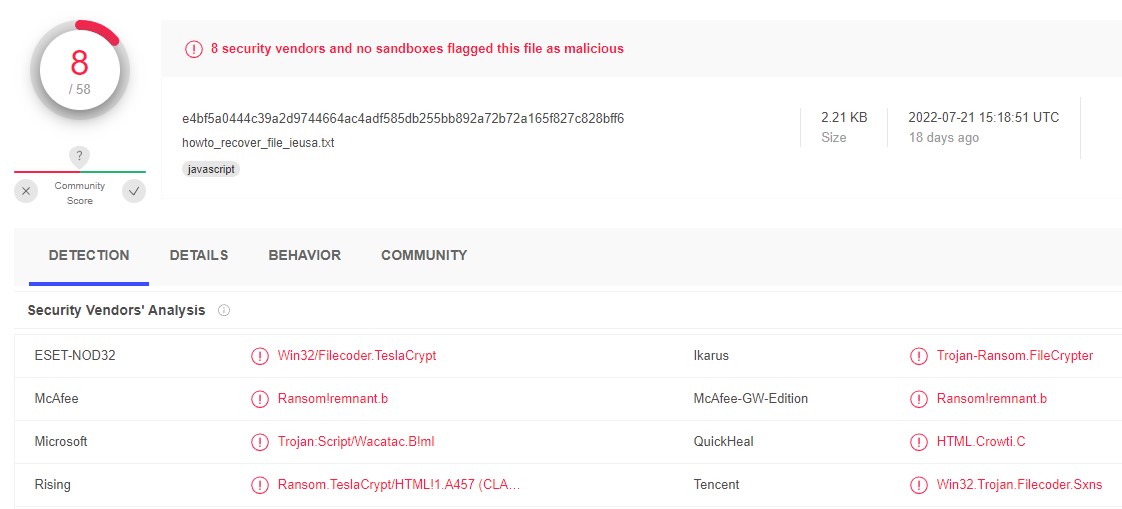
#### ▪ ANALISIS DE MALWARE “57150e9a-bd5a-4aca-acea-9d966d03f772.zip”

Al analizar el contenido almacenado en el archivo comprimido de etiqueta “**57150e9a-bd5a-4aca-acea-9d966d03f772.zip**” con el servicio web "**VirusTotal**", se constató la existencia del archivo “**DISCO D/DISCO D/MI CARPETA/CAPACITACION CIOS/howto\_recover\_file\_suuao.txt**”, tal como se puede apreciar a continuación:



Se evidencio que cuenta con ocho (08) coincidencias de malware en la base de datos del servicio web “**VirusTotal**”. A continuación, se detallan las coincidencias en relación con las firmas de virus identificadas:

|  |  |
| --- | --- |
| **ANTIVIRUS** | **FIRMAS DE VIRUS COINCIDENTES** |
| ESET-NOD32 | Win32/Filecoder.TeslaCrypt |
| McAfee | Ransom!remnant.b |
| Microsoft | Trojan:Script/Wacatac.B!ml |
| Rising | Ransom.TeslaCrypt/HTML!1.A457 (CLASSIC) |
| Ikaru | Trojan-Ransom.FileCrypter |
| McAfee-GW-Edition | Ransom!remnant.b |
| QuickHeal | HTML.Crowti.C |
| Tencent | Win32.Trojan.Filecoder.Sxns |

