

Descubriendo más credenciales con **Mimikatz**



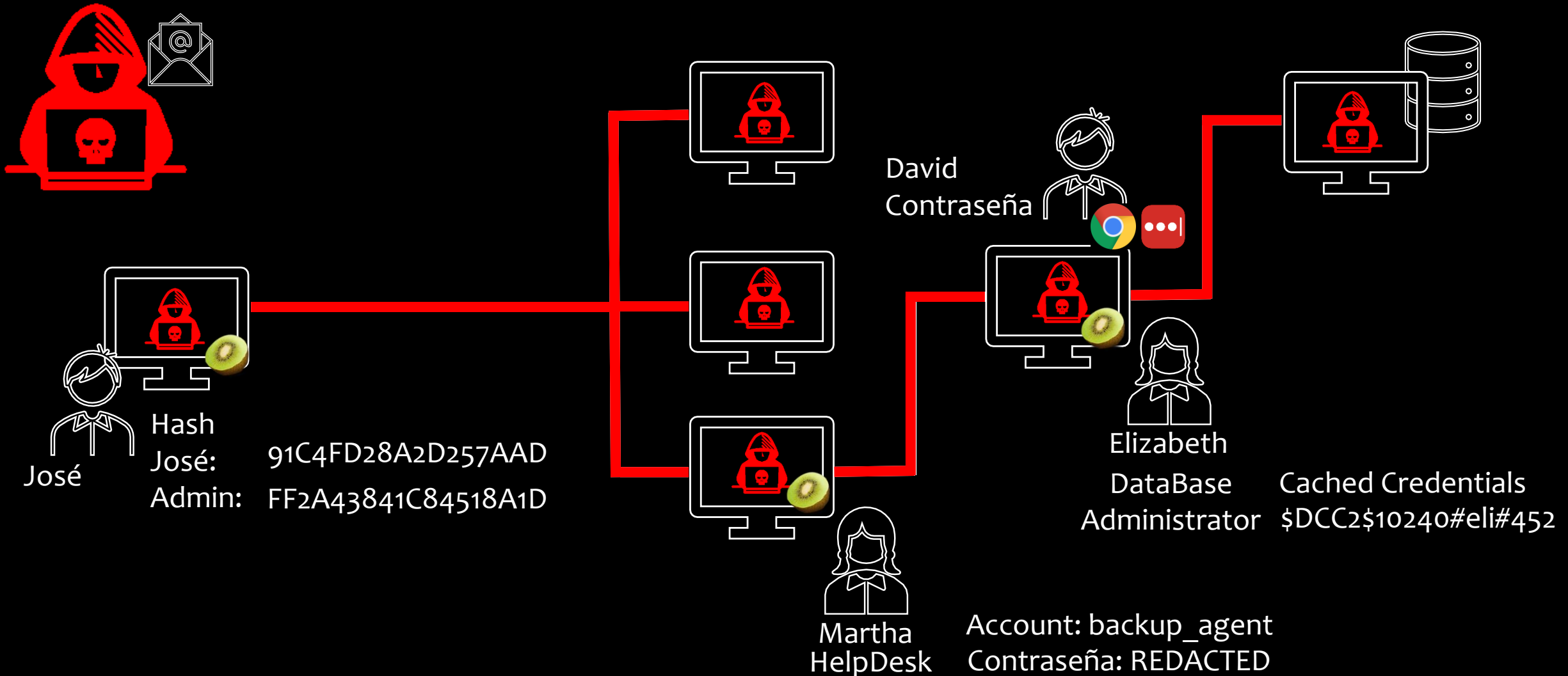
Julio Ureña (PlainText)

net user PlainText

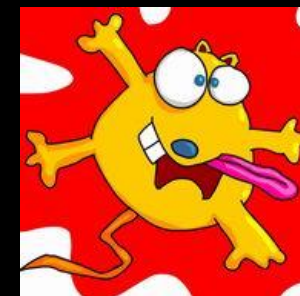
- ❑ Julio Ureña
- ❑ Cristiano / Esposo / Padre / Amigo
- ❑ Líder de la Comunidad RedTeamRD
- ❑ HackTheBox Ambassador
- ❑ Microsoft Technical Specialist Security & Compliance
- ❑ Twitter: @JulioUrena
- ❑ Blog: <https://plaintext.do>
- ❑ YouTube: <https://www.youtube.com/c/JulioUreña>




Todo empezó con una contraseña...



La Historia detrás de Mimikatz...



- ❑ Creado por Benjamin Delpy  @gentilkiwi
- ❑ Primeros nombres (2007 – 2010): Kdll, kdllpipe, katz, mimikatz
- ❑ Mimikatz es Cute Cat en Frances. Lindo gato, gato lindo o gatico.
- ❑ Empezó con la necesidad de Benjamin de entender mejor PTH y exportación de certificados, en ese momento no había una herramienta que funcionara en 64bits y decidió crear su propia herramienta y aprender C & C++ en el proceso.
- ❑ Primera presentación de Mimikatz 2011 y luego fue a Rusia en 2012 donde recibió una visita de espías Rusos ...



❑ Initial Commit



gentilkiwi committed on Apr 6, 2014



Recycle Bin



Microsoft Edge



Microsoft Teams



Policy Manager

File

Home

Share

View

Application Tools

Manage

tools

Local Disk (C:) > tools

Search tools

Name	Date modified	Type	Size
DefenderCheck	7/2/2020 10:31 PM	Application	9 KB
mimidrv.sys	7/5/2020 8:59 PM	System file	37 KB
mimikatz	7/5/2020 8:59 PM	Application	1,235 KB
mimilib.dll	7/5/2020 8:59 PM	Application extens...	46 KB
Rubeus	7/2/2020 7:41 AM	Application	223 KB

5 items 1 item selected 1.20 MB

Windows Defender Security Center

Exclusions

Add or remove items that you want to exclude from Windows Defender Antivirus scans.

+

Add an exclusion

C:\tools
Folder

Contraseñas la memoria (LSASS)

- ❑ El modulo de **sekurlsa** tiene comandos para extraer credenciales de LSASS
- ❑ **logonpasswords** – extrae todas las credenciales soportadas por los diferentes proveedores: msv, wdigest, tspkg, kerberos,ssp and credman
- ❑ **sekurlsa::msv** – NTLM, LM hashes and cleartext
- ❑ **sekurlsa::wdigest** – Wdigest hashes and cleartext
- ❑ **sekurlsa::tspkg** – Terminal service SSP cleartext
- ❑ **sekurlsa::kerberos** - Lists Kerberos credentials
- ❑ **sekurlsa::ssp** – CredSSP cleartext
- ❑ **sekurlsa::credman** – Credential Manager cached cleartext





Contraseñas de Usuarios Locales...

- ❑ El modulo de **Lsadump** nos permite interactuar con LSA (Local Security Authority) local y remotamente, listar los paquetes de Seguridad y trabajar con credenciales guardas en los registros de SAM.

❑ **Lsadump::sam**

Este comando extrae la base de datos Security Account Managers (SAM). Contiene NTLM, y a veces LM hash, de las contraseñas de los usuarios.

Puede funcionar en dos modos: en línea (con el usuario o token SYSTEM) o sin conexión (copia de seguridad SYSTEM & SAM)



tools

FileHomeShareView

This PC > Local Disk (C:) > tools

Search tools

Quick access

Desktop

Downloads

Documents

Pictures

Music

System32

Videos

OneDrive

This PC

New Volume (D:)

Network

Name	Date modified	Type	Size
mimidrv.sys	7/5/2020 8:59 PM	System file	37 KB
mimikatz	7/5/2020 8:59 PM	Application	1,235 KB
mimilib.dll	7/5/2020 8:59 PM	Application extens...	46 KB
procexp64	7/8/2020 10:15 PM	Application	1,456 KB
rdcman	7/8/2020 8:32 PM	Windows Installer ...	1,161 KB
SharpChromium	6/28/2020 4:54 PM	Application	571 KB

6 items

Windows Defender Security Center

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable.

Off

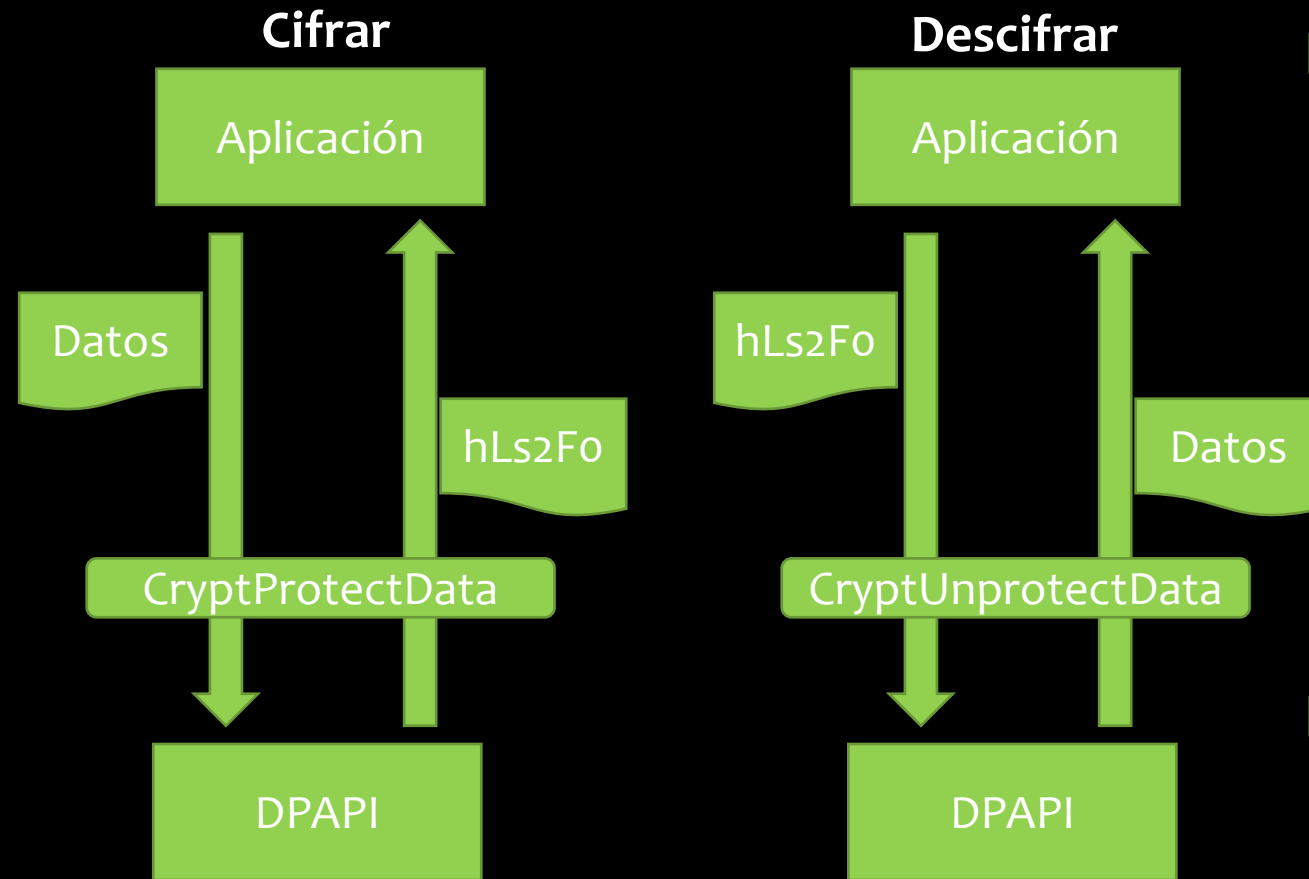
[Privacy statement](#)

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable.

Data Protection API (DPAPI)



- ❑ La API de protección de datos (DPAPI) es un componente integrado en Windows que proporciona un medio para cifrar y descifrar "blobs" de datos. Utiliza claves criptográficas que están vinculadas a un usuario o computadora específicos y permite que tanto la funcionalidad nativa de Windows como las aplicaciones de terceros protejan / desprotejan los datos de manera transparente para el usuario.
- ❑ Dos implementaciones comunes de DPAPI incluyen el Administrador de credenciales de Windows y Google Chrome.

Application Tools tools				
File Home Share View Manage				
Local Disk (C:) > tools				
Search tools				
Quick access	Name	Date modified	Type	Size
Desktop	DefenderCheck	7/2/2020 10:31 PM	Application	9 KB
Downloads	mimidrv.sys	7/5/2020 8:59 PM	System file	37 KB
Documents	mimikatz - Copy	7/5/2020 8:59 PM	Application	1,235 KB
Pictures	mimikatz	7/5/2020 8:59 PM	Application	1,235 KB
Music	mimilib.dll	7/5/2020 8:59 PM	Application extens...	46 KB
Videos	rdcman	7/8/2020 8:32 PM	Windows Installer ...	1,161 KB
OneDrive	Rubeus	7/2/2020 7:41 AM	Application	223 KB
This PC	SharpChromium	6/28/2020 4:54 PM	Application	571 KB
Local Disk (C:)				
New Volume (D:)				
Network				
8 items 1 item selected 1.20 MB				

Windows Defender Security Center

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable.

Off

[Privacy statement](#)

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable.

Credenciales en Cache & Control de lsass

- ❑ **lsadump::cache** por default Windows 10 guarda hasta 10 credenciales
 - ❑ `hashcat -m2100 hash.txt wordlist.txt (MsCacheV2)`
- ❑ **misc::memssp** nos permite manipular el funcionamiento de LSASS e inyectar una porción de código que provocará que cada vez que un usuario haga inicio de sesión en el equipo, sus credenciales sean guardadas en texto plano.
- ❑ Las credenciales son guardadas en **C:\Windows\System32\mimilsa.log**
- ❑ Una vez el equipo es reiniciado, SSP no estará presente.



Google Chrome & Edge Chromium

- ❑ **SharpChromium** es un proyecto creado por **Dwight Hohnstein** en .NET 4.0+ CLR para recuperar datos de Google Chrome, Microsoft Edge y Microsoft Edge Beta. Actualmente, puede extraer:
 - ❑ Cookies (en formato JSON)
 - ❑ Historial (con cookies asociadas para cada elemento del historial)
 - ❑ Inicios de sesión guardados

Nota: Todas las cookies devueltas están en formato JSON. Si tiene instalada la extensión Cookie Editor, simplemente puede copiar y pegar en la sección "Importar" de este complemento del navegador para recorrer la sesión extraída.

- ❑ <https://github.com/djhohnstein/SharpChromium>



¿Qué más puedo hacer con Mimikatz?



- ❑ Manipulación de Procesos & Tokens
- ❑ Remover Protección de Procesos
- ❑ Claves de Wireless & SSH
- ❑ Skeleton Keys
- ❑ Verificación de hooks de procesos
- ❑ Cambiar el fondo del escritorio
- ❑ Monitorear el clipboard
- ❑ Modificar Privilegios
- ❑ Manipular Eventos y Logs
- ❑ Control remoto vía RPC
- ❑ Manipulación de Servicios
- ❑ Manipular el Terminal Service
- ❑ Volcados de Memoria
- ❑ Pass The Ticket
- ❑ Golden Tickets / Silver Tickets
- ❑ Golden Tickets + SID History



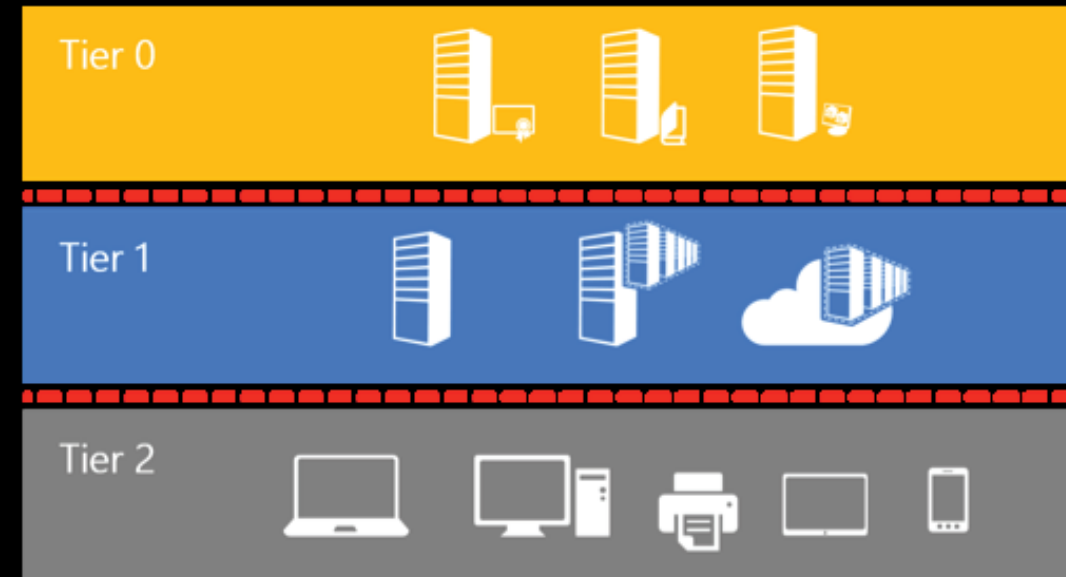
Consejos Generales del Blue Team

- ❑ Protección del Endpoint (Mimikatz requiere Administrator)
- ❑ LAPS (Local Administrator Password Solution)
- ❑ Tier Model



Cuentas:

- julio_da
- julio_adm
- julio



Consejos Generales del Blue Team

- ❑ Microsoft: [Mitigating Pass-the-Hash and Other Credential Theft, version 2](#)
 - ❑ LSA Protection
 - ❑ Protected Users Group
 - ❑ Credential Guard
- ❑ [PAW \(Privilege Access Workstations\)](#)

Para el RedTeam & BlueTeam



- ❑ **Mimikatz** puede ser utilizado de diferentes formas, aún cuando alguno de estos controles estén implementados, ejemplos cómo:
 - ❑ Remover la protección de LSASS
 - ❑ Cambiar la configuración wdigest para permitir credenciales en PlainText
 - ❑ Crear volcados de memoria y usar Mimikatz Offline
- ❑ **Probar y establecer mecanismos de detección.**
 - ❑ Attack Surface Reduction Rules (ASR)
 - ❑ Eventos
 - ❑ Sysmon
 - ❑ Network
 - ❑ Otras Herramientas como (EDR's, Monitoreo de Comportamiento, etc).



¿Preguntas?