CERT-In

Indian Computer Emergency Response Team

ANTI VIRUS POLICY & BEST PRACTICES

Department of Information Technology
Ministry of Communications and Information Technology

Government of India

1.0 Introduction:

What is a Computer Virus?
Computer viruses are data destructive programs written with the intent of copying and spreading the destruction to other computers and programs.

2.0 Computer virus types
Viruses are classified depending on how they infect the computer systems on a network and they are of the following types.

2.1 Boot Viruses
They attack the boot record, the master boot record, the File Allocation Table (FAT), and the partition table of a computer hard drive. They generally propagate from a infected diskette placed in the disk drive of a computer while it starts or otherwise.
Joshi and Michelangelo are examples of boot sector viruses.

2.2 File Viruses (Trojan Horse)
Trojan horse, also called RAT (remote access Trojan, or remote access trapdoor) are examples of file virus. They attack program files (e.g. .exe; .com; .sys, .drv; .ovl; .bin; .scr etc.) by attaching themselves to executable files. The virus waits in memory for users to run another program and use the event to infect and replicate.

2.3 Macro virus
These virus attack programs that runs macros. Most common are in Microsoft word documents. These virus starts when a document or a template file in which it is embedded is opened by an application. Example: Melissa.

2.4 Stealth Viruses
These disguise their actions and can be passive or active. Passive viruses can increase the file size yet present the size of the original thus preventing detection, while active ones attack the anti virus software rendering them useless. Example: Tequila.

2.5 Multipartite Viruses
These have characteristics of both the boot and program viruses.
Example: Natas

2.6 Encrypted virus
These have built in encryption software code that mask the viral code making it difficult to identify and detect the virus.
Example: Cascade

2.7 Polymorphic Viruses
These are growing rapidly and have a inbuilt mechanism that changes the virus signature.
Example: SMEG

2.8 Worms
A worm is a independent program that reproduces by copying itself from one system to another usually over a network. They infiltrate legitimate programs and alter or destroy data. Unlike other virus worms cannot replicate itself.

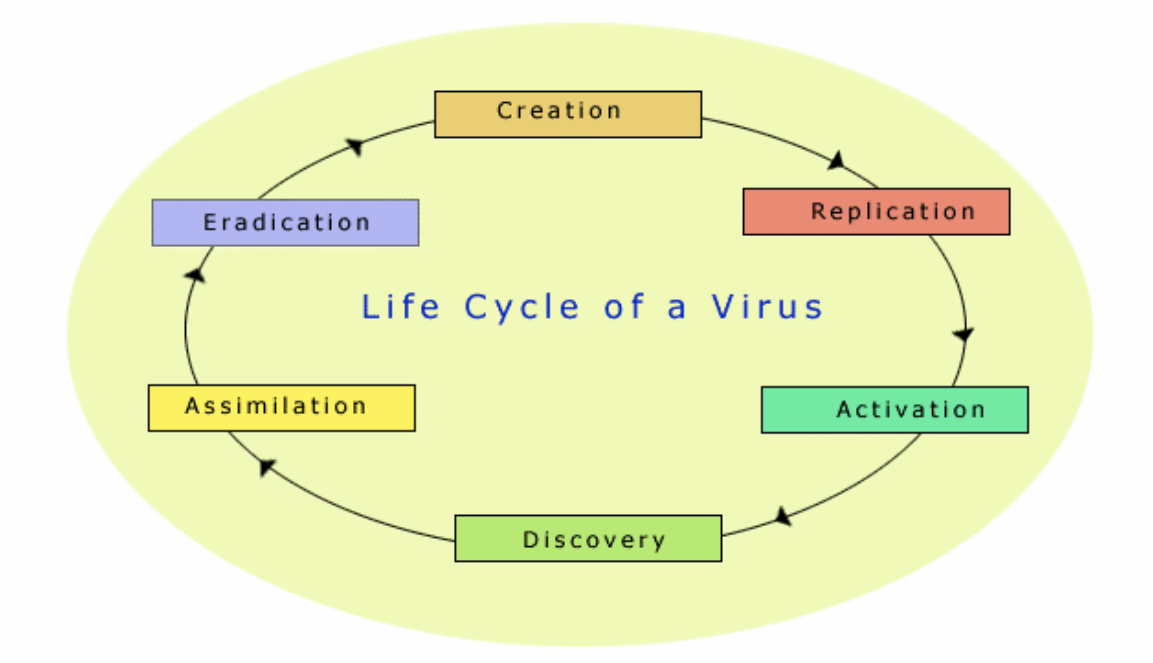
2.9 Logic Bombs
Logic Bombs are programs that are triggered by a timing device such as a date or an event and are highly destructive.

