Messenger Attack (Problems and Solutions)

Rana Jumaa Surayh Al-janabi
Al-Qadesya University- College of Medicine

Abstract

For years, people think that the major threat to various companies' computer networks doesn't come from outside hackers,but from internal(often disgruntled) employees.

However, a new study disputes that, saying that outside hack attacks are the largest threat. In fact, the outside hackers use the ability of messenger to not only transfer text messages,but also to files transferring. Consequently, messengers can transfer worms and other malicious software (malware).

This research includes many practical methods and tricks to attack yahoo messenger by sending executable files that are compressed and masqueraded, that files are responsible for converting Yahoo! Music and other options to malicious web site, and also it is possible to insert messenger into infinite loop, delete messenger after forcing it to close, or convert its path into malicious program path, insuring that done even after restart computer. And also it contains protection methods for that attack which are responsible for disabling system program such as (task manager, system restore, system configuration utility…etc) to ensure that the user couldn't remove the program that caused attack.

Finally in this research, software is designed to break that attack by enabling system tools and that will lead to facilitate the task of ending attack. Actually, this software is considered as a solution to widespread problem caused by many malware.

1. Introduction

Our world has become interconnected in ways not previously imaginable. Real-time digital communication (instant messages (IM)) is one of that ways. IM is a form of real-time communication between two or more people based on typed text; its services fill the niche between a phone call and an email. While email is ideal for non-synchronized communications, IM offers the ability to identify people who are online at the same time and exchange information in near real-time. It can be a much more efficient way to communicate with others than sending multiple e-mails back and forth. But in fact, that communication relies in large part on our ability to protect the networks that create those connections. Unfortunately, and despite the best efforts of network security managers, the last five years have seen hackers and criminals become increasingly effective at compromising these networks, as they have quickly developed new and ever more malicious threats to network security. These newly created threats have been so successful in large part because most people have no idea how these new network security attacks work, and have only a vague conception that these new threats even exist.[9,10]

In this paper, collection of attack methods using instant messages are practically discussed, how to diagnostic and (prevent or remedy) that type of risks.

System Tools targeted by Malware Writers

In reviewing many security articles about malware characteristics, it's noticed that the most of them use multi-component threats (attack and actions in support of this attack). Recently, Kaspersky, MacAfee, Microsoft and threat expert publish several malware that use many methods to infect computer system such as (Trojan-Downloader.Win32.Agent.tuc,Virus. Win32. VB.dl,Virus.Win32.AutoRun.ah, Worm: Win32/ Autorun.AR, Worm:Win32/Hary.A, Generic Dropper). Actually, in spite of multiplicity of these methods and their targets by those malware, they partly share in scheme of attack protection and ensure its continuation by disabling system tools.[12,13,14,16,17,18,24]

System tools are really important since it can be used to return computer to its previous healthy situation. For instance, The Task Manager is targeting, because it's such a vital tool in the Windows world. Hackers and malware writers have been targeting security applications such as anti-virus and firewalls for years, since disabling protections will leave a target wide open for exploitation. But the Task Manager is more than a security tool; it's an administrative tool that allows users and administrators to control the entire Windows environment. And, in some cases the malware can be quite stuck and virtually impossible to extricate from the system. In fact, user can employ system restore instead of scanning, identifying and removing the threat. This is truly hard, so user could just go back in time to a point before the computer was compromised to avoid the site or application that infected the computer.[15]

Finally, System tools can be considered as really valuable means that should be protected because if they are breached, the whole system becomes easy to attack.

