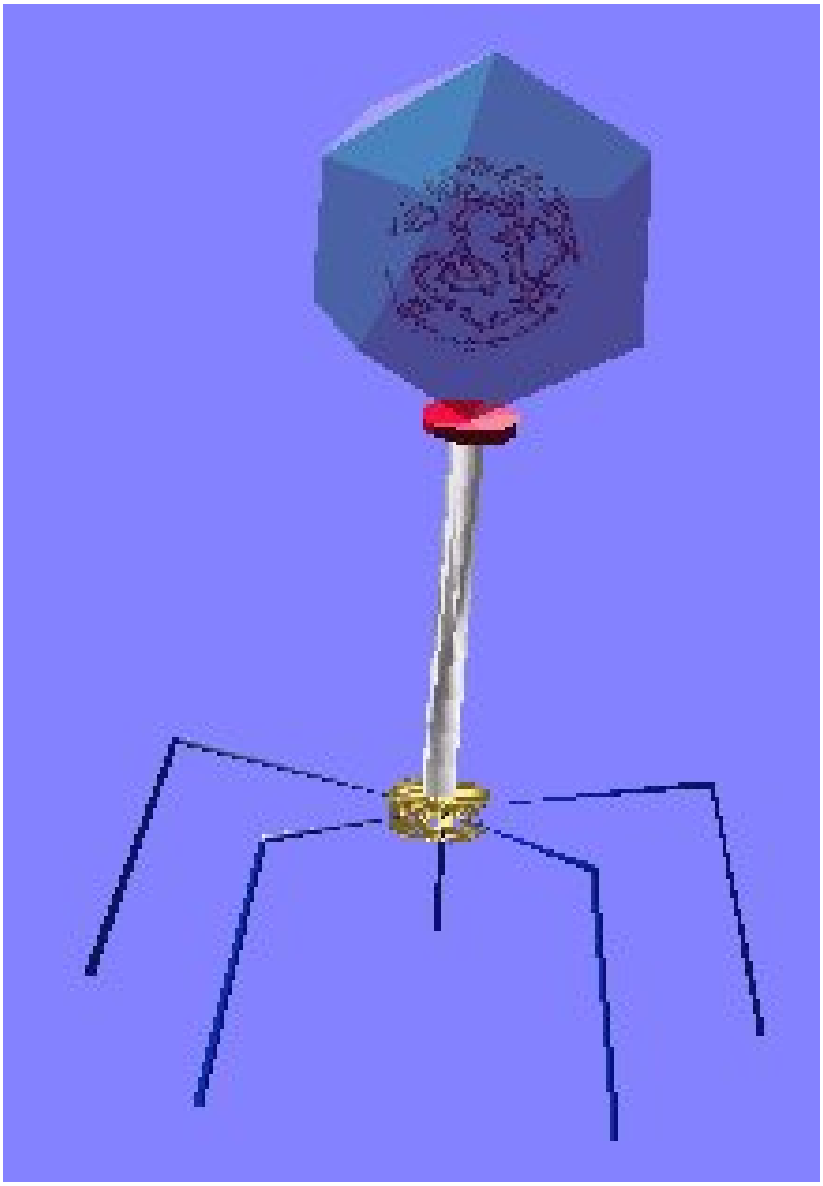
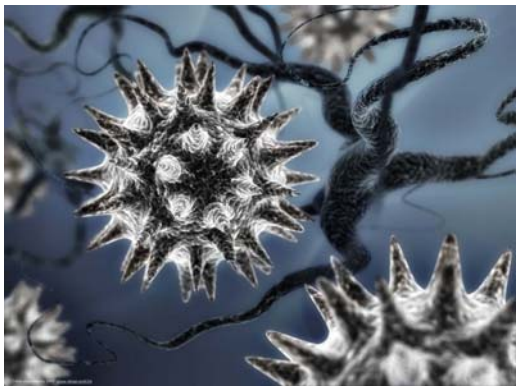
The
New York Society Library
Presents:



Computer Viruses

By Ingrid Richter
Head of Systems

INDEX:



HISTORY:

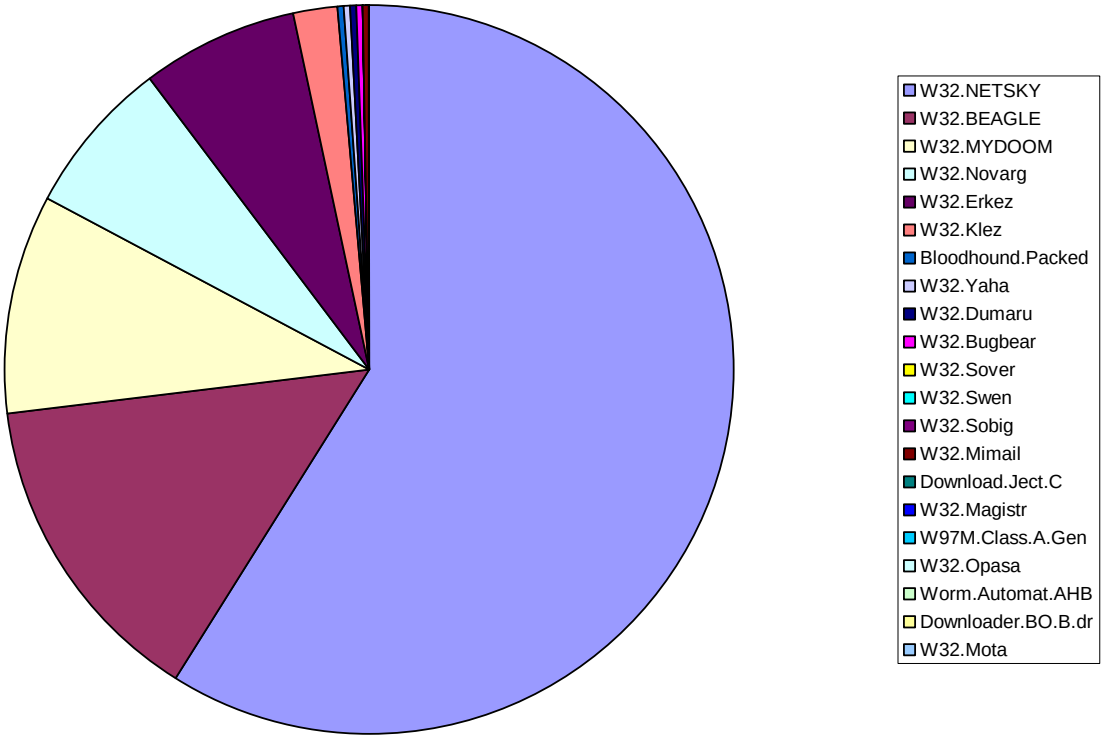
1981: Elk Cloner virus spread through Aplle II floppy disks
1986: Brain virus infects MS-DOS through the floppy boot sector
1987: IBM Chrismas worm replicates and infects IBM mainframe computers
1988: MagMac worm infects Macintosh computers through Hypercard
1988: Morris worm cripples approximately 10% of all computers on Internet.
1989: Aids Trojan encrypts hard drives; demands payment for decryption

1990: Hackers suspected of bringing down AT&T Network
1991: Tequila virus morphs itself to avoid detection
1992: Michaelangelo virus causes fear, but does little damage
1995: Major companies hit by the "Internet Liberation Front" hackers
1995: Concept macro first macro virus created (Microsoft Word)
1996: Boza first virus for Windows 95; Staog first virus for Linux
1996: Laroux first virus designed for Microsoft Excel
1998: Back Orifice Trojan looks like administrator tool, allows remote access
1999: Melissa virus first to use Outlook/Express address book to spread
1999: Bubbleboy worm infects e-mail users simply reading their e-mail

2000: Love Letter worm spreads fast and shuts down network systems
2000: Viruses created to infect Internet-connected phones and PDA's
2001: Gnuman virus disguises itself as MP3 file & infects file-sharing groups.
2001: Peachy-PDF worm spreads through Adobe PDF files
2001: Nimda worm spreads though networks, corrupting *.exe files
2002: LFM-926 virus infects Shockwave files
2002: Sharp-A virus infects .NET files; written by a woman
2002: Benjamin worm spreads through Kazaa file-sharing
2003: Sobig worm carries own SMTP mail program to spread
2003: Slammer worm brings down South Korea from Internet
2003: Lovgate combines worm and Trojan for first time

2004: Witty worm attacks security software directly (BlackIce)
2004: Sasser worm spreads through FTP port instead of e-mail
2004: Rugrat worm attacks only 64-bit Windows files (Windows 95/98 safe)

VIRUS ACTIVITY: NYSL



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
2002												11	**11**
2003	37	22	30	80	14	7	2	6	10	7	3	26	**244**
2004	651	1055	487	1658	112	1130	1534	2493	491	449	51		**10,111**

1.	**W32.NETSKY**	**6705**	12.	W32.Swen	10
2.	**W32.BEAGLE**	**1632**	13.	W32.Sobig	7
3.	W32.MYDOOM	1111	14.	W32.Mimail	4
4.	W32.Novarg	798	15.	Download.Ject.C	3
5.	W32.Erkez	782	16.	W32.Magistr	3
6.	W32.Klez	208	17.	W97M.Class.A.Gen	3
7.	Bloodhound.Packed	49	18.	W32.Opasa	2
8.	W32.Yaha	35	19.	Worm.Automat.AHB	2
9.	W32.Dumaru	29	20.	Downloader.BO.B.dr	1
10.	W32.Bugbear	11	21.	W32.Mota	1
11.	W32.Sover	10			

NETSKY & BEAGLE ATTACHMENTS:

W32.Netsky Attachments (sample): mails.zip, talk.zip, all_document.pif, application.pif, document.pif, document_4351.pif, document_word.pif, message_details.pif, message_details.pif, message_part2.pif, my_details.pif, your_bill.pif, your_details.pif, your_document.pif, your_document.pif, your_file.pif, your_letter.pif, your_picture.pif, your_product.pif, your_text.pif, your_website.pif, yours.pif, about_you_rlevy.pif, abuse_list.zip, details.txt.pif, details03.txt, details05.txt, document.zip, game.zip, id04009.doc, id04009.zip, information.doc.pif, message.doc.exe, message.scr, message.zip, msg.pif, msg_carrie.zip, my_list01.zip, old_photos_csilberman.zip, readme.zip, report01.scr, your_document.zip, Bill.zip, Data.zip, Details.zip, Informations.zip, Notice.zip, Part-2.zip, Textfile.zip,

Netsky Virus E-Mail Subject/Content:
- Illegal / Please do not sent me your illegal stuff again!!! / abuses.pif
- Question / Does it hurt you? / your_picture.pif
- Letter / Do you have written the letter? / your_letter_03.pif
- Picture / Do you have more photos about you? / all_pictures.pif
- More samples / Do you have more samples? / your_picture.pif
- Only love? / Wow! Why are you so shy? / loveletter02.pif
- Funny / You have no chance... / your_text.pif
- Numbers / Are your numbers correct? / pin_tel.pif
- Found / Ive found your creditcard. Check the data! / visa_data.pif
- Stolen / Do you have asked me? / my_stolen_document.pif
- Money / Do you have no money? / your_bill.pif
- Letter / True love letter? / your_letter.pif
- Text / The text you sent to me is not so good! / your_text01.pif
- Pictures / Your pictures are good! / your_picture01.pif
- Criminal / Hey, are you criminal? / myabuselift.pif
- Wow / Why do you show your body? / image034.pif
- Password / Ive your password. Take it easy! / passwords02.pif
- Privacy / Still? / document1.pif
- Hurts / How can I help you? / hurts.pif
- Correction / Please use the font arial! / corrected_doc.pif

W32.Beagle Attachments (sample): Cat.com, Dog.cpl, Doll.cpl, foto2.com, foto3.scr, Garry.cpl, Garry.scr, Joke.com, Joke.exe, Joke.scr, price.com, Price.com, price.exe, price.scr, Alive_condom.scr, Message.scr, Readme.com, the_message.com, Your_money.com

Beagle/Bagle Virus E-Mail Content:
Hello user of *Nysoclib.org* e-mail server,
Some of our clients complained about the spam (negative e-mail content) outgoing from your e-mail account. Probably, you have been infected by a proxy-relay trojan server. In order to keep your computer safe, follow the instructions.
Advanced details can be found in attached file.
For security reasons attached file is password protected. The password is "44785".
The Management,
The Nysoclib.org team *http://www.nysoclib.org*

VIRUSES

CURRENT VIRUSES:

November 2004 Viruses (from Symantec):

1. W32.Gaobot.BQJ	November 8, 2004
2. Backdoor.IRC.Bifrut	November 8, 2004
3. VBS.Midfin@mm	November 7, 2004
4. Trojan.Beagooz.B	November 7, 2004
5. W32.Randex.BTB	November 6, 2004
6. W32.Linkbot.A	November 5, 2004
7. X97M.Avone.A	November 5, 2004
8. Trojan.Beagooz	November 5, 2004
9. Backdoor.Hacarmy.F	November 4, 2004
10. Backdoor.Maxload	November 4, 2004
11. Backdoor.Ranky.L	November 4, 2004
12. Backdoor.Alnica	November 3, 2004
13. W32.Josam.Worm	November 3, 2004
14. W32.Shodi.D	November 3, 2004
15. W32.Bagz.H@mm	November 2, 2004
16. VBS.Yeno.C@mm	November 1, 2004
17. VBS.Yeno.B@mm	November 1, 2004

November 2004 Viruses (from McAfee):

1. W32/Mydoom.ag@MM	11/08/2004	Virus / E-mail Low
2. Exploit-MS04-032!gdi	11/03/2004	Trojan / Exploit Low
3. Exploit-MS04-022	11/03/2004	Trojan / Exploit Low
4. Exploit-IframeBO	11/02/2004	Vulnerability / Exploit Low-Profiled
5. W32/Bagle.dldr	11/01/2004	Trojan / Downloader Generic Low

- Virus Advisory W32/Bagle.bd@MM is a Medium Risk worm.
- Virus Advisory W32/Bagle.bb@mm is a Medium Risk worm.
- Virus Advisory W32/Bagle.az@mm is a Medium Risk worm.

AN OUNCE OF PREVENTION:

1. Back up your computer weekly
Imagine the worst-case scenario (computer hard drive unrecoverable), and back up all of your files. If you have your original installation CD's, you'll only need to back up the documents that you have created (i.e. Microsoft Word files, photos, etc). Put them in some location removed from your computer (i.e. floppy disk, CD-ROM). You will need these disks in case your data gets corrupted by a virus.

2. Download Critical Updates weekly
If you are using a Microsoft operating system (i.e. Windows 98/2000/ME/XP), visit: http://windowsupdate.microsoft.com and download the Critical Updates for your computer. It's free, and it will patch up many of the security holes that the viruses exploit on your system.

3. Disable Macros in Microsoft Word & Excel permanently
Macros are mini-programs that run in Microsoft Word and Excel. If you don't need to use them, disable this feature (a handful of viruses exploit the macro program)
Microsoft Word 98: Tools -> Options -> General -> Macro virus protection
Microsoft Word 2000: Tools -> Macro -> Security -> High/medium/low.

4. Install & Learn to Use AntiVirus Software
It doesn't have to be Norton AntiVirus or McAfee VirusScan, but make sure you have some sort of virus protection software running on your system. Most new computers come with a year-long subscription to an anti-virus program. Make sure you renew your subscription at the end of the year. Both Norton & McAfee run around $30-40/year; other virus software can be found for free.

5. Keep Virus Definitions Up to Date
Your anti-virus software will only protect you against the viruses up to the virus definition date. Since new viruses are being created every week, you will need to download newer definitions to avoid becoming infected. Make sure your anti-virus software updates the definitions every time you are on the Internet.

6. Beware of All E-Mail Attachments
Don't open e-mail attachments from people you don't know. Be very cautious of e-mail attachments even *from* people you know - often times, the virus will use an e-mail address book from one of your friends to send you.

AVOIDING COMPUTER WORMS

From: http://www.f-secure.com/virus-info/tips.shtml

1. Most of the worms which use e-mail to propagate use Microsoft Outlook or Outlook Express to spread. If you need to use Outlook, download and install the latest Outlook security patch from Microsoft. In general, keep your operating system and applications up-to-date and apply the latest patches when they become available. Be sure to get the updates directly from the vendor.

2. When possible, avoid e-mail attachments both when sending and receiving e-mail.

3. Configure Windows to always show file extensions. In Windows 2000, this is done through Explorer via the Tools menu: Tools/Folder Options/View - and uncheck "Hide file extensions for known file types". This makes it more difficult to for a harmful file (such as an EXE or VBS) to masquerade as a harmless file (such as TXT or JPG).

4. Never open e-mail attachments with the file extensions VBS, SHS or PIF. These extensions are almost never used in normal attachments but they are frequently used by viruses and worms.

5. Never open attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS

6. Do not share your folders with other users unless necessary. If you do, make sure you do not share your full drive or your Windows directory.

7. Disconnect your network or modem cable when you're not using your computer - or just power it down.

8. If you feel that an e-mail you get from a friend is somehow strange - if it is in a foreign language or if it just says odd things, double-check with the friend before opening any attachments.

9. When you receive e-mail advertisements or other unsolicited e-mail, do not open attachments in them or follow web links quoted in them.

10. Avoid attachments with sexual filenames. E-mail worms often use attachments with names like PORNO.EXE or PAMELA_NUDE.VBS to lure users into executing them.

11. Do not trust the icons of attachment file. Worms often send executable files which have an icon resembling icons of picture, text or archive files - to fool the user.

12. Never accept attachments from strangers in online chat systems such as IRC, ICQ or AOL Instant Messenger.

13. Avoid downloading files from public newsgroups (Usenet news). These are often used by virus writers to distribute their new viruses.

DETECTION & REMOVAL

The easiest way to tell that your computer has a virus is by running a complete system scan with updated virus definitions. The tools listed below are all free to download or scan online; anti-virus companies make their money off of ongoing subscriptions - not removing the viruses on your computer. Hence, all the virus removal tools online are free.

Another symptom, but not always reliable, that your computer is infected with a virus, is that your Internet connection is extremely slow and sluggish, and that your computer is working overtime to perform even simple tasks. This sometimes means that a virus is using most of your computer resources to replicate and spread, leaving very little RAM available for you to do work.

Also beware of icons popping up on your desktop with strange names and extensions. Again, it's not always a sign that your computer is infected, but it's a good idea to start scanning your hard drive anyway.

FREE SCANNING TOOLS:

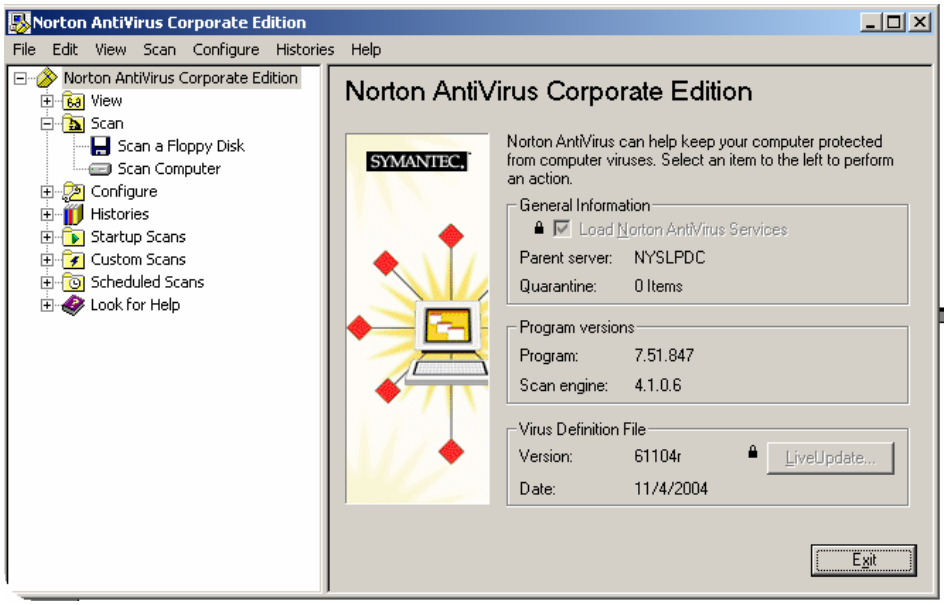
1. **AVG Anti-Virus Free Edition**:
http://free.grisoft.com/freeweb.php/doc/1/

2. **McAfee ADVERT Stinger**:
http://vil.nai.com/vil/stinger/

3. **Symantec Security Check**:
http://www.symantec.com/index.htm

4. **TrendMicro Housecall: Online Virus Check**
http://housecall.trendmicro.com/

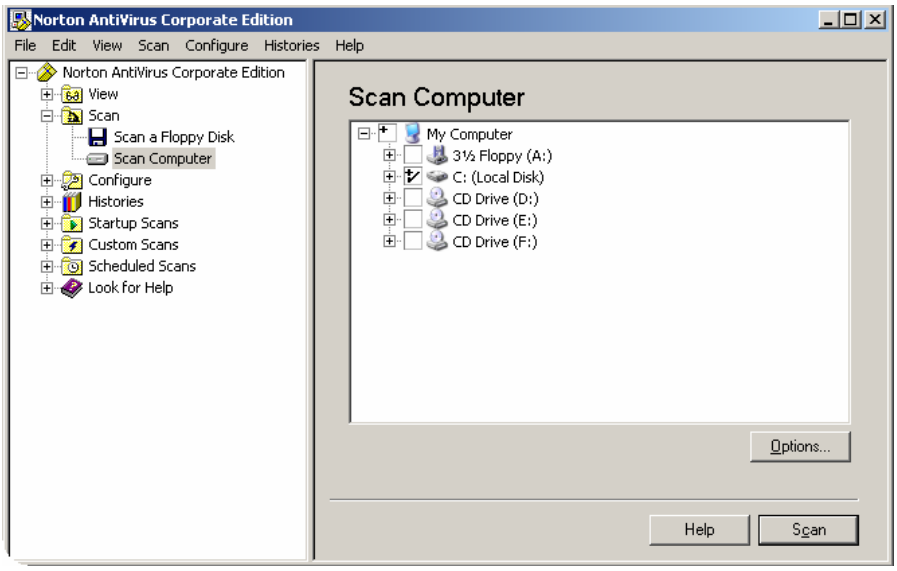
NORTON ANTIVIRUS CORPORATE EDITION



VIRUS DEFINITIONS

The library uses a professional version of Norton Antivirus called "Corporate Edition". Your own virus protection software at home should look somewhat similar.

First off, notice the Virus Definition File on the bottom right hand side. The date of the last update is 11/4/2004. You always want this date to be within a week of the current date - otherwise your computer won't catch the most recent viruses.



NORTON ANTIVIRUS CORPORATE EDITION: SCAN COMPUTER FEATURE

To scan your computer, select Scan -> Scan Computer from the left-hand drop down menu. Select the complete C: drive and hit "Scan". This will take a bit of time, depending on the size of your C: drive. You can do other work while it's scanning, but everything will run slower on your computer.

HOAXES:

Subject: New Virus Alert

Very Urgent!!!!!!!...

PASS THIS ON TO ANYONE YOU HAVE AN E-MAIL ADDRESS FOR.

If you receive an email titled: "It Takes Guts to Say Jesus" DO NOT OPEN IT. It will erase everything on your hard drive. This information was announced yesterday morning from IBM; AOL states that this is a very dangerous virus, much worse than "Melissa," and that there is NO Remedy for it at this time. Some very sick individual has succeeded in using the reformat function from Norton Utilities causing it to completely erase all documents on the hard drive. It has been designed to work with Netscape Navigator and Microsoft Internet Explorer. It destroys Macintosh and IBM compatible computers.

This is a new, very malicious virus and not many people know about it. Pass this warning along to EVERYONE in your address book ! and please share it with all your online friends ASAP so that this threat maybe stopped. Please practice cautionary measures and tell anyone that may have access to your computer. Forward this warning to everyone that you know that might access the Internet.

Joyce L. Bober IBM Information Systems Pittsburgh Mailing Systems 412 - 922-8744

The "Guts to Say Jesus" Hoax

WHAT ARE HOAXES:

From: http://hoaxbusters.ciac.org/

Internet hoaxes and chain letters are e-mail messages written with one purpose; to be sent to everyone you know. The messages they contain are usually untrue. Hoax messages try to get you to pass them on to everyone you know using several different methods of social engineering. Most of the hoax messages play on your need to help other people. Who wouldn't want to warn their friends about some terrible virus that is destroying people's systems? It is hard to say no to these messages when you first see them, though after a few thousand have passed through your mail box you (hopefully) delete them without even looking.

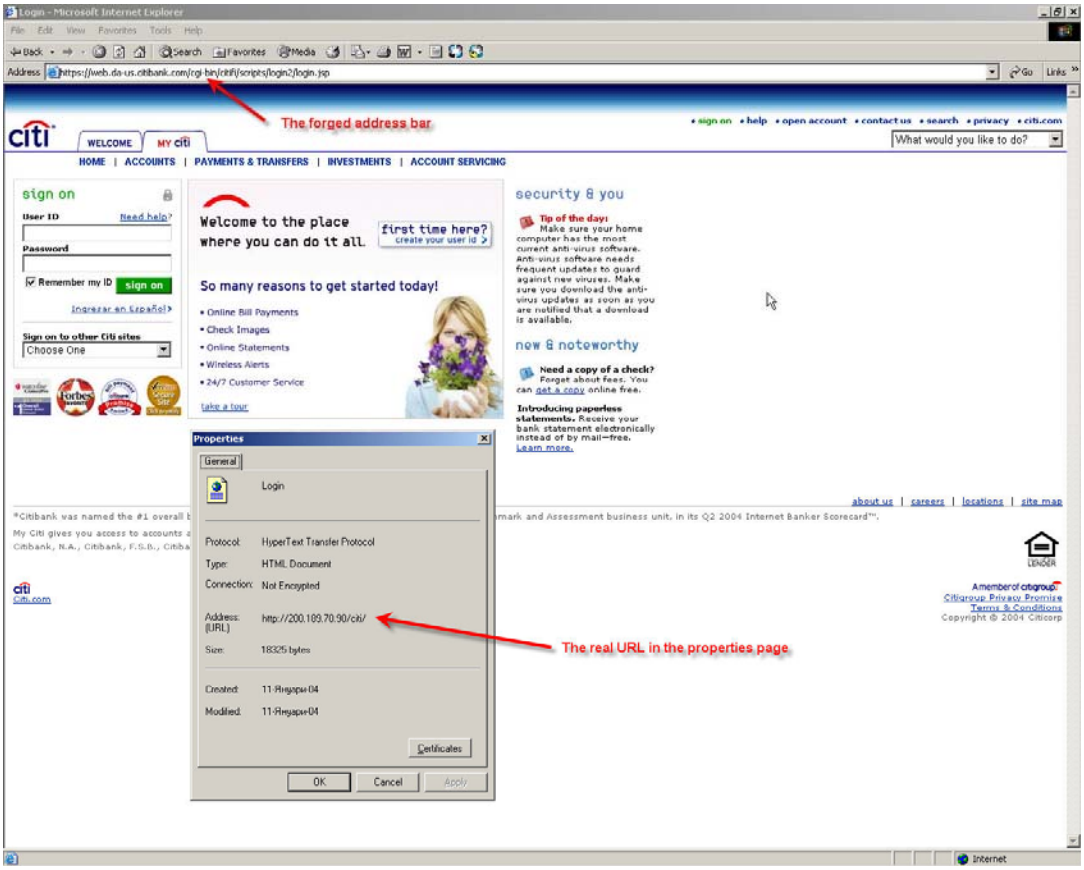
HOAX SYMPTOMS:

1. The sender is known to the user.
2. The threat sounds realistic
3. The urgent nature prompts immediate action.

CURE:

1. Go online and research the supposed virus. Check the major anti-virus sites. Symantec keeps a list of hoaxes at: http://www.symantec.com/avcenter/hoax.html McAfee keeps a similar list at: http://vil.mcafee.com/hoax.asp
2. Do not forward this e-mail to your friends. The more you spread it, the more the hoax continues and the more e-mail gets clogged up with useless messages.

PHISHING SCAMS:



Citibank Phishing Site

WHAT IS PHISHING?

From: http://www.antiphishing.org/index.html

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

FDIC Policy:
Since January 23, 2004, criminals have been using the FDIC's name and reputation to perpetrate various “phishing” schemes. It is important to note that the FDIC will never ask for personal or confidential information in this manner. If you suspect an e-mail or Web site is fraudulent, please report this information to the real bank, company or government agency, using a phone number or e-mail address from a reliable source. Example: If your bank's Web page looks different or unusual, contact the institution directly to confirm that you haven't landed on a copycat Web site set up by criminals. Also, contact the Internet Crime Complaint Center (www.ifccfbi.gov), a partnership between the FBI and the National White Collar Crime Center.

ACRONYMS & DEFINITIONS:

- DOS: denial of service attack
- Hoax - a warning of impending doom that will result from a virus that doesn't exist.
- Macro viruses - viruses hiding in Microsoft Word and Excel documents.

- Malware – short for malicious software – refers to any malicious or unexpected program or code such as viruses, Trojans, and droppers. Not all malicious programs or codes are viruses. Viruses, however, occupy a majority of all known malware to date including worms. The other major types of malware are Trojans, droppers, and kits.

- Payload - the set of instructions that dictates what a virus will do.
- Phishing: messages that "fish" for personal information (i.e. bank account numbers and passwords, credit card numbers, social security numbers).

1. Trojan Horse - dangerous files disguised as useful or desirable programs. A Trojan is malware that performs unexpected or unauthorized, often malicious, actions. The main difference between a Trojan and a virus is the inability to replicate. Trojans cause damage, unexpected system behavior, and compromise the security of systems, but do not replicate. If it replicates, then it should be classified as a virus. A Trojan, coined from Greek mythology's Trojan horse, typically comes in good packaging but has some hidden malicious intent within its code. When a Trojan is executed users will likely experience unwanted system problems in operation, and sometimes loss of valuable data.

2. Virus - specific kind of file designed to cause damage. Viruses generally damage files on your computer's hard drive, then spread to other computers. A computer virus is a program – a piece of executable code – that has the unique ability to replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to just about any type of file and are spread as files that are copied and sent from individual to individual.

3. Worm - software parasite that replicates itself again and again. Unlike viruses, worms usually do not infect other programs on the host machine. Example: program designed to spread itself by exploiting bugs in a network software package.

NOTES: