SYNACKTIV

DLHell : L'enfer du remote DLL Hijack via DCOM

Kévin Tellier

WineRump 2024

@k3vinTell, @Synacktiv

Whoami

SYNACKTIV

- Kévin Tellier
- Pentesteur chez Synacktiv depuis 3 ans à Paris
- Intéressé par les sujets relatifs à Windows/AD

DCOM DLL Hijacking

SYNACKTIV

- Recherche de mouvement latéraux via DCOM
- Concept présenté par @domchell de MDSec en 2020
- Exploitation un peu painful si pas automatisée
- Cherchais tool ./ qui permet de faire ça facilement
- Here comes DLHell

What is DCOM ?

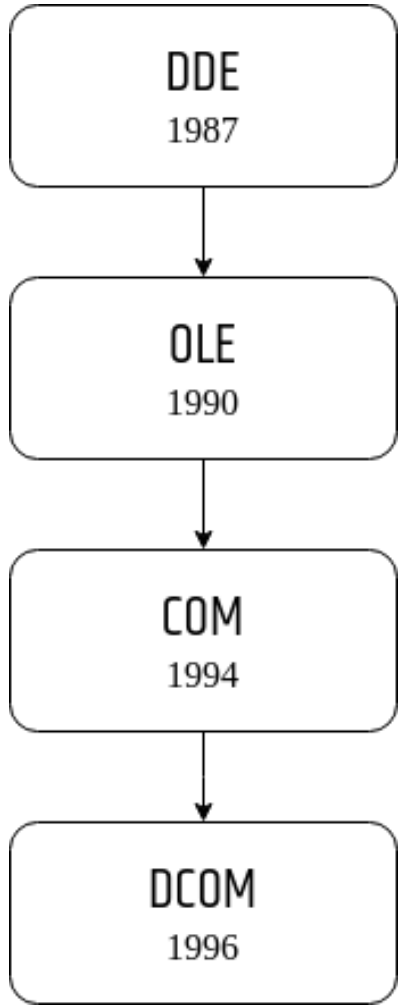
SYNACKTIV

- On part déjà bien…

Les Origines

SYNACKTIV

- Introduction de DDE (Dynamic Data Exchange) en 1987
- Protocole client-serveur pour échanger des données entre applications
- Utilisé initialement par le presse-papier
- Evolution vers OLE (Object Linking and Embedding) en 1990
- Puis vers COM en 1994
- ActiveX, DCOM, COM+ sont des technologies COM



COM

Component Object Model

SYNACKTIV

Framework permettant le développement de composants orientés objets réutilisables via différents languages de programmation

Le but étant de pouvoir manipuler des objets indépendemment de leur emplacement (même processus, même thread etc...)

DCOM

Distributed COM

SYNACKTIV

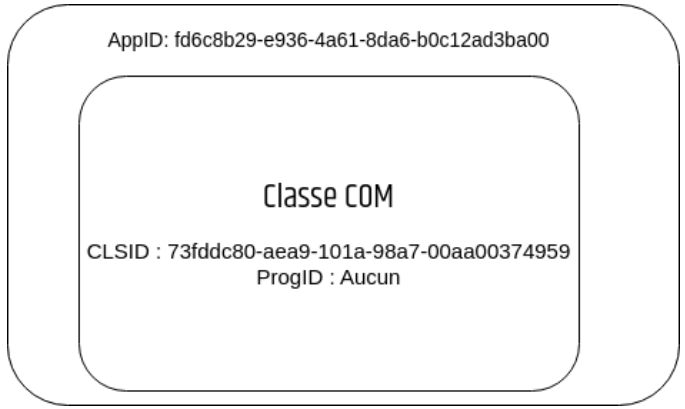
- Adversaire de CORBA (demander à *<vieux_collègue>* pour + de détails)
- Conçu comme une extension de COM sur le réseau
- Protocole propriétaire de Microsoft permettant d'exposer des objets applicatifs à travers des appels RPC
- Grosso-modo : DCOM = COM + RPC
- Résoud les problèmes suivants:
  - Le mashalling ("serialisation"/"désérialisation") des paramètres
  - Garbage collector
  - Gestion de l'authentification et du transport

COM

SYNACKTIV

Définitions

- **CLSID (Class Identifier)** : GUID identifiant chaque objet de classe COM (ex: 49B2791A-B1AE-4C90-9B8E-E860BA07F889)
- **ProgID (Programmatic Identifier)** : Identifiant friendly (optionnel) désignant la classe COM (ex: MMC20.Application)
- **AppID (Application Identifier)** : Identifiant regroupant plusieurs objets COM relatifs à un executable. Permet de fixer des paramètres de sécurité par défaut pour un groupe d'objets



Enumération

CLSID

L'ensemble des objets COM sont listés dans la base de registre et peuvent être énumérés via Powershell.