2. Tools

In this research, the following tools are used:-

1. Batch files: - is a text file containing a series of commands intended to be executed by the command interpreter. When a batch file is run, the shell program (usually COMMAND.COM or cmd.exe reads the file and executes its commands, normally line-by-line. Batch files are useful for running a sequence of executables automatically.[25]
2. B2Econverter (Batch to Execution file converter) :- converts batch-script files to EXE program. An .EXE file is much harder to casually reverse-engineer, so this could be a way to conceal a particular batch file's operations from an end user. Content of batch file will be encrypted and protected from changes.[2,6]
3. Software Implementation (Problem and Solution)

In the following stages, three files are designed (service.bat, protection.bat and setup.bat) that caused attack (problem) and converted into exe form, where service.bat attack yahoo messenger while protection.bat protect him. And finally, setup.bat will run previous two files, hide, load them into system32 and ensure their run each time user logs on, as well as, how build software that find (solution) to this problem by (enabling system program):-

4.1. Malicious batch file creation stage:-

Batch file (service.bat) can do **one** of the following situations] :- [5,19,20,21]

4.1.A. Changing registry key to the following :- these changes convert Yahoo!

Music and other options to malicious web sites

HKCU\Software\Yahoo\Pager\View\YMSGR_buzz\content url

HKCU\Software\Yahoo\Pager\View\YMSGR_Games\content url

HKCU\Software\Yahoo\Pager\View\YMSGR_Headline\content url

HKCU\Software\Yahoo\Pager\View\YMSGR_Lanchcast\content url

HKCU\Software\Yahoo\Pager\View\YMSGR_Sport\content url

HKCU\Software\Yahoo\Pager\View\YMSGR_Weather\content url

Content URL can be set to any malicious web site using (reg add instruction).

4.1.B. keeps opening copies of itself, messenger continuing until system crash and that file take form of messenger. This may done using (Goto trap , delete real messenger and put that faking one).

In this case, the batch file and yahoo messenger surely entered into infinite loop. [4, 7]

4.1.C. Forcing messenger to close using (taskkill to force messenger to close, Echo off to prevent Batch file from showing itself, delete /f to force messenger to delete.[4,7]

4.1.D. Converting yahoo messenger path into malicious program path

HKLM\Software\Microsoft\Windowsnt\Currentversion\Image file execution options\ypager. exe\Debugger= malicious program path such as c:\windows\ trojan. exe, Figure (1). [8,22]

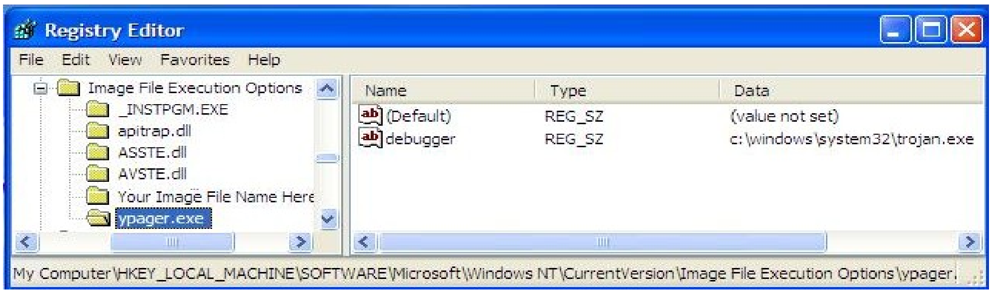


Image File Execution Options
_INSTPGM.EXE
apitrap.dll
ASSTE.dll
AVSTE.dll
Your Image File Name Here
ypager.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
debugger	REG_SZ	c:\windows\system32\trojan.exe

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ypager.

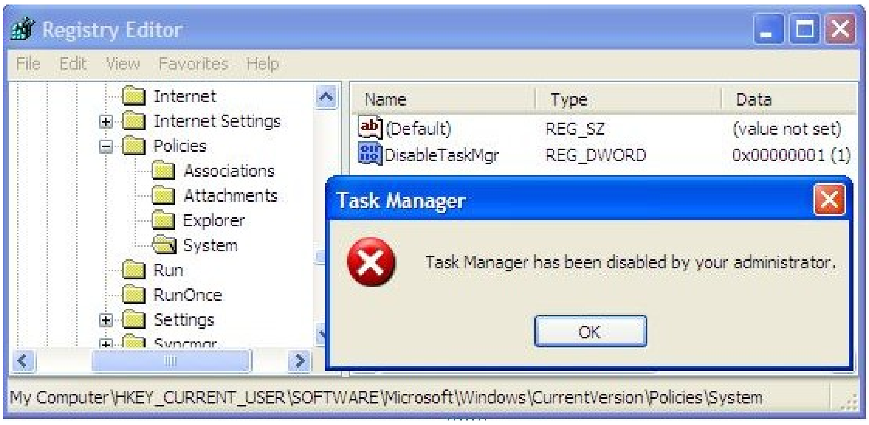
Figure (1):- Redirecting the path of yahoo Messenger

4.2. Malicious batch file protection stage:- it includes building another program (protection.bat)to protect malicious program by modifying registry to disable system tools (registry editor, folder options, system configuration, task manager and system restore). Designer can use one of the following sitiuations :-

4.2.A. The following modifications give this message (X has been disabled by your administrator). Where X either task manager, registry tools, or System restore.

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools=1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr=1
HKLM\SOFTWARE\Policies\Microsoft\WindowsNT\SystemRestore\DisableSR = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\nofolderoptions=1

To make these modifications, researchers use (reg add instruction) to add system key and set Disable Registry Tools, Disable Taskmgr……… etc to one, Figure(2). [1, 12, 13, 14, 19, 21, 23].



Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableTaskMgr	REG_DWORD	0x00000001 (1)

Task Manager has been disabled by your administrator.

My Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Figure (2):- registry value that responsible for disable task manager and message that appeared when user try to run it.

In case that, NoFolderOptions is set to one, it gives the following result as shown in figure (3)

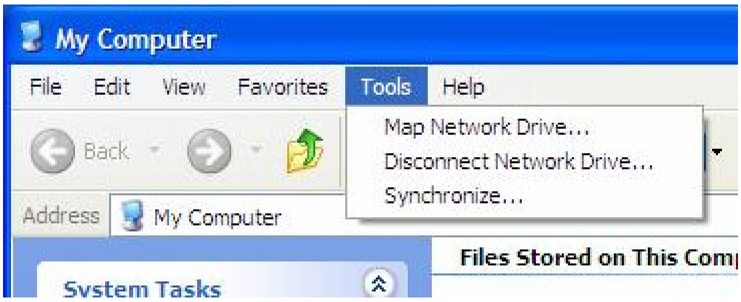
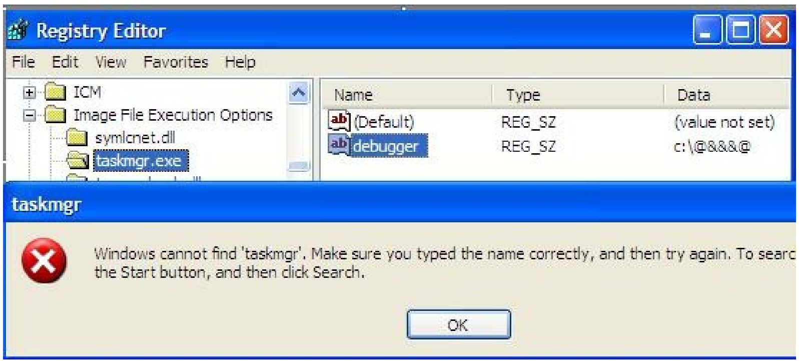


Figure (3):- FolderOption from is removed from tools

In fact, this problem is caused by several worms, viruses and other malicious programs, to solve this problem same registry value that mentioned above should set to zero.

4.2.B. While the following Modifications give this message (Windows cannot find (file name), make sure you typed the name correctly ...etc.), Figure(4):- [8,19,21,22]

For example, HKLM\ Software\ Microsoft\ Windows nt \Currentversion\Image file execution options\taskmgr.exe\Debugger=c:\@ &&&@ (Illusion path)



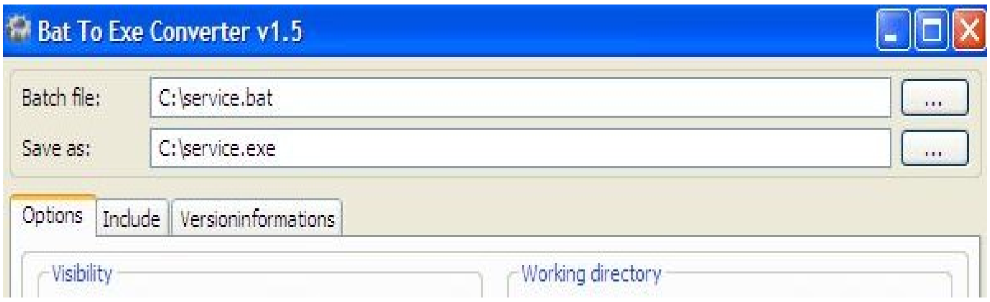
Name	Type	Data
(Default)	REG_SZ	(value not set)
debugger	REG_SZ	c:\@&&&@

Windows cannot find 'taskmgr'. Make sure you typed the name correctly, and then try again. To searc the Start button, and then click Search.

Figure (4):- Disabling Task manager by redirecting its path to an illusion path

The same manner can be applied to MsConfig.exe, RegEdit.exe and rstrui.exe to solve this problem is either by using (reg delete instruction to delete key that has been created by virus) or simply changing file name that windows can't find it to another name.

4.3. Batch to execution file converting stage:- in this stage, the previous programs in stage one and two are converted into (exe) file to protect it from reverse engineering as illustrated in figure (5). [6]



Batch file: C:\service.bat

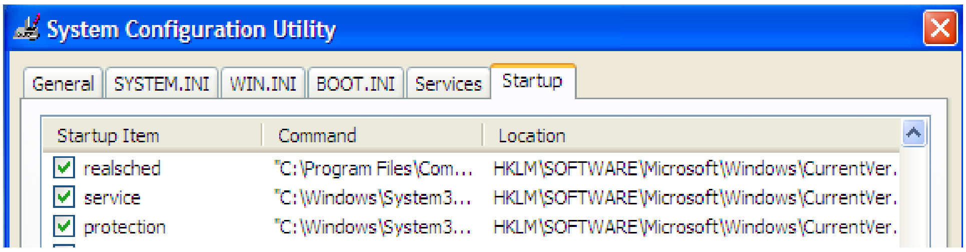
Save as: C:\service.exe

Figure (5) :- Bat to exe converter interface

4.4. Setup file designed stage:- It includes creating a new file (setup.exe) to run and add (protection.exe, service.exe) from previous stage to Run key which causes these files run each time that a user logs on:- [5].

HKLM \SOFTWARE\Microsoft\ Windows\ CurrentVersion\Run

(service.exe) are responsible for messenger attack and (protection.exe) protect that attack by disabling system tools. In case that designer doesn't disable system configuration utility user can see these exe files in system configuration utility as shown in Figure (6)

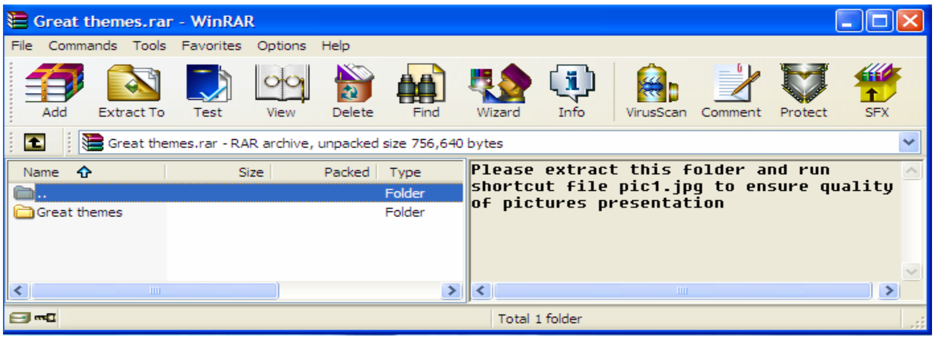


Startup Item	Command	Location
☑ realsched	"C:\Program Files\Com...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.
☑ service	"C:\Windows\System3...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.
☑ protection	"C:\Windows\System3...	HKLM\SOFTWARE\Microsoft\Windows\CurrentVer.

Figure (6):- Malicious program at start up

4.5. Masquerading stage:- execution file (setup, protection and service) are placed together into folder, and rename them into pic1.jpg, pic2.jpg and pic3.jpg respectively to ensure that receiver doesn't doubt these files may cause any kind of damage, after that make shortcut to pic1.jpg , change its target, and compressed that folder. In fact, shortcut pic1.jpg is only one file can be run as explained in figure (7).[3]

After extracting the compressed folder, the following four image files will appeared. If Receiver tries to run any of original file, it doesn't work, only shortcut file (pic1.jpg) can work. These files are illustrated in figure (8):-


Great themes.rar - WinRAR
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX

Great themes.rar - RAR archive, unpacked size 756,640 bytes

Name	Size	Packed	Type
..			Folder
Great themes			Folder

```
Please extract this folder and run
shortcut file pic1.jpg to ensure quality
of pictures presentation
```

Total 1 folder

Figure (7):- Masquerading compressed folder

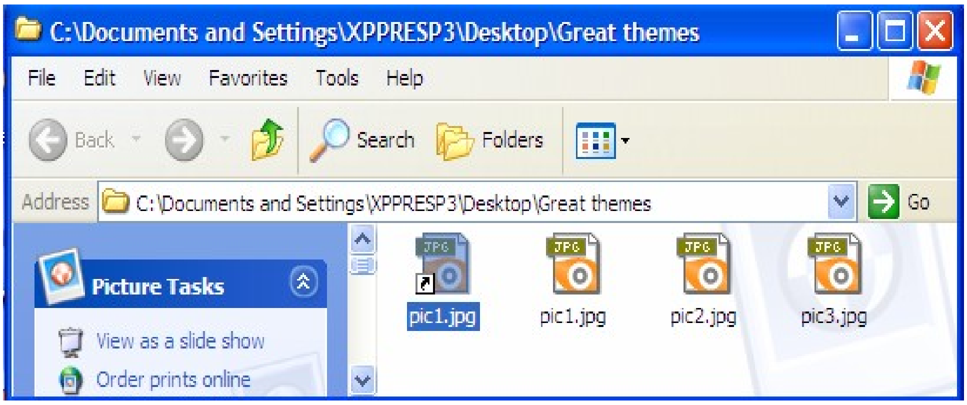

C:\Documents and Settings\XPPRESP3\Desktop\Great themes
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\XPPRESP3\Desktop\Great themes Go
Picture Tasks
View as a slide show
Order prints online
JPG
pic1.jpg
pic1.jpg
pic2.jpg
pic3.jpg

Figure (8):- Content of Extract folder (Great themes)

In fact, to explain stages very clearly, figure (9) represent messenger attack processes and way of its ending:-

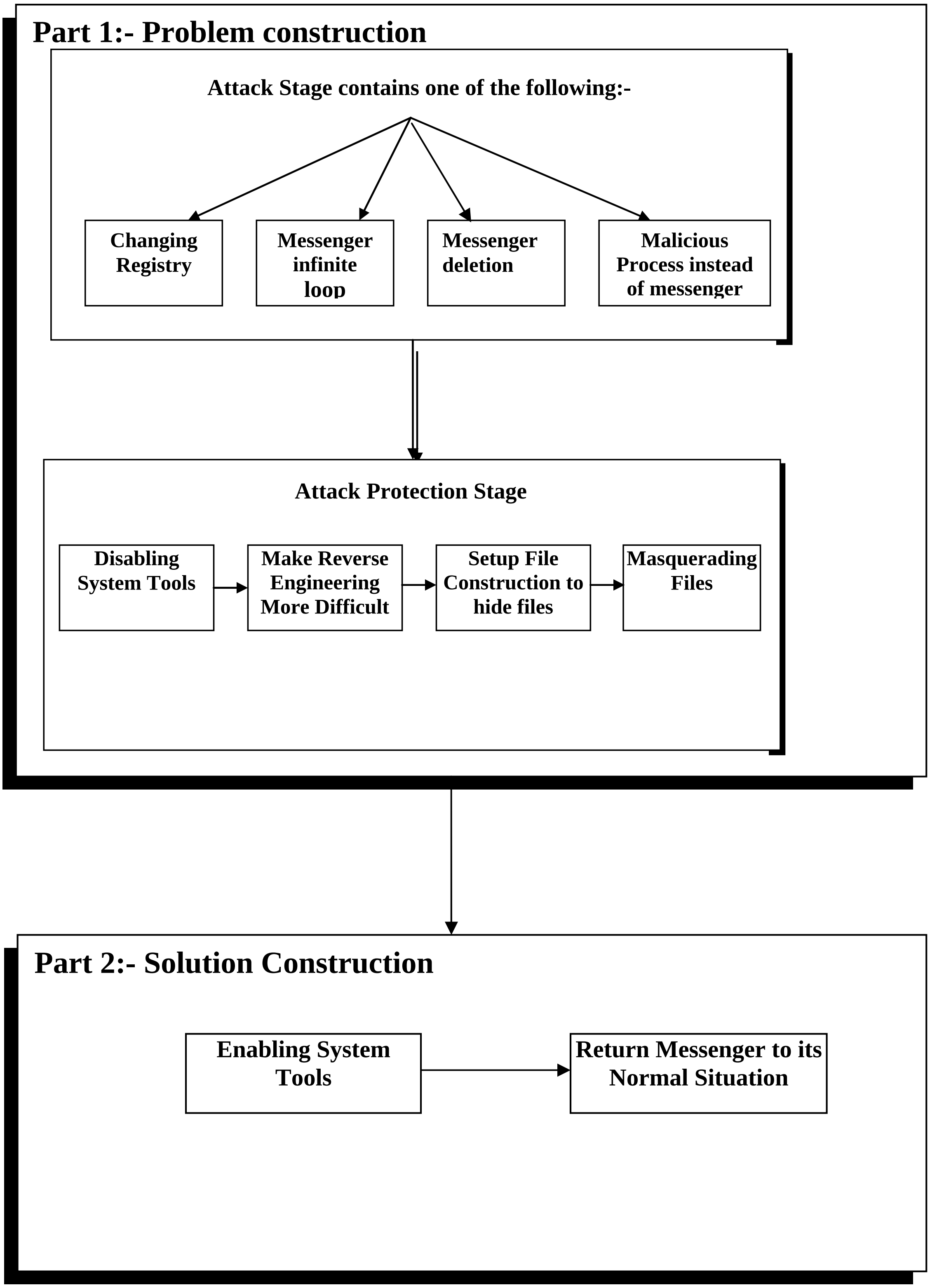

Part 1:- Problem construction
Attack Stage contains one of the following:-
Changing Registry
Messenger infinite loop
Messenger deletion
Malicious Process instead of messenger
Attack Protection Stage
Disabling System Tools
Make Reverse Engineering More Difficult
Setup File Construction to hide files
Masquerading Files
Part 2:- Solution Construction
Enabling System Tools
Return Messenger to its Normal Situation

Figure (9):- Practical methods to attack yahoo messenger and how encounter these methods

Of course, user may not be able to return messenger to its normal situation in all cases , cause removing threat can be considered as impossible in some cases.

4. Results

In case that receiver run the .jpg shortcut file, all other files will be renamed and converted from jpg into exe form, transferred to system32, hide, run them and disable all tools (task manager, folder options, system configuration utility, registry tools and system restore) through which receiver can return computer to previous situation. Actually, (protection.exe) does that because it is probable for experts to remove malicious program (service.exe) using the system tools without any external tools. So protection.exe disable task manger because manager may end malicious process. Possibly, advanced users can use folder options to show malicious hidden files and remove them, can run msconfig.exe to stop the Malicious program from auto startup ,can use registry tools to manually remove all that harmful previous changes and remove malicious file or can use system restore to undo harmful changes but it can't because all of them are disabled by (protection.exe).

In fact, many Anti Virus product delete that malicious programs but doesn't remove their infections and to solve those problems that are caused by several malware such as (Worm, Trojan, virus,….etc), it should be determined the type of massage that appeared when user try to run one of system tools (X has been disabled by your administrator or windows couldn't find….etc). In administrator massage case, registry can be fixed using (reg add instruction) to set the same registry key value that mentioned previously in (4.2.A) to zero.

In second message case, the easiest way to resolve that problem is by changing file name of any system tools that couldn't run, for instance, (msconfig.exe) to (msconfig1.exe) as illustrated in figure (10) .

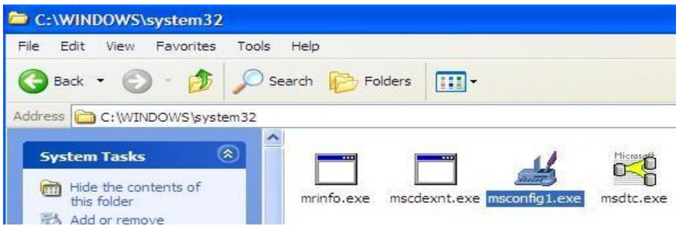


Figure (10):- Changing name in second case will solve the problem.

5. Conclusion

In fact, prevention is better than cure, so user should not trust any shortcut file even jpg file because its target may be changed. But in case that infection is done, type of message determine the type of registry modification. And according to registry modification, remedy is decided. Always, remedy is divided into two parts. First, by destroy protection to attacker program, second return messenger to its normal situation (removing threat).But in some cases, threat can be impossible to extricate from the system.

Reference

1. Aaron Faloon, Win32/Sadra.A, http://www.ca.com/us/securityadvisor/virusinfo/virus.aspx?id=77094 , 2009.
2. Abyss media company, Quick Batch File Compiler, http://www.abyssmedia.com , 2009.
3. Ankur Gandhi, How to convert .exe to .jpg, http:// www. hackingethics. com/ blog/2008/07/22/how-to-convert-exe-files-to-jpg , 2008.
4. Amanda Morin, How to write a batch file, http:// www. ehow. Com /how _2277553_write-batch-file.html? ref= fuel&utm_source=yahoo&utm_medium=ssp&utm_campaign=yssp_art , 2009.
5. Derrrick J. Farmer , A windows Registry Quick-Reference for the everyday Examiner,http://www.forensicfocus.com/downloads/windows-registry-quick-reference.pdf , 2009.
6. Fatih Kodak, Bat To Exe Converter 1.5, http://www.goloads.com/program.php?ID=56435, 2009.

Gail Allinson, Batch files 101, http://tips.oncomputers.info/archives2003/0305/2003-may-04.htm , 2003.

7. 8.Greggm, Inside 'Image File Execution Options' debugging, http:// blogs. msdn. com/greggm/archive/2005/02/21/377663.aspx , 2005.
8. Gunter Ollmann, Securing Against the Threat of Instant Messengers, http:// www.windowsecurity.com/whitepapers/Instant-Messenger- Security.html, 2006.
9. IT Security Editors, Network Security Threats, http:// www. itsecurity. com/ features/network-security-threats-011707, 2007.
10. *Jason Bruce*, THE CHALLENGE OF DETECTING AND REMOVING INSTALLED THREATS, http://www. sophos.com/security/technical-papers/ detecting-and-removing.pdf, 2006.
11. Kaspersky Lab, Trojan-Downloader.Win32.Agent.tuc, http://www.viruslist.com/en/virusesdescribed?chapter=152540538,jun , 2008.
12. Kaspersky Lab, Virus.Win32.AutoRun.ah, http://www.viruslist.com/en/viruses/encyclopedia?virusid=160221, 2007.
13. Kaspersky Lab, Virus.Win32.VB.dl, http://www.viruslist.com/en/viruses/encyclopedia?virusid=155837, 2007.
14. Larry Walsh, Windows Task Manager Targeted by Malware Writers, http://blogs.channelinsider.com/secure_channel/content/windows_security/windows_task_manager_targeted_by_malware_writers.html, September 02, 2009.
15. Mcafee, Virus Profile: Generic Dropper!9fe0af39e1f9, http://home.mcafee.com/VirusInfo/VirusProfile.aspx?key=189271#, 2009.

Microsoft, Worm:Win32/Autorun.AR , http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3AWin32%2FAutorun.AR, Sep 24, 2008.

16. Microsoft, Worm: Win32/ Hary. A!autorun, http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3AWin32%2FHary.A!autorun, Jul 11, 2007.
17. Preston Gralla, Windows XP Hacks, O'Reilly, 2003.
18. Rahul Mohandas, Hacking the Malware-A reverse-engineer's analysis , http://rahulmohandas.blogspot.com/ , 2006.
19. Robbie Allen and Preston Gralla, Windows XP Cookbook, O'Reilly, 2005.
20. Sefo, Image File Execution Options, http://www.osix.net/modules/article/?id=781 ,2006.
21. Spyware Detector, Worm.Anilogo.b Technical Details, http://www.spywaredetector.net/spyware_encyclopedia/Worm.Anilogo.b.htm , 2008.
22. Threat expert, submission summary, http://www.threatexpert.com/report.aspx?uid=84d56255-2f58-4d49-976b-0a4d4038a9ad, 2008.
23. Wikipedia, Batch file, http://en.wikipedia.org/wiki/Batch_file , 2009.

الخلاصة

لسنوات ، يعتقد الناس إن التهديد الرئيسي لمختلف شركات الشبكات الحاسوبية لا يأتي من القراصنة الخارجيين، ولكن من الموظفين الساخطين من الداخل . ومع ذلك ، أظهرت دراسة جديدة إن هجمات الاختراق الخارجية هي الأكثر تهديداً .في الحقيقة،استخدم القراصنة الخارجيين قدرة المرسل ليس فقط لنقل الرسائل النصية ، وإنما أيضا لنقل الملفات. ونتيجة لذلك ، أصبح بالا مكان نقل الديدان وغيرها من البرامج الضارة عن طريق المرسل.

هذا البحث يتضمن العديد من الطرق العملية والخدع للهجوم على مرسل الياهو من خلال إرسال ملفات تنفيذية مضغوطة ومتنكرة وهذه الملفات مسؤولة عن تحويل موقع موسيقى الياهو وبقية الاختيارات الى مواقع خبيثة ، وأيضا من الممكن إدخال المرسل في تكرار غير منتهي أو من الممكن حذفه بعد إجباره على الإغلاق أو تحويل مساره إلى مسار يحتوي على برنامج ضار وضمان حدوث هذا حتى بعد إعادة تشغيل الكومبيوتر.و أيضا يحتوي على طرق لحماية الهجوم والتي تكون مسؤولة عن تعطيل برامج النظام مثل (مدير المهام ،استعادة النظام،أدوات تهيئة النظام ...... الخ)وذلك لضمان عدم قدرة المستخدم على حذف البرنامج المسبب للهجوم .

أخيرا في هذا البحث ، تم تصميم برنامج لكسر هذا الهجوم من خلال تفعيل برامج النظام وهذا بدوره سوف يسهل مهمة إنهاء الهجوم.وحقيقة هذا البرنامج يعتبر كحل لمشكلة عامة متسببة من قبل الكثير من البرامج الخبيثة .