

Hecho por:

*Ruiz Muñoz Martin Guadalupe.*



*Estudios de casos de ciberseguridad.*

*Mtro. Enrique Hoyos Peña*

Fecha: 28/04/2025

***Introducción:***

el análisis de evidencias en sistemas operativos obsoletos —como Windows 7— representa un desafío técnico y metodológico. Este reporte documenta el proceso de investigación realizado sobre la imagen forense win7.img, asociada a la computadora de un usuario, utilizando eventos potencialmente maliciosos.

La investigación se centró en tres hallazgos clave obtenidos mediante Axiom Examine:

Un archivo winlogon.exe corrupto, sugerente de manipulación por malware (ej. inyección de código o rootkits).

La recuperación de la contraseña de la máquina virtual, permitiendo el acceso al sistema.

Un archivo cv {1}.pdf malicioso, vinculado a posibles exploits de la época.

Además, se realizaron pruebas de conexión remota para determinar si el sistema fue comprometido mediante protocolos como RDP (Remote Desktop Protocol).

El objetivo final es sustentar técnicamente las hipótesis sobre el daño del sistema y como sufrió el ataque la víctima.

Método Analítico:

Objetivo: Entender el origen.

Identificar la fuente:

- Posiblemente descargada. (Un CV).

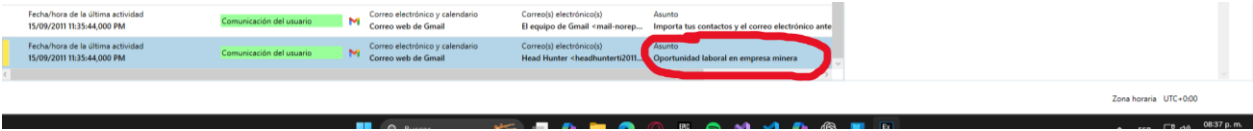
EVIDENCIA (5)

TODA LA EVIDENCIA

Nombre	Tipo	Extensión	Tamaño	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

Contexto de aparición:

- Enviada por terceros, en los correos que tenía, se menciona una entrevista de trabajo, por una posible “Empresa minera” quizá le mandaron un (CV) como ejemplo de le gustan los currículos a la empresa y ahí inicio.



- Direcciones del posible intruso. (Dominio externo "186.73.132.237").

Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo \\FNC\Users\Vassa\Documents\winlogon.exe	INFORMACIÓN DEL ARTEFACTO
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo \\FNC\Users\Vassa\Downloads\winlogon.exe	URL http://186.73.132.237/winlogon.exe
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo \\FNC\Users\Vassa\Documents\winlogon.exe	Última marca por fecha/hora de host local 13/09/2011 09:51:59,907 PM
Sistema operativo Shim Cache	Nombre del archivo winlogon.exe	Ruta de archivo C:\Users\Vassa\Documents\winlogon.exe	Recuento de recuperación de caché 1
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe	Nombre de archivo winlogon[1].exe
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe	Tipo 3 Registros de caché de Internet Explorer
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe	ID del elemento 44888
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe	INFORMACIÓN DE EVIDENCIA
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe	Fuente win7.img - Partition 1 (Microsoft NTFS, 20 GB)\System Volume Information\{bae4141e-de30-11e0-bc54-000c29b8c4af}\3808876b-c176-4e48-b7ae-04046ebcc752
Web relacionada Historial de Internet Explorer	URL http://186.73.132.237/winlogon.exe	Método de recuperación Moldeado	Fuente borrada
		Ubicación File Offset 9012768	

Definición: Término general para cualquier software malicioso.

Ejemplos: Virus, gusanos, troyanos, ransomware, spyware, etc.

## 2. Malware por inyección

Definición: Técnica donde el malware se introduce en un sistema explotando vulnerabilidades, como inyección de código (ej. SQL, DLL, JavaScript).

Cómo funciona: Inyección SQL: Inserta comandos SQL maliciosos en entradas de bases de datos.

Inyección de DLL: Carga bibliotecas maliciosas en procesos legítimos.

Objetivo: Robar datos, tomar control o corromper sistemas.

## 3. Indicadores de phishing

Frases como "Join our Community" o "plan an API key" son señales de engaño.

## 4. Troyano (Trojan)

Definición: Malware que se disfraza de software legítimo para engañar a los usuarios y ejecutar acciones maliciosas.

## 5. Exploit

Definición: Código o técnica que aprovecha vulnerabilidades en software/hardware para causar comportamientos no deseados.

## 6. Backdoors

Definición: Punto de acceso secreto que evade los controles de seguridad para permitir acceso remoto no autorizado.

## 7. Rootkits

Definición: Conjunto de herramientas que ocultan procesos, archivos o privilegios de malware para mantener acceso administrativo (root) en un sistema.

## ***Análisis estructural:***

Objetivo: Detectar incoherencias.

Iniciamos por validar en VirusTotal, las primeras evidencias encontradas en Examine brindadas por la misma aplicación, las cuales son las CV.

## EVIDENCIA (5)

Todas las subcarpetas Vista de

Nombre	Tipo	Ext...	Tama...	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

39/60 security vendors flagged this file as malicious

7a274612f5179b01fbd1df7c765497a5170ff45d133b3b879a9ad3c3b11d

plugin-aiEL10WT1yqYiw

Size: 44.96 KB | Last Analysis Date: 2 years ago

pdf js-embedded exploit autoaction invalid-refacroform cve-2010-2883

DETECTION DETAILS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Vendor	Detection	Do you want to automate checks?
Ad-Aware	Exploit.PDF-Name.2.Gen	AhnLab-V3 JS/SARS.S149
ALYac	Exploit.PDF-Name.2.Gen	Antiy-AVL Trojan/Generic.ASDOH.F
Avast	JS:Pdfka-ASM [Exp]	AVG JS:Pdfka-ASM [Exp]
Avira (no cloud)	EXP:Pdfka.CA.2	Baidu JS.Exploit.Pdfka.aaa
BitDefender	Exploit.PDF-Name.2.Gen	ClamAV Pdf.Dropper.Agent-6237548-0
Comodo	Malware@#24vds0334let2	Cynet Malicious (score: 99)
Cyren	ShellCode.CV.gen	DrWeb SCRIPTVirus
Emsisoft	Exploit.PDF-Name.2.Gen (B)	eScan Exploit.PDF-Name.2.Gen
ESET-NOD32	JS/Exploit.Pdfka.PAO	Fortinet JS/Pdfka.PAO/exploit
GData	Exploit.PDF-Name.2.Gen	Google Detected

En esa imagen podemos encontrar un ejemplo legítimo de lo que viene siendo un malware que es:

Trojan: Win32/Emotet.D!MTB (Microsoft) vs. inventado: English/MP4-slama.Gen.

Falsificación de herramientas:

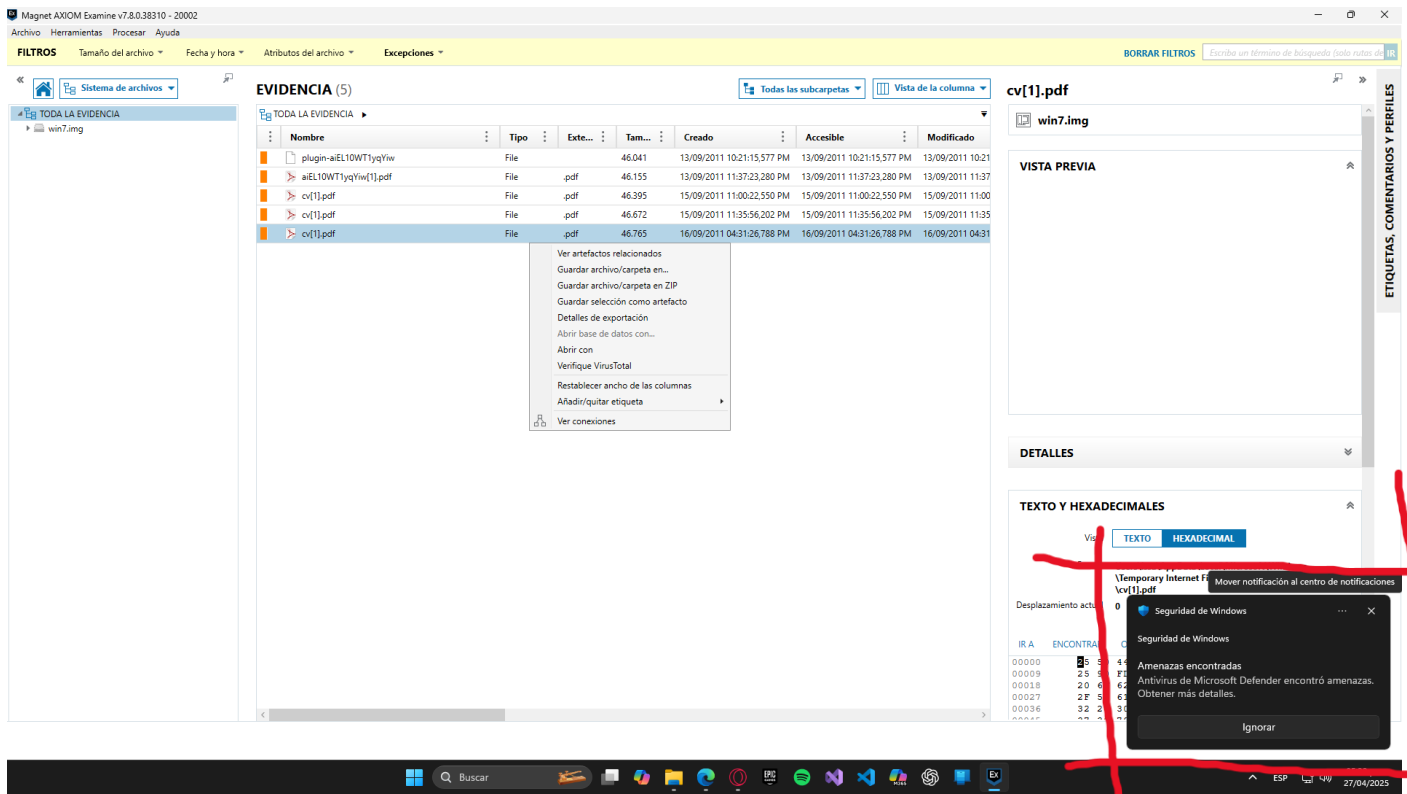
Marcas como "Claw MJ" o "Gymel" que no existen en la industria.

## Análisis Técnico:

Objetivo: Buscar evidencias técnicas de manipulación o malware.

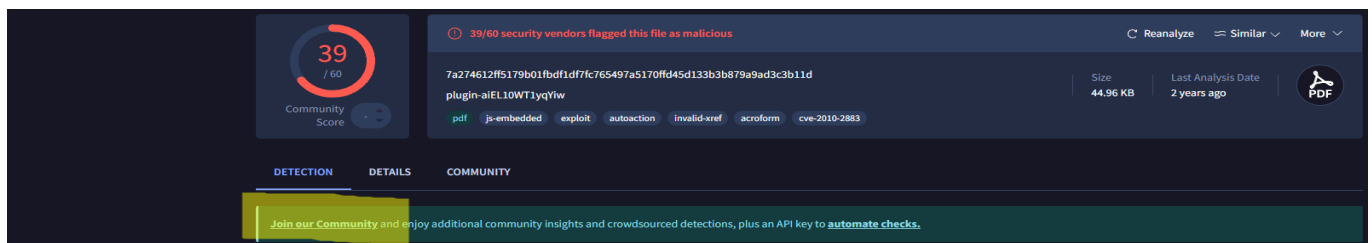
Extraer y analizar artefactos:

De las imágenes del punto anterior, podemos observar cómo nuestra evidencia parte de 5 archivos, de los cuales 4 son pdf e inclusive 3 cuentan con el mismo nombre, al usar Axiom Examine y VirusTotal, podemos obtener que cualquiera de los 5 archivos son maliciosos. Incluso al ejecutar cualquiera de estos 5, se recomienda abrir el Windows defender apenas hacer clic.



Al iniciar con la línea del tiempo, detectamos rutas que son el host de la maquina y rutas o direcciones externas, indicadores de phishing:

Frases como "Join our Community" o "plan an API key" son señales de engaño. (Referencia de VirusTotal).



Con esto, podemos tener correlación con amenazas y determinar que el reporte está vinculado a softwares maliciosos.

Malware activo: Archivo asociado a software malicioso.

**Método Sintético:**

Al iniciar con el escenario de ataque y continuando con la investigación por la línea del tiempo, obtenemos 3 archivos importantes, el primero un winlogon.exe posiblemente externo, ya que es detectado como aplicación, otro con el mismo nombre, pero de 2 años después y un host, también ejecutable y también como aplicación.

