WHITE PAPER
SEPTEMBER 2001

Computer Viruses – from an Annoyance to a Serious Threat

F-Secure Corporation

Securing the Mobile Enterprise

Computer Viruses – From an Annoyance to a Serious Threat

White Paper September 2001

All product names referenced herein are trademarks or registered trademarks of their respective companies. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

USA	***Europe***
F-Secure Inc. 675 N. First Street, 5th floor San Jose, CA 95112, USA Tel (408) 938 6700 Fax (408) 938 6701 http://www.F-Secure.com/	***F-Secure Corporation*** PL 24 FIN-00180 Helsinki, Finland Tel +358 9 2520 0700 Fax +358 9 2520 5001 http://www.F-Secure.com/

Contents

1. Executive Summary

Fighting computer viruses is a familiar task for every network administrator and most home users today. Several reports have shown that more than 90% of business users encounter viruses in their work. The damages caused by viruses are also significant.

The term virus covers a wide range of computer programs that have one thing in common. Once released, they replicate in a way that cannot be controlled by their author. This can easily, intentionally or unintentionally, lead to worldwide epidemics where millions of computers may become infected. Significant damage may result even if the virus author did not include malicious code in the virus. The virus problem has increased in importance over the past ten years. The first viruses were merely an annoyance that did not cause much harm for any business. Our way to conduct business has, however, become more and more dependent on computers and the Internet. New viruses that benefit from modern networking technology have also emerged. This leads to a situation where new viruses spread faster and faster. Much more critical systems may also be hit by viruses today. This trend can clearly be verified by examining reports about economical damage caused by computer-related crime.

The purpose of this paper is to shed some light on the way viruses work, what they require from the environment to succeed and how the virus situation has evolved over the past ten years. The ultimate benefit for the reader is better understanding of the problem, which makes it easier to assess the threat from computer viruses, to plan computer systems and to handle virus outbreaks. However, this paper does not cover virus prevention and scanning techniques.

Viruses may occur on almost any computer platform with enough programming capability. All kinds of personal computers such as PCs, Macintoshes etc. belong to this category. Handheld computers, such as Palm, Psion and PocketPC, are actually also suitable environments for viruses. The virus problem, however, is worst in the PC environment. Both the number of known viruses and the likelihood of being infected is by far the highest in this environment. For that reason, only PC viruses will be covered in this paper.

F-Secure Corporation strongly discourages anyone from attempting to write viruses. This paper has deliberately been written in such a way that it will not provide significant help to persons attempting to do so. The functionality and impact of computer viruses are described using high-level terminology only; there are no examples of code in this paper.

2. What is a virus?

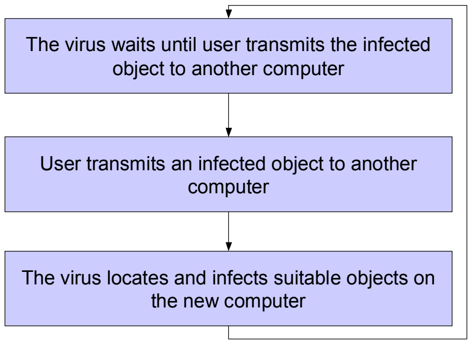
2.1. How does a virus work?

2.1.1. How does a virus spread?

A virus is by definition a computer program that spreads or replicates by copying itself. There are many known techniques that can be used by a virus, and viruses appear on many platforms. However, the ability to replicate itself is the common criterion that distinguishes a virus from other kinds of software.

The term virus is quite often misused. Some viruses contain routines that damage the computer system on which it runs. This so called payload routine may also display graphics, play sounds or music etc. This has lead to a situation where viruses are assumed to cause deliberate damage, even if there are many viruses that don't. The term virus has, for these reasons, become a synonym for malicious software, which is incorrect from a technical point of view.

The process of spreading a virus includes both technical features in the virus itself and the behavior of the computer user. Most viruses are by nature parasitic. This means that they work by attaching themselves to a carrier object. This object may be a file or some other entity that is likely to be transmitted to another computer. The virus is linked to the host object in such a way that it activates when the host object is used. Once activated, the virus looks for other suitable carrier objects and attaches itself to them. This dependency on the human factor slows down the replication of viruses. Another closely related program type, a worm, reduces this dependency and is able to replicate much faster. Worms will be discussed separately in this paper.


The virus waits until user transmits the infected object to another computer
User transmits an infected object to another computer
The virus locates and infects suitable objects on the new computer

A typical lifecycle of a computer virus

From this we can draw the conclusion that a virus does not appear as an object in itself. A virus always resides hidden in some useful object. A macro virus may, for example, infect an important document, but the user does not notice this as the document looks perfectly normal and may be used just like any other document. This means that it is hard for an ordinary user to tell if a system is or is not infected. Special software is needed to examine the system and detect a virus infection.

2.1.2. The anatomy of a virus

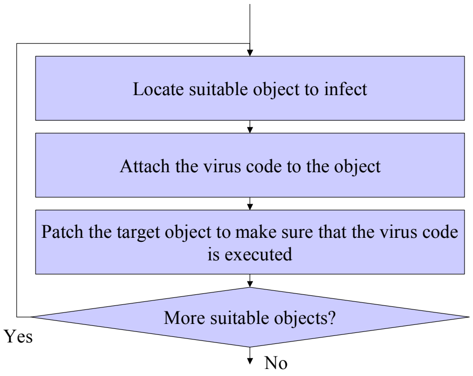
The main parts of a virus' code are the **replication routine** and the **payload routine**. The replication routine is a mandatory part of every virus. If it is missing, the program is not a virus by definition. Some other kinds of malicious software, also called malware, which lack a replication routine but are frequently assumed to be viruses, are briefly covered elsewhere in this paper.

The payload routine is, contrary to common belief, not mandatory. As a matter of fact, there are many viruses that lack a payload routine altogether. The lack of a payload routine may actually be beneficial for the virus and enable it to replicate more efficiently. This is covered in more detail elsewhere in this paper.

The replication routine

The replication mechanism is the most important part of the virus. This part of the virus code locates suitable objects to attach the virus to and copies the virus to these objects. A large number of various techniques have been used for this purpose.

The first problem the replication routine must solve is how to find suitable objects. A virus is always written so as to work attached to a certain type of carrier object, such as a program file or text document created by MS Word, or a limited number of carrier object types. The replication routine must be able to locate objects of the correct type. This can be done by searching through the computer, file by file. However, this is rather inefficient and requires a great deal of computer power. A more elegant approach is for the virus to remain in memory and monitor system activity. This enables the virus to infect files when they are used. The performance impact of infecting a single file is so small that the user would not notice it. This behavior also improves the ability of the virus to spread, as recently accessed files are more likely to be transmitted to another system.


Locate suitable object to infect
Attach the virus code to the object
Patch the target object to make sure that the virus code is executed
More suitable objects?
Yes
No

Functions performed by a typical replication mechanism

The next problem that the replication mechanism must solve is how to attach the virus to the carrier object. This step is done using totally different techniques for different types of viruses. However, one common requirement is that the virus' code be executed when the object is used. Viruses that infect program files may attach the virus code to the beginning or the end of the program file, and patch the entry point so that when the program is run the virus code is executed first. The virus usually transfers control to the original program when it has finished its tasks. This ensures that the original program works properly and the virus avoids detection. Other types of carrier objects, such as MS Word documents, may provide features for embedding macros in the document files. These features make it easy for the replication routine of the virus to attach the code. It can ensure that the code is run properly by using certain naming conventions for the virus' macros.

The payload routine

The payload routine is not a mandatory part of a virus. It does not take part in the replication of the virus in any way. The payload is just a routine that performs something that the author of the virus wants it to perform on all infected computers. The payload routines of different viruses can be divided into two groups, malicious and non-malicious. Some viruses also lack a payload routine altogether.

Mars Land is an example of a virus with a payload that displays animated graphics.

Malicious payloads can, for example, delete files, modify data, plant backdoors in the system or reveal confidential data. Non-malicious payloads may play music, show pictures or animations, promote the author's favorite heavy-metal band etc.

A payload can actually do anything that can be done using programming. The payload of a virus usually cannot damage the hardware of a computer. For a long time, this was considered an absolute truth. New hardware architectures do, however, open some possibilities to damage even the hardware. A good example of this is the W32/CIH virus that became one of the world's most common viruses in 1998-1999. This virus contains a payload that erases the flash BIOS chip in the computer on April 26th of every year[1]. The BIOS chip is responsible for the initial phase when the computer is started. Erasing the chip makes the computer unusable; it cannot even be started using a floppy disk. The chip can be reprogrammed in many computers, but it must be removed from the computer's motherboard for this operation. Some modern computers, especially laptops, use soldering technology that makes it

[1] There are also other variants of the CIH virus with slightly different activation criteria, but this is the most common variant. See http://www.f-secure.com/v-descs/cih.shtml for more details.

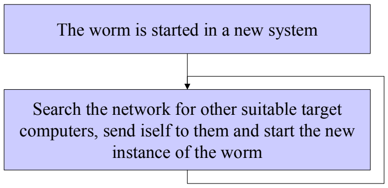
impossible to remove the chip for reprogramming. This means that the BIOS chip cannot be reprogrammed and the motherboard must be discarded and replaced. From a technical point of view, the CIH virus only damages software (the program in the BIOS chip), but due to inflexible hardware design, a hardware component is made unusable. This is a good indication that the old rule of computer viruses only damaging software and data is no longer completely accurate.

The payload routine usually contains some criteria that must be met before the payload activates. This is necessary because a virus needs to remain undetected for some time to give it time to spread. A virus that activates immediately will be detected and removed before it has a chance to replicate. The activation criteria may be almost any data that can be found in the system. The most popular methods are probably to check the system date and activate on a certain date or when a certain number of days have elapsed since the infection. Other possible triggers may be the number of certain events in the system, usage of a certain application or the country code etc.

The payload routines of viruses tend to get a lot of attention from users, media etc. This is natural as the payload often is the only visible part of the virus. The payload may contain funny or exciting effects and it is easy to show pictures of it in TV, magazines etc. Virus researchers are, however, generally less interested in these routines because they are not a significant part of the replication chain of the virus. Payloads usually represent routine programming and the technically exciting stuff is located in the replication mechanisms.

2.1.3. Viruses and worms

The term virus is familiar to most users of computer equipment. This term is often used to describe all kinds of software that replicate from computer to computer, and even incorrectly for some other kinds of software that do not replicate. However, it is not widely known that there are two different groups of replicating software, viruses and worms. The difference between these two groups may not be obvious to the computer user who encounters a virus or worm, but the difference is significant from a technical point of view. A worm, for example, is able to use services provided by a modern networked environment much more efficiently than a virus.


The worm is started in a new system
Search the network for other suitable target computers, send iself to them and start the new instance of the worm

The lifecycle of a typical pure worm

This results in an advantage that enables worms to spread much faster than viruses.

The name **virus** is borrowed from biological science. A biological virus is a passive element that floats around until it hits a suitable cell. The mechanisms of the matching cell are then used to reproduce the biological virus, to express it in a simplified way. The term virus is rather suitable for computer-based equivalents, as computer viruses are passive in the same way. They attach to a carrier object and wait for the object to be transmitted to another computer. Once transmitted, they activate and start looking for other objects to infect.

A pure **worm** is more independent than a virus. A pure worm works by itself as an independent object. It does not need a carrier object to attach itself to. The worm can also spread by initiating telecommunications by itself. There is no need to wait for a human to send the file or document.

There are also intermediate forms that resemble both viruses and worms. Many of the mass-mailing worms that have become widespread actually belong to this category. They may spread attached to documents or other objects just like viruses, but still use email clients to mass mail themselves in a worm-like way. Another fact that separates these from pure worms is that the user must usually open an attachment in the mail before the worm activates. This slows down the replication speed compared to pure worms, as the worm must wait for actions from the receiver. This category of worms does, however, spread much faster than viruses because of the automatic transmission of the worm.

A computer environment must naturally meet some requirements to make worms possible. A worm's method of replication cannot work unless computers are networked in some way. It must be possible for a program to browse the network for other computers, connect to these computers and remotely install and start the worm without user intervention. This is the main reason for the fact that viruses were the most common form of malware in PC environments for a long time. The rapid growth of the Internet has provided worms with the functionality they need. Worms have actually caused almost all of the big “virus-incidents” after the year 1999.

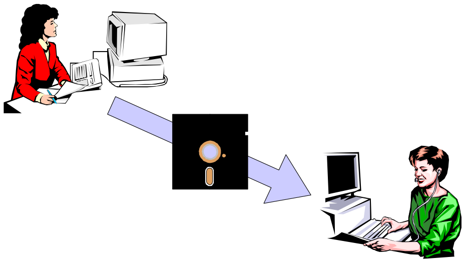
2.2. Different types of viruses

2.2.1. Boot sector viruses

A boot sector virus infects the boot sector of floppy disks or hard drives. These blocks contain a small computer program that participates in starting the computer. A virus can infect the system by replacing or attaching itself to these blocks.

These viruses replicate very slowly because they can only travel from one computer to another on a diskette. In addition, a boot attempt must be made on the target computer using the infected diskette before the virus can infect it. The virus may, however, reside on the diskette and infect new computers even if there is no operating system on it.

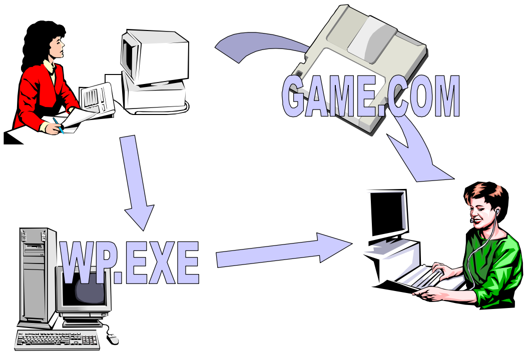
Network communications have replaced diskettes as a means of sharing data. Software is also distributed using networks or CD-ROMs rather than diskettes. This has made the boot sector viruses almost extinct. Some boot sector viruses still remain on stored diskettes, but they are rarely activated and usually do not work in modern operating systems. However, some damage does occur because these viruses may unintentionally damage file systems that they do not understand (i.e. the NTFS file system used by Windows NT).



A boot sector virus spreads when data or programs are transferred to another computer using diskettes

2.2.2. Traditional file viruses

This group of viruses replicates when attached to MS-DOS program files with the EXE or COM extensions. They cannot infect 32-bit EXE files used by newer versions of MS Windows. This group of viruses can replicate over any media that can transfer files, such as diskettes, local area networks, remote lines etc. Email did not play a significant role in spreading these viruses, as it was an unusual way of communicating in MS-DOS and Windows 3.x-based environments. These viruses, however, have a clear disadvantage compared to boot sector viruses; they require that program files be transmitted. In business environments this is usually done only as part of a maintenance procedure, not as part of everyday computer usage. Home users



A traditional file virus can spread when program files are transmitted or shared, regardless of the used media writing their own computer programs provide a much better environment for file viruses.

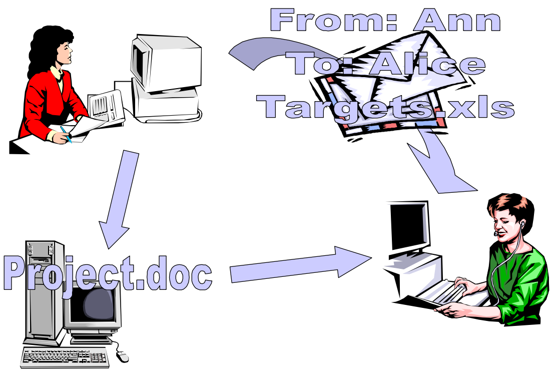
This group of viruses is extinct due to the fact that they rely on operating systems that are no longer used.

2.2.3. Document or macro viruses

Document or macro viruses are written in a macro language. Such languages are usually included in advanced applications such as word processing and spreadsheet programs. The vast majority of known macro viruses replicate using the MS Office program suite, mainly MS Word and MS Excel, but some viruses targeting other applications are known as well.

Documents created using these applications are actually quite complex container files. The files work internally like miniature file systems. Separate so called "data streams" are created for the actual document data, data saved for undo operations, revisions of the document, embedded objects, macro procedures etc. It is usually easy for a virus to add its macros to the file using the application's own functions. High-level interfaces are available and the virus author does not need to understand how the macros are stored. The macro systems of these applications usually include features that make it possible to run certain macros automatically when a document is opened. Viruses use these features to activate when the virus is copied to a new computer.

Macro viruses differ from earlier boot sector and file viruses in many ways. Most differences are beneficial to macro viruses and enable them to spread much faster than any other kind of virus seen thus far. The most important difference is that macro viruses infect data files rather than program files. This takes advantage of a computer environment in a much more efficient way than previous virus types. The purpose of a computer system is to store, refine and communicate data. Moving program files is a maintenance task that does not produce any direct benefit to the owner of the computer system. The system is optimized to handle and communicate data files as efficiently as possible, and the users of the system also



A document or macro virus spreads when documents are exchanged, regardless of the media used use these features frequently. It is clear that a virus that infects data files rather than program files spreads much more efficiently. Another factor that enabled macro viruses to spread even faster was the fact that email was becoming popular in large corporations at the same time (1995). A clear trend could be seen at that time, as multinational companies that used email heavily internally suffered from the most severe macro virus epidemics.

Most macro viruses also contain the virus code in readable source format. Previous virus types were written in low-level languages and compiled into machine code format. This made them unreadable for humans without special tools and advanced programming skills. Macro viruses, on the other hand, were written in a high-level basic-like language that can be understood by most computer professionals. The ability to read, understand and even modify the virus code produced numerous variants of the widespread macro viruses. Some modified versions were even made by mistake when a computer user apparently opened the virus code accidentally and made changes to it.

The macro virus technology also opened new dangerous opportunities for the payload routines. The macro interfaces of the applications made it possible to alter data stored in documents. Some macro viruses deliberately altered data in a way that made it hard to spot the changes.

2.2.4. 32-bit file viruses

Previous file viruses were made for 16-bit program files used by MS-DOS. The 32-bit versions of Windows, such as Windows 95, 98 and NT, use a different and more complex format for the program files. Traditional files viruses cannot infect these files. A new group of file viruses emerged as the 32-bit operating systems became more popular. These viruses are by nature similar to the previous file viruses with the exception that they can infect the new file format and work in 32-bit environments. This category is also called PE-viruses, because the new executable file format’s name is PE (portable executable). The new format is also used by many other modules in the system, such as DLLs, system drivers etc. Some viruses infect these modules as well, but most stick to program files with the EXE extension.

The number of known 32-bit file viruses is rather small. The most probable reason is that the new file format is complex and making a virus that infects these files is significantly harder than making other types of viruses.

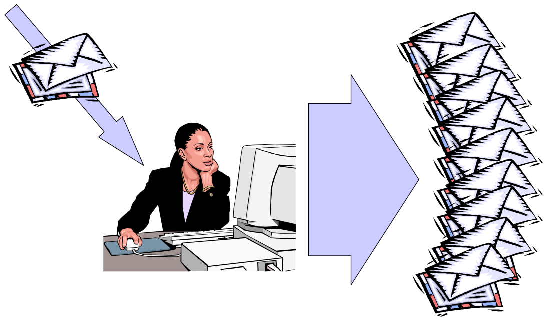
This type of virus has become widespread mainly among home users who tend to exchange program files more frequently than business users.

2.2.5. Worms

Mail worms

A worm is by definition similar to a virus but more independent. The first wave of worms was seen when Internet mail became a standard way to communicate. An email client, and especially address books and mailing lists, provide a powerful way to reach a large number of recipients worldwide with very little effort. Modern, advanced email programs also provide this functionality through APIs that make it possible for computer programs to automatically send messages. All this together provides an environment that enables mail worms to spread much faster than viruses.

A mail worm is carried by an email message, usually as an attachment but there have been some cases where the worm is located in the message body. The recipient must open or execute the attachment before the worm can activate. The attachment may be a document with the worm attached in a virus-like manner, or it may be an independent file. The worm may very well remain undetected by the user if it is attached to a document. The document is opened normally and the user's attention is probably focused on the document contents when the worm activates. Independent worm files usually fake an error message or perform some similar action to avoid detection.



An e-mail worm sends a large number of messages automatically when the user has activated the worm

Once activated, the worm usually searches the address book for suitable addresses. New email messages are created and sent to the selected recipients. The mass mailing may very well contain hundreds of recipients, or as many recipients as there are in the address books. The mass mailing is especially powerful if mailing list addresses can be found in the address books. Another strategy is to remain active in the system and monitor mail traffic. In this case, the worm can, for example, reply to inbound messages as soon as they arrive.

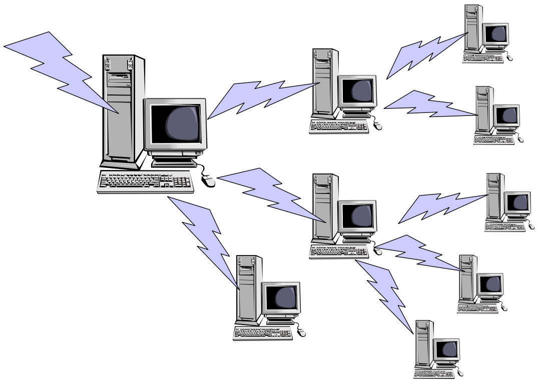
This type of malware replicates much more rapidly for two reasons. It can send itself to as many recipients as it likes and it can do it immediately. A document mailed by a user is under normal circumstances addressed to no more than a handful of colleagues, but the worm can send mail to everyone in the company at once. The mailing may also commence immediately when the computer becomes infected, since the worm does not have to wait until the user wants to share something with his or her colleagues.

Pure worms

A worm is a replicating program that works independently without a host file and without user intervention. Pure worms meet all these requirements, whereas mail worms represent an intermediate form that resembles both viruses and worms.

Pure worms have the potential to spread very quickly because they are not dependent on any human actions, but the current networking environment is not ideal for them. They usually require a direct real-time connection between the source and target computer when the worm replicates. A significant number of the computers connected to the Internet, however, are on-line only temporarily and perhaps behind dial-up connections. Servers are currently the main group of computers that meet these criteria. A larger number of machines, including workstations, may be suitable targets for a worm in local area networks that provide constant connectivity. Some technique to transfer and start the worm on the remote machine is also needed. These kinds of actions are usually blocked for security reasons and worms typically rely on known security holes or misconfigured security policies.

The computers that are connected to the Internet in such a way that worms could access them are usually servers that are maintained by rather security-conscious administrators. The number of such servers is small, compared to the number of workstations in the Internet, and it is hard to find common security holes that enable a worm to spread to all of them. The number of workstations is a lot greater and the likelihood of finding suitable security holes in them is bigger, but they usually do not have a constant connection to the Internet. This means that only a fraction of the computers in each group are vulnerable to worms, and this limits a pure worm's possibilities for success.



A pure worm locates and infects other machines on the same network without user interventions

2.2.6. Other kinds of malware

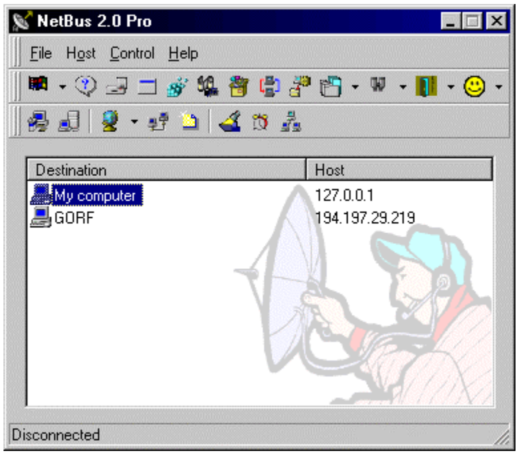
Trojan horses

The name Trojan horse is borrowed from Greek mythology. In the computer world the term refers to a program that contains hidden malicious functions. The program may look like something funny or useful such as a game or utility, but harms the system when executed. Many Trojans contain activation criteria that enable the Trojan to work for a while. The user is convinced that the program is safe and useful, and forwards it to other users before the malicious code strikes.

Trojans lack a replication routine and thus are not viruses by definition. A Trojan is spread to other computers only through deliberate transfer by the users.

Backdoor Trojans

Backdoor Trojans are a special kind of Trojan that grant unauthorized access to computer systems. This type of Trojan is rather common and can pose a significant threat to business users. These Trojans consist of two programs that interoperate: the silent server module planted in a victim's computer and the console used by a hacker. The silent server module acts as a spying tool. The console connects to it using networking protocols and transmits commands to it. This system can then be used to retrieve data from the target computer, modify data, alter system settings, execute programs and even record video and sound if the computer is equipped with multimedia capabilities.



Destination	Host
My computer	127.0.0.1
GORF	194.197.29.219

Disconnected

NetBus is a backdoor Trojan. Its console allows an attacker to perform actions remotely on the victim's computer

The server module of a backdoor Trojan is often hidden in a useful program such as a game or a utility. There are several tools that allow hackers to attach backdoor Trojans to virtually any computer program. The modified program still works normally, but installs the spying tool in the target computer in addition to its normal functionality.

Jokes

A joke program does something funny or tasteless, but does not harm the computer environment. The effect may be music or sounds, video or animations, interactive functions etc. Some jokes may disturb the computer's user interface and be rather annoying, but the effect is temporary and no permanent damage is done. If permanent damage is done, then the program is by definition a Trojan rather than a joke.

2.3. Hoaxes

A hoax is a chain letter that is usually circulated as an email message. These chain letters may have any content and are actually not related to computer viruses in any way. However, the problem is well known to vendors of anti-virus software because many hoaxes warn about a non-existing computer virus.

A trained security expert can usually tell a hoax from a real virus warning. Many hoaxes describe viruses with functionalities that cannot exist in real life. There are also several other attributes that usually disclose the real nature of the message. The source is often not a reliable security expert and the message contains the famous sentence “Forward this warning to all your friends immediately”.

2.4. Who writes viruses and why?

A common belief is that viruses are written by teenage boys. This is true in part, but the situation is changing as new virus writing techniques enter the scene. Writing a working virus is not too difficult, but writing a successful virus is not an easy task. It is not enough to be a good programmer, and knowledge of how modern IT systems work on a larger scale is needed as well. This has lead to a situation where more mature persons, even IT professionals, are involved as well.

It is hard to provide accurate information about who is writing viruses and why. Most virus writers want to remain anonymous and their motives are rarely known. There are several reasons for this.

- Most individuals realize that writing a virus is not ethically acceptable, even if it is legal. Most virus writers want to remain anonymous, or use a pseudonym if they give statements about their creation.

- Computer viruses are a new problem. There are still many countries where the laws do not address virus writing explicitly, even if significant improvements have taken place during in recent years.

- Even if writing a computer virus is illegal, the authorities often lack resources and skills to investigate and trace virus authors.

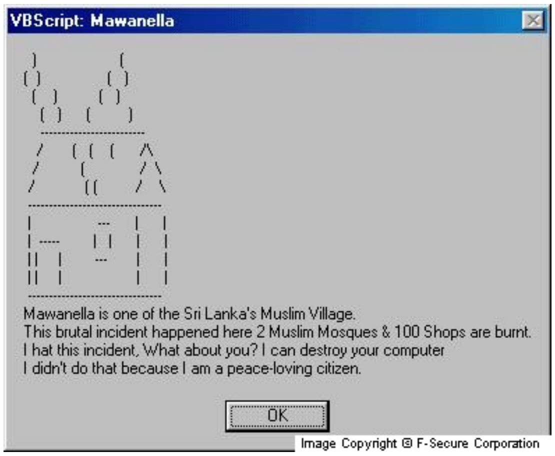
These facts have led to a situation where most virus authors want to remain unknown, and the authorities are not willing to investigate a case due to unclear legislation or lack of resources. However, some successful investigations have been performed. The targets have usually been the authors of the most successful and widespread viruses, which have also caused the most damage.

Another visible phenomenon is the forming of virus writing groups. These groups consist of a varying number of members with a common hobby: writing viruses or performing hacking-related activities. Group members are usually active on the Internet under pseudonyms. Because of efficient networking, the members of a virus-writing group may be located anywhere in the world but still work together on common virus projects. New viruses or hacking tools made by the group are usually clearly labelled with the group's name. Different groups tend to compete about who can write the most advanced viruses or other hacking tools, or attain the most publicity.

The motives of most virus writers remain unknown. There are however some motives that can be identified by examining virus samples or talking to known or anonymous virus authors.

- **Challenge and curiosity**. There are no courses or good books about how to write viruses. Many programmers want to see if they can do it, and do not necessarily realize that the virus may cause significant damage.

- **Fame and power**. Even if the author remains anonymous, it probably gives a kick to read about the virus in headlines. The virus, and possibly the damage it has caused makes other people work and react in some way.



Mawanella is one of the Sri Lanka's Muslim Village.
This brutal incident happened here 2 Muslim Mosques & 100 Shops are burnt.
I hat this incident, What about you? I can destroy your computer
I didn't do that because I am a peace-loving citizen.

Image Copyright © F-Secure Corporation

Mawanella is an example of a virus that spreads a political message

- **Protest and anarchy**. A virus is quite a powerful way to cause intentional damage. There have been cases where a virus is intended to harm a school's network.

- **Proof of concept**. Someone may for example want to prove that a certain replication technique works. This type of virus may also appear on new platforms or applications capable of hosting viruses.

- **Political motives**. A virus may be used to spread a political message. This may, for example, be protests against totalitarian governments, multinational corporations etc. Organized political parties do not use viruses.

Many viruses contain some information about the author of the virus. This information should be used with great care, especially if the indicated author is the real name of an existing person. Virtually no one puts his or her own name in a virus, and any real name in a virus is probably an attempt to harm the reputation of that person. One should also be very careful when drawing conclusions about the virus author based on political messages in the virus. The apparent party or person behind the message may or may not be the real author of the virus. The author may just as well be someone who wants that party to look like a virus writer.

3. Virus history

3.1. Before the viruses – UNIX worms and academic papers

1970 – 1988. Viruses are not a new invention. The idea of self-replicating computer programs has been around for decades. This idea has emerged in science fiction literature, scientific papers and even experiments at least since the early 1970s. Some attempts to perform maintenance tasks in large networks using worms were made, but this technology did not become widespread or well known.

One of the milestones in virus history was the research performed by Dr. Fred Cohen in the early 1980s. Cohen formed the original definition of a virus; a program that can infect other programs by modifying them to include a copy of itself. Cohen's work was truly groundbreaking as it was published before the first viruses were ever made.

In the 1980s the Internet was a network that connected university computers to each other. This network was pretty vulnerable to pure worms, which was to be demonstrated by a young student named Robert Morris. The first major malware incident was probably the Morris worm in November 1988. This UNIX-based worm knocked out almost all computers on the Internet, causing a lot of media interest and many headlines.

3.2. The initial era – Standalone computers and LANs

1987 – 1990. The first PCs were made in the early 1980s. The personal computer concept was new and revolutionary, and its popularity grew faster than anyone expected. PCs were already a usable and affordable technology for companies in the late 1980s. The rapid growth also brought computer technology closer to a larger number of individuals.

Several early viruses were made around 1987 – 1988, at least partly inspired by Cohen's work. Lehigh[2], Jerusalem[3] and Brain[4] are examples of the earliest viruses.

Boot sector viruses were the first type of virus to become common. Floppy diskettes were the only way to transfer data from one PC to another so it is natural that the first viruses used this media to replicate. The other basic type of virus, traditional file viruses, also started to become more common at this time.

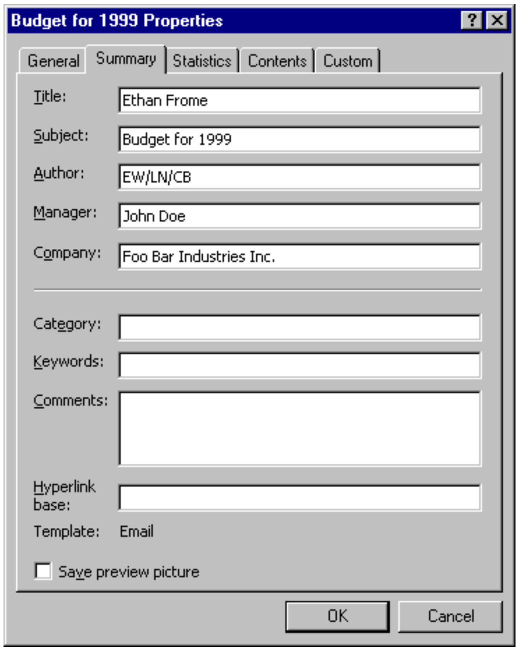
1990 – 1995. Local area networks began to appear in business environments. This development gave the traditional file viruses a small advantage compared to boot sector viruses. However, both groups were still common.

The virus problem was not very well known at this time. Many computer users were able to work for several years without encountering a virus. Finding a virus was a rare event and some users collected the samples they found. Some viruses did, however, cause damage and business users started to become aware of the problem.

The boot sector virus Form[5] became the most widespread virus during this period. Another well-known virus of this era was Dark Avenger, also known as Eddie[6], and which was a very destructive virus.

3.3. The document viruses – Towards a major problem

1995 – 1998. From 1995, local area networks are already standard equipment in most companies using personal computers. Internet connections also started to become popular, especially in larger companies. The concept of email had been known in the UNIX world for decades, but now this technology entered PC-based corporate networks as well. The presence of a local area network and Internet



Budget for 1999 Properties

Title: Ethan Frome
Subject: Budget for 1999
Author: EW/LN/CB
Manager: John Doe
Company: Foo Bar Industries Inc.
Category:
Keywords:
Comments:
Hyperlink base:
Template: Email
□ Save preview picture

The Ethan macro virus modifies the properties of infected documents

[2] Description at http://www.f-secure.com/v-descs/lehigh.shtml
[3] Description at http://www.f-secure.com/v-descs/jerusale.shtml
[4] Description at http://www.f-secure.com/v-descs/brain.shtml
[5] Description at http://www.f-secure.com/v-descs/form.shtml
[6] Description at http://www.f-secure.com/v-descs/eddie.shtml

connectivity opened totally new ways to communicate. The LAN was not just a way to share disks and printers anymore. Email had become a significant communication channel, especially in large multinational companies.

The new technology introduced by email and the Internet revolutionized the way to work with personal computers. But the existing viruses were not able to benefit from the new technology. The number of boot sector virus infections started to decline when LANs, email and CD-ROMs made floppies obsolete. File viruses did not benefit either as email was rarely used for sending program files.

The first macro virus, WM/Concept[7], was discovered in August 1995. This virus was clearly a proof-of-concept virus, as the name also indicates. The virus contained a routine called "Payload" but the only line in this routine was "This should be enough to prove my point".

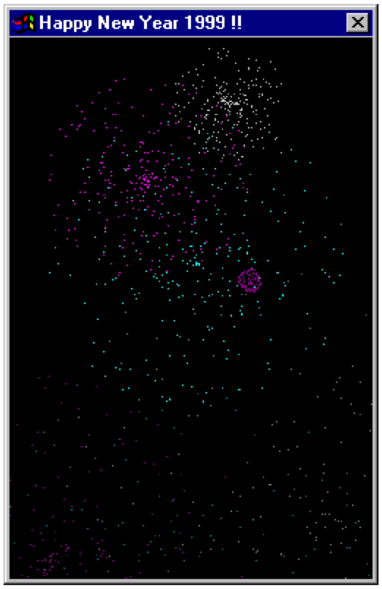
It soon became clear that this new category of viruses, one that infected document files, was spreading quickly. An infected document could be transmitted to a large number of users in minutes. More and more of a company's IT support resources were used for cleaning up virus infections. Viruses were not a funny joke anymore; they had become a real problem especially for large companies.

Some of the common viruses at this time were WM/Cap[8] and XM/Laroux[9].

3.4. Email worms – Increasing replication speed

1999 - . The basic requirements for email worms were already met when corporations started to use email. The trend continued and more and more home users were connected to the Internet. At the same time, email clients evolved and offered more and more functionality.

Happy99[10] was probably the first widespread PC malware program that can be called a worm. This "Happy new year" greeting arrived in a message that was apparently sent by a friend. While the user was



The Happy99 or Ska worm displays a fireworks animation when the recipient activates the attachment

[7] Description at http://www.f-secure.com/v-descs/concept.shtml
[8] Description at http://www.f-secure.com/v-descs/cap.shtml
[9] Description at http://www.f-secure.com/v-descs/laroux.shtml
[10] Description at http://www.f-secure.com/v-descs/ska.shtml

watching the animated fireworks, the worm installed itself in the system so that mail traffic could be monitored.

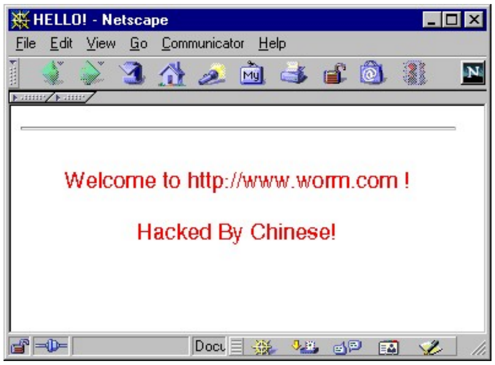
Several large-scale worm outbreaks have occurred between 1999 and 2001. The techniques used vary somewhat, but all these worms have one thing in common, they replicate using email attachments. This also means that they are not pure worms, as the user must open the attachment to activate them. Making the email message look realistic and interesting usually ensures this.

Some of the large outbreaks were caused by well-known worms such as Melissa[11], Loveletter[12] and ExploreZip[13].

3.5. *Pure worms – Getting rid of the human factor*

2001 - . The number of computers on the Internet keeps growing and the connecting lines become faster and faster. Always-on broadband connections are getting popular for home users as well as business users. This leads to a situation where pure worms can find enough target computers to replicate sufficiently.

An email worm replicates significantly faster than a virus, because the delays of waiting for a human user to send stuff is eliminated. Pure worms take this one step further and eliminate the human dependency at the receiving end as well. For this reason, pure worms have the potential to replicate much faster than other types of malware. The number of computers on the Internet that are suitable for pure worm replication is, however, small compared to the number of machines that can replicate email worms. Pure worms have, at the time of writing, not been able to cause large-scale damage on the Internet, despite some smaller outbreaks. However, more and more computers meet the requirements of a pure worm host and this technique has the potential to be one of the major threats in the future.



Welcome to http://www.worm.com !

Hacked By Chinese!

The Code Red worm, also called Bady, was the first widespread pure worm in the modern Internet. It spreads using web-servers and may modify the contents of the server.

To date, the best known pure worm in the

[11] Description at http://www.f-secure.com/v-descs/melissa.shtml
[12] Description at http://www.f-secure.com/v-descs/love.shtml
[13] Description at http://www.f-secure.com/v-descs/zipped.shtml

modern Internet (not counting early UNIX worms such as the Morris worm) is Code Red[14]. Code Red makes use of a security hole in Microsoft's IIS server software that is one of the most common software platforms for web servers. Web servers must be available to the Internet 24 hours a day through a constant connection, and this makes them suitable targets for pure worms. Code Red had the ability to produce a new generation very quickly but difficulties in locating suitable target machines slowed down the outbreak. The Code Red incident did not reach the same dimensions as earlier successful email worms such as LoveLetter and ExploreZip.

3.6. Trends & Conclusions

Adapting to new architectures

The computer systems used by business and home users have developed tremendously over the past ten years. Both system architecture and the way we use computers is totally different from the late 1980s and early 1990s. But the virus problem is still there, worse than ever. As a matter of fact, viruses and worms have been able to adopt and benefit from the new features that modern computer environments offer.

Virus strains do not evolve as they spread. Some argue that viruses are primitive computer-based life forms, but they certainly lack one of the fundamental capabilities of living creatures: to produce descendants that are slightly more adapted to a new environment than their parents. This means that as viruses cannot adapt to new system architectures, they become extinct when the number of suitable host systems decreases. New strains are always created by a human, never through natural evolution.

However, the whole virus problem does adapt to new architectures and benefit from them. New viruses are written as old ones become extinct. This means that there are always new viruses that take advantage of the latest computer architectures. There are always some viruses or worms that are able to efficiently use the latest and most powerful ways to communicate, sometimes even more efficiently than the human users.

Increased replication speed

The replication speed of viruses depends on the replication strategy and the available communication methods. Today's more powerful computer

[14] Description at http://www.f-secure.com/v-descs/bady.shtml

environments enable viruses and worms to spread much faster than a decade ago. This table describes typical replication speeds for the most common virus types.

Virus type	Widespread	Replication media	Typical time needed to produce a new generation	Typical time to become widespread worldwide
Boot viruses	1988 – 1995	Diskettes	Weeks[15]	> 1 year
16-bit file viruses	1988 – 1995	Program files	Weeks[16]	> 1 year
Macro viruses	1995 -	Document files	Days[17]	1 month
E-mail worms	1999 -	E-mail messages	Hours[18]	24 h[19]
Pure worms	2001 -	TCP/IP connection	Minutes[20]	Hours[21]

The conclusion is that replication speed has increased dramatically over the past decade. This emphasizes even further the fact that anti-virus software must be kept up to date to protect the system efficiently. A typical update rate for anti-virus software has accordingly decreased from monthly or bi-monthly to daily or real-time.

[15] The average time from infection of a computer until its user has accessed a diskette, moved it to another computer and booted the other computer from the diskette.

[16] The average time from infection of a computer until its user has moved a program file to another computer and executed it.

[17] The average time from infection of a computer until the user has mailed a document attachment to another user, and the recipient has opened the document.

[18] The average time from reception of the worm until the recipients of the automatically sent next generation opens the attached files.

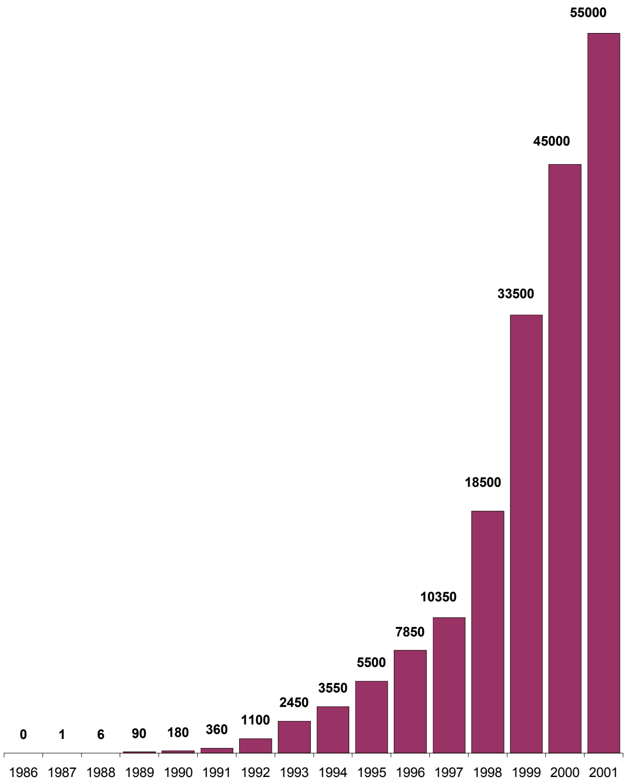
[19] E-mail worms usually spread "following the sun" as users go to work and access their e-mail around the globe.

[20] The time needed for the worm to locate a suitable target, connect to it and transfer the worm file.

[21] This is somewhat speculative because all pure worm outbreaks so far have been rather small.

Fighting viruses gets harder

For a long time, the viruses on the PC platform used a limited number of methods to spread. The viruses were operating system dependent and the number of common operating systems is small.



The number of known viruses on the PC platform has grown dramatically.

Nowadays viruses and worms may use virtually any module in the computer, such as the operating system, sever software or applications, to replicate. This results in a situation where the anti-virus industry must maintain a much wider range of skills to be able to provide antidotes successfully.

There are actually three different factors that make the fight against viruses harder all the time: the increased technical complexity of the virus problem, the increased replication speed of viruses, and the constantly growing number of viruses. Recruiting top researchers and maintaining a skilled research team is one of the keys to success in this area. This factor makes the nature of anti-virus companies different from ordinary software vendors. The constant research effort and real-time publishing of anti-virus definition updates requires a totally different way of working.

A serious threat to business users

The virus situation has increased from a rare phenomenon to an everyday threat. The increased ability of viruses to spread quickly has also made them much more common. At the same time, computer systems have become the backbone of our business infrastructure. This makes companies much more vulnerable for even small disturbances in the computer systems. These two factors together have made computer viruses one of the major concerns for IT security managers. Studies have shown that 94 % of the companies have encountered viruses, compared to 85% the previous year[22]. It is clear that computer viruses are a threat that cannot be ignored in business environments, and this fact is well known and widely accepted.

4. Impact on IT systems

The damage caused by viruses and worms can be divided into two categories: intentional damage and unintentional damage. Intentional damage, or harmless effects, is caused explicitly by the payload routine. Unintentional damage may be caused as a side effect when the virus replicates.

It is a common misconception that all viruses are malicious by nature. As a matter of fact, many common viruses lack a payload altogether. It is natural that a virus that does not harm its hosts spreads much more efficiently than a destructive virus. The virus is dependent on the host and harming it also reduces the virus' chances to replicate.

The term harmless virus is sometimes used to describe a virus that lacks a payload routine, or has a payload routine that only contains non-malicious effects. However, this term is misleading as most viruses are likely to cause some kind of unintentional damage.

