Malware Analysis for Fun and Profit

TABLE OF CONTENTS

Introduction

In the current IT environment, where everything is getting computerized, malware posses the biggest threat to the computer users on the internet today. Malware also represents a significant challenge to the security experts as malware author's uses new techniques to hide the presence of malware in the systems. Malware and other potentially unwanted software might have significant impact on users's security, reliability and privacy [1].

Initially when a Malware were developed their main goal is to disrupt service and to propagate further. But now their goal is getting changed from disrupting service to financial gain. Recent malware are designed to steal sensitive information such as username, passwords, credit card numbers, social security numbers, pin codes.

This white paper will help the newbie users how to do malware analysis. This paper will serve as a guideline for the reader to perform malware analysis by providing definitions, tools used and real time examples, to the reader with enough information to successfully perform malware analysis. After reading this paper newbie can kick off their professional as a malware analyst.

What is Malware

Malware (malicious code) are software programs that are built or designed to cause damage to you computer system or interrupt the normal computing activity. Virus, worm, Trojan horse, Keyloggers, spyware, adware, bots, rootkits etc are all the different types of malware.

In 2009, social networking sites such as Facebook, Twitter, orkut, hi5 etc have became a primary target for hackers. [4]

Types of Malware

I will only cover the most common malware.

Virus

Virus are the software programs that copies itself and infect a PC spreading from one file to another and then from one computer to another when the files are shared on the network without the permission or knowledge of the user. USB is also a very common worm of spreading Malwares.

Worms

Worms is again a malicious code like virus but have a greater potential to cause huge damage. Worm spread from one computer to another computer but unlink a virus they don't need human action to perform. They are self propagating and self replicating.

Keyloggers

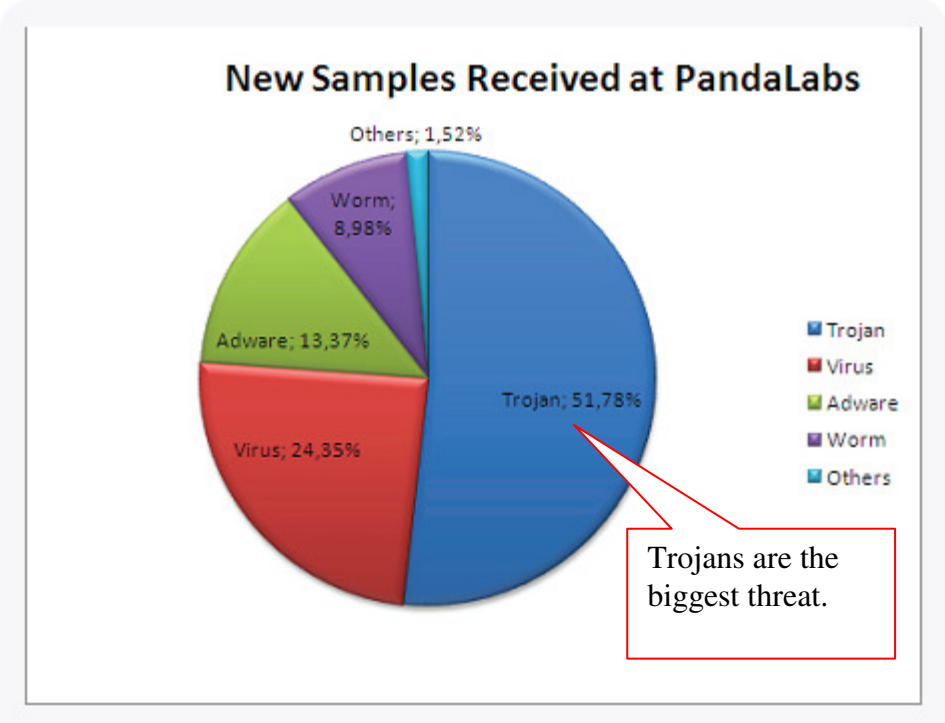
Keyloggers are the software programs that records all the key strokes typed by the users. There are two type of keylogger available, Software keylogger and hardware keylogger.

Trojans Horse

Trojans horse are the software that at first glass will appear to perform a useful software but will actually cause damage to your system once they are install on your computer system. Trojans horse will normally create a backdoor on your computer system by opening a specific port to give malicious users access to your system.

Backdoors

A piece of software that opens a port on your computer system secretly that allows malicious user to access your system remotely.



Trojans continue to rank as the weapon of choice of cyber-criminals, given that most of their revenue comes through identity theft or stolen bank and credit card details. As such, Trojans accounted for 52% of all malware created. The next category is the viruses, which accounts over 24.35%. [5]

CodeRed, a blended threat, launched DoS attacks, defaced Web servers, and its variant, CodeRed II, left Trojan horses behind for later execution. CodeRed was processed in memory — not on a hard disk — allowing it to slip past some anti-virus products. Computer Economics has estimated the worldwide cost of CodeRed at $2.62 billion dollars. [2]

Types of Malware Analysis

There are two types of malware analysis are performed by the security experts: code (static) analysis and behavioral (dynamic) analysis.

Although both of the above analysis will give you a very clear picture about the working of the malware but tools, time and skills required to perform the analysis are very different.

In this white paper I will only cover how to do behavioral analysis of the malware. I am going to write a second paper on Malware analysis soon and will cover the code analysis.

Behavioral Analysis

Behavioral analysis is a method where a behavior of malware is monitored upon its execution in a sandbox environment. The behavioral is being monitored such as creation or deletion of process, adding and deleting entries in the register, whether malware is connecting to a remote server, added itself in auto-run, monitoring Network traffic etc.

This technique is comparatively easy to code analysis where the source code of malware is analysis obtained using a technique called reverse engineering.

Code Analysis

Code Analysis is a method in which the actual code of the malware is examined by reverse engineering the malicious executable. The approach gives us a better understanding of the malware functions.

Tools used

Well there are lots of open source tools that are available on internet. I have mentioned the most used tools used for behavior analysis. As mentioned above, I will write a separate paper on code analysis and will also mentioned the tool used in code analysis.

Sysinternals Tools
Link: http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Process Explorer: Sysinternal tool that find out what files, registry keys and other objects have open, which DLL's have been loaded.

Tcp View: Again comes with sysinternal and list all the TCP and UDP endpoints on your system.

ProcMon: tool that shows file system, registry and process activity in a real time.

Auto run: Shows you what programs are configured to run during system bootup or login.

Rootkit Revealer: Advance rootkit detection utility and reveals the presence of a both user-mod and kernel-mode rootkit.

Strings: shows you the ASCII strings inside the executables.

Wire shark: Wireshark will allows you to capture the network traffic that is going in and out from your PC.

Regshot: Regshot will allow you to take a snapshot of the registry before and after a malware execution.

Hfind: Application that will scan for the disk for hidden files.
http://www.foundstone.com/us/resources-free-tools.asp

VMWare: VMware is powerful virtualization software that will allow you to run multiple Operating system simultaneously on one workstation.
www.vmware.com

Resource hacker: tool to view, modify, rename, add, delete and extract resources in 32bit Windows executables and resource files

Winalysis: Tool that will allow to take a snapshot of a computer's configuration and then monitor for changes to files, the registry, users, local and global groups, rights policy, services, the scheduler, volumes, shares.

Snapshots in Test Environment

I will analyse a malware in a sandbox environment as it is always recommended. For this I will used VMware. VMware is an application that allows you to run multiple operating systems on a single computer. The operating System that is running on the VMware, I will call it as Guest Operating System. I will provide temporary internet connection to the Guest Operating system as malware may try to communicate with remote server.

Creating a snapshot of the baseline

Step 1) Taking a snapshot of the registry

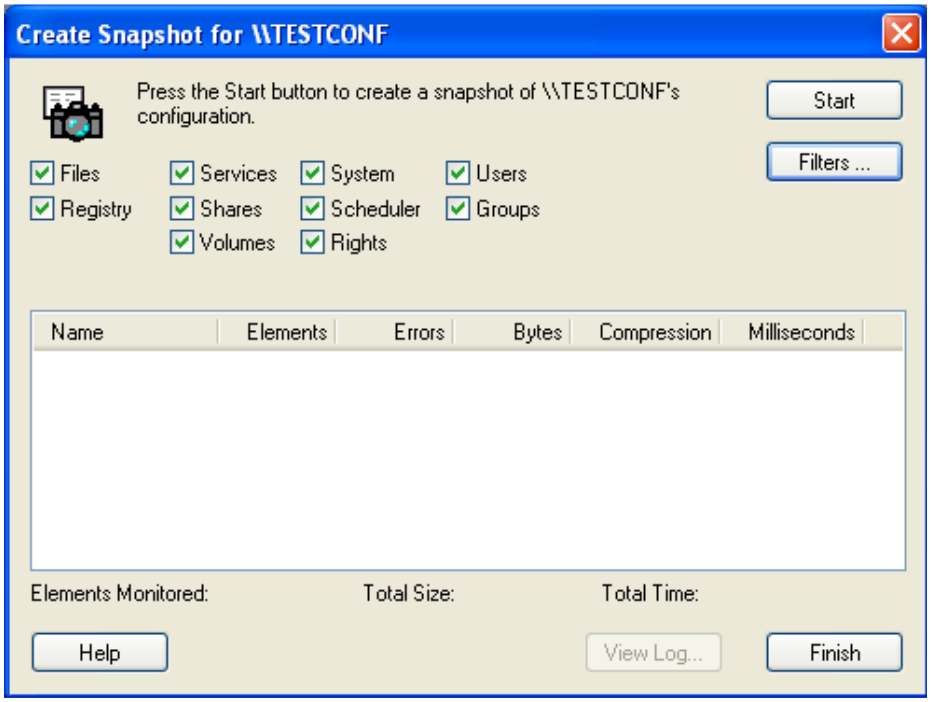


Figure 1

Step 2) Taking a snapshot of the running process

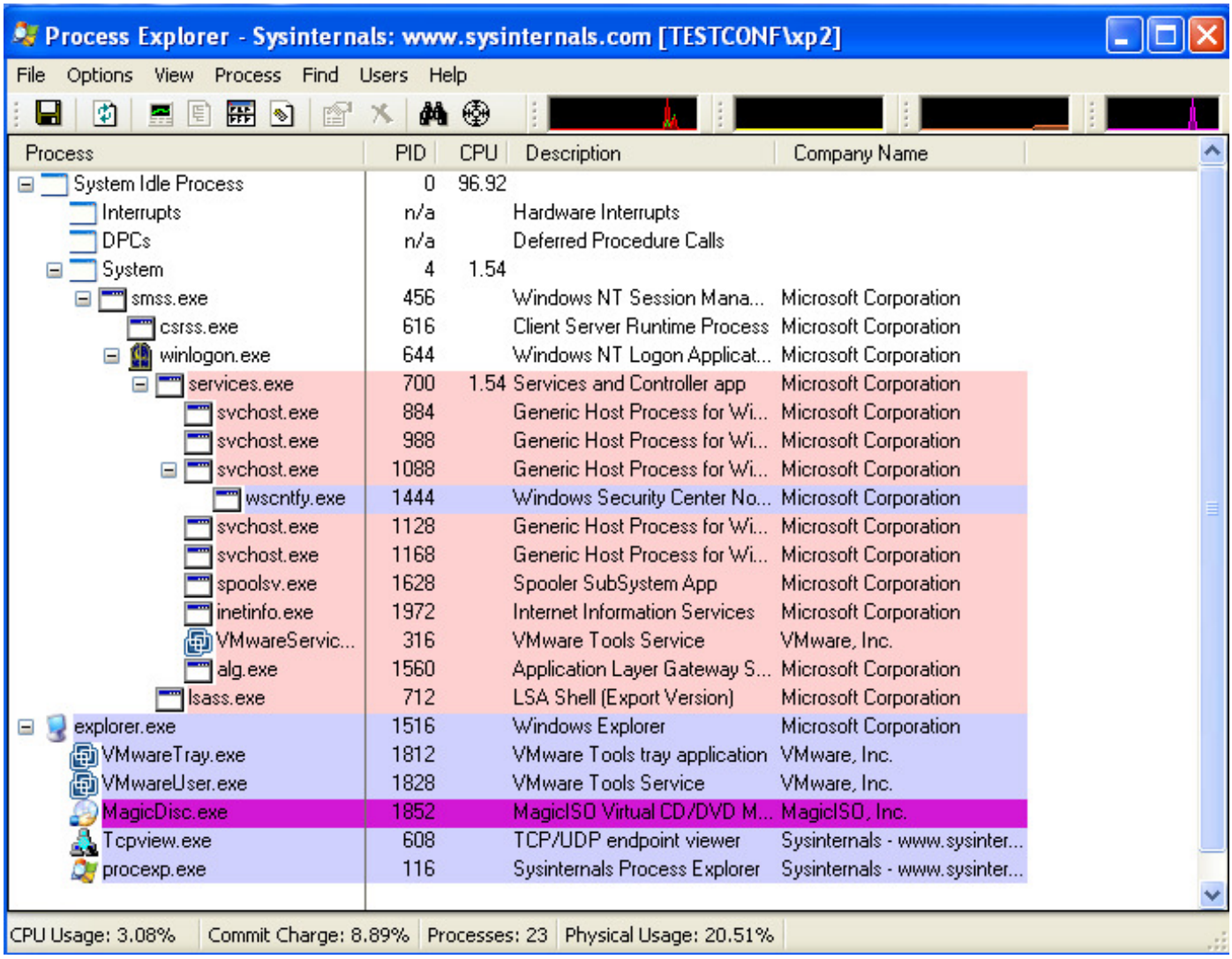


Figure 2

Step 3) Taking a snapshot of the TCP & UDP Ports

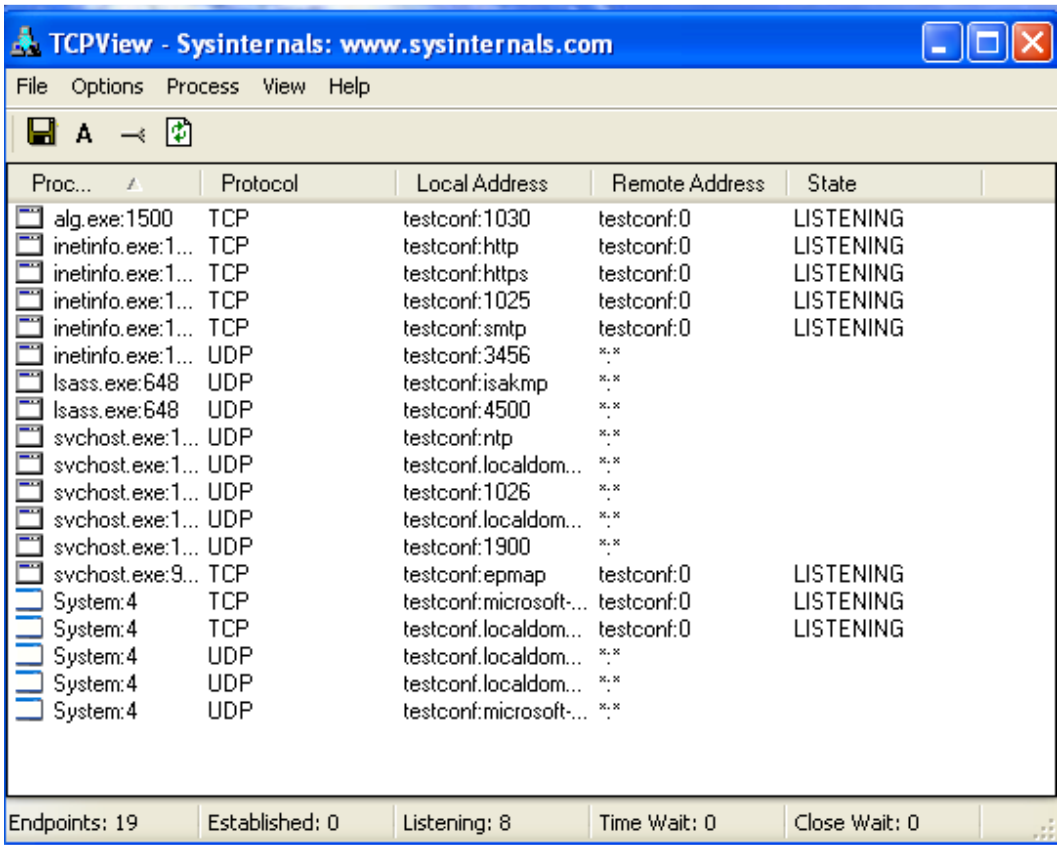


Figure 3

Step 4) Taking a snapshot of the autorun

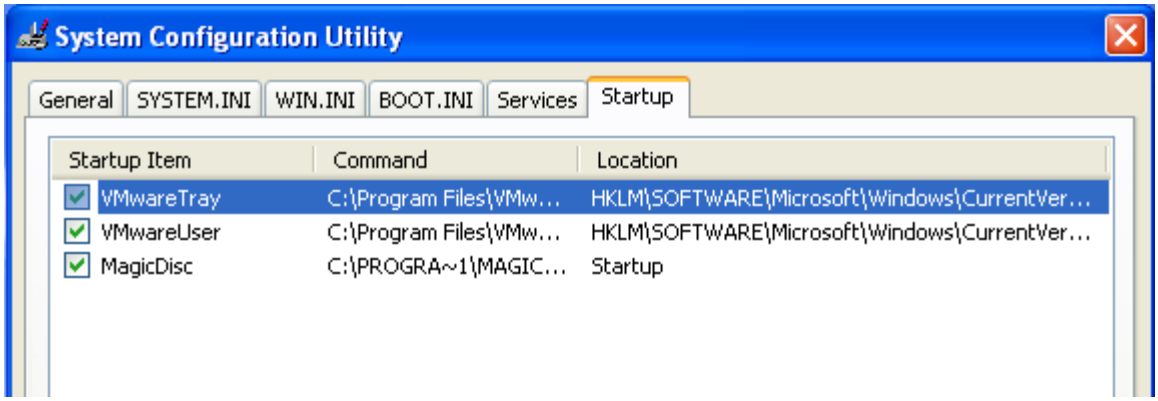


Figure 4

Step 5) Taking a snapshot of the running services

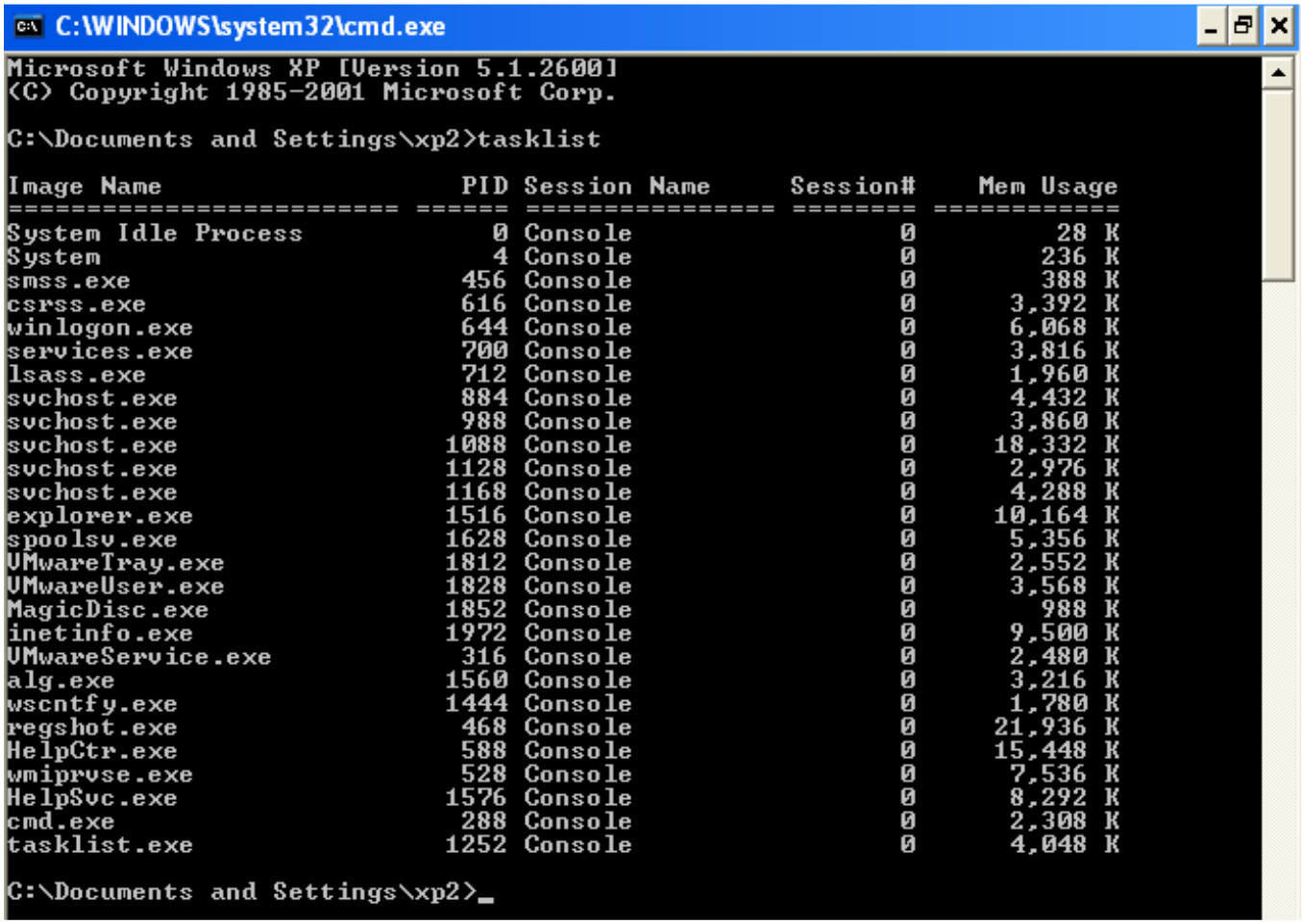


