Air Force Association's CyberPatriot

The National High School Cyber Defense Competition

Windows Operating Systems: Basic Security
Module 4

Objectives

- Define Threats and Vulnerabilities
- Different types of threats
- Examples
- How you get infected
- What can be done with compromised computers
- Preventions and protections

Definitions

- Threat
  - Any circumstance or event with the potential to adversely impact operations (including mission, functions, image, or reputation), assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

- Vulnerability
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

http://www.expertglossary.com/security/definition/

Malware

- Malicious Software = Malware
- Software designed and written to
  - Annoy computer users
  - Steal information from a computer or spy on a computer user
  - Gain control of a computer
  - Destroy or corrupt information or computer software
- Categorized by type (how the malware spreads) and by the malicious activity performed

Types of Malware

- Virus
- Worms
- Trojans

Virus

"…**computer virus** (a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer) *'a true virus cannot spread to another computer without human assistance'*"

- Oldest type of malware, known for attaching itself to other programs (i.e., infecting a program, disk, etc.)

From: http://wordnetweb.princeton.edu/perl/webwn

How Do You Get Infected?

- Virus
  - Email attachment
  - Malicious website or link
  - Downloaded or shared program, media, or document file

ILOVEYOU Virus Example

- Infected more than 45 million computers
- Estimated damages of $10 billion

From: F-Secure.
URL: http://www.f-secure.com/v-descs/love.shtml

Worm

"A computer worm is a program which copies itself across a network. A computer worm differs from a computer virus in that a computer worm can run itself. A virus needs a host program to run, and the virus code runs as part of the host program. A computer worm can spread without a host program, although some modern computer worms also use files to hide inside."

- Worms spread quickly (minutes to spread world-wide)

http://www.tech-faq.com/computer-worm-virus.shtml

Sasser Worm Example

- Infected more than 1 million computers
  - Shut down satellite communications for some French news agencies
  - Infected Britain's Coastguard control centers
  - Resulted in cancellations of Delta Airline flights
  - Shut down numerous companies worldwide
  - Impacted government offices
  - Impacted banks and financial networks
  - Shut down at least one hospital X-ray machine
- Estimated damages at hundreds of millions of dollars
- Exploited network vulnerability and did not use e-mail to propagate

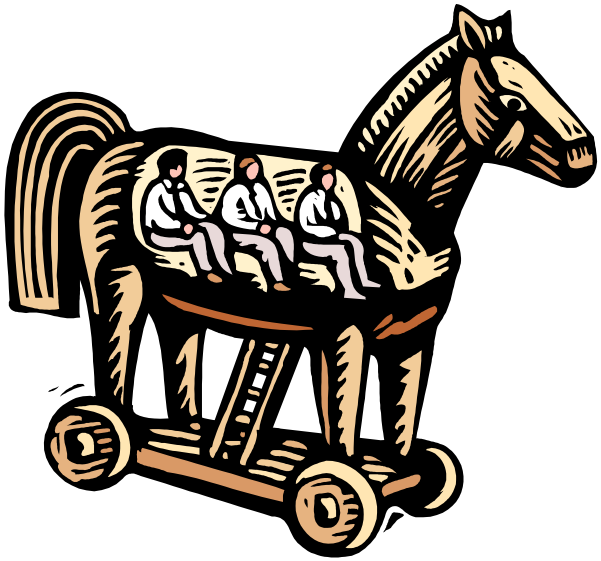
How Do You Get Infected?

- Worms
  - Vulnerable operating system or application
  - Email attachment
  - Malicious website or link
  - Downloaded or shared program, media, or document file

Trojans

"...A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program."

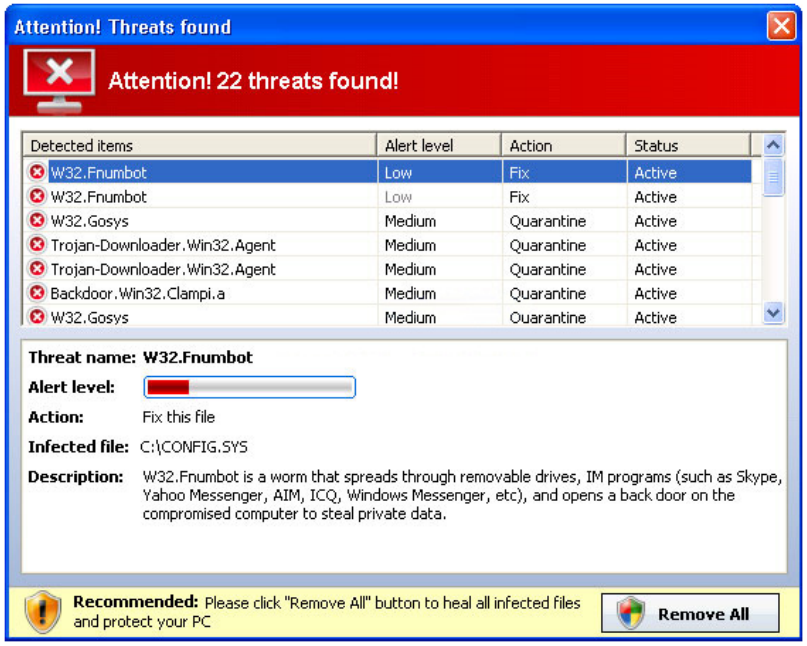
http://www.sans.org/resources/glossary.php



How Do You Get Infected?

- Trojans
  - Downloaded or shared program, media, or document file
    - Peer-to-Peer file sharing (Napster)
    - Downloading an e-mail attachment
    - Fake software download

Trojan Example



- Antivir is promoted through the use of Trojans that come mostly from fake online anti-malware scanners

Malicious Activity

- Many different kinds of malicious activity
- Some malware simply destroys information while others allow the attacker access to information
  - Backdoor/trapdoor (a.k.a. Remote Access Trojan/Remote Administrative Tool (RAT))
  - Logic/Time bomb
  - Keylogger
  - Spyware/Adware

Backdoor/Trapdoor

"A 'back door' is an entry point into a program that the programmer leaves himself in order to gain quick access without having to go through all the normal, built-in security checks. In theory, the back doors are taken out of the final release of the software, but history has shown that often they are not.

…a back door is generally considered to be a program that has been placed on a computer (usually surreptitiously) that allows a remote user to gain and maintain complete administrative control over the computer - almost always without the knowledge of the computer's owner or primary user."

http://www.upenn.edu/computing/security/malware.html

Backdoor Examples

- Energizer's Duo USB charger software allows unauthorized remote system access
  - The monitoring software contains "rogue code" that "listens for commands on TCP port 7777" and it can "download and execute files, transmit files stolen from the PC, or tweak the Windows registry."
  - Even after unplugging the device, the virus executes each time you turn on the PC and remains active until you turn off the PC

Energizer Duo USB Charger

Logic/Time Bomb

"A program, or portion of a program, which lies dormant until a specific piece of program logic is activated. In this way, a logic bomb is very analogous to a real-world land mine. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes it's code. A logic bomb could also be programmed to wait for a certain message
from the programmer."

When the activation of a logic bomb is based on a time/date, the variation is sometimes referred to as a "time bomb."

http://www.tech-faq.com/logic-bomb.shtml

Logic Bomb Example

NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2009/012909-fannie-mae-computer-time-bomb.html

Ex-Fannie Mae employee accused of planting computer time bomb

Former computer contract employee indicted on computer intrusion charges, report says
By Ellen Messmer, Network World
January 29, 2009 09:40 AM ET

A computer-engineering employee fired from troubled mortgage giant Fannie Mae is accused of preparing a malware computer time bomb, which had it not been detected, might have destroyed millions of files, according to reports.

Rajendrasinh Makwana, the computer contract employee in question, was indicted earlier this week on computer intrusion charges, according to the "DC Examiner" report citing court documents. Makwana, said to be an Indian citizen and former contract employee at Fannie Mae for three years, was terminated Oct. 24 for changing computer settings without permission from his employer and allegedly hiding malware code in a server that was programmed to become active Jan. 31.

Sponsored by:


View a slide show of the 10 worst moments in network security history

Court documents include a statement from FBI agent Jessica Nye that the malicious script, had it gone off, would have "reduced if not shut down operations" at Fannie Mae for at least a week. "The total damage would include cleaning out and restoring of 4,000 servers, restoring and securing the automation of mortgages, and restoring all data that was erased."

Keylogger

- "… keyloggers are applications that monitor a user's keystrokes and then send this information back to the malicious user. This can happen via email or to a malicious user's server somewhere on the Internet. These logs can then be used to collect email and online banking usernames and passwords from unsuspecting users or even capture source code being developed in software firms."

http://www.securityfocus.com/infocus/1829

Keylogger Example

United Nations hit by keylogger and trojan attack

UN serves dangerous malware after online attack

By Darren Pauli, Computerworld | Published 10:56, 29 August 07

The United Nations (UN) has been hit by a string of hacking attacks aimed at identity and credit card theft, and the building of botnets.

The attack on the UN Asia Pacific website is believed to originate from the same group responsible for attacks on the US-based Biotechnology Information Organization and the prominent Indian Syndicate Bank.

The financially-motivated incursions, launched from the same remote location, infected a server common to all three websites and downloaded a Trojan to visitor computers via drive-by attacks.

A keylogger and a Trojan were downloaded to visitor computers, flagged by an online scanner as positive to multiple Microsoft vulnerabilities, via hidden Java iFrames which is an old trick to refer visitors to a compromised server.

The Trojan maintains a backdoor, allowing attackers to monitor and hijack user machines to steal valuable user data, and turn the computer into a

Also in this channel

- News
- In Depth
- How-Tos
- Blogs
- Slideshows

Related Articles

Zurich fined £2.3m for massive customer data loss

Insurer's data was lost in

Other Uses for Keyloggers

- **System Administrators**
  Keylogger will help you to find out what took place on the system in your absence.
- **Office Managers**
  Monitor actions performed by your employees in the office hours on the Laptop or Desktop PCs.
- **Parental Monitoring**
  Using parental control software you will be able to find out what your children surf on the net and kind of website logged by them.
- **Personal User**
  You will able to find out what is being done on your PC in your absence.
- **Internet Cafe**
  Keylogger will let you find out what users have been doing on the computers.

Spyware/Adware

- Spyware is computer software that gathers information about a computer user (such as browsing patterns or credit card numbers) and then transmits this information to an external entity without the knowledge or informed consent of the user.

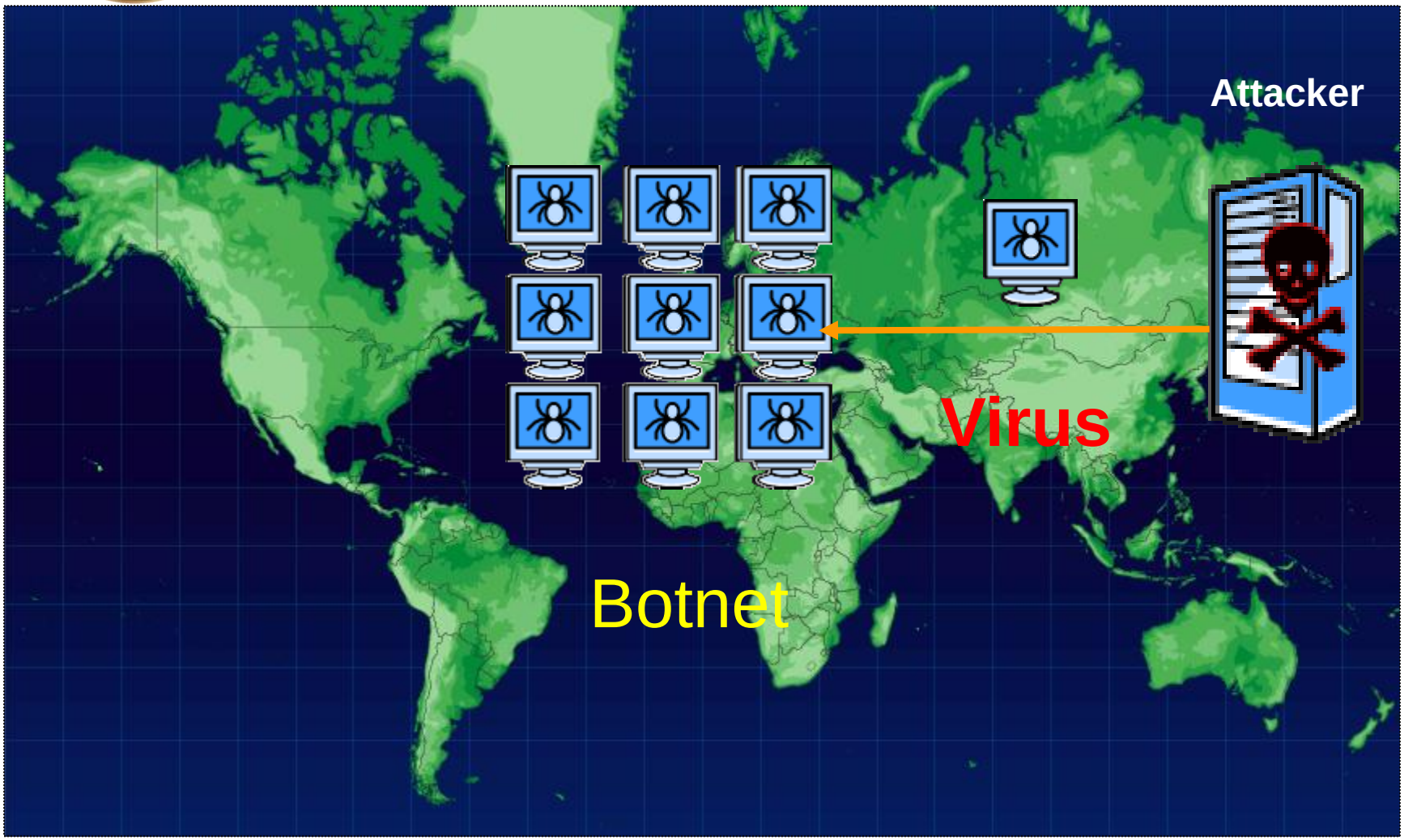
- Adware or advertising-supported software is any software application in which advertisements are displayed while the program is running. Display ads appear in pop-up windows or through a bar that appears on a computer screen.

http://www.jellico.com/spyware.html

How are Compromised Computers Used?

- Zombie computers are compromised computers under the control of an attacker. A zombie computer can be part of a “Botnet”
- A Botnet is a collection (or network) of compromised computers under the control of an attacker, using a server or servers to relay commands from the attackers to the Botnet zombies

Botnet



How are Compromised Computers Used?

- Denial of Service (DoS) Attack – denying access to a system or its information by consuming resources (CPU, memory, or network)
- Distributed Denial of Service (DDoS) Attack – a DoS attack mounted by many computers around the internet, usually performed by a Botnet
- Spam – unwanted and unsolicited email (most common use of Botnet is to send out spam)

Denial of Service Example

- In February of 2000, leading Web sites under attack from denial of service attacks.
- Big name companies such as Yahoo and Buy.com were down for up to 3 hours.

Web sites under fire

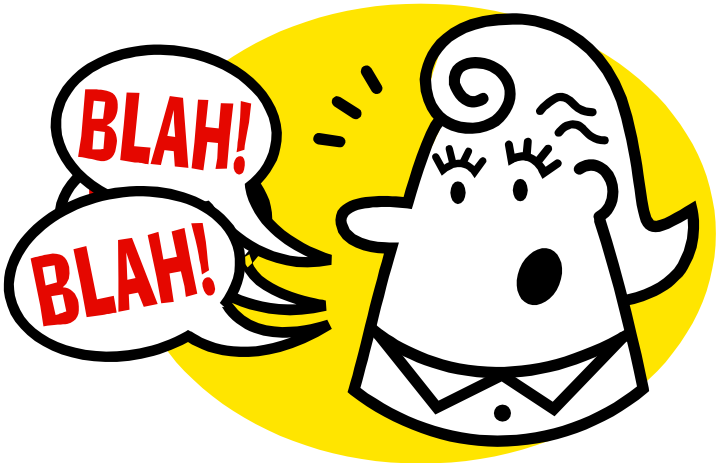
	Hit by attack*	Approximate duration
Yahoo	10:20 a.m. Mon.	3 hours
Buy.com	10:50 a.m. Tues.	3 hours
eBay	3:20 p.m. Tues.	90 minutes
CNN.com	4:00 p.m. Tues.	110 minutes
Amazon.com	5:00 p.m. Tues.	1 hour
ZDNet	6:45 a.m. Wed.	3 hours
E*Trade	5:00 a.m. Wed.	90 minutes
Datek	6:35 a.m. Wed.	30 minutes

*All times PST

DoS and DdoS Example

Social Engineering

- Any act of manipulating a person into performing actions or divulging confidential information



James Banicar | **Apr 20, 2009**

Types

- Physical
  - Face to face
  - Shoulder surfing
  - Piggy-backing or tailgating
  - Dumpster diving
- Technology
  - Phishing
- Telecommunications
  - Vishing

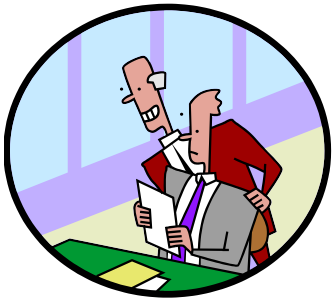
Face to Face

- Physical
  - To impersonate someone who is likely to be trusted. This could be someone from your organization, an emergency responder, the pizza guy etc.

