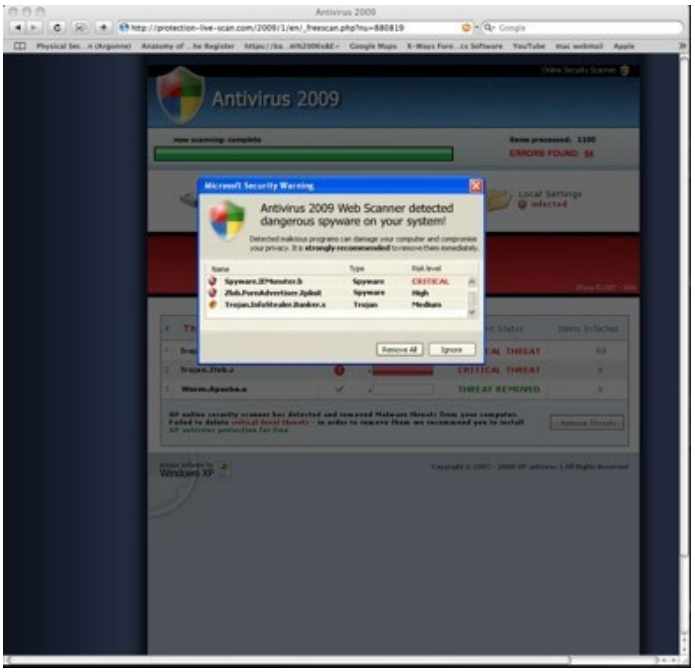
Attacks on Desktop Computers

MALICIOUS SOFTWARE ATTACKS (MALWARE)

Software makes your computer useful, right?

What if that software is Malware?

Malware is malicious code planted on your computer that gives your computer usefulness, but only to an attacker. It can give the attacker an alarming degree of control over your system, network, and data - without your knowledge.



MALWARE VIRUSES

Viruses can get into your system just by you clicking a button. Since viruses attach to carriers (like a human virus), they are installed immediately when a user executes (opens) a file, program, image, or attachment.

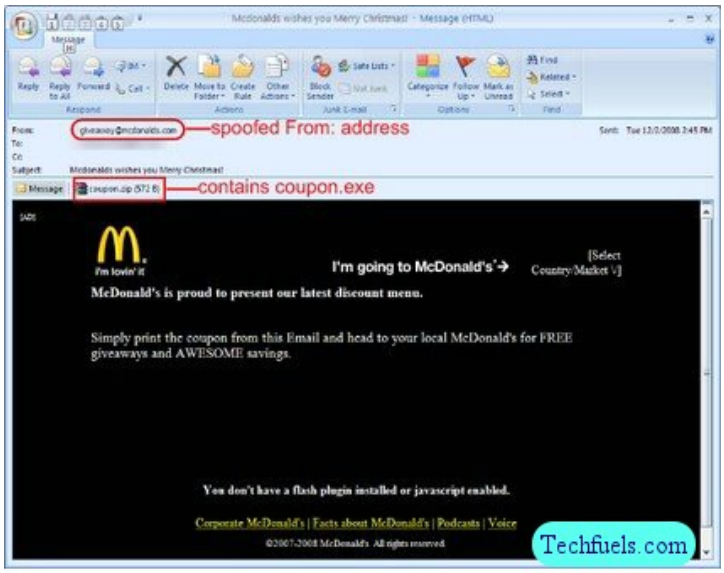
A virus must have a carrier and it must be initiated by a user!

HOW THEY SPREAD

Once a virus is on your system it first tries to spread to other systems:

Thru files …

Thru emails …



Websense

Thru pop-ups …

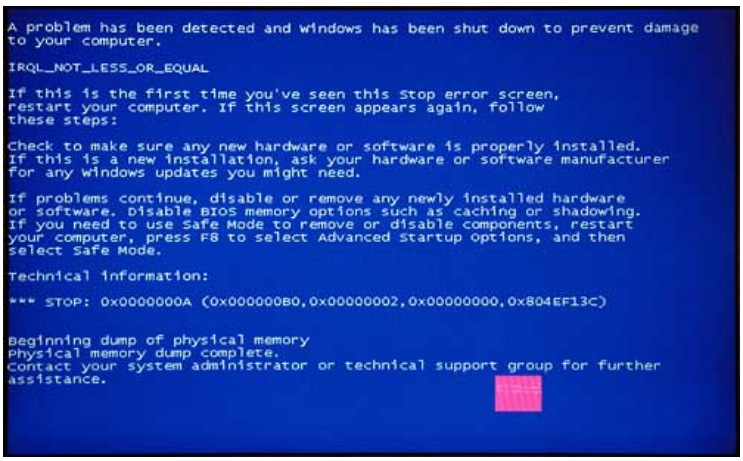
Thru jump-drives …

and thru instant-messaging …

WHAT HARM CAN THEY DO?

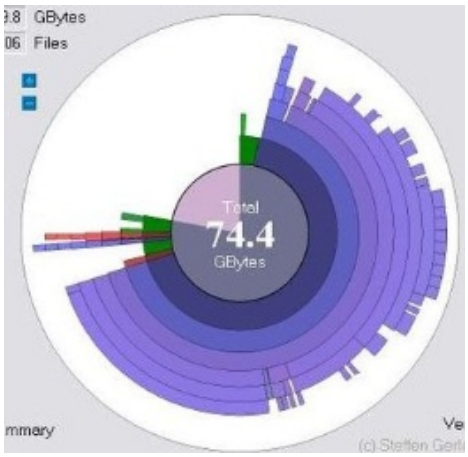
Once the pesky viruses get on your system and replicate to other systems, they dump their payload such as:

Crashing the computer …

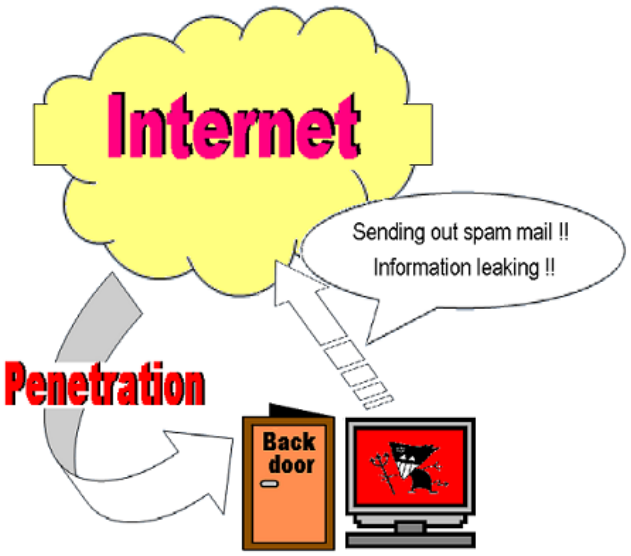


Deleting important files …

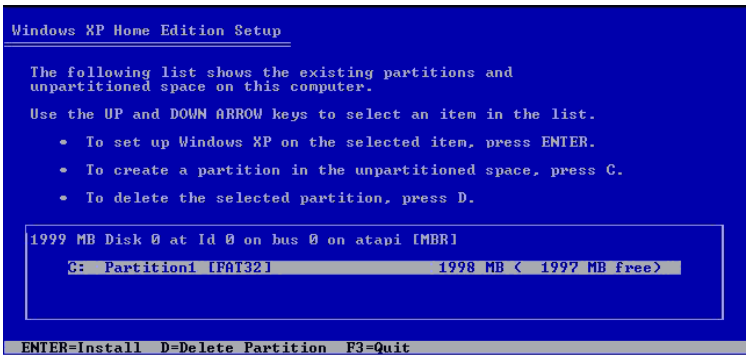
Consuming disk space …



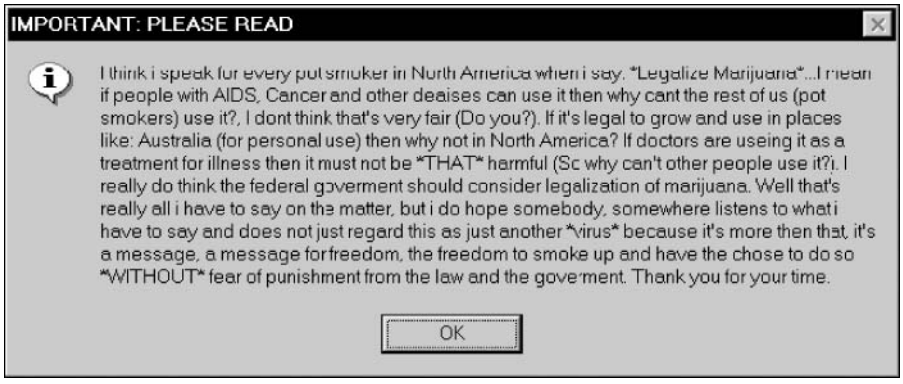
Creating a back-door …



Reformatting the hard drive …



And by giving you annoying messages …



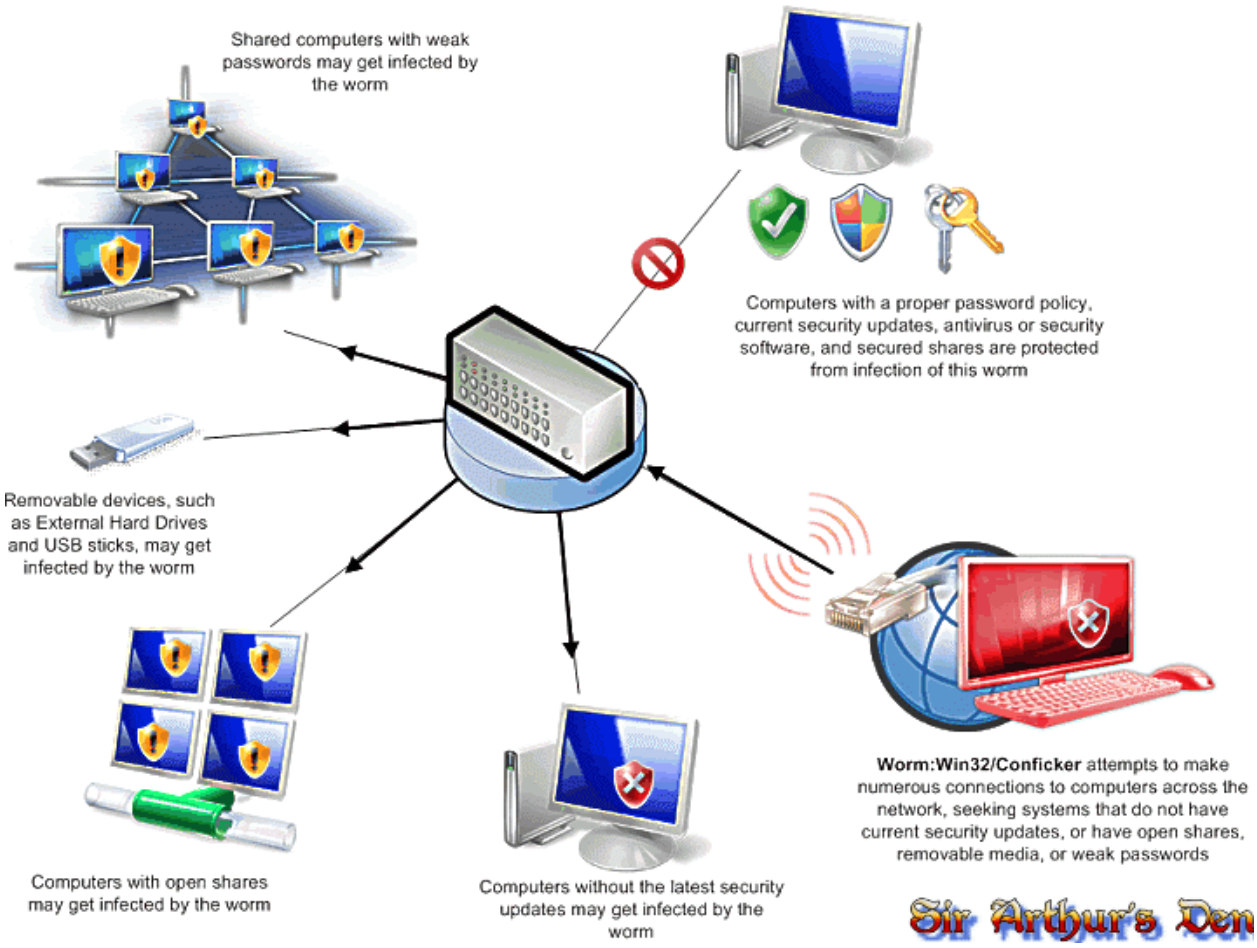
There are a multitude of virus types. Click on the image or link below to get more information.

http://online-pc-support.com/virus-troubleshooting.htm

MALWARE WORMS

A worm is like a virus, but does not need to have a carrier like a virus does, it can travel by itself.

Worms take advantage of vulnerabilities and spread through the Internet and Intranets (locally connected computers). Like viruses, it too will search for other systems with similar vulnerabilities.



MALWARE CONCEALMENT

Some malware can hide itself on a computer system waiting for the opportunity to inflict pain.

Click on the image or link below to get more information.

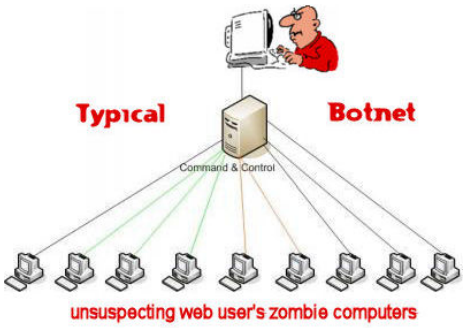
http://coursecontent.ntc.edu/CIT/husband/pois/lp2/m11-malwareconcealment.html

THE BIG BAD BOTNET!

Really clever but really bad are the little zombies (bots) that live on the Internet and communicate using Internet Relay Chat (IRC) channels to await orders from a cracker (bot herder) to release their payload to unsuspecting computers in unison.

Botnets are formed because of vulnerabilities, mostly with browsers. Botnets will typically do one or more of the following:

- Key logging: Monitor keystrokes to get passwords, credit card numbers, etc.
- Spamming: Unsolicited e-mail.
- Spreading malware: Zombies will install malware sent by an attacker.
- Distributed denial of service attacks (DDOS): Brings either a network or a service to its knees.
- Poll bending: Manipulating online polls.



HARDWARE ATTACKS

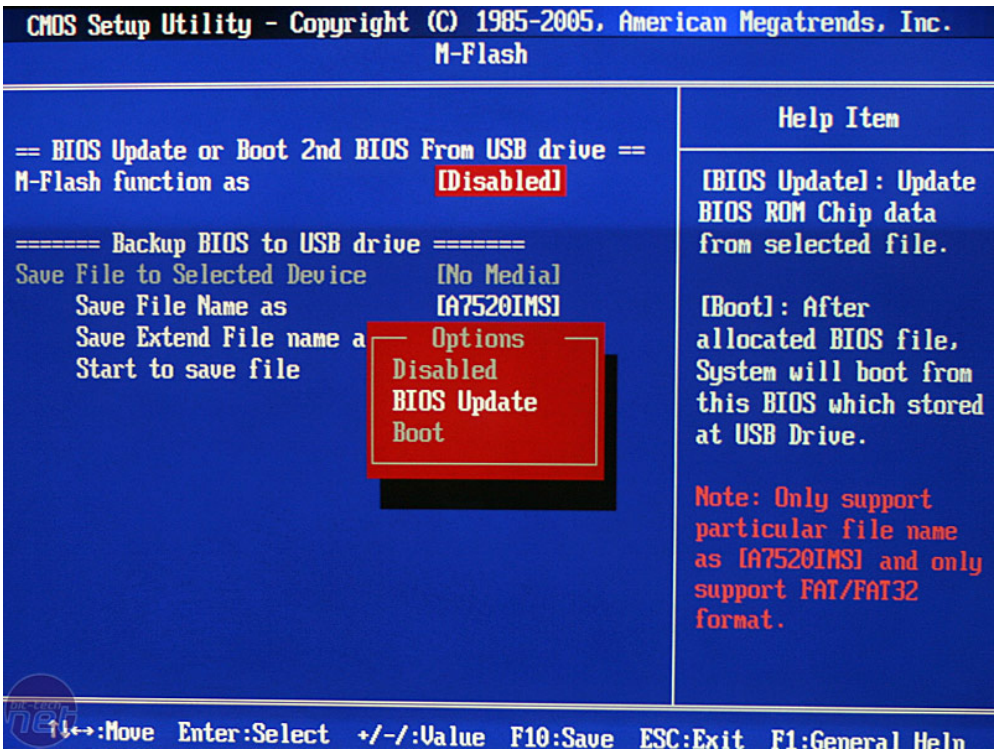
Attacks are not limited to software, files, and system services. They can also compromise your hardware.

BIOS (BASIC INPUT/OUTPUT SYSTEM)

All personal computers have them and they occasional have to be updated to better support new hardware devices such as large disk drives.

When BIOS is updated it is flashed. If the BIOS is flashed by an attacker from the operating system you could end up with malware or a non-bootable computer. The only fix to a compromised BIOS is either another BIOS or legitimate flash.

Since the BIOS is very hardware dependent, flashing a BIOS is sometimes difficult to do even when you are in control. You can make it difficult for an attacker to flash the BIOS by **disabling the flashing of the BIOS** from within the BIOS setup utility. See image below for an example of what this BIOS configuration parameter looks like.



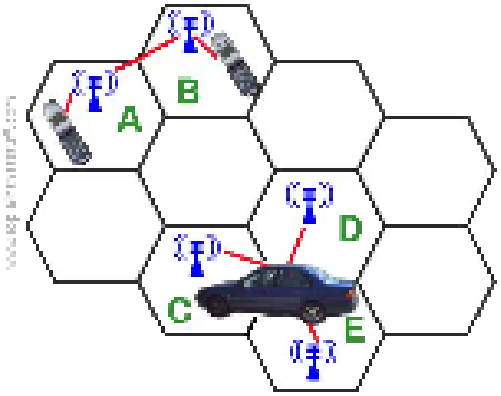
USB DEVICES

USB (Universal Serial Bus) devices are very convenient for file storage and transfer. Because of their portability, they are also known as "the modern path for viruses".

Viruses are spread to your system from USB devices mostly through the autorun feature of Windows. Fortunately, this feature can be manually disabled, but may already be disabled with a patch from Microsoft.

CELL PHONES

Cell phones work at a given frequency that is confined to a cell (shaped like a hexagon) that is about 10 sq. miles. Each cell has a transmitter that communicates with a base station. Each base station communicates with a mobile telecommunications switching office (MTSO) which is the link between the cellar world and the wired world.



Many cell phones can send and receive messages and connect to the Internet. They can also store information, both financial and personal. Basically, function much like a desktop computer.

The additional threats for cellular handheld devices stem mainly from two sources:

1. Their size and portability
2. Their available wireless interfaces and associated services.

Click on the image or link below to get more information.

http://coursecontent.ntc.edu/CIT/husband/pois/lp2/m12-cellphonethreats.html

Do we need a little mobile device control?

How about these user-oriented measures:

- Maintain physical control of your devices
- Enable access authentication to your device
- Backup data that is on your device in case of loss
- Reduce exposure of your data to those that don't need to see it
- Don't perform questionable actions while on the Internet
- Deactivate compromised devices
- Add prevention and detection software

How about these organizational-oriented measures:

- Establish a mobile device security policy
- Instill a security awareness training program
- Properly manage software and device controls

PHYSICAL THEFT

Small, portable devices such as laptops and cell phones are easy targets for theft. Sometimes these devices have valuable information on them that can damage personal identities or release corporate financial information and/or secrets.

Theft of information can come from computers sold or given away in legitimate transactions - such as rummage sales, charities, schools, selling online, or computer recycling centers.

Even though data may have been deleted, if the space where the data resided had not been wiped clean, the data can still be obtained.


GetData
www.getdata.com
Recover My Files
Advanced Data Recovery Software
Recover Files
Lost, Deleted,
Emptied from Recycle bin,
From a program crash
More info
Recover Files
Recover a Drive
Accidental format,
Windows reinstall,
System restore,
Corrupt or missing drive letter
More info
Recover Drive
Help
Next >
Cancel