

Red Stealer Lab

Escenario:

Formas parte del equipo de Inteligencia de Amenazas del SOC (Centro de Operaciones de Seguridad). Se ha descubierto un archivo ejecutable en el ordenador de un compañero y se sospecha que está vinculado a un servidor de Comando y Control (C2), lo que indica una posible infección de malware. Tu tarea es investigar este ejecutable analizando su hash. El objetivo es recopilar y analizar datos útiles para otros miembros del SOC, incluido el equipo de Respuesta a Incidentes, para responder eficazmente a este comportamiento sospechoso.

Para este escenario solo se nos proporciona un HASH en formato SHA-256 el cual tenemos que analizar en las diferentes plataformas de Inteligencia de Amenazas

P1-La categorización del malware permite comprender con mayor rapidez y claridad sus comportamientos únicos y vectores de ataque. ¿Qué categoría ha identificado Microsoft para ese malware en VirusTotal?

Malwarebytes	MachineLearning/Anomalous.96%	MaxSecure	Trojan.Malware.300983.susgen
McAfee Scanner	TiI248FCC901AFF	Microsoft	Trojan:Win32/Redline!trf
NANO-Antivirus	Trojan.Win32.GenKryptik.kbtmcs	Palo Alto Networks	Generic.ml
Panda	Trj/Chgt.AD	QuickHeal	Trojan.Ghanarava.1742509062c95cf9
Rising	Trojan.Nikto!8.18B19 (CLOUD)	Sangfor Engine Zero	Trojan.Win32.Save.a

Como podemos ver aparecen todo los vendors que han detectado el malware, si nos vamos hasta la parte donde esta Microsoft vemos que lo ha clasificado como Trojan

P2-Identificar claramente el nombre del archivo de malware mejora la comunicación entre el equipo del SOC. ¿Cuál es el nombre del archivo asociado a este malware?

En el inicio de Virus total vemos que debajo de Hash nos dan el nombre del archivo asociado

59 / 71
Community Score -9

59/71 security vendors flagged this file as malicious

WEXTRACT.EXE .MUI

Size: 1.83 MB | Last Analysis Date: 17 days ago

peexe detect-debug-environment persistence spreader checks-disk-space executes-dropped-file checks-user-input long-sleeps

Pero también en la parte de Details lo vamos a visualizar

Names ⓘ
malicious.exe
Wextract
WEXTRACT.EXE .MUI
248fcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe
malicious.exe (2)
red.exe
18cbe55c3b28754916f1cbf4dfc95cf9.exe
NEAS.248fcc901aff4e4b4c48c91e4d78a939bf681c9a1bc24addc3551b32768f907b.exe

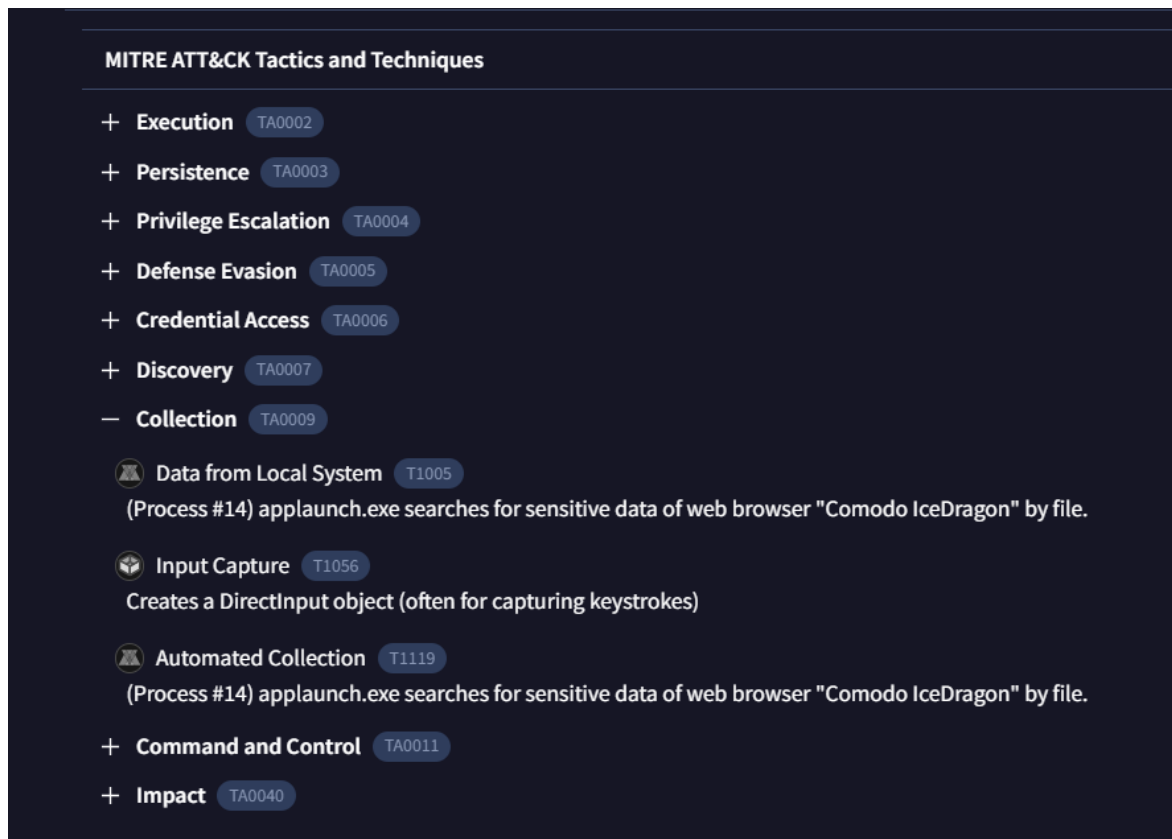
P3-Conocer la fecha y hora exactas de la primera detección del malware puede ayudar a priorizar las acciones de respuesta. El malware recién detectado puede requerir contención y erradicación urgentes, en comparación con amenazas más antiguas y bien documentadas. ¿Cuál es la fecha y hora UTC del primer envío del malware a VirusTotal?

Esta información la encontramos igualmente en la pestaña de Deatils de Virus Total en el History:

History ⓘ	
Creation Time	2022-05-24 22:49:06 UTC
First Submission	2023-10-06 04:41:50 UTC
Last Submission	2025-03-26 08:32:31 UTC
Last Analysis	2025-03-24 05:03:18 UTC

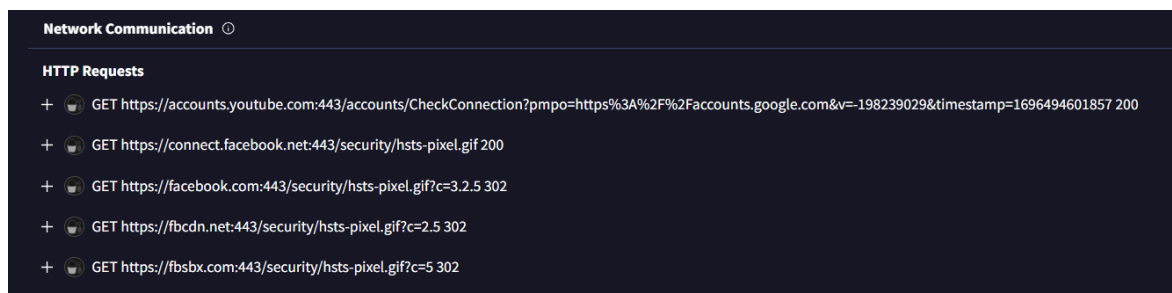
P4-Comprender las técnicas que utiliza el malware facilita la planificación estratégica de la seguridad. ¿Cuál es el ID de la técnica MITRE ATT&CK para la recopilación de datos del sistema por parte del malware antes de la exfiltración?

En la pestaña de Behavior de Virus Total se muestran todas Técnicas y tácticas utilizadas, para la recopilación de datos encontramos bajo que técnica fueron recopilados los datos



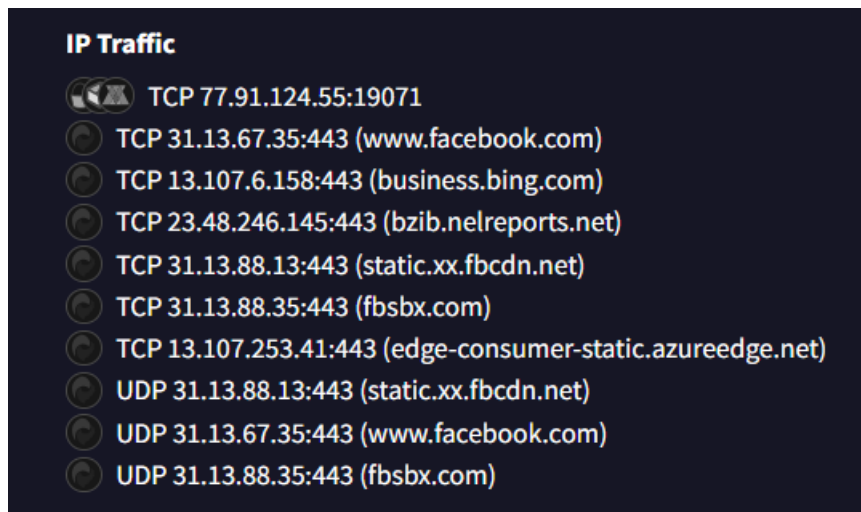
P5-Después de la ejecución, ¿qué nombres de dominio relacionados con las redes sociales resolvió el malware a través de consultas DNS?

Seguimos en Virus Total en la parte de Behavior y posterior en el apartado de Network Communication vemos que se hacen solicitudes a facebook



P6-Una vez identificadas las direcciones IP maliciosas, se pueden configurar dispositivos de seguridad de red, como firewalls, para bloquear el tráfico hacia y desde estas direcciones. ¿Puede proporcionar la dirección IP y el puerto de destino con el que se comunica el malware?

Más adelante en la pagina de virus total también tenemos la sección de IP traffic



Aquí podemos ver la comunicación TCP y el puerto asociado a la misma

P7- Las reglas de YARA están diseñadas para identificar patrones y comportamientos específicos de malware. Utilizando MalwareBazaar, ¿cómo se llama la regla de YARA creada por "Varp0s" que detecta el malware identificado?

Nos cambiamos a Malware Bazaar donde vamos a la sección de Yara y encontramos el nombre que le a dado el grupo asociado:

YARA Signatures





MalwareBazaar uses YARA rules from several public and non-public repositories, such as [Malpedia](#). Those are being matched against malware samples uploaded to MalwareBazaar as well as against any suspicious process dumps they may create. Please note that only results from **TLP:WHITE** rules are being displayed.

Rule name:	detect_Redline_Stealer  Alert
Author:	Varp0s

*P8- Comprender qué familias de malware atacan a la organización facilita la planificación estratégica de seguridad para el futuro y la priorización de recursos según la amenaza. ¿Podría proporcionar los diferentes alias de malware asociados con la dirección IP maliciosa según **ThreatFox** ?*

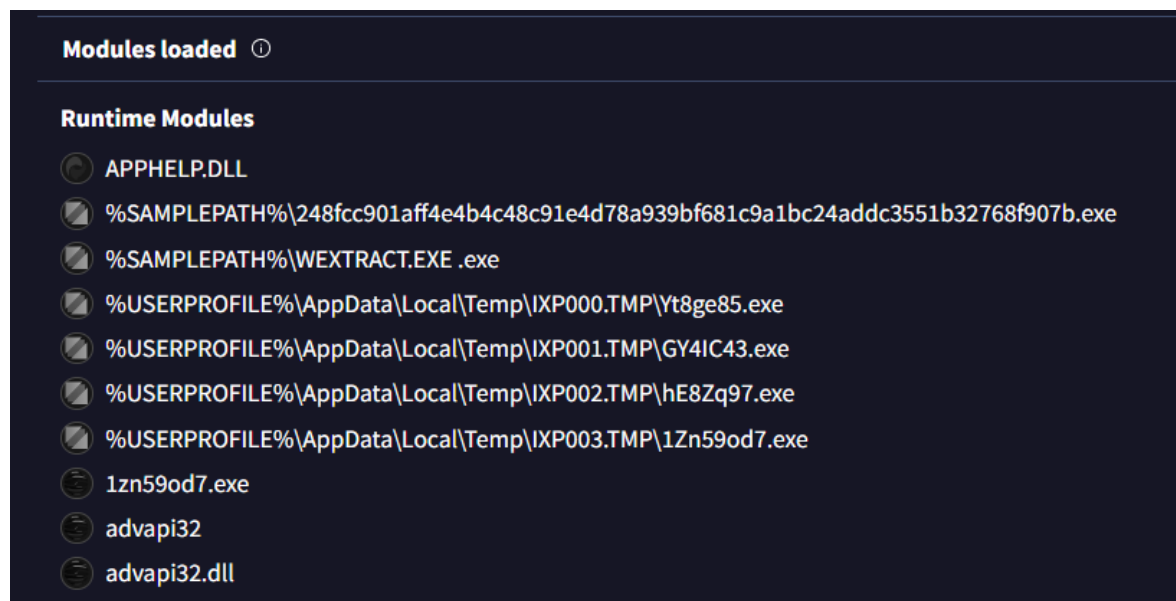
Nos vamos ahora a la pagina de ThreatFox y metemos la IP de la pregunta 6 en el buscador de IOC's donde vamos a ver los alias del Malware:

Database Entry

IOC ID:	1188205
IOC:	 77.91.124.80:46502
IOC Type @:	ip:port
Threat Type @:	botnet_cc
Malware:	 RedLine Stealer
Malware alias:	RECORDSTEALER
Confidence Level @:	 Confidence level is high (100%)
ASN:	AS203727 ALTAWK
Country:	 UA

P9-Al identificar las DLL importadas del malware, podemos configurar herramientas de seguridad para supervisar la carga o el uso inusual de estas DLL específicas. ¿Podría proporcionar la DLL que utiliza el malware para la escalada de privilegios?

Aquí volvemos a Virus Total y nos vamos casi hasta a bajo de la pestaña de Behavior en Modules loaded donde veremos todas las rutinas generadas en el sistema por el Malware.



Si te sirvió la información recuerda irme a seguir a mis redes sociales:

Youtube: <https://www.youtube.com/c/Or4kM4cCiberseguridad>

Facebook: <https://www.facebook.com/orackmac>

Instagram: <https://www.instagram.com/orackmac/>

Tiktok: <https://www.tiktok.com/@orackmac>