# GitHub - TheWover/CertStealer: A .NET tool for exporting and importing certificates without touching disk.

By TheWover

Archived: 2026-04-05 22:00:29 UTC

A (v3.5 compatible) .NET tool for stealing and importing certificates in the Windows certificate store without touching disk. Useful for red team operations where you need to poach a certificate for pivoting purposes and want to do so with an in-memory post-ex payload.

This tool is flagged as malware by Defender. DO NOT run it from disk on-target. DO NOT run it in memory on target WITHOUT AMSI BYPASSED. And DO obfuscate it with a tool like ConfuserEx, just in case.

If you export a certificate with a private key as PFX then the password will be blank by default. *Blank*, not non-existent. Optionally, you may specify a password with the `--password` argument.

If keys are marked as not exportable then you will have to patch CAPI to allow export of non-exportable keys in the current process. This can be done with mimikatz via the `crypto::capi` command. If you are trying to export device certificates that are not exportable, mimikatz can instead patch the memory of the running lsass.exe process to bypass protections using the `crypto::cng` command.

Alternatively, you may extract the private keys manually using DPAPI operations. Use the user's DPAPI masterkey, (or a password, domain DPAPI private key, or system backup key to first decrypt the user's masterkey) to extract and decrypt the user's certificates from the registry. This can be done with SharpDPAPI or mimikatz. For more details, checkout the THEFT2 and THEFT3 sections of SpecterOps's whitepaper: Certified Pre-Owned. (Really you should just read that whole paper.)

```
 Examples:

Display this help message: CertStealer.exe --help
Listing all certs: CertStealer.exe --list
Listing all certs within the My store in CurrentUser: CertStealer.exe --name user --store My --list
Listing all certs within the CA store in LocalMachine: CertStealer.exe --name local --store CA --list
Exporting a cert by its thumbprint: CertStealer.exe --export AF724CB571166C24C0799E65BE4772B10814BDD2
Exporting a cert by its thumbprint as PFX: CertStealer.exe --export pfx AF724CB571166C24C0799E65BE4772B10814BDD2
Exporting a cert by its thumbprint as PFX, specifying a password: CertStealer.exe --password pass123 --export pf
Importing a cert into the My store in CurrentUser: CertStealer.exe --import My user Dw...snipped...gY=
Importing a cert into the CA store in LocalMachine: CertStealer.exe --import CA local Dw...snipped...gY=
Use verbose output (works for list and import): CertStealer.exe --list --verbose
```

---