The screenshot displays the Magnet AXIOM Examine v7.8.0.38310 interface. The left pane shows the file system structure of 'win7.img', with 'System Volume Information' expanded. The main pane, titled 'EVIDENCIA (3)', lists three files:

Nombre	Tipo	Ext...	Tama...	Creado	Accesible	Modificado
SVCHOST.EXE-135A30D8.pf	File	.pf	18.068	13/09/2011 08:25:18,078 AM	13/09/2011 08:25:18,078 AM	15/09/2011 08
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01

The right pane shows the 'winlogon.exe' file selected, displaying its 'VISTA PREVIA' (Preview) and 'DETALLES' (Details). The preview shows the file's content, including registry paths and system files. The details section shows the file's metadata:

DETALLES DE ARCHIVO	
Nombre del archivo	winlogon.exe
Extensión del archivo	.exe
Tamaño lógico	285.696 bytes
Creado	13/07/2009 11:37:04,754 PM
Accesible	13/07/2009 11:37:04,754 PM
Modificado	14/07/2009 01:14:45,558 AM
MFT modificado	13/09/2011 09:15:43,640 AM

Como se muestra en la imagen en la parte inferior derecha, podemos ver que el archivo “Winlogon” cuenta con 4 fechas, de creación, de acceso, de modificación y de modificación MFT que es la modificación de la carpeta sin necesidad del contenido como tal.

NOTA:

“La Fecha de Modificación MFT es clave en análisis forense para:

Identificar cambios en metadatos (no solo en contenido).

Detectar manipulación maliciosa de archivos.

Reconstruir eventos en investigaciones de seguridad.” Obtenido de: [DeepSeek - Into the Unknown](https://www.deepseek.com/) .

Lo interesante de esto, es que si vamos a la ultima fecha, nos redirecciona a el 13 de septiembre de 2011, donde encontramos otros archivos winlogon y algunos otros sospechosos, sin ruta perteneciente al host principal, además de más evidencia que puede servirnos para más adelante. Como contraseñas, información personal, correo, descargas e historial de navegación.

Magnet AXIOM Examine v7.8.0.38310 - 20002

Archivo Herramientas Procesar Ayuda

FILTROS Evidencia Artefactos Tipos de datos Fecha y hora Atributos de fecha y hora Categorías de línea de tiempo Etiquetas y comentarios

13/07/2009 09:08:20 PM - 13/07/2009 11:57:43 PM

IR A LA FECHA 2:00M HORAS + PÁGINA

Establecer tiempo relativo

Para ver pruebas en torno a la hora de una fecha específica, establezca una fecha como ancla y, luego, establezca un rango de horas en torno a esa fecha.

ANCLA RELATIVA A

Fecha 13/09/2011

Hora 09 : 15 AM

ESTABLECER RANGO

☒ Use el mismo rango de hora para antes y después de la fecha definida.

Rango Minutos

CANCELAR ACEPTAR

data @.reloc USER32.dll msvcrt.dll ntdll.dll API-MS-Win-Core-LocalRegistry-L1-1-0.dll API-MS-Win-Security-Base-L1-1-0.dll WINSTA.dll RPCRT4.dll KERNEL32.dll TracingControlLevel SYSTEM CurrentControlSet Control Winlogon

DETALLES

DETALLES DE ARCHIVO

Nombre del archivo winlogon.exe

Extensión del archivo .exe

Tamaño lógico 285.696 bytes

Creado 13/07/2009 11:37:04,754 PM

Accesible 13/07/2009 11:37:04,754 PM

Modificado 14/07/2009 01:14:45,558 AM

MFT modificado 13/09/2011 09:15:43,640 AM

Clúster 189911

Recuento de clúster 70

Ubicación física 777875456

Sector físico 1519288

Hash MD5 8ec6a4ab12b8f3759e21f8e3a388f2cf

Número de registro de MFT 20640

Número de registro de MFT principal 1990

Identificación de seguridad 454 (S-1-5-80-95600885-3418522649-1831038044-1853292631-2271478464)

Atributos del archivo Archive

Zona horaria UTC+000

13 de sep. de 2011 8:36 13 de sep. de 2011 9:06 13 de sep. de 2011 9:36 13 de sep. de 2011 10:06 13 de sep. de 2011 10:36 13 de sep. de 2011 11:06 13 de sep. de 2011 11:36 13 de sep. de 2011 12:06 13 de sep. de 2011 12:36 13 de sep. de 2011 13:06

< 4 DE 4 MARCAS DE TIEMPO >

Fecha/hora	Categoría de línea...	Artefacto	Información de...	Información de a...
MFT modificado 13/09/2011 09:15:43,640 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe
MFT modificado 13/09/2011 09:15:43,640 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre x86_microsoft-windows-...environment-windows...	Extensión del archivo .exe_75835076
MFT modificado 13/09/2011 09:15:43,640 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe
MFT modificado 13/09/2011 09:15:43,656 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winmm.dll	Extensión del archivo .dll
MFT modificado 13/09/2011 09:15:43,656 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre x86_microsoft-windows-winlogon_31bf3856ad36...	Extensión del archivo .exe_ac37d0c5
MFT modificado 13/09/2011 09:15:43,656 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winmm.dll	Extensión del archivo .dll
MFT modificado 13/09/2011 09:15:43,671 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winnsi.dll	Extensión del archivo .dll
MFT modificado 13/09/2011 09:15:43,671 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winnsi.dll	Extensión del archivo .dll
MFT modificado 13/09/2011 09:15:43,671 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre x86_microsoft-windows-audio-mmecore-base_31...	Extensión del archivo .dll_08d445e8
MFT modificado 13/09/2011 09:15:43,671 AM	Conocimiento del archivo	Sistema de archivos Archivo	Nombre winnsi.dll	Extensión del archivo .dll

Nombre del archivo winlogon.exe

Extensión del archivo .exe

Tamaño lógico 285.696 bytes

Creado 13/07/2009 11:37:04,754 PM

Accesible 13/07/2009 11:37:04,754 PM

Modificado 14/07/2009 01:14:45,558 AM

MFT modificado 13/09/2011 09:15:43,640 AM

Clúster 189911

Recuento de clúster 70

Ubicación física 777875456

Sector físico 1519288

Hash MD5 8ec6a4ab12b8f3759e21f8e3a388f2cf

Número de registro de MFT 20640

Número de registro de MFT principal 1990

Identificación de seguridad 454 (S-1-5-80-95600885-3418522649-1831038044-1853292631-2271478464)

Atributos del archivo Archive

INFORMACIÓN DE EVIDENCIA

Fuente win7.jmg - Partition 1 (Microsoft NTFS, 20 GB)\Windows\winsxs\x86\_microsoft-windows-winlogon\_31bf3856ad364e35\_6.1.7600.16385\_none\_6f99573a36451166\winlogon.exe

Número de evidencia win7.jmg

TEXTO Y HEXADECIMALES

Vista TEXTO HEXADECIMAL

Zona horaria UTC+000

Esto puede significar o relacionar el winlogon.exe corrupto con posibles inyecciones de malware como un troyano o incluso un rootkit completo.

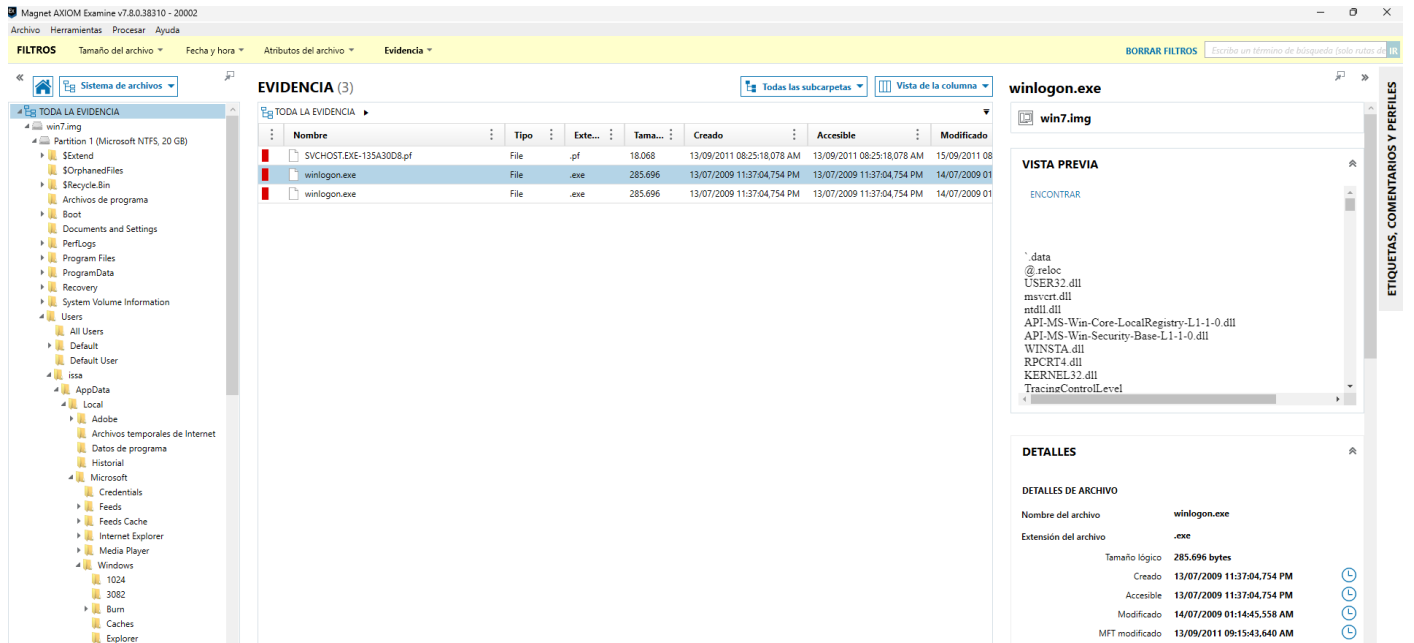
## ***MATERIAL DE ESTUDIO***

Contamos con diversos materiales, iniciando por la imagen forense: win7.img natural para la extracción de información en Axiom process y los datos de examine y esta misma en una máquina virtual (convertida a VDI).

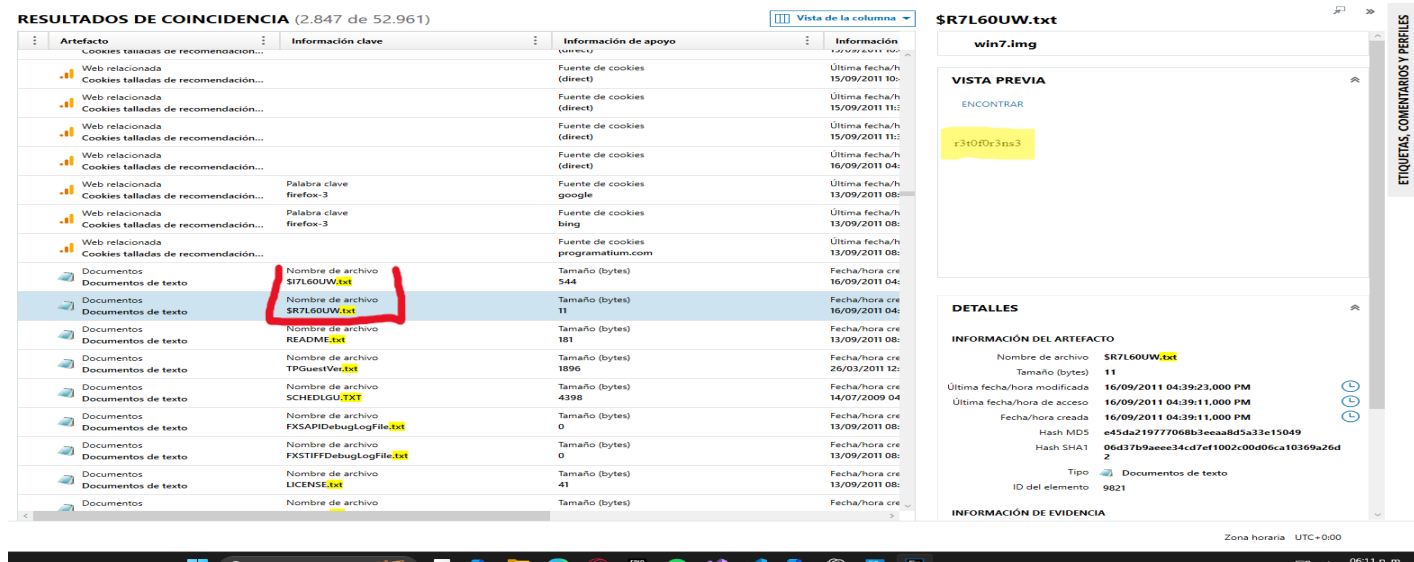
Utilizamos herramientas tales como: Axiom Process, Examine, kali linux y VirtualBox.

Evidencias:

Winlogon corrupto.



Contraseña ¿de la VM?... (r3t0f0r3ns3)



PDFs maliciosos.



