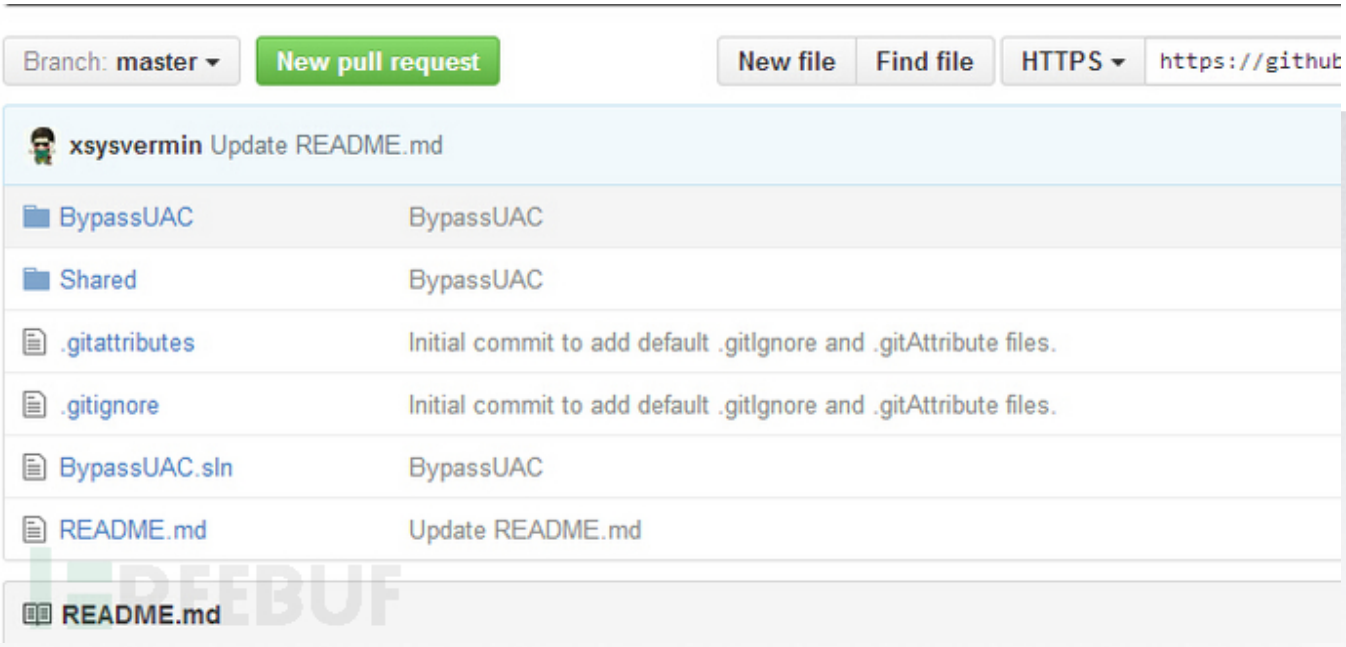

BypassUAC

BypassUAC是一款使用Windows系统内置的AutoElevate后门攻陷Windows用户帐户控制（UAC）机制的工具。

系统环境要求

1、x86-32/x64 Windows 7/8/8.1/10（然而，一些方法同样能够在服务器版本系统上工作）。

2、管理员账户，且要求UAC处于默认设置状态。

方法介绍

以命令行方式运行可执行文件：BypassUAC_x86[键值][取消]，或者BypassUAC_x64[键值][参数]。在后面的“使用举例”一节中可以查看更多信息。

其中，第一个参数是所使用方法的编号，第二个参数是运行的可选命令（包含完整路径的可执行文件名），且第二个参数可以为空—在这种情况下，程序将执行system32文件夹中提权后的cmd.exe。

键值（可以查看dbgview或类似工具的输出内容，以了解更多信息）：

1、Leo Davidson sysprep方法，该方法只能在Windows 7共Windows 8上工作，用于多个恶意软件的情况下；

2 、调整的Leo Davidson sysprep方法，该方法只能在Windows 8.1.9600系统上工作；

3 、WinNT/Pitou开发者调整的Leo Davidson方法，能够在Windows 7到Windows 10.210532之间所有系统上工作；

4、来自WinNT/Gootkit的应用程序兼容性Shim RedirectEXE方法，能够在Windows 7到Windows 8.1.9600之间的系统上工作；

5、ISecurityEditor WinNT/Simda方法，用于关闭UAC，可以在Windows 7到Windows 10.1 100136之间的系统上工作；

6、Win32/Carberp使用的Wusa方法，经过调整后该方法也能工作在Windows 8/8.1系统安全

7 、Wusa方法，调整之后可以工作于Windows 7到Windows 10.110136之间的系统上；

8 、Win32/Tilon使用的经过轻微修改的Leo Davidso方法，只能在Windows 7上工作；

9、混合方法，WinNT/Simda和Win32/Carberp+AVrf的结合方法，可以工作于Windows 7到Windows 10.110136之间的系统上；

10、混合方法，滥用appinfo.dll的白名单方式对应用程序和已知的dll文件自动提权，能够在Windows 7到Windows 10.210532之间的系统上工作；

11、WinNT/Gootkit的第二个方法，它基于从MS “Fix it” patch shim的内存补丁（副作用是会导致任意dll文件注入），能够在Windows 7到Windows 8.1.9600系统上工作；

12、Windows 10 sysprep方法，它利用了Windows 10中增加的不同dll依赖性，最高能够工作于Windows 10.2 10558系统；

13、混合方法，利用了appinfo.dll列举MMC控制台命令白名单和事件查看器（EventViewer）的非依赖性，工作于Windows 7到Windows 10rs1 1082系统上；

14、WinNT/Sirefef方法，利用appinfo.dll列举OOBE.exe白名单的方式，工作于Windows 7到Windows 10.2 10558系统上；

15、Win32/Addrop方法，该方法也用于Metasploit uacbypass模块中，工作于Windows 7到Windows 10rs1 1082系统上；

16、混合方法，与微软GWX后门配合工作，工作于Windows 7到Windows 10rs1 1082系统上。

注意事项

其中的几种方法需要进程注入，所以它们在64位上不能正常工作，此时可以使用该工具的x64版本；

1、由于Shim的限制，方法（4）在该工具的64位版本中不可用；

2、从Windows 8开始，方法（6）在wow64环境下不可用。并且，目标应用程序在Windows 10中也不存在；

3、方法（11）在x86-32版本中实现；

4、方法（13）只在x64版本中实现。

使用举例

```
BypassUAC_x86.ex 1 cmd.exe
BypassUAC_x64.ex 3 cmd.exe
```

***参考来源：github，FB小编JackFree编译，转载请注明来自FreeBuf黑客与极客（FreeBuf.com）**