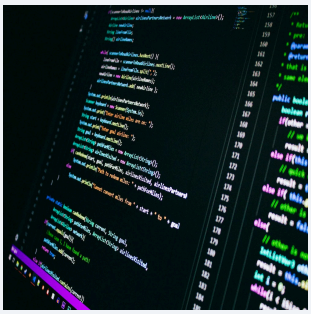
Security MARCH 23, 2023 | 11 MINUTE READ

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

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

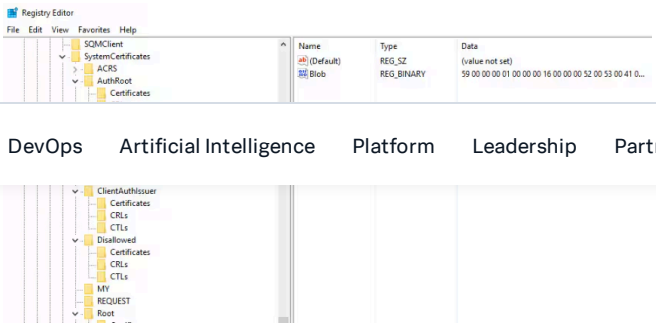
Certificate Services, including certificate theft, account persistence, domain escalation, and domain persistence.

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\System Certificates.
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 cryptdll.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 then enabling CAPI2 logs.

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

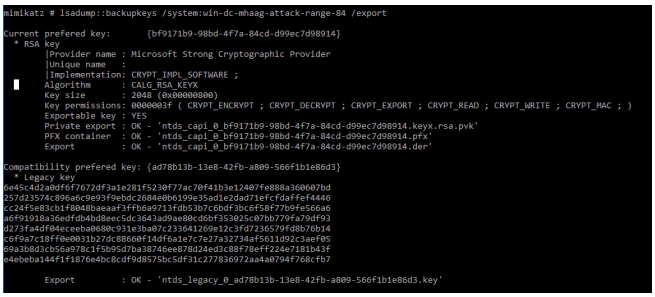
```
lsadump::backupkeys /system:<computer> /export
```

or

```
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



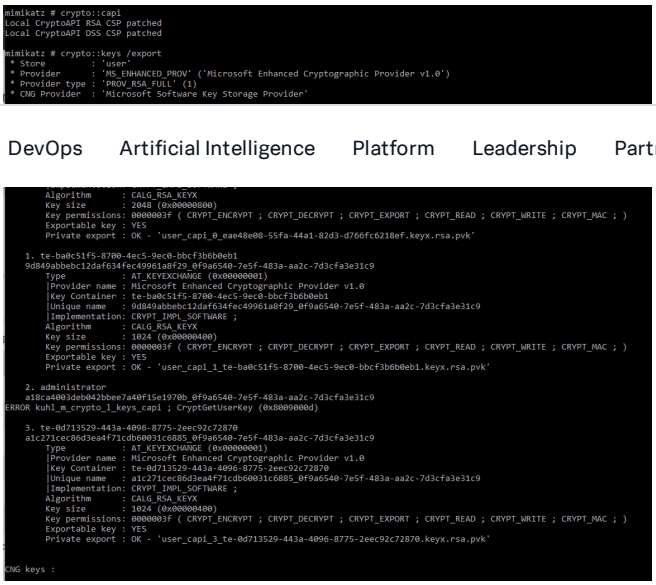
Splunk, 2023, MimiKatz LSADump

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
```

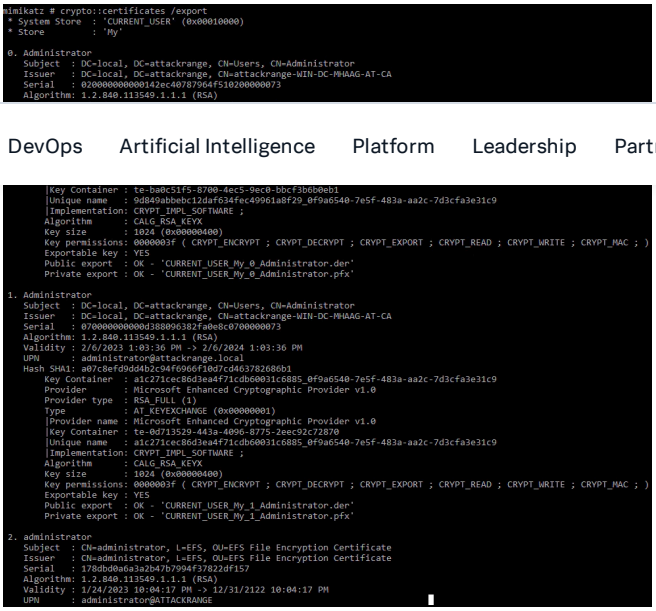


Splunk, 2023, MimiKatz Crypto CAPI

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)

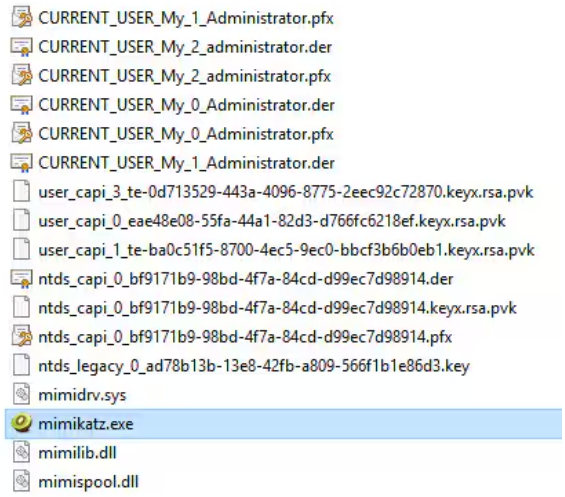
```
crypto::certificates /export
```

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.



Splunk, 2023, MimiKatz Crypto Certificates

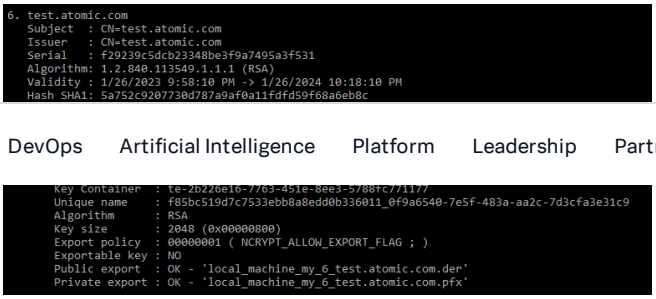
As found on disk -



Splunk, 2023, MimiKatz files on disk

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

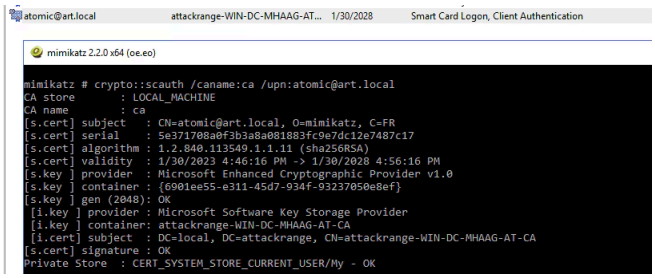
This command specifies which store to export the certificate - again .pfx and .der written to disk.



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?



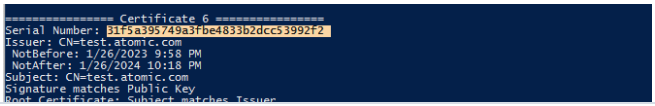
Splunk, 2023, MimiKatz Crypto scauth

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
```

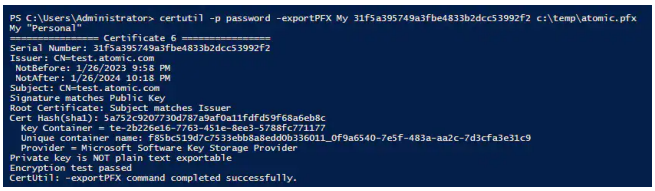
This command will list all certificates under “My” store. Get the serial of the certificate to extract.



Splunk, 2023, CertUtil.exe Certificate Output

Export

```
certutil -p password -exportPFX My 31f5a395749a3fbe4833b2dcc5399
```



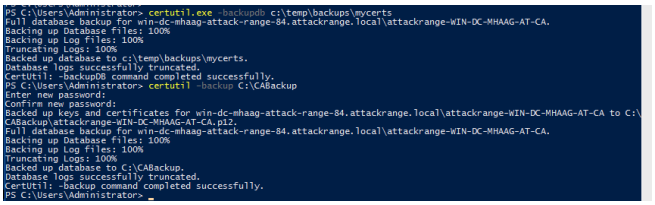
Splunk, 2023, CertUtil ExportPFX

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
```



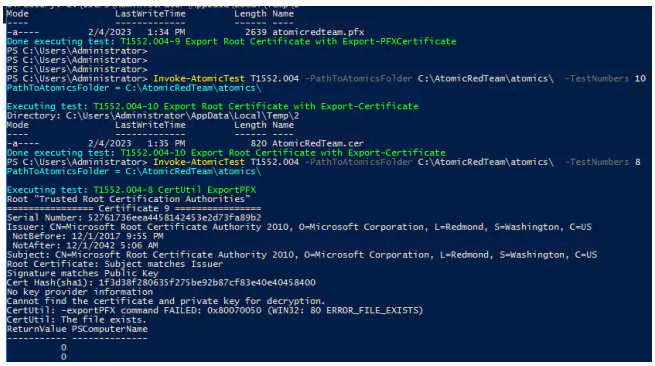
Splunk, 2023, CertUtil Backup

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

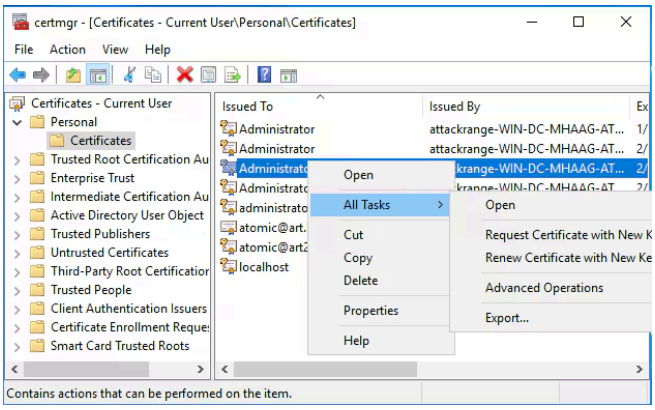
Certificate Cmdlets. Both are similar enough that if an adversary was attempting to extract a certificate both would provide the avenue needed.



Splunk, 2023, PowerShell Export-Certificate

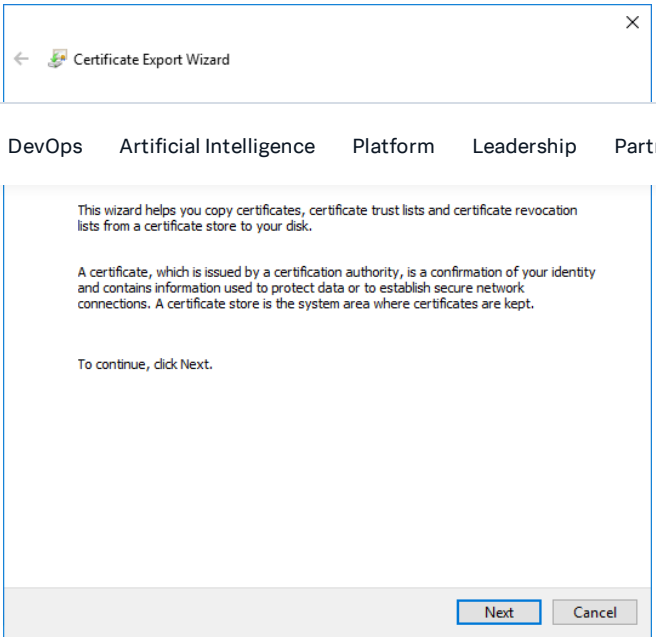
Certmgr.msc

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



Splunk, 2023, CertMGR

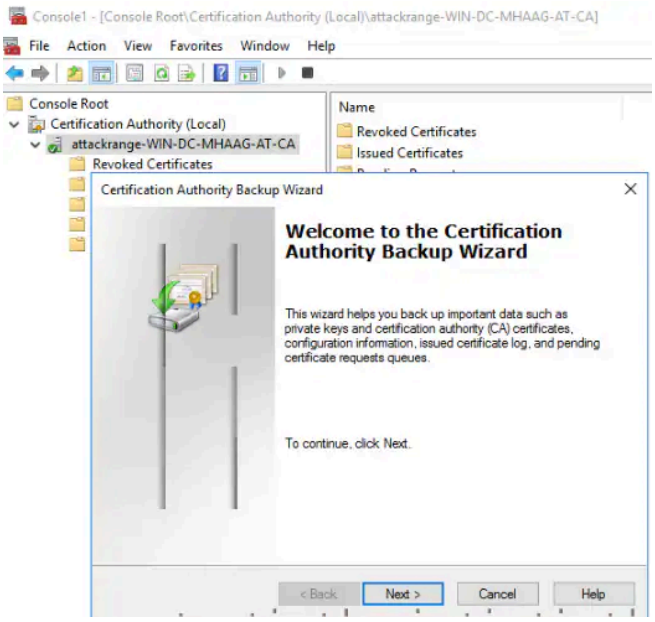
Once export is selected, the Certificate Export Wizard will appear and walk through the steps to export the certificate.



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

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 | Forma
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.

collection. Our focus is to identify exported certificates, EID 1007. However, there may be interest in monitoring others like EID 1006 or errors like EID 1008 and EID 1009.

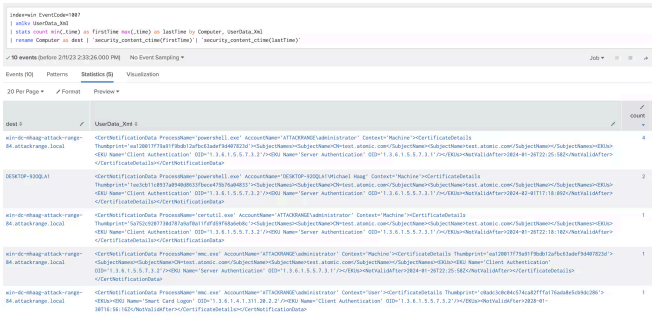
Utilize the following inputs to gather the event ID 70 from the CAPI log and event ID 1007 from the Certificate Lifecycle log sources.

```
[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.

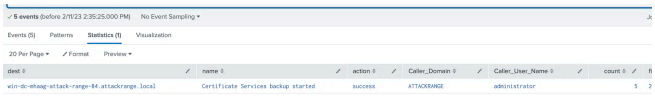


Splunk, 2023, Export Certificate

Windows Steal Authentication Certificates CS Backup

This analytic identifies when the Active Directory

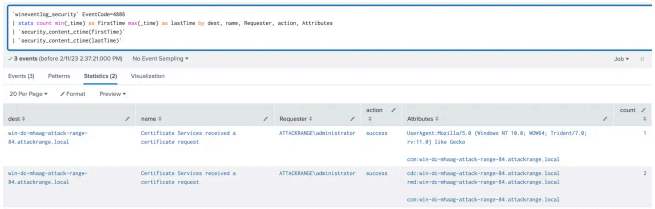
4876. This event triggers whenever the backup occurs in the UI of CertSrv.msc or via CertUtil.exe -BackupDB occurs.



Splunk, 2023, Export Certificate

Windows Steal Authentication Certificates Certificate Request

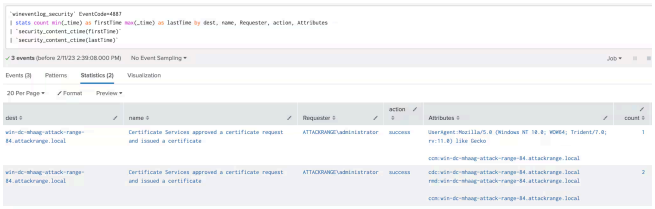
This analytic identifies when a new certificate is requested against the Certificate Services - AD CS. By its very nature this is not malicious, but should be tracked and correlated with other events related to certificate requests. When an account requests a certificate, the CA generates event ID 4886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



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."

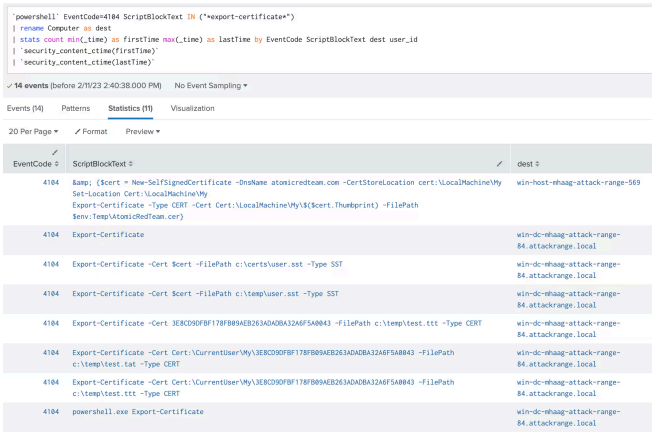


Splunk, 2023, Cert Issued

Windows PowerShell Export Certificate

This analytic identifies the PowerShell Cmdlet export-

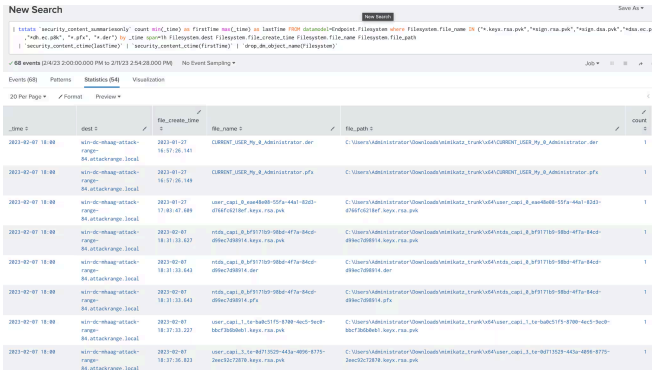
certificates local to the Windows endpoint within the Certificate Store.



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.



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.

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.

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
- 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 straight to your inbox.

Sign Up Now

Follow @Splunk ›

Follow @Splunk ›

© 2005 - 2024 Splunk LLC All rights reserved.