TODA LA EVIDENCIA ▶

Nombre	Tipo	Ext...	Tama...	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

## ANÁLISIS DEL CASO:

- La víctima descargó archivos “pdf” dañados, aparentemente lo que es un CV y uno más que podría ser parte de lo mismo del CV u otro intento con algún nombre random sin conocer como luego a descargarse.
- Se ejecuta con dicho código malicioso.
- El archivo abre espacio a la ejecución de un Troyano que cuenta con un winlogon externo perteneciente a un dominio 186.73.132.237.
- El atacante obtiene acceso al pc de la víctima.
- Cambia la configuración de sistema y ejecuta el malware apenas se inicie el sistema.

no olvidemos que, en 2011, malware como Duqu o ZeroAccess secuestraba winlogon.exe para persistencia.

### Evidencia

PDF malicioso:

Exploits en PDF reader (Que curiosamente el icono del CV es de adobe acrobat a pesar de ser PDF.).

### Datos

Hasta el momento, podemos observar y obtener los siguientes datos y son, que el exploit se intento mas de una sola vez, pues tenemos el mismo malware en el pdf en distintas fechas y algún otro pdf también con código malicioso, tenemos que a través de ellos se obtuvieron unos datos personales como lo son su correo y lo que conlleva a que sea seguramente su nombre.

Correo: [miguelsalinas.listas@gmail.com](mailto:miguelsalinas.listas@gmail.com)

Posible nombre de la víctima: Miguel Salinas

## MARCO TEÓRICO / Análisis del caso

Hasta el momento, hemos recabado información suficiente para hacer una posible hipótesis de lo sucedido.

Tenemos que examinando a win7.img nos topamos con una imagen de un disco virtual infectado con malware, trabajando con el llegamos a la sospecha de que se realizó la descarga del malware a través de un presunto CV y con ello se le dio acceso al atacante con el posible troyano, si lo desarrollamos en el mismo formato que en estudios del caso, podemos obtener lo siguiente:

#### Hipótesis:

Nuestra víctima de posible nombre Miguel, descargo un CV interesado en algún trabajo, sin darse cuenta de que estaba siendo víctima de malware y dando entrada a los atacantes a su máquina.

El CV se puede relacionar a la oferta de trabajo que tenía en su correo y a su vez a la descarga de Adobe Acrobat Reader para poder descargar el CV o cualquier otro PDF infectado sin que él lo supiera.

Lo que a mí me hace pensar e hilar que se le ofreció un trabajo, se le pidió que descargara un PDF dañado y para descargarlo o poderlo ejecutar, se le pidió que se instalara “Adobe Acrobat Reader”.

Elementos del hecho:  
Esta persona en base a sus correos recibidos, historial de navegación y hechos observados en Axiom, descargo Adobe Acrobat Reader, tiene o tuvo en su máquina PDF infectados y también tiene ofertas de trabajo en una empresa minera, ejecuto el malware pensando que era un CV y daño su máquina.

Datos de prueba:  
Su historial y descargas.  
Los PDFs como evidencia en Axiom Examine por el mismo software  
El winlogon de host y el de aplicación.

#### ¿Qué necesito?

Detalles de la ejecución del malware.

Recopilación de los datos personales robados y para que.

Evidencia valida y dar con el posible atacante para llevarlo a un proceso legal.

#### ¿Por qué paso?

Porque Miguel descargo “PDFs” infectados.

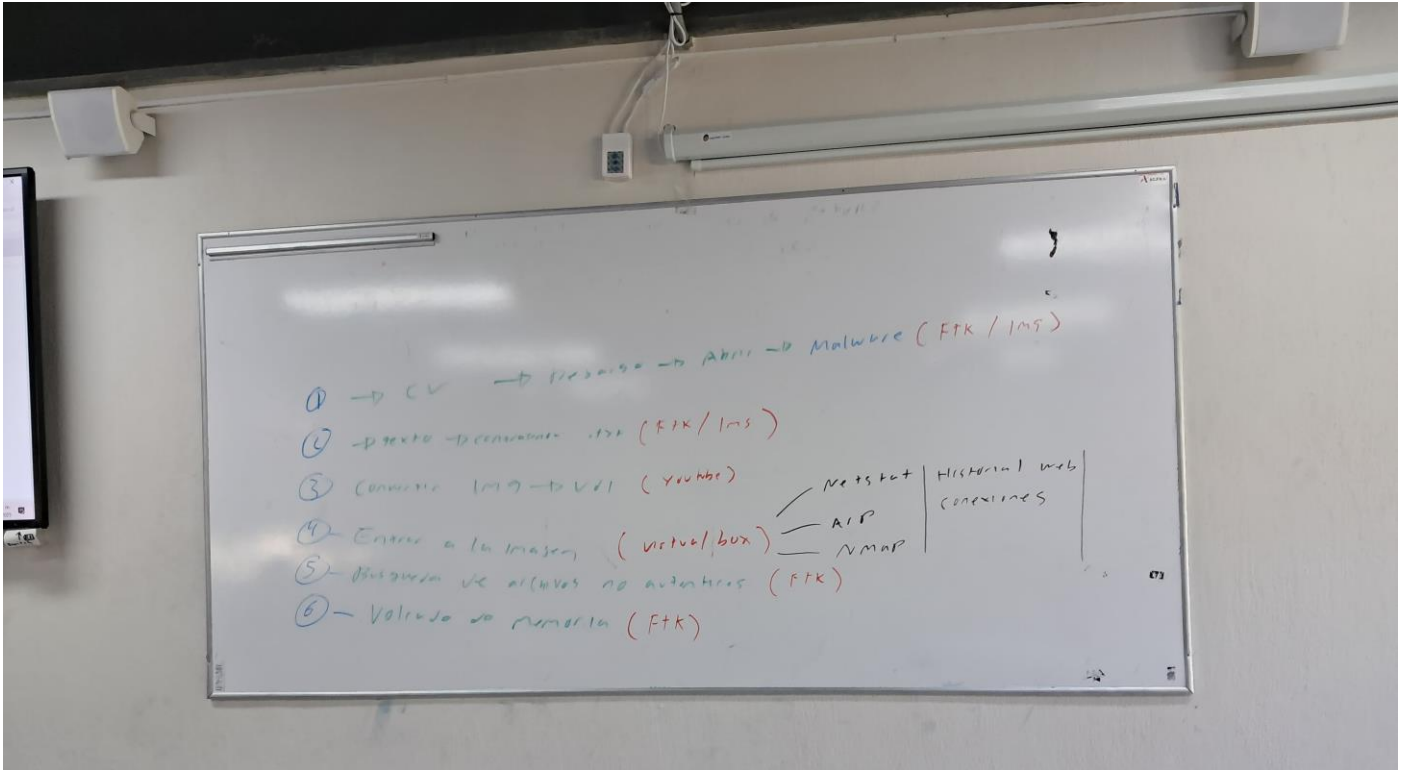
#### ¿Quién es el responsable?

El atacante y Miguel.

¿Cómo se puede prevenir?  
Ahora basta con tener tu sistema actualizado y con un antivirus, en ese año desconozco cuales eran los protocolos o las medidas de seguridad, pero supongo verificar que fuese un PDF, aunque quizá para el año y si no saben del tema, mas personas como Miguel podrían caer.

## ***Procedimiento con capturas: (Paso a Paso).***

Primero, iniciamos con lo que sabemos desde clase:

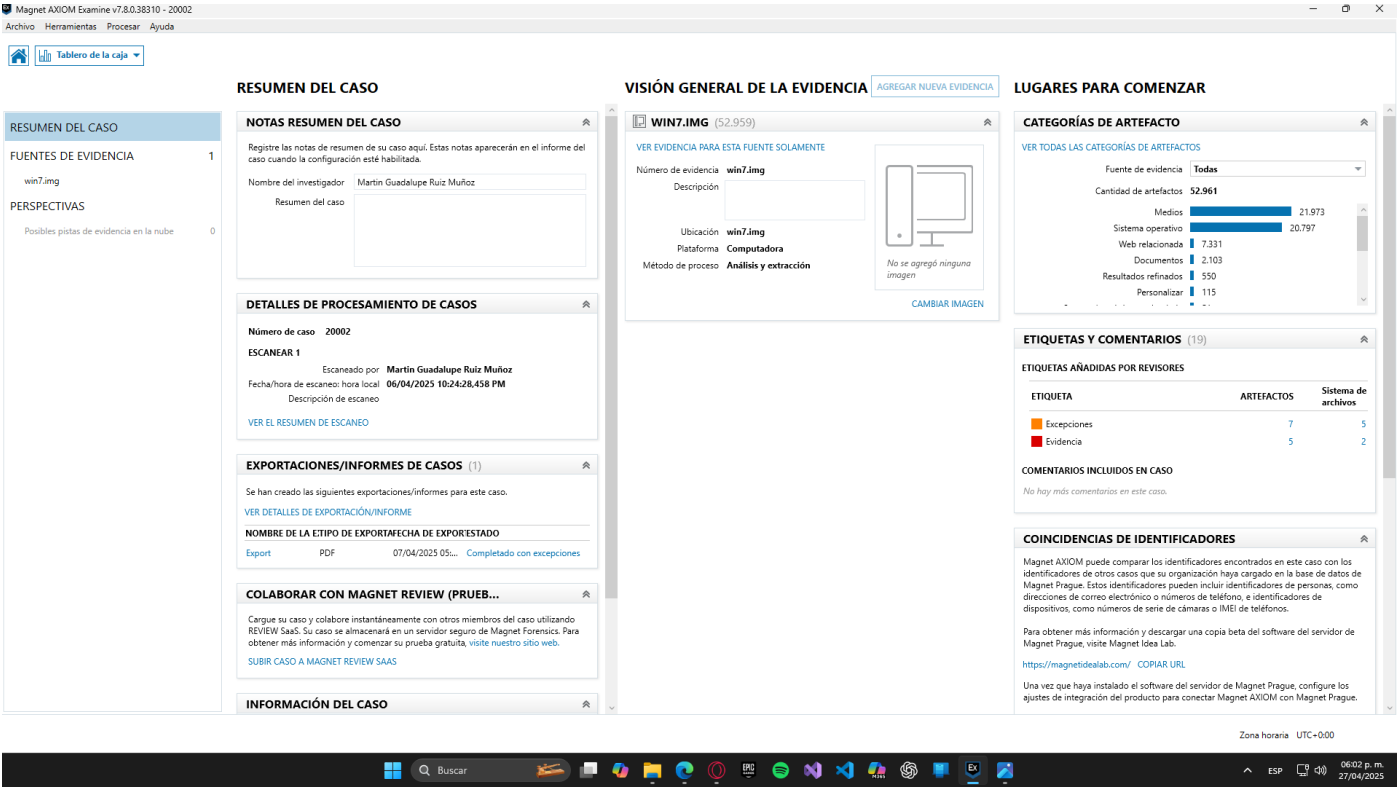


Donde contábamos con 6 puntos claves

- El CD infectado.
- El txt de la contraseña en caso de requerirse de alguna.
- La conversión de img a vdi para VB.
- La extracción de la imagen en la VB.
- La búsqueda de archivos.
- Y el volcado de memoria.

Una vez sabiendo esto, realizaríamos la mayoría de los puntos con el Axiom y con la ayuda del virtual box, los restantes.

Iniciamos cargando el caso y el img al Axiom, después, seleccionando la img y realizando el proceso de examinación hasta llegar al Examine.



Después Analizamos la evidencia de sistema dada por la app examine (Los CVs).

## EVIDENCIA (5)

TODAS LAS SUBCARPETAS

VISTA DE

Nombre	Tipo	Ext...	Tama...	Creado	Accesible	Modificado	MFT modificado
plugin-aiEL10WT1yqYiw	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:23,061 PM	13/09/2011 10:21:23,061 PM
aiEL10WT1yqYiw[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:26,655 PM	01/01/1601 01:57:31,117 PM
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:24,691 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:57,702 PM	01/01/1601 12:31:37,156 PM
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:28,163 PM	01/01/1601 12:31:37,156 PM

Documento 16.docx

VirusTotal - File - Be633276b762d774c1a81a2f9fc46adb073fce0c67b1c1db74c2811507baadc

https://www.virustotal.com/gui/file/Be633276b762d774c1a81a2f9fc46adb073fce0c67b1c1db74c2811507baadc

Importar favoritos

WhatsApp

resovet

YouTube

ChatGPT

8e633276b762d774c1a81a2f9fc46adb073fce0c67b1c1db74c2811507baadc

Sign in

Sign up

42 / 65

Community Score

42/65 security vendors flagged this file as malicious

Be633276b762d774c1a81a2f9fc46adb073fce0c67b1c1db74c2811507baadc

cv[1].pdf

pdf

autoaction

invalid.sref

js-embedded

exploit

acroform

cve-2010-2883

Size

45.58 KB

Last Analysis Date

5 months ago

PDF

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.name/pdfka

Threat categories

trojan

Family labels

name pdfka pdfdef

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3

PDF/Exploit

ALYac

Exploit.PDF-Name.2.Gen

Arcabit

Exploit.PDF-Name.2.Gen

Avast

JS.Pdfka.ASM [Exp]

AVG

JS.Pdfka.ASM [Exp]

Avira (no cloud)

EXP/Pdfka.F.B.31

Baidu

JS.Exploit.Pdfka.aaa

BitDefender

Exploit.PDF-Name.2.Gen

ClamAV

Heuristics.PDF.ObfuscatedNameObject

CTX

Pdf.exploit-kit.name

Cyance

Unsafe

Cynet

Malicious (score: 98)

DrWeb

SCRIPT.Virus

Emsisoft

Exploit.PDF-Name.2.Gen (B)

eScan

Exploit.PDF-Name.2.Gen

ESET-NOD32

JS/Exploit.Pdfka.PAO

Fortinet

JS/Pdfka.PAO.exploit

GData

Exploit.PDF-Name.2.Gen

Luego, pasamos a la línea del tiempo, donde manualmente tenemos que buscar actividad sospechosa o directamente malwares.

