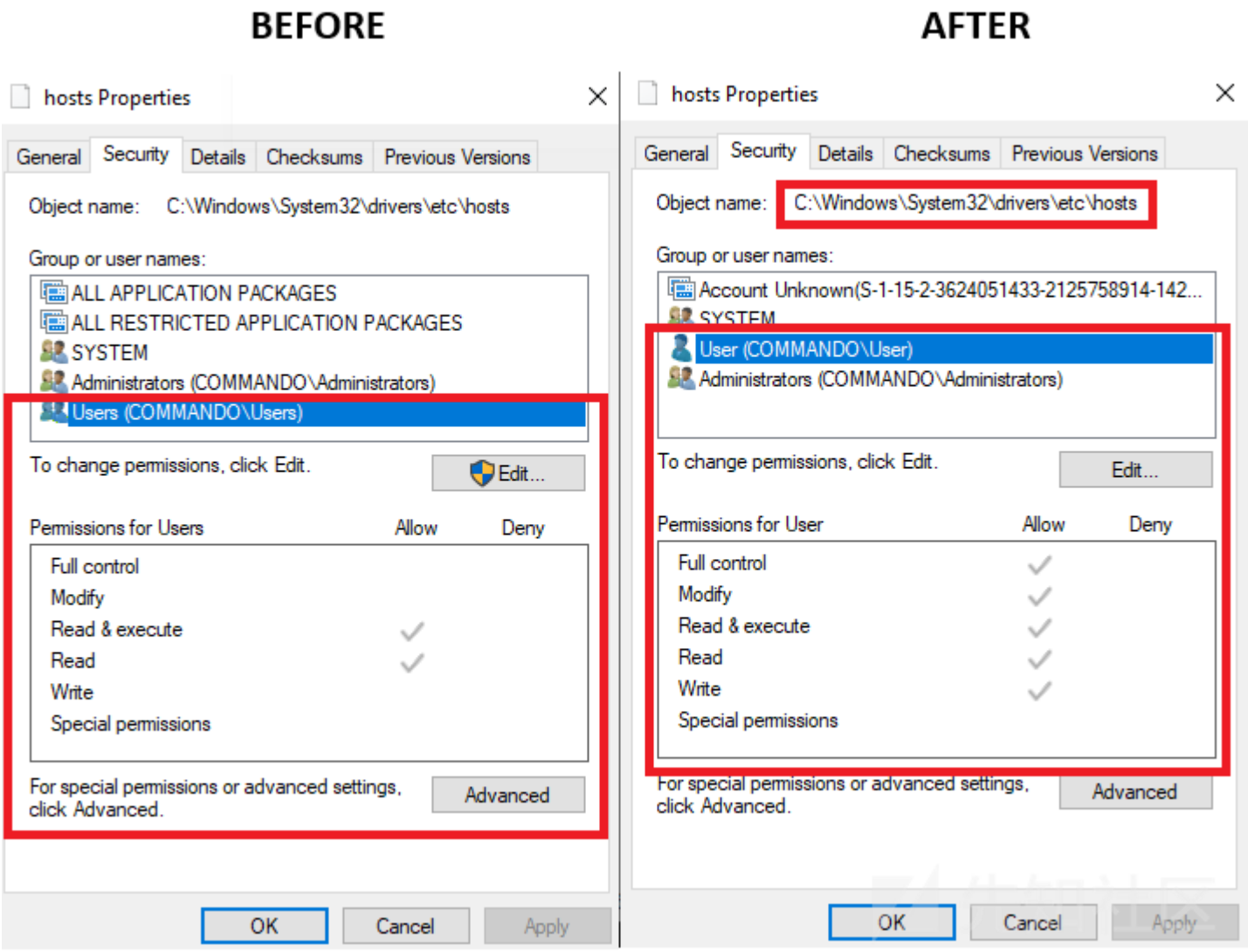
CVE-2019-0841：Windows DACL权限覆写权限提升漏洞

angel010 / 2019-04-15 09:30:00 / 浏览数 6115 安全技术 漏洞分析 顶(0) 踩(0)

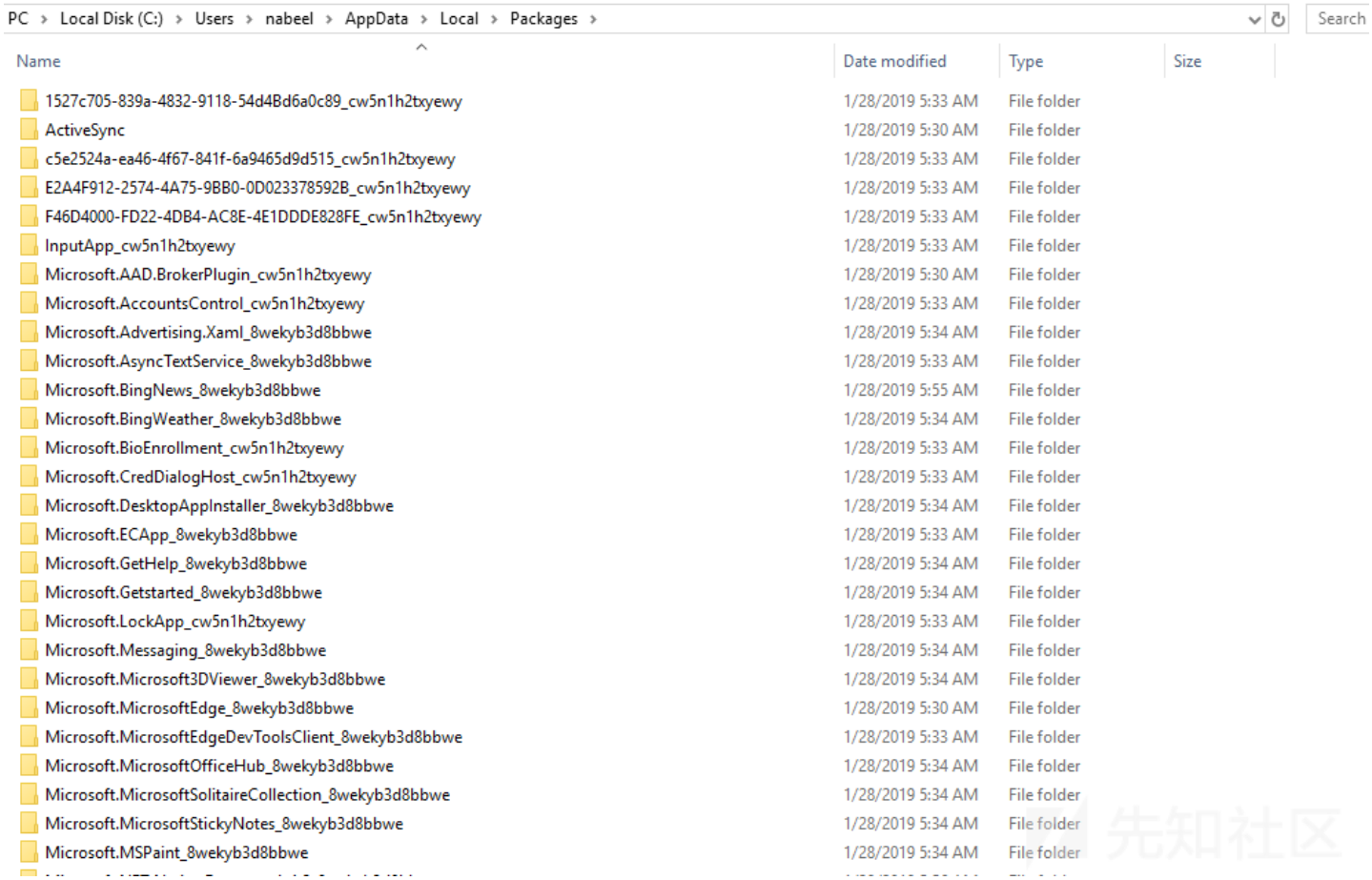
该漏洞允许低权限的用户通过覆写目标文件的权限来劫持属于NT AUTHORITY\SYSTEM的文件。成功利用就可以使低权限的用户获得对目标文件的完全控制权限。



所有的Windows APP都有一个settings.dat文件用来记录APP的注册表设置。该文件是一个可以在注册表中加载和修改的注册表文件。
如果用户启动一个Windows APP比如Microsoft Edge，就可以访问NT AUTHORITY\SYSTEM的settings.dat文件，并以低权限用户访问该文件。问题是如何滥用该特权文件访问呢？

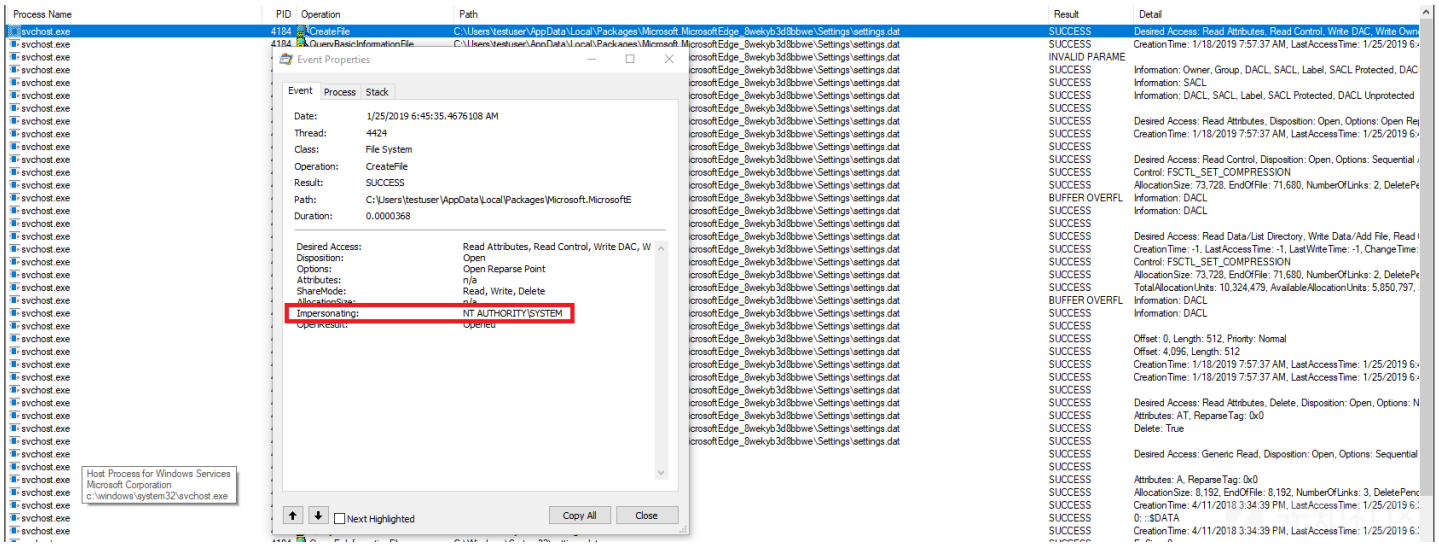
漏洞

首先看一下Microsoft Edge的settings.dat文件。
所有的Windows APPs用户配置文件都保存在当前用户的APPDATA文件夹：
C:\Users\<username>\AppData\Local\Packages\<Packagename>



Windows 10有一些安装的默认APP

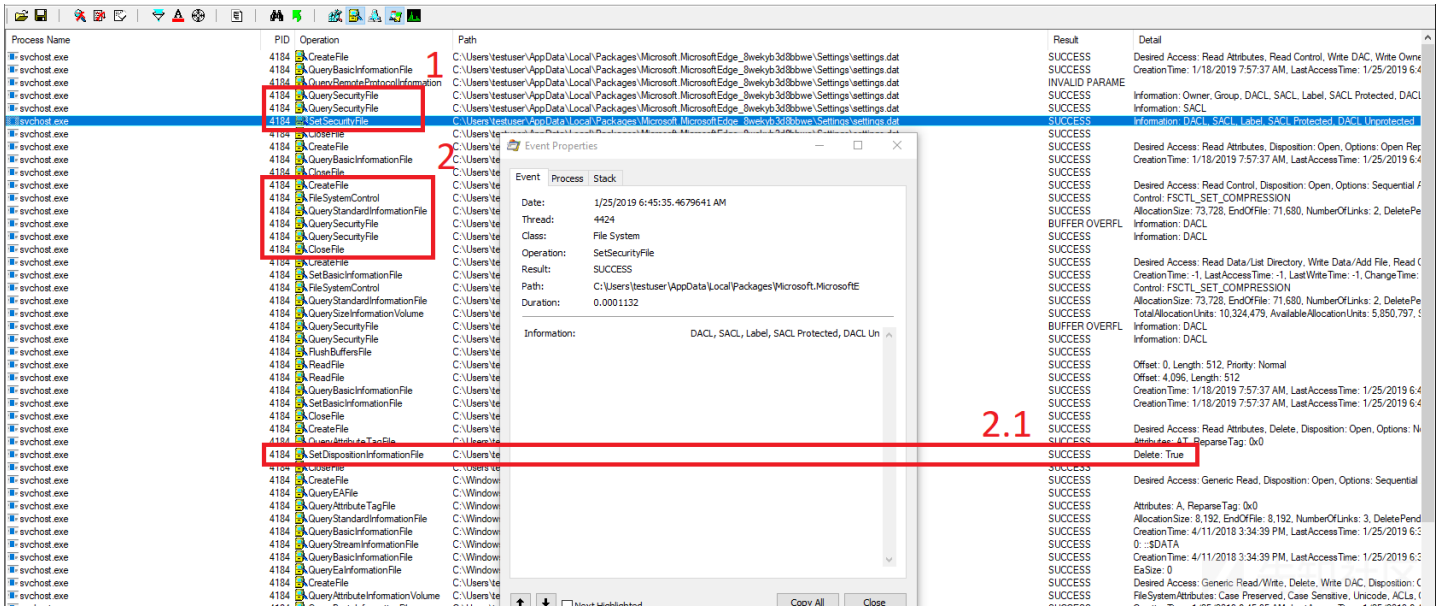
每个package都有一个`settings.dat`文件，是`NT AUTHORITY\SYSTEM`来写入配置变化的。
Windows App启动后，系统会使用`OpLock`操作来预防其他进程在APP运行时使用或访问该文件。
在本例中，启动Microsoft Edge后，`settings.dat`文件会以`NT AUTHORITY\SYSTEM`打开，如下图所示：

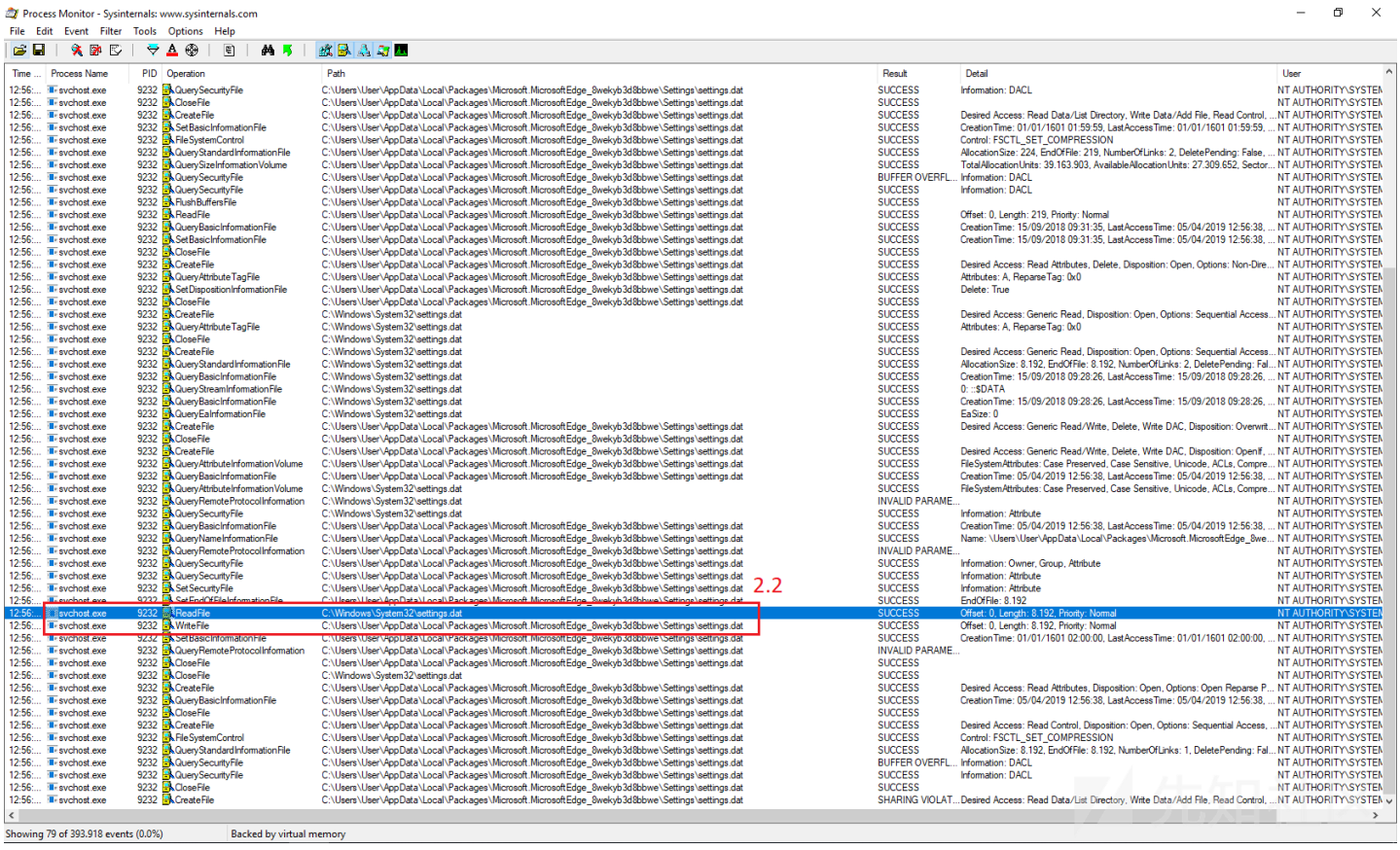


打开后，会看到执行一些基本的完整性检查：

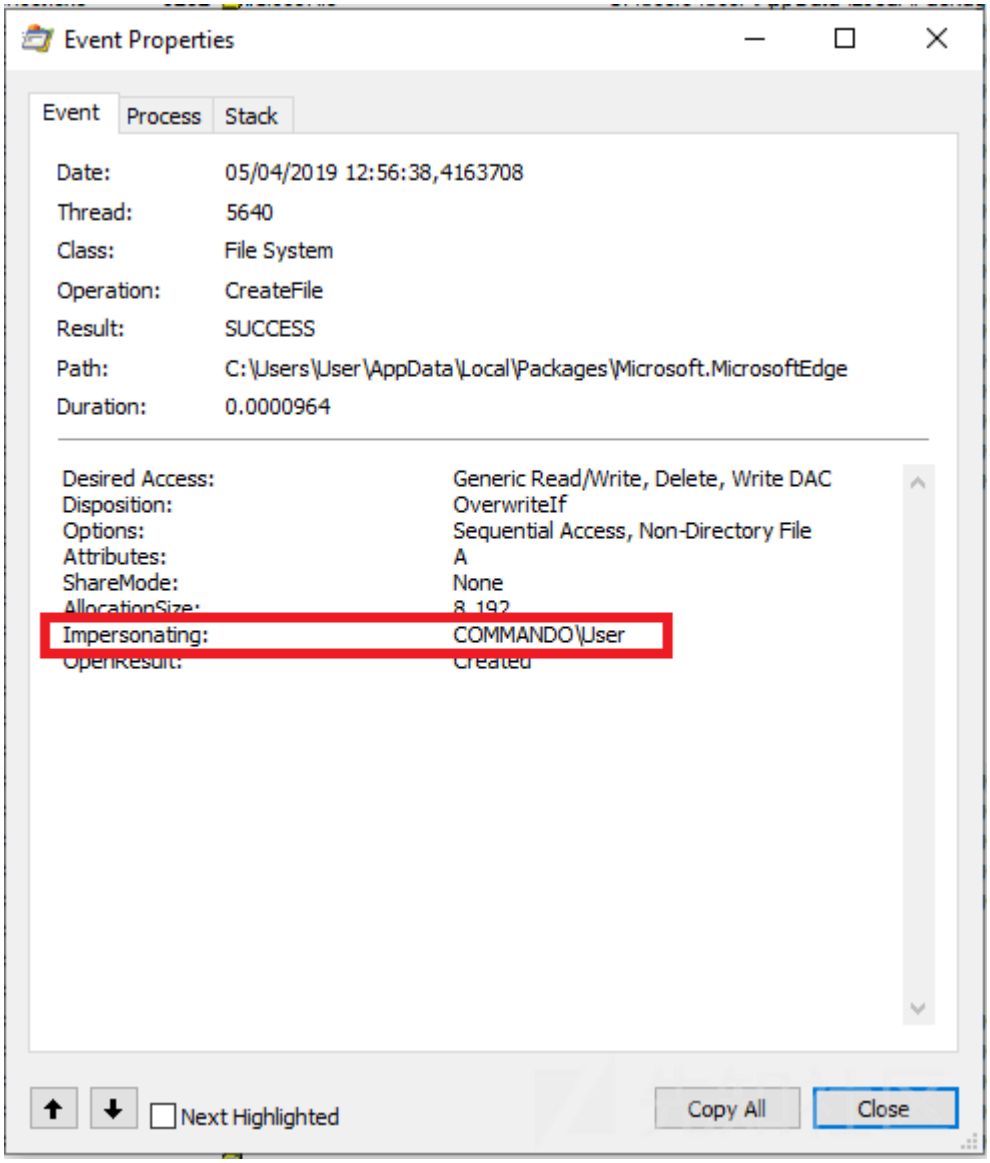
1. 检查文件权限
   - 如果文件权限不准确，修正文件权限
2. 读取文件内容
   - 如果文件内容被破坏，就删除该文件
   - 从中中复制设置模板文件来重设配置
3. 在新复制的文件上获取Exclusive Lock
4. 启动Windows APP

该过程如下图所示：





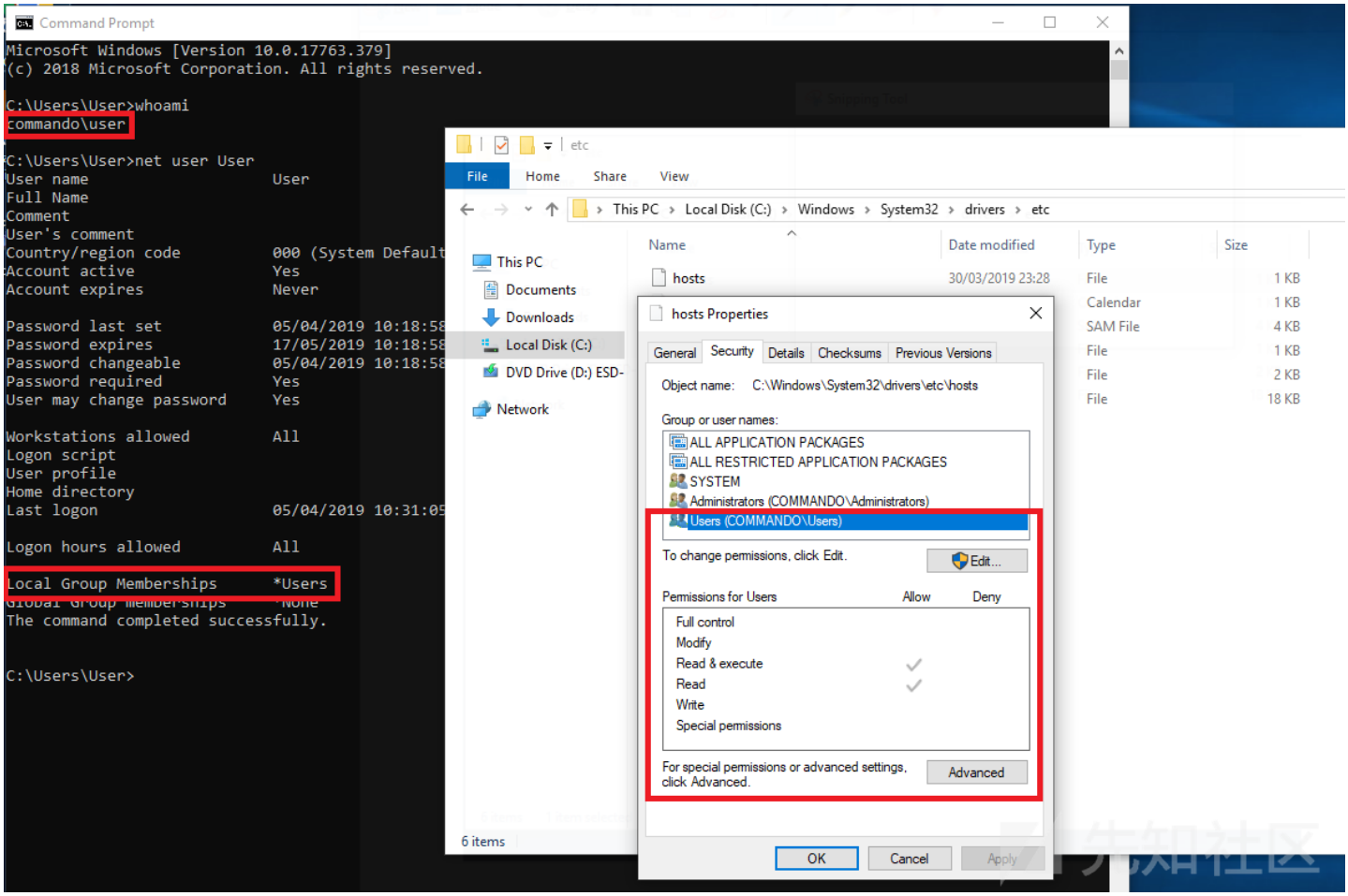
前面也提到在读取文件内容后在`SetSecurityFile`操作过程中会首先设置正确的文件权限，在本例中内容并不与正确的`settings.dat`文件对应。之后，删除该文件，复
APP。
绝大多数这些操作都是通过`impersonating`当前用户权限来执行的，这会防止滥用这些操作：



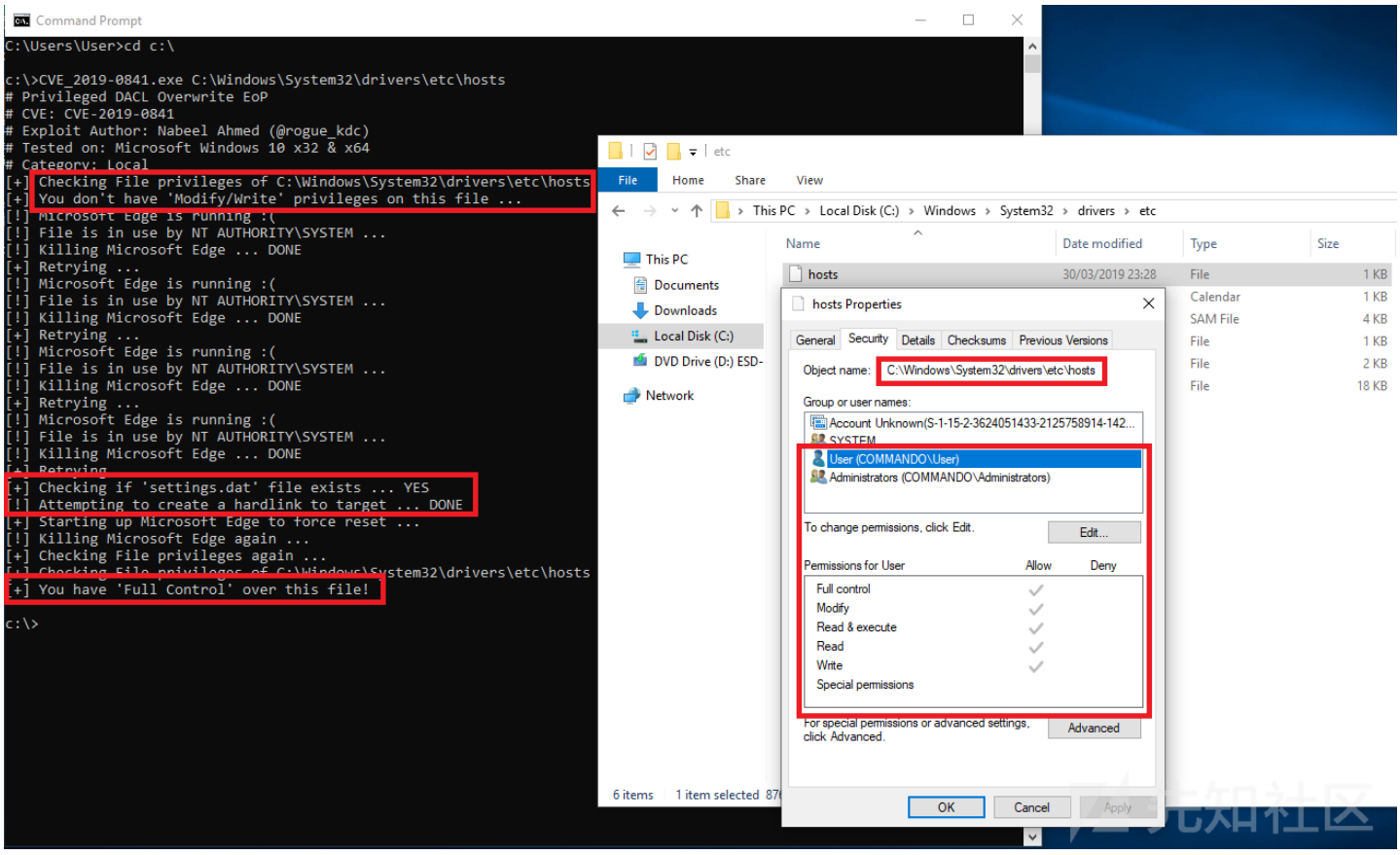
因此可以利用这一行为来对任意文件通过硬链接来设置文件权限。

漏洞利用

下面的漏洞利用过程是基于知识：设置硬链接的文件权限会改变原始文件的权限。
下面劫持位于`C:\Windows\System32\drivers\etc\hosts`的HOSTS文件。普通用户是没有该文件的修改访问权限的。



研究人员开发了漏洞利用可以自动创建硬链接并触发该漏洞，成功利用的结果如下图所示：



1. 漏洞利用首先检查目标文件是否存在，如果存在就检查其权限。研究人员使用Microsoft Edge来进行漏洞利用，它会杀掉Microsoft Edge的进程来获取`settings.dat`文件的访问权限。
2. Microsoft Edge被杀后，会检查`setting.dat`文件并删除该文件以创建到请求的目标文件的硬链接。
3. 硬链接创建后再次启动Microsoft Edge以触发漏洞。然后检查确认是否为当前用户设置完全控制权限。

研究人员同时指出一些漏洞利用所必须的条件：

- `NT AUTHORITY\SYSTEM`应该有对目标文件的完全控制权限；
- 低权限的用户或用户组应该有读写权限；
- 读和执行权限应该可以继承。

PoC

PoC代码见：https://github.com/rogue-kdc/CVE-2019-0841
Video PoC
www.youtube.com/embed/vP468ZjJ3hU
POC视频证明了使用DLL和注入恶意代码来利用Chrome Update Service来进行权限提升，这也是完整利用该漏洞的过程。
https://krbtgt.pw/dacl-permissions-overwrite-privilege-escalation-cve-2019-0841/

上一篇：Hackerone 50m-ctf... 下一篇：Hackerone 50m-ctf...
1. 0 条回复
   - 动动手指，沙发就是你的了！