Malicious software. Attacks and countermeasures, II

Antivirus Approaches

- **Prevention**: do not allow a virus to get into the system (in general, impossible to achieve);
- **Detection**: once infection has occurred, determine that it has occurred and locate the virus;
- **Identification**: once a virus is detected, identify it;
- **Removal**: once the specific virus has been identified, remove all traces of the virus and restores the infected programs to their original states.

Generations of antivirus software

- **First generation**: simple scanners;
- **Second generation**: heuristic scanners;
- **Third generation**: activity traps;
- **Fourth generation**: full-featured protection;

Simple scanners

- Require a virus signature to identify a virus;
- May detect viruses which have essentially the same structure and bit patterns in all copies;
- Signature-based scanners are limited to the detection of known viruses;
- May maintain a record of the length of programs and look for changes in length;
Heuristic scanners

• Rely on heuristic rules to search for probable virus infection.
• One may look for fragments of code that are often associated with viruses:
  • Encryption loop and a key in polymorphic viruses;
• One may use integrity checking:
  • Simple checksum;
  • Encrypted hash functions.

Activity detection

• Memory-resident programs that identify a virus by its actions in run time rather than by its signature or its structure;
• Here, it is not necessary to develop signatures and heuristics for various classes of viruses;
• It is necessary to identify the small set of indicative actions.

Fourth-generation antivirus packages

• Packages consisting of a variety of antivirus techniques used together:
  • Scanning;
  • Activity trap;
  • Control capability; etc
• Usually combined with other security defence systems (IDS, firewalls, etc)

Generic decryption and simulation

• Polymorphic viruses use encryption to hide malicious code;
• However, to execute such a code it has to be decrypted;
• Generic decryption (GD) tools are used to detect (fragments of ) viruses at the stage they are decrypted and ready to be executed;
• CPU simulator is used for this purpose.
**Generic decryption and simulation**

GD tools contain the following elements:
- **CPU simulator**: a software-based virtual computer. Instructions in an executable file are interpreted by the emulator not affecting underlying processor;
- **Virus signature scanner**: a module that scans the code looking for the signatures of known viruses;
- **Emulation control module**: controls the execution of the target code switching between simulation and scanning modes.

**Behaviour-Blocking software**

- Integrates with the operating system of the host computer and monitors program behaviour in real-time for malicious actions;
- Blocks potentially malicious actions before they affect the system;
- Potentially malicious actions may include:
  - Attempts to open, view, delete, modify files;
  - Attempts to format disk drives, etc
  - Modification of system settings (start-up, etc)
  - Initiation of network communication, etc

**Monitoring and Detection of Internet Worms**

- **Speed** is a crucial aspect here:
  - SQL Slammer worm, appeared in January 2003 and infected more than 90% of vulnerable computers in the internet within 10 minutes;
  - Successful worm attack typically lasts several days infecting hundreds of thousands of computers (Code Red, Nimda, Blaster...);

- **Aim**: early detection.

**Worm monitoring system**

The system consists of:
- **local scan monitors** for incoming and outgoing traffic;
- **data mixers** gathering information coming from monitors, or other data mixers (located at the lower levels in a tree structure);
- **warning center** accumulating information about the whole network and performing detection
Worm detection

- The whole range of methods developed for Intrusion Detection Systems can be used for worm detection;
- Special role of anomaly detection systems (suitable for detection unknown worms) :
  - **Threshold based:** detection of bursts of the network traffic;
  - **Trend based:** detection of trends in the network traffic. Based on a fact that at early stages a worm propagates exponentially.

Trend based detection

Typical picture of the worm propagation: Code Red simulation.