**FILTROS** Evidencia ▾ Artículos ▾ Tipos de datos ▾ Fecha y hora ▾ Alímbitos de fecha y hora ▾ Categorías de línea de tiempo... ▾ Etiquetas y comentarios ▾ BÚSCUDA 🔍

**Línea de tiempo**

13/07/2009 09:08:20 PM - 13/07/2009 11:57:43 PM

IR A LA FECHA [icon] ZOOM [slider] HORAS [dropdown] PÁGINA [arrows]

< 2 DE 4 MARCAS DE TIEMPO >

Fecha/hora	Categoría de línea...	Artículo	Información clave	Información de a...	Tamaño
Creado 13/07/2009 11:37:04,754 PM	[icon] Conocimiento del archivo	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe	Tai 28
Accesible 13/07/2009 11:37:04,754 PM	[icon] Apertura de archivo/carpeteta	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe	Tai 28
Accesible 13/07/2009 11:37:04,754 PM	[icon] Apertura de archivo/carpeteta	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe	Tai 28
Creado 13/07/2009 11:37:04,754 PM	[icon] Conocimiento del archivo	Sistema de archivos Archivo	Nombre winlogon.exe	Extensión del archivo .exe	Tai 28
Creado 13/07/2009 11:37:05,705 PM	[icon] Conocimiento del archivo	Sistema de archivos Archivo	Nombre winbiosensoradapter.dll	Extensión del archivo .dll	Tai 11C
Accesible 13/07/2009 11:37:05,705 PM	[icon] Apertura de archivo/carpeteta	Sistema de archivos Archivo	Nombre winbiosensoradapter.dll	Extensión del archivo .dll	Tai 11C
Accesible 13/07/2009 11:37:05,705 PM	[icon] Apertura de archivo/carpeteta	Sistema de archivos Archivo	Nombre winbiosensoradapter.dll	Extensión del archivo .dll	Tai 11C
Creado 13/07/2009 11:37:05,705 PM	[icon] Conocimiento del archivo	Sistema de archivos Archivo	Nombre winbiosensoradapter.dll	Extensión del archivo .dll	Tai 11C
Accesible 13/07/2009 11:37:06,345 PM	[icon] Apertura de archivo/carpeteta	Sistema de archivos Archivo	Nombre winblostoragelocation.dll	Extensión del archivo .dll	Tai 57
Accesible	[icon]	Sistema de archivos	Nombre	Extensión del archivo	Tai

### VISTA PREVIA

ENCONTRAR

```
.data
@reloc
USER32.dll
msvrt.dll
ntdll.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
API-MS-Win-Security-Base-L1-1-0.dll
WINSTA.dll
RPCRT4.dll
KERNEL32.dll
TracingControlLevel
SYSTEM CurrentControlSet Control Winlooeon
```

### DETALLES

#### DETALLES DE ARCHIVO

Nombre del archivo winlogon.exe

Extensión del archivo .exe

Tamaño lógico 285.696 bytes

Creado 13/07/2009 11:37:04,754 PM

Accesible 13/07/2009 11:37:04,754 PM

Modificado 14/07/2009 01:14:45,558 AM

MFT modificado 13/09/2011 09:15:43,640 AM

Clúster 189911

Recuento de clúster 70

Ubicación física 777875456

Sector físico 1519288

Hash MD5 8cc6a4b12b8f3759e2118e3a388f2cf

Número de registro de MFT 20640

Zona horaria UTC+000

### RESULTADOS DE COINCIDENCIA (159 de 52.961)

Artefacto	Información clave	Información de apoyo
Sistema operativo Archivos de búsqueda previa de Win...	Nombre de la aplicación MCONFIG.EXE	Ruta de la aplicación \\DEVICE\\HARDISK\\VOLUME\\WINDOWS\\SYSTEM.
Sistema operativo Archivos de búsqueda previa de Win...	Nombre de la aplicación <b>WINLOGON.EXE</b>	Ruta de la aplicación \\DEVICE\\HARDISK\\VOLUME\\USERS\\ISSA\\DOWN.
Sistema operativo Shim Cache	Nombre del archivo <b>winlogon.exe</b>	Ruta de archivo \\77\\C\\Users\\Issa\\Documents\\ <b>winlogon.exe</b>
Sistema operativo Shim Cache	Nombre del archivo <b>winlogon.exe</b>	Ruta de archivo \\77\\C\\Users\\Issa\\Downloads\\ <b>winlogon.exe</b>
Sistema operativo Shim Cache	Nombre del archivo <b>winlogon.exe</b>	Ruta de archivo \\77\\C\\Users\\Issa\\Documents\\ <b>winlogon.exe</b>
Sistema operativo MUICache	Nombre del archivo <b>winlogon.exe</b>	Ruta de archivo C:\\Users\\Issa\\Documents\\ <b>winlogon.exe</b>
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo x-msdos-program
Web relacionada Registros de caché de Internet Explorer	Nombre de archivo winlogon[1].exe	Tipo de archivo exe
Web relacionada Historial de Internet Explorer		URL <a href="http://186.73.132.237/winlogon.exe">http://186.73.132.237/winlogon.exe</a>
Web relacionada Historial de Internet Explorer		URL <a href="http://186.73.132.237/winlogon.exe">http://186.73.132.237/winlogon.exe</a>
Web relacionada Historial de Internet Explorer		URL <a href="http://186.73.132.237/winlogon.exe">http://186.73.132.237/winlogon.exe</a>
Web relacionada Historial de Internet Explorer		URL <a href="http://186.73.132.237/winlogon.exe">http://186.73.132.237/winlogon.exe</a>
Etiquetado desde el sistema de archivos EXE	Nombre <b>winlogon.exe</b>	Tipo File
Etiquetado desde el sistema de archivos EXE	Nombre <b>winlogon.exe</b>	Tipo File

### http://186.73.132.237/winlogon.exe

win7.img

DETALLES

**INFORMACIÓN DEL ARTEFACTO**

URL <http://186.73.132.237/winlogon.exe>

Última marca por fecha/hora de host local  
13/09/2011 09:41:49.907 PM

Recuento de recuperación de caché  
1

Nombre de archivo  
**winlogon[1].exe**

Tipo de archivo  
**exe**

Tipo  
Registros de caché de Internet Explorer

ID del elemento  
44888

**INFORMACIÓN DE EVIDENCIA**

Fuente  
[win7.img - Partition 1 \(Microsoft NTFS, 20 GB\)\\System Volume Information\\\[9ac4141e-de50-11e0-bc54-000c29b8c4af\]\[3808876b-c176-4e48-b7ae-04046e6cc752\]](#)

Método de recuperación  
Moldeado

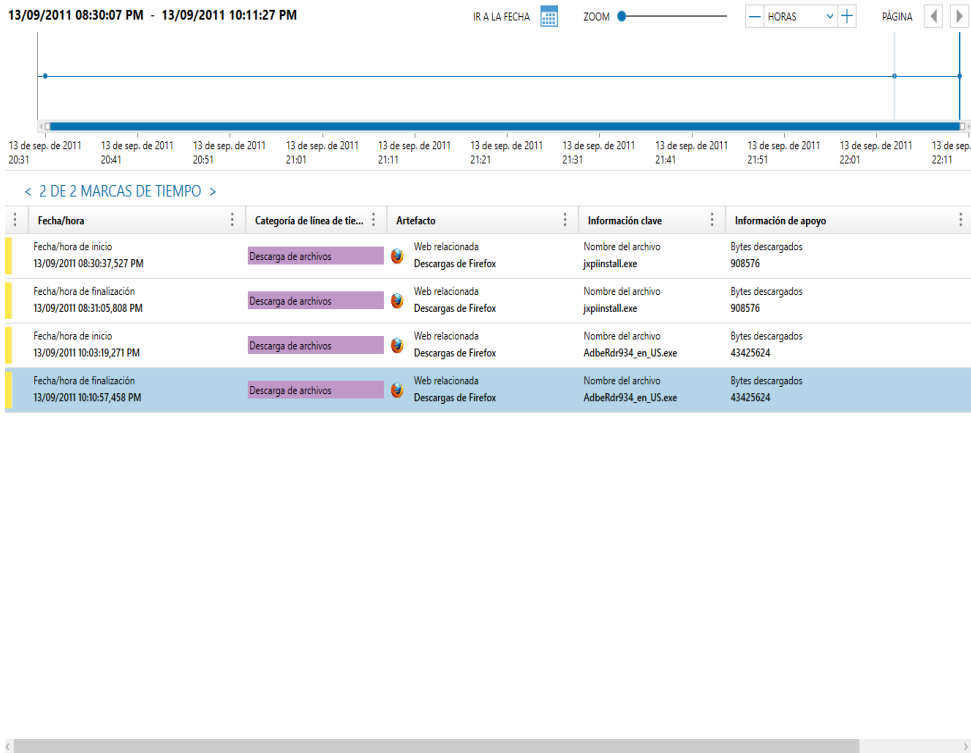
Fuente borrada

Ubicación  
[File Offset 9012768](#)

Número de evidencia  
win7.img

Zona horaria UTC+0:00

La descarga de adobe reader.



### win7.img

#### DETALLES

##### INFORMACIÓN DEL ARTEFACTO

Nombre del archivo: AdbRdr934\_en\_US.exe  
Descargar fuente: [http://download.oldapps.com/Adobe\\_Reader/AdbRdr934\\_en\\_US.exe](http://download.oldapps.com/Adobe_Reader/AdbRdr934_en_US.exe)  
Fecha/hora de inicio: 13/09/2011 10:03:19.271 PM  
Fecha/hora de finalización: 13/09/2011 10:10:57.458 PM  
Guardado en: file:///C:/Users/issa/Downloads/AdbRdr934\_en\_US.exe  
Estado: Download Complete  
Referente: [http://www.oldapps.com/adobe\\_reader.php?old\\_adobe=247download](http://www.oldapps.com/adobe_reader.php?old_adobe=247download)  
Bytes descargados: 43425624  
Tamaño de archivo (bytes): 43425624  
Tipo: Descargas de Firefox  
ID del elemento: 40063

##### INFORMACIÓN DE EVIDENCIA

Fuente: win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\issa\AppData\Roaming\Mozilla\Firefox\Profiles\z9lx75up.default\downloads.sqlite  
Método de recuperación: Analizado  
Fuente borrada  
Ubicación: Table: moz\_downloads(id: 2)  
Número de evidencia: win7.img

## Y los ejecutables del winlogon y el host en .exe

Magnet AXIOM Examine v7.8.0.38310 - 20002

Archivo Herramientas Procesar Ayuda

FILTROS Tamaño del archivo Fecha y hora Atributos del archivo Evidencia BORRAR FILTROS Escribe un término de búsqueda (solo rutas de

### EVIDENCIA (3)

Nombre	Tipo	Ext...	Tama...	Creado	Accesible	Modificado
SVCHOST.EXE-135A30D8.pf	File	.pf	18.068	13/09/2011 08:25:18,078 AM	13/09/2011 08:25:18,078 AM	15/09/2011 08
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01
winlogon.exe	File	.exe	285.696	13/07/2009 11:37:04,754 PM	13/07/2009 11:37:04,754 PM	14/07/2009 01

### winlogon.exe

#### VISTA PREVIA

ENCONTRAR

.data  
@ reloc  
USER32.dll  
msvert.dll  
ntdll.dll  
API-MS-Win-Core-LocalRegistry-L1-1-0.dll  
API-MS-Win-Security-Base-L1-1-0.dll  
WINSTA.dll  
RPCRT4.dll  
KERNEL32.dll  
TracinaControlLevel

#### DETALLES

##### DETALLES DE ARCHIVO

Nombre del archivo: winlogon.exe  
Extensión del archivo: .exe  
Tamaño lógico: 285.696 bytes  
Creado: 13/07/2009 11:37:04,754 PM  
Accesible: 13/07/2009 11:37:04,754 PM  
Modificado: 14/07/2009 01:14:45,558 AM  
MFT modificado: 13/09/2011 09:15:43,640 AM

Días después, obtenemos su historial: 15 de sep de 2011

RESULTADOS DE COINCIDENCIA (2.847 de 52.961)

Vista de la columna

Artefacto	Información clave	Información de apoyo	Información
Cookies talladas de primera visita de...	argentinawarez.com	1	13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión disqus.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión elcomercio.pe	Coincidencias 1	Fecha/hora de 15/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión filehippo.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión filetram.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 16/09/2011 04:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 15/09/2011 10:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 15/09/2011 10:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 15/09/2011 11:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 15/09/2011 11:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión google.com	Coincidencias 1	Fecha/hora de 16/09/2011 04:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión oldapps.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión peru21.pe	Coincidencias 1	Fecha/hora de 15/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión programatium.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de primera visita de...	Anfitrión softonic.com	Coincidencias 1	Fecha/hora de 13/09/2011 08:...
Web relacionada Cookies talladas de sesión de Google...	Anfitrión argentinawarez.com	Vistas de página 1	Eventos de enl 10
Web relacionada	Anfitrión	Vistas de página	Eventos de enl

peru21.pe

win7.img

DETALLES

INFORMACIÓN DEL ARTEFACTO

Anfitrión peru21.pe

Fecha/hora de creación 15/09/2011 08:57:21,000 PM

Fecha/hora de visita más reciente 15/09/2011 08:57:21,000 PM

2.ª fecha/hora de visita más reciente 15/09/2011 08:57:21,000 PM

Coincidencias 1

Tipo Cookies talladas de primera visita de Goo

ID del elemento 40385

INFORMACIÓN DE EVIDENCIA

Fuente win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\Issa\AppData\Roaming\Microsoft\Windows\Cookies\Low\Issa@peru21[1].txt

Método de recuperación Moldeado

Fuente borrada

Ubicación File Offset 89

Número de evidencia win7.img

Zona horaria UTC+0:00

Los primeros dos intentos de ejecución del CV.

Magnet AXIOM Examine v7.8.0.38310 - 20002

Archivo Herramientas Procesar Ayuda

FILTROS Tamaño del archivo Fecha y hora Atributos del archivo Excepciones BORRAR FILTROS

Sistema de archivos

win7.img

EVIDENCIA (5)

TODAS LAS SUBCARPETAS

Vista de la columna

Nombre	Tipo	Ext...	Tam...	Creado	Accesible	Modificado
plugin-aiEL10WT1yqf1w	File		46.041	13/09/2011 10:21:15,577 PM	13/09/2011 10:21:15,577 PM	13/09/2011 10:21
aiEL10WT1yqf1w[1].pdf	File	.pdf	46.155	13/09/2011 11:37:23,280 PM	13/09/2011 11:37:23,280 PM	13/09/2011 11:37
cv[1].pdf	File	.pdf	46.395	15/09/2011 11:00:22,550 PM	15/09/2011 11:00:22,550 PM	15/09/2011 11:00
cv[1].pdf	File	.pdf	46.672	15/09/2011 11:35:56,202 PM	15/09/2011 11:35:56,202 PM	15/09/2011 11:35
cv[1].pdf	File	.pdf	46.765	16/09/2011 04:31:26,788 PM	16/09/2011 04:31:26,788 PM	16/09/2011 04:31

Ver artefactos relacionados

Guardar archivo/carpet...

Guardar archivo/carpet...

Guardar selección como artefacto

Detalles de exportación

Abrir base de datos con...

Abrir con

Verifique VirusTotal

Restablecer ancho de las columnas

Añadir/quitar etiqueta

Ver conexiones

cv[1].pdf

win7.img

VISTA PREVIA

DETALLES

TEXTO Y HEXADECIMALES

Vista TEXTO HEXADECIMAL

Fuente Users\Issa\AppData\Local\Microsoft\Windows\Temporary Internet F...

Desplazamiento actual 0

IR A ENCONTRAR

Seguridad de Windows

Seguridad de Windows

Amenazas encontradas

Antivirus de Microsoft Defender encontró amenazas.

Obtener más detalles.

Ignorar

05:22 p. m.

27/04/2023



# Los correos recibidos:

15/09/2011 09:22:11 PM - 15/09/2011 11:36:23 PM

IR A LA FECHA

ZOOM

HORAS

PÁGINA



1 MARCA DE TIEMPO

Fecha/hora	Categoría de línea de tiempo	Artefacto	Información clave	Información de apoyo
Fecha/hora de la última actividad 15/09/2011 09:22:51,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Obtener Gmail en tu teléfono móvil
Fecha/hora de la última actividad 15/09/2011 09:22:51,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Personaliza Gmail con colores y temas.
Fecha/hora de la última actividad 15/09/2011 09:22:51,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Personaliza Gmail con colores y temas.
Fecha/hora de la última actividad 15/09/2011 09:31:21,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) Head Hunter <headhunter2011...	Asunto Oportunidad laboral en empresa minera
Fecha/hora de la última actividad 15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) Head Hunter <headhunter2011...	Asunto Oportunidad laboral en empresa minera
Fecha/hora de la última actividad 15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) Head Hunter <headhunter2011...	Asunto Oportunidad laboral en empresa minera
Fecha/hora de la última actividad 15/09/2011 10:46:47,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Importa tus contactos y el correo electrónico ante
Fecha/hora de la última actividad 15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) Head Hunter <headhunter2011...	Asunto Oportunidad laboral en empresa minera
Fecha/hora de la última actividad 15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Importa tus contactos y el correo electrónico ante
Fecha/hora de la última actividad 15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) El equipo de Gmail <mail-norep...	Asunto Importa tus contactos y el correo electrónico ante
Fecha/hora de la última actividad 15/09/2011 11:35:44,000 PM	Comunicación del usuario	Correo electrónico y calendario Correo web de Gmail	Correo(s) electrónico(s) Head Hunter <headhunter2011...	Asunto Oportunidad laboral en empresa minera

win7.img

DETALLES

INFORMACIÓN DEL ARTEFACTO

Correo(s) electrónico(s) Head Hunter <headhunter2011@gmail.com>  
Asunto Oportunidad laboral en empresa minera  
Fecha/hora enviada - hora local 15 de septiembre de 2011 16:31  
Fecha/hora de la última actividad 15/09/2011 11:35:44,000 PM  
Fragmento Estimado señor, hemos revisado su hoja de vida y tenemos interés en realizarle una entrevista ...  
Estado Read  
Tipo Correo web de Gmail  
ID del elemento 42145

INFORMACIÓN DE EVIDENCIA

Fuente win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\Visa\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\4XDWZ09\mail[1].htm  
Método de recuperación Moldeado  
Fuente borrada  
Ubicación File Offset 26149  
Número de evidencia win7.img

Zona horaria UTC+000

Y lo que aparentemente son ejecuciones de correo, donde se pueden obtener sus datos.

FILTROS Evidencia Artefactos Tipos de datos Fecha y hora Atributos de fecha y hora Categorías de línea de tiempo Etiquetas y comentarios mail listas@gmail.com BORRAR FILTROS Escribe un término de búsqueda...

Línea de tiempo

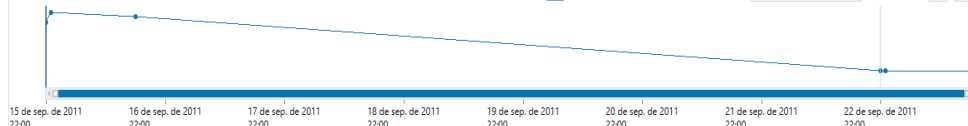
15/09/2011 09:51:08 PM - 23/09/2011 05:26:50 PM

IR A LA FECHA

ZOOM

DÍAS

PÁGINA



< 1 DE 2 MARCAS DE TIEMPO >

Fecha/hora	Categoría de línea de tiempo	Artefacto	Información clave	Información de apoyo
Fecha/hora creada 15/09/2011 10:46:52,215 PM	Uso del navegador	Web relacionada Cookies de Internet Explorer	Anfitrión mail.google.com/mail	Nombre gmailchat
Última fecha/hora modificada 15/09/2011 10:47:06,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Última fecha/hora de acceso 15/09/2011 10:47:06,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Fecha/hora creada 15/09/2011 10:47:06,000 PM	Conocimiento del archivo	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10520
Última fecha/hora modificada 15/09/2011 10:47:09,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
Última fecha/hora de acceso 15/09/2011 10:47:09,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
Fecha/hora creada 15/09/2011 10:47:09,000 PM	Conocimiento del archivo	Documentos Documentos de texto	Nombre de archivo mail[1].txt	Tamaño (bytes) 10527
Fecha/hora creada 15/09/2011 10:48:53,000 PM	Conocimiento del archivo	Documentos Documentos de texto	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Última fecha/hora de acceso 15/09/2011 11:03:19,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Última fecha/hora modificada 15/09/2011 11:03:19,000 PM	Apertura de archivo/carpet	Documentos Documentos de texto	Nombre de archivo issa@mail.google[1].txt	Tamaño (bytes) 116
Fecha/hora creada 15/09/2011 11:35:47,007 PM	Uso del navegador	Web relacionada Cookies de Internet Explorer	Anfitrión mail.google.com/mail	Nombre gmailchat

win7.img

DETALLES

INFORMACIÓN DEL ARTEFACTO

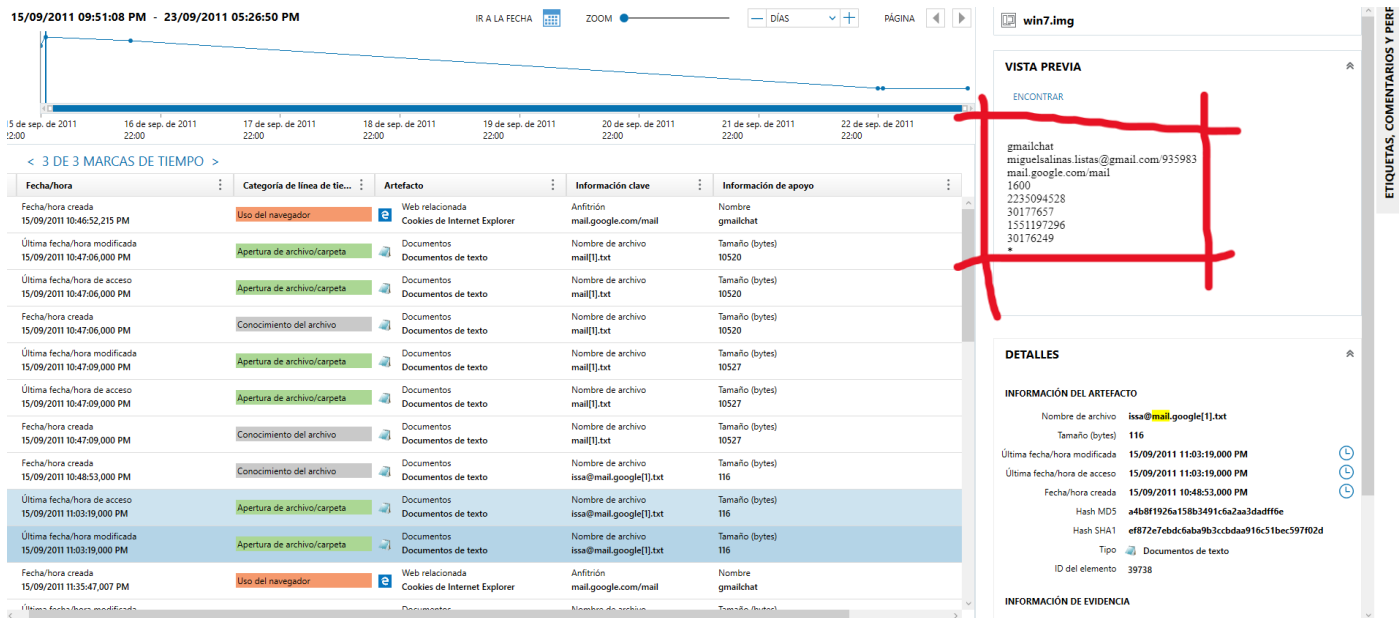
Anfitrión mail.google.com/mail  
Nombre gmailchat  
Valor miguelsalinas.listar@gmail.com/935983  
Fecha/hora creada 15/09/2011 10:46:52,215 PM  
Fecha/hora de caducidad 22/09/2011 10:46:52,000 PM  
Etiquetas 1600  
Tipo Cookies de Internet Explorer  
ID del elemento 39739

INFORMACIÓN DE EVIDENCIA

Fuente win7.img - Partition 1 (Microsoft NTFS, 20 GB)\Users\Visa\AppData\Roaming\Microsoft\Windows\Cookies\Low\issa@mail.google[1].txt  
Método de recuperación Analizado  
Fuente borrada  
Ubicación File Offset 0  
Número de evidencia win7.img

Zona horaria UTC+000





Pasando así al último día revisado el 16 de sep de 2011 obteniendo la contraseña para abrir el vdi en la máquina virtual.