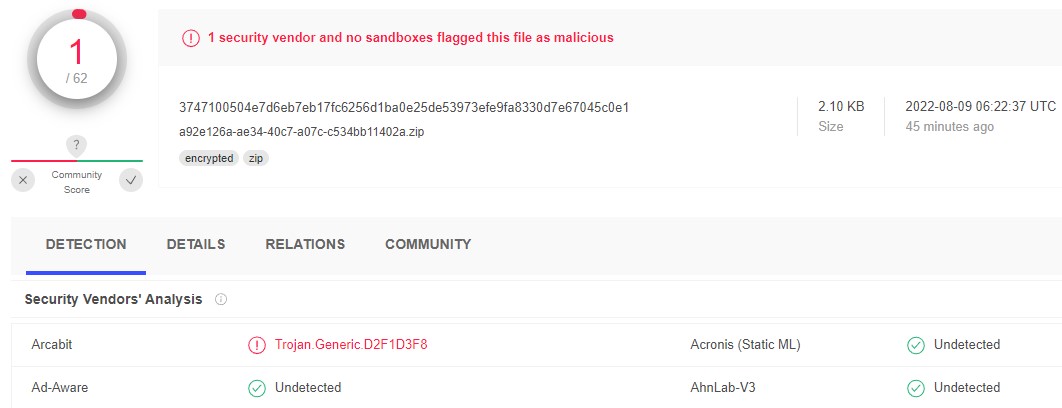


#### ▪ ANALISIS DE MALWARE “a92e126a-ae34-40c7-a07c-c534bb11402a.zip”

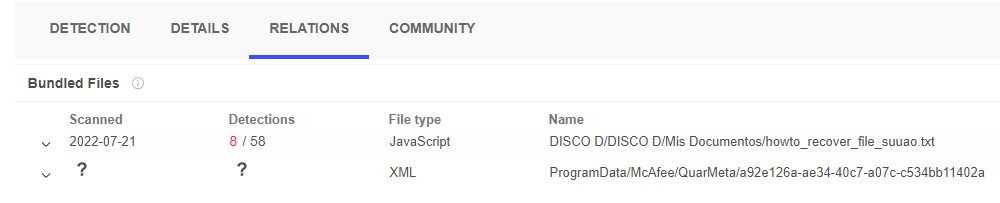
Al analizar el archivo comprimido de etiqueta “**a92e126a-ae34-40c7-a07cc534bb11402a.zip**” se evidencio que el servicio web “**VirusTotal**” reconoció una

(01) coincidencia de malware en su base de datos con el nombre

“**Trojan.Generic.D2F1D3F8**”, tal como se puede apreciar a continuación:

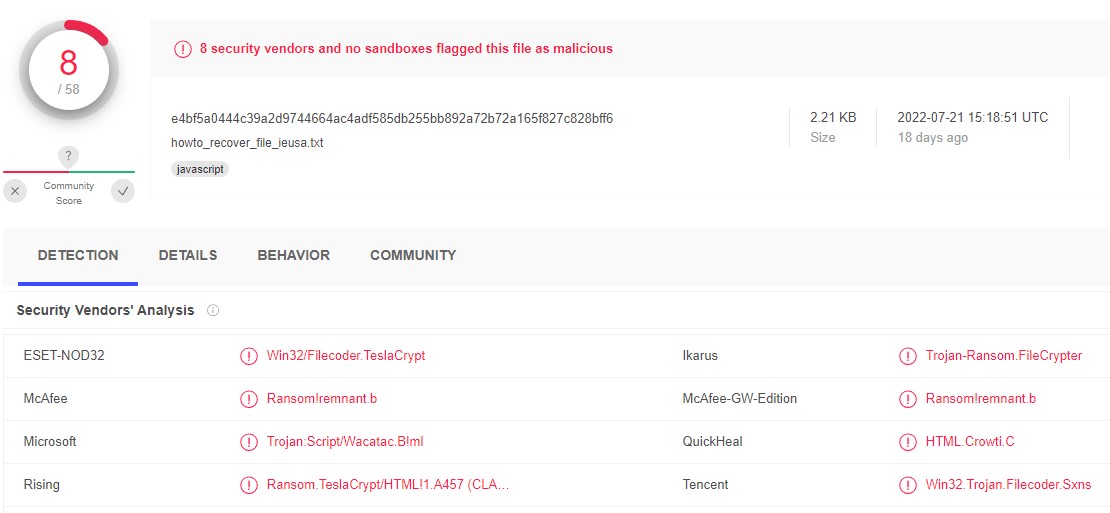


Al analizar el contenido almacenado en el archivo comprimido de etiqueta “**a92e126a-ae34-40c7-a07c-c534bb11402a.zip**” con el servicio web "**VirusTotal**", se constató la existencia del archivo “**DISCO D/DISCO D/MI CARPETA/CAPACITACION CIOS/howto\_recover\_file\_snvha.txt**”, tal como se puede apreciar a continuación:



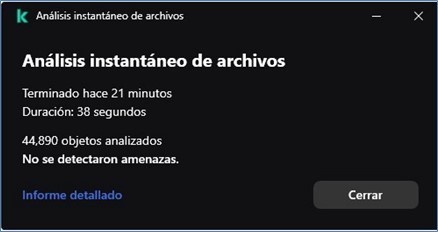
Se evidencio que cuenta con ocho (08) coincidencias de malware en la base de datos del servicio web “**VirusTotal**”. A continuación, se detallan las coincidencias en relación con las firmas de virus identificadas:

|  |  |
| --- | --- |
| **ANTIVIRUS** | **FIRMAS DE VIRUS COINCIDENTES** |
| ESET-NOD32 | Win32/Filecoder.TeslaCrypt |
| McAfee | Ransom!remnant.b |
| Microsoft | Trojan:Script/Wacatac.B!ml |
| Rising | Ransom.TeslaCrypt/HTML!1.A457 (CLASSIC) |
| Ikaru | Trojan-Ransom.FileCrypter |
| McAfee-GW-Edition | Ransom!remnant.b |
| QuickHeal | HTML.Crowti.C |
| Tencent | Win32.Trojan.Filecoder.Sxns |



#### ◦ ANALISIS DE MALWARE – COPIA LOGICA CONTENIDO EN “D:\”

Se realizo la copia lógica del contenido almacenado en la unidad lógica “D:\**”** para su posterior análisis de malware con el software antivirus **Kaspersky V. 21.7** con la base de datos de malware actualizaday se evidencio que no almacena archivos infectados o maliciosos.



#### ◦ ANALISIS DE ARCHIVOS DIGITALES CON EXTENSION “. CCC” – COPIA LOGICA CONTENIDO EN “D:\”

A partir de haber realizado una copia lógica a la partición ¨D:\¨ y haber indexado por la herramienta forense Magnet Axiom V.6.3.0.32040, se ha verificado que existen cuatrocientos cincuenta y cuatro (454) archivos digitales que al final de su extensión de formato nativo cuenta con caracteres no reconocidos, siendo la extensión alterada ‘\*.ccc’, esta evidencia indica que estos archivos han sido afectados por un código malicioso (malware) y que ha cifrado su contenido de información.

De los cuatrocientos cincuenta y cuatro (454) archivos digitales solo cuatrocientos cincuenta y dos (452) archivos tienen como fecha/hora de creación y acceso el XX de XX del XX entre las XX:19 y XX:24 horas, y los otros dos (02) archivos indican tener fecha 16 de diciembre del 2021 a las X:28:28 y X:28:29. Sin embargo, la fecha de modificación de los cuatrocientos cincuenta y dos (452) corresponden al 28 de octubre del 2015 entre las 13:22 y 13:23 horas. Se debe entender que los campos de creación y acceso corresponden a la fecha en la que se han creado como nuevos documentos en la unidad de almacenamiento destino empleada para su copiado, y respecto a la columna de modificación correspondería a la ultima fecha de modificación que presentaba el archivo origen.

Respecto a la fecha 3 de agosto del 2020, presente en la columna de creación y acceso, se precisa que corresponde al día en que se encendió e inicializo el sistema operativo del computador para realizar la copia lógica de los archivos de la partición

¨D:\¨.

A continuación, se detallará la evidencia hallada:

INSERTAR LA IMAGEN

# CONCLUSIONES

* NO SE HA PODIDO ACCEDER A LA PARTICION “D:/” DE LA IMAGEN FORENSE CREADA DE UNIDAD DE ALMACENAMIENTO DEL EQUIPO DE COMPUTO PROPORCIONADO POR LA PARTE SOLICTANTE POR ENCONTRARSE CIFRADA.
* SE EVIDENCIÓ QUE DENTRO DEL ARCHIVO

**/USERS/XXXX/NTUSER.DAT.LOG1** SE HA ENCONTRADO EL TEXTO “HOWTO\_RECOVER\_FILE”, EL CUAL GUARDA RELACIÓN CON LA NOMENCLATURA DE LOS ARCHIVOS “TXT” QUE SE HAN IDENTIFICADO COMO MALWARE.

* SE EVIDENCIO QUE EN FECHA XX DE XX DEL XX SE REALIZÓ LA CONEXIÓN CON DOS DISPOSITIVOS DE ALMACENAMIENTO, LA PRIMERA CORRESPONDIENTE A LAS 17:18 HORAS, Y LA SEGUNDA A LAS 19:04 HORAS.