3.0 Symptoms of a Infected Computer
The following are common symptoms of a computer infected with a virus:

1. The computer fails to start
2. Programs will not launch or they fail when simple commands are performed
3. Names of files are changing or become unreadable
4. File contents change or are no longer accessible
5. Unusual words or graphics appear on the screen
6. Hard or floppy disks are formatted
7. Variations occur in computer performance, such as slowing down in loading or operation

4. 0 Need for eradication of Virus:
Some viruses are deliberately designed to damage files or otherwise interfere with your computer's operation, while others don't do anything but try to spread themselves around. But even the ones that just spread themselves are harmful, since they (generate a lot of traffic and slow down the network leading to the denial of critical services) damage files and may cause other problems in the process of spreading. This may cause loss to individuals/organizations which may be massive. Hence the need for eradication of viruses.

5.0 Virus Life Cycle:



6.0 Deployment of Antivirus:

1. For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed.
2. In a networked environment, an antivirus server should be deployed and all the workstations should have the corresponding antivirus client. It is recommended that all these clients be configured from the central antivirus server for routine tasks such as updation of antivirus signatures, scheduled scanning of the client workstations. The management of the client workstations should be done centrally from the antivirus server in order to have a centralized monitoring of all the activities.
3. Identify all the possible entry points in the network through which a virus attack is possible and all the traffic entering the network through these points should be routed via an antivirus gateway application for monitoring all the types of traffic flowing through the network, whether be it HTTP, FTP, SMTP or POP3. This ensures that the risk of any virus entering the network by any means is greatly reduced.
4. Application based Antivirus should be installed for applications like MS-Exchange, Lotus Notes etc.

7.0 Integration of Antivirus with Other Tools

1) Content Filtering:
Mobile Malicious Code like unsigned ActiveX, MIME, java applets are routes of possible virus infection. Content Filtering should be used for protocols like HTTP/SMTP/POP3/FTP. Antivirus Software is to be integrated with Content Filtering Software.

2) Firewall :
A firewall with Antivirus support will give additional security for the network.

8.0 Best Practices:

The suggested best practices for keeping PC's free from a possible virus attack.

1. A good anti-virus product should be chosen for the organization. A centralized server based antivirus system is suggested for an organization with a computer network.
2. The latest version of the antivirus with the latest signature is required to be loaded in all the machines of the organization. This is important as new and more potent viruses are discovered every day and even a few month old anti virus program may be ineffective against newer viruses.
3. For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
4. For a networked environment there must be a central server to check for viruses' in all the machines automatically.
5. The following schedule is suggested for a full scan of the PC's.
    a. Servers: Daily
    b. Workstations: Daily

    Schedule the operation when there is least human interaction with the work stations.
6. The antivirus software should auto-update virus signatures automatically from the service providers, as and when an update of signature or virus engine is available.
7. External media (ex. Floppy, CD's) is one of the most potent medium for transmission of viruses', hence it must not be used in the network except for a few pre determined PC's.
8. Anti-virus logs should be maintained for a period of 7-15 days or as determined by the policies of the organization. Ideally a weekly analysis of the logs should be done to obtain an infection profile of viruses and the machines infected.
9. Unneeded services should be turned off and removed. By default many operating systems install auxiliary services that are not critical e.g. an FTP, telnet or a web server. These services are avenues to attack. If these services are stopped, blended threats have less avenues of attack and the system administrator has a fewer services to maintain.
10. Enforce a password policy. Complex password makes it difficult to crack password files on compromised systems/computers. This helps to prevent damage when a computer is compromised.
11. The mail server is one of the easiest routes for virus attack through e-mail attachments. Mail server should be configured to block or remove email that contains attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif, and .scr files.
12. To prevent spamming to mails in the organization, mails only authenticated by users in your organizations should be allowed.
13. Do not allow mails from servers that have an open relay, the data base of such servers can be accessed from various sites like mail-abuse.org.
14. All employees must be made aware of the potential threat of viruses and the various mechanisms through which they propagate.
15. Employees must be trained not to open attachments unless they are expecting them.
16. Do not allow user to execute software downloaded from internet unless certified safe by system administrator.

17. The latest patches for web browsers have to apply or else simply visiting a compromised web site can cause infection.
18. If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
19. Always keep patch level up-to-date, especially on computer that host public services and are accessible through the firewall. Such as HTTP, FTP, mail and DNS services.
20. Since all online viruses arrive from the internet, a good antivirus software should be loaded at the logical gateway of the network.
21. In the case of a virus attack the following steps are required to be taken.
    a. The network share of the machine has to be stopped
    b. The contact person for cleaning the machine of virus has to be notified
    c. There must be a mechanism where an authorised expert/work station is notified automatically in case of a virus attack.
22. The notified expert should perform the following action on the infected work station.
    a. Determine the type of virus
    b. Isolate all infected systems and floppy disks
    c. Try to clean the infected file
    d. In case of failure above the file should be deleted from the work station.
    e. In case of failure above the work station should be removed from the network and remedial action taken.
    f. Remedial action may include reformatting depending on the severity of the problem and as per specific policy of the company.

References:

1. www.nai.com
2. www.symentac.com
3. www.trendmicro.com
4. www.bullguard.com