#### RESULTADOS DE COINCIDENCIA (2.847 de 52.961)

Vista de la columna

\$R7L60UW.txt

Artefacto	Información clave	Información de apoyo	Información
Cookies talladas de recomendación...			
Web relacionada		Fuente de cookies (direct)	Última fecha/h 15/09/2011 10:
Cookies talladas de recomendación...		Fuente de cookies (direct)	Última fecha/h 15/09/2011 11:
Web relacionada		Fuente de cookies (direct)	Última fecha/h 15/09/2011 11:
Cookies talladas de recomendación...		Fuente de cookies (direct)	Última fecha/h 16/09/2011 04:
Web relacionada	Palabra clave firefox-3	Fuente de cookies google	Última fecha/h 13/09/2011 08:
Cookies talladas de recomendación...	Palabra clave firefox-3	Fuente de cookies bing	Última fecha/h 13/09/2011 08:
Web relacionada		Fuente de cookies programatium.com	Última fecha/h 13/09/2011 08:
Cookies talladas de recomendación...	Nombre de archivo \$17L60UW.txt	Tamaño (bytes) 544	Fecha/hora cre 16/09/2011 04:
Documentos	Nombre de archivo \$R7L60UW.txt	Tamaño (bytes) 11	Fecha/hora cre 16/09/2011 04:
Documentos de texto	Nombre de archivo README.txt	Tamaño (bytes) 181	Fecha/hora cre 13/09/2011 08:
Documentos	Nombre de archivo TPGuestVer.txt	Tamaño (bytes) 1896	Fecha/hora cre 26/03/2011 12:
Documentos de texto	Nombre de archivo SCHEDLGU.TXT	Tamaño (bytes) 4398	Fecha/hora cre 14/07/2009 04:
Documentos	Nombre de archivo FXSAPIDebugLogFile.txt	Tamaño (bytes) 0	Fecha/hora cre 13/09/2011 08:
Documentos de texto	Nombre de archivo FXSTIFFDebugLogFile.txt	Tamaño (bytes) 0	Fecha/hora cre 13/09/2011 08:
Documentos	Nombre de archivo LICENSE.txt	Tamaño (bytes) 41	Fecha/hora cre 13/09/2011 08:
Documentos de texto	Nombre de archivo	Tamaño (bytes)	Fecha/hora cre

win7.img

VISTA PREVIA

ENCONTRAR

r3t0r3ms3

DETALLES

INFORMACIÓN DEL ARTEFACTO

Nombre de archivo \$R7L60UW.txt  
Tamaño (bytes) 11  
Última fecha/hora modificada 16/09/2011 04:39:23.000 PM  
Última fecha/hora de acceso 16/09/2011 04:39:11.000 PM  
Fecha/hora creada 16/09/2011 04:39:11.000 PM  
Hash MD5 e45da219777068b3eeaa8d5a33e15049  
Hash SHA1 06d37b9aee34cd7ef1002c00d06ca10369a26d  
Tipo Documentos de texto  
ID del elemento 9821

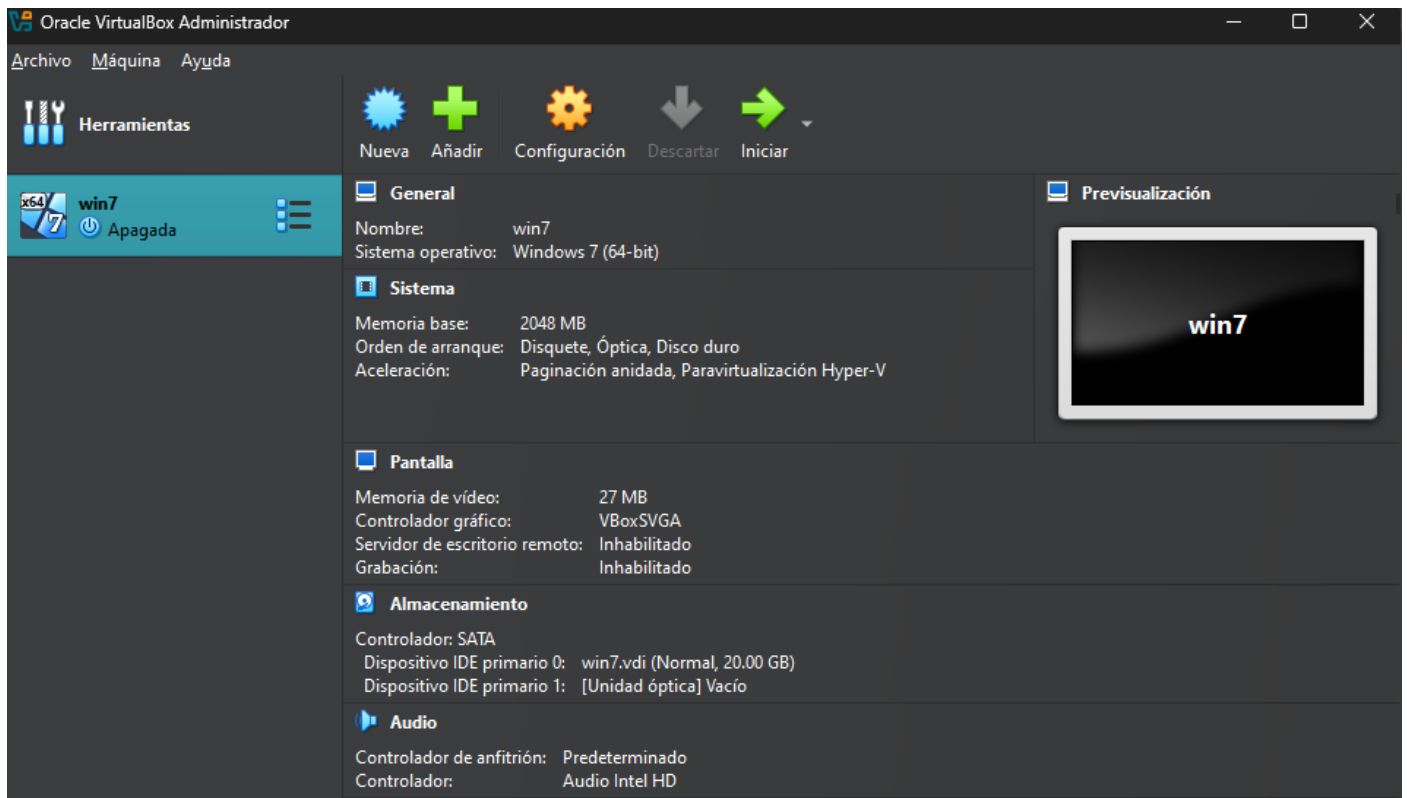
INFORMACIÓN DE EVIDENCIA

Zona horaria UTC+000

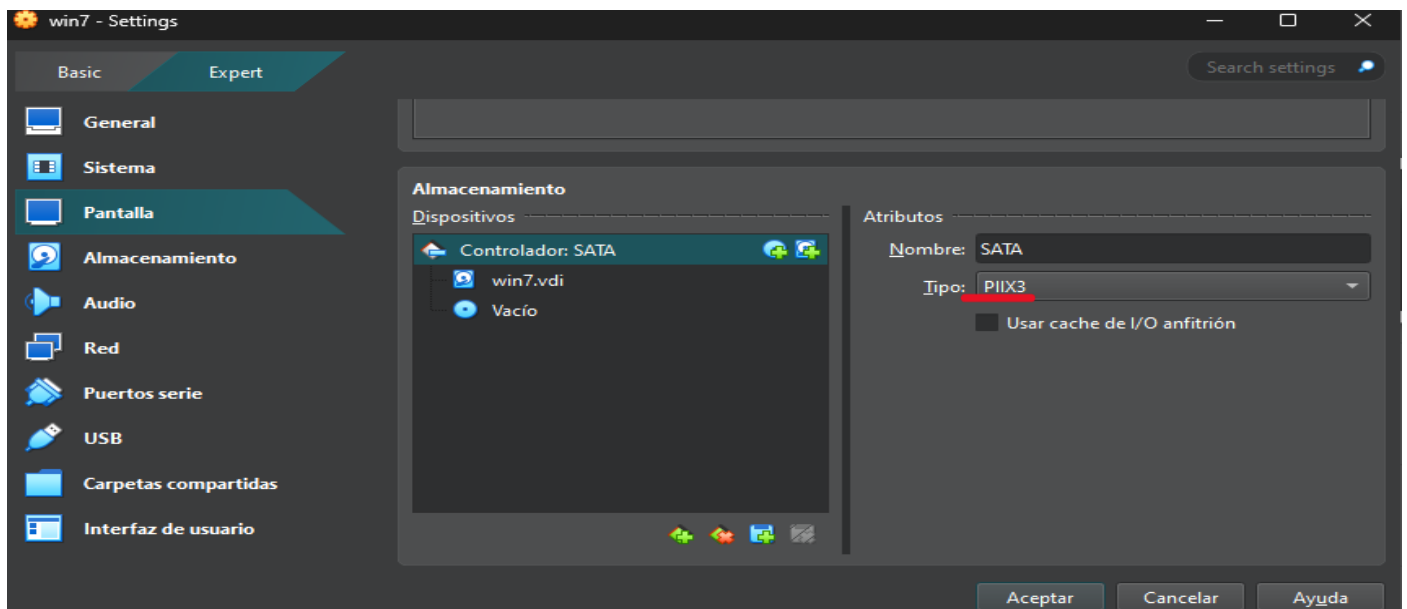
Encontrando un programa llamado forensincs que viene desde la ruta del winlogon ejecutable.



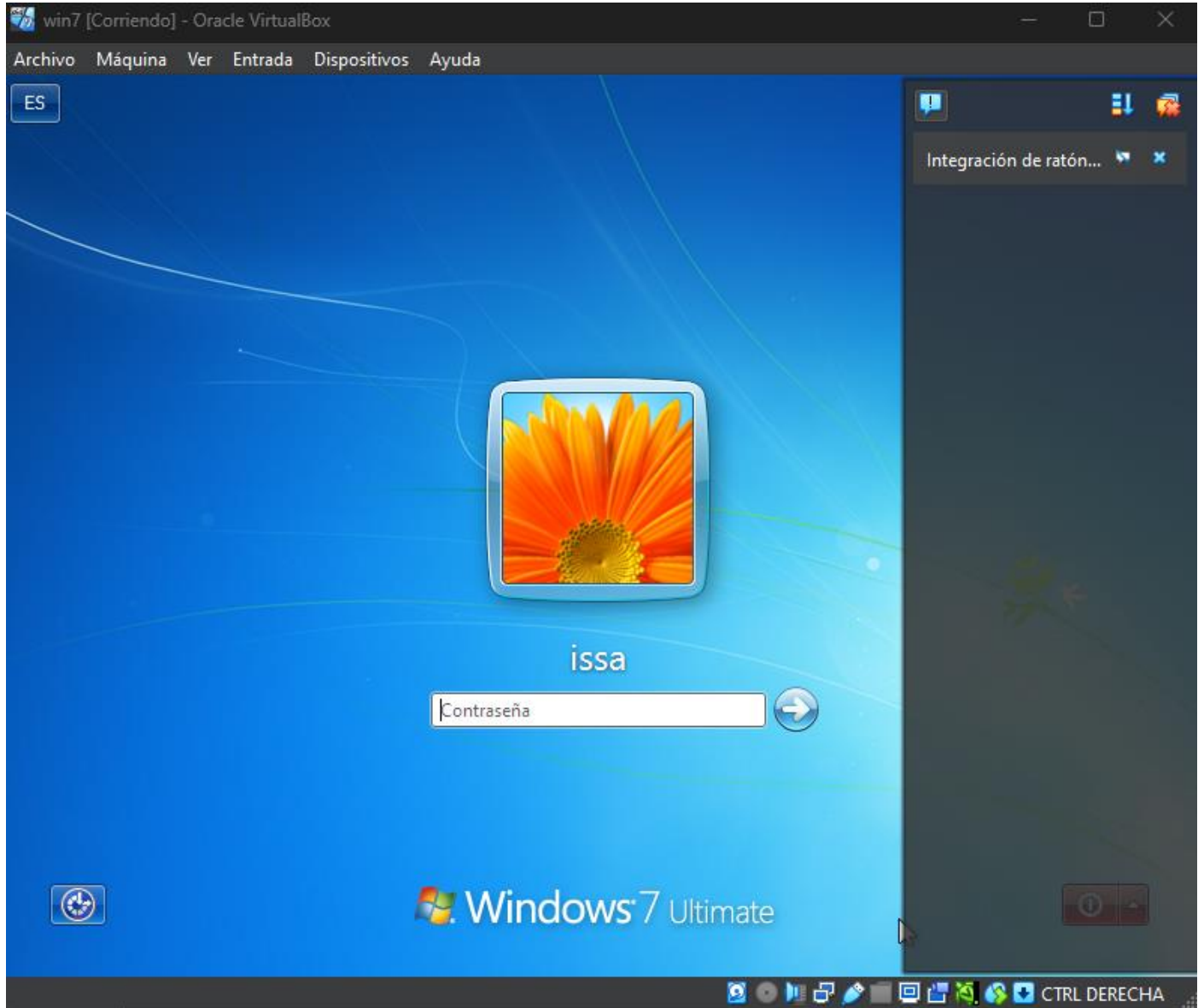
Despues, ejecutamos la VM:



Nota: si intentamos correrla sin más, nos dará un problema, ya que es un reconvertido de img a vdi, pero solo necesitamos entrar a configuración, pantalla, y cambiar el tipo a “PIIX3” y será la solución:

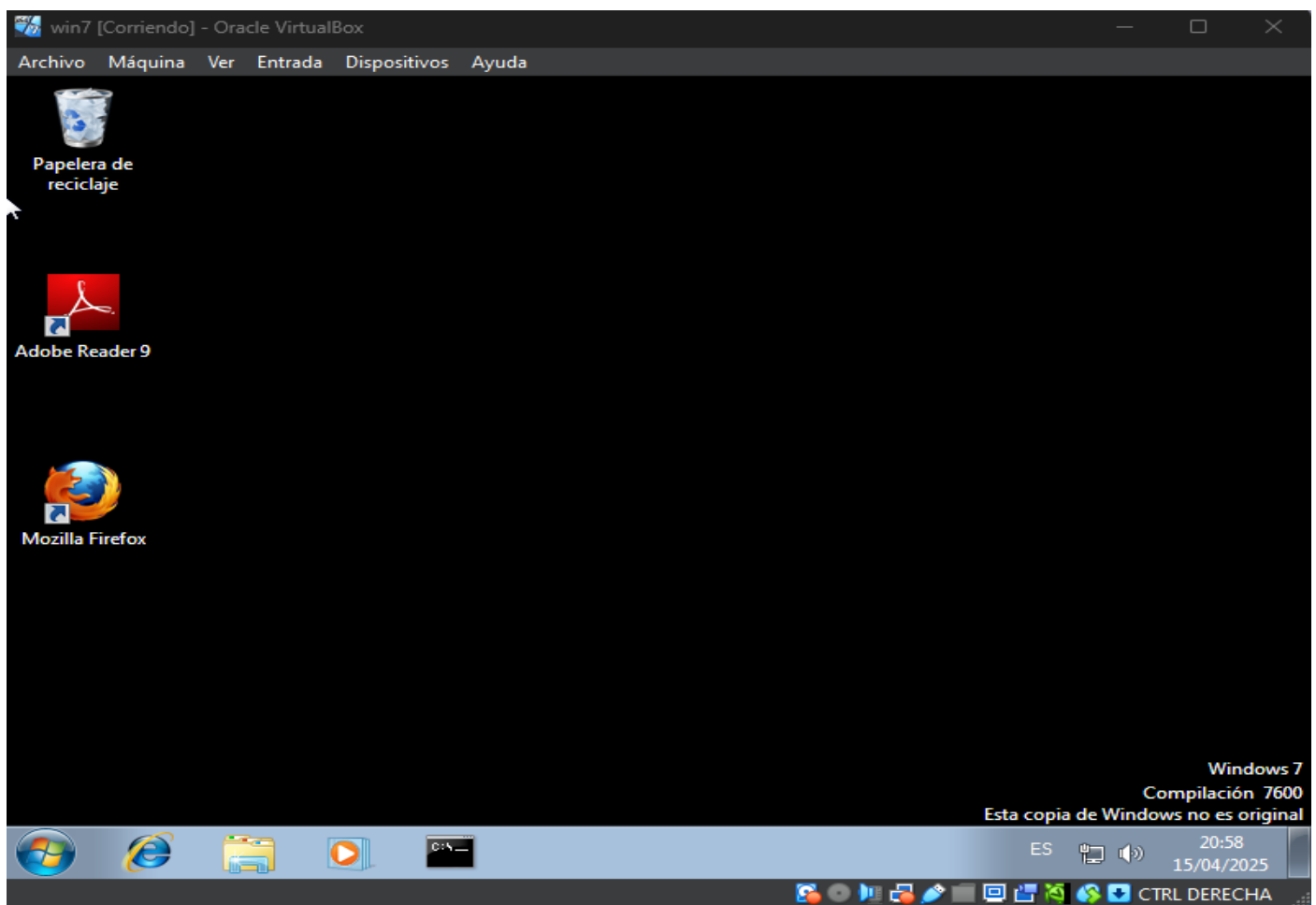
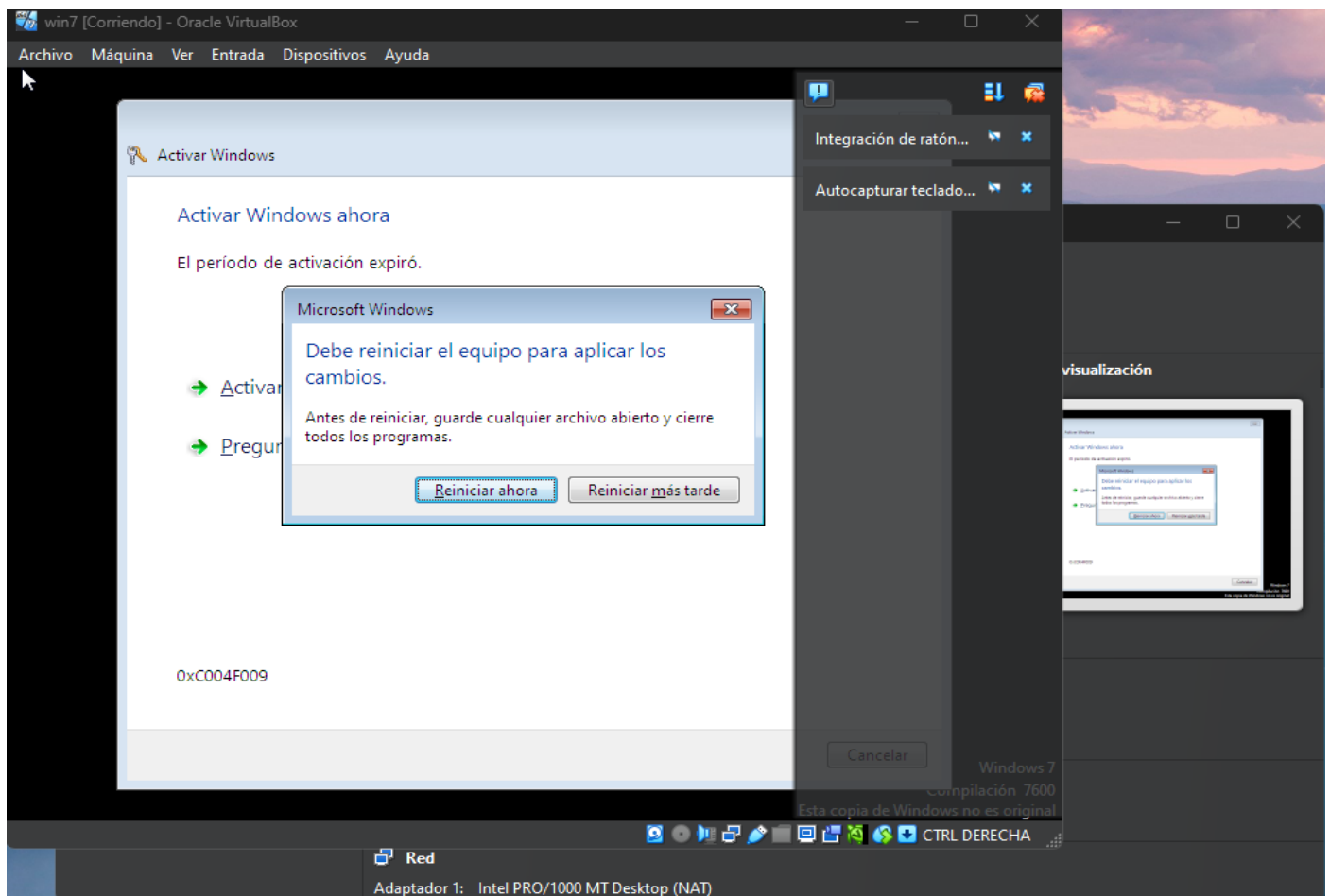


Corremos con normalidad la maquina:



E iniciamos sesión con la contraseña obtenida:

“r3t0f0r3ns3”



Ejecutamos algunos de los comandos recomendados en clase: netstats y arp.

```
win7 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
C:\> Símbolo del sistema

Conexiones activas

Proto Dirección local Dirección remota Estado PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 640
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 364
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 692
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 848
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 456
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING 464
TCP 10.0.2.15:139 0.0.0.0:0 LISTENING 4
TCP [::]:135 [::]:0 LISTENING 640
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:49152 [::]:0 LISTENING 364
TCP [::]:49153 [::]:0 LISTENING 692
TCP [::]:49154 [::]:0 LISTENING 848
TCP [::]:49155 [::]:0 LISTENING 456
TCP [::]:49156 [::]:0 LISTENING 464
UDP 0.0.0.0:5355 *:* 1120
UDP 10.0.2.15:137 *:* 4
UDP 10.0.2.15:138 *:* 4
UDP 10.0.2.15:1900 *:* 800
UDP 127.0.0.1:1900 *:* 800
UDP 127.0.0.1:65404 *:* 800
UDP [::]:5355 *:* 1120
UDP [::]:1900 *:* 800
UDP [::]:65403 *:* 800
UDP [fe80::8002:5de3:d5ac:17f2%14]:1900 *:* 800

C:\Users\issa>arp -a

Interfaz: 10.0.2.15 --- 0xe
Dirección de Internet Dirección física Tipo
10.0.2.2 52-55-0a-00-02-02 dinámico
10.0.2.3 52-55-0a-00-02-03 dinámico
10.0.2.255 ff-ff-ff-ff-ff-ff estático
224.0.0.22 01-00-5e-00-00-16 estático
224.0.0.252 01-00-5e-00-00-fc estático
255.255.255.255 ff-ff-ff-ff-ff-ff estático

C:\Users\issa>
```

Windows 7

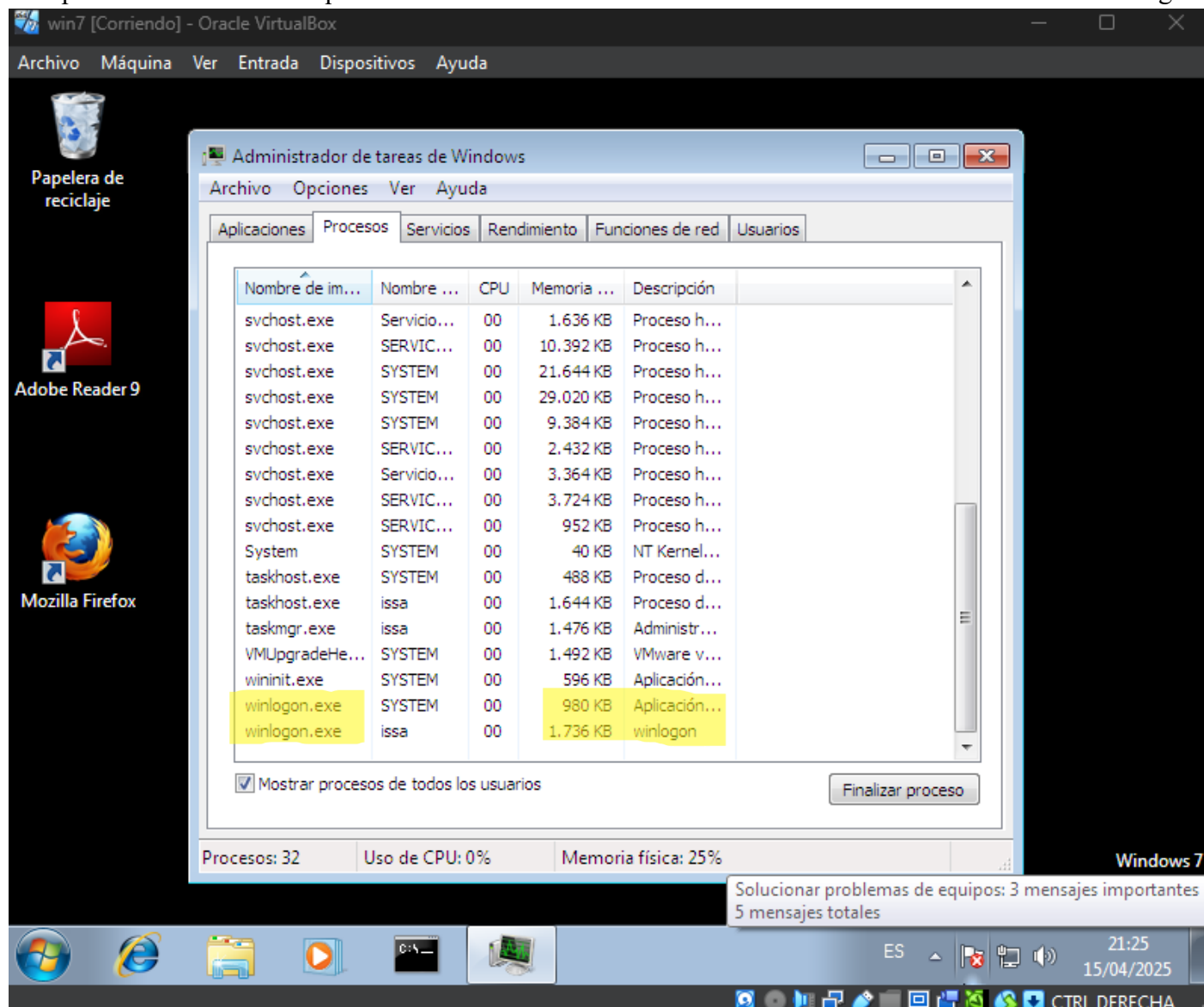
Compilación 7600

Esta copia de Windows no es original

FS 3:10

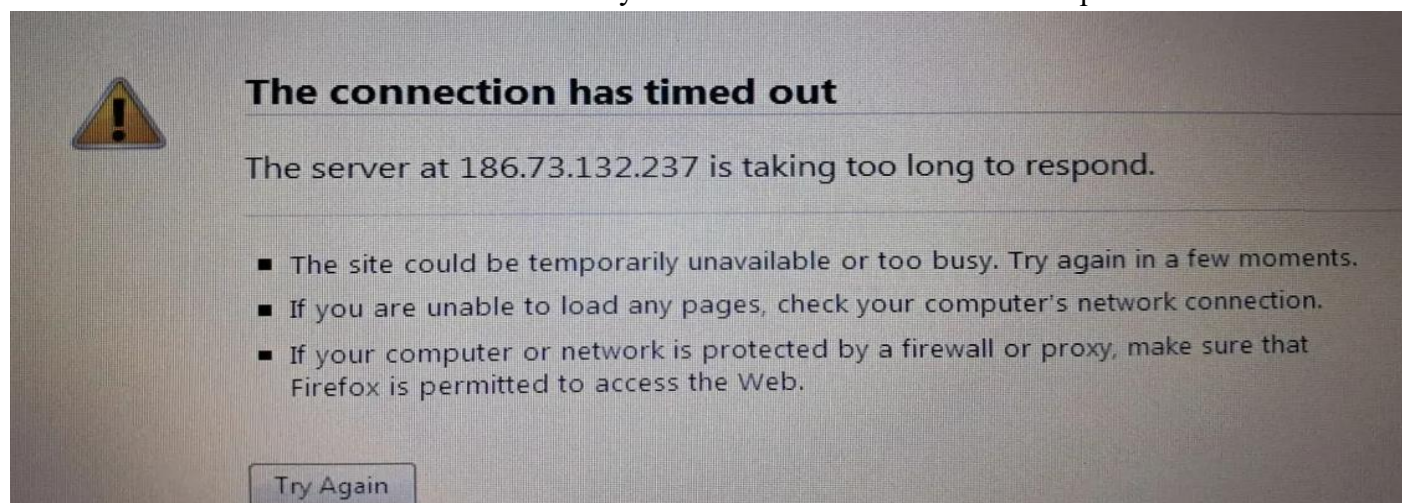


Comprobamos que existen los dos winlogon:



Intentamos otros comandos para verificar la conexión con el atacante, pues los puertos de arp y netstats no coinciden con el puerto del malware.

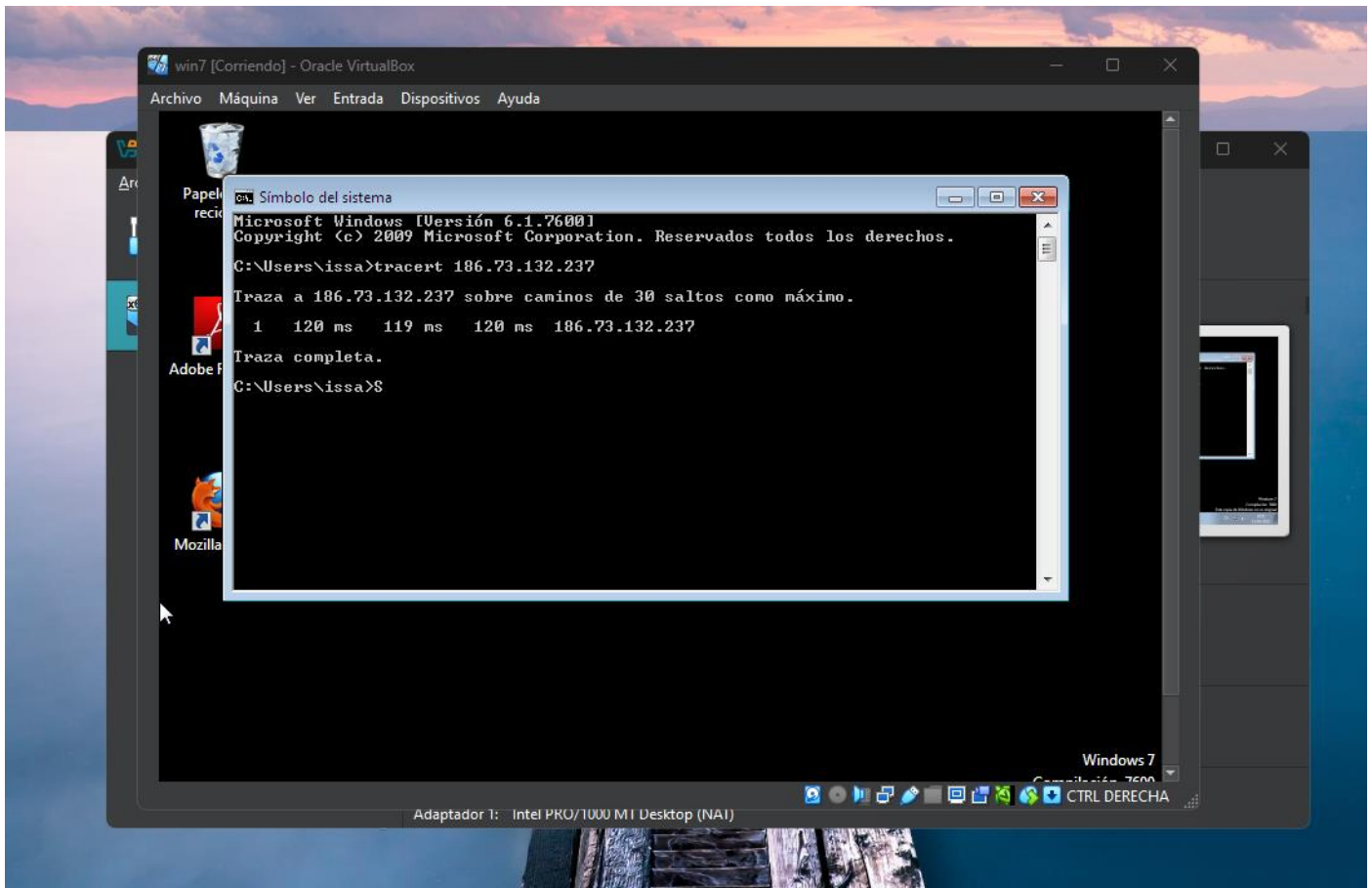
Revisamos Firefox y nos topamos con:



## PRUEBAS DE CONEXIÓN REMOTA

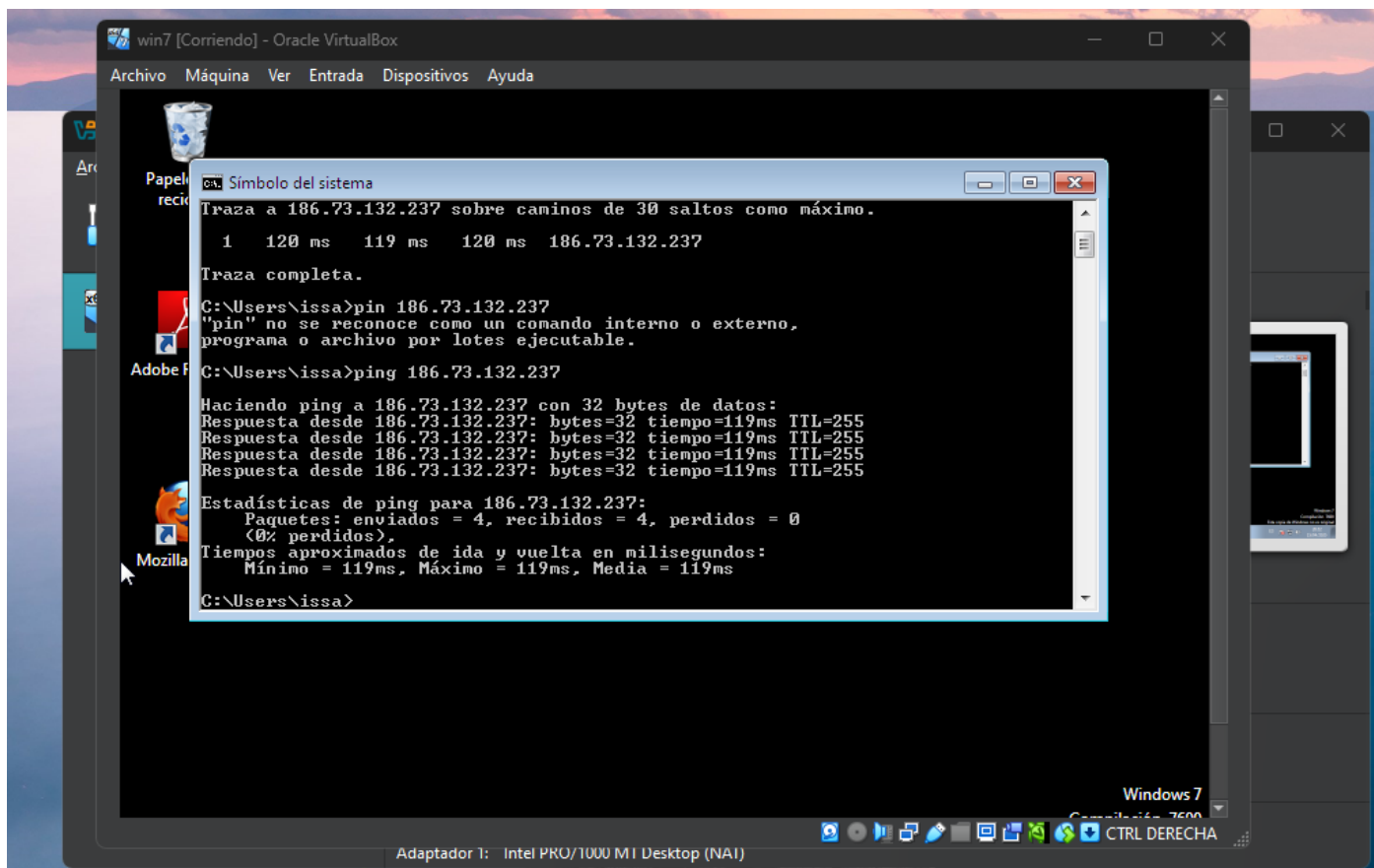
Objetivo: Demostrar si hubo acceso remoto al sistema.

Como podemos ver en la máquina virtual y su navegador, existen los dos winlogon y si existe una conexión a otro servidor, a otro host, entonces podemos intentar nuevas maneras de ver si hay conexión con este, probando a trazo directo a dicho server y ver si hay caminos hacia el, con el comando tracert y seguido del dominio.



Y, por último, realizaremos un ping con dicho server, para ver si no se pierden los paquetes.





Como podemos observar, los paquetes son enviados y recibidos, obteniendo respuesta, por lo que podemos comprobar las conexiones remotas.

## ***EVIDENCIAS PARA SUSTENTAR***

- ✓ Winlogon corrupto y doble winlogon en la máquina virtual.
- ✓ Capturas de Axiom Examine mostrando archivos maliciosos.
- ✓ PDF malicioso:
- ✓ Reporte de Examine.
- ✓ Registro de logs.
- ✓ Captura de la Virtual corriendo la VDI.
- ✓ Conexiones remotas.

Conclusiones:

En conclusión, sostengo lo que dije en mi hipótesis creyendo que la víctima fue engañada con una posible oportunidad de empleo, dando ejecución a un software con malware dañando su sistema y llevando consigo todo lo demás.