



Anti-Malware

Introduction Malicious software (**Malware**) is any executable code designed to disrupt or subvert a computer system. Malware includes Viruses, Worms, Trojan Horses, Spy-ware, Rootkits and some forms of Adware.

Overview Anti-Malware programs operate in two different modes: **detection and containment**.

- **Malware Detection** requires both anti-virus and anti-spyware software, these programs are able to recognize malware by comparing suspect software to a list of known malware or behaviors.
 - **Policy-Based** recognition is the identification of known and suspicious behavior patterns and file integrity checking. These products require frequent updates to their data files to ensure that the latest Malware can be identified during regular security scans.
 - **Behavior-Based** recognition is the identification of anti-malware through suspicious program activity. These products observe the behavior all software and can identify the inappropriate behavior exhibited by malware.
 - **File Integrity** Malware are often concealed within corrupted system files. In Checking anti-malware programs can detect even the smallest unauthorized changes to critical system files.
- **Malware containment** focuses on preventing the damage from malicious programs can do, it amounts to using safe computing practices such as:
 - Not executing programs of unknown origin.
 - Only using 'login' accounts with limited privileges.

Security Issues A **Rootkit** is malware that operates at the system level and represents a serious compromise of the systems security.

A Rootkit Detector typically operates within an infected system, but since Rootkits are developed to evade detection, it is good practice to use more than one Rootkit Detector. Rootkits are engineered

to compromise the operating system and are very difficult to remove.

To sanitize an infected system it is highly recommended that the operating system be reinstalled.

Malware authors try to evade detection by creating:

- **Encrypted Viruses and Worms** this hides its fingerprint - anti-malware software should be able to detect encrypted malware.
- **Polymorphic Viruses** are designed to change their contents every time they replicate altering its appearance so as to hide its signature and evade detection.
- **Virus Compression** is primarily intended to obscure the malware signature; most viruses propagate in compressed formats.
- Malware may also have **Multiple Layers of Compression** wherein it is packed multiple times using different technologies. Anti-malware solutions should be capable of detecting compressed malware.
- A **Zero-Day Exploit** is an attack that has never been seen before and therefore cannot be detected using conventional signature analysis.

Behavior-Based anti-malware products are able to identify malware based on its behavior, it provides some defense from Zero-Day Exploits and should be included in the overall anti-Malware solution.

Safe Computing Practices Anti-Malware data files should be updated on a daily basis.

However anti-malware programs are only part of the solution:

- Corporate policy should prohibit users from downloading or using unauthorized software.
- User accounts should have only limited system access privileges.
- Users should receive regular Security Awareness Briefings to be reminded of corporate security policies and practices.