MALWARE AVOIDANCE USING REDIRECTION TECHNIQUE

Rana Jumaa Surayh Al-janabi
College of Medicine, Al-Qadissiya University, Qadissiya-Iraq.

Abstract

The Windows registry is behind almost every great feature in the operating system. Image file execution options (IFEO) is assumed as useful key in registry. In spite of that, malicious software (Malware) uses this key to convert a lot of system program's paths to their malicious code using redirection technique. Actually, IFEO can be considered as a very important key that can be used beneficially or harmful to both.

In this research, redirection technique is analyzed and used to build software that employ this useful key to provide helpful service by changing malware paths to illusion paths as preventive method in order to protect computer against attack by those malware. This software is designed using assembly language and WinAsm to build friendly user interfaces.

Keywords: IFEO, Image File Execution Options, debugger, RegCreateKeyEx, RegSetValueEx, Disable system tools.

1. Introduction

The biggest threat to technological security at this point is the technology itself. Technological systems, especially newer ones, are exceedingly complex—and complexity is the worst enemy of security. This is true for a number of reasons. One is that in rush to build new systems, programmers generally ignore security or only pay attention to it at the last minute. But the other is that complex systems, especially tightly coupled systems are naturally less secure. [1]

Windows is a complex system and a very important part of it is the registry. In spite of that importance but when it comes to hacking windows, no other tool comes close to the Registry. It contains the underlying organization of the entire operating system, and its often-incomprehensible settings hold the key to countless hacks. Unfortunately, malware employ Windows registry to achieve automatic execution, destruction and propagation. They use interesting registry key called Image File Execution Options (IFEO). It provides a mechanism to always launch an executable files directly under the debugger. It is rarely useful to users but is total bliss for viruses. Worst part–modifications that viruses make there often cripple system for good even after virus itself is removed. [2,3,4]

In addition to important hints for IFEO and how to use IFEO by viruses, this research includes method to counter malware also using IFEO.

2. Very Interesting Implication for IFEO

IFEO provides a mechanism to always launch an executable directly under the debugger. This can lead to many things, including perhaps some things that it wasn't intended for, the following explains some of these things: - [5,6]

1. Although this feature is for debugging, it is really just a general mechanism of redirecting what application gets launched, which is kind of interesting.
2. It becomes very difficult to start the application _outside_ of a debugger. Usually trying to start the application outside of the debugger will just launch an instance of the debugger.
3. This can confuse whatever called Create Process. Instead of getting back the handle/process id of the debugging program, it will instead get back the handle/ process id of the debugger. Probably not what was expected.

3. IFEO from Useful Standpoint

Debugging processes are very important for drivers, applications, services on systems or to debug operating system itself such as Windows XP, Windows Vista, ..etc. Microsoft Developers network says that "There are times that you need to debug the startup code for an application, but something else is launching the application such as service or setup custom action". And in other cases, you may need to debug service itself (i.e. It is possible to start the service under debugger, just like a “normal” application. If this could be done, it

would be possible to debug the startup code of the service (For example, the service's main () function. Actually, it takes time to attach debugger to the service, and by the time when it has finally attached, the startup code has most likely been already executed. So it is too late). At first glance, it looks like it cannot be done, because services are started by a dedicated application–Service Control Manager (SCM). But fortunately and using IFEO, the operating system provides a way to intercept the attempts to launch any Win32 application, and start another application instead). This feature can be used to start the service under debugger.[5,7]

Actually, security labs say that IFEO can redirect execution of a file. For example, if you want to run AA.exe, the computer can be made to run BB.exe instead of AA.exe. This is done because IFEO has an item in the Windows registry as HKLM\ SOFTWARE\ Microsoft\ Windows NT\ CurrentVersion\ Image File Execution Options\ AA.exe that tells it to run BB.exe instead. And based on this foundation, Mcafee published an article talking about how to use IFEO to run Anti-virus instead of malware.[8,9]

To start service (or any other application) under debugger or any exe instead another, the following steps should be followed:- [10,11]

1. Start the Registry Editor: Click Start, click Run, and then type regedit.exe.
2. Locate the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ Windows NT\ Current Version\ Image File Execution Options**
3. To this hive, add the SOURCE exe as a key. For example service.exe: (Right click and select **New**, and then **Key** and name it ***service.exe***).
4. Right-click the ***service.exe*** folder and choose **New String Value** from the shortcut menu and name it (debugger).
5. In the **Value data** box, type the path of debugger for example (**c:\debugger.exe**).

Using any method to start service.exe. Debugger will start and load Service.exe.

4. IFEO from Harmful standpoint

Most malware writers have the same dream: to disable anti-virus software or system tools so the malware can run itself on a computer without any limitation. Therefore, many malware authors try many different methods to disable anti-virus software and system tools. In 2008, Virus Bullitin says that IFEO is an advanced technique which current malware in the wild makes extensive use of it. Anti-virus Killer (AV Killer) is this kind of virus that uses the IFEO method. [8, 12]

Malware utilize important fact that says Windows doesn't verify that the "debugger" is truly a debugger. It just runs the application or system program in the debugger value. Malware use several methods to attack system program or even anti-virus. First method, malicious put "illusion path "in the debugger value under system program such as "Task manager", as it explained in Fig.(1). [4]

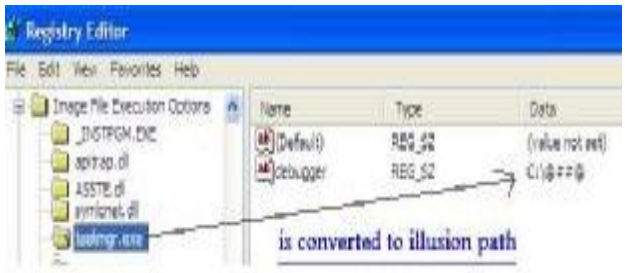

Fig. (1) : Registry editor explains that task manager is converted to illusion path.

And every time user try to run Task manager the path will not found in this case the following message will appear as explained in Fig.(2).

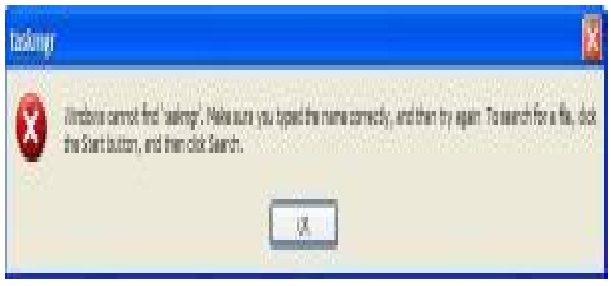

Fig. (2) : Malware converts task manager to illusion path so Windows give this massage.

Actually, significant tools are used to discover a new added registry key which is responsible for converting or disabling programs. It is Autorun from

www.systeminternals.com as illustrated in Fig. (3).

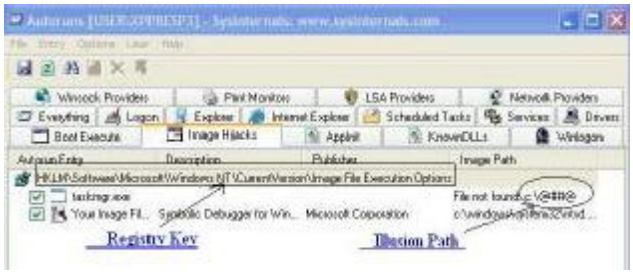

Fig. (3) : Autorun Software explains that task manager is disabled.

Second method, task manager is not converted to illusion path, it is converted to malicious path, in this case if user try to run task manger, malware will run instead as explained in Fig.(4).

Fig. (4) : Autorun Software explains that worm.exe will run instead of task manager.

And finally, antivirus software can even prevented from running by attaching executables to illusion path or even malicious file as explained in Fig.(5). If antivirus utility or system program can't start it is worth to try renaming its executable file.

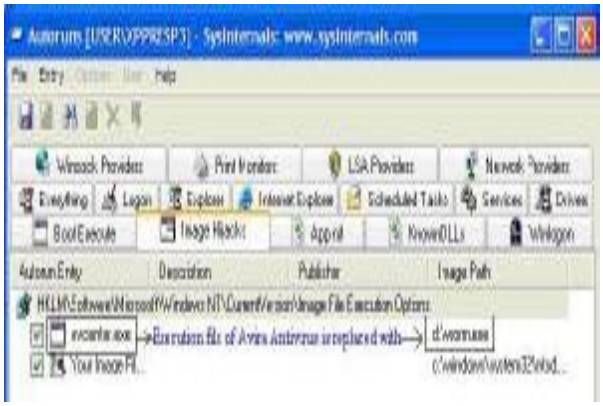

Fig. (5) : Autorun Software explains that worm.exe will run instead of Avira antivirus.

5. Tools

In this research the following tools were used:-

1. MASM32:- ASM is one step higher than machine code, and it is the lowest level language. Every program that is compiled from any language such as C^{++} or Delphi is then converted to PC ASM through compiler. PC ASM is what the CPU reads and it is quite difficult to read. However, with MASM32, it can be coded in a similar fashion to C^{++} but without the complexity and hassle of PC ASM that the processor reads. It can be downloaded from http://www.masm32.com/masmdl.htm. [13,14]
2. WinAsm:-WinAsm Studio is a free Integrated Development Environment IDE for developing 32-bit Windows using the Assembler. In fact, MASM32 is supported inherently. It can be downloaded from http://www.winasm.net.[15]
3. Autorun:-This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows user what programs are configured to run during system bootup or login, and also shows the entries in the order Windows processes them. These programs include ones in startup folder, Run, RunOnce, and other Registry keys. Autoruns comes close to the MSConfig utility in Windows XP. It can be downloaded from http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx. [16]
4. Avira:-The professional virus detection and removal application. In the end of January 2008 Avira Antivirus was rated 6.5 out of 8 in tests for detection and removal of rootkits and 71% for proactive virus detection by Anti-Malware Test Lab; both scores qualified for "gold" status, the highest award. However, it also received "poor results", the lowest grade, for infection treatment. It can be downloaded from http://www.download.com/Avira-AntiVir-Personal-Free-Antivirus/3000-2239_4-10322935.html. [17].

6. Method (Software Implementation and How to Use)

In fact, IFEO registry key is used to force a program to run under the debugger, it allows to create entries that say if application A is launched then start application B instead. While applications B is a debugger and in case

that path of B is illusion, then application A is disabled. And this is the principle of the work. [4]

This method includes the following stages:-

1. **First Stage:-** Determine malware name as shown in Fig.(6).

Fig.(6) : Avira discovers worm (newfolder.exe) in USB flash.

2. **Second Stage:-** merge (Malicious File Name(newfolder.exe)) with this path (HKLM\Software\Microsoft\Windows NT\ Current Version\ Image File Execution Options\) to become (HKLM\ Software\ Microsoft\ Windows NT\ Current Version\ Image File Execution Options\ newfolder.exe) using (Istrcat instruction).[18].
3. **Third Stage:-** Create Key and name it (Malicious File Name(newfolder.exe)) in this path (HKLM\ Software\ Microsoft\ Windows NT\ Current Version\ Image File Execution Options\) using **(RegCreatKeyEx instruction)** in MASM32 as shown in Fig. (7).[19].
4. **Forth Stage**:-Create Value and name it **(debugger)** and set this value to illusion path using **(RegSetValueEx instruction)** as shown also in figure (7) .[20].

Fig. (7) : Registry Editor explains that malware is converted to illusion path.

To understand the structure of major instructions that build our software, this is an explanation of them:-

1. RegCreateKeyEx function

Creates the specified registry key. If the key already exists, the function opens it. In Masm32, the structure of RegCreateKeyEx is the following :-[19]

Invoke RegCreateKeyEx, hkey, Ipsubkey, reserved, Ipclass, dwoptions, samDesired, IpSecurity attributes, phkResult, IpdwDisposition.

Hkey: - A handle to an open registry key. It can be one of the following predefined keys:

HKEY_CLASSES_ROOT
HKEY_CURRENT_CONFIG
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS

Ipsubkey: - The name of a subkey that this function opens or creates. The subkey specified must be a subkey of the key identified by the hKey parameter. This parameter cannot be NULL.

Reserved: - This parameter is reserved and must be zero.

Ipclass: - The user-defined class type of this key. This parameter may be ignored. This parameter can be NULL.

Dwoptions: - This parameter can be several values. One of them is REG_OPTION_NON_VOLATILE which mean this key is not volatile; this is the default. The information is stored in a file and is preserved when the system is restarted.

samDesired:- A mask that specifies the access rights for the key.

IpSecurity attributes: - A pointer to a SECURITY_ATTRIBUTES structure that determines whether the returned handle can be inherited by child processes. If lpSecurityAttributes is NULL, the handle cannot be inherited.

PhkResult:-pointer to a variable that receives a handle to the opened or created key. If the key is not one of the predefined registry keys, call the RegCloseKey function after you have finished using the handle.

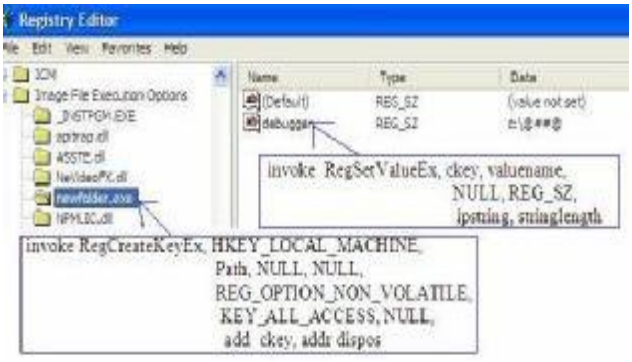

Fig. : (8) RegCreateKeyEx and RegSetValueEX instructions effecting.

IpdwDisposition:-pointer to a variable that receives one of the following disposition values.:-

REG_CREATED_NEW_KEY:-The key did not exist and was created.

REG_OPENED_EXISTING_KEY:- The key existed and was simply opened without being changed.

2. RegSetValueEx function

Sets the data and type of a specified value under a registry key. In Masm32, the structure of RegSetValueEx is the following:-[20]

Invoke RegSetValueEx, Hkey, lpValueName, Reserved, dwType, IPData, cbData

Hkey:-A handle to an open registry key. This handle is returned by the RegCreateKeyEx. It can also be one of the following predefined keys:

HKEY_CLASSES_ROOT
HKEY_CURRENT_CONFIG
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_PERFORMANCE_DATA
HKEY_USERS

lpValueName:-The name of the value to be set. If a value with this name is not already present in the key, the function adds it to the key.

Reserved:-This parameter is reserved and must be zero.

dwType:-The type of data pointed to by the lpData parameter.

IPData:-The data to be stored. For string-based types, such as REG_SZ, the string must be null-terminated. With the REG_MULTI_SZ data type, the string must be terminated with two null characters.

cbData:-The size of the information pointed to by the lpData parameter, in bytes. If the data is of type REG_SZ, REG_EXPAND_SZ, or REG_MULTI_SZ, cbData must include the size of the terminating null character or characters.In fact, these instructions effect on registry editor and Fig. (8) explain that effecting.

According to this example, programmer should define the following:-

1. path represent "Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\newfolder.exe"
2. valuename represent " debugger"
3. ipstring represent "c:\@##@"

7. Results

In fact, sometimes anti-virus discovered the name of malware, but it failed to delete malware or remove its infection from the computer. In case that user needs to move some data from that infected computer to hale computer, the user can utilize this software by entering malware name (execution name discovered by anti) in textbox and stop it before connecting any removable media that contain those data in order to prevent the execution of that malware on the hale computer, Fig.(9) explain that. This software can be run on windows XP and Vista. But on Vista, this software can be run by choosing (Run as administrator).

Fig. (9) : Preventive software that convert malware to illusion path.

If user runs newfolder.exe accidentally, windows gives the following massage as explained in Fig.(10).

Fig. (10) : Malware (newfolder.exe) is converted to illusion path.

Since Autorun tool explains Paths which added to IFEO. So, Autorun gives the following result as explained in Fig. (11)

Fig. (11) : Autorun software explains that malware (newfolder.exe) is disabled.

In fact, in case that anti-virus fails even to discover existence of these malicious codes or incase that malicious code executed before using method. This method will fail because it totally depends on two things. First is the execution file name of malicious code, second this method doesn't repair any infection in computer system but it only change malware path before it executes for this reason it is preventive method.

8. Result Discussion

This method has great significance by preventing the execution of malware and therefore system tools can't be affected unlike many other anti-virus software that delete the malware, but it can't remove their infection. In spite of that, this method can be considered as limited method for the following reasons:-

1. The names of all malware may not be determined because some are up to date. The presence of any new malware means that user must add this name to Image file execution option registry key.
2. there is a Probability that User's files with the same name of malware therefore it can not be executed although it is legitimate programs.
3. This method doesn't work with script files.

9. Conclusion

Malware use redirection technique in IFEO to attack system programs by changing their paths to malicious code causing computer system infection. In fact, the same technique can be used to convert those malware paths to illusion paths. This method can be used as useful preventive procedure because it prevents the execution of malware.

In spite of that, this method like any other protection method has its weaknesses. Since, it depends entirely on knowing the name of malware, as well as, it doesn't work with script files.

Actually, since IFEO redirection technique has weaknesses (depending on file name) so user can take benefit of this situation by renaming anti-virus or system program that is disabled by malware that use this technique.

Reference

[1] James Maguire, Securing Your PC and Your Privacy, http://www.schneier.com/news-070.html, 2008.

[2] Beijing Rising International Software Co., Windows Registry and computer security, http://www.rising-global.com/Published/InformationCenter/SecurityArticles/2007-08-09/20070809175627.htm , 2007.

[3] Preston Gralla, Windows XP Hacks, O'Reilly, 2003.

[4] Rarst, How to cleanup viruses hijacking executables, http://www.rarst.net/software/image-file-execution-options/, 2009.

[5] greggm, Inside 'Image File Execution Options' debugging, http://blogs.msdn.com/greggm/archive/2005/02/21/377663.aspx, 2005.

[6] Mithun Shanbhag, Image File Execution Options, http://www.debugtricks.com/?p=15, 2007.

[7] Oleg Starodumov, debugging startup code of services and com servers, http://www.debuginfo.com/articles/debugstartup.html, 2006.

[8] Security Labs, AV Killer Analysis Report, http://securitylabs.websense.com/content/Blogs/2826.aspx, 2007.

[9] Lokesh Kumar, Image File Execution Options, http://www.avertlabs.com/research/blog/index.php/2008/12/09/image-file-execution-options/, 2008.

[10] hzqedison, Using Image File Execution options as an Attack Vector on Windows, http://www.hzqedison.cn/blog/read.php?26, 2007.
[11] Visual Studio Developer Center, Launching the Debugger Automatically, http://msdn.microsoft.com/en-us/library/ a329t4ed(VS.71).aspx, 2009.
[12] Alisa Shevchenko, Advancing Malware techniques 2008, http://esagelab.com/files/ AlisaShevchenko-Jan09.pdf, 2009.
[13] AntonChuvakin and Cyrus Peikari, Security Warrior, O'Reilly, 2004.
[14] Baran Ornarli, Introduction to MASM32, http://www.infernodevelopment.com/articles/masm32, 2008.
[15] The winasm.net team, The x86 Assembly community and official home of WinAsm Studio and HiEditor, http://www.winasm.net/, 2007.
[16] Mark Russinovich and Bryce Cogswell, Autoruns for Windows, http://technet.microsoft.com/en-us/sysinternals/ bb963902.aspx, 2009.
[17] Wikipedia, Avira, http://en.wikipedia.org/ wiki/Avira, 2009.
[18] Iczelion, Tutorial 11: More about Dialog Box, http://win32assembly.online.fr/tut11.html.
[19] Microsoft Developer Network, RegCreateKeyEx Function, http://msdn.microsoft.com/en-us/library/ms724844 (VS.85).aspx, 2009.
[20] Microsoft Developer Network, RegSetValueEx Function, http://msdn.microsoft.com/en-us/library/ms724923 (VS.85).aspx, 2009.

الخلاصة

سجل نظام التشغيل وندوز هو السبب في الكثير من المزايا العظيمة لنظام التشغيل. خيار التنفيذ لشكل الملف من المفترض أن يكون مفتاح مفيد في السجل. بالرغم من هذا، البرامج الخبيثة تستخدم هذا المفتاح لتحويل الكثير من مسارات برامج النظام إلى شفراتها الخبيثة باستخدام تقنية إعادة التوجيه. في الحقيقة ان خيار التنفيذ لشكل الملف يعتبر مفتاح مهم جدا وممكن ان يستخدم اما بشكل مفيد أو مؤذي على حد سواء.

في هذا البحث، تم تحليل تقنية اعادة التوجيه واستخدمت في بناء برنامج يستطيع توظيف هذا المفتاح لتقديم خدمة مفيدة من خلال تغيير مسار البرامج الخبيثة الى مسار وهمي كاجراء وقائي لحماية الكومبيوتر من الهجوم من قبل تلك البرامج الخبيثة. تم تصميم هذا البرنامج باستخدام لغة التجميع والـ(WinAsm) لبناء واجهات مستخدم صديقة.