Evolution! From Creeper to Storm

Presentation for the Seminar on "Malware" Daniel Loebenberger

Robin Wielpütz

Bonn - Aachen Institute of Technology
wielpuet@cs.uni-bonn.de

Abstract This presentation shows how malware evolved from times when a computer virus was considered to be a myth until today, when malware is a serious threat to everyone, tied to the history of computing hardware, computer networks, and the antivirus community.

1 Malware

The term „Malware" is a combination of the words „Malicious" and „Software". It serves as a collective term for many different forms of malicious software such as computer viruses, worms, trojan horses, spyware, or adware. A software is considered to be malware if it is „deliberately created to perform an unauthorized, often harmful, action." [VIRUSLIST] Malware is a remarkable threat to users data security and privacy nowadays.

We distinguish three different types of malware [MITP] by the way they spread:

1. The Computer virus is a program which is able to "infect" other programs by modifying them to install copies of itself.
2. A worm is a standalone program that replicates but does not infect other programs.
3. A Trojan Horse is a program with hidden side-effects which are undocumented and not intended by the user, e.g. a video game that installs some other malicious software secretly in a background process.

We can also categorize malware by its function: Spyware for example is such a special type of malware; it is a program that secretly monitors the user's behaviour and collects certain user information. This has not necessarily to happen in a passive way; it might actively redirect the web browser to a designated website or even install other software in the background. It is usually installed by a trojan horse or a worm. There are more types of malware such as dialers, adware, loggers, or botnets. The categories are overlapping and it is sometimes ambiguous to which category a piece of malicious software belongs.

The creators of malware form mainly four groups [VIRUSLIST]. The largest group are the "kids". They want to test their skills without a concrete aim or target to attack. Many of them will later belong to the nect group: The "students". Their malware is more successful but they are still learning and gaining experience. The most dangerous group are the "professionals" which found a commercial use for their skills. They research in hard- and software and organize themselves in communities in the "underground scene" to share experience. A small but also remarkable group are the "researchers". They research at universities or antiviral companies and write proof-of-concept malware. It often happens that the professionals get hold of their conceptual work and misuse it.

The aims of malware writers a also very different. The most harmless use is for advertisement. The software displays paid ads or redirects the user's web browser to pay-per-view sites or installs a dialer. If the software is used to steal passwords, login information, or serial numbers, we speak of computer fraud. Some malware is programmed to intentionally steal money by collecting paypal and bank account information or credit card data. But even the organized crime is present on computers; it maintains and sells spamming platforms or commits Denial-of-Service blackmailing.

2 The Evolution of Malware [VIRUSLIST, WIKI]

All types of Malware depend on an infrastructure to survive and to spread. The infrastructure consists of special computer hardware, portable storage devices, computer networks, operating systems, and common software products. Technical advances in hard- and software as well as in antivirus programs force malware continuously to adapt to new environment conditions, to hide from removal tools and antiviral software, and to find new security holes when known ones have been fixed.

2.1 Before 1970

The only computers were mainframe computers or so called "minicomputers". These large, costly systems used punch cards or magnetic tapes for data storage and only large corporations, universities, or government agencies could afford and maintain them. There was no real machine-to-machine at that time. There was actually no suitable environment for viruses.

2.2 The 1970s [CP92]

Creeper, the first computer virus which was actually a worm, appeared in the early 1970s. By that time, the ARPANET was the first operational packet switching network which was continuously developed. It is regarded as the predecessor of todays global internet. Creeper copied itself to other computers over the network and displayed a simple message on the infected machine: "I'M THE CREEPER: CATCH ME IF YOU CAN". It was comparatively harmless but to stop it, the "Reaper" was anonymously released to catch the Creeper.

Two advances cleared the way for affordable PCs ("Microcomputers") in these years: The Microprocessor for use in the CPU and the first read-write floppy disk drive, a Memorex 650 with a data capacity of 175 kB. Many hardware companies were founded and the number of PCs was rapidly increasing. In 1974, a program called "Rabbit" spread and quickly multiplied itself on an infected machine until it crashed when it reached a certain number of copies. One year later in 1975 the "Pervading Animal"-Game was released. It is still a controversial issue if it was either the first trojan horse or just a badly programmed game. Actually it asked questions in an attempt to guess the type of animal that the user was thinking of. As a side effect it copied itself to every writeable directory marking it with an illegal creation date.

2.3 The 1980s [CP92]

The Apple II Computer released in 1977 was the first highly successful mass-produced PC. It is not astonishing that it was the target of the first real computer virus. In 1981 the "Elk Cloner" infected many PCs. The Apple II computer loaded its operating from floppy disks. Elk Cloner used this characteristic by installing itself to the boot sector of a floppy disk and thus was already loaded before the operating system. Every time when an uninfected floppy disk was accessed, it copied itself to its boot sector. Elk Cloners payload was rather harmless again: It displayed blinking text and joke messages.

Elk Cloner benefited from the fact that most people didn't know what viruses were and even much less how they spread. This unawareness also promoted the next global virus epidemic. The "©Brain" was the first IBM-compatible virus and also the first stealth virus. A stealth virus tries to hide itself from being discovered. When ©Brain detected an attempt to read the infected boot sector, the virus would display the original, uninfected data. The virus was written by a 19 year-old Pakistani programmer and his brother. According to their statement, they wanted to gauge the level of software piracy in their country. Therefore the virus had an internal counter that was incremented every time when a new floppy was infected. Unfortunately, they lost control over their experiment and the virus spread all over the world.

In the later 80s, more dangerous viruses got into the news. In 1987, the Vienna virus was the first to infect .COM-files (parasitic virus). Every time an infected program was called, it infected another .COM-file in the same directory and modified files to cause system reboots. It was also the first virus that could be successfully neutralized (by Bernd Fix) and the idea of antivirus software was born.

The Lehigh virus appeared in the same year and was the first virus that actively damaged data. In its destructive routine it first infected the command.com – by that becoming memory resistant – and afterwards infected four other programs, before it started to randomly destroy data, eventually even destroying

itself. Cautious users began to monitor command.com file size to get aware of an infection.

The Cascade virus was the first self-encrypting virus and for this reason actually the predecessor of polymorphic viruses. Polymorphic viruses have no permanent program code but still maintain their functionality. Cascade only encrypted the program code, but not the decryption routine which remaines unchanged and made it easy for a context sensitive antivirus scanner to detect it. The virus was called Cascade because it made characters cascading down to the bottom line of the screen. In its payload it started deleting files.

The Suriv Family of viruses were memory resident DOS file viruses; Suriv-1 infected .com files in real time, Suriv-2 was the first virus that infected .exe files, Suriv-3 (also known as "Jerusalem") infected both program file types. Released in 1987, Jerusalem caused a major epidemic in 1988. It destroyed all loaded files on an infected machine on every Friday 13th. More and more small antivirus companies released context sensitive virus scanners and so called "Immunizers". Immunizers simply "infected" files like the virus itself but did not contain the dangerous payload.

In 1988, the first Virus Hoax was spread. By that time, "fast" modems made the Bulletin Board System (BBS) very popular. The rumors actually spread like a virus from one scared user to another. In this special case, Mike RoChennel (a pseudonym derived from "Microchannel") send messages containing a warning about a virus that was transferring itself from one 2400 baud modem to another and the only antidote was was to use 1200 baud modems. Many users did indeed heed this advice.

In 1983 the ARPANET hosts switched to the TCP/IP network protocol. This was actually the birth of the internet which was steadily growing from now on. It opened its doors for commercial interest in 1988 and the first to come were the electronic mail services. This was the environment for the first e-mail worm, the so called "Morris Worm". It infected Unix systems over the internet and caused an estimated damage of $96,000,000 by highly increasing the global network traffic. The creator revealed his intention to gauge the size of the internet. It was probably again an out-of-control experiment.

One year later, in 1989, the extremely dangerous "Datacrime" virus spread. After the first harddisk was sold in 1980 – a 5.25-inch harddisk with a capacity of 5MB – it initiated a low-level formatting of a hard disc's zero cylinder, destructing FAT tables and causing an irrevocable loss of data. In reaction to that, many new antivirus companies were founded; among these the Kaspersky Lab, F-Prot, ThunderBYTE, and Norman Virus Control.

2.4 The 1990s

In the early 1990s the DOS/Windows based computer systems gained supremacy over the PC market and the World Wide Web grew.The Chameleon virus – actually a research virus to demonstrate a new concept – which appeared in 1990 infected MS-DOS and Windows. It was a polymorphic virus and used encryption for its body and it scrambled even the decryption routine with junk instructions to avoid detection by context sensitive antivirus software. The antivirus software companies accepted the challenge and came up with more sophisticated detection algorithms. To better fight the increasing number of viruses, many antivirus software companies formed alliances and made takeovers and buy-outs. Mosaic, the first real web browser, was released in 1993. Along with some automatic virus generators that were distributed over the internet.

In 1995, the first macro virus was born and spread through MS-Word documents – it was named "Concept Virus". Scripting code was executed when a Word document was opened. It had access to most Windows system calls. It spread very quickly around the globe in just one month. The macro virus was the most common virus type in the mid 90s. In 1998, CIH Virus caused a major epidemic. The computer virus written by Chen Ing Hau (therefore CIH). Its target was the Portable Executable file format (PE) on the Win9x operating system family. It embedded its very small (about 1kB) code into the file header and did thereby not cause a change in the size of the original file. CIH had a very dangerous payload: When triggered, it filled the first megabit of HDD with Zeros where the partition table and the FAT table are stored. Afterwards it tried to flash the BIOS; on success, the Flash BIOS chip had to be replaced by an expert. From the laypersons view it was obviously "destroying hardware": The PC was no longer bootable and it could cause an irrevocable loss of data.

The World Wide Web and e-mail became ubiquitous and the primary environment for malware to spread. The Melissa Worm was a macro virus that infected Word97 and Word2000 documents. It spread through Outlook by mass-mailing itself to all recipients in the local address book and infected other Word documents on the same machine. It had no dangerous payload but caused severe damage when flooding the mail servers.

2.5 The Year 2000 and beyond

The VBS/Loveletter in the year 2000 – also known as ILOVEYOU – worked very similar. It used Visual Basic Scripting. New was the fact that it made use of social engineering techniques to entice the user to open the infected attachment "LOVE-LETTER-FOR-YOU.TXT.vbs" – of course everyone wanted to who loved him and double clicked the attachment. This tiny little piece of malware caused an estimated $5.5 billion damage.

Another year later in 2001, the Code Red Worm exploited a vulnerability in Microsoft's IIS webserver. It caused an buffer overflow to execute code on the target machine. It spread by randomly checking IP addresses and looking for other IIS servers. In the payload, it was defacing websites by showing the message "Hacked by Chinese!" in the first two thirds of each month and starting distributed denial of service (DDoS) attacks on fixed IP addresses in the last third of each month. About 359,000 hosts were infected in just a few days.

In the year 2003 the Blaster Worm – also known as "Lovesan" – exploited a vulnerability in the operating systems Windows 2000 and Windows XP. A buffer overflow in the DCOM RPC Service made a system vulnerable. Blaster started a DDoS attack on August 15, 2003 against port 80 of windowsupdate.com. Micrsoft could minimize the damage caused by simply turning off this particular domain, while its alternative windowsupdate.microsoft.com remained intact. As a side effect, the Worm caused a system instability that forced Windows' to shutdown; the OS displayed a message that warned the user about the planned shutdown in 60 seconds. The worm contained also a message to Bill Gates: "billy gates why do you make this possible ? Stop making money and fix your software!!". About 9,5 million PCs were infected.

"MyDoom" and "Sasser" caused the major epidemics in the next year. MyDoom spread via E-Mail attachment and installed a backdoor when executed. Then it searched for e-mail addresses to send itself to. The backdoor was used to send spam mails through the infected machine. Sasser, a worm "Made in Germany" by a 17yo boy from Rotenburg, exploited a vulnerable network port of a system. The infected machine was eventually shut down or turned on.

This year's public enemy is the "Storm Worm". It is a highly successful backdoor trojan horse that installs itself on Windows 2000, Windows XP and Windows Vista and mass-mails itself to other computers via e-mail attachment. The infected machines are building peer-ot-peer connections among each other and merge into one large botnet. They constantly being updated to avoid detection by antivirus software. The Storm Worm is a mixture of almost all kinds of today's malware. It is used to send spam mails or perform DDoS attacks. The maintainers of the network are unknown but allegedly belong to the organized cyber crime scene.

3 Summary

As long as computer hard- and software evolve, there will be persons writing and distributing malware to exploit security holes for their own interest. The primary distribution channel will stay the internet and the World Wide Web. With the growing importance of online applications, it is necessary to defend this infrastructures with all possible means against malware.

References

[DF92] David Ferbrache: A Pathology of Computer Viruses. London, 1992
[CP04] Cyrus Peikari, Anton Chuvakin: Security Warrior. O'Reilly, Sebastopol, 2004
[MITP] Ryan Russels et al.: Die mitp-Hacker-Bibel. Bonn, 2002
[VIRUSLIST] Kaspersky Lab: The Virus Encyclopedia
http://www.viruslist.com/en/viruses/encyclopedia
[WIKI] Wikipedia: Timeline of Notable Computer Viruses and Worms
http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms