ADCS: La Amenaza Persistente que Vive en tu Dominio

Una mirada defensiva a uno de los vectores más críticos y menos monitoreados del dominio.

Meetup RedTeamRD / Junio

Presentado por:

Leonardo Núñez

Leonardo Núñez

- ➔ Ingeniero Telemático
- ➔ Red Team Lead @CBRT
- ➔ Director de CTFs @RaicesCyberOrg
- ➔ 4+ Años de Experiencia en Seguridad Ofensiva
- ➔ 2+ Años sufriendo por ADCS (todavía no es suficiente)
- ➔ Vivo en Discord: LeonVQZ
- ➔ Certificaciones: OSCP, Pentest+
- ➔ En el camino: CRTO, CESP-ADCS

Contenido

La Pesadilla del Blue Team

¿Qué es ADCS?

¿Qué es ADCS?

- Solución de Microsoft para Public Key Infrastructure (PKI) en premisa
- Emite, Gestiona y Revoca certificados
- Puede ser usado para::
  - Kerberos
  - Smart Card logins
  - Wi-Fi security
  - Y mucho más...

Es útil.

Se puede confiar

Pero es un vector furtivo para el compromiso total del dominio si no se maneja con extremo cuidado.

¿Por qué es la pesadilla del Blue Team?

- Fácil de configurar de manera insegura
- Proveedores que fomentan configuraciones peligrosas
- Permisos Excesivos Suceden Rápidamente
- Difícil de auditar automáticamente

¿Por qué los hackers aman ADCS?

- Escalaciones de Privilegios
- Robo de Certificados
- Métodos de Persistencia
- CVEs

Explotación de ADCS

- Escalaciones de Privilegios:
    - **ESC1**: Se le dan permisos de enrolamiento a usuarios de bajos privilegios a plantillas que permiten autenticación, permitiendo que los mismos provean el usuario a autenticar.
    - **ESC2**: El mismo escenario que ESC1, pero en vez de permitir solo autenticación, permite cualquier uso.
    - **ESC3**: Abusa los certificados con la funcionalidad de "Enrollment Agent Templates" la cual permite pedir certificados en nombre de otro usuario.
    - **ESC4**: Abusa los permisos excesivos que tienen que ver con el manejo de plantillas de certificados.
    - **ESC5**: Cualquier objeto de Active Directory que competa a la infraestructura de PKI.
    - **ESC6**: CVE-2022-26923 (Parcheado) EDITF_ATTRIBUTESUBJECTALTNAME2
    - **ESC7**: Abusa los permisos excesivos que tienen que ver con el manejo de certificados y/o Autoridades Certificadoras
    - **ESC8**: NTLM Relay hacia ADCS HTTP

