International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

An Introduction of Computer Virus, History & its Evolution

Manoj Kumar Dhruw
Student, Bachelor of Engineering in Computer Science & Engineering
Kirodimal Institute of Technology, Raigarh (C.G.), India
dhruwmanoj2010@gmail.com

Yogita Dewangan
Student, Bachelor of Engineering in Computer Science & Engineering
Kirodimal Institute of Technology, Raigarh (C.G.), India
yo.gitafriends03@gmail.com

Purushottam Patel
HOD, Department of Computer Science & Engineering
Kirodimal Institute of Technology, Raigarh (C.G.), India
puru_patel123@rediffmail.com

Abstract

Today we live in age of information world and we are using many electronic devices in our daily life. At present, most common and very useful electronic devices are computers and cell phones. Using these devices, today most of people connected through the Internet services and they are unaware of Computer Viruses, Worm, and Malware etc. It is also important to keep secure our electronic data from viruses. In this paper we are trying to tell about Computer Viruses, Worm, Malware etc. and what can it does?

1. What is a Computer Virus ?

There is some difficulty in producing a definition for the term "Computer Virus". Dr. Cohen has presented a mathematical definition of computer virus, which may be roughly expressed as:

> A virus is a program that can 'infect' other program by modifying them to include a possibly evolved version of itself.

However, this definition classifies as viruses many things which would not be considered viruses by those working in the anti-virus field. At the same time this definition would not consider as viruses programs that infect another without modifying the target program itself. [1]

A virus is a piece of software that can "infect" other programs by modifying them; the modification includes a copy of the virus program, which can then go on to infect other programs. [2]

2. How does a virus work ?

2.1 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. [3]

A virus can be successful only if it has a way to propagate from computer to computer. Otherwise, the virus remains only on the computer where it originated, doesn't attract

notoriety or vandalize big networks, and is (from its own point of view) a non-event. [4]

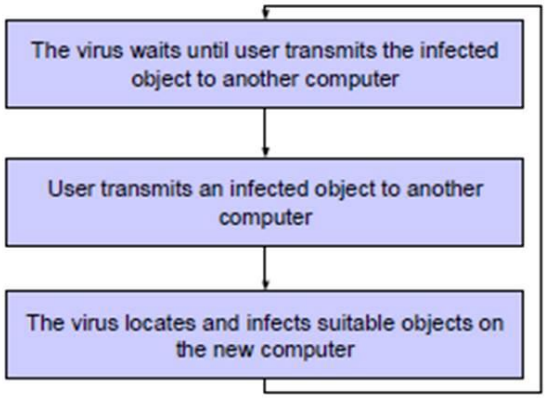

Fig-1 A typical lifecycle of a computer virus

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. [3]

2.2 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.

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. [3]

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.

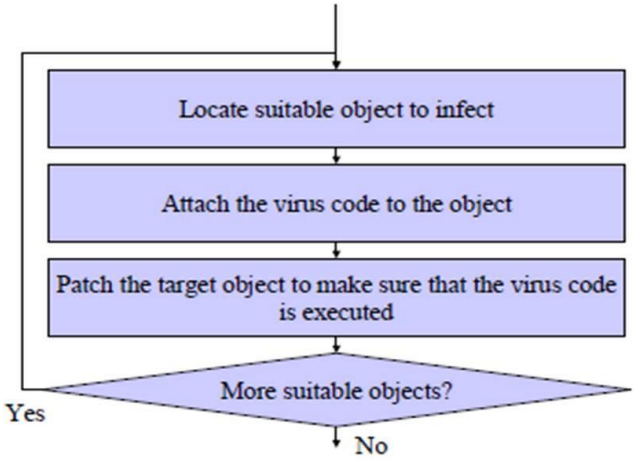

Fig-2 Functions performed by a typical replication mechanism.

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. [3]

3. Variety of Viruses

There are a number of different ways that viruses use to infect a computer system. The two main types of viruses are:

File Infectors: -

These are viruses that attach themselves to some form of executable code. There is a variety of ways in which a virus might attempt to infect a file. On a DOS-based system, file infectors will commonly attach themselves to .COM or .EXE files, although there are many other kinds of infect able objects. [1]

Boot Sector Infectors:-

Only discussed in the context of a PC-compatible system. These kinds of viruses infect executable code which is loaded from disk and called when a computer is starting up. There are a number of different pieces of code which may be modified by a virus to infect a system, such as:

- DOS boot sector [floppy disk and hard disk].
- Master Boot Record (MBR) [hard disk only].
- Partition table [hard disk only].

A virus that is capable of spreading by infecting files and by infecting via any code executed at boot time is known as a multipartite virus.

Boot sector viruses are extremely widespread; as a group they are easily the most commonly found variety of virus on PC-compatible systems.

A virus may be **direct-action or resident**. A direct-action virus is one that when initially executed in the course of normal use of a computer system identifies executable objects for infection and exits once infection has been accomplished. Direct-action viruses may also be referred to as **non-resident** viruses.

A resident virus is one which installs itself some-where in memory, and makes arrangements for the virus body in memory to be executed at some future time; the virus may infect files or take other action (to conceal its presence, for example) at the time it is next executed. For example, some Macintosh viruses if resident in memory will infect an application when that application commences running and performs certain system calls that initialize the Macintosh Toolbox, which consists of a set of utility functions available to all applications.

Some programs useful to the user are also resident programs this includes some antivirus program that monitor computer system operations for actions which may indicate the presence of a virus. [1]

There are some other types of viruses which should be mentioned:

Macro virus:-

Macro viruses infect data files, or files that normally are perceived as data files, like documents and spreadsheets. Many “data file types” have the possibility to include instructions along with the normal content – e.g. Microsoft Word files can contain instructions that tells Word how to show a particular document, or instructions that tells Windows to do certain actions. Just about anything that you can do with ordinary programs on a computer can be done through such so-called macro instructions.

Macro viruses are among the most common viruses today. These are able to infect over networks. [7]

A virus classification by concealment strategy includes the following categories:

- **Encrypted virus:** A typical approach is as follows. A portion of the virus creates a random encryption key and encrypts the remainder of the virus. The key is stored with the virus. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected. Because the bulk of the virus is encrypted with a different key for each instance, there is no constant bit pattern to observe.

- **Stealth virus:** A form of virus explicitly designed to hide itself from detection by antivirus software. Thus, the entire virus, not just a payload is hidden.

- **Polymorphic virus:** A virus that mutates with every infection, making detection by the “signature” of the virus impossible.

- **Metamorphic virus:** As with a polymorphic virus, a metamorphic virus mutates with every infection. The difference is that a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance. [2]

File System or Cluster Viruses:-

Rather than infecting files directly, such a virus modifies directory table information so that the virus is executed first. It would then pass control to the program that the caller really wants so as to avoid rapid detection. "Dir-II" is an example of this variety of virus. [1]

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

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. [3]
- Another common reason for writing viruses was to "punish" users for some perceived infraction. The Brain virus, for example, was said to have been written to punish users of illegal copies of software (software pirates). Users could become legitimate by contacting Brain Computer Services for help. [5]
- Back in the dim mists of time, most virus writers were people who just wanted to test the system and push the envelope. They delighted in finding a way to insert their code into places where others might not find it and held contests of sorts to see who could do what the fastest during various conferences. [5]

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 labeled 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.
- **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. [3]

Fig-3 Mawanella is an example of a virus that spreads a political message

- **Sabotage:** Sometimes the purpose of malicious code might be directly targeted at disrupting the operations of some class of people one doesn't like. While this sort of behavior might seem superficially similar to that of "terrorism" as described in the Political Agitation paragraph above, or to vandalism as described above, it's not terrorism, and it's more personal than typical vandalism. It is a simple criminal act, aimed at a specific target, more akin to assault. People with business interests may do this not for profit or for political purposes, but to damage other businesses' ability to compete, at least temporarily. Government agencies may do so to try to bully another government into doing something it doesn't want to do, as appears to have been the case in the Estonian "cyberwar". The motivation to sabotage may even be based on something as petty as personal revenge. [6]

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]

5. Terminology of Malicious Programs:

Name	Description
Virus	Malware that, when executed, tries to replicate itself into other executable code; when it succeeds the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
Logic bomb	A program inserted into software by an intruder. A logic bomb lies dormant until a predefined condition is met; the program then triggers an unauthorized act.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the Trojan horse program.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality.
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Downloaders	Program that installs other items on a machine that is under attack. Usually, a downloader is sent in an e-mail.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Kit (virus generator)	Set of tools for generating new viruses automatically.
Spammer programs	Used to send large volumes of unwanted e-mail.
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.
Spyware	Software that collects information from a computer and transmits it to another system.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.

[2]

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

6. Virus History

6.1. 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]

6.2. 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. Lehigh2, Jerusalem3 and Brain4 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. [3]

6.3. 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 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.

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.

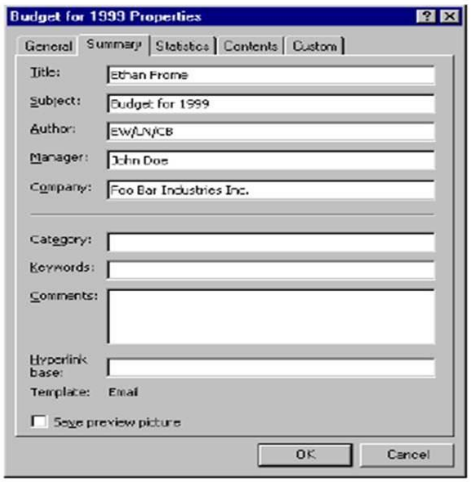

Fig - 4 The Ethan macro virus modifies the properties of infected documents. [3]

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 04
February 2016

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

Fig- 5 The Happy99 or Ska worm displays a fireworks animation when the recipient activates the attachment.

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. [3]

6.5. 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.

Fig- 6 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 modern Internet (not counting early UNIX worms such as the Morris worm) is Code Red. 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]

7. The Evolution of the Virus Problem

- In the beginning, computers were not connected together very well, and computer viruses spread extremely slowly. Files were transmitted via BBSs (bulletin board systems) or on diskette. As a result, the transmission of infected files and boot sectors was geographically limited.

- However, as soon as connectivity increased, mostly by the use of computers in the workplace, the boundaries of computer viruses widened. First there was the local area network (LAN), then there was the wide area network (WAN), and now there is the Internet. The extensive use of e-mail has also contributed to the meteoric rise in the number of macro virus incidents.
- We are now living in a society in which global technology has taken the forefront, and global commerce is driven by communication pathways. Computers are an integral part of this technology and so the information they contain (as well as the malicious code they unwittingly contain) also becomes global.
- Consequently, it is much easier to get a virus today than it was a few years ago. However, the types of viruses that are common today are different than those that were common two years ago.
- Steve White, Jeff Kephart, and David Chess of the IBM Thomas J. Watson Research Center have been following the evolution of viruses, and (among other things) they have concluded that the prevalence of certain types of viruses have been in part determined by changes in operating systems. [7]

Conclusion

The Computer Virus is a major issue at present which is very harmful for various software companies, government organizations, schools, colleges and also one who uses computer or smart phone (cell phone). Computer viruses are very dangerous because of these lots of money and resources are wasted. There is always being a risk for most of software companies or any organization where they afraid of viruses their stored data or important data does not damage by virus. The virus creates many problems, it increases workload and also losses of our valuable time. Mainly Malicious software is designed for harmful purpose. In this paper we have mentioned about the definition of virus, terminology of unwanted programs or malware, and history of virus.

REFERENCES:

[1] Computer Viruses an Introduction, Jeffrey Horton and Jennifer Seberry Department of Computer Science University of Wollongong, Northfields Avenue, Wollongong.

[2] Cryptography and Network Security Principles and Practice, Fifth Edition by William Stallings, published by Pearson Education, Inc. publishing as prentice Hall, Copyright 2011. (Online chapter 21), ISBN 978-81-317-6166-3

[3] Computer Viruses – from an Annoyance to a Serious Threat, White Paper September 2001, F-Secure Corporation.

[4] Computer Viruses for Dummies by Peter Gregory, Published by Wiley Publishing, Inc.

[5] http://www.cknow.com/cms/vtutor/why-do-people-write-viruses.html.

[6] http://www.techrepublic.com/blog/it-security/why-do-people-write-viruses/

[7] Norman Book on Computer Viruses, Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretteville Edited by Yngve Ness.