Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

Análisis KaperskyPackets.CAP

Héctor Ramírez López

Índice

1. Introducción

1.1. Identificación del perito

- **Nombre:** Héctor Ramírez López.
- **Fecha del análisis:** 12 de diciembre de 2024.
- **Cargo:** Analista Forense.

1.2. Objeto del análisis

El objetivo de este informe es realizar un análisis forense de red sobre el fichero de captura que no han dado. Se busca identificar los equipos involucrados, reconstruir las sesiones de comunicación, extraer credenciales comprometidas y determinar si hay transferencia de ficheros sospechosos o exfiltración de información.

1.3. Descripción del material recibido

Se ha recibido un fichero de captura de tráfico de red con las siguientes características:

- **Nombre del fichero:** KasperskyPackets.CAP
- **Formato:** Libpcap (Wireshark/tcpdump)
- **Origen:** Captura de tráfico proporcionada para realizar el análisis forense.

2. Metodología

2.1. Herramientas utilizadas

Para el análisis se han usado las siguientes herramientas:

- **Wireshark:** Versión 4.6.2 (Analizador de protocolos de red).
- **Hash Calculation:** PowerShell (para verificar integridad).
- **Hash del fichero (SHA256):**

```
PS C:\Users\rami> Get-FileHash "KasperskyPackets (1).CAP"

Algorithm       Hash
---------       ----
SHA256          2C6E4300A154AAD7B132B55298D265A859D008829A73ADFFE97E1C13789C81C4
```

.

2.2. Procedimiento de trabajo

Se ha seguido una metodología que garantiza la integridad de la evidencia:

1. **Preservación:** Se ha trabajado sobre una *copia* del archivo original, manteniendo el original intacto.
2. **Aislamiento:** El análisis se realizó en un entorno aislado sin salida a internet para evitar interacciones no deseadas.
3. **Identificación:** Uso de estadísticas de jerarquía de protocolos para entender el tráfico.
4. **Extracción:** Filtrado de flujos TCP para reconstruir sesiones.

3. Análisis técnico

3.1. Datos generales de la captura

- **Tiempo de captura:**
  Último paquete: 2005-07-07 20:33:49
- **Duración total:**
  Transcurrido: 00:01:20
- **Protocolos principales:** TCP, HTTP, FTP, DNS.

3.2. Identificación de equipos y roles

Tras analizar las conversaciones (Estadísticas -> *Conversaciones* -> *IPv4*), se han identificado las siguientes direcciones:

- **Cliente:** 81.131.131.6.

Dirección A	Dirección B
81.131.131.6	64.246.6.133
81.131.131.6	80.239.144.76
81.131.131.6	83.140.65.130

- **Servidores:** 64.246.6.133, 80.239.144.76, 83.140

Dirección A	Dirección B
81.131.131.6	64.246.6.133
81.131.131.6	80.239.144.76
81.131.131.6	83.140.65.130

- **Dirección MAC del Cliente:** 00:00:01:00:00:00

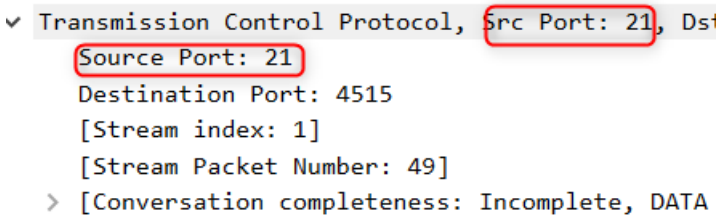
Dirección A	Dirección B
00:00:01:00:00:00	e8:72:20:00:01:00

3.3. Descripción de las sesiones FTP, HTTP u otras

Se han observado sesiones de texto claro sin cifrar.

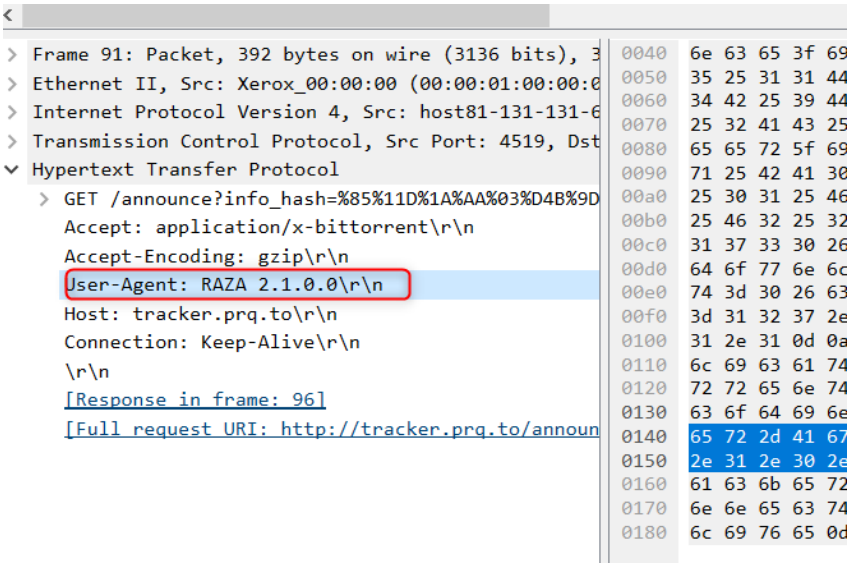
3.3.1. Análisis FTP (File Transfer Protocol)

- **Filtro utilizado:** ftp || ftp-data
- **Observación:** Se detectó una conexión al puerto 21.



3.3.2. Análisis HTTP

- **Filtro utilizado:** http
- **Observación:** Se observan peticiones GET hacia un servidor web.
  - **User-Agent detectado:** [Clic en paquete HTTP -> Hypertext Transfer Protocol -> User-Agent] (Esto identifica el navegador o herramienta usada por el atacante/usuario).



3.4. Credenciales

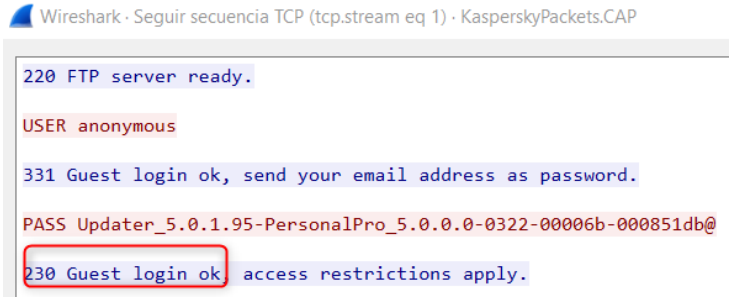
Al analizar el tráfico en texto claro, se extrajeron las siguientes credenciales de autenticación:

- **Protocolo:** FTP
- **Usuario (USER):** anonymous

```
220 FTP server ready.

USER anonymous
```

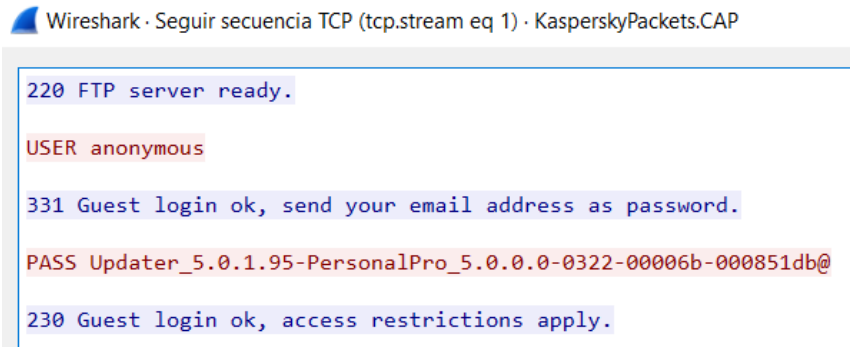
- **Estado del login:** se realizó la conexión



3.5. Comandos y respuestas

Durante la sesión FTP, se ejecutaron los siguientes comandos críticos:

- USER: Autenticación.



- RETR o STOR: (RETR es descargar, STOR es subir).
  - *Ejemplo:* Se observa el comando RETR /updates50/index/master.xml
  - indicando una descarga.

```
RETR /updates50/index/master.xml
```

3.6. Ficheros listados/transferidos

Se identificó la transferencia de los siguientes ficheros:

Nombre del fichero	Tamaño	Tipo de contenido (Estimado)
master.xml	1643 bytes	Texto / XML (Configuración)
avp.klb	~10 kB	Datos Binarios (Base de virus)
avp.set	1446 bytes	Datos Binarios / Config
avp_ext.set	1520 bytes	Datos Binarios / Config
avp_x.set	1546 bytes	Datos Binarios / Config
black.lst	~34 kB	Lista Negra (Texto o Binario)
ca.avc	~63 kB	Base de datos AV (Kaspersky)
daily.avc	~44 kB	Actualización diaria AV
daily-ex.avc	4130 bytes	Actualización diaria AV

3.7. Cronología detallada

- **[00:00:14]**: Inicio de la conexión TCP .
- **[00:00:15]**: Envío de credenciales FTP en claro.
- **[00:00:18]**: Solicitud de descarga/subida de fichero .
- **[00:00:18]**: Fin de la transferencia de datos .
- **[00:00:80]**: Cierre de la conexión.

