Supplementary Reading Material – Lecture-1

--NSF Virii Group

for any query mail to f2002001@bits-pilani.ac.in or f2002601@bits-pilani.ac.in

History Of Computer Virus

1981 - The First Virus In The Wild

As described in Robert Slade's history, the first virus in the wild actually predated the experimental work that defined current-day viruses. It was spread on Apple II floppy disks (which contained the operating system) and reputed to have spread from Texas A&M. The virus was named Elk Cloner and displayed a little rhyme on the screen:

It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!
It will stick to you like glue
It will modify ram too
Send in the Cloner!

For more info on Elk Cloner see http://www.skrenta.com/cloner/

1983 - The First Documented Experimental Virus

Fred Cohen's seminal paper *Computer Viruses - Theory and Experiments* from 1984 defines a computer virus and describes the experiments he and others performed to prove that the concept of a computer virus was viable.

1986 - Brain, PC-Write Trojan, & Virdem

The common story is that two brothers from Pakistan analyzed the boot sector of a floppy disk and developed a method of infecting it with a virus dubbed "Brain" (the origin is generally accepted but not absolutely). Because it spread widely on the popular MS-DOS PC system this is typically called the first computer virus; even though it was predated by Cohen's experiments and the Apple II virus. That same year the first PC-based Trojan was released in the form of the popular shareware program *PC-Write*. Some reports say Virdem was also found this year; it is often called the first file virus.

1987 - File Infectors, Lehigh, & Christmas Worm

The first file viruses started to appear. Most concentrated on COM files; COMMAND.COM in particular. The first of these to infect COMMAND.COM is typically reported to be the Lehigh virus. At this time other work was done to create the first EXE infector: Suriv-02 (Suriv = Virus backward). (This virus evolved into the Jerusalem virus.) A fast-spreading (500,000 replications per hour) worm hit IBM mainframes during this year: the IBM Christmas Worm.

1988 - MacMag, Scores, & Internet Worm

MacMag, a Hypercard stack virus on the Macintosh is generally considered the first Macintosh virus and the Scores virus was the source of the first major Macintosh outbreak. The Internet Worm (Robert Morris' creation in November) causes the first Internet crisis and shut down many computers. CERT is created to respond to such attacks.

1989 - AIDS Trojan

This Trojan is famous for holding data hostage. The Trojan was sent out under the guise of an AIDS information program. When run it encrypted the user's hard drive and demanded payment for the decryption key.

1990 - VX BBS & Little Black Book (AT&T Attack)

The first virus exchange (VX) BBS went online in Bulgaria. Here virus authors could trade code and exchange ideas. Also, in 1990, Mark Ludwig's book on virus writing (*The Little Black Book of Computer Viruses*) was published. While there is no proof, hackers are suspected of taking down the AT&T long-distance switching system.

1991 – Tequila

Tequila was the first polymorphic virus; it came out of Switzerland and changed itself in an attempt to avoid detection.

1992 - Michelangelo, DAME, & VCL

Michelangelo was the first media darling. A wordwide alert went out with claims of massive damage predicted. Actually, little happened. The same year the Dark Avenger Mutation Engine (DAME) became the first toolkit that could be used to turn any virus into a polymorphic virus. Also that year the Virus Creation Laboratory (VCL) became the first actual virus creation kit. It had pull-down menus and selectable payloads (though it's reported to not have worked very well).

1995 - Year of the Hacker

Hackers attacked Griffith Air Force Base, the Korean Atomic Research Institute, NASA, Goddard Space Flight Center, and the Jet Propulsion Laboratory. GE, IBM, Pipeline and other companies were all hit by the "Internet Liberation Front" on Thanksgiving.

1995 – Concept

The first macro virus to attack Word, Concept, is developed.

1996 - Boza, Laroux, & Staog

Boza is the first virus designed specifically for Windows 95 files. Laroux is the first Excel macro virus. And, Staog is the first Linux virus (written by the same group that wrote Boza).

1998 - Strange Brew & Back Orifice; JetDB

Strange Brew is the first Java virus. Back Orifice is the first Trojan designed to be a remote administration tool that allows others to take over a remote computer via the Internet. Access macro viruses start to appear (JetDB).

1999 - Melissa, Corner, Win95.SK, Tristate, Infis, & Bubbleboy

Melissa is the first combination Word macro virus and worm to use the Outlook and Outlook Express address book to send itself to others via E-mail. It arrived in March. Corner is the first virus to infect MS Project files. Win95.SK, in April 1999, is believed to be the first viral HLP file infector. Tristate is the first multi-program macro virus; it infects Word, Excel, and PowerPoint files. Infis installs itself as an NT driver and then takes over some undocumented functions. Bubbleboy is the first worm that would activate when a user simply opened and E-mail message in Microsoft Outlook (or previewed the message in Outlook Express). No attachment necessary. Bubbleboy was the proof of concept; Kak spread widely using this technique.

2000 - DDoS, Love Letter, Timofonica, Liberty (Palm), Stream, & Pirus

The first major distributed denial of service attacks shut down major sites such as Yahoo!, Amazon.com, and others. In May the Love Letter worm became the fastest-spreading worm (to that time); shutting down E-mail systems around the world. June 2000 saw the first attack against a telephone system. The Visual Basic Script worm Timofonica tries to send messages to Internet-enabled phones in the Spanish telephone network (later in 2000 another Trojan attacked the Japanese emergency phone system). August 2000 saw the first Trojan developed for the Palm PDA. Called Liberty and developed by Aaron Ardiri the co-developer of the Palm Game Boy emulator Liberty, the Trojan was developed as an uninstall program and was distributed to a few people to help foil those who would steal the actual software. When it was accidentally released to the wider public Ardiri helped contain its spread. Stream became the first proof of concept NTFS Alternate Data Stream (ADS) virus in early September. As a proof of concept, Stream has not circulated in the wild (as of this writing) but as in all

such cases a circulating virus based on the model is expected. Pirus is another proof of concept for malware written in the PHP scripting language. It attempts to add itself to HTML or PHP files. Pirus was discovered 9 Nov 2000.

2001 - Gnuman, Winux Windows/Linux Virus, LogoLogic-A Worm, AplS / Simpsons Worm, PeachyPDF-A, Nimda

Gnuman (Mandragore) showed up the end of February. This worm cloaked itself from the Gnutella file-sharing system (the first to specifically attack a peer-to-peer communications system) and pretended to be an MP3 file to download. In March a proof of concept virus designed to infect both Windows and Linux (and cross between them) was released. Winux (or Lindose depending on who you talk to) is buggy and reported to have come from the Czech Republic. On 9 April a proof of concept Logo Worm was released which attacked the Logotron SuperLogo language. The LogoLogic-A worm spreads via MIRC chat and E-mail. May saw the first AppleScript worm. It uses Outlook Express or Entourage on the acintosh to spread via Email to address book entries. Early August, the PeachyPDF-A worm became the first to spread using Adobe's PDF software. Only the full version, not the free PDF reader, was capable of spreading the worm so it did not go far. September, the Nimda worm demonstrated significant flexibility in its ability to spread and used several firsts. While not new in concept, a couple of worms created a fair amount of havoc during the year: Sircam (July), CodeRed (July & August), and BadTrans (November & December).

2002 - LFM-926, Donut, Sharp-A, SQLSpider, Benjamin, Perrun, Scalper

Early in January LFM-926 showed up as the first virus to infect Shockwave Flash (.SWF) files. It was named for the message it displays while it's infecting: "Loading.Flash.Movie...". It drops a Debug script that produces a .COM file which infects other .SWF files. Also in early January Donut showed up as the first worm directed at .NET services. In March, the first native .NET worm written in C#, Sharp-A was announced. Sharp-A was also unique in that it was one of the few malware programs reportedly written by a woman. Late May the Javascript worm SQLSpider was released. It was unique in that it attacked installations running Microsoft SQL Server (and programs that use SQL Server technology). Also in late May the Benjamin appeared. Benjamin is unique in that it uses the KaZaa peer-to-peer network to spread. Mid-June the press went wild over the proof-of-concept Perrun virus because a portion of the virus attached itself to JPEG image files. Despite the hype, JPEG files are still safe as you must have a stripper program running on your system in order to strip the virus file off the image file (see 2004 for another JPEG attack). On 28 June the Scalper worm was discovered attacking FreeBSD/Apache Web servers. The worm is designed to set up a flood net (stable of zombies which could be used to overwhelm one or more systems).

2003 - Sobig, Slammer, Lovgate, Fizzer, Blaster/Welchia/Mimail

Sobig, a worm that carried its own SMTP mail program and used Windows network shares to spread started the year. Sobig variants continued to multiply throughout the year. Slammer, exploiting vulnerabilities in Microsoft's SQL 2000 servers, hit Super Bowl weekend. Its spreading technique worked so well that for some period of time all of South Korea was effectively eliminated from the Internet (obscured). It received significant media coverage. The unique entry that February saw was Lovgate. This was unique as it was a combination of a Trojan and a worm; two pieces of malware that generally don't get combined. Starting in early May Fizzer spread via usual E-mail methods but also used the KaZaa peer-to-peer network to spread. While generally not unique types, August is in)famous for a combination of Sobig.F, Blaster (also known as Lovsan and MSBlast), Welchia (or Nachi), and Mimail; all spreading rapidly through a security vulnerability in a Windows Distributed Component Object Model (DCOM) Remote Procedure Call (RPC) interface. 2003 also saw what appeared to be a use of worm-like techniques used in the spreading of spam. Sobig dropped a component that could later be used by spammers to send mail through infected machines. The social engineering techniques used by virus/worm writers improved dramatically as well. Some of the malware this year was accompanied by very realistic graphics and links in an attempt to make you think the mail actually came from the likes of Microsoft or Paypal.

2004 - Trojan.Xombe, Randex, Bizex, Witty, MP3Concept, Sasser, Mac OS X, W64.Rugrat.3344, Symb/Cabir-A, JS/Scob-A, CE/Duts-A, W32/Amus-A, WinCE/Brador-A, JPEG Weakness, SH/Renepo-A, Bofra/IFrame, Santy

Year 2004 started where 2003 left off with social engineering taking the lead in propagation techniques. Trojan.Xombe was sent out to a wide audience. It posed as a message from Microsoft Windows Update asking you to run the attached revision to XP Service Pack 1. (This, and like messages that "phish" for personal information, are expected to take a lead role in 2004 -- and, yes, phish is the correct term for a message designed to "fish" for personal information; the technique is called phishing.) In February it was demonstrated that virus writers were starting to ply their craft for money. A German magazine managed to buy a list of infected IP addresses from a distributor of the virus Randex. These IP addresses were for sale to spammers who could use the infected machines as mail zombies. The end of February saw Bizex go after ICQ users through an HTML link that downloaded an infected SCM (Sound Compressed Sound Scheme) file. The weekend of 20/21 March introduced Witty, the first worm to attack security software directly (some Internet Security Systems' RealSecure, Proventia and BlackICE versions). The worm was malicious in that it erased portions of the hard drive while sending itself out. A Mac OS X scare in the form of MP3Concept was announced 8 April. Said to be a benign Trojan, MP3Concept turned out to be nothing more than a bad proof-of-concept that never made it into the wild. The end of April saw the Sasser worm which is the first to effectively use

the LSASS Windows vulnerability; a vulnerability that allowed the worm to spread via an open FTP port instead of through E-mail (even though Microsoft had already issued a patch for the vulnerability -- yet another example of people not paying attention to operating system security updates). Toward the end of May Apple issued critical patches to OS X when a vulnerability that could spread via E-mail and mal-formed Web pages was found. The vulnerability would allow AppleScript scripts to run unchecked; even to the point of deleting the home directory. The proof-of-concept Worm W64.Rugrat.3344 showed up the end of May. This is claimed to be the first malware that specifically attacks 64-bit Windows files only (it ignores 32-bit and 16-bit files). It was created using IA64 (Intel Architecture) assembly code. In June Symb/Cabir-A appeared to infect Nokia Series 60 mobile phones. The worm is designed to spread to nearby Bluetooth-enabled devices. JS/Scob-A appeared in the last half of June. It was special in that it used Javascript to infect Microsoft's IIS Server HTML files through an unpatched vulnerability. User's visiting infected sites were then infected via a download from a Russian site (which was quickly closed down) using an unpatched vulnerability in the IE browser. Mid-July WCE/Duts-A showed up. This was another crude proof-of-concept virus relating to the PocketPC. The virus writer was apparently trying for attention as this text is in the virus: "This is proof of concept code. Also, i wanted to make avers happy.The situation when Pocket PC antiviruses detect only EICAR file had to end ..." Early September saw W32/Amus-A show up. The only thing that qualified this beast to even be mentioned here was that it uses the Microsoft Speech engine in Windows to read out loud: "hamsi. I am seeing you. Haaaaaaaa. You must come to turkiye. I am cleaning your computer. 5. 4. 3. 2. 1. 0. Gule. Gule." where "Gule" is Turkish for "Bye" and "Hamsi" is a small fish found in the Black Sea. August saw WinCE/Brador-A, a backdoor for PocketPC devices. On 14 September that paragon of virus-free file type, the JPEG image, came under attack. To be accurate, the image file itself is not so much to blame as a Microsoft common .DLL file that processes the image file type and has a buffer overrun error that could allow someone to add malicious code to a JPEG image which can then open holes in an attacked system. Shortly after, some Trojan exploits started to appear. In Mid-October SH/Renepo-A showed up on Macintosh OS X systems. This is a shell script worm that installs itself to System/ Library/ StartupItems and other sites and can make files on the system vulnerable to further exploitation. Bofra/IFrame made history over the 20/21 November weekend by becoming the first malware to be placed into Internet ads. It is a MyDoom variant that made its way into AdSolution ad serving software. A hacker broke into the system and inserted the malware into served ads until it was noticed and shut down after about 12 hours. Just before Christmas the Santy worm showed up. The unique thing about this beast was that it used Google to find its victims. The worm used a phpBB vulnerability to deface vulnerable sites running that popular bulletin board software and queried Google to find the sites. The worm was of no danger to users of the sites; it just defaced the sites.

2005 - Bropia, Troj/BankAsh, Commwarrior, Chod, PSPBrick, DSTahen, Troj/Stinx-E

In 2005 the end of January saw the Bropia Worm which targets MSN Messenger for spreading. A bit later the "F" version of this worm became popular because of the sexy.jpg file that spread with it. The 9th of February then saw Troj/BankAsh, the first Trojan to attack the new (still in beta) Microsoft *AntiSpyware* product. This Trojan also was reported to go after various British online banking services. The start of March saw distribution of another mobile phone worm: Commwarrior, which spread via MMS messaging. The end of March/start of April saw variants of Chod appear. This is a sophisticated worm that spreads via E-mail and the MSN Messaging client. Its messages are very close to what a real user would send and, for the first time, attempts to spoof the return address as being from an anti-virus company (Trend or Symantec, and Microsoft, although coming from Microsoft has been a social engineering ploy for some time now). 6 Oct brought the first Playstation Portable Trojan, PSPBrick. This malware does not spread by itself but comes disguised as a MOD for the PSP. When placed on the PSP the MOD erases a number of system files that prevent the PSP from being restarted and basically turns it into a brick; thus the name. And, not to be outdone, on 12 Oct the Trojan DSTahen showed up which basically does the same thing for the Nintendo DS system. Install the Trojan and you end up with a brick. The 10th of November Troj/Stinx-E Trojan horse appeared with a trick that hid itself beneath the Sony DRM software on systems with that software installed. The DRM software is designed to protect copyrighted audio but, in hiding itself, it provided an opportunity for malware to hide behind that software in the hope to avoid detection.

Are There Good Viruses?

By definition virus need to do something bad. Virus researcher, Fred Cohen, had argued that good computer viruses are a serious possibility and offered a reward of $1,000 for the first clearly useful virus; but, he hasn't paid yet.

Most researchers, take the other side and argue that the use of self-replicating programs are never necessary; the task that needs to be performed can just as easily be done without the replication function.

Vesselin Bontchev has written a paper originally delivered at the 1994 EICAR conference, titled *Are "Good" Computer Viruses Still a Bad Idea?*. The paper covers all aspects of the topic. As of this writing, the paper is available at:
ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/goodvir.zip

Still there had been proposals of “Good” Viruses:

The "Anti-Virus" Virus: Several people have had the idea to develop an "anti-virus" virus - a virus which would be able to locate other (presumably malicious) computer viruses and remove them.

The "File Compressor" Virus: This is one of the oldest ideas for "beneficial" viruses. The idea consists of creating a self-replicating program, which will compress the files it infects, before attaching itself to them.

The "Disk Encryptor" Virus: This virus has been published. The idea is to write a boot sector virus, which encrypts the disks it infects with a strong encryption algorithm (IDEA in this particular case) and a user-supplied password to ensure the privacy of the user's data.

The "Maintenance" Virus: The idea consists of a self-contained program, which spawns copies of itself across the different machines in a network (thus acting more like a worm) and performing some maintenance tasks on those machines (like deleting temporary files).