A

P

A

R

L

O

S

E

V

I

D

E

M

Á

Q

U

“

**L**

**T**

**L**

**I**

**G**

D

I

R

E

C

P

L

A

N

E

A

C

C

E

D

“

A

s

i

g

n

a

c

o

r

p

o

r

a

D

E

L

S

R

U

T

A

:

P

R

O

C

E

S

.

A

\

T

E

A

S

I

G

N

C

O

R

P

O

c

a

t

e

g

o

P

M

P

.

x

l

A

P

A

L

O

S

E

V

I

D

L

A

D

E

N

A

C

C

M

C

0

c

e

l

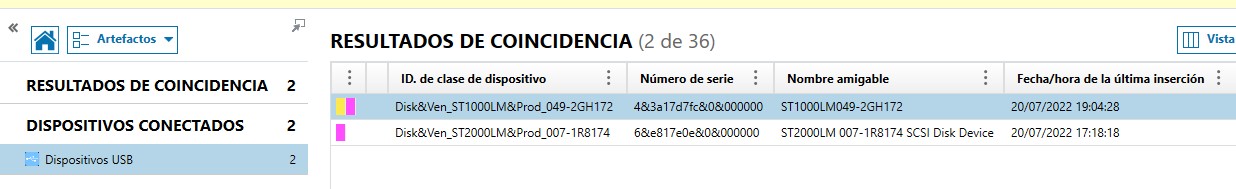
u

(

V

E

R



* SE CONSTATA QUE EXISTEN CINCO (05) REGISTROS DE LA EJECUCIÓN DEL

MALWARE EN EL REGISTRO DE ACTIVIDADES DE LA APLICACIÓN **MCAFEE,** LA

PRIMERA EJECUCIÓN SE SUSCITO EN FECHA 21 DE JULIO DEL 2020 A LAS 03:26:37 HORAS Y LA ULTIMA A LAS 10:37:40 HORAS DEL MISMO DIA.

* SE EVIDENCIO QUE EXISTEN CUATRO (04) ARCHIVOS DIGITALES QUE AL FINAL DE SU EXTENSIÓN DE FORMATO NATIVO CUENTA CON CARACTERES NO RECONOCIDOS, SIENDO LA EXTENSIÓN ALTERADA ‘\*.CCC’, ESTA EVIDENCIA INDICA QUE ESTOS ARCHIVOS HAN SIDO AFECTADOS POR UN CÓDIGO MALICIOSO (MALWARE) Y QUE HA CIFRADO SU CONTENIDO DE INFORMACIÓN DENOMINADOS: Amex Directory.pdf.ccc, ACUERDO DE CONFIDENCIALIDAD.docx.ccc, CAPA - MAESTRO PERU.docx.cc Y

CAPACITACION COMERCIOS.pdf.ppt.ccc, A LAS 10:34:27, 10:34:41, 10:34:49 Y 10:42:44 RESPECTIVAMENTE.

* SE EVIDENCIO QUE DE LA REVISIÓN DEL LOG DE EVENTOS DE LA APLICACIÓN MCAFEE, PRESENTA REGISTROS CORRESPONDIENTES A LA DETECCIÓN DE ARCHIVOS MALICIOSOS (MALWARE) A PARTIR DEL DÍA 21 DE JULIO DEL 2020, NO HABIÉNDOSE ENCONTRADO NINGÚN REGISTRO EN FECHA 20 DE JULIO DEL 2020 NI EN FECHAS ANTERIORES.
* SE HA EVIDENCIADO EXISTEN CUATROCIENTOS CINCUENTA Y CUATRO (454) ARCHIVOS DIGITALES QUE AL FINAL DE SU EXTENSIÓN DE FORMATO NATIVO

CUENTA CON CARACTERES NO RECONOCIDOS, SIENDO LA EXTENSIÓN ALTERADA ‘\*.CCC’, ESTA EVIDENCIA INDICA QUE ESTOS ARCHIVOS HAN SIDO AFECTADOS POR UN CÓDIGO MALICIOSO (MALWARE) Y QUE HA CIFRADO SU CONTENIDO DE INFORMACIÓN.