

GIFD (Gestión de Incidentes y Forensia Digital)

Laboratorio Final

Identificación y manejo de rastros de delitos cibernéticos

Profesor: Gerson David Quintero Rodríguez
Ingeniero de Sistemas, Magíster en Seguridad Informática y de Sistemas.

Examinadora: Angie Daniela Ruiz Alfonso
Ingeniera de Sistemas.

Bogotá, Colombia - 9 de noviembre del 2021, Caso No. 1,
hora de inicio y fin de la investigación: 1:00 pm - 5:00 pm. (UTC-5)

Contents

1	Introducción	2
2	Resumen Ejecutivo	2
3	Objetivos Generales	2
4	Glosario	3
5	Acciones Realizadas en la Investigación	3
5.1	Preparación del Ambiente de Trabajo	4
5.2	Búsqueda y Captura de Evidencias	9
5.3	Análisis de los Resultados	14
5.4	Material Generado Durante la Investigación	16
6	Declaración Examinadora	16
7	Conclusiones	16
8	Referencias	17

1 Introducción

Los tribunales de justicia son la entidad encargada de determinar si un acto realizado por una persona fue lícito o no, basándose en la EVIDENCIA presentada. Hoy en día existe la evidencia electrónica, la cual no es diferente a la evidencia tradicional, por ende, es obligatorio que la parte que la introduce en un proceso judicial pueda demostrar las pruebas están intactas desde el momento en que empezó su recolección.

Al ser esta evidencia mucho más fácil de manipular que los demás tipos, se requiere de un mayor cuidado en general, para ser admisibles en un tribunal de justicia. Desde la incautación, custodia, control, transferencia, hasta el análisis y disposición de las pruebas, las cuales deben estar adecuadas y cronológicamente documentadas, cumpliendo la 'Cadena de Custodia' (CoC) por completo.

Y es allí, donde resalto la labor de La Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA), la cual busca el desarrollo de habilidades en el campo de seguridad de la información para el personal involucrado en el proceso de recopilación de datos, por medio de materiales de apoyo. Habilidades como lo son el conocimiento de las características y métodos de identificación de los malware populares, los principios de la recopilación de pruebas, los requisitos relativos a la admisibilidad de la prueba en un tribunal de justicia y las herramientas que se pueden usar.

2 Resumen Ejecutivo

En base a un material de formación que proporciona ENISA, el cual se enfoca especialmente en investigaciones de fraude con eventos que conlleven a cabo acciones legales, se realizó una investigación de phishing para un banco, donde en las primeras dos fases se recopilaban las pruebas y en la tercera se verificó su relevancia al caso.[1]

3 Objetivos Generales

- **Recopilar las pruebas conservando su forma y contenido original.**
- **Mantener el impacto en los datos lo más bajo posible y guardar el estado de los datos antes de alterarlos.**
- **Documentar toda actividad realizada sobre los datos, junto a las herramientas y métodos utilizados.**
- **Aprender a usar la capacidad de los datos de red como medio de recopilación de pruebas.**
- **Verificar que toda la información que fue recopilada de la computadora del usuario es suficiente para probar la actividad maliciosa y que se conecten las evidencias.**
- **Conectar las evidencias halladas con la información recopilada por el banco.**

4 Glosario

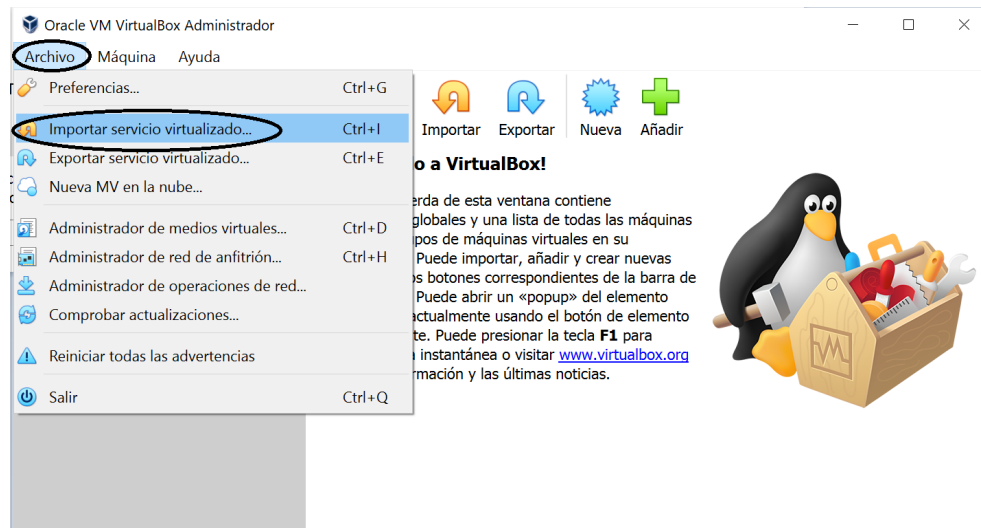
- **Evidencia:** Cualquiera de los elementos materiales o afirmaciones de hecho que se pueden presentar a un tribunal como un medio para determinar la verdad de cualquier supuesto hecho bajo investigación.[2]
- **Malware:** Cualquier tipo de software malicioso, diseñado para infiltrarse en un dispositivo sin su conocimiento.[3]
- **Memoria del Sistema:** Es donde se almacenan de forma temporal los datos de los programas que estás utilizando en este momento.[4]
- **Volcado de Memoria:** Volcar la memoria consiste en copiar el contenido de la memoria principal en un archivo, el cual puede ser analizado posteriormente para obtener información del estado de la computadora en el momento del volcado.[5]
- **Servidores CCs:** Un servidor de comando y control (CC), es una computadora controlada por un atacante, el cual la utiliza para enviar comandos a Sistemas comprometidos por malware y recibir datos robados de una red objetivo.[6]
- **Botnet (Red de Bots):** Es una red constituida por un gran número de equipos informáticos que han sido "secuestrados" por malware, de forma que quedan a disposición del atacante, el cual los usa para enviar spam o virus, para robar información personal o para realizar ataques de denegación de servicio distribuido (consiste en enviar varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes y de evitar que este funcione correctamente), por ende, se consideran una de las mayores amenazas en Internet actualmente.[7]
- **Enlace API:** Consiste en una forma de pedirle al Sistema Operativo que llame a una función específica cada vez que algo específico sucede en el sistema.[2]
- **Zeus:** El virus Troyano Zeus detectado por primera vez en el 2007, es un malware dirigido a Microsoft Windows, el cual es usado para robar datos financieros. Ha logrado infectar millones de equipos y se ha generado una gran variedad de componentes similares a partir de su código, a pesar de que su creador se retirara en el 2010, como su código fuente se hizo público fueron apareciendo numerosas variantes, pero en la actualidad ha sido neutralizado en gran medida.[8]

5 Acciones Realizadas en la Investigación

Sistema Operativo utilizado: Ubuntu One. Virtualizador utilizado: VirtualBox.

5.1 Preparación del Ambiente de Trabajo

Haciendo uso del virtualizador se importó la imagen virtual que nos ofrecía ENISA en su página web, de la siguiente manera: [9]



← Importar servicio virtualizado

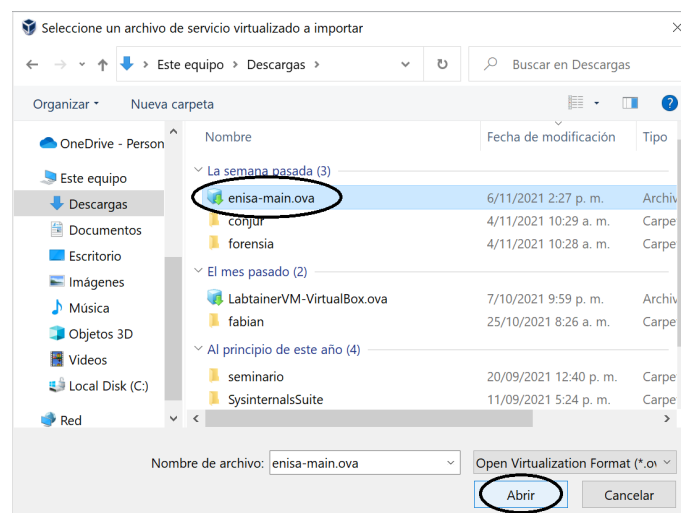
Servicio a importar

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Fuente: Sistema de archivos local

Seleccione un archivo desde el que importar el servicio virtualizado. VirtualBox actualmente soporta importar servicios guardados en Open Virtualization Format (OVF). Para continuar, seleccione el archivo a importar abajo

Archivo:



← Importar servicio virtualizado

Servicio a importar

Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Fuente: Sistema de archivos local

Seleccione un archivo desde el que importar el servicio virtualizado. VirtualBox actualmente soporta importar servicios guardados en Open Virtualization Format (OVF). Para continuar, seleccione el archivo a importar abajo

Archivo: C:\Users\Daniela Ruiz\Downloads\enisa-main.ova

Modo experto

Next

Cancelar

← Importar servicio virtualizado

Preferencias de servicio

Estas son las máquinas virtuales contenidas en el servicio y las preferencias sugeridas de las máquinas virtuales importadas de VirtualBox. Puede cambiar varias de las propiedades mostradas haciendo doble clic en los elementos y deshabilitar otras usando las casillas de verificación de abajo.

Sistema virtual 1	
Nombre	enisa-main
Descripción	ENISA Virtual Appliance
Tipo de SO invitado	Ubuntu (32-bit)
CPU	1
RAM	1024 MB
Adaptador de red	<input checked="" type="checkbox"/> Intel PRO/1000 MT Desktop (82540EM)
Controlador de almacenamiento (IDE)	PIIX4
Controlador de almacenamiento (IDE)	PIIX4
Imagen de disco virtual	enisa-main-disk1.vmdk
Carpeta base	C:\Users\Daniela Ruiz\VirtualBox VMs
Grupo primario	/

Carpeta base de máquina: C:\Users\Daniela Ruiz\VirtualBox VMs

Política de dirección MAC: Incluir solo las direcciones NAT de adaptador de red

Opciones adicionales: Incluir todas las direcciones de adaptador de red

Servicio virtualizado no f... Incluir solo las direcciones NAT de adaptador de red

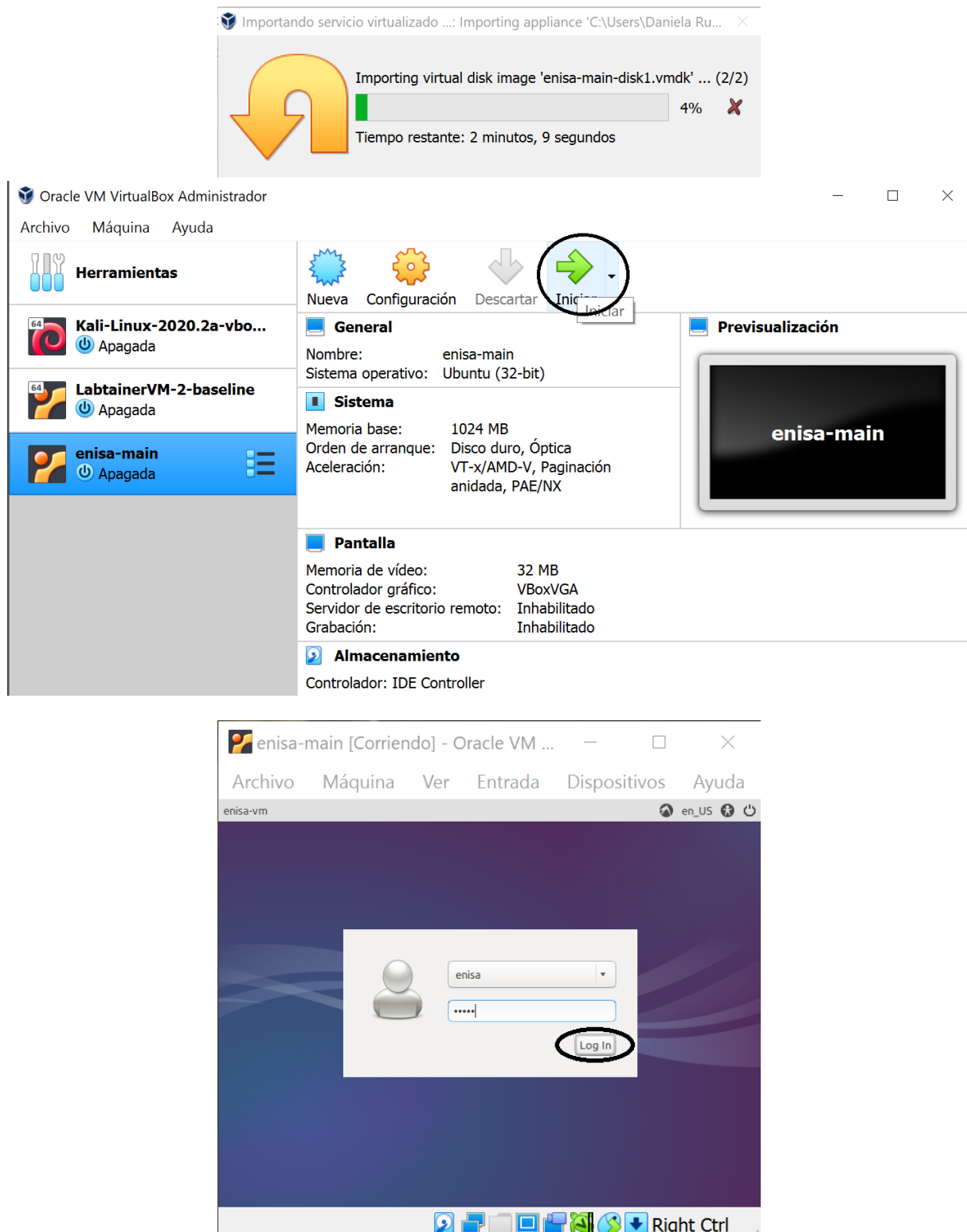
Generar nuevas direcciones MAC para todos los adaptadores de red

Generate new MAC addresses for all network adapters during importing.

Restaurar valores predeterminado

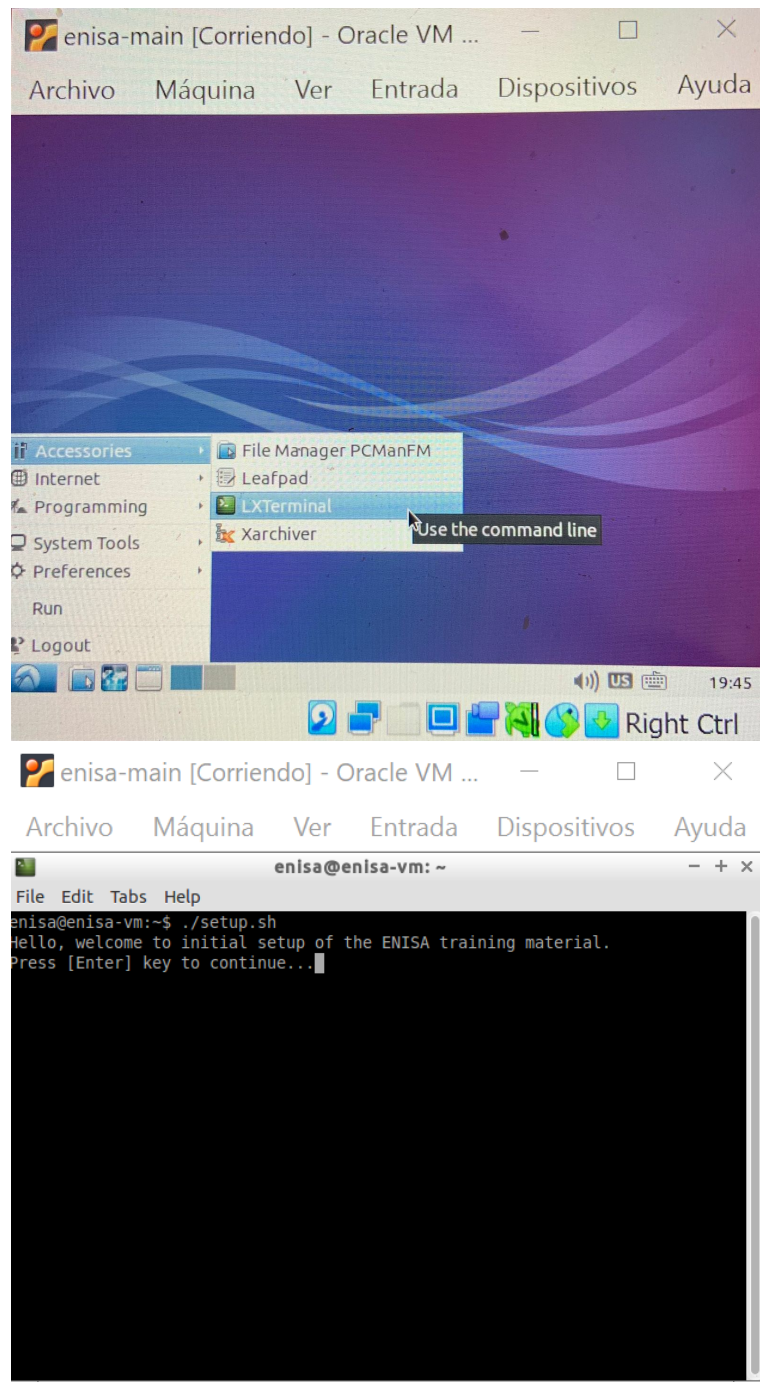
Importar

Cancelar

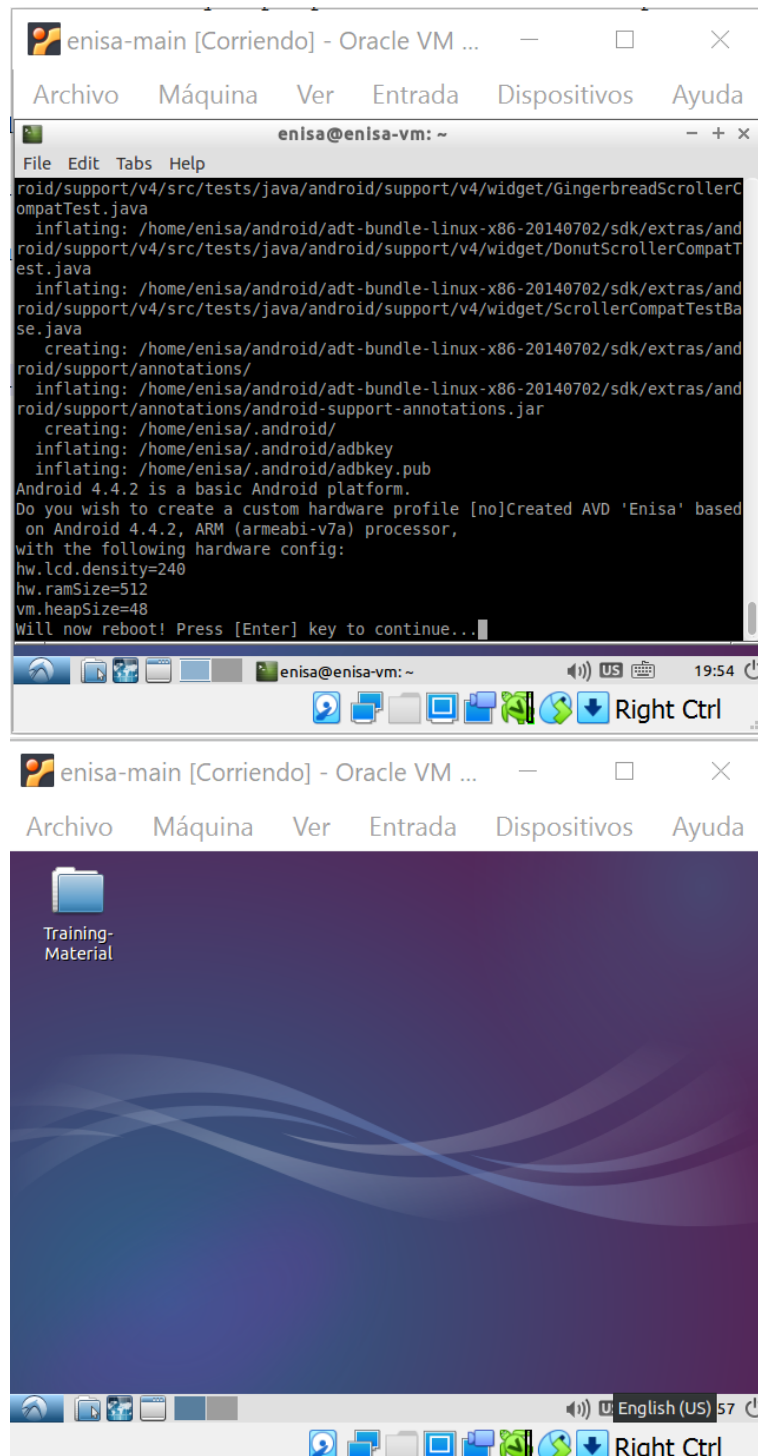


Se ingresó a la máquina virtual usando las credenciales usuario - clave: enisa - enisa.

Luego se hizo clic al simbolo del Sistema, dentro de accesorios se accedió a LXTerminal y se digitó el comando `./setup.sh`, el cual se encargó de descargar el material necesario para el ejercicio en la máquina. Luego se presionó la tecla ENTER.

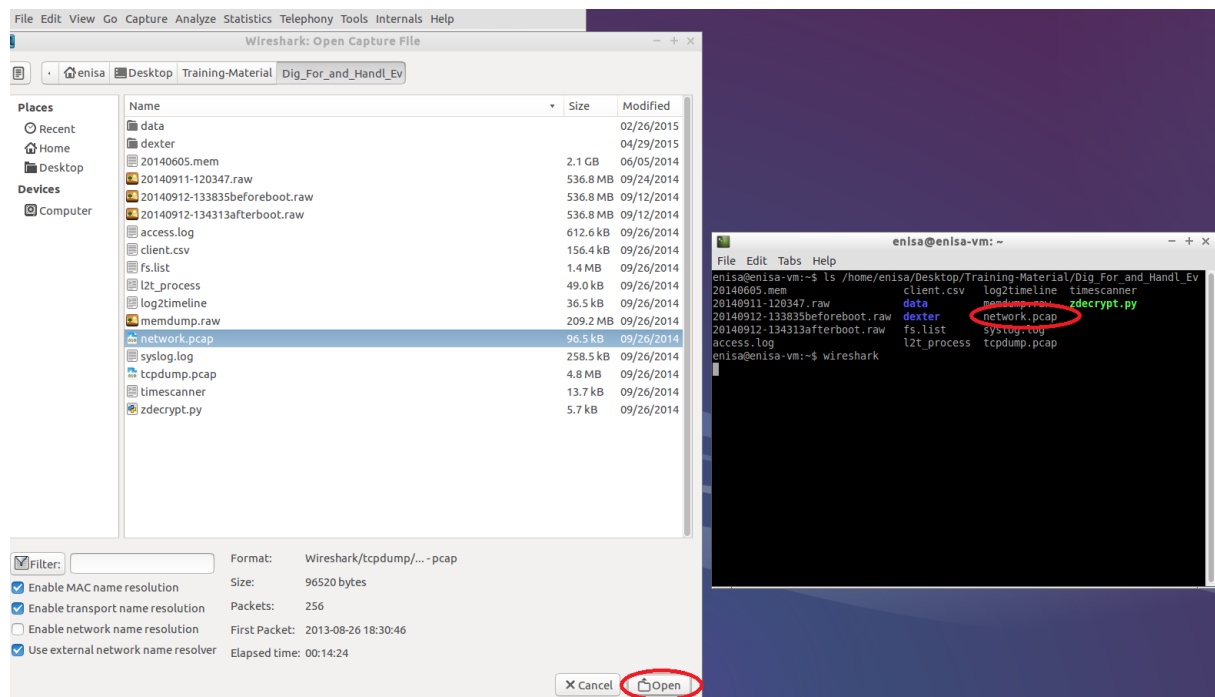


Al finalizar la descarga de todo el material, se presionó ENTER nuevamente para que la máquina virtual se reiniciará. Luego se volvió a ingresar a la máquina y en el escritorio ahora estaba la carpeta "Training-Material".



5.2 Búsqueda y Captura de Evidencias

- **1. Recopilación de pruebas mediante la clonación en frío del disco duro:** Se realizó una imagen completa del Sistema por medio del comando "dd", el cual se encargó de transferir la imagen de bits y por cuestiones de espacio, usando la herramienta "nc" se almacenó en red, lo cual quiere decir que la copia exacta quedó almacenada de forma segura en otra computadora, pero sobre la misma red para un examen más detallado o para restaurar la computadora a su estado original, debido a que se compararon ambos hash y se obtuvo el mismo.
- **2. Recopilación de datos en vivo de un Sistema en funcionamiento :** El archivo PCAP con el tráfico de la computadora examinada real a analizar, se encontró en la siguiente ruta "/home/enisa/Desktop/Training-Material/Dig_For_and_Handl_Ev". Luego con el comando "wireshark" se abrió la aplicación y se seleccionó el archivo PCAP que se ve encerrado en color rojo en la imagen; para abrirlo se hizo clic en File -> Open y se seleccionó:



Al cargar se obtuvo todo el tráfico de red que contenía este archivo, se aplicó un filtro "dns" para lograr ver si el computador que no debe tener conexiones exteriores las tenía. Luego se evidenció que efectivamente había comunicación con el exterior, se observa como la computadora preguntó la dirección IP de 'alazqwryx.cn' y obtuvo una respuesta con una dirección IP, siendo este uno de los patrones habituales que utiliza el malware, al solicitar direcciones no identificadas (que probablemente son de los servidores CC de la botnet), con el fin de enviar los datos recolectados, por ende, se aplicó un segundo filtro para ver las comunicaciones "http and ip.addr == 172.27.128.9" y nos arrojó que el computador de la víctima se conectó al servidor del atacante e hizo peticiones GET y POST, además de que se evidencia un patrón, debido a que se repitió después de aproximadamente 600 segundos:

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, packet selection, and analysis. The filter bar at the top shows 'dns' selected in the filter field and 'Apply' in the action field. The packet list pane on the left shows a list of captured packets, with packet 122 selected. The packet details pane on the right shows the structure of the selected packet, which is a DNS Standard query response (0x6e51) from 172.27.128.9. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
73	3.341282	192.168.0.44	192.168.0.1	DNS	74	Standard query 0x1d50 A www.google.com
8	3.347498	192.168.0.44	192.168.0.1	DNS	72	Standard query response 0x1d50 A www.google.com
9	3.347869	192.168.0.1	192.168.0.44	DNS	122	Standard query response 0x6e51 A 172.27.128.9
20	3.418261	192.168.0.1	192.168.0.44	DNS	381	Standard query response 0x1d50 A 173.194.70.99 A 173.194.70.103 A 173.194.70.104 A 173.194.70.105 A 173.194.70.106 A 173.194.70.107 A 173.194.70.108 A 173.194.70.109 A 173.194.70.110 A 173.194.70.111 A 173.194.70.112 A 173.194.70.113 A 173.194.70.114 A 173.194.70.115 A 173.194.70.116 A 173.194.70.117 A 173.194.70.118 A 173.194.70.119 A 173.194.70.120 A 173.194.70.121 A 173.194.70.122 A 173.194.70.123 A 173.194.70.124 A 173.194.70.125 A 173.194.70.126 A 173.194.70.127 A 173.194.70.128 A 173.194.70.129 A 173.194.70.130 A 173.194.70.131 A 173.194.70.132 A 173.194.70.133 A 173.194.70.134 A 173.194.70.135 A 173.194.70.136 A 173.194.70.137 A 173.194.70.138 A 173.194.70.139 A 173.194.70.140 A 173.194.70.141 A 173.194.70.142 A 173.194.70.143 A 173.194.70.144 A 173.194.70.145 A 173.194.70.146 A 173.194.70.147 A 173.194.70.148 A 173.194.70.149 A 173.194.70.150 A 173.194.70.151 A 173.194.70.152 A 173.194.70.153 A 173.194.70.154 A 173.194.70.155 A 173.194.70.156 A 173.194.70.157 A 173.194.70.158 A 173.194.70.159 A 173.194.70.160 A 173.194.70.161 A 173.194.70.162 A 173.194.70.163 A 173.194.70.164 A 173.194.70.165 A 173.194.70.166 A 173.194.70.167 A 173.194.70.168 A 173.194.70.169 A 173.194.70.170 A 173.194.70.171 A 173.194.70.172 A 173.194.70.173 A 173.194.70.174 A 173.194.70.175 A 173.194.70.176 A 173.194.70.177 A 173.194.70.178 A 173.194.70.179 A 173.194.70.180 A 173.194.70.181 A 173.194.70.182 A 173.194.70.183 A 173.194.70.184 A 173.194.70.185 A 173.194.70.186 A 173.194.70.187 A 173.194.70.188 A 173.194.70.189 A 173.194.70.190 A 173.194.70.191 A 173.194.70.192 A 173.194.70.193 A 173.194.70.194 A 173.194.70.195 A 173.194.70.196 A 173.194.70.197 A 173.194.70.198 A 173.194.70.199 A 173.194.70.200 A 173.194.70.201 A 173.194.70.202 A 173.194.70.203 A 173.194.70.204 A 173.194.70.205 A 173.194.70.206 A 173.194.70.207 A 173.194.70.208 A 173.194.70.209 A 173.194.70.210 A 173.194.70.211 A 173.194.70.212 A 173.194.70.213 A 173.194.70.214 A 173.194.70.215 A 173.194.70.216 A 173.194.70.217 A 173.194.70.218 A 173.194.70.219 A 173.194.70.220 A 173.194.70.221 A 173.194.70.222 A 173.194.70.223 A 173.194.70.224 A 173.194.70.225 A 173.194.70.226 A 173.194.70.227 A 173.194.70.228 A 173.194.70.229 A 173.194.70.230 A 173.194.70.231 A 173.194.70.232 A 173.194.70.233 A 173.194.70.234 A 173.194.70.235 A 173.194.70.236 A 173.194.70.237 A 173.194.70.238 A 173.194.70.239 A 173.194.70.240 A 173.194.70.241 A 173.194.70.242 A 173.194.70.243 A 173.194.70.244 A 173.194.70.245 A 173.194.70.246 A 173.194.70.247 A 173.194.70.248 A 173.194.70.249 A 173.194.70.250 A 173.194.70.251 A 173.194.70.252 A 173.194.70.253 A 173.194.70.254 A 173.194.70.255 A 173.194.70.256 A 173.194.70.257 A 173.194.70.258 A 173.194.70.259 A 173.194.70.260 A 173.194.70.261 A 173.194.70.262 A 173.194.70.263 A 173.194.70.264 A 173.194.70.265 A 173.194.70.266 A 173.194.70.267 A 173.194.70.268 A 173.194.70.269 A 173.194.70.270 A 173.194.70.271 A 173.194.70.272 A 173.194.70.273 A 173.194.70.274 A 173.194.70.275 A 173.194.70.276 A 173.194.70.277 A 173.194.70.278 A 173.194.70.279 A 173.194.70.280 A 173.194.70.281 A 173.194.70.282 A 173.194.70.283 A 173.194.70.284 A 173.194.70.285 A 173.194.70.286 A 173.194.70.287 A 173.194.70.288 A 173.194.70.289 A 173.194.70.290 A 173.194.70.291 A 173.194.70.292 A 173.194.70.293 A 173.194.70.294 A 173.194.70.295 A 173.194.70.296 A 173.194.70.297 A 173.194.70.298 A 173.194.70.299 A 173.194.70.300 A 173.194.70.301 A 173.194.70.302 A 173.194.70.303 A 173.194.70.304 A 173.194.70.305 A 173.194.70.306 A 173.194.70.307 A 173.194.70.308 A 173.194.70.309 A 173.194.70.310 A 173.194.70.311 A 173.194.70.312 A 173.194.70.313 A 173.194.70.314 A 173.194.70.315 A 173.194.70.316 A 173.1

- **3. Comprobación de los datos obtenidos en búsqueda de valor forense :** La información combinada que teníamos hasta el momento sugería que teníamos una computadora infectada con una variante de Zeus, por ende, se usó Volatility Framework y se buscó las conexiones activas y luego todas las conexiones:

```

enis@enis-vm:~$ cd /home/enisa/Desktop/Training-Material/Dig_For_and_Handl_Ev
enis@enis-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ volatility -f m
emdump.raw connections
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Local Address      Remote Address      Pid
-----
0x811d0680 192.168.0.44:1044      172.27.128.9:80     236
enis@enis-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ volatility -f m
emdump.raw connscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Local Address      Remote Address      Pid
-----
0x010c4680 192.168.0.44:1044      172.27.128.9:80     236
0x058c3b48 192.168.0.44:1043      173.194.70.94:80     236
0x0a5b1b48 192.168.0.44:1043      173.194.70.94:80     236
0x0c06add8 192.168.0.44:1030      172.27.128.9:80     236
enis@enis-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$

```

```

enis@enis-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ volatility -f m
emdump.raw pslist
Volatility Foundation Volatility Framework 2.3.1
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Star
-----
0x8132b020 System                4    0     54   523  -----  0
0x81231c60 smss.exe             408   4     3    21  -----  0 2013
-08-26 15:32:08 UTC+0000
0x8119b698 csrss.exe            564  408    10   341    0    0 2013
-08-26 15:32:09 UTC+0000
0x811f4b00 winlogon.exe       588  408    18   503    0    0 2013
-08-26 15:32:09 UTC+0000
0x81232020 services.exe  792  588    15   253    0    0 2013
-08-26 15:32:09 UTC+0000
0x81235020 lsass.exe       804  588    20   331    0    0 2013
-08-26 15:32:09 UTC+0000
0xffbd5530 VBoxService.exe  988  792     8   107    0    0 2013
-08-26 15:32:09 UTC+0000
0x81230020 svchost.exe      1060  792    22   215    0    0 2013
-08-26 15:32:09 UTC+0000
0x81195790 svchost.exe      1172  792     9   239    0    0 2013
-08-26 15:32:10 UTC+0000
0xffac11d8 svchost.exe      1368  792    59  1139    0    0 2013
-08-26 15:32:10 UTC+0000
0xffab8688 svchost.exe      1424  792     6    76    0    0 2013
-08-26 15:32:10 UTC+0000
0x811d7760 svchost.exe      1456  792    14   206    0    0 2013
-08-26 15:32:10 UTC+0000
0xffa92c08 spoolsv.exe     2008  792    10   106    0    0 2013
-08-26 15:32:11 UTC+0000
0x811c62f0 explorer.exe        236  216    18   365    0    0 2013
-08-26 15:32:12 UTC+0000
0xffa7b8c0 VBoxTray.exe     288  236     7    71    0    0 2013
-08-26 15:32:12 UTC+0000
0xffa7b280 msmsgs.exe       296  236     3   176    0    0 2013
-08-26 15:32:12 UTC+0000
0xffa7a660 emneo.exe        304  236     0  -----  0    0 2013
-08-26 15:32:12 UTC+0000
0xff9d6d08 alg.exe         868  792     6   104    0    0 2013
-08-26 15:32:29 UTC+0000
0xffbb7228 wscntfy.exe       200 1368     3    48    0    0 2013
-08-26 15:32:30 UTC+0000
0x811d5c08 taskmgr.exe      340  588     3    76    0    0 2013
-08-26 15:32:35 UTC+0000
0x8119a130 cmd.exe          1432  236     1    53    0    0 2013
-08-26 15:32:56 UTC+0000
0x811e3a58 wpabaln.exe      1356  588     1    77    0    0 2013
-08-26 15:34:08 UTC+0000
0xffa9f800 mdd.exe          744 1432     1    41    0    0 2013
-08-26 15:42:21 UTC+0000
enis@enis-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$

```

Volatility arrojó que la computadora tenía una conexión activa a la dirección IP 172.27.128.9 que causó interés anteriormente, de ahí se extrajo el ID del proceso de Windows que abrió las conexiones (236) y en las conexiones pasadas se obtuvo que antes también hubo conexiones con el sospechoso, junto con la IP 173.194.70.94 puerto 80. Luego en el listado de los procesos, lo que más llamó la atención fue el proceso 'emneo.exe' que se inició y se cerró casi al tiempo.

Al obtener los 'enlaces API', los resultados quedaron guardados en un archivo, la cual se abrió para observar los resultados. Después, se observa la lista de hooks con procesos registrados y se pudo evidenciar que "explorador.exe" estaba en la lista, este es el nombre de un ejecutable del Explorador de Windows, el cual condiciona al proceso a no hacer ninguna conexión externa, por ende, el binary fue modificado o algún otro proceso inyectó código malicioso en uno de los hilos del explorador, esta última es una técnica popular utilizada por software malicioso para ocultar su existencia.

```
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ cd data
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ ls
apihooks.out
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ cat apihooks.out | grep Process | sort -u
Process: 1356 (wpabaln.exe)
Process: 1432 (cmd.exe)
Process: 200 (wscntfy.exe)
Process: 236 (explorer.exe)
Process: 288 (VBoxTray.exe)
Process: 340 (taskmgr.exe)
Process: 744 (mdd.exe)
```

Se extrajo la imagen de la memoria de la computadora del espacio de memoria hayado anteriormente, para poder hacer posteriormente uso de una herramienta interna en el Sistema UNIX - llamada 'strings', la cual sirve para extraer información de un archivo binario. Y en todos los casos, las cadenas que se buscaron anteriormente estaban presentes en el volcado de la memoria, el sitio web del banco, numerosas referencias al dominio 'alazqwryx.cn' y las URL dentro de él, para finalmente visualizar una referencia al archivo 'emneo.exe', proceso que se ejecuta justo después de encender el Sistema y luego se usa para inyectar código malicioso en el proceso 'explorer.exe':

```
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ cd ..
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ volatility -f memdump.raw memdump -p 236 -D data/
Volatility Foundation Volatility Framework 2.3.1
*****
Writing explorer.exe [ 236] to 236.dmp
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ cd data
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep bank.pl
http://bank.pl/*
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep alazqwryx.cn
: alazqwryx.cn
://alazqwryx.cn/z12/config.bin
alazqwryx.cn
alazqwryx.cn
://alazqwryx.cn/z12/gate.php
://alazqwryx.cn/z12/gate.php
http://alazqwryx.cn/z12/config.bin
http://alazqwryx.cn/z12/config.bin
http://alazqwryx.cn/z12/bot.exe#N
http://alazqwryx.cn/z12/gate.php%N
://alazqwryx.cn/z12/gate.php
http://alazqwryx.cn/z12/config.bin
alazqwryx.cn
http://alazqwryx.cn/z12/config.bin
alazqwryx.cn
http://alazqwryx.cn/z12/config.bin
http://alazqwryx.cn/z12/config.bin
http://alazqwryx.cn/z12/config.bin
http://alazqwryx.cn/z12/config.bin
Host: alazqwryx.cn
Host: alazqwryx.cn
Host: alazqwryx.cn
Host: alazqwryx.cn
Host: alazqwryx.cn
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep emneo.exe
emneo.exe
Myw\emneo.exe
Myw\emneo.exe
Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
emneo.exe
enisa@enisa-vm:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$
```

enisa-main [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Edit Search Options Help

Hook mode: Usermode
 Hook type: Inline/Trampoline
 Process: 236 (explorer.exe)
 Victim module: ntdll.dll (0x7c900000-0x7c9b0000)
 Function: ntdll.dll!LdrLoadDll at 0x7c9161ca
 Hook address: 0x1246b69
 Hooking module: <unknown>

Disassembly(0):
 0x7c9161ca e99a099384 JMP 0x1246b69
 0x7c9161cf 681863917c PUSH DWORD 0x7c916318
 0x7c9161d4 e8e98bffff CALL 0x7c90edc2
 0x7c9161d9 a134c0977c MOV EAX, [0x7c97c034]
 0x7c9161de 8945e4 MOV [EBP+0x1c], EAX
 0x7c9161e1 8b DB 0x8b

Disassembly(1):
 0x1246b69 55 PUSH EBP
 0x1246b6a 8bec MOV EBP, ESP
 0x1246b6c e8169dffff CALL 0x1240887
 0x1246b71 84c0 TEST AL, AL
 0x1246b73 7507 JNZ 0x1246b7c
 0x1246b75 5d POP EBP
 0x1246b76 ff2500332501 JMP DWORD [0x1253300]
 0x1246b7c 53 PUSH EBX
 0x1246b7d 56 PUSH ESI
 0x1246b7e 8b7514 MOV ESI, [EBP+0x14]

Hook mode: Usermode
 Hook type: Inline/Trampoline
 Process: 236 (explorer.exe)
 Victim module: ntdll.dll (0x7c900000-0x7c9b0000)
 Function: ntdll.dll!LdrCreateThread at 0x7c90d7d2
 Hook address: 0x1246989
 Hooking module: <unknown>

Disassembly(0):
 0x7c90d7d2 e9b2919384 JMP 0x1246989
 0x7c90d7d7 ba0003fe7f MOV EDI, 0x7ffe0300
 0x7c90d7dc ff12 CALL DWORD [EDI]
 0x7c90d7de c22000 RET 0x20
 0x7c90d7e1 90 NOP
 0x7c90d7e2 90 NOP
 0x7c90d7e3 90 NOP
 0x7c90d7e4 90 NOP
 0x7c90d7e5 90 NOP
 0x7c90d7e6 90 NOP
 0x7c90d7e7 b8 DB 0xb8
 0x7c90d7e8 36 DB 0x36
 0x7c90d7e9 00 DB 0x0

Disassembly(1):
 0x1246989 55 PUSH EBP
 0x124698a 8bec MOV EBP, ESP
 0x124698c 83e4f8 AND ESP, 0x8
 0x124698f 83ec20 SUB ESP, 0x20
 0x1246992 53 PUSH EBX
 0x1246993 57 PUSH EDI
 0x1246994 e8ee9effff CALL 0x1240887
 0x1246999 8b7d14 MOV EDI, [EBP+0x14]
 0x124699c 84c0 TEST AL, AL
 0x124699e 747c JZ 0x1246a1c
 0x12469a0 8d DB 0x8d

Hook mode: Usermode
 Hook type: Inline/Trampoline
 Process: 236 (explorer.exe)
 Victim module: ntdll.dll (0x7c900000-0x7c9b0000)
 Function: ntdll.dll!LdrCreateThread at 0x7c90d7d2

236.dmp - GHex

File Edit View Windows Help

0069D760	7B 76 6B 6F 33 6B 74 65 16 40 2A 2F 6C 6F 67 69	{vko3kte.0/lo
0069D770	6E 2E 4B 30 60 4F 76 6D 70 12 61 74 6C 10 00 00	n.K0'0vmp.atl...
0069D780	00 00 00 00 00 48 00 FF 26 4E 00 00 00 00 10	H &N
0069D790	24 00 00 00 24 00 00 00 68 74 70 3A 2F 2F 62	...\$.http://b
0069D7A0	61 6E 6B 2E 70 6C 2F 2A 00 75 73 65 72 6E 61	ank.pl/*.usernam
0069D7B0	65 3B 70 61 73 73 77 6F 72 64 00 00 00 00 00	e;password.....
0069D7C0	00 00 00 00 00 00 00 00 06 00 30 00 41 01 0A0.A...
0069D7D0	40 28 43 01 3A 2F 2F 61 6C 61 7A 71 77 72 79	@(C.://alazqwr
0069D7E0	2E 63 6E 2F 7A 31 32 2F 67 61 74 65 2E 70 68	.cn/z12/gate.php
0069D7F0	00 00 00 00 00 00 00 00 08 00 06 00 47 01 0CG...

Signed 8 bit: 42 Signed 32 bit: 1869360938 Hexadecimal: 2A

Unsigned 8 bit: 42 Unsigned 32 bit: 1869360938 Octal: 052

Signed 16 bit: 12074 Float 32 bit: 7.309548e+28 Binary: 00101010

Unsigned 16 bit: 12074 Float 64 bit: 4.892067e-85 Stream Length: 8 - +

☒ Show little endian decoding ☐ Show unsigned and float as hexadecimal

Offset: 0x69D76A

Luego al buscar en el archivo generado con el editor hexadecimal (dentro de la carpeta data, haciendo clic derecho sobre el archivo, Open With -> Programming -> GHex) se encontró información relevante al caso, lo que se espera que sea una URL electrónica del banco junto con una parte del formulario de entrada.

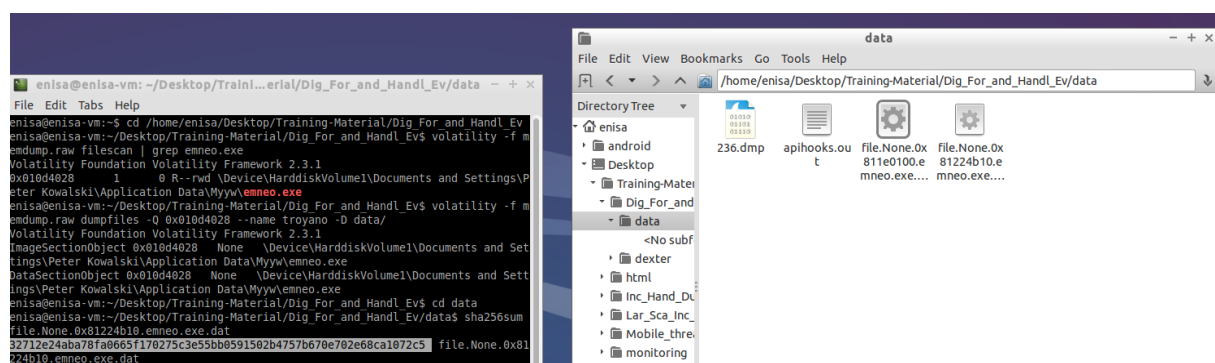
Teniendo la evidencia solo hacia falta relacionarla con la información del banco, se procedió a buscar y copiar archivos relacionados con el malware encontrado. Y se pudo ver la fecha y hora de la creación del archivo "26th August 16:12:05 2013", este fue probablemente el momento en que el equipo fue infectado, o al menos el último momento en que se actualizó el malware. Se sigue la pista en búsqueda de otros archivos creados en esa franja de tiempo, se encuentran dos archivos sospechosos más y por sus nombres sugirieron que podían contener información sobre las teclas presionadas por el usuario, por ende, estos archivos fueron guardados para la investigación:

```

enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ cd ..
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ volatility -f memdump.raw memdump -p 236 -D data/
Volatility Foundation Volatility Framework 2.3.1
*****
Writing explorer.exe [ 236 ] to 236.dmp
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ cd data
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep bank.pl
http://bank.pl/*
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep alazqwrxy.cn
: alazqwrxy.cn
//alazqwrxy.cn/z12/config.bin
alazqwrxy.cn
alazqwrxy.cn
//alazqwrxy.cn/z12/gate.php
//alazqwrxy.cn/z12/gate.php
http://alazqwrxy.cn/z12/config.bin
http://alazqwrxy.cn/z12/config.bin
http://alazqwrxy.cn/z12/bot.exe#N
http://alazqwrxy.cn/z12/gate.php#N
//alazqwrxy.cn/z12/gate.php
http://alazqwrxy.cn/z12/config.bin
alazqwrxy.cn
http://alazqwrxy.cn/z12/config.bin
alazqwrxy.cn
http://alazqwrxy.cn/z12/config.bin
http://alazqwrxy.cn/z12/config.bin
http://alazqwrxy.cn/z12/config.bin
http://alazqwrxy.cn/z12/config.bin
Host: alazqwrxy.cn
Host: alazqwrxy.cn
Host: alazqwrxy.cn
Host: alazqwrxy.cn
Host: alazqwrxy.cn
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ strings 236.dmp | grep emneo.exe
emneo.exe
Myw\emneo.exe
Myw\emneo.exe
Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
C:\Documents and Settings\Peter Kowalski\Application Data\Myw\emneo.exe
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev/data$ cd ..
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ cat fs.list | grep emneo.exe
Mon Aug 26 16:12:05 2013, /Documents and Settings/Peter Kowalski/Application Data/Myw/emneo.exe
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$ cat fs.list | grep "26 16:1"
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Application Data/Microsoft/Address Book
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Application Data/Microsoft/Address Book/Peter Kowalski.wab
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Application Data/Microsoft/Address Book/Peter Kowalski.wab-
Mon Aug 26 16:12:05 2013, /Documents and Settings/Peter Kowalski/Application Data/Myw
Mon Aug 26 16:12:05 2013, /Documents and Settings/Peter Kowalski/Application Data/Myw/emneo.exe
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Application Data/Uhan
Mon Aug 26 16:14:57 2013, /Documents and Settings/Peter Kowalski/Cookies/peter.kowalski@google[1].txt
Mon Aug 26 16:12:34 2013, /Documents and Settings/Peter Kowalski/Cookies/peter.kowalski@google[2].txt
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft/Outlook Express
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft/Outlook Express/Folders.dbx
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft/Outlook Express/Inbox.dbx
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft/Outlook Express/Offline.dbx
Mon Aug 26 16:12:06 2013, /Documents and Settings/Peter Kowalski/Local Settings/Application Data/Identities/{BAD605FE-6ED6-4C5C-9A8C-515509B3AA9B}/Microsoft/Outlook Express/Sent Items.dbx
Mon Aug 26 16:12:30 2013, /WINDOWS/Prefetch/EE34FD5H425.EXE-35053617.pf
Mon Aug 26 16:12:30 2013, /WINDOWS/Prefetch/EMNEO.EXE-22992292.pf
Mon Aug 26 16:12:13 2013, /WINDOWS/system32/keylog1.bin
Mon Aug 26 16:12:14 2013, /WINDOWS/system32/keylog2.bin
enis@enis-virtual-machine:~/Desktop/Training-Material/Dig_For_and_Handl_Ev$

```

5.3 Análisis de los Resultados



VirusTotal Analysis:

File: 32712e24aba78fa0665f170275c3e55bb0591502b4757b670e702e68ca1072c5
 Size: 140.00 KB
 Date: 2020-06-17 14:45:50 UTC
 63 security vendors flagged this file as malicious

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Heur.Dreidel.ImX@wS0j68l
AegisLab	Trojan.Win32.Generic.4lc	AhnLab-V3	Trojan/Win32.Zbot.R4880
ALYac	Gen:Heur.Dreidel.ImX@wS0j68l	Antiy-AVL	Trojan/Win32.AGeneric
Arcabit	Trojan.Dreidel.E7DC90	Avast	Sf.Crypt-BT [Trj]
AVG	Sf.Crypt-BT [Trj]	Avira (no cloud)	TR/Spy.Zbot.aogb.5
Baidu	Win32.Trojan.Zbot.a	BitDefender	Gen:Heur.Dreidel.ImX@wS0j68l
BitDefenderTheta	Gen:NN.ZexaF.34128.ImX@aS0j68l	Bkav Pro	W32.AIDetectVM.malwareA
CAT-QuickHeal	Trojan.Necurs.MUE.A3	ClamAV	Win.Spyware.Zbot-1275

IBM X-Force Exchange Analysis:

Informe de programa malicioso de X-Force
 32712e24aba78fa0665f170275c3e55bb0591502b4757b670e702e68ca1072c5

Riesgo: **Alta**

Exportar como STIX 2 | Se recomienda editar | Seguir

Comentarios (0) | Recopilaciones (0) / Reports (0)

Este informe no contiene etiquetas. Añade etiquetas en el recuadro de comentarios.

Detalles:

- Tipo hash: sha256
- Visto por primera vez: 16 jun. 2016
- Visto por última vez: 24 dic. 2020
- Nombre: 791US
- Tipo: Trojan
- Cobertura de la comunidad: 89%
- Plataforma: Win32

Powered by: ReversingLabs Titanium Platform

¿Sabía que tenemos una API?
 X-Force Threat Intelligence es práctico y está disponible mediante nuestras API (JSON y STIX), que se pueden introducir en los SIEM. Obtenga más información en nuestra [documentación de las API](#)

```
curl -X GET --header 'Accept: application/json' -u {API_KEY:API_PASSWORD} 'https://exchan
```

En base a los hallazgos obtenidos anteriormente, se identificó el espacio del volcado de memoria donde se encontraba el ejecutable y al encontrarlo, se extrajo el ejecutable del volcado de memoria, luego se obtuvo el hash para poder analizarlo desde Virus Total[10] y en IBM XForce[11].

5.4 Material Generado Durante la Investigación

- 236.dmp
- apihooks.out
- file.None.0x811e0100.emneo.exe
- file.None.0x81224b10.emneo.exe

6 Declaración Examinadora

Yo Angie Daniela Ruiz Alfonso, Ingeniera de Sistemas de la Escuela Colombiana de Ingeniería Julio Garavito, identificada con cedula de ciudadanía 1019150998 de Bogotá, doy fe de mi imparcialidad y veracidad en la labor profesional de investigación brindada, al no poseer conflictos de interés que puedan suscitarse a partir de la investigación realizada, por lo cual mi objetividad, conformidad y toma de decisiones no se vieron afectadas.

7 Conclusiones

En este laboratorio se realizó un análisis del lado del cliente en un caso de fraude bancario, donde se aplicó los principios básicos de recopilación de pruebas, desde las imágenes forenses, el rastreo y captura de tráfico de red, hasta la examinación de actividades sospechas, sin llegar a alterar en ningún momento la evidencia.

Durante todos los pasos se siguieron los principios de mantener el impacto en los datos lo más bajo posible, guardar el estado de los datos antes de alterarlos y documentando todas las alteraciones, herramientas y métodos utilizados. Para finalmente haciendo uso de los conceptos aprendidos, deducir la ubicación del malware y el posible tiempo de infección.

Por lo analizado, Zeus en este caso actuó como un virus troyano de servicios financieros, diseñado para robar credenciales de banca en línea de los equipos infectados, por medio de que el malware reconoce el momento en el que el usuario se encuentra en un sitio web bancario y además registra las pulsaciones de teclas usadas para iniciar sesión, por ende, el troyano puede eludir la seguridad que aplican estos sitios web registrando las pulsaciones de teclas para iniciar sesión mientras el usuario las introduce. [8]

Para prevenir este tipo de ataques, se recomienda contar con un potente y actualizado antivirus, evitar sitios web potencialmente peligrosos, al igual que tampoco hacer clic en enlaces de correos electrónicos, ni en mensajes de redes sociales a menos que esperes recibirlos (el mensaje puede estar infectado si la fuente fue infectada por Zeus, así el mensaje venga de una fuente confiable) y por último, así existan variantes populares de este tipo malware que también afectan a dispositivos móviles saltando la autenticación de dos factores en el ámbito financiero, se recomienda siempre interactuar de forma segura con las instituciones financieras en línea, usando un Sistema de autenticación de dos factores.[8]

8 Referencias

- [1] A. de la Unión Europea para la Seguridad de las Redes y de la Información (ENISA), *How to*, <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/virtual-image-how-to>, Accessed on 2021-09-11.
- [2] ENISA, *Identifying and handling cyber-crime traces*, <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/identification-and-handling-of-electronic-evidence-toolset?classId=0f21248c-8977-4571-b77d-bad02b653b9f&assignmentId=0d9d3197-2516-4182-aa16-3cb3462cfc3f&submissionId=b5acf865-36d7-20ac-cbe5-1fa4914bb6fa>, Accessed on 2021-09-11.
- [3] Avast, *¿qué es el malware?* <https://www.avast.com/es-es/c-malware>, Accessed on 2021-10-11.
- [4] Xataka, *Memoria ram: Qué es, para qué sirve y cómo mirar cuánta tiene tu ordenador o móvil*, <https://www.xataka.com/basics/memoria-ram-que-sirve-como-mirar-cuanta-tiene-tu-ordenador-movil>, Accessed on 2021-10-11.
- [5] U. N. A. de México (UNAM), *Análisis de volcado de memoria en investigaciones forenses computacionales*, <https://revista.seguridad.unam.mx/numero-17/an%C3%A1lisis-de-volcado-de-memoria-en-investigaciones-forenses-computacionales>, Accessed on 2021-10-11.
- [6] TrendMicro, *Command and control [cc] server*, <https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server>, Accessed on 2021-10-11.
- [7] Avast, *¿qué es una botnet?* <https://www.avast.com/es-es/c-botnet#gref>, Accessed on 2021-10-11.
- [8] Kaspersky, *Zeus trojan malware*, <https://latam.kaspersky.com/resource-center/threats/zeus-virus>, Accessed on 2021-10-11.
- [9] A. de la Unión Europea para la Seguridad de las Redes y la Información, *Identification and handling of electronic evidence*, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational/#identification_handling, Accessed on 2021-09-11.
- [10] V. Total, *Virustotal*, <https://www.virustotal.com/gui/file/32712e24aba78fa0665f170275c3e55bb0591502b4757b670e702e68ca1072c5>, Accessed on 2021-10-11.
- [11] IBM, *Ibm x-force exchange*, <https://exchange.xforce.ibmcloud.com/malware/32712e24aba78fa0665f170275c3e55bb0591502b4757b670e702e68ca1072c5>, Accessed on 2021-10-11.