

Anti-Virus Evasion Techniques and Countermeasures



Author: Debasis Mohanty
www.hackingspirits.com

Email ID: debasis_mty@yahoo.com
mail@hackingspirits.com

Table of Contents

1. INTRODUCTION	3
2. ANTI-VIRUS EVASION TECHNIQUES	4
2.1 <i>USE OF BINDERS AND PACKERS.....</i>	4
2.2 <i>CODE OBFUSCATION.....</i>	6
2.3 <i>CODE CONVERSION FROM EXE TO CLIENT SIDE SCRIPTS.....</i>	8
2.4 <i>FAKE FILE TYPE EXTENSION.....</i>	9
3. MALICIOUS CODES IDENTIFICATION AND REMOVAL TECHNIQUES	10
3.1 <i>MANUALLY IDENTIFYING MALICIOUS CODES.....</i>	10
3.2 <i>MANUALLY REMOVING VIRUSES AND WORMS.....</i>	11
4. COUNTERMEASURES AGAINST MALICIOUS CODES	15
5. CONCLUSION	16
6. ABOUT AUTHOR.....	16

1. Introduction

The objective of this article is to demonstrate different possible ways that viruses and worms coders use to evade any Anti-Virus products while coding malicious programs and at the same time I shall also be discussing about the countermeasures techniques to prevent against such attacks. Before I go in depth I assume that the readers of this article are well aware of the difference between worms and viruses.

It is not just an anti-virus product which can help protect the corporate and the end-users from malicious program attacks but rather what is most important is the general user awareness about such risks and general responsibility towards defending against such attacks.

This article will also try to educate various kind computer users in the simplest way to deal with viruses and worms and defend against such malicious attacks where the AV engine become helpless when special techniques are used by this malicious codes to prevent detection.

In this article I shall highlight on the following things:

- *Anti-Virus Evasion Techniques*
 - Use of binder and packers
 - Codes Obfuscation
 - Code conversion from EXE to client side scripts
 - Fake file type extension
- *Malicious Codes Identification and Removal Techniques*
- *Countermeasures against Malicious Codes*

2. Anti-Virus Evasion Techniques

As stated earlier the primary aim of this article is to educate normal computer users and as well as corporate end-users, system administrators and security professionals on how to dealt with malicious codes. For better understanding I shall take you through various techniques used by these malicious codes to get past an anti-virus product. Below given are various techniques used by viruses and worms to evade most of the anti-virus products.

2.1 Use of binders and packers

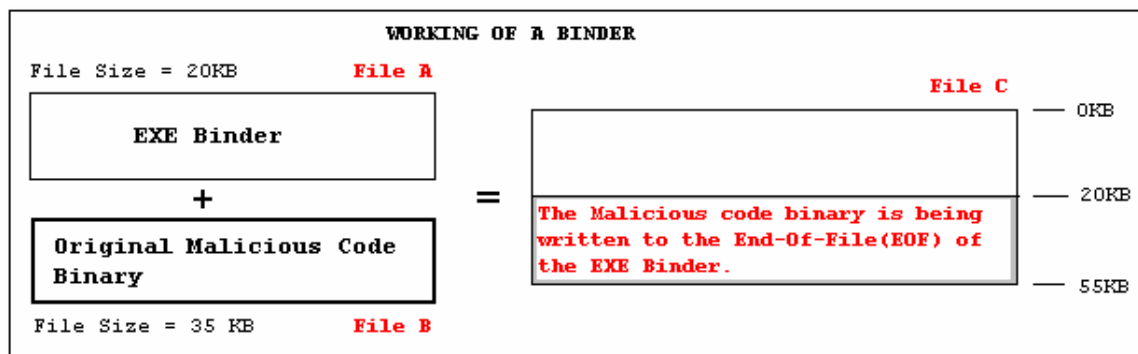
Before I could discuss about how binders and packers are used for anti-virus evasion, it is very much important to understand how an anti-virus detects any malicious files based on its signature database.

