COM Object hijacking后门的实现思路——劫持explorer.exe

嘶吼roartalk / 2017-09-01 03:52:31 / 浏览数 2417 安全技术 技术讨论 顶(0) 踩(0)

0x00 前言

在之前的文章介绍了两种利用COM对象劫持实现的后门，利用思路有一些区别：

第一种，通过CLR劫持.Net程序

正常CLR的用法：

设置注册表键值HKEY_CURRENT_USER\Software\Classes\CLSID

cmd下输入：

```
SET COR_ENABLE_PROFILING=1
SET COR_PROFILER={11111111-1111-1111-1111-111111111111}
```

CLR能够劫持当前cmd下所有.Net程序的启动

后门利用思路：

我尝试通过WMI修改环境变量，使CLR作用于全局，就能够劫持所有.Net程序的启动

经实际测试，该方法有效，系统启动后默认会调用.Net程序，加载CLR，后门触发

第二种，劫持CAccPropServicesClass和MMDeviceEnumerator

该方法曾被木马COMpfun使用，所以思路也是从COMpfun学到的

设置注册表键值HKEY_CURRENT_USER\Software\Classes\CLSID能够指定实例CAccPropServicesClass和MMDeviceEnumerator对应加载的dll

而IE浏览器进程iexplore.exe启动时会调用以上两个实例

所以通过注册表设置CAccPropServicesClass和MMDeviceEnumerator对应加载的dll，能够劫持IE浏览器的启动，实现后门触发

当然，该方法只能算得上是一个被动后门，只有用户启动IE浏览器，才能触发后门

然而，在众多COM对象中，可供利用的劫持对象不唯一，甚至存在能够劫持桌面进程explorer.exe的方法，相当于一个主动后门

例如：劫持MruPidlList

注：

该方法曾被多个已知的恶意软件使用

本着通过研究所有已公开的COM对象后门利用方法，进而总结应对COM劫持防御方法的原则，本文将要介绍另外两种COM劫持的后门利用方法

之前的文章：

《Use CLR to maintain persistence》

《Use COM Object hijacking to maintain persistence——Hijack CAccPropServicesClass and MMDeviceEnumerator》

0x01 简介

本文将要介绍以下内容

· 通过劫持MruPidlList实现的后门思路

· 恶意利用实例

· 总结应对COM劫持的防御方法

0x02 通过劫持MruPidlList实现的后门思路

注册表位置：HKCU\Software\Classes\CLSID

创建项{42aedc87-2188-41fd-b9a3-0c966feabec1}

创建子项InprocServer32

Default的键值为测试dll的绝对路径：C:\test\calc.dll

创建键值： ThreadingModel REG_SZ Apartment

如下图

该注册表位置对应COM对象MruPidlList，作用于shell32.dll

而shell32.dll是Windows的32位外壳动态链接库文件，用于打开网页和文件，建立文件时的默认文件名的设置等大量功能

直观的理解，explorer.exe会调用shell32.dll，加载COM对象MruPidlList

系统在启动时默认启动进程explorer.exe，如果劫持了COM对象MruPidlList，就能劫持进程explorer.exe，实现后门随系统开机启动，相当于是主动后门

当然，为便于测试，不需要重启系统，结束进程explorer.exe再新建进程explorer.exe就好

新建进程后，加载calc.dll，弹出计算器，如下图

测试64位系统，注册表位置不变，但是需要换用64位dll，重启时后门触发，启动calc.exe，如下图

Win8系统同样适用，如下图

0x03 恶意利用实例

1、COMRAT

怀疑与Uroburos和Agent.BTZ同源

Uroburos：至今发现的最先进rootkit恶意程序之一

Agent.BTZ：一款在2008年用于渗透五角大楼的恶意软件

详细资料：

https://www.nsec.io/wp-content/uploads/2015/05/uroburos-actors-tools-1.1.pdf

2、ZeroAccess rootkit

ZeroAccess rootkit：感染过大约900多万台计算机

详细资料：

https://nakedsecurity.sophos.com/2012/06/06/zeroaccess-rootkit-usermode/

https://www.sophos.com/en-us/threat-center/technical-papers/zeroaccess-botnet.aspx

注：

ZeroAccess rootkit还使用过另一个COM劫持的位置

注册表位置：HKCU\Software\Classes\clsid{fbeb8a05-beee-4442-804e-409d6c4515e9}

利用方法同上，也能够劫持explorer.exe

3、BBSRAT

详细资料：

https://researchcenter.paloaltonetworks.com/2015/12/bbsrat-attacks-targeting-russian-organizations-linked-to-roaming-tiger/

http://2014.zeronights.org/assets/files/slides/roaming_tiger_zeronights_2014.pdf

0x04 防御

由于COM对象是操作系统的正常功能，禁用COM对象不太现实

以下键值指向的dll路径应该特别注意：

· HKCU\Software\Classes\CLSID{42aedc87-2188-41fd-b9a3-0c966feabec1}

· HKCU\Software\Classes\CLSID{fbeb8a05-beee-4442-804e-409d6c4515e9}

· HKCU\Software\Classes\CLSID{b5f8350b-0548-48b1-a6ee-88bd00b4a5e7}

· HKCU\Software\Classes\Wow64\32\Node\CLSID{BCDE0395-E52F-467C-8E3D-C4579291692E}

防御方法：

1、使用应用程序白名单规则，禁止加载第三方dll

2、对注册表HKCU\Software\Classes\CLSID的写入和修改操作进行记录并调查

更多关于COM对象劫持的资料可参考：

https://attack.mitre.org/wiki/Technique/T1122

0x05 小结

本文介绍了两种利用COM劫持实现的后门方法，结合之前文章的两种利用方法，综合分析COM劫持的防御方法。
特别值得注意的是，COM劫持后门能够绕过Autoruns对启动项的检测，实际防御时应该注意该细节。

>本文为 3gstudent 原创稿件， 授权嘶吼独家发布，如若转载，请注明原文地址： http://www.4hou.com/technology/7402.html