3.8. Exportación y análisis básico de ficheros

Se procedió a la extracción del fichero transferido (*File -> Export Objects -> FTP-DATA*).

Nombre del fichero	Tamaño	Tipo de archivo	Hash MD5
avp.klb	~10 kB	Base de datos virus	3F2FC1C0D32557C6AD29A53DBDA6E9C5
avp.set	1446 Bytes	Configuración AV	ECAAEC7514890377864ADD5E72515B7D
avp_ext.set	1520 Bytes	Configuración extendida AV	A19922664F7A3D6D49F0DD739EE38C32
avp_x.set	1546 Bytes	Configuración extendida AV	2472A7A4A7B0B974172D110F01F51E4B
black.lst	~34 kB	Lista Negra	D506151FB707E0914D3C76E8526725B2
ca.avc	~63 kB	Base de firmas AV	18EE6BE984C627AD4943FE292761D91D
daily-ex.avc	4130 Bytes	Actualización diaria AV	47C7B00D89DF0144643C2BCCB29BF0E0
daily.avc	~44 kB	Actualización diaria AV	BF459F63DA7EC0B3E792150D9A7F6025

4. Hallazgos

4.1. Existencia de credenciales en claro

Se confirma que las credenciales de acceso al servidor FTP viajaron sin cifrar. Cualquier actor en la misma red (Man-in-the-Middle) podría haberlas interceptado, como se ha demostrado en este análisis.

4.2. Posible exfiltración / subida de ficheros

- "El análisis del tráfico FTP muestra múltiples comandos RETR, lo que indica que el host interno inició la **descarga** de ficheros desde el servidor externo (80.239.144.76).
- Los ficheros transferidos (daily.avc, avp.klb, etc.) corresponden a firmas y bases de datos de actualización del antivirus Kaspersky. No se identificó exfiltración de información o subida de datos sensibles ni la descarga de ejecutables (.exe) convencionales, sino de binarios de actualización."

4.3. Evidencias de comportamiento anómalo

Se han detectado las siguientes anomalías en el comportamiento de red analizado:

Uso de protocolo no seguro (FTP) para infraestructura crítica:

- Se identificó que la actualización de las bases de firmas del antivirus (Kaspersky) se realizó mediante FTP (Puerto 21).

- Este protocolo transmite toda la información en texto plano, sin cifrado. Esto permitió visualizar en pasos anteriores tanto las credenciales de acceso como el contenido de los ficheros transferidos.

5. Conclusiones

5.1. Evaluación del impacto potencial

Se clasifica con riesgo **ALTO** debido a la combinación de factores de confidencialidad e integridad:

1. **Exposición de Credenciales (Confidencialidad):** Al utilizar el protocolo FTP estándar, las credenciales de autenticación (usuario y contraseña) viajaron en texto claro. Esto permite que cualquier actor malicioso en la red capture estas credenciales y obtenga acceso no autorizado al servidor o servicio.

2. **Falta de Integridad en el Canal (Integridad):** La ausencia de cifrado (como TLS/SSL) implica que no existe garantía de que los ficheros recibidos sean auténticos. Un atacante en posición de *Man-in-the-Middle* podría haber interceptado la descarga de las bases de datos antivirus (.avc, .klb) y haberlas sustituido por ficheros corruptos o malware, comprometiendo la seguridad del host que intentaba protegerse.

5.2. Probables acciones del usuario/atacante

Basado en la traza, el usuario intentó conectarse a un servidor para gestionar ficheros posiblemente relacionados con Kaspersky. La falta de cifrado expuso toda la sesión. Se recomienda cambiar las credenciales inmediatamente y validar la integridad de cualquier fichero descargado en esa sesión mediante hashes oficiales del fabricante.

Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.12.28 18:35:58 +01'00'