Most of the anti-virus products create viruses or worms signature based on the file properties and first few bytes of the malicious code binaries. It usually create a checksum value based on the file properties and apart from that it takes first few bytes of the binaries to create the signature for the malicious code. The signature for a particular malicious code will look something like:

Anti-Virus Signature File Format For Any Malicious Code	
File Properties	First Few Bytes Of The Malicious Code
Checksum = File Type + File Size	For e.g. Few bytes (e.g. 40Bytes) starting from particular offset till next 39 Bytes.

Binders

Binders are used to bind two or more than two EXE files to one single EXE file. It usually binds other EXE files to itself and generates a new binary. For example the original size of the Binder file is 20 KB and the size of the EXE to be attached is 35 KB then the final size of the new EXE generated will be 20 KB + 35 KB = 55 KB (Refer to the figure shown below).



From the above figure, the Binder (File A) binds the malicious code binary (File B) to the end-of-file (EOF). This creates another EXE (File C) which combines both File A and File B. Now on executing File C, the file read offset sets at 20 KB and read for rest 35KB to extract the original malicious code binary (File B).

This is how viruses or worms can be hidden using binders and can get past undetected by all anti-virus products. Since, the original signature of the malicious code gets shifted to a different offset in the newly generated binary which can easily evade any static anti-virus products.

Few good binders available on internet are Infector v2, Exe-Maker, Exe-Joiner, Trojan Man, Elitewrap and TOP.

Packers (Compressors)

Packers work very similar to the way binders work but the only difference between them is in case of packers the malicious binary is compressed before it gets embedded to the packer's binary to generate the final EXE. This makes any anti-virus product helpless in detecting the compressed malicious binaries since, the signature changes because of the compression.

Few good packers available on internet are Shrinker, PKLite, AS-pack, Petite, and WWpack.

2.2 Code Obfuscation

Code obfuscation is a process where the binary of the malicious program undergoes various transformations (Ex Code Morphing) which are undetected by anti-virus products. There are various kinds of code obfuscation techniques like polymorphism, metamorphism etc but in this section; I shall discuss about a technique called “Code Morphing” which prevents anti-virus from detecting malicious patterns in the binaries.

In case of “Code Morphing”, the malicious code is encrypted and a small routine is embedded to decrypt the code before running the malicious code. This kind of code obfuscation undergoes several transformations which are nondeterministic and destroys the visible logical code structure and hence it not only prevent detection by anti-viruses but also prevents disassembling or debugging by tools like SoftIce and IDAPro etc. One such tool called “EXECryptor” does this kind of code obfuscation.

Various kinds of transformations used in such techniques are: NOP-Insertion, Code Transposition (i.e. changing the order of instructions and placing jump instructions to maintain the original semantics), and register reassignment (permuting the register allocation). These transformations effectively change the malicious binaries signature, inhibiting effective signature scanning by an antivirus tool.

The screenshots 2.2.1 and 2.2.2 shows the analysis done on “NetBus” Trojan horse. Screenshot 2.2.1 displays the disassembled information before the code was obfuscated and screenshot 2.2.2 displays the disassembled information after the code was obfuscated. The changes in the assembly instructions are clearly visible in screenshot 2.2.1 and 2.2.2 starting from address “00401000” till “00401006”.

Screenshot 2.2.1 (“NetBus” signature before code obfuscation)

NetBus Binary Analysis Before Code Obfuscation			
Address		ASSEMBLY	
00401000	. 04104000	DD	NBSvr.00401004
00401004	03	DB	03
00401005	. 07	DB	07
00401006	. 42 6F 6F 6C 65	>ASCII	"Boolean"
Address		Hex Dump	ASCII
00470000	32 13 8B C0 02 00 8B C0		Z<A<A<A
00470008	00 8D 40 00 CC 47 40 00		.@.iG@.
00470010	CC 47 40 00 00 00 00 00		iG@.....
00470018	00 00 00 00 0C 21 40 00	!@.
00470020	94 22 40 00 08 26 40 00		""@.i&@.

Since, after the code obfuscation the signature of the malicious patterns has changed, anti-virus products fails to detect such obfuscated binaries.

