Practical No 7

Aim : -

Study different approaches for Anti-virus software and write one document.

a. Examine files to look for viruses by means of a virus dictionary.
b. Identifying the suspicious behaviour from any computer program which might indicate infection.

Theory : -

Definition

Software that is created specifically to help detect, prevent and remove malware (malicious software).

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. Once installed, most antivirus software runs automatically in the background to provide real-time protection against virus attacks.

Comprehensive virus protection programs help protect your files and hardware from malware such as worms, Trojan horses and spyware, and may also offer additional protection such as customizable firewalls and website blocking.

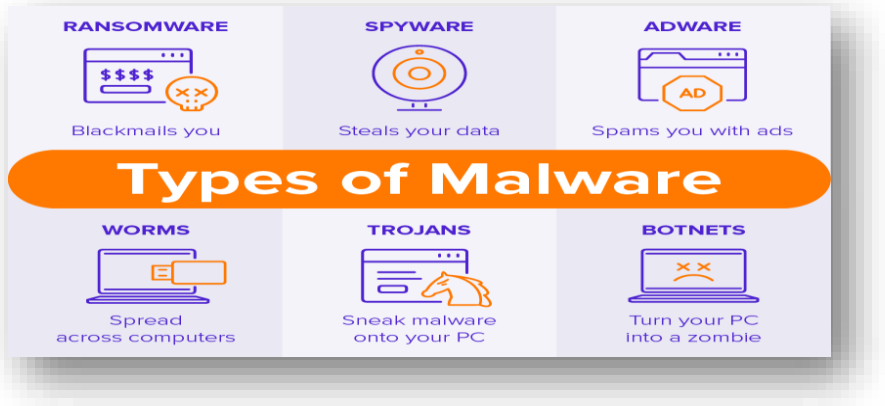
Common types of cyber threats

As the Internet of Things (IoT) grows, so does the risk of cybercrime for mobile phones and other internet-connected devices, not just your personal computer. According to Symantec's Internet Security Threat Report 2018, malware for mobile devices including spyware, ransomware and viruses increased 54% in 2017; and data breaches and identity theft are also on the rise.

What is malware?

Malware, short for "malicious software," is a blanket term that refers to a wide variety of software programs designed to do damage or do other unwanted actions to computer, server or computer network Common examples include viruses, spyware and trojan horses. Malware can slow down or crash your device or delete files.

Criminals often use malware to send spam, obtain personal and financial information and even steal your identity.

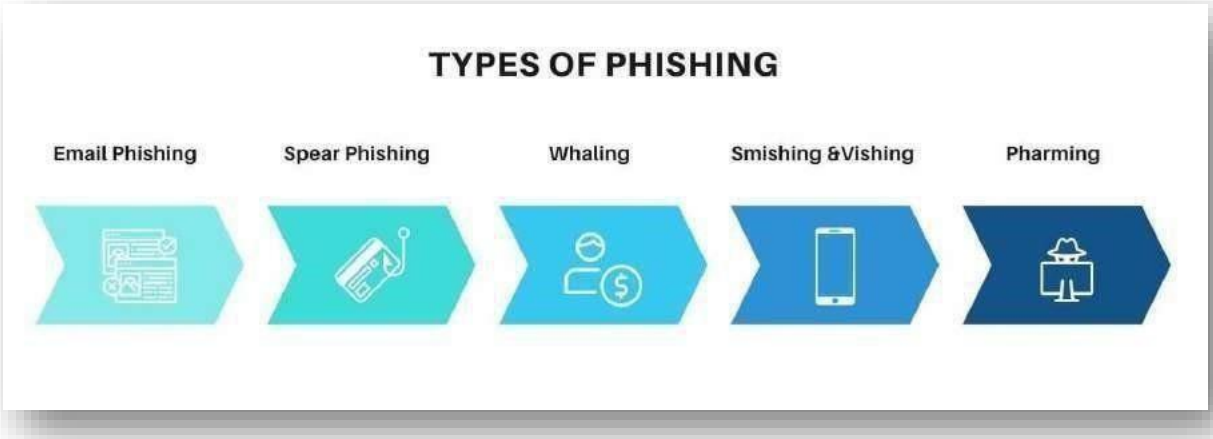


What is spyware?

Spyware is a type of malware that attaches itself and hides on a computer's operating system without your permission to make unwanted changes to your user experience. It can be used to spy on your online activity and may generate unwanted advertisements or make your browser display certain website sites or search results.

What is phishing?

Phishing attacks use email or fraudulent websites to try to trick you into providing personal or financial information to compromise an account or steal money by posing as a trustworthy entity. They may claim there's a problem with payment information or that they've noticed activity on an account and ask you to click on a link or attachment and provide personal information.



Antivirus programs and computer protection software

Antivirus programs and computer protection software are designed to evaluate data such as web pages, files, software and applications to help find and eradicate malware as quickly as possible.

Most provide real-time protection, which can protect your devices from incoming threats; scan your entire computer regularly for known threats and provide automatic updates; and identify, block and delete malicious codes and software.

Because so many activities are now conducted online and new threats emerge continuously, it's more important than ever to install a protective antivirus program. Fortunately, there are a number of excellent products on the market today to choose from.

How does antivirus work?

Antivirus software begins operating by checking your computer programs and files against a database of known types of malware. Since new viruses are constantly created and distributed by hackers, it will also scan computers for the possibility of new or unknown type of malware threats.

Typically, most programs will use three different detection devices: specific detection, which identifies known malware; generic detection, which looks for known parts or types of malware or patterns that are related by a common codebase; and heuristic detection, which scans for unknown viruses by identifying known suspicious file structures. When the program finds a file that contains a virus, it will usually quarantine it and/or mark it for deletion, making it inaccessible and removing the risk to your device.

Different Detection Methods

Sandbox Detection

This detection method is similar to a behavioral based detection method. It executes programs in a virtual environment and logs what action the program performs instead of detecting at run time, the behavioural fingerprint (Antivirus Software). Identification of the programs maliciousness by the antivirus software is enabled by verifying the actions of the program that are logged in (How antivirus software works: Virus detection techniques).

Data Mining Techniques

As one of the latest approach applied in malware detection, data mining techniques are used to attempt to classify behaviour of a file as either malicious or not. This is achieved given a series of file features which are extracted from a file itself (Antivirus Software).

Heuristic based Detection

In many cases, viruses are mutated or refined by other attackers following the single infection and can grow into dozens of slightly different strains called variants. The detection and removal of multiple threats using a single virus definition are called generic detection. It may seem like an advantageous endeavor to identify a specific virus but it can be much quicker to detect a virus family through a generic signature. Another quick way is to use an inexact match to an existing signature. Common areas that all viruses in a family share uniquely are found by virus researchers and are observed of where they can create a single generic signature. Non-contiguous code, are often contained by these signatures by using wildcard characters where differences lie.

The scanner can detect viruses even if they are padded with extra and meaningless code with these wildcards. In summary, heuristic based detection statically examines files for suspicious characters without an exact signature match to detect new malware. This tool does not noticeably slow down the system. A downside of this is that it can sometimes flag legitimate files as malicious inadvertently (How antivirus software works: Virus detection techniques).

Behavioural based Detection

Instead of merely emulating an execution, behavioral detection observes how a program executes. It identifies malware by looking for suspicious behaviors and unpacks malcode while modifying host files or observing keystrokes. The antivirus tool can detect the presence of previously unseen malware by noticing such actions on the protected system. These actions are not sufficient to classify the program as malware but when they are taken together, they could indicate so (How antivirus software works: Virus detection techniques).

Signature based Detection

Signature based detection is heavily reliant on signatures to identify malware. This detection method creates a static fingerprint of known malware using key aspects of examined files. This signature can represent a series of bytes in a file or a cryptographic hash of the file or its sections. One of the limitations of this method is that for signatures which have not yet developed, it will be unable to flag those malicious files. Creations are frequently mutated by modern attackers to retain the malicious functionality (How antivirus software works: Virus detection techniques).

Rootkit Detection

The definition of a rootkit is a type of malware that is designed to, without being detected, gain administrative level control over a computer system. They are designed to change operating system functions and can possibly affect the anti-virus program as well as make it ineffective. These can be extremely tedious as they cannot be easily removed and can require the operating system to be completely reinstalled. This kind of detection basically attempts to scan for these rootkits (Mitra).

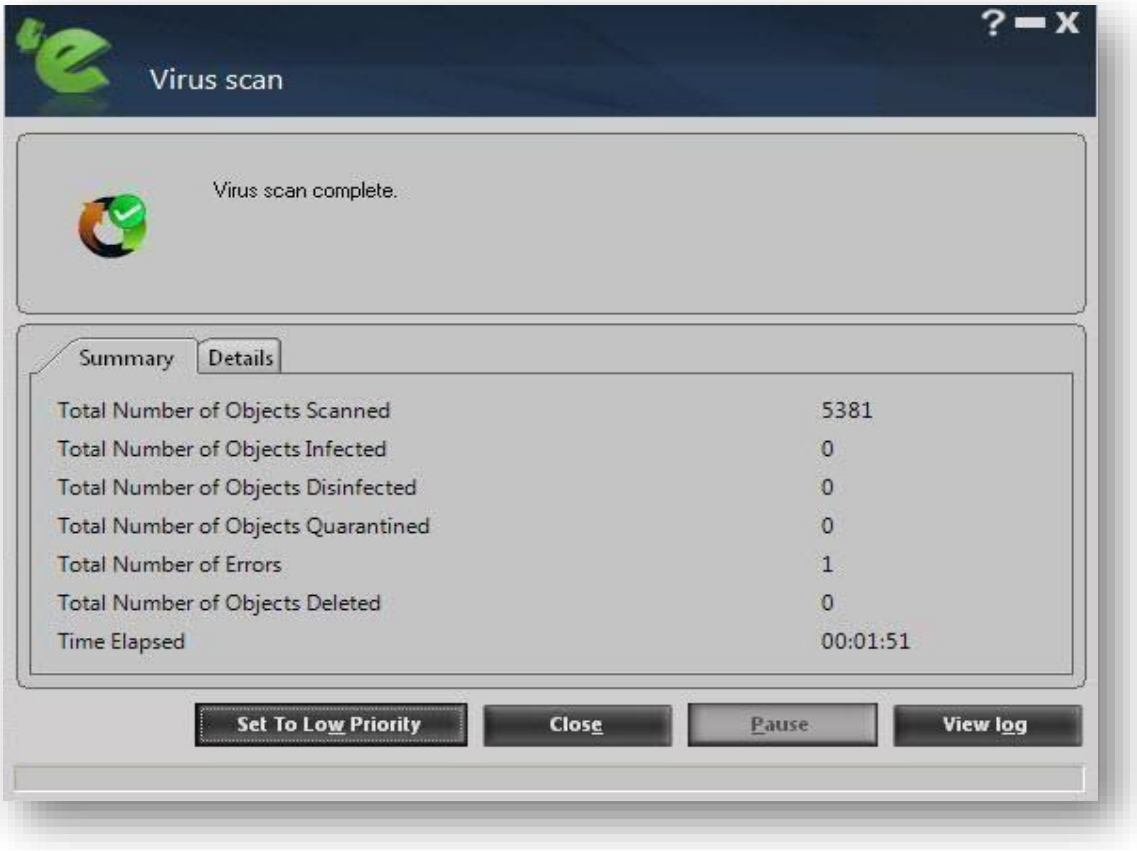
Exact Identification

The exact identification method searches and scans more than a number of constant bytes in the virus code which improves the virus detection in a number of false positives (Mitra).

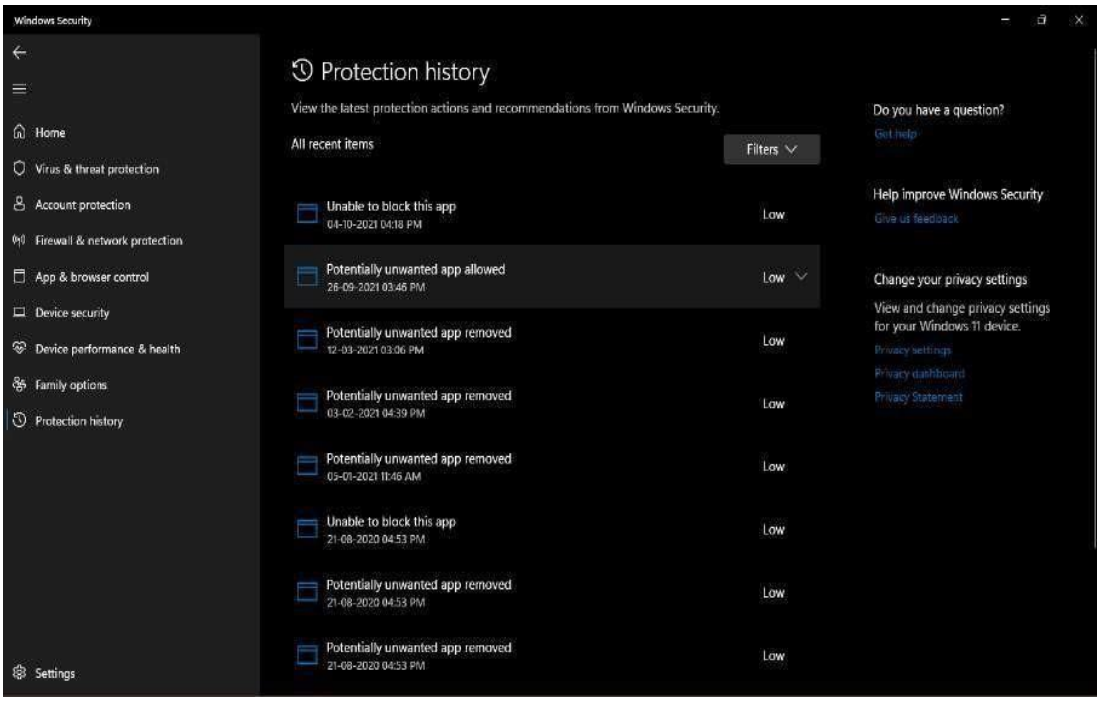
Static descriptor Detection

The static descriptor detection can be used to scan a particular virus so that the descriptor of virus can be detected (Mitra).

Virus Scanning log



Suspicious Behaviour From Different Apps:



Conclusion : - Hence we have Studied different approaches for Anti-virus software.