Malware & Spyware, Viruses

Patrick.j.rice@gmail.com

Virus

The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

There are differences!!

Virus

- Viruses are just programs
- They are not special in any way
- The are just programs that are hidden so that a user cannot see them.

Malware

Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code

Why do people create malware

- since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for black-market exploitation.
- Infected "zombie computers" are used to send email spam
- host contraband data such as child pornography or to engage in distributed denial-of-service attacks as a form of extortion.

Types of viruses

Trojan horses

- a Trojan horse is any program that invites the user to run it, concealing a harmful or malicious payload.
- The payload may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software.

Rootkits

- Rootkits allow this concealment, by modifying the host operating system so that the malware is hidden from the user.
- Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read.

Backdoors

- A backdoor is a method of bypassing normal authentication procedures.
- Crackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection.
- To install backdoors crackers may use Trojan horses, worms, or other methods.

Malware for profit

- Spyware
- Botnets
- Keystroke loggers
- Dialers

Spyware

- Spyware is a type of malware that is installed on computers and collects little bits information at a time about users without their knowledge.
- spyware is secretly installed on the user's personal computer
- Spyware programs can collect various types of personal information.
  - Internet surfing habits
  - sites that have been visited
  - interfere with user control of the computer in other ways
    - They can
    - install additional software
    - redirecting Web browser activity
    - Spyware is known to change computer settings, resulting in slow connection speeds,

Botnet

- Botnet is a jargon term for a collection of software agents, or bots, that run autonomously and automatically.
- A botnet's originator (aka "bot herder" or "bot master") can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes.

Keystroke logging

- Keystroke logging (often called keylogging) is the practice of tracking (or logging) the keys struck on a keyboard,
- Done in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
- There are numerous keylogging methods, ranging from hardware and software-based to electromagnetic and acoustic analysis.

Dialers

- electronic device that is connected to a telephone line to monitor the dialed numbers and alter them to seamlessly provide services that otherwise require lengthy access codes to be dialed.
- "dialer" often refers specifically to dialers that connect without the user's full knowledge as to cost, with the creator of the dialer intending to commit fraud.
- In Ireland the often dialled uk numbers and charged you international rates.

Virus removal

- Tools
  - Malware bytes
  - Clamwin