Shoulder Surfing

- Physical
  - Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci802244,00.html



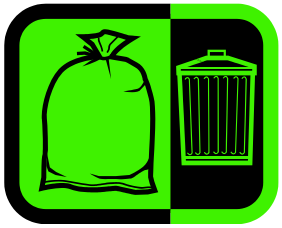
Piggy-backing or tailgating

- Physical
  - A person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

http://en.wikipedia.org/wiki/Piggybacking_(security)

Dumpster Diving

- Physical
  - Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using techniques to gain access to the network. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci801970,00.html



Phishing

- Technology
  - Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking e-mail in an attempt to gather personal and financial information from recipients.

Vishing

- Telecommunications
  - Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice e-mail, VoIP (voice over IP), landline or cellular telephone.

http://searchunifiedcommunications.techtarget.com/sDefinition/0,,sid186_gci1301120,00.html

How Valuable Is This Information?

- Access the network by using user ID and passwords
- Physical access to a data center
- Spam / Spoof e-mail addresses
- Known vulnerabilities on certain versions of software

Top 10 Information Security Threats

1. Malware
2. Malicious Insiders
3. Exploited vulnerabilities
4. Careless employees
5. Mobile devices
6. Social networking
7. Social engineering
8. Zero-day exploits
9. Cloud computing security threats
10. Cyber espionage

http://www.net-security.org/secworld.php?id=8709

How to Protect Yourself

- Keep your system up to date by patching – most operating systems have an automatic update feature
  - Microsoft http://microsoft.com
- Use anti-spyware/adware software - freeware examples
  - Malwarebytes http://http://www.malwarebytes.org/
  - Spybot Search & Destroy http://www.safer-networking.net/
- Use a firewall

How to Protect Yourself

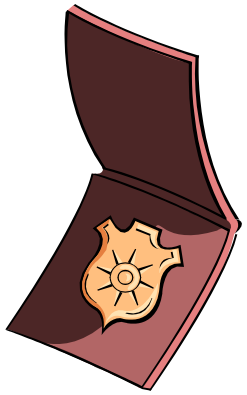
- Use an antivirus program and keep the definitions updated
- Free Anti-virus Options
  - AVG
  - Avast!
  - Microsoft Security Essentials
  - Comodo Antivirus
  - Avira AntiVir Personal
  - Panda Cloud Antivirus
  - Immunet Protect Free
  - Digital-defender Antivirus
  - PC Tools AntiVirus Free

How to Protect Yourself

- Check file system
  - Windows
    - Check Task Manager to examine .exe files or unknown processes running
    - Check 'Startup' to examine.exe files
    - Monitor .dll changes
  - Unix
    - Check cron to see what commands or scripts are being automatically executed at a specified time/date.
- Monitor open ports
  - Free tools available for both linux and windows (i.e.,wireshark)
  - Trojan horse scanners typically attempt connections on high-numbered ports
- Stay up to date on the latest vulnerabilities
  - http://www.us-cert.gov/cas/alerts/index.html

How to Protect Yourself

- Security awareness training
- Always verify who you are speaking with
- Never give out sensitive information over the phone or in an e-mail
- Verify websites are secure before submitting any personal or corporate information
- Do not let anyone in without proper ID – escort them to security to get a new one
- Make sure no one is looking over your shoulder to see your UserID or passwords
- Use your hand to shield anyone's view of your PIN in a store or at an ATM



References

- Some anti-virus and security companies
  - Kaspersky http://www.kaspersky.com/
  - McAfee http://www.mcafee.com/us/threat_center/
  - Panda Security http://www.pandasecurity.com/usa/
  - Sophos Labs http://www.sophos.com/
  - Symantec http://www.symantec.com/index.jsp
  - Trend http://us.trendmicro.com/us/home/
- About.com
  - http://antivirus.about.com/od/virusdescriptions/Latest_Malware_and_Vulnerabilities.htm
- HowStuffWorks.com
  - http://computer.howstuffworks.com/worst-computer-viruses.htm

References

- Cybersecurity Websites
  - US-CERT http://www.us-cert.gov/cas/tips/
  - FBI http://www.fbi.gov/cyberinvest/escams.htm
  - Symantec http://www.symantech.com/
- Social engineering
  - Social Engineering – Security Through Education
    http://www.social-engineer.org/
  - US-CERT – Avoiding Social Engineering
    http://www.us-cert.gov/cas/tips/ST04-014.html