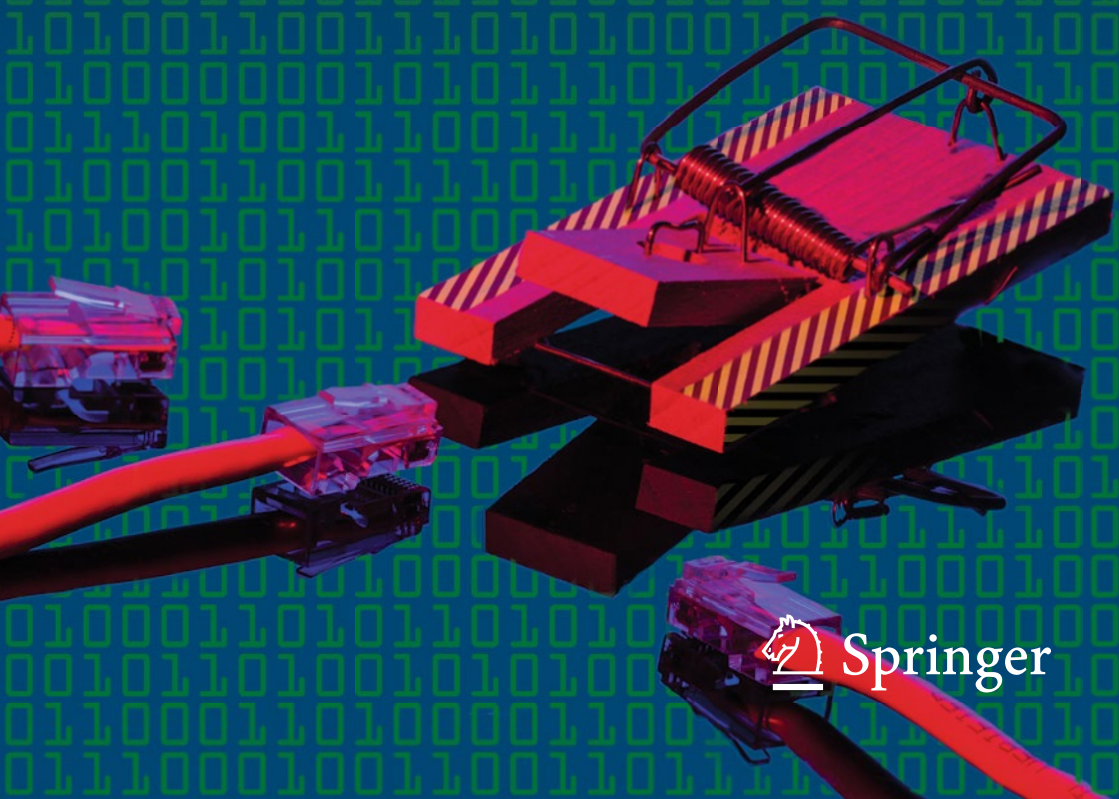
Eddy Willems

Cyberdanger

Understanding and Guarding Against Cybercrime



Springer

Cyberdanger

Eddy Willems

Cyberdanger

Understanding and Guarding Against Cybercrime

Springer

Eddy Willems
G DATA Software
Elewijt, Belgium

ISBN 978-3-030-04530-2 ISBN 978-3-030-04531-9 (eBook)
https://doi.org/10.1007/978-3-030-04531-9

Library of Congress Control Number: 2019935500

Based on a translation from the Dutch-language edition: Cybergevaar by Eddy Willems © Uitgeverij Lannoo nv, 2013. All Rights Reserved.

Cover illustration: The image on the book cover was designed by Tim Berghoff

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgments

You don't write a book on your own. That's why I want to thank some people.

First, Nadine, my wife. She deserves special thanks, because after discussing this project with her for several years, it was she who made the final decision that I should start writing. She was my nontechnical but very active editor, because she wanted to fully understand every detail, and as a result I had to completely rewrite several chapters. She always identifies the essential issues and she knew what she could help me with.

I would like to thank Stef Gyssels, a good friend and journalist, who helped me immensely with countless creative tips. He taught me that writing a book is quite different to writing blog posts or interviews with newspapers. Without his valuable contributions, it would probably have taken me much longer to write this book.

My colleagues at G Data, Jan Van Haver and Danielle van Leeuwen, were my secret weapon. I have benefited enormously from their many critical explanations and comments. Jan, thank you for a booklover's good tips, and Danielle, thank you for your research and your detailed stylistic additions.

I would like to especially thank my good friend, David Harley, for his incredibly valuable help and editing of the English-language manuscript. We evaluated and updated together the content where it was needed. And I thank David as well as Ronan Nugent for their work on the translation that resulted in the first English draft of this book. And I thank Andrew Hayter for his much-valued last-minute review of the final content.

It was very difficult for me to decide which people to ask for a contribution or opinion. I had to limit myself to 15 people. Therefore my thanks in alphabetical order to: Dennis Batchelder, Ralf Benzmüller, Klaus Brunnstein, Bob Burls, Graham Cluley, Luis Corrons, Rainer Fahs, Richard Ford, Nikolaus Forgó, Jeannette Jarvis, Natalya Kaspersky, Guy Kindermans, Peter Kruse, and Righard Zwienenberg.

It would be nice if we could make the world a little safer with this team!

Eddy Willems

Introduction

In recent years, one aspect of cyberlife has been brought to our attention again and again: the days of careless emailing and surfing without undue risk are finally a thing of the past. First came the PRISM affair, followed by the discovery that the United States is monitoring the online activities of the European Union's representatives in New York and in Washington. Again and again we are reminded that the information superhighway is littered with potholes and booby traps. I would like to inform each one of you—young and old, IT expert or layperson, security professional or end user—about the possible dangers that you may face online and warn you of undesirable consequences.

I also want you to be able to use the findings from my book as a tool to defend yourself against danger and to prevent damage to your PC, smartphone, or other device.

I have split *Cyberdanger* into three parts.

In the first part (Chaps. 1 and 2), we immerse ourselves in the history of security threats, from the very first virus to the development of all the other dangers that now threaten us daily. In Chap. 2, I pay particular attention to virus writers: what kind of people are involved in writing malware, what motivates this type of person, and how do anti-malware programs deal with these very special adversaries? This may not seem very important to the reader, not least because he or she wants to know what threatens him today and how she/he can protect himself from it, rather than what was happening in the heyday of "true" viruses. However, I am convinced that this background will help the reader to better understand the chapters that follow: you will learn many terms that you will encounter later in the book. It will give you a deeper insight into the complexity of today's cyberworld—which unfortunately is full of dangers—and you'll understand why so many people are captivated by everything that has to do with malware. With a little luck you will be infected by this memetic "virus"—rather than the malicious kind of (computer) virus (see https://en.wikipedia.org/wiki/Viruses_of_the_Mind).

In the second part (Chaps. 3–6) we delve deeper into the topic of cyberdanger: who are the people behind the threats, what are the threats, and how can we fight them? In Chap. 3 you will gain a deep insight into the functioning of this

"underground economy"—the work and field of activity of cybercriminals. The extent of this "industry," the professional approach of the criminals, and the wide range of suitable products and services to which it gives a home will probably leave you speechless. The content of this chapter is largely the result of various studies by my colleagues at G Data SecurityLabs, people who are dedicated to this topic. At this point I should offer them my sincere thanks.

When talking about cyberthreats, one area should not be left out of the discussion: politically motivated cyberattacks. Chapter 4 is about cyberespionage, cybersabotage, terrorism, and cyberwarfare.

Chapter 5 is dedicated to the antivirus/anti-malware industry: the manufacturers and companies that are working hard to make the Internet safer for users. Chapter 6 enables you to take stock of what threats we currently see as having the greatest impact to those who go online . . . currently almost half the world's population.

The third part of this book contