INFORME TÉCNICO PERICIAL DISPOSITIVO PORTÁTIL Y USB

Análisis de evidencias del dispositivo portátil XXXX y del USB para la obtención de evidencias

21 DE JUNIO DE 2022

NOMBRE PERITO
perito@mail.com

Contenido

1. Introducción

Bajo petición del cliente XXXX se va a llevar a cabo el análisis del clonado de disco duro como del volcado de memoria del dispositivo portátil XXXX y un dispositivo USB.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce aliquam dui odio, eu porta risus faucibus et. Nunc eget nisl gravida, efficitur dui non, luctus neque. Cras sodales magna vitae pretium ultricies. Integer malesuada vehicula mauris quis tincidunt. Praesent sed tellus eget nunc sagittis pretium. Maecenas pulvinar non mi vel dictum. Curabitur nec risus nunc. Cras ac hendrerit massa. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam euismod nisi quis ligula tincidunt rutrum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce aliquam dui odio, eu porta risus faucibus et. Nunc eget nisl gravida, efficitur dui non, luctus neque. Cras sodales magna vitae pretium ultricies. Integer malesuada vehicula mauris quis tincidunt. Praesent sed tellus eget nunc sagittis pretium. Maecenas pulvinar non mi vel dictum. Curabitur nec risus nunc. Cras ac hendrerit massa. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam euismod nisi quis ligula tincidunt rutrum.

2. Información del perito

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce aliquam dui odio, eu porta risus faucibus et. Nunc eget nisl gravida, efficitur dui non, luctus neque. Cras sodales magna vitae pretium ultricies. Integer malesuada vehicula mauris quis tincidunt. Praesent sed tellus eget nunc sagittis pretium. Maecenas pulvinar non mi vel dictum. Curabitur nec risus nunc. Cras ac hendrerit massa. Interdum et malesuada fames ac ante ipsum primis in faucibus. Nullam euismod nisi quis ligula tincidunt rutrum.

Información de contacto:

- webperito.es
- linkedin
- teléfono de contacto
- correos de contacto

3. Objetivos

El objetivo principal del análisis pericial es examinar las diferentes evidencias recopiladas para evidenciar todo acerca de ellas. Dicho objetivo principal se divide en dos objetivos:

1. Analizar el volcado de memoria RAM y el clonado del disco duro para evidenciar la diferente información que contiene.
2. Obtener acceso al dispositivo USB cifrado.

4. Análisis de Evidencias

4.1. Memoria RAM

En la memoria RAM se puede visualizar que el hash NTLM del usuario se encuentra cargado en memoria. La contraseña del usuario es test.

```
root@kali:/media/seguridad# volatility -f MemoryDumpWH.raw --profile=Win7SP0x86 hashdump
Volatility Foundation Volatility Framework 2.6
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
PC-0048:1000:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537:::
```

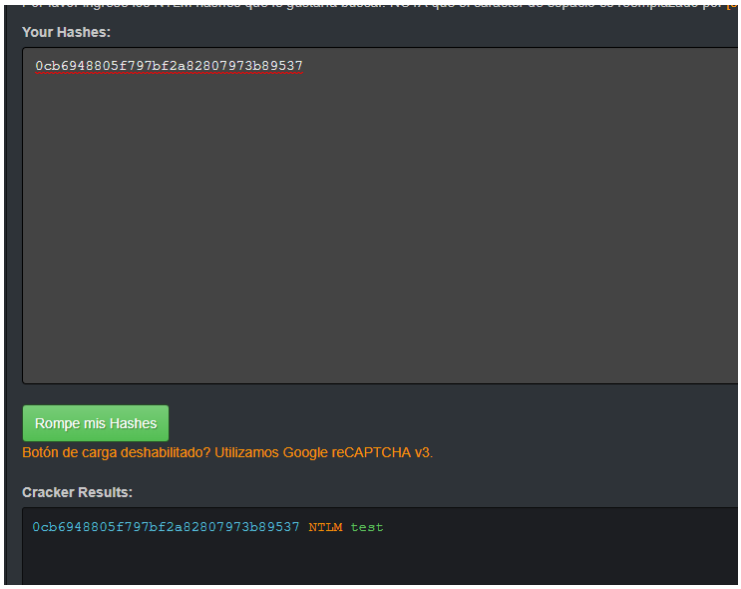

Ilustración 1 – Contraseña del usuario del dispositivo

Se observa que ha sido eliminado el fichero “F1ch3r0_D3l3t333333.txt” del dispositivo mediante el comando del.

```
root@kali:/media/seguridad# volatility -f MemoryDumpWH.raw --profile=Win7SP0x86 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 3904
CommandHistory: 0x3c0470 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x58
Cmd #0 @ 0x3bbc00: cd Desktop
Cmd #1 @ 0x3b4d30: del F1ch3r0_D3l3t3333333.txt
Cmd #2 @ 0x3bd890: dir
```

Ilustración 2 – Historial de comandos

4.2. Disco Duro

Se ha realizado un clonado del disco duro que tiene los siguientes hashes.

- **SHA256**: XXXXXXXXXXXXXXX
- **MD5**: XXXXXXXXXXXXXX

En el disco duro se puede observar que se encuentra instalado el navegador TOR Browser. Para ello se ha extraído la base de datos SQLite de los iconos de las páginas web para poder visualizar si ha accedido a algún .onion. En ello nos encontramos que el usuario ha accedido a la siguiente web en la red TOR.

- http://xxxxxxxxxxx.onion

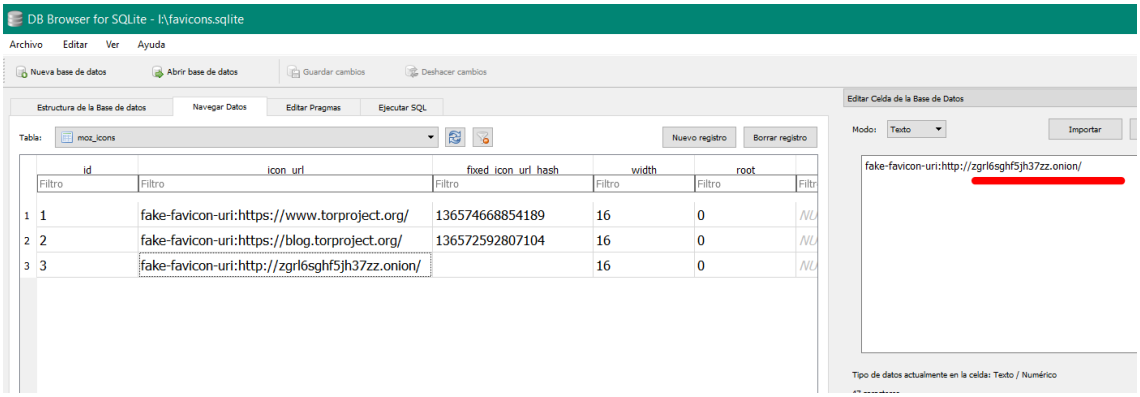

Ilustración 3 – Base de datos favicons.sqlite

En el dispositivo se han encontrado restos de una instalación del cliente de correo electrónico Thunderbird. En este aún se encuentra algunos correos electrónicos donde se han analizado y extraído la información.

```
Return-Path: <terros12@xxxx.xx>
X-SpamCatcher-Score: 1 [X]
Received: from localhost (xxxx.xx [xx.xx.xx.xx])
    with ESMTP-TLS id 61258719 for usuario@xxxx.xx; Fri, 22 Jun 2019 14:23:24
Message-ID: <4129F3CA.2020509@xxxx>
Date: Fri, 22 Jun 2019 14:23:24
From: Información Terros12 <terros12@xxxx.xx>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1) Gecko/20020823 Netscape/7.0
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: Usuario <usuario@xxxx.xx>
Subject: Atentado
Content-Type: text/html; charset=ISO-8859-1
Content-Transfer-Encoding: base64
Message Body:
Como ya sabes te envio el mensaje encriptado como siempre:
4E7H9L|`Cc8b06D06=0_3;bE`G_N
```

Emisor	terros12@xxxx.xx
Receptor	usuario@xxxx.xx
Asunto	Atentado
Servidor de correo	xx.xx.xx.xx
Fecha y envío	22/06/2019 14:23:24 UTC+1
ID Mensaje	4129F3CA.2020509@xxxx
Mensaje	Como ya sabes te envio el mensaje encriptado como siempre: 4E7H9L|`Cc8b06D06=0_3;bE`G_N

Se ha realizado un análisis al mensaje cifrado que ha dado como resultado que se encuentra cifrado con el método de cifrado ROT47. El contenido desencriptado del mensaje es el siguiente:

- M1r4g3_es_el_0bj3t1v0

Se ha encontrado una base de datos de contraseñas del gestor Keepass pero está cifrada con una contraseña. Se ha realizado un ataque mediante diccionario donde se ha determinado que la contraseña de la base de datos es **iloveyou2**

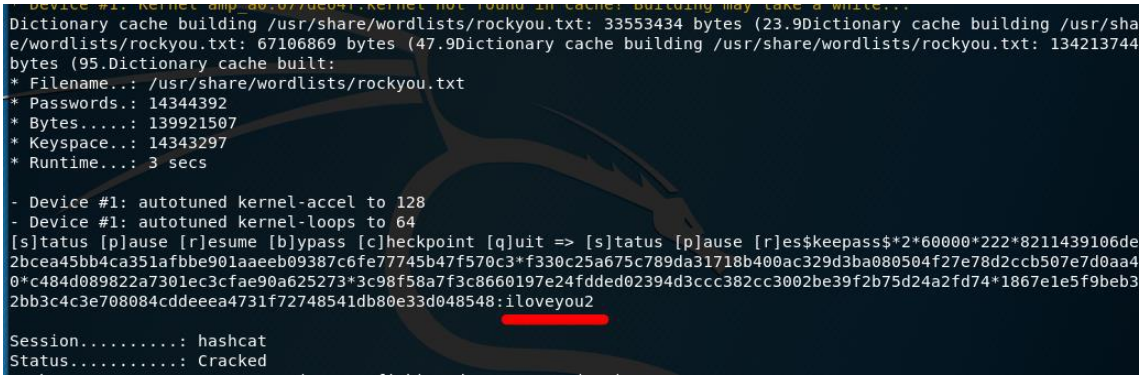

Ilustración 4 – Rompiendo el hash de la contraseña de la base de datos de Keepass

Dentro de la base de datos se ha encontrado una entrada con la siguiente información.

Usuario	USB01
Contraseña	KcJ0rpg0Dp85B6yfb8FL

4.3. Dispositivo USB

El dispositivo USB se encuentra cifrado mediante BitLocker. Anteriormente en la base de datos de Keepass se encontró una contraseña que hacía referencia a un dispositivo USB. Al probar la contraseña se desencripto sin problemas en dispositivo USB y se pudo acceder a su contenido.

En este dispositivo se ha encontrado un fichero PDF que hace referencia a la contraseña de una bomba.

Ilustración 5 – Contraseña de la bomba

5. Conclusiones

Una vez realizado el análisis de los diferentes dispositivos podemos afirmar las siguientes conclusiones:

1. Que se han encontrado evidencias de un posible ataque terrorista mediante una comunicación vía correo electrónico contra la ciudad de Mirage.
2. Que se ha encontrado en el dispositivo USB la contraseña de una bomba.
3. Que el usuario ha estado utilizando la red TOR para navegar por Internet.