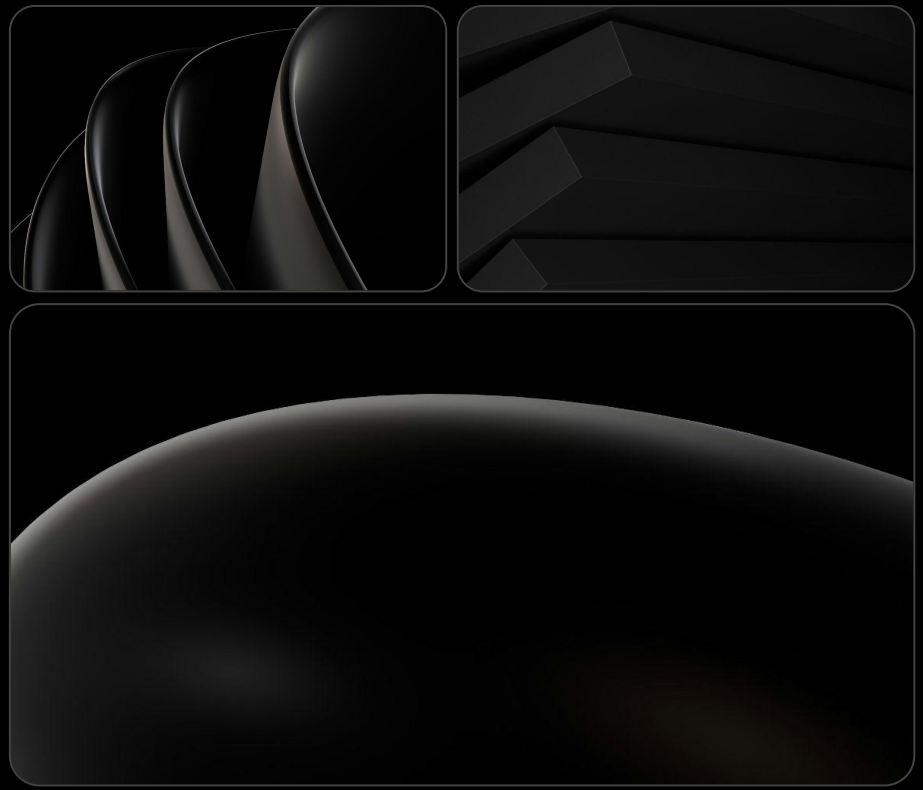
Explotación de ADCS

- **ESC9**: extensiones de seguridad deshabilitadas, UPN no válido de usuario
- **ESC10**: asignaciones de seguridad débiles
- **ESC11**: Relay NTLM hacia ICPR (ICertPassage Remote Protocol)
- **ESC12**: ADCS CA with YubiHSM `HKEY_LOCAL_MACHINE\SOFTWARE\Yubico\YubiHSM\AuthKeysetPassword`
- **ESC13**: Abuso de políticas
- **ESC14**: Abuso de ajustes no seguros de mapeos explícitos débiles
- **ESC15**: CVE-2024-49019 - Abuso de versiones 1 de plantillas, un atacante puede crear un CSR para incluir nuevas funcionalidades.
- **ESC16**: similar a ESC9, pero a nivel de CA

Explotación de ADCS

- Robo de Certificados:
    - Carpetas Compartidas
    - Almacenamiento Local de Certificados (Máquina y/o Usuario)
- CVEs:
    - CVE-2021-36942 (petitpotam)
    - CVE-2022-26923 (certifried)

¿Cuáles son los puntos débiles de ADCS?



Muchos

Fácil de Configurar de manera no segura

- TI necesita conocimientos expertos antes del primer despliegue.
- La configuración ADCS por defecto *no es segura por diseño* - es segura si ya conoces las trampas.
- Plantillas a menudo:
  - Permiten la entrada de **nombre alternativo del asunto (SAN)**
  - Se **publican a Usuarios Autenticados** por defecto
  - Incluyen **EKUs para cualquier propósito**
- El mero despliegue de ADCS en estado «funcional» puede introducir múltiples vías de ataque.

Los permisos se extienden por todas partes y es fácil pasarlos por alto

- Los atacantes sólo necesitan una ruta mal configurada, el blue team deben auditarlas todas.
- Los permisos de ADCS se extienden a través de:
  - Plantillas (ACLs)
  - Objetos CA (en Active Directory)
  - Derechos de inscripción/enrolamiento
  - DACLs en **NTAuth store**, **Objetos OID**, etc.
- Algunos de los **permisos más peligrosos parecen inofensivos** a menos que se comprendan sus implicaciones.
  - Por ejemplo, **ManageCA**, **Enrollment Agent**, o **GenericWrite** en objetos plantilla.

Sin visibilidad nativa / Registro débil

- El registro de Windows para ADCS es **insuficiente por defecto**:
  - No es fácil registrar quién solicitó qué certificado.
  - Es difícil rastrear qué certificado corresponde a qué identidad
- Las solicitudes de certificados pueden ser **silenciosas y no supervisadas** a menos que la auditoría esté bien configurada.

Suposiciones de confianza engañosas

- ADCS se encarga de la confianza entre los usuarios y las máquinas, pero no se impone límites por sí mismo.
- Si **NTAuthCertificates store** es envenenado, o un CA falsa es introducida - toda la confianza se rompe.
- Las configuraciones entre bosques **amplían el radio de explotación de un compromiso** silenciosamente.

Integración de Directorio Activo = Radio de Explotación Masivo

- Un certificado que pasa la autenticación con tarjeta inteligente = **Emisión de TGT** por KDC.
- Esto significa:
  - La autenticación basada en certificados puede suplantar completamente a **Administradores de dominio**.
  - Ataques de retransmisión NTLM a Web Enrollment = persistencia basada en certificados
- ADCS es una de las **pocas formas de saltarse completamente MFA** y obtener acceso como otra persona, completamente.
- Los certificados son identidad. Si comprometes la emisión de certificados, comprometes AD.

Plantillas de Legacy aún publicadas

Plantillas V1 son:

- Todavía instaladas por defecto
- A menudo publicadas sin intención
- No admiten el endurecimiento de la seguridad (por ejemplo, **sin aprobación del administrador**)

Requiere una revisión Manual y Especializada

- Auditar ADCS significa:
  - Revisar **cada configuración de plantilla**
  - Revisión cruzada de **permisos**
  - Inspección de **políticas de tarjetas inteligentes**
  - Comprobación del registro y de los **indicadores de configuración de CA**.
- No hay ninguna herramienta proporcionada por Microsoft que haga esto de principio a fin.
  - Herramientas como **PSPKIAudit**, **Certipy**, **ADCSKit**, o **ForgeCert** ayudan pero no son plug-and-play.
- Dificulta la operatividad la defensa en grandes organizaciones.

Vendors e integradores recomiendan valores por defecto inseguros

Muchos sistemas de terceros:

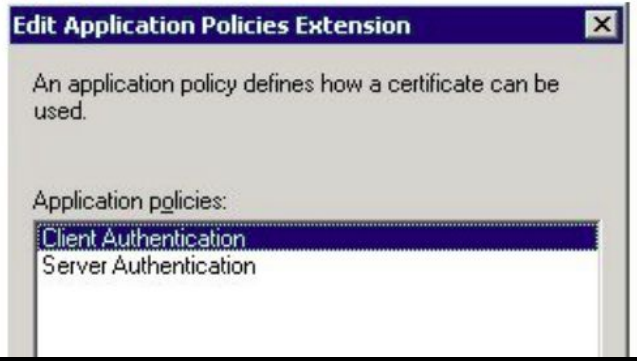
- Requerir la publicación de plantillas inseguras (por ejemplo, SAN permitido).
- Confían en una inscripción demasiado permisiva
- Ofrecen documentación deficiente para una integración segura

Start an administrative command prompt on one of your intermediate CA server and issue the following command;

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
```

Vendors e integradores recomiendan valores por defecto inseguros

7. Add **Client Authentication** to the set of application policies:
   a. Click **Add**
   b. Select **Client Authentication** and click **OK**
   c. Click **OK**



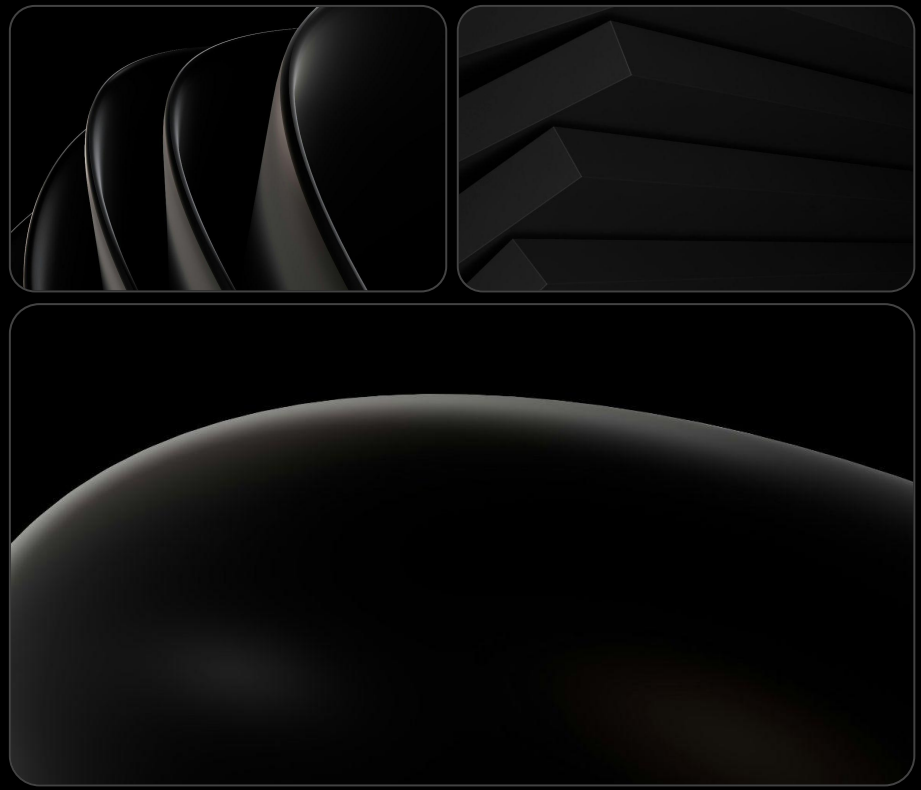
Claves y secretos mal protegidos

- YubiHSM u otros HSMs:
  - A veces almacenan **contraseñas de claves de autenticación en texto plano en el registro** (ESC12)
- Muchas organizaciones dejan **private CA keys exportable** (ESC8)

La superficie de ataque es vasta, pero oculta

- El abuso de ADCS puede ser:
  - **Acceso inicial** (retransmisión NTLM a Web Enrollment)
  - **Movimiento lateral** (suplantación de plantilla)
  - **Persistencia** (certificados de apariencia legítima)
- Los ataques parecen «legítimos»: sin malware, sin scripts, solo PKI.
- Los certificados no son detectados por EDR.

Recomendaciones Prácticas



Aprender

Inventario completo de plantillas y triaje

Objetivo: *Identificar y clasificar todas las plantillas de certificados en función de su potencial de abuso.*

- Utilice `Certipy`:

```shell
certipy find -u 'usuario@dominio' -p 'contraseña' -target 192.168.1.1
# No utilizar la opción -vulnerable
```

- Hacer triage de plantillas utilizando esta lógica:
  - ¿Permite **ENROLLEE_SUPPLIES_SUBJECT**?
  - ¿Permite **Any Purpose EKU / ClientAuth**?
  - ¿Requiere **ManagerApproval**?
  - ¿Quién puede **Enrolar / AutoEnrolar**?
- Marcar todas las plantillas con características **ESC1-4** como **críticas**. Marcar como no publicas si no es necesario.

Acción: *Eliminar o bloquear cualquier plantilla que permita la entrada SAN o la autenticación de clientes sin autorización estricta.*

Bloquear la inyección de nombres alternativos de asunto (SAN)

***Objetivo**: Evitar que los atacantes suplanten identidades en las solicitudes de cert.*

- Enforce `EDITF_ATTRIBUTESUBJECTALTNAME2` como **disabled**:

```PowerShell
certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2 net stop certsvc && net start certsvc
```

***Acción**: Elimina todas las rutas que permiten a los atacantes especificar sus propios UPNs / SANs.*

Auditar y minimizar plantillas de agentes de inscripción

***Objetivo**: Prevenir el abuso de «solicitud en nombre de».*

- Encontrar plantillas con **EnrollmentAgent** EKU:

```powershell
Get-CATemplate | Where-Object {$_.EKUs -match "Enrollment Agent"}
```

- Restrinja los derechos de **Inscripción** a *sólo cuentas de servicio PKI*.
- Nunca permita que **Usuarios autenticados** o grupos grandes de AD accedan a ellos.

***Acción**: Asumir cualquier plantilla pública de EA = toma de dominio.*

Comprobación de integridad del almacén de NTAuth

***Objetivo**: Asegurarse de que sólo **se utilizan CA de confianza** para los inicios de sesión con tarjeta inteligente / certificado.*

- Consultar el almacén:

```cmd
certutil -viewstore NTAuth
certutil -store my
certutil -store -enterprise
certutil -user -store My
```

- Valide cada huella digital de CA: elimine las CA falsas o heredadas:

```cmd
certutil -delstore NTAuth "<huella>"
```

Acción: Limpiar CAs antiguas de cross-forest o de prueba añadidas sin una revisión.

Auditar y bloquear permisos de CA

***Objetivo**: Impedir que los usuarios gestionen CA, plantillas o emitan certificados.*

- Utilice `ADExplorer` o `PowerView` para comprobar:
  - `ManageCA`
  - Emitir y gestionar certificados
  - Gestionar plantillas
- Valide las ACL de CA en AD mediante:

```PowerShell
Get-ACL "CN=CAName,CN=Public Key Services,CN=Services,CN=Configuration,DC=domain,DC=com"
```

***Acción**: Sólo las cuentas PKI de nivel 0 o reforzadas deben tener derechos de gestión de CA.*

Implementar la auditoría del ciclo de vida de los certificados

***Objetivo**: Detectar el abuso de certificados, realizar un seguimiento de la emisión y crear una trazabilidad forense.*

- Habilitar:
  - Auditoría de acceso a servicios de directorio
  - Auditoría de servicios de certificación
  - Habilitar los siguientes eventos: 4886, 4887, 4888, 4899, 4900 4871, 4872
- Envía los registros a SIEM y alerta:
  - Plantillas ClientAuth inesperadas
  - Inicio de sesión con tarjeta inteligente para cuentas DA
  - Logins basados en certificados con SANs inesperados

Acción: Construir detección alrededor del abuso de certificados. La mayoría de las organizaciones no lo controlan en absoluto.

ID de evento	Descripción	Relevancia
4886	Los servicios de certificación recibieron una solicitud de certificado	Se activa cuando se envía una solicitud de certificado (independientemente del resultado). Útil para detectar *cuándo* y *quién* solicita un certificado.
4887	Los servicios de certificación aprobaron una solicitud de certificado y emitieron un certificado	El certificado **se emitió correctamente**. **Importante para el seguimiento de abusos**.
4888	Los Servicios de Certificación denegaron una solicitud de certificado	Útil para violaciones de políticas o para detectar intentos de sondeo (atacantes probando plantillas).
4899	Ha cambiado la extensión de una solicitud de certificado	Señala **modificación de solicitudes de certificado** - puede detectar manipulación o abuso de los campos SAN/UPN.
4900	Se ha modificado una plantillas de certificado	Útil para la detección de ESC4.
4871	Servicios de certificación recibió una solicitud para publicar la lista de revocación de certificados (CRL)	Indica una acción de mantenimiento a nivel de CA. Puede ser relevante durante la limpieza de ataques o el backdooring de los puntos de distribución de CRL.
4872	Los servicios de certificación han publicado la CRL	Confirma que la CRL se ha publicado correctamente. Los cambios aquí podrían formar parte de pistas de encubrimiento o envenenamiento de CA.

YubiHSM / Auditoría de almacenamiento de claves privadas

***Objetivo**: Garantizar que las claves privadas de la CA se almacenan de forma segura.*

- Validar:
  - Las claves privadas de CA son *no exportables*.
  - Los secretos del HSM (por ejemplo, `AuthKeysetPassword` de YubiHSM) **no están en texto plano**.
- Compruebe si hay valores en texto plano en el registro:

```powershell
Get-ItemProperty -Path "HKLM:\SOFTWARE\Yubico\YubiHSM" | Format-List
```

***Acción**: Revisar todos los secretos PKI y ubicaciones de almacenamiento de claves CA. Tratar como credenciales de nivel 0.*

Eliminar plantillas heredadas v1

***Objetivo**: Eliminar las plantillas que no se pueden proteger.*

- Ejecutar:

```cmd
certutil -v -template | findstr "Schema Version"
```

- Elimina las no utilizadas:

```cmd
certutil -deltemplate "User"
```

***Acción**: Eliminar rutas de ataque heredadas. Ya no estás ejecutando 2003.*

Detección de desviación de la línea de base de ADCS

***Objetivo**: Saber si alguien introduce plantillas backdoor o modifica el acceso.*

- Monitorizar:
  - Creación de nuevas plantillas
  - Cambios en las ACL de inscripción
  - GPO que modifican el comportamiento de los certificados
- Construir un mecanismo de detección de cambios frente a una configuración buena y válida.

Acción: Defiéndase contra las amenazas internas o la persistencia silenciosa mediante la supervisión de la desviación.

Locksmith

Vival el Open Source

Modos de Operación

1. Identificar Problemas y Soluciones - Output en Consola
2. Identificar Problemas - Output en CSV
3. Identificar Problemas y Soluciones - Output en CSV
4. Corregir todo de manera automática

Gracias

LinkedIn: in/leonardo-n/
Discord: LeonVQZ
Email: lnunez@cbrt.com.do /
contact@leonvqz.com