

Escenario de Capacitación - Robo de Identidad

Nombre del Grupo

Datos de Capacitación - Robo de Identidad (Redline)

Escenario

En este escenario de capacitación, ejecutaremos un fragmento de malware “stealer” (ladrón de información) con el fin de llevar a cabo la primera etapa de un ataque: el robo de credenciales. A diferencia del escenario de **RAT**, este no utiliza los mismos comportamientos que el ransomware. En cambio, forma parte de las crecientes capacidades de protección de identidad de Cyber Crucible.

A menudo, antes de que ocurra siquiera una extorsión, los primeros pasos que realiza un atacante son propagarse por la red y obtener acceso a la mayor cantidad posible de credenciales. En algunos casos se trata de una combinación de usuario/contraseña de AD; en otros, son claves de API extraídas de sesiones del navegador.

Identificándolo

Por ahora, profundicemos en cómo se ve un acceso anormal para el administrador.

Accessing Program Path	Untrusted Remote Threads	Modified Memory	No Trusted Cert
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True

Los accesos a datos de identidad son muy claros y directos: ¡si los administradores no reconocen un programa, este no debería estar accediendo a esos datos! Esto de inmediato resalta como algo sospechoso que está ocurriendo.

¿Cuál es el lado opuesto de esto que ve el atacante? ¡Texto plano!

RedLine | Main v20.2 | License expires 31.12.9999 23:59:59

Lock

X

Logs

Selected logs: 1

ID	HWID	IP	BuildID	LogDate	Country	SeenBefore	Checked	Comment	Creds	PDD	CDD
1	AF4F45833C13F1A0971CA6DEE3DFB21A	169.254.71.86	victim86753	10/19/2022 7:15...	US	☒	☐		4j0j0j0		

Statistic

Guest Links

Loader Tasks

Logs Sorter

Wallet Checker

Builder

Misc

Telegram

Notifications

Black Lists

Settings

Contacts

Total logs: 1

Total pages: 1

Search filter:

Search

Save all logs

<<

>>

Go to Page

Current page: 1

Enter a comment:

Set

Clear all logs

23:50:50

RedLine | Password Viewer

	Host	Login	Password	Comment
▶	https://account.proton.me/signup	4abaa73cde2f4d00a347ba48c22fdc...	[REDACTED]	
	https://www.cybercrucible.com/c...	4abaa73cde2f4d00a347ba48c22fdc...	[REDACTED]	

RedLine | Autofill Viewer

	Name	Value
▶	Username	5480d46ef2aa40b1a0a9882d704
	username	4abaa73cde2f4d00a347ba48c22fdc51@prot...

Estas respuestas no son respuestas como los eventos tradicionales de extorsión de datos, por lo que no son acciones de suspensión automatizada. En cambio, se asemejan más a inyecciones de procesos, en las que Cyber Crucible no se interpuso. A medida que nuestros análisis han ido creciendo, hemos aprendido cómo se ve el acceso “normal” a los almacenes de identidad para varios tipos de aplicaciones. Para 2023 habilitaremos nuestra función de protección, que restringirá el acceso, a nivel del kernel, a diversas formas de bases de datos de identidad, permitiendo el acceso únicamente al software asociado.

Documentación relevante

- **Inyección de Procesos**
- [Mitre T1559](#) - La comunicación entre procesos (Inter-Process communication) puede proporcionar control sobre el proceso objetivo desde el inyector una vez que se completa la inyección.
- [Mitre T1106](#) - Las API nativas suelen ser el acceso más directo a la funcionalidad del sistema operativo para acceder a archivos, procesos en ejecución y más.
- [Mitre T1569](#) - Inyectar en un servicio del sistema, como un `svchost` existente, puede disfrazar el código malicioso para que se reporte como si estuviera ejecutándose desde un proceso conocido y confiable.
- [Mitre T1055](#) - Inyección de procesos, generalmente utilizada para ejecutar código malicioso dentro de un proceso objetivo mientras se permite que el proceso original continúe.
- [Mitre T1543](#) - Crear o modificar un proceso del sistema puede disfrazar el código malicioso como un proceso del sistema normal y confiable, evitando así la detección de malware.
- [Mitre T1555](#) - Las credenciales almacenadas en gestores o navegadores sin cifrar pueden utilizarse para obtener acceso a datos privilegiados.
- [Mitre T1212](#) - Las credenciales podrían ser robadas aprovechando software vulnerable que no cifra las credenciales ingresadas por un usuario.

Revision #1

Created 2026-07-24 01:15:20 UTC by Dennis Underwood

Updated 2026-07-24 01:15:20 UTC by Dennis Underwood