Screenshot 2.2.2 (“NetBus” signature after code obfuscation)

NetBus Binary Analysis After Code Obfuscation		

Address		ASSEMBLY

004BC000	A4	MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI]
004BC001	C00B 00	ROR BYTE PTR DS:[EBX],0 ; shift constant
004BC004	0000	ADD BYTE PTR DS:[EAX],AL ; out of range 1..31
004BC006	0000	ADD BYTE PTR DS:[EAX],AL

Address	Hex Dump	ASCII

00470000	00 00 00 00 00 00 00 00
00470008	00 00 00 00 00 00 00 00
00470010	00 00 00 00 00 00 00 00
00470018	00 00 00 00 00 00 00 00
00470020	00 00 00 00 00 00 00 00

Various other tools those are popularly used by hackers and malicious code programmers to obfuscate malicious codes are “*Mistfall*” by z0mbie and “*Burneye*” by TESO.

Similarly, a polymorphic virus is a virus that encrypts itself, changing it's 'signature' so that it is difficult to detect by anti-virus software, by using a 'mutation engine' to change the appearance of the virus in an attempt to evade detection and destruction.

2.4 Fake File Type Extension

Malicious program coder uses various attractive names such as “nude-britney-spears.pif” or “sex-photo.jpg” while spreading the viruses and worms by emails to trick the recipients in opening and running the attachment. Some viruses & worms use multiple fake file type extensions to trick its victim in running the file. For example the AnnaKournikova worm uses the fake file type extension as “.jpg.vbs” (i.e. "AnnaKournikova.jpg.vbs") which entices the recipients into believing that they are receiving a harmless JPG image file of the famous tennis star instead of any malicious code. This is how fake file type names are being used by malicious programs to get past various security filters and fool the recipient in opening the email attachment.

One more method which malicious programmers, hackers and crackers use to fool its victim is by using CLSID (Class ID) extension for the malicious program. This method hides the original extension of the file.

3. Malicious Codes Identification and Removal Techniques

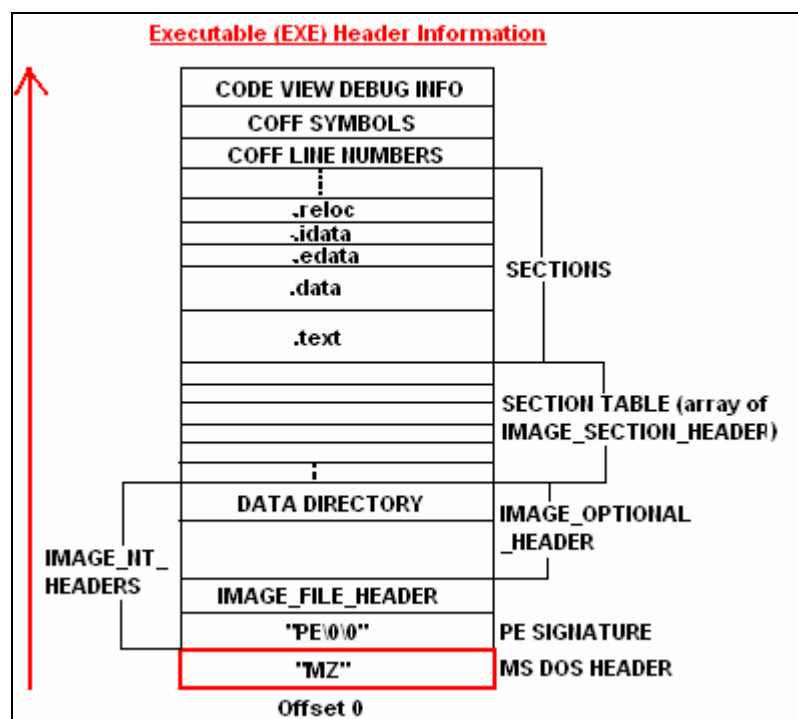
Most of the cases viruses and worms change their file extensions from “.exe” to some other extensions like “.pif”, “.scr” or “.jpeg” etc to trick its victim to download such files from internet or mails and execute it. Since, most of the cases these files are executables they gets executed once the users click on them and infects the user’s system.

3.1 Manually Identifying Malicious Codes

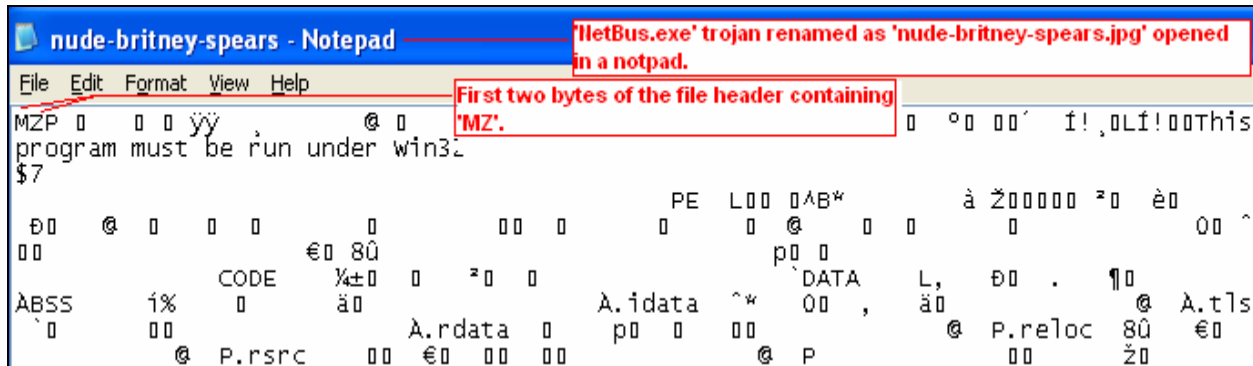
Here I shall discuss a simple method to detect any malicious binary with a fake file extension. This method can be used by ordinary computer user and as well as advance network security administrators for defense against such malicious binaries. Before we go further, it is important for the readers to know in brief about the structure of any executable or binary (.exe).

The header information of any executable file (.exe) is present in the first 27 bytes of the exe file. But one doesn’t have to go into so much of technical details to find out whether a file is an executable or not. The first two bytes of any executable file contains ‘MZ’ and is enough to prove whether a file is an executable or not. Different file types have different header properties and these properties don’t change even if the file extensions are changed.

Screenshot 3.1.1 (Executable or Binary Header Information)



Screenshot 3.1.2 (Executable or Binary Header Information)



Any users who receive such suspicious files through emails or from some other sources must verify by opening that file in the notepad. If the first two bytes contains 'MZ' then it is possibly an executable file whose file name has been changed to fool the recipient.

3.2 Manually Removing Viruses and Worms

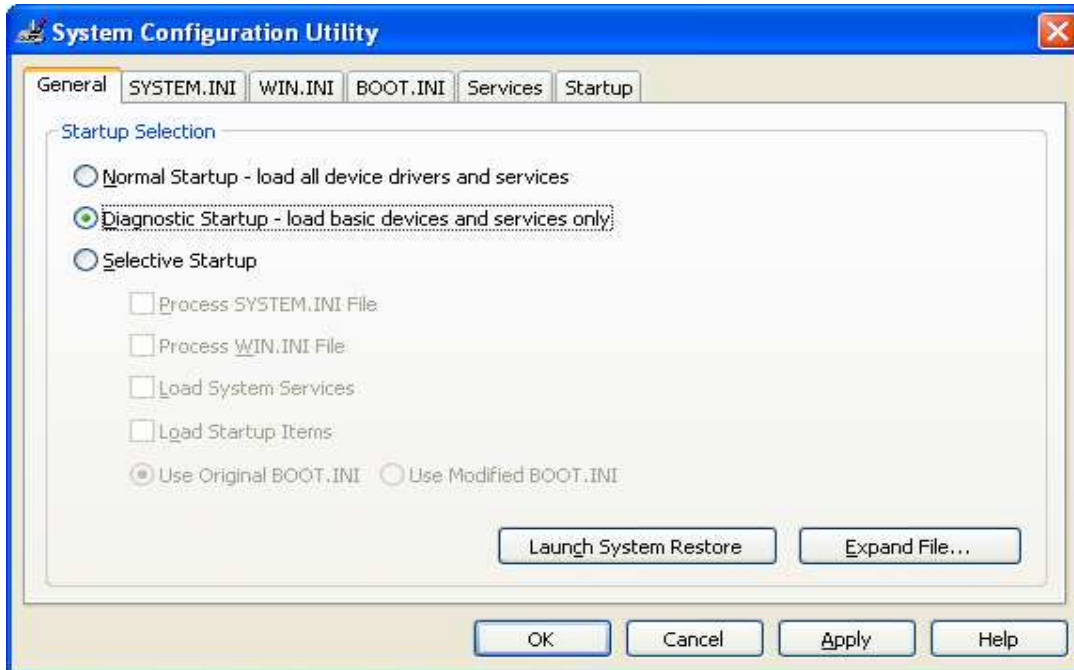
Here I shall discuss about manual techniques to remove any malicious program from an infected system. Below given are the steps to be followed while removing any malicious file manually.

- The first step is always isolating the system by removing it from any network (e.g. dial-up, LAN, VPN or DSL etc) if connected.
- Disable system restore and reboot the system in safe mode (Since, in safe mode very minimal services runs preventing any unknown services to start during system startup).
- This step is to remove un-necessary or any malicious programs from system startup. Windows "msconfig" tool can be used removing un-necessary programs from the system startup.

Note: "msconfig" is not present in all versions of windows. Incase msconfig is not present then the startup entries has to be removed manually which I shall discuss in further steps.

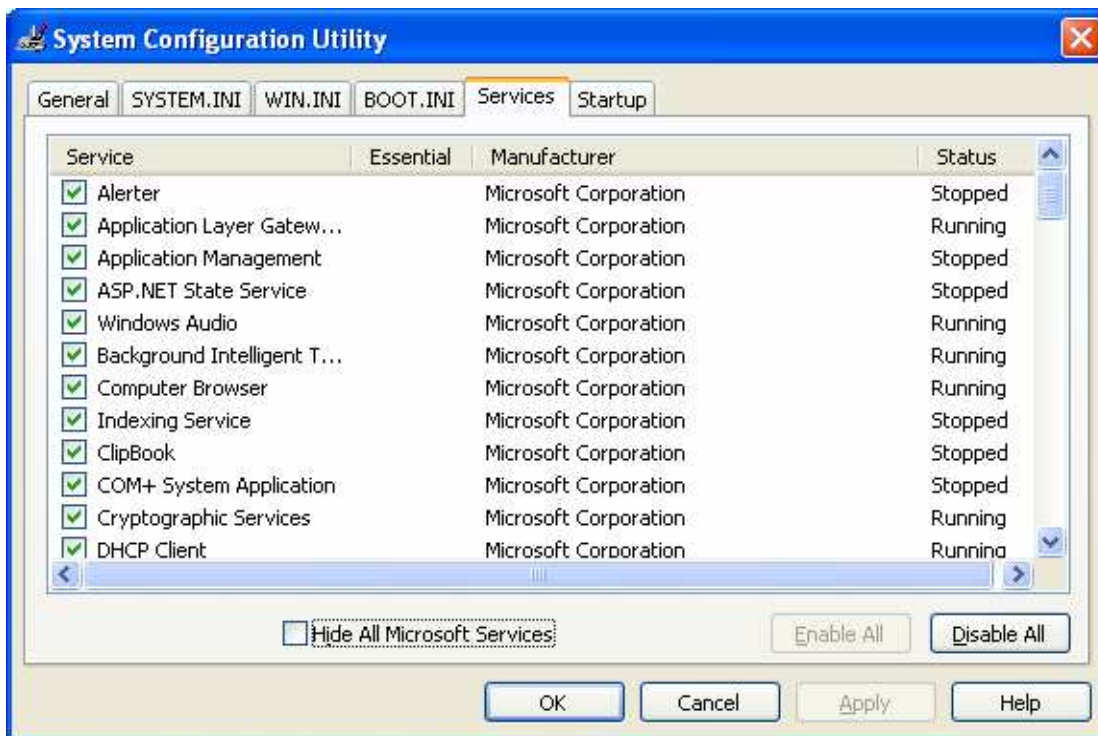
Go to Start => Run => Type "msconfig" (without quotes) => Press Enter
Select the option "Diagnostic Startup" (view **Screenshot 3.1.3.a**) in the "General" tab.

Screenshot 3.1.3.a (msconfig window)



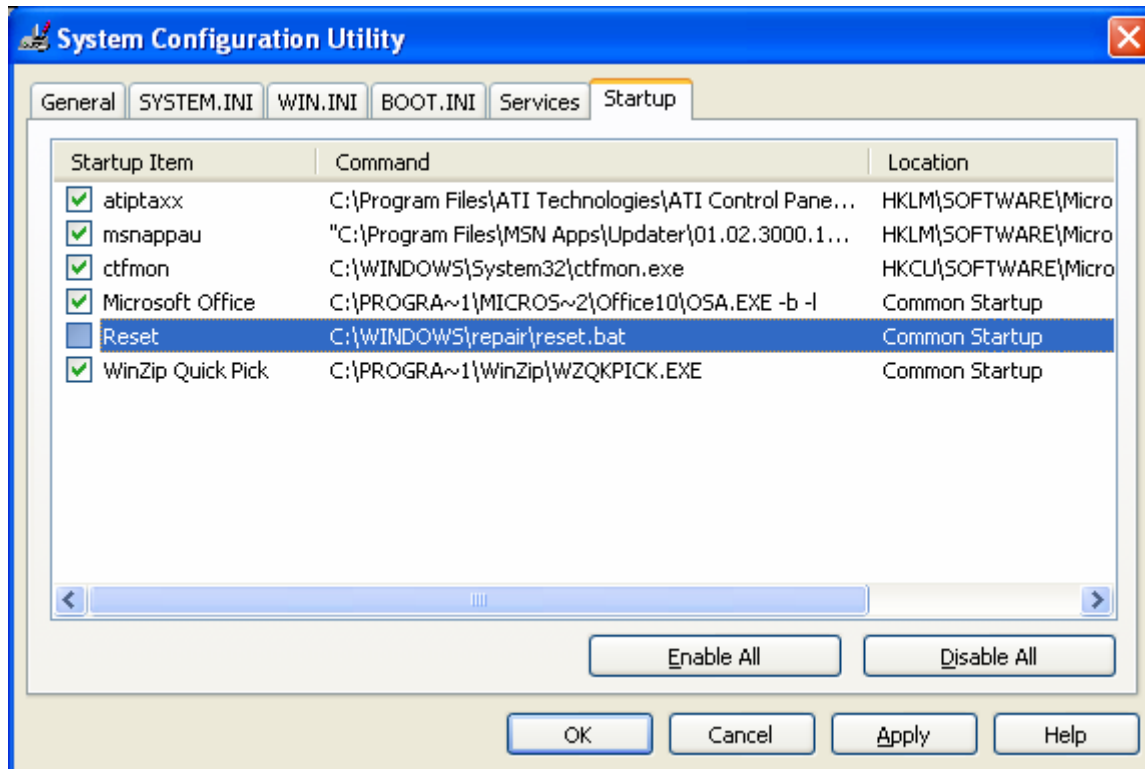
Switch to “Services” tab (view Screenshot 3.1.3.b). Click “Enable All” and check click "Hide Microsoft services".

Screenshot 3.1.3.b (msconfig window – services tab)



Now switch to “Startup” tab (view **Screenshot 3.1.3.c**). Un-check all unnecessary startup items or any suspicious startup file. Now press “OK” button in “msconfig”.

Screenshot 3.1.3.c (msconfig window – startup tab)



- d. In some versions of windows (e.g. Windows 2000) “msconfig” is not present. In that case one has to remove the un-necessary startup files manually. Startup items can be manually removed from the following locations:
Start => Programs => Startup => Right click item => delete or it can be found at C:\Documents and Settings\All Users\Start Menu\Programs\Startup

Similarly, the un-necessary services have to be disabled manually in the “services.msc” manually.

To disable the un-necessary services manually Go to Start => Run => Type “services.msc” (without quotes) => Press Enter. Then right click the service that has to be disabled => properties => stop (if running) => disable => press enter.

- e. Most of the malicious programs make entries in the registries to start on system boot. These entries can be found in the following locations:

HKEY_LOCAL_MACHINE => Software => Microsoft => Windows => CurrentVersion => Run
HKEY_LOCAL_MACHINE => Software => Microsoft => Windows => CurrentVersion =>
RunOnce
HKEY_LOCAL_MACHINE => Software => Microsoft => Windows => CurrentVersion =>
RunServices (Only for windows 9x/ME)

and

HKEY_CURRENT_USER => Software => Microsoft => Windows => CurrentVersion => Run

To remove the entries from the registries, go to Start => Run => Type “regedit” (without quotes) => press enter. Then go to the above mentioned keys and delete all un-necessary entries.

- f. Purge recycle bin and restart window in normal mode. Connect to internet and update the Anti-Virus signature and once the signatures are up-to-date then a complete system scan should be done.
- g. Go to Start => Run => Type “msconfig” (without quotes) => Press Enter. Select the option "Normal Startup" (view Screenshot 3.1.3.a) in the “General” tab and press OK. Reboot the system again into normal startup.

Note: To get detailed information of any particular virus / worms, one can visit any commercial anti-virus products sites. These sites also contain further details of manual removal techniques for any virus / worm.

Visit the following links to download free viruses / worms removal tools:

Microsoft Security Tools

<http://www.microsoft.com/technet/security/tools/default.mspx>

McAfee

<http://vil.nai.com/vil/stinger/>

McAfee AVERT Tools

<http://vil.nai.com/vil/averttools.asp>

4. Countermeasures Against Malicious Codes

Countermeasures for corporate end-users or home pc users:

- The desktop Anti-Virus (AV) signature must be kept up-to-date.
- Don't open attachments unless you are sure of its authenticity.
- Make sure the system is updated with the latest security patches. To install any windows related patches visit <http://windowsupdate.microsoft.com/>.
- If possible install a desktop based firewall (e.g. sygate or zone-alarm etc).
- Always do a virus scan for any external drives when attached to the system
- Never download any free tools if you are not sure of it's authenticity
- Always stay tuned with latest virus alerts or outbreaks

Countermeasures for corporates security administrators:

- The AV gateway must have the entire signature up-to-date to be pushed into its client PCs.
- A content filter at the SMTP gateway is always advisable
- Desktops attached to the corporate network must be installed with latest security patches
- There must be a patch management system like (SMS or SUS) in place and the systems must be updated with the latest security patches.
- Conduct anti-virus schedule scan on all the desktops attached to the corporate network
- An IDS if installed would be a great device to keep you alerted about any attacks in the network but it would be really helpful if an IPS can be afforded.
- Big organization that has huge amount of network devices and servers to manage must use Security Information Management (SIM) systems like NetIQ, ArcSight or NetForensic etc. This make the job easy for a security administrator to monitor huge networks for any kind of security alerts.
- Security should not be confined to just perimeter level but rather it should also be considered seriously at the desktop level which are attached to the corporate network.
- Conduct end-users training to make them aware of various risks related to virus or worms attacks.
- Last but not the least always stay tuned with latest virus alerts or outbreaks

5. Conclusion

The purpose of writing this article is to educate various categories of computer users like ordinary end-users to expert security professionals to handle any threats from viruses / worms by demonstrating those different possible ways that viruses and worms use to evade any Anti-Virus products. Virus coders will always look for different ways and means to evade any anti-virus products and infect the systems but I must always say user's awareness & user's responsibility is enough to defend any kind of malicious program attacks rather than just having an anti-virus with the latest signatures.

6. About Author

There is nothing much to talk about me other than my research work on which I spend several hours a day. My focus area is vulnerability research and malicious program (viruses/worms/malware) analysis.

To know more about me, visit my site www.hackingspirits.com.

For any feedback and comments, mail me at:

debasis_mty@yahoo.com or mail@hackingspirits.com.

Debasis Mohanty
www.hackingspirits.com