Figure 5

Step 6) Sniffing the packets on the Guest Machine

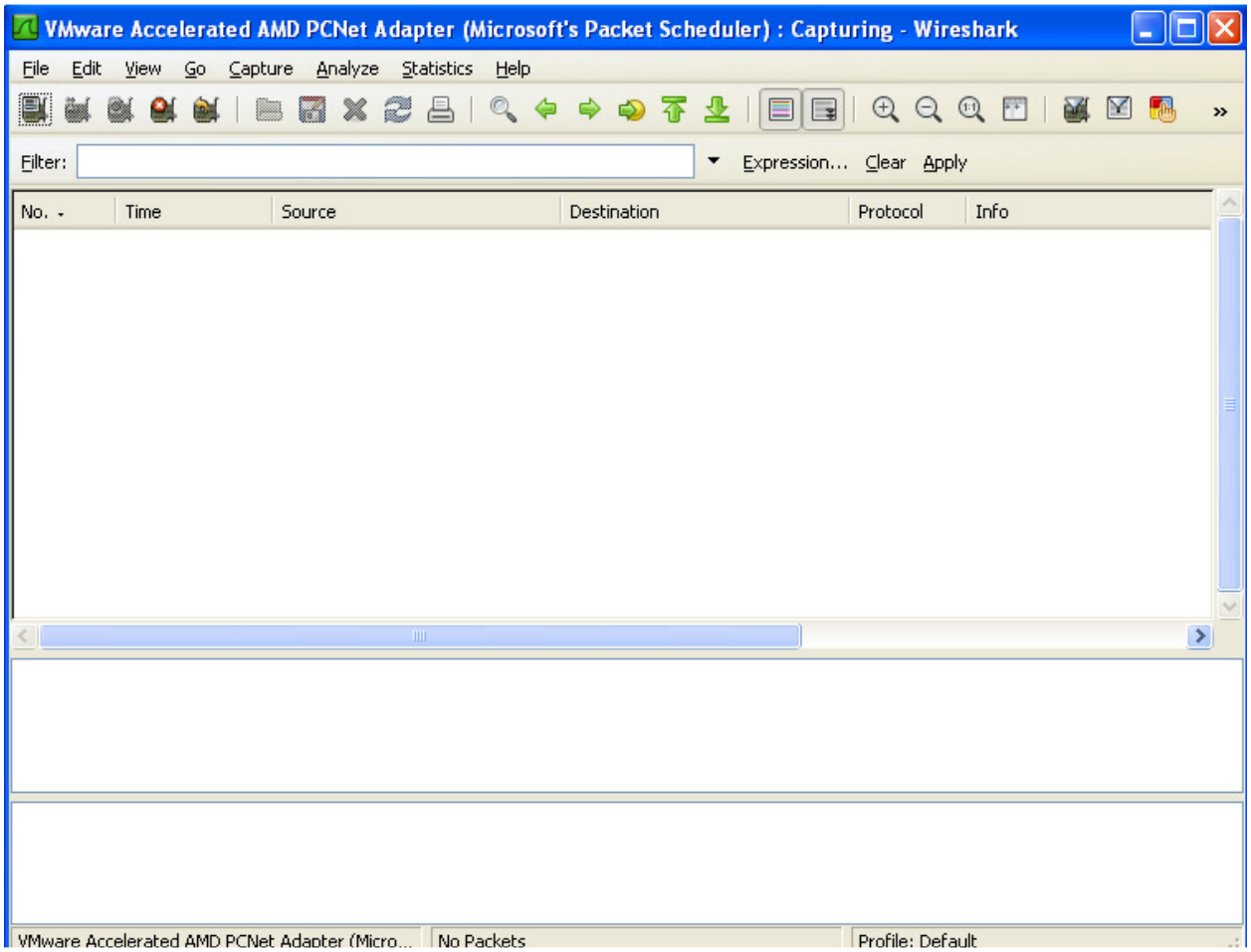


Figure 6

From above snapshot we can see no packets are transmitted in and out from the machine.

Once we have taken the snapshot of all the above things the computer we can now start with Analysing the malware.

The Fun Stuff start from here……..

Case Study of Malware "FIWSIVST"

Once I have taken the snapshots of the Operating system and can now begin with the malware analysis.

