National Computer Board

ANTIVIRUS BEST PRACTICES

ANTIVIRUS BEST PRACTICES

1. INTRODUCTION

This guideline covers the basics on Antivirus Software and its best practices. It will help to have an overall understanding of the subject and tips to safeguard against the dangers of viruses.

1.1. What is a Virus?

A virus is a piece of code that attaches itself to a program or file so it can spread from one system to another. It may damage software, files and even hardware. In order to replicate itself, a virus must be permitted to execute code and write to memory. For this reason, many viruses attach themselves to executable files that may be part of legitimate programs. If a user attempts to launch an infected program, the virus code may be executed simultaneously.

A virus can run as an application, therefore it can:

- Remotely access a computer, giving anyone complete control of the machine.
- Run as a background process, using internet connection to send private data anywhere, anytime.
- Delete files, run programs, edit registry and steal information.
- Corrupt Windows files to make a machine become unusable, causing it to crash and turn off at any time.
- Key log information such as passwords, usernames and credit card details.

1.2. Types of Viruses

- **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 an infected diskette placed in the disk drive of a computer while it starts or otherwise.
  Joshi and *Michelangelo* are examples of boot sector viruses.

- **File Viruses (Trojan Horse)**
  They attack program files (e.g. .exe; .com; .sys, .drv; .ovl; .bin; .scr) 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.
  Trojan horse, also called RAT (remote access Trojan, or remote access trapdoor) is an example of a file virus.

- **Macro virus**

  This virus attacks applications that run macros, for example Microsoft word. The virus is activated when a document or a template file in which it is embedded, is opened by an application. Example: *Melissa*.

- **Stealth Viruses**

  These viruses can disguise their actions and can be passive or active also. The passive viruses can increase the file size yet present the size of the original file, thus preventing detection. The active ones attack the antivirus software rendering them useless. Example: *Tequila*.

- **Encrypted virus**

  This virus has inbuilt encryption software code which masks the viral code making it difficult to identify and detect the virus.

  Example: *Cascade*

- **Polymorphic Virus**

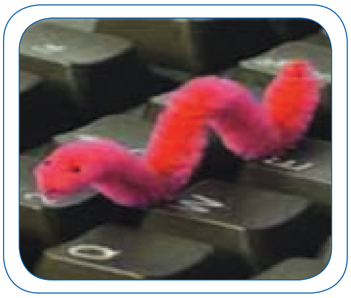
  Polymorphic virus has an inbuilt mechanism that can alter the virus signature. During the process of infection, it creates slightly modified and fully functional copies of itself. This is primarily done to elude the detection of a virus scanner as some are not able to identify different instances of an infection. One method it commonly uses to bypass a scanner involves self-encryption performed with a variable key.

  Example: *SMEG*

- **Worms**

  A worm is an 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.

  Examples: *SQL Slammer Worm, Melissa worm, Mydoom*.



1.3. Sources of Viruses

- **Storage devices: CDs, floppies, mobile disks**

  Floppy disks can have a virus in the boot sector. They can also hold infected programs or documents. When shared with other users, through a network or the infection can spread very quickly.

- **E-Mail**

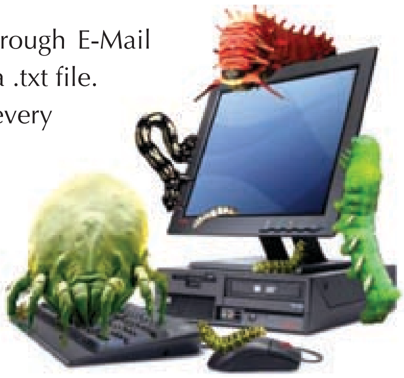
  E-Mail messages can include infected attachments. Double-clicking on an infected attachment can infect a machine. Certain E-Mails even include malicious scripts that run as soon as it is previewed.

- **The Internet**

  Infected programs or files can be downloaded through the internet. Vulnerabilities found in operating systems can also allow viruses to infect a computer via the internet, without the user's knowledge.