Several of the groups listed here apply to all viruses, especially the unintentional PR damages and IT support workload. Many viruses also contain a single or multiple intentional effects.

[22] Computer Security Institute, CSI/FBI Computer Crime and Security Survey 2001, http://www.gocsi.com/

4.1. Harmless effects

These effects are always produced by the payload routine, but they are not malicious. The effect may be a picture, animations or video, music or sounds, interactive functions, political messages etc. These effects usually give you an idea about the virus author's way of thinking, age or nationality. These effects may be funny or annoying and may distract or disturb the user, but they do not cause any permanent damage.

4.2. Compatibility problems

Individuals make viruses and worms and they do not have resources to test their creations on a wide range of computer systems. Nor do they develop the viruses according to quality control systems and guidelines. This makes it likely that they cause compatibility problems when run on systems that differ from the one on which they were developed. These problems can occur as error messages, crashes, inability to access certain functions etc. These problems are grouped as unintentional damage.

4.3. Compromising system integrity

Intentional damage is often caused by erasure or modification of data. Erasing files is perhaps the most obvious way to cause damage. Erasing files, however, is a clumsy way and modern, well maintained, systems can usually recover from backups. Modifying data is a much more sophisticated strategy. Small changes are made to the system now and then. The backup routine stores partially corrupted data until the virus is detected. Restoring the data is hard or impossible as several generations of backups are compromised. The last correct backups may be too old and it may even be hard to tell which backups are or are not valid.

High-level viruses, such as macro viruses, do not have to operate on binary data as previous viruses did. The macro languages provide powerful functions for modifying data in documents. This enables viruses to perform sinister modifications that are critical but hard to detect. For example, it is possible for a macro virus to alter the text of a document before printing, but show the correct form on screen.

Usage of corrupted data may lead to severe damage. An Excel sheet may, for example, be used to calculate the amount of concrete needed for a bridge, or calculate how much fuel a jumbo jet needs to cross the Pacific.

4.4. Granting unauthorized access

Viruses may plant backdoors in the system, or steal passwords. These functions can later be used by hackers to access the system. Damage caused by such hacking activities is hard to predict. Unauthorized usage of the system may, for example, continue unnoticed for a long time.

4.5. Disclosure of confidential data

Viruses and worms have access to the same communication methods as the user, and even use them to replicate. A payload routine may easily locate documents that match certain criteria and send them to anyone on the Internet. Some email worms also cause disclosure of data as a part of replication. The worms that replicate when attached to a document, such as Melissa, send this document to recipients to whom the user had no intention of sending the document.

The following example illustrates this. A company asks for offers from several vendors. One of the vendors is infected with Melissa. The offer is mailed to the buyer as a document infected with Melissa. The buyer opens the document and becomes infected immediately. The Melissa worm examines the address book and send itself to the first 50 addresses on the list. The document that is sent is the offer from the infected vendor, and the list of recipients probably contains the competitors.

4.6. Computer resource usage

Viruses and worms can disturb computer systems by spending resources, either intentionally or unintentionally. Some viruses contain payloads that deliberately eat system resources, but resource consumption is probably unintentional in most cases. Unintentional resource consumption may be caused by errors in the virus or the replication. Code Red is an example of this. Searching for new hosts to spread to requires both network traffic and CPU resources. This load was obvious in the slower response time from the infected web servers or even in the total inability to serve users.

Another type of intentional resource usage is known as denial-of-service or DOS. This is typically performed using distributed technology where a large number of computers run so-called ‘zombies’. All these zombies are programmed to connect to the same computer simultaneously. This does not significantly harm the systems that run the zombies, but the target system is usually blocked due to an overloaded Internet connection.

4.7. Human resource usage

Cleaning virus infections means extra work for the IT support staff. This damage, and the downtime for the user, may result in great expense unless the viruses are stopped properly using anti-virus software.

Even if viruses are successfully stopped using anti-virus software, the cost of maintaining this system may be seen as a cost caused by viruses.

4.8. PR aspects

The attitude towards viruses is negative. The problem is well known and all business users know the severity. Sending a virus to a customer or business partner is not good for the company's image. This may be especially dangerous if the incident makes it to the headlines. This is not at all impossible, especially if the virus was included in a mass-produced software product.

5. Appendix A – Virus terminology

Term	Description
Backdoor Trojan	A Trojan horse that grants unauthorized access to computer systems. A spying tool.
Boot sector virus	A virus that infects the boot record on floppies or hard drives.
Bug	A programming error in a computer program. Viruses are sometimes incorrectly called bugs, "the love bug" for example instead of the virus' real name VBS.Loveletter.
Direct action virus	A direct action virus does not remain active in the computer. It only activates when infected objects are used and terminates when the replication and/or payload routine has been executed.
File virus	A virus that infects executable program files.

Hoax	A chain letter that usually circulates as an email message. Hoaxes are not related to viruses in any way, expect for the fact that many hoaxes warn about a non-existing computer virus.
Host	The object, file or other kind of object to which the virus is attached.
In the wild, ITW	A large number of viruses exist only in virus researchers' collections because they rely on some system or architecture that is no longer in common use. The viruses that are working in today's computer environment and encountered in real life are called "in the wild" viruses.
Joke	A computer program that does something funny or tasteless, but does not harm the computer system.
Macro virus	A virus that infects documents using application specific macro languages.
Malware	A common term for all kind of unwanted software, such as viruses, worms, Trojans etc.
Memory resident virus	A memory resident virus remains in memory as long as the computer is turned on. This enables the virus to monitor system activities and infect other objects efficiently.
Multipartite virus	A virus that can infect several types of objects. Mostly used for hybrids that can infect both boot sectors and 16-bit programs.
Overwriting virus	A virus that overwrites the host file and destroys it.
Parasitic virus	Most viruses require an object to attach themselves to. These viruses are called parasitic, as they cannot exist without their host.
Payload	The part of the code of the virus that does

	intentional damage, funny effects etc.
Polymorphic virus	A virus that changes its own code to avoid detection.
Replication mechanism	The part of the virus' code that replicates (copies) the virus.
Retro virus	A virus that attempts to damage or disturb the function of anti-virus software.
Script viruses	A virus that replicates using scripting languages.
Stealth virus	A virus that attempts to hide its presence from anti-virus software.
Trojan horse (Trojan)	A computer program that contains a hidden, malicious functionality.
Virus	A computer program that replicates by copying itself. The term virus is often used for both viruses and worms, which is not exactly correct from the technical point of view.
Virus creation kit	A programming tool that makes it easy to create viruses without actual knowledge about how a virus works.
Worm	A more independent form of computer virus. Viruses usually depend on humans to copy objects, but worms are able to initiate the copying procedure by themselves.