

# Computer Virus Presentation

By Bob D'Evelyn

April 6, 2010

## Opening: tonight we will talk computer viruses

1. Availability of a "hand Out"
2. What a virus looks like
3. What kind of a person create them
4. Their education level
5. Virus definitions
6. What they look like when you see them
7. Suggested antivirus features
8. Safe practices
9. What's out there to buy

## A Computer Virus

- Here is an example of a real live **Virus**.
- This 10 instruction machine language program is an actual virus.
- Most people, looking at this, have no idea what it is, much less what it can do to their computer.
- It looks like 10 rows of letters and numbers; nothing else.

## Virus Example

A: Jump to B

D1 = 11010011 "Byte constant"

D2 = 00111000 "Byte constant"

D3 = 11000101 "Bye constant"

B: Set Exec mode "Set processor to Exec mode"

Load A1(C:1,100) "load MBR"

Merge A1, D1, D2, D3 "Change MBR contents"

Store A1, (C:1,100) " Replace MBR content"

Reset exec mode "Return to normal mode"

Return "Return to main program"

- If it manages to get into a computer and is executed by the computer processor, it completely disables that computer....

### Virus Developer Education

- What level of education might the Virus developer have?
  - Highly Educated e.g. Computer Science major in collage
  - Requires detailed knowledge of machine language programming.
  - In particular the Intel processors

### Motivation for Virus Developers

- Angry at the world
  - Cause grief for ordinary computer owners
  - Attempt to infect as many computers as possible.
- Desire to be noticed
  - Show everyone that I exist and can invade your computer
- Develop future sales
  - Gather customer information for a sales organization

### Virus Definitions

- Virus

- A small software program that infects a computer as soon as they arrive in a user's computer.
- They sometimes show up as unexpected images on a computer screen.
- They sometimes create multiple non useful active processes so as to slow down the computer.
- Worms
  - A virus that replicates itself and attempts to infect a user's Emails so as to infect as many computers as possible
- Adware/ spyware/ keyloggers/ screen scrapers
  - Periodically puts ads up on your screen
  - Creates a record of your keyboard entries and images from your monitor
  - Allows companies to profile your online spending habits
  - Most antivirus software can't detect these kinds of viruses unless specifically designed to detect them.
- Trojan Horses
  - These viruses are hidden in software downloaded by the user.
  - A virus that lies dormant in your computer until a predestined time or activation by its designer.
- Root kits
  - There are several kinds of rootkits
  - One of them is a virus that attacks the root addressing system in your hard drive
  - This virus is the most dangerous of all because it is very hard to detect and can cause a complete breakdown of the computer's operating system.
    - Most of the time the users are required to format the hard drive and reload all software starting with the operating system.

### Root kit Attack Scenario

- Describe start up sequence: BIOS (Basic Input/ Output System), Master Boot Record and the Windows
  - When the power ON button is pushed, BIOS (a small firmware program built into the motherboard) executes and checks the computer hardware.
  - When BIOS completes its check, it “beeps” to the user.
  - A single beep tells us that everything is OK.
  - Then BIOS links to the Master Boot Record (MBR) in the hard drive Sector 0 and the computer instructions in this table begin which begins starting up Windows.
  - The **Root Kit Virus** changes the contents of the MBR so the Windows computer instructions in this table are now “garbage”.
  - So Windows does not start.
  - The computer is now unusable...
- In some cases, the virus modifies the Master Boot Record which stops any attempt to reload the operating system.
- Quite often the remedy is to perform a low level formatting.

- This type of formatting is similar to hard drive build process by the hard drive manufacturer.
- The software, supplied by the hard drive manufacturer, is called "zero-fill & diagnostic utility".
- While we computer owners can obtain this software and can execute it, we don't recommend it.
- So we suggest you take your computer to a professional such as the Data Doctors.

## **Virus Definitions Continued**

- Phishing
  - This is a technique used by spammers to trick the user to go to a web site that appears to be legitimate but has been altered.
  - The user goes to this website that contains malware.
- Botnets
  - a virus program that resides inside your computer and, when activated by its designer, floods the internet with garbage web site requests
- Drive-by-downloads
  - Sometime just visiting a web site a virus designer can take advantage of a security hole in your browser and download a virus into your computer.
  - Windows Explorer is the primary target.
  - Using other browsers minimizes this type of attack. For this reason, I use Mozilla Fire Fox.

## **Malware Red Flags**

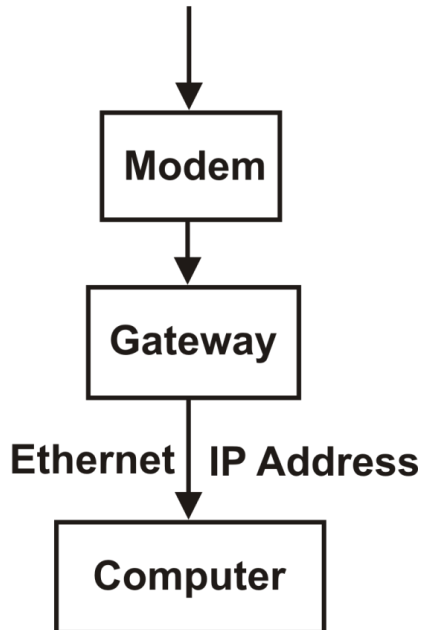
- Nonstop Pop-ups
  - This is a clear indication that your computer is virus infected.
- Poor computer performance
  - Your computer becomes bogged down and normal processing software takes much much longer to complete.
  - Checking your active processes shows a large number of active processes.
- Home page hijack (your Web Browser)
  - Your home page suddenly changes
- Unidentified browser toolbars show up
  - Quite often when downloading software, the download wizard asks if you want to update your toolbar to either Google or Yahoo.
  - A virus, on the other hand will ask you if you want to install an unknown toolbar.
  - But an unknown toolbar signals the presence of a virus
- Strange search results
  - If suddenly your search provider (other than Google or Yahoo) is something else, there is a virus in your computer making this request.
- You receive Emails asking for account information.
  - Don't respond as this may be a phishing attack.

- Your antivirus program suddenly stops working
  - A very dangerous virus has clobbered your antivirus program.
  - Turn your computer off and take it to the Data Doctors or other professional computer “geek”.

## 1. Safe practices

- If your connection to the Internet is via “dial-up” then there’s no reason to install a hardware Firewall.
- I recommend you buy and install a hardware Gateway which acts as a firewall.

### Cable/ DSL/ Satellite



- A Gateway connects between your computer and your internet modem.
- The advantage of a hardware gateway is that it provides a physical barrier between the internet with its potential virus attackers and your computer.
- If an internet virus wants to attack your computer, it must first obtain your computer’s internet address.
- A Gateway provides real-time addresses which cannot be obtained by a would-be external virus.
- This prevents any direct virus insertion into your computer from out on the Internet.
- A Gateway is ideal if you have more than one computer connected to the internet

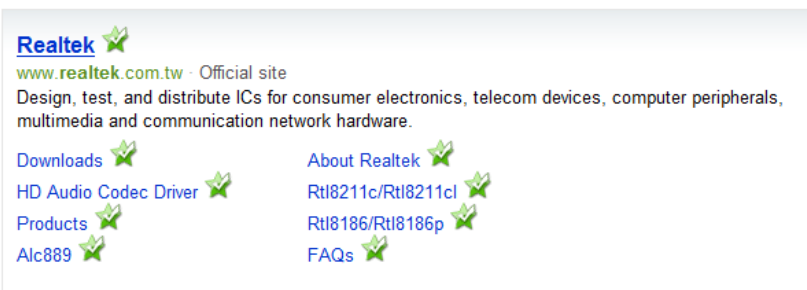
## 2. Safe Practices

- Be suspicious of any "flash" drive offered to you by a friend.
- Be suspicious of all Email attachments
  - Even from your friends
  - Recent discussion with Data Doctor people tell me that this is the major source of viruses

- They say that every day a computer comes in their door with a virus that got into that computer this way....
- Check every web site before you (visit it)
  - You haven't actually entered any web site until you "click" it....
- Scan every download before executing it.
  - Note: downloads from major companies are free of viruses...
- If you normally "surf" the web, use an up-to-date browser which includes antivirus software that scans any web site you before you go to it.

### 3. Safe Practices

- Some current antivirus software include a feature that checks websites before you "enter" them
- Here's an example of my Mozilla Firefox browser with/ AVG antivirus software telling me which web sites are "ok".



[Realtek - Wikipedia, the free encyclopedia](#)

**Realtek Semiconductor Corp.** (traditional Chinese: 瑞昱半導體股份有限公司), a fabless IC design house situated in the Hsinchu Science Park, Hsinchu, Taiwan, was founded in ...  
[en.wikipedia.org/wiki/Realtek](http://en.wikipedia.org/wiki/Realtek) · [Wikipedia on Bing](#)

- Those little green stars with a check tell me that this web site is OK to visit.
- If the web site had a red X, which indicates that this web site is not OK.

### Suggested Antivirus software features

- Customizable Firewalls
  - Antivirus software learns which processes in your computer normally attempt to reach an Internet website.
    - AVG Free does not provide this feature.
    - So each time one of your software programs wants to get something from the web, AVG Free interrupts you and asks for your permission.....
    - AVG Purchased does, however, provide this capability.
- Real time scanning is preferable to scheduling later hard drive scanning
  - e.g. Stopping attack when it happens vs. scanning your hard drive afterwards
- Scans web sites before you "click" on them
  - avoid attacks before you browse a website
- Scans all Emails before opening them.
  - avoid attacks if possible

- My Internet Service provider (AOL) scans all my EMail before I open them.
- When I ask to read my EMail, AOL shows me which ones are suspicious; so I can delete them if I agree with AOL.
- Scheduling scans when you aren't occupying the processor.
  - Scanning your hard drive takes up a lot of your processor's power.
  - So it's to your benefit to schedule antivirus scan when it's more convenient to you.

## Buying Antivirus Software

- If you have decided to buy Antivirus Software, you have 2 possibilities: buy it directly from a retail store or buy it from a website:
- Boxed software
  - Allows you to browse and compare prices before committing to a purchase
  - All office supply stores sell antivirus software
  - Best Buy also sells antivirus software
- Downloaded from the Internet
  - Potential Risks
    - Easiest but involves some risk.
    - Data Doctors said that most of their customers' computers were infected by viruses claiming to be "antivirus software."
    - These viruses offered "free" antivirus software that was available NOW.
    - Their customers, thinking that this was a "**good**" deal, downloaded this software only to find out that this bogus "antivirus" software had infected their computer after downloading it.
    - Therefore, minimize your risk by downloading antivirus software only from nationally known vendors.
    - National brands web sites and their products are not infected by viruses.
    - Save the download in a file whose name is the software you bought.
      - Remember this file you downloaded is not the "antivirus" software itself; it is an **exec** file that unzips and installs the antivirus software you bought.
    - Save this **exec** file within a file named "Downloaded Files" under My Documents
  - Print and save the license number and the validation period from the vendor
  - Launch this exec file to install your antivirus software.

## Boxed Antivirus Software

- Boxed name brand software
  - Most of these brands are advertized as, what I call, **Good**, **Better** or **Best**

- Features and cost of the “boxed” software increase from Good to Better and then to Best.
- The features listed by brand name software below are described using their language.
- If you don't understand what that means, ask a sales person for its definition.
- For this reason, know which features you want before you enter a retail store with the goal to buy
- Pay attention to the number of PCs and the length of the license.
  - A license covering only 1 PC is cheaper than a license which covers more than 1 PC.
  - A 1 year license is standard for the “Good” brand.
- Start with **Good** and work up.

## Boxed Antivirus Software

1. Norton from Symantec
  - Norton AntiVirus 2010
    - \$40 per year for 1 PC
    - antivirus
    - Anti Spyware
    - Bot Protection
    - Anti Root kit
    - Download Insight
    - File Insight
    - Threat Insight
  - Norton Internet Security 2010
    - \$70 per year for up to 3 PCs
    - Same as Norton Antivirus 2010
    - Spyware Protection
    - Identity Protection
    - Network Monitoring
    - Vulnerability Protection
  - Norton 360 Version 3.0
    - \$80 per year for up to 3 PCs
    - Antivirus
    - Botnet Protection
    - Safe Web
    - Automated Backup and Restore
    - Insight
    - Antispyware
    - Identity Safe
    - Firewall Protection
    - Browser Protection
    - Pulse Updates
2. Kaspersky Lab
  - Kaspersky Anti-Virus 2010

- \$60 per year for 3 PCs
- viruses and spyware
- infected Web sites
- Virus and vulnerability scanner
- Proactive protection against programs based upon their behavior
- Restriction of access to private data by suspicious programs
- Real-time scanning of email
- Virtual keyboard
- Kaspersky Internet Security 2010
  - \$80 per year for 3 PCs
  - Virus protection of Anti-Virus 2010 plus
  - Hacker attacks
  - Spam & phishing
  - Identity theft
  - Restriction of access to private data by suspicious programs
  - Safe run mode
  - Two-way personal firewall
  - anti-spam, anti-phishing

### 3. McAfee

- McAfee AntiVirus Plus
  - \$40 duration?
  - Malware Detection
  - Faster PC performance
  - Schedules scans when user not using computer
  - Scans web sites
- McAfee Internet Security
  - \$50 duration?
  - Includes AntiVirus Plus features plus
  - Anti spam and email protection
  - child protection
- McAfee Total Protection
  - \$60 duration?
  - Includes Internet Security features plus
  - Anti theft protection of files
  - Scans web sites

## Antivirus Software purchased from the Internet

4. Panda Internet Security 2010 [[www.pandasecurity.com](http://www.pandasecurity.com)]
  - \$36 for 6 months on 1 PC
  - Antivirus, customizable Firewall, anti spam filter
5. Avast [www.doubleantispay.com]
  - \$29 with 14 day free trial
  - Adware, spyware, Trojan Horses
  - Email scanning

- Real time protection
- Light resource load
- 6. F - Secure Internet 2010 [www.f-secure.com]
  - \$60 for 1 year for 3 PCs
  - Real time virus, spyware, root kits detection
  - Reduces drain on system resources
  - Scans web sites
  - Firewall protection
- 7. Internet Security 2010 Pro [www.trendmicro.com]
  - \$50 for 1 year for 3 PCs
  - Anti-spyware
  - Anti-spam filtering engine
  - Block wireless home network intruders
  - Personal firewall protection
  - Stops attempts to change your operating system and critical software
- 8. Web Root Spy Sweeper [www.webroot.com]
  - **Standard** Version \$30 for 1 year for 1 PC
  - Advanced Anti-spyware Detection and Removal
  - Real-Time Anti-spyware threat protection
  - Enhanced Root Kit Discovery Methods
  - Free updates during license period
  - Scanning during off peak hours
  - Accurate Risk Assessment
- 9. Web Root Spy Sweeper [www.webroot.com]
  - **This is Data Doctor's current recommendation**
  - **Advanced** Version
  - \$40 for 1 year for 1 PC
  - Includes Standard Protection
  - Plus Virus Protection
    - Removes viruses, Trojans, Worms, Root Kits, and Key Loggers
    - Scans EMail Attachments & Files for downloading
    - Blocks fake alerts, pop-ups & Browser hijacking
- 10. Web Root Spy Sweeper [www.webroot.com]
  - **Complete Protection** Version
  - \$60 for 1 year for 3 PCs
  - Includes Advanced Protection
  - Plus System Cleanup
    - Automatic Photo & File protection
- 11. AVG [www.avg.com]
  - AVG Free Edition
    - Provides the bare necessities
    - Does include web site scanner
    - Does not provide a dynamic firewall
    - I used this version for years; but today, I do not recommend it.
  - AVG Internet Security 9.0

- **This is the Anti-Virus I currently use and am happy with it.**
- \$44 for 1 year for 1 PC
- Identity protection
- Web shield
- Anti-spam
- Anti-virus and anti-spyware
- Link Scanner
  - Attached to Web Browser
  - Scans Web Sites
- Enhanced firewall protection