1.4. Examples of common Viruses and their effects

- ***Nimda:*** Nimda is one of the most popular viruses, as it has used almost every possible method to spread very effectively. Within 22 minutes, it became the Internet's most widely spread virus. The virus spells 'admin' if reversed.



- ***ILOVEYOU:*** The ILOVEYOU virus was massively spread through E-Mail which would be sent to recipients with what appeared to be a .txt file. Once opened, it would run a .vbs script and send itself to every contact in the victim's address book.
- ***Sasser:*** The Sasser virus carried itself across network computers causing whole systems and companies to go down, reportedly causing over $500 million damage to businesses.
- ***Blaster:*** This virus exploited a Windows vulnerability causing the system to shut down. A message would appear on the screen indicating that in 30 seconds the computer will turn off.
- ***MyDoom:*** This is one of the most famous viruses of all time which spread via E-Mail. The E-Mail was sent with an apparent failure message *(e.g. Error, Mail Delivery System, Mail Transaction Failed)* containing an executable. When ran, it would send itself to all E-Mail addresses found in the victim's contact list. It also opened up a backdoor on the machine, which could be exploited by hackers.

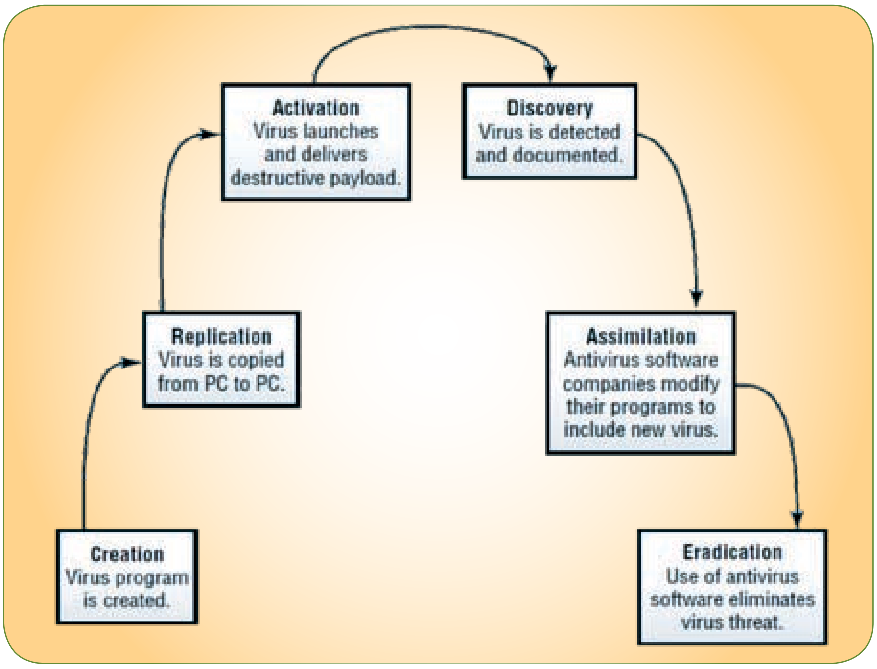
2. SYMPTOM OF INFECTED SYSTEMS

Viruses operate in a multitude of ways. Some will stay active only when the application it is attached to, is running while others will run whenever the machine is on.
Common symptoms of Infected Systems are:

- The computer runs slower than usual.
- Computer applications are not working right.

- Disk drives and disks become inaccessible
- Printing failure.
- Unusual, error messages are displayed.
- Dialog boxes and menus are distorted.
- Double extensions detected on recently opened attachments (e.g. gif, jpg, vbs).
- Antivirus program is suddenly disabled or cannot be restarted.
- Antivirus programs cannot be installed.
- New and unusual icons appear on desktop.
- Strange music or sounds play from the speakers.
- A common application suddenly disappears from the computer without the user purposely removing it.
- The computer stops responding, or it locks up frequently.
- The computer crashes, and then it restarts every few minutes.
- The computer restarts on its own and does not run as usual.
- Out-of-memory error messages appear even though the computer has sufficient RAM.
- A disk utility such as Scandisk reports multiple serious disk errors.
- A new partition disappears.
- Windows Task Manager cannot be started.
- Common folders become hidden.

3. LIFE CYCLE OF A VIRUS


Activation
Virus launches and delivers destructive payload.
Discovery
Virus is detected and documented.
Replication
Virus is copied from PC to PC.
Assimilation
Antivirus software companies modify their programs to include new virus.
Creation
Virus program is created.
Eradication
Use of antivirus software eliminates virus threat.

4. ANTIVIRUS SOLUTIONS

4.1 Antivirus

Antivirus software is used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. A variety of strategies are typically employed by Antivirus software.

*Signature-based **detection*** involves searching for known patterns of data within executable code. However, it is possible for a user to be infected with new malware for which no signature exists yet.

To counter such so-called zero-day threats, **heuristics** can be used.
One type of heuristic approach, generic signatures, can identify new viruses or variants of existing viruses by looking for known malicious code (or slight variations of such code) in files.

Some antivirus software can also predict what a file will do if opened/run by ***emulating it in a sandbox and analyzing*** what it does to see if it performs any malicious actions. If it does, this could mean the file is malicious.

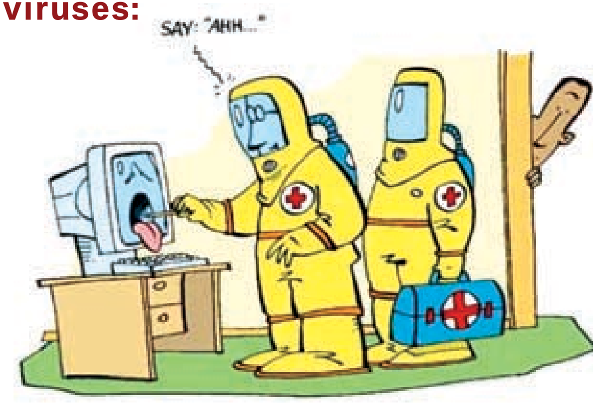
4.2 Deployment of Antivirus

- For Laptop and Standalone Machine, Desktop Antivirus with Latest Update should be installed.
- 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 updating of antivirus signatures and 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.

- 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.
- Application based Antivirus should be installed for applications such as MS-Exchange and Lotus Notes.

4.3 Some examples of Popular Antiviruses:

- Norton Antivirus (Symantec)
- McAfee Antivirus
- Bitdefender
- Trend Micro
- AVG



5. INTEGRATION OF ANTI-VIRUS WITH OTHER SECURITY TOOLS

- ***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 should be integrated with Content Filtering Software.
- ***Firewall***
  A firewall with Antivirus support will give additional security to the network.

6. ANTI-VIRUS BEST PRACTICES

- 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. This is important as new and more potent viruses are discovered every day and even a few months old program may be ineffective against newer viruses. The latest version of the antivirus with the latest signature is required to be loaded in all the machines of the organization.
- For standalone PC's the antivirus software loaded into PC should be automatically enabled for checking viruses.
- For a networked environment there must be a central server to check for viruses' in all the machines automatically.

- The following schedule is suggested for a full scan of the PC's.
  - Servers: Daily
  - Workstations: Daily
  - Schedule the operation when there is least human interaction with the work stations.
  - 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- To prevent spamming to mails in the organization, mails only authenticated by users in the organizations should be allowed.
- 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.
- All employees must be made aware of the potential threat of viruses and the various mechanisms through which they propagate.

7. REFERENCES

CERT-IN - www.cert-in.org.in
Media Wiley - http://media.wiley.com
NIST - www.nist.gov

CERT–MU

A division of the National Computer Board

In Collaboration with

IT Security Unit
Ministry of Information
and Communication Technology

Mauritian Computer Emergency Response Team

National Computer Board
7th Floor, Stratton Court
La Poudrière Street, Port-Louis, Mauritius
Tel: (230) 2105520 | **Fax:** (230) 2080119

Email: info@cert-mu.gov.mu
CERT-MU Website: http://cert-mu.org.mu