- Lister les CLSID

```
PS C:\Users\user> reg query "HKCR\CLSID\"
HKEY_CLASSES_ROOT\CLSID\CLSID
HKEY_CLASSES_ROOT\CLSID\{0000002F-0000-0000-C000-000000000046}
HKEY_CLASSES_ROOT\CLSID\{00000300-0000-0000-C000-000000000046}
HKEY_CLASSES_ROOT\CLSID\{00000301-A8F2-4877-BA0A-FD2B6645FB94}
HKEY_CLASSES_ROOT\CLSID\{00000303-0000-0000-C000-000000000046}
[...]
```

Enumération

CLSID

SYNACKTIV

La clé de registre CLSID pointe également vers l'implémentation de la classe via les valeurs suivantes :

- **LocalServer32**
  - Crée un processus à partir d'un executable
- **InProcServer32**
  - Charge une DLL

Activation

SYNACKTIV

- Droits par défaut
  - **Remote** : Administrateur
  - **Local** : Utilisateur intéractif
- Utilise le port 135/tcp pour activer la classe remote
- Utilise le composant DCOM Activator de RPCSS

DLL Hijacking

SYNACKTIV

Un certain nombre de classes DCOM chargent des librairies qui ne sont pas signées/n'existent pas lorsqu'elle sont instanciées.

On peut alors obtenir une RCE à partir d'un accès en lecture/écriture au disque de la victime en déposant une DLL malveillante.

DLL Hijacking

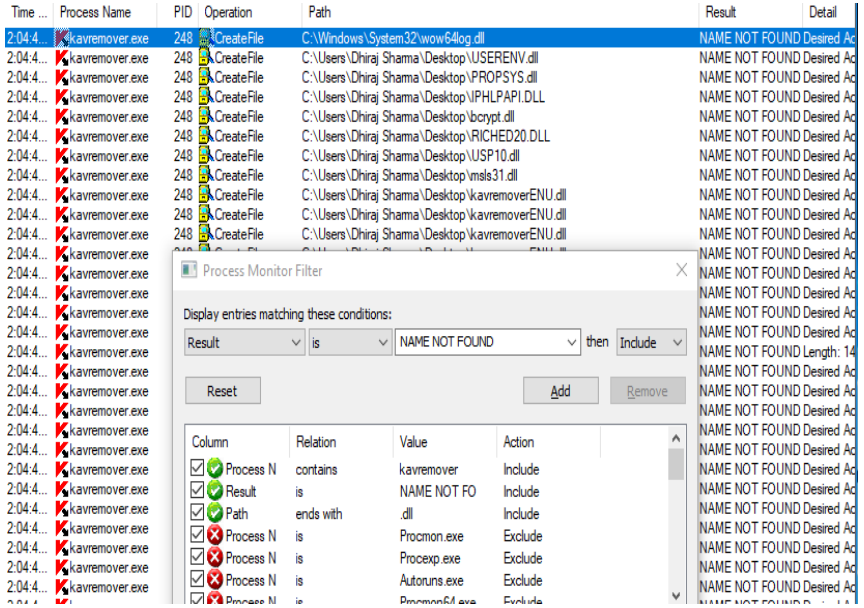
SYNACKTIV

1. On récupère la DLL vulnérable
2. On liste les exports de fonctions vulnérables
3. On compile la DLL malveillante avec les fonctions exportées extraites
4. On remplace la DLL malveillante par une DLL légitime ou une DLL n'existant pas
5. On instancie la classe DCOM vulnérable
6. Enjoy

Trouver des classes vulnérables

SYNACKTIV

1. Lancer Procmon
2. Activer la classe COM
3. Ajouter un filtre "Result is NAME NOT FOUND" sur les fichiers .dll



DLHell

SYNACKTIV

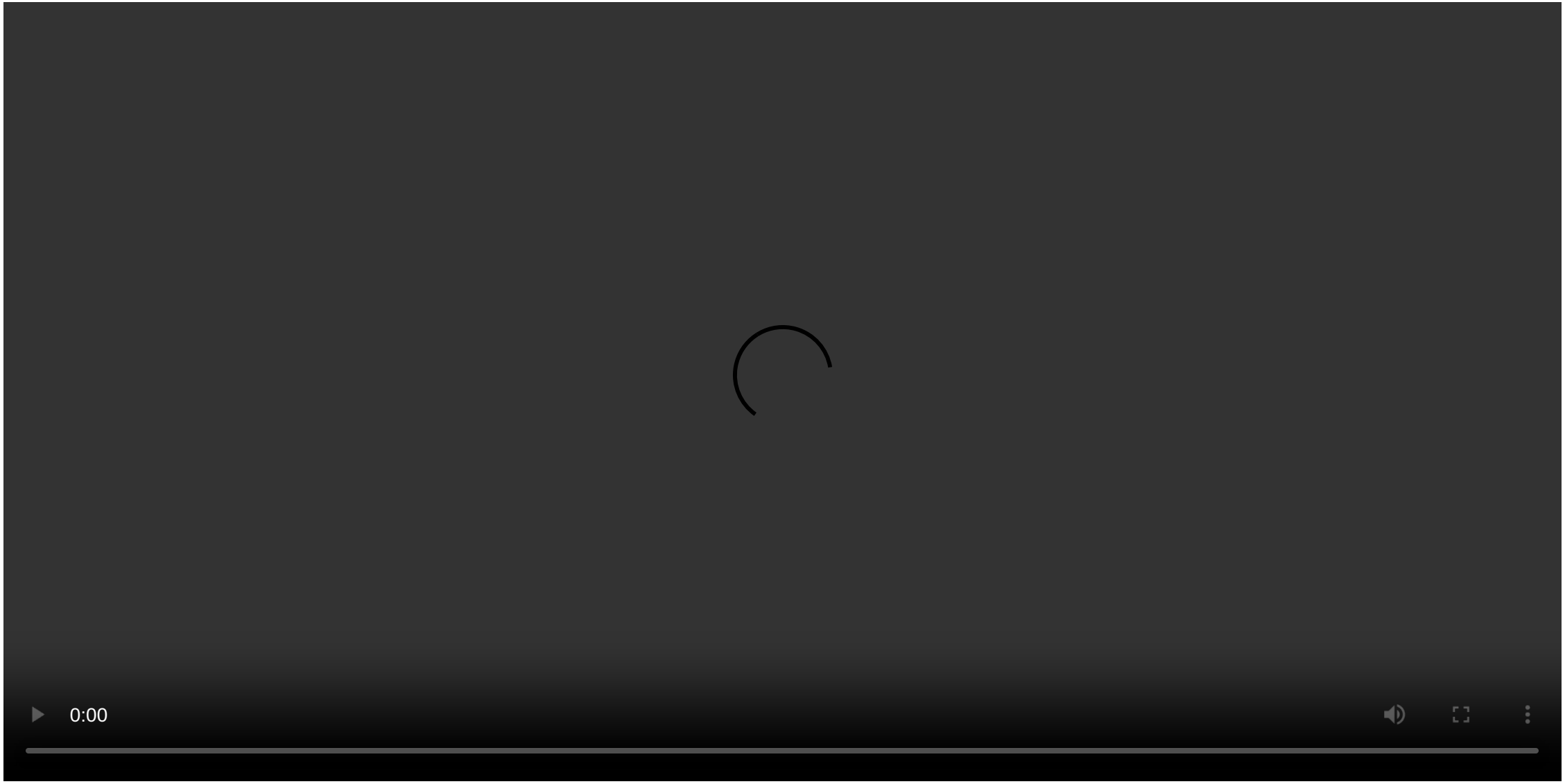
- Avec DLHell (https://github.com/synacktiv/DLHell)

```
$ DLHell.py -list
$ DLHell.py -t template.tpe -c 'calc.exe' -target 'domain/user:password@ip' -progid WordPad.Document.1
```

- Réalise les étapes de la slide précédente
- Syntaxe Impacket
- Les CLSID/ProgID vulnérables sont pré-renseignés dans un fichier json

DLHell : Demo time

SYNACKTIV



SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com