Introduction to Computer Viruses

What is a Computer Virus?

A computer virus is a small program that can be spread from one computer to another and can even affect a computer's operations. Such viruses can modify or destroy any data stored on a computer. Most viruses nowadays are executable files that attach themselves to emails and spread from one computer to another. Once executed or opened, these viruses will spread to other applications or computers.

Most common forms of Virus

There several types of viruses, or malware, which include Spyware, Adware, Trojan Horses, and Worms. All these types of malware can destroy or steal your data without your knowledge.

Spyware – One of the most common types of virus. These collect user data/information and details on the operation of computers without the knowledge of the computer's owner/user (This might include data or services accessed, web browsing data, etc.).

Adware – These display advertisements on your display by installing itself on a computer without a user's permission. Adware will track internet usage data and habits of the user.

Trojan Horses – This type of virus cannot self-activate, and are harmful programs that disguise themselves as useful at first, but will collect personal data in the background and wait for an exact date or time to begin exploiting and harming the computer.

Worms – These are different from traditional viruses. They do not need human interaction to spread from one computer to another. Worms have the ability to self-activate within a computer. For example, they will create thousands of copies of itself and send emails to all email addresses in the computer's address book. This will repeat in other computers, and due to this, worms can spread automatically at a rapid rate within a computer network.

How do viruses enter a computer?

Computer viruses can be easily spread via emails and email attachments. Most email viruses are disguised in a very attractive manner (e.g. photos, audio and video files, e-greetings cards etc.). Unwitting users can fall prey to such tricks perpetrated by attackers. Users must be very careful when opening suspicious emails, and those from unknown parties. It is better to avoid opening them. One should also be careful when downloading files from the Internet, as they may contain viruses.

Symptoms of a virus infection on a computer

- The computer will start to slow down without good reason
- The computer will abruptly restart itself often and will show abnormal behavior
- Applications installed on the computer will not function as expected
- There might be unusual (typically badly written) error messages.
- There might be new shortcuts or other icons in the computer that were not created by the user
- Users may find that their files or applications have been deleted without their permission.

How can a computer be protected from virus attacks?

- Use a firewall when using the Internet
- Update all software and the operating systems on all computers when necessary
- Use an up-to-date anti-virus software
- Do not open emails that are received from unknown sources
- Do not open unknown attachments or content (links etc.) even from a known source
- Complete a virus scan before opening any email attachments
- Do not visit unknown or suspicious websites
- Do not share your personal details with unknown parties or services (your email, bank accounts, credit card numbers etc.)
- Use trusted websites to download applications or content

What is a firewall?

A firewall is a software or a hardware device that checks information that is received from the Internet or a network, and either blocks it or allows it to pass through to a computer, depending on the firewall settings. For example, a firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet. A firewall can also help stop your computer from sending malicious software to other computers.

Users can install a firewall to their personal computers to protect them from virus attacks from the Internet. A firewall checks all data going through it and allows it to reach its destination, or denies data from reaching the destination, depending on the set of rules defined by an authorized user.

What is an Anti-Virus software?

An anti-virus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software such as viruses and worms. Up-to-date anti-virus software helps users against the latest virus threats.

How does anti-virus software work?

Anti-virus software typically uses two different techniques to find and remove viruses:

- Virus Dictionary Approach
- Suspicious Behavior Approach

Virus Dictionary Approach

In the virus dictionary approach, when an anti-virus software examines a file, it refers to a dictionary of known viruses that have been identified by the author of the anti-virus software. If a piece of code in the file matches any virus identified in the dictionary, then the anti-virus software can then either delete the file, quarantine it so that the file is inaccessible to other programs and the virus is unable to spread, or attempt to repair the file by removing the virus itself from the file. To be successful in the medium and long terms, the virus dictionary approach requires periodic online downloads of updated virus dictionary entries. This will minimize the risk of known virus attacks on your computer.

Suspicious Behavior Approach

The suspicious behavior approach, by contrast, doesn't attempt to identify known viruses, but instead monitors the behavior of all programs. If a program tries to write data to another executable program, for example, this is flagged as suspicious behavior and the user is alerted to this, and asked what to do. Unlike the dictionary approach, the suspicious behavior approach therefore provides pro-active protection against brand-new viruses that do not yet exist in any virus dictionaries.

Factors to be considered when selecting anti-virus software

Today, there are a lot of anti-virus software product companies. Selecting an anti-virus software to protect a computer will depend on users' requirements. There are, however, some considerations to be made when selecting an anti-virus software.

- Whether it can update itself automatically
- Whether the software product owner is provided a detailed updates summary
- Whether the software can be integrated with the email software
- Whether it can scan for viruses automatically

- Whether the software product owner is provided accurate and updated information about new viruses

Some of the most popular and commonly used anti-virus software today

1 Kaspersky Lab	6 Trend Micro
2 McAfee	7 F-Secure
3 Symantec	8 Sophos
4 Avast	9 Bitdefender
5 ESET	10 Microsoft Security Essentials

If you have any questions, please inform us:

https://techcert.lk/en/report-form
Tel - +94 11 4 462 562
e-mail - help@techcert.lk

This document was prepared by the Training Division of LK Domain Registry in collaboration with the Internet Society Sri Lanka Chapter.
For more details please visit http://nic.lk/index.php/training-materials.