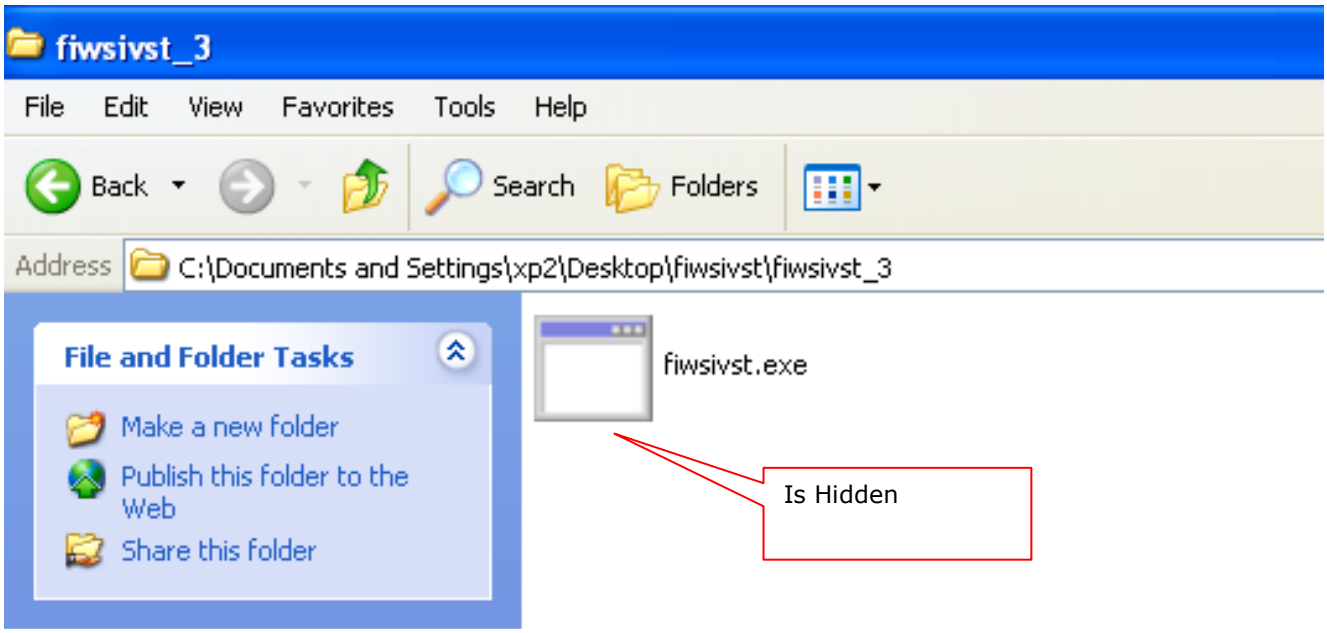
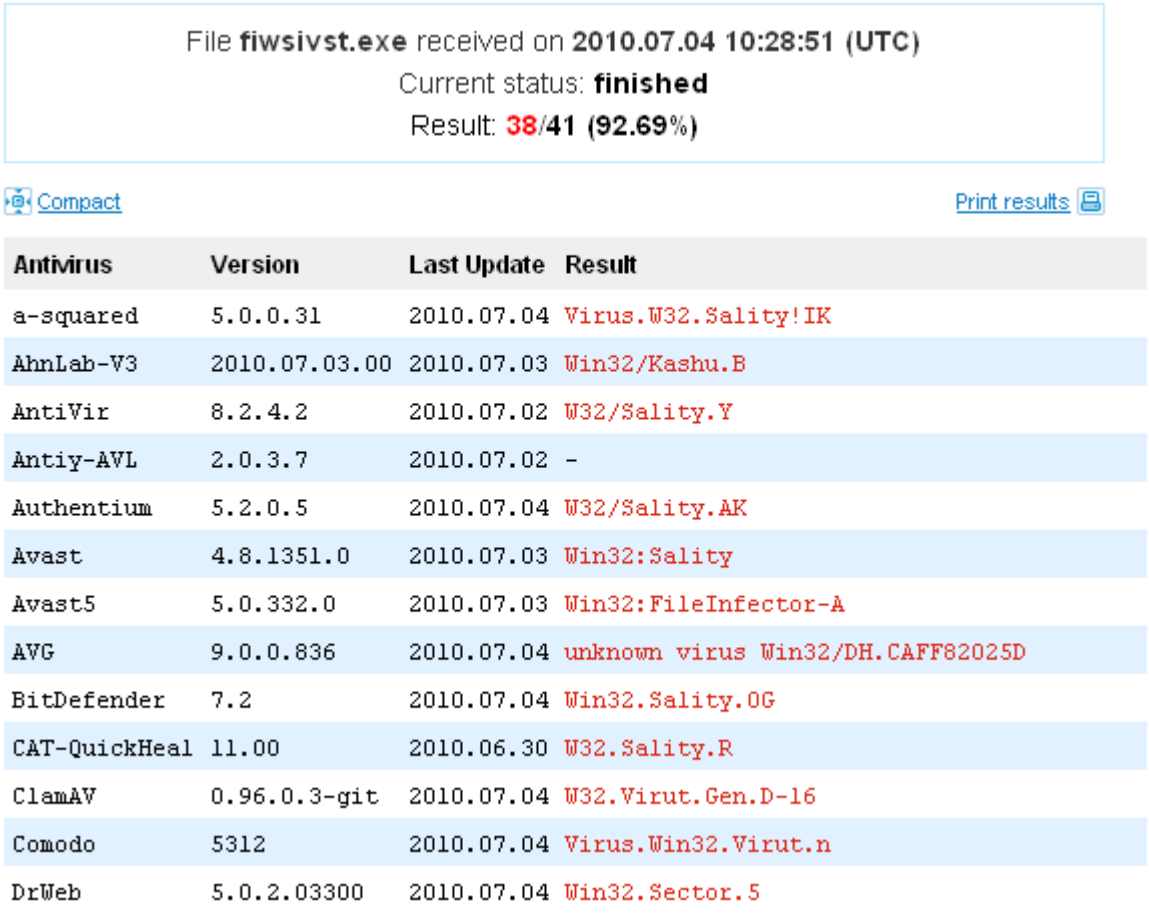


Figure 6

I will do malware analysis for the fiwsivst.exe which is hidden as show above.



File **fiwsivst.exe** received on **2010.07.04 10:28:51 (UTC)**
Current status: **finished**
Result: **38/41 (92.69%)**

Compact Print results

Antivirus	Version	Last Update	Result
a-squared	5.0.0.31	2010.07.04	Virus.W32.Sality!IK
AhnLab-V3	2010.07.03.00	2010.07.03	Win32/Kashu.B
AntiVir	8.2.4.2	2010.07.02	W32/Sality.Y
Antiy-AVL	2.0.3.7	2010.07.02	-
Authentium	5.2.0.5	2010.07.04	W32/Sality.AK
Avast	4.8.1351.0	2010.07.03	Win32:Sality
Avast5	5.0.332.0	2010.07.03	Win32:FileInfector-A
AVG	9.0.0.836	2010.07.04	unknown virus Win32/DH.CAFF82025D
BitDefender	7.2	2010.07.04	Win32.Sality.OG
CAT-QuickHeal	11.00	2010.06.30	W32.Sality.R
ClamAV	0.96.0.3-git	2010.07.04	W32.Virut.Gen.D-16
Comodo	5312	2010.07.04	Virus.Win32.Virut.n
DrWeb	5.0.2.03300	2010.07.04	Win32.Sector.5

Figure 7
[Most of the Anti-virus confirmed that fiwsivst.exe is a malware]

The fiwsivst.exe is a malware which have already been confirmed by most of the Antivirus. 38/41 anti-Virus had shown fiwsivst.exe is a malicious code.

Note: Virus total (www.virustotal.com) provides free virus and malware online scan service. If there is any file that looks suspicious and infected with malware you can upload suspicious file on virus total to scan against multiple Anti-Virus software's.

Once the malware is executed I can start the malware behavior analysis.

I will start the malware analysis with first comparing the register snapshot with the baseline as it will give me lot of information such as changes in the registry, new files added or deleted, new service added and then I will cross-verify every information

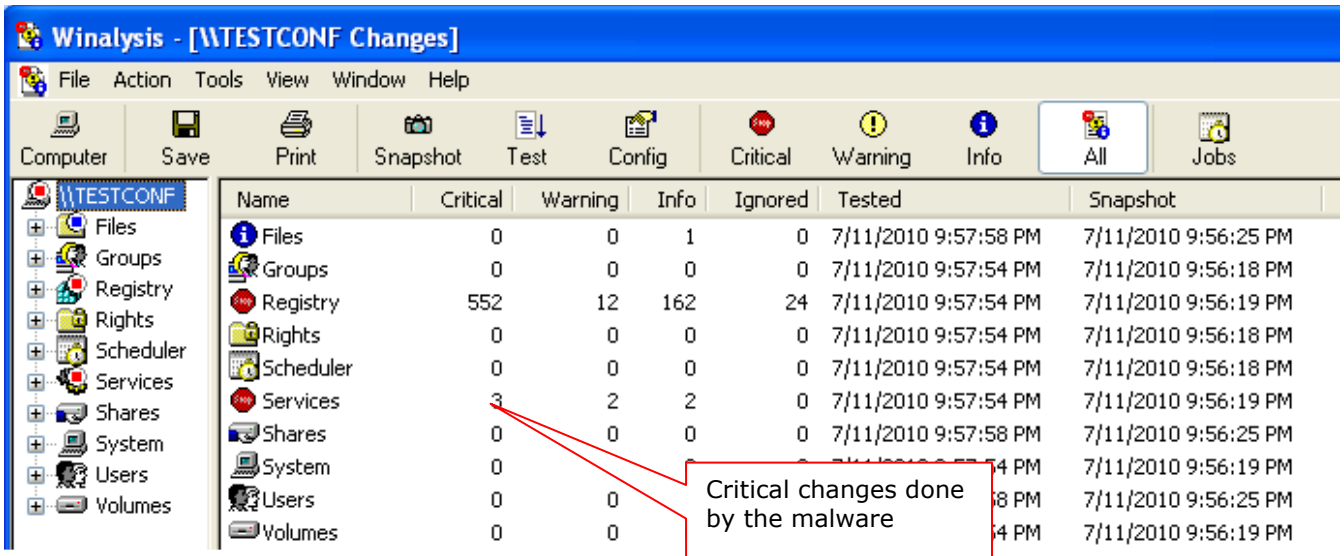


Figure 8

[Most of the Anti-virus confirmed that fiwsivst.exe is a malware]

From the above figure we can identify 552 critical changes in the registry and 3 critical changes in the service were made by the malware.

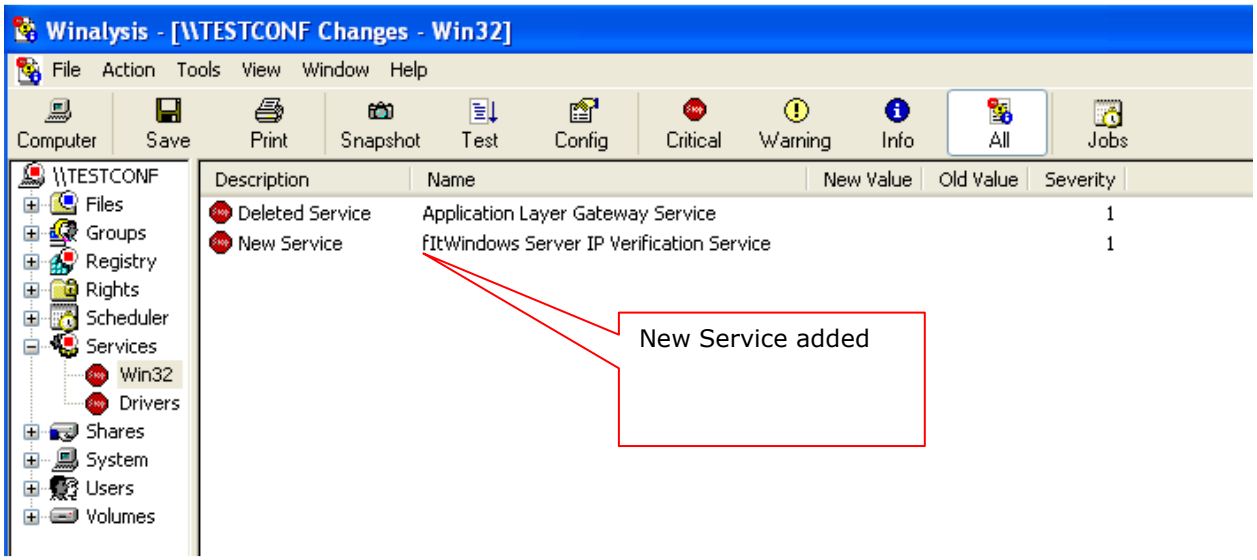


Figure 9

A new service is added which we will confirm later.

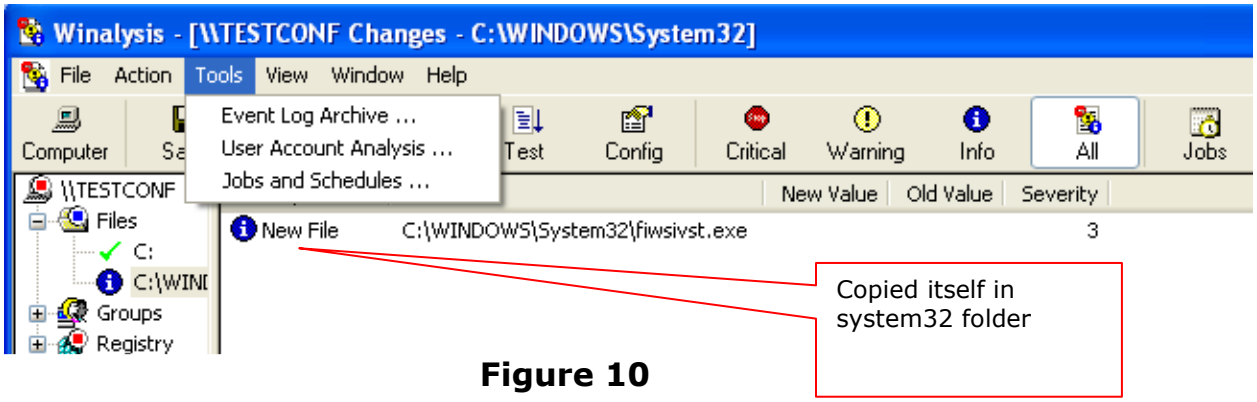


Figure 10

Malware made a copy of itself in C:\WINDOWS\System32\fiwsivst.exe

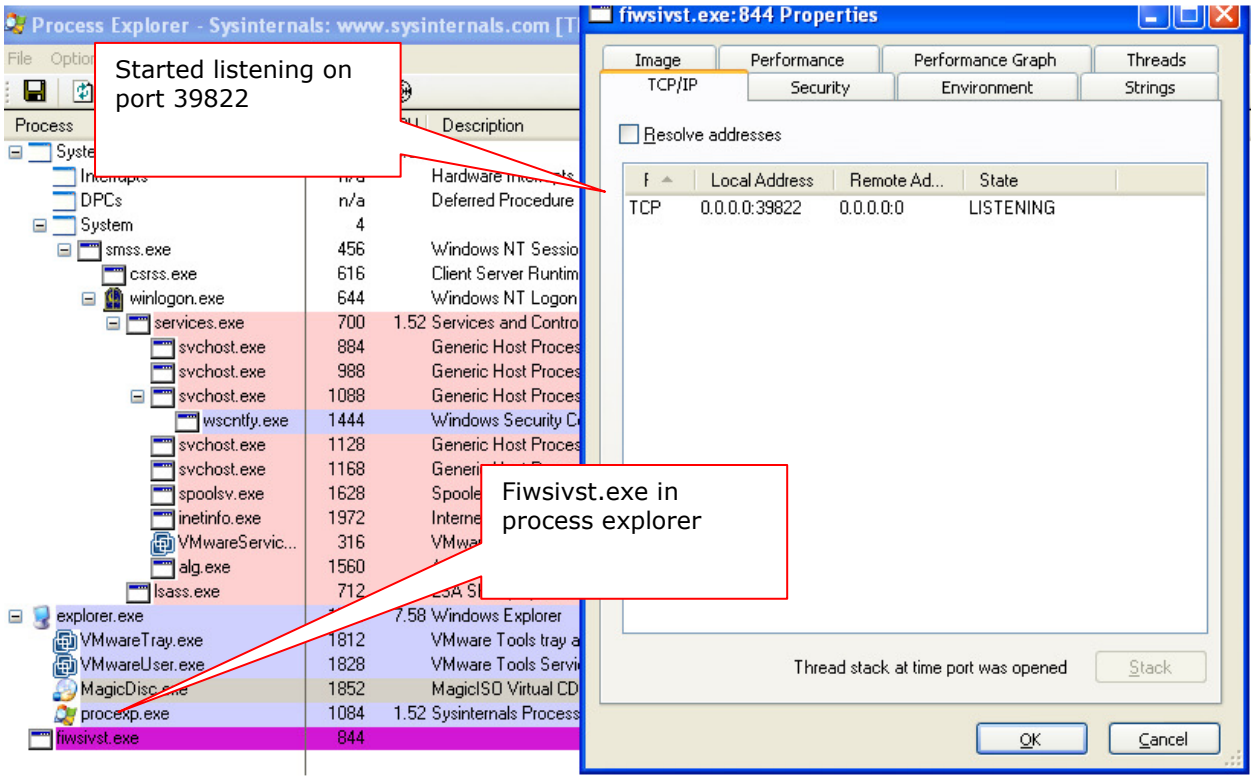


Figure 11

[Comparing with Figure2 a new process have been created]

After executing fiwsivst.exe, it has started showing in process explore and open a backdoor by starting listening on port 39222(next snapshot). Most malware especially trojans will open a backdoor like this.

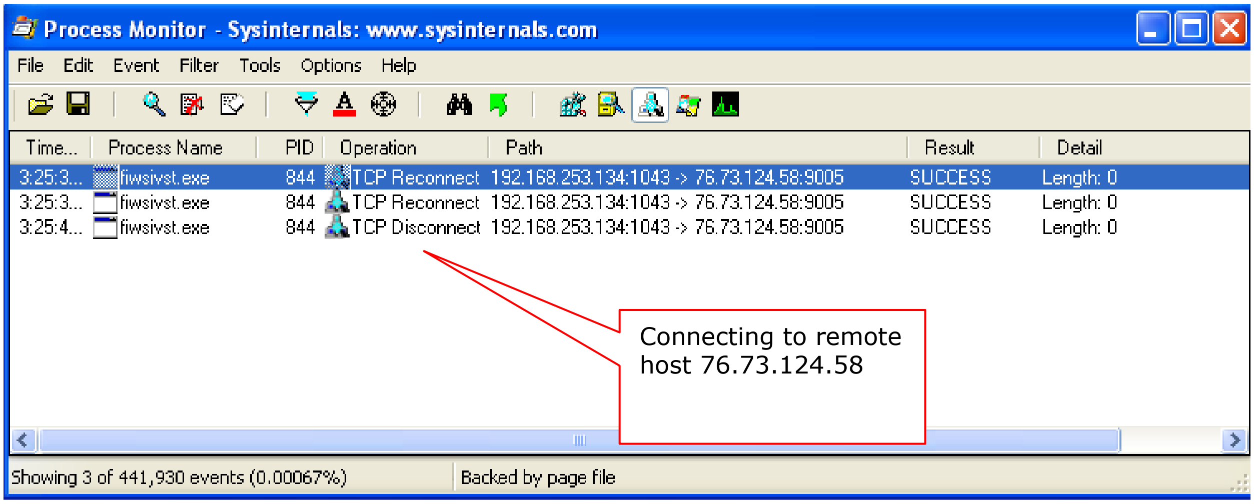


Figure 12

[Comparing with Figure 3, fiwsivst.exe making a remote connection]

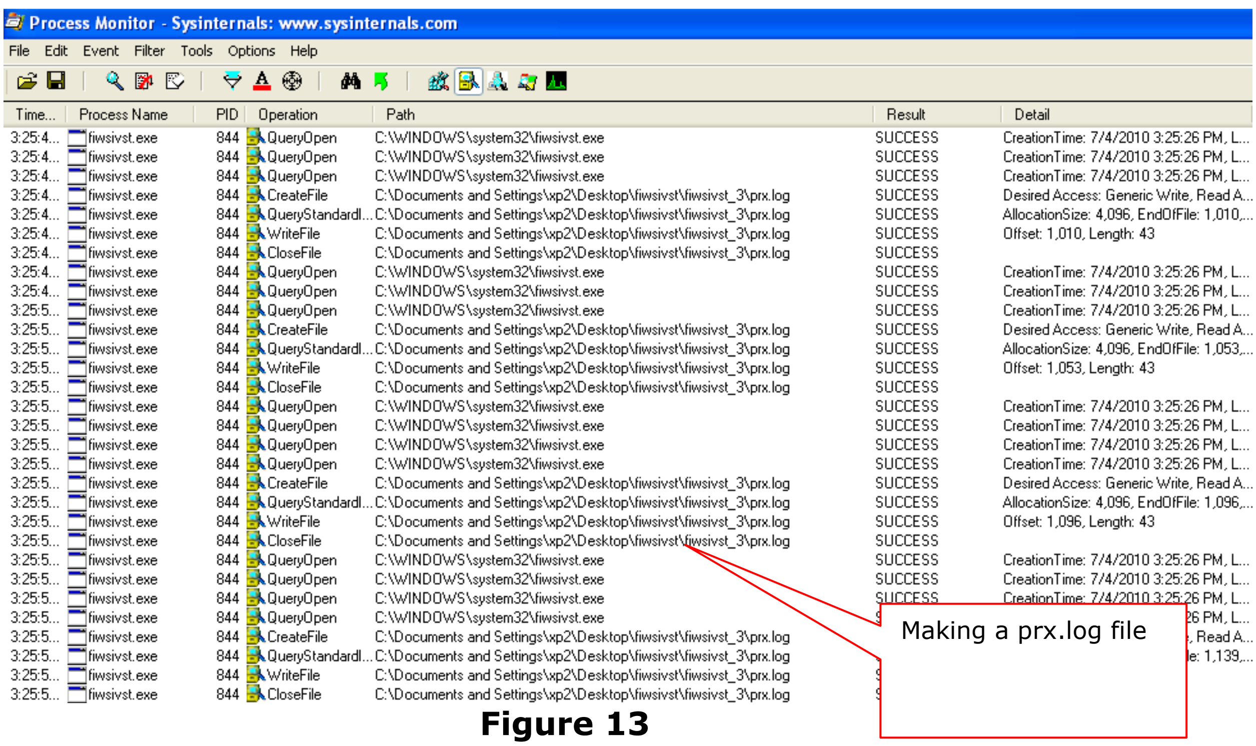


Figure 13

The Process monitor show that it added a copy of itself in **C:\WINDOWS\system32\fiwsivst.exe** and starting making a log file in **C:\Documents and Settings\xp2\Desktop\fiwsivst\prx.log**

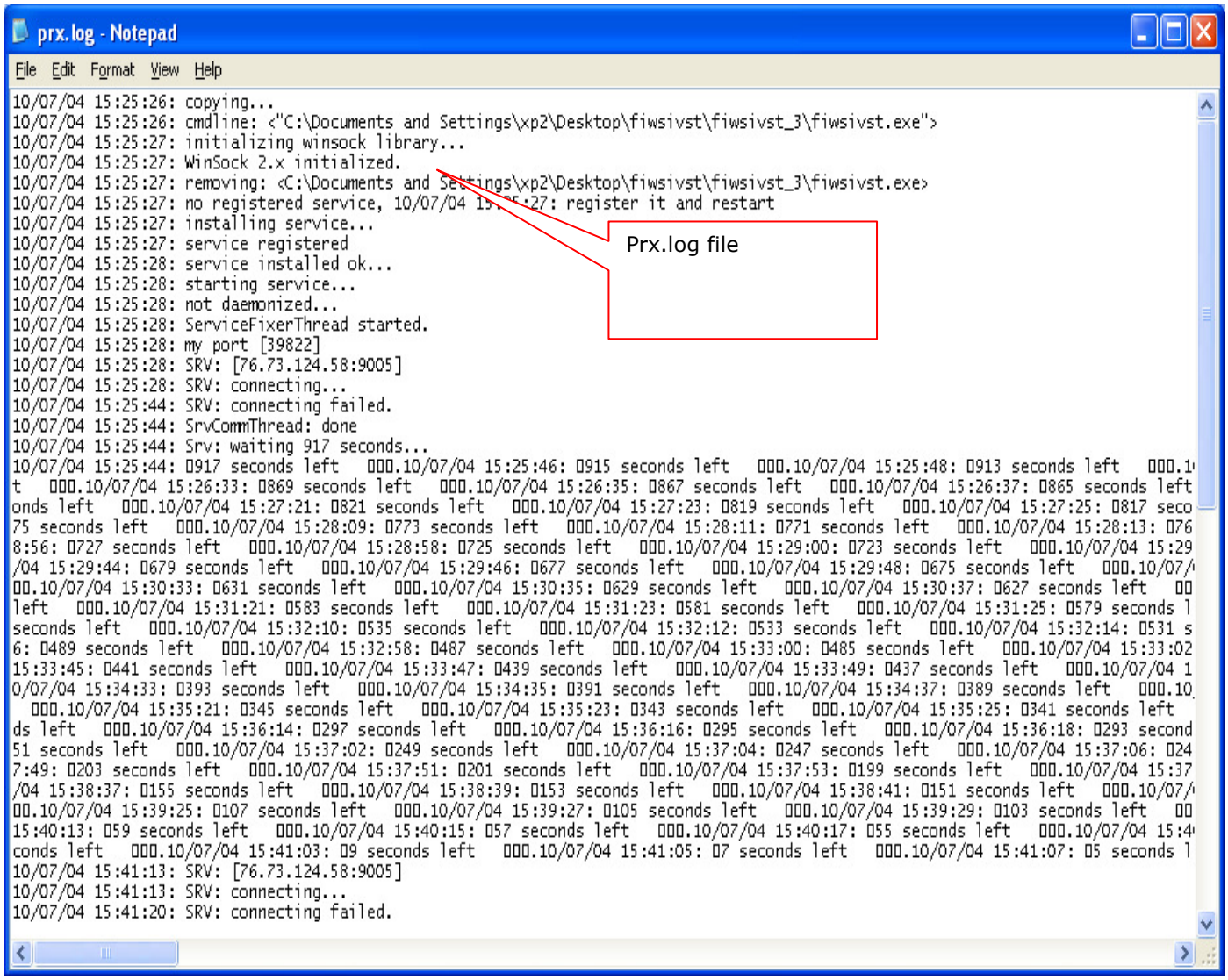


Figure 14

The prx.log file indicates it is trying to establish a remote connection 76.73.124.58 on port 9005. The initial log file indicated it has installed and added itself in the services.msc. Let's check it out.

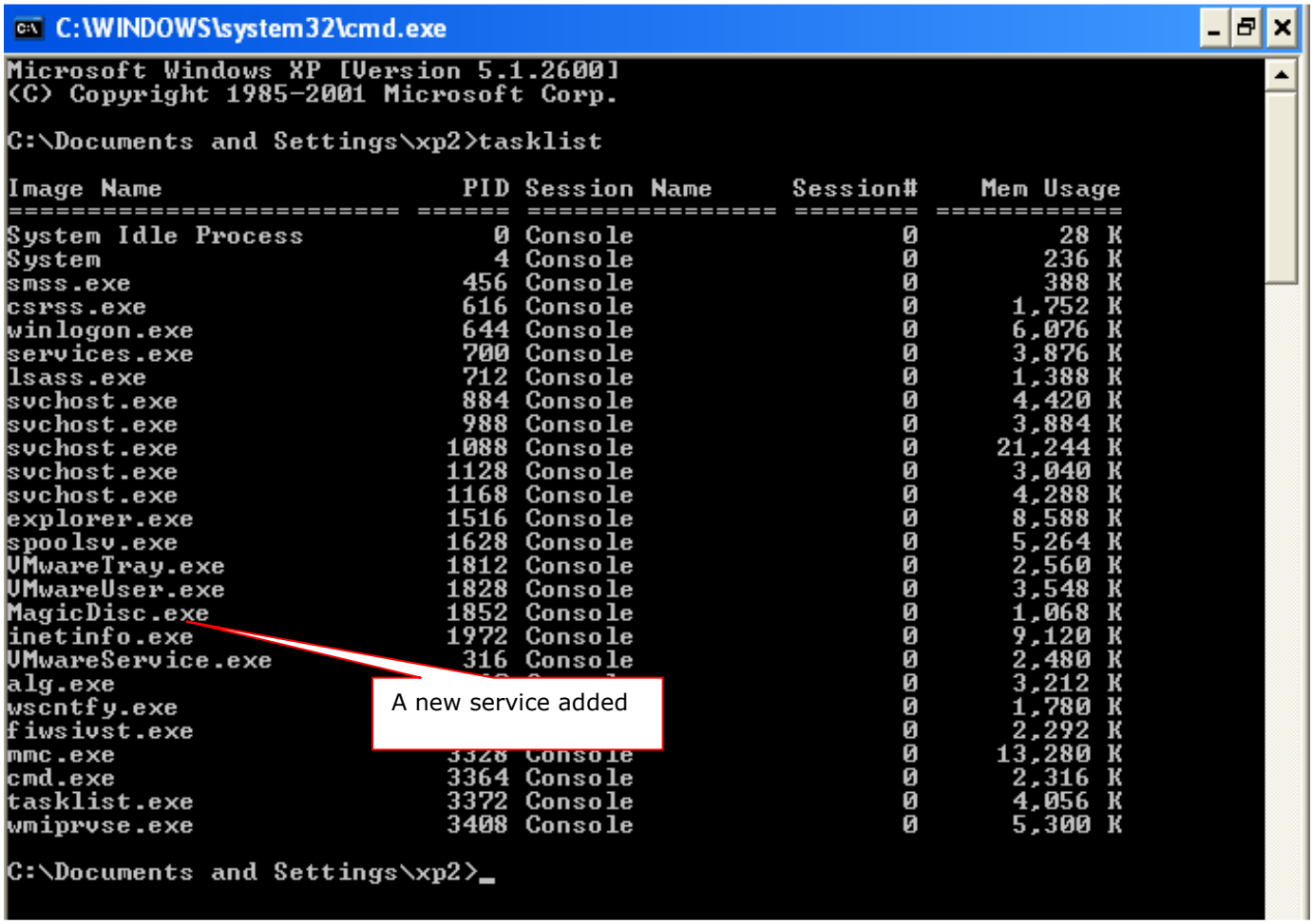


Figure 15

[Comparing with Figure 5 a new process have been created]

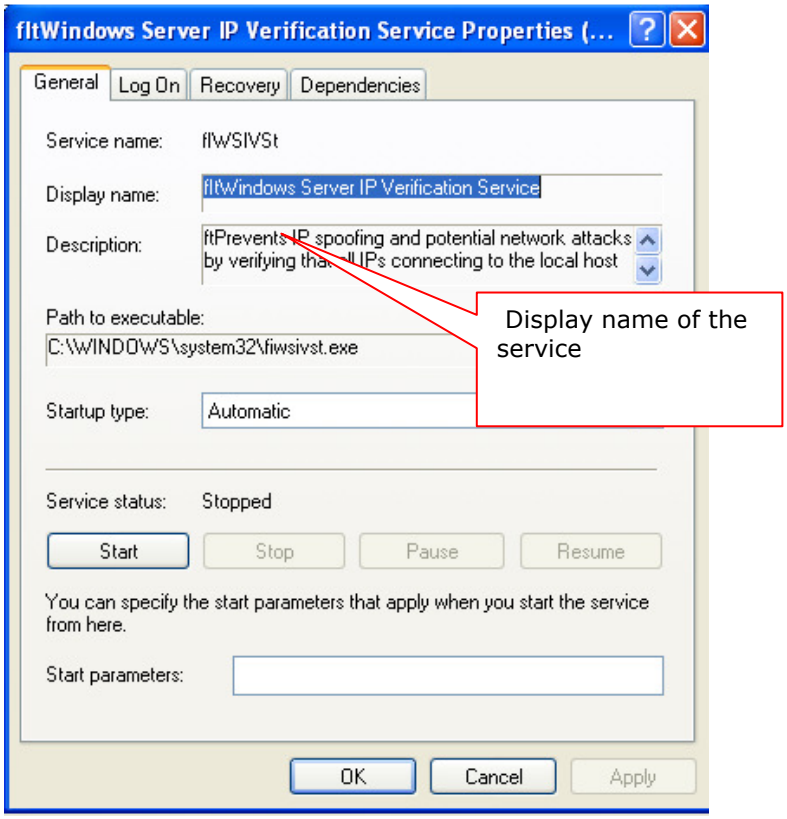


Figure 16

The malware added itself as a service with the Display name as **"fItWindows Server IP Verification Service"** and it is executed from path **C:\WINDOWS\system32\fiwsivst.exe**

From the above snapshot we can see fiwsivst.exe has added itself.

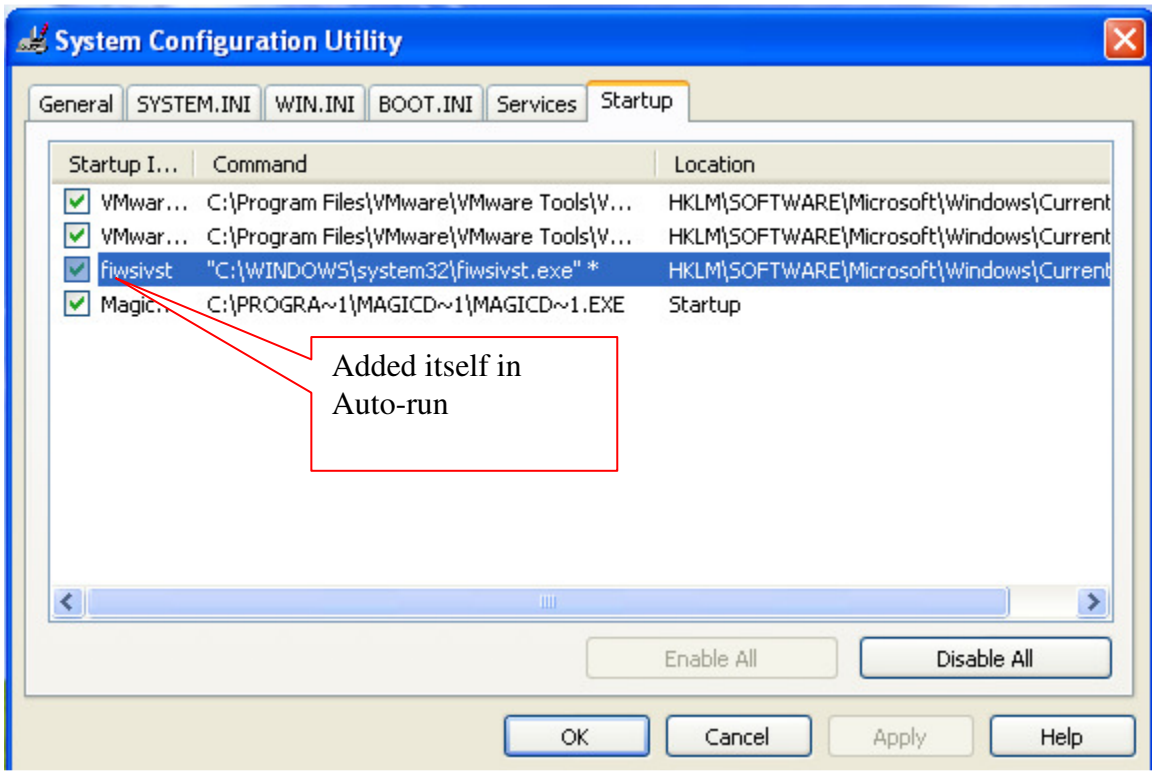
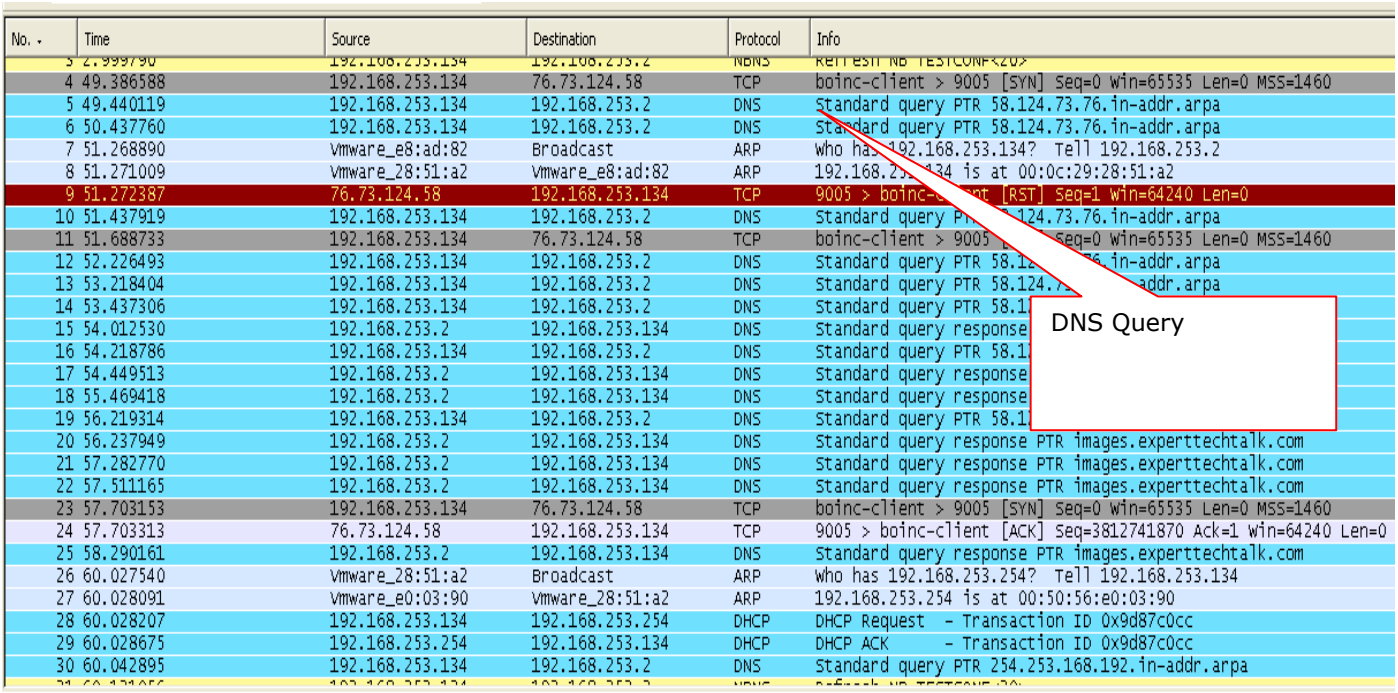


Figure 17

[Comparing with Figure 4 a new startup have been added]

As most of the malware have a habit of adding themselves in auto-run so that they can start itself after a computer reboot.

Now let see the packet capture by the wireshark

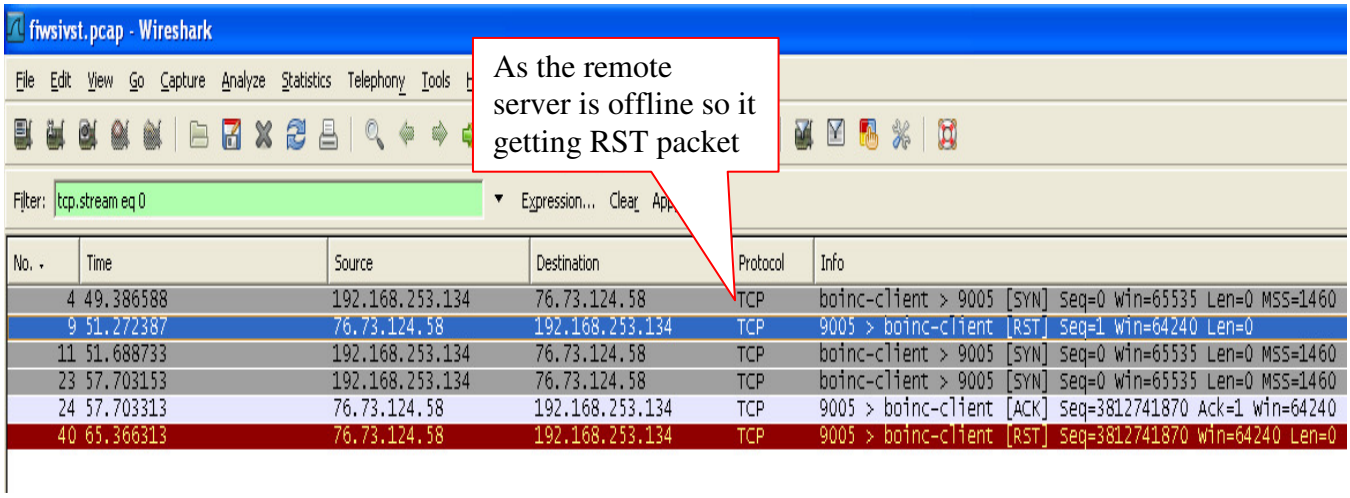


No.	Time	Source	Destination	Protocol	Info
4	49.386588	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
5	49.440119	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
6	50.437760	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
7	51.268890	Vmware_e8:ad:82	Broadcast	ARP	Who has 192.168.253.134? Tell 192.168.253.2
8	51.271009	Vmware_28:51:a2	Vmware_e8:ad:82	ARP	192.168.253.134 is at 00:0c:29:28:51:a2
9	51.272387	76.73.124.58	192.168.253.134	TCP	9005 > boinc-client [RST] Seq=1 Win=64240 Len=0
10	51.437919	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
11	51.688733	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
12	52.226493	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
13	53.218404	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
14	53.437306	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
15	54.012530	192.168.253.2	192.168.253.134	DNS	Standard query response
16	54.218786	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
17	54.449513	192.168.253.2	192.168.253.134	DNS	Standard query response
18	55.469418	192.168.253.2	192.168.253.134	DNS	Standard query response
19	56.219314	192.168.253.134	192.168.253.2	DNS	Standard query PTR 58.124.73.76.in-addr.arpa
20	56.237949	192.168.253.2	192.168.253.134	DNS	Standard query response PTR images.experttechtalk.com
21	57.282770	192.168.253.2	192.168.253.134	DNS	Standard query response PTR images.experttechtalk.com
22	57.511165	192.168.253.2	192.168.253.134	DNS	Standard query response PTR images.experttechtalk.com
23	57.703153	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
24	57.703313	76.73.124.58	192.168.253.134	TCP	9005 > boinc-client [ACK] Seq=3812741870 Ack=1 Win=64240 Len=0
25	58.290161	192.168.253.2	192.168.253.134	DNS	Standard query response PTR images.experttechtalk.com
26	60.027540	Vmware_28:51:a2	Broadcast	ARP	Who has 192.168.253.254? Tell 192.168.253.134
27	60.028091	Vmware_e0:03:90	Vmware_28:51:a2	ARP	192.168.253.254 is at 00:50:56:e0:03:90
28	60.028207	192.168.253.134	192.168.253.254	DHCP	DHCP Request - Transaction ID 0x9d87c0cc
29	60.028675	192.168.253.254	192.168.253.134	DHCP	DHCP ACK - Transaction ID 0x9d87c0cc
30	60.042895	192.168.253.134	192.168.253.2	DNS	Standard query PTR 254.253.168.192.in-addr.arpa

Figure 18

[Comparing with Figure 6 a DNS query to malicious IP have been sent]

The packet capture shows that it is first making and DNS query for 76.73.124.58 and then sending a SYN packet to again 76.73.124.58



No.	Time	Source	Destination	Protocol	Info
4	49.386588	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
9	51.272387	76.73.124.58	192.168.253.134	TCP	9005 > boinc-client [RST] Seq=1 Win=64240 Len=0
11	51.688733	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
23	57.703153	192.168.253.134	76.73.124.58	TCP	boinc-client > 9005 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
24	57.703313	76.73.124.58	192.168.253.134	TCP	9005 > boinc-client [ACK] Seq=3812741870 Ack=1 Win=64240
40	65.366313	76.73.124.58	192.168.253.134	TCP	9005 > boinc-client [RST] Seq=3812741870 Win=64240 Len=0

Figure 19

The above snapshot indicates 76.73.124.58 is sending a RST packet when Guest machine (infected machine) is trying to communicate. The RST packet

we are receiving because the Destination port on 76.73.124.58 may be closed.

On doing whois, we got to know that this IP belongs to FDCserver.net which offers virtual and dedicated servers to host applications.

76.73.124.58 | Track IP, host or website

Examples: 213.86.83.116 (IP address) or google.com (Website)

76.73.124.58 IP address location & more:	
IP address [?]:	76.73.124.58 [Whois] [Reverse IP]
IP country code:	US
IP address country:	United States
IP address state:	Illinois
IP address city:	Woodstock
IP postcode:	60098
IP address latitude:	42.3222
IP address longitude:	-88.4671
ISP of this IP [?]:	FDCservers.net
Organization:	FDCservers.net
Host of this IP: [?]:	images.experttechtalk.com [Whois] [Trace]
Local time in United States:	2010-07-15 02:34

Summary of Malicious Code

After executing fiwsivst, a malware

- Fiwsivst is a malware that has been confirmed by most of the Anti-Virus.
- Next I took the Snapshot of the Windows XP Operating System on which I am going to do Malware Analysis.
- I executed Malware and compared the snapshot with the baseline.
- Malware made 552 critical change and 3 critical changes in the services.
- Made a copy of itself in **C:\WINDOWS\system32\fiwsivst.exe**
- Added itself in the windows process as "**fItWindows Server IP Verification Service"**
- Added itself in Auto-run
- Opened a backdoor on local machine by listing on port 1043
- Starting making a remote connection to 76.73.124.58
- On doing IP trace on 76.73.124.58, we got to know this IP belongs to FDC Server in US.

RECOMMENDATIONS

- Should keep operating system up-to-date with latest patch level
- Should have a genuine and licensed version of Anti-virus software
- Should update Anti-virus signatures on a regular basis
- Should scan their systems daily
- Should not open any sites related pornography, illegal softwares, free softwares, free games, lottery etc.
- Should not download any software from unknown sites or sites which looks suspicious
- Should scan a software before installing it
- Should never click on a link given in an email
- Should always scan a USB after connecting to the PC
- Should disable auto run feature in operating system
- Always scan an attachment before opening it in an email
- Should have firewall install on the system
- Take a backup of your critical data

Appendix: Related Resources

Addition security information and resources can be found below

1) Understanding Anti-Malware Technologies, An Overview of client-side security software for business, Microsoft
http://download.microsoft.com/download/a/b/e/abefdf1c-96bd-40d6-a138-e320b6b25bd3/understandingantimalwaretechnologies.pdf

2) Combating Viruses, Worms and Trojan Horses, webopedia
http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp

3) Security Threat Report 2010, Sophos
http://www.sophos.com/security/topic/security-report-2010.html

4) Quarterly Report Pandalabs (April-June 2010), Pandalabs
http://www.pandasecurity.com/homeusers/downloads/register?Tipo=5&CodigoProducto=99&Idioma=2&TipoUsuario=11&Country=US&TipoLead=2&Ref=WW-EN-T2PLABS07

Written By:

Sachin Chadha
Information Security Consultant
MSc Computer System Security (UK), MCSA, CEH
Sachin.glam@gmail.com

Special thanks to Asheesh Kumar Tripathi & Vaibhav Gupta