A brief overview about viruses

David Rozas Domingo

April 12, 2008

1 Introduction: what is (and what is not) a virus?

A virus is a computer program which can copy itself, and can spread from one computer to another, leaving infections while it travels. It is a common mistake to confuse virus with other kinds of malware (malicious software), but the main difference consist of requiring a host program, as a human virus requires a host cell. Other kinds of malware, like zombies or worms, are self-contained and can exist independently. There is not a common agreement about the classification: for instance some authors consider worms as a subclass[1], whereas other authors consider them as a completely different kind[3] due to they have different characteristics:

- Viruses require user interaction to spread, whereas worms do not require any interaction.
- Worms require vulnerabilities in the system, whereas viruses usually rely on unintelligent decision from the user (ex.: open an attachment from an unknown person).
- ...

Due to the space limitations, we cannot extend on the discussion about classification (see the references to find more information), but in this text viruses are considered to be a different class, due to the strong differences in its design and functionality.

2 How do viruses work?

In order to explain how viruses work, we will use the following pseudo-code, which is considered to be the first virus pseudo-code[2]

```
program virus:=
{Goto main-program;
1234567;

subroutine infect-executable:=
{loop:  file = get-random-executable-file;
if first-line-of-file = 1234567
then goto loop;
append virus to file;}

subroutine do-damage:=
{whatever damage is to be done}

subroutine trigger-pulled:=
{return true if some condition holds}

main-program:=
{infect-executable;
if trigger-pulled then do-damage;
goto next;}

next:  }
```

The first line is a jump to the main virus program, and the second line is a special marker to determine if the victim has already been infected. Once in the main virus program part, the virus looks for uninfected executable files and infects them. Then performs a detrimental action to the system (all the time, or depending on a condition).

This kind of virus is easily detectable because the size of the infected program grows (compression techniques discussed in the following section can be used to make more difficult the detection process), but it shows essentially how a virus works.

3 Types of viruses

There has been a big discussion about the different attempts to classify viruses. A good approach is the one suggested in "Cryptography and Network Security" [7], which classifies viruses in the following categories:

- *Parasitic virus*: The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
  Jerusalem[5] is an example of parasitic virus. It is one of the oldest and most common viruses around, and as a result there are numerous variants of it. Jerusalem activates on every Friday the 13th, deleting programs run on that day. 30 minutes after an infected program is run, the virus will also cause a general slowdown of the computer and make a part of the screen scroll up two lines.

- *Memory-resident virus*: Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
  Black Ice [8](discovered in 1995) is an example of memory-resident virus. BlackIce infects .exe files that are less than 10 KB or greater than 32 KB in size. If the month is September through December, the virus deletes files.

- *Boot sector virus*: Infects a master boot record or boot record[1] and spreads when a system is booted from the disk containing the virus.

[1]

Stoned[9] is an example of boot sector virus. It is believed that was created in 1987, and it moves the original master boot record in hard drives to cylinder 0, head 0, sector 7. On floppy disks, the original boot sector is moved to cylinder 0, head 1, sector 3.

- *Stealth virus*: A form of virus explicitly designed to hide itself from detection by antivirus software. Techniques used for hiding are diverse, being compression the easiest to implement, and therefore the easiest to detect. A virus which uses this technique compresses the original program and then adds its code, giving as a result a program with the original size.
  Other viruses, as FRODO[6], manipulate the File Allocation Table[2] to avoid detection, and it appears that there are hardware problems.

- *Polymorphic virus*: A virus that mutates with every infection, making detection by the ”signature” of the virus impossible. A polymorphic virus can use different techniques: it can create superfluous instructions, change the order of independent instructions, etc. Most sophisticated polymorphic viruses use encryption techniques. These viruses use a random key which changes when the virus is duplicated. This random key is used later in order to decrypt a reminder of the virus.
  One of the most famous polymorphic virus is Dark Avenger (also known as Eddie)[4], which codes the most famous polymorphic engine ever: the Mutation Engine (MtE) (1988). MtE could be linked to the plain virus in order to generate polymorphic decryptors.

- *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.
  Win32/Simile (also known as Etap)[10] is a metamorphic computer virus written in assembly language for Microsoft Windows. It was released in 2002. When the virus is first executed, it checks the current date. If the host file imports the file User32.dll[3] then on the 17th of March, June, September, or December, a message is displayed. The virus then rebuilds itself. This metamorphic process is very complex and accounts for around 90% of the virus’ code. After the rebuild, the virus searches for executable files in folders on all fixed and remote drives, infecting some of them (around 50%).

– The “starting point” where the key information about a disk is stored.

[2] – Computer file system used in many Microsoft Operating Systems.

[3] – A file where Windows stores instructions for graphical elements such as dialog boxes and windows.

4 Conclusion

Through this text we have tried to give a brief overview of the huge and exciting world of computer viruses. Although it is a matter which deserves to be discussed in a bigger extension, we would like to tackle the matter of ethics in the creation of viruses to finalize this text.
The creation of viruses has been sometimes related with the passion for discovering and experimenting through the practice, and in some cases has helped to promote the effort in the creation of more robust systems. This is especially notable in the case of other kinds of malware as worms, where vulnerabilities in the system are necessary to attack. On the other hand, viruses are a nuisance for users, and they can produce substantial damages. We can find many cases where there is not any kind of ethic and the only purpose is damaging as much as possible.
It is very important to stand out as well the importance of the virus countermeasures business (topic which has not been tackled due to the space limitations), where in many cases we can find that the same people who were learning through the creation of viruses, are now experts in how to fight against viral attacks. Anyway viruses are here to stay, and we consider that their comprehension and study is as interesting as necessary.

References

[1] Beal, V. A. (2006). The difference between a virus, worm and trojan horse. *http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp*.

[2] Cohen, F. (1987). Computer viruses theory and experiments.

[3] Cooper, R. (2000). Viruses are from venus and worms are from mars. *http://cns.esf.edu/virusvworm.htm*.

[4] Descriptions, F.-S. V. (LastUpdateDateUnknown-a). F-secure virus descriptions : Eddie. *http://www.f-secure.com/v-descs/eddie.shtml*.

[5] Descriptions, F.-S. V. (LastUpdateDateUnknown-b). F-secure virus descriptions : Jerusalem. *http://www.f-secure.com/v-descs/jerusale.shtml*.

[6] McAfee (1990). Mcafee virus descriptions : Frodo.

[7] Stallings, W. (2003). Cryptography and network security: Principles and practices.

[8] Symantec (2007a). Symantec virus descriptions : Blackice.

[9] Symantec (2007b). Symantec virus descriptions : Stoned.standar.

[10] Symantec (2007c). Symantec virus descriptions : W32.simile.