What is DPAPI?

DPAPI (Data Protection API) is the built-in Windows service that encrypts and decrypts user secrets, browser passwords, saved credentials, Wi-Fi keys, and more, tied to the user's login. The encryption uses a per-user master key derived from the user's password. An attacker running as the user, or who steals the master key (and on a domain, the DPAPI backup key from a DC), can decrypt all of that user's protected secrets. It is abused to turn account access into a pile of cleartext credentials.

HOW IT WORKS

01 The abuse and payload

Once an attacker has a user's context or master key, DPAPI hands over their secrets:

- Decrypt the user's secrets in their session with a DPAPI tool (browser logins, Credential Manager, vaults).
- Steal and decrypt the master key offline with the user's password or hash.
- On a domain, abuse the DPAPI domain backup key from a Domain Controller to decrypt any user's DPAPI secrets, a powerful, quiet harvest.

Documented techniques shown for defenders.

> THE MASTER KEY IS EVERYTHING
>
> *DPAPI's protection collapses to the master key. Steal it (or the domain backup key) and every browser password, saved credential, and vault entry the user protected becomes cleartext.*

HOW TO DEFEND

- Protect the DPAPI domain backup key: it is a Domain-Controller secret that unlocks every user's DPAPI data; guard the DC accordingly.
- Limit local admin and enable [Credential Guard](/learn/active-directory/what-is-credential-gu to make stealing keys and the user context harder.
- Avoid storing sensitive secrets in browser/credential stores on high-value hosts.
- Detect access to DPAPI master-key files and abnormal credential-store reads.
- Strong user passwords, since the master key is derived from them.

SOURCES

[1] MITRE ATT&CK: Credentials from Password Stores (T1555)

[2] Microsoft: Data Protection API

[3] MITRE ATT&CK: Credential Access (TA0006)

Find the exposed credentials before an attacker does.

securelayer7.net/learn/credential-access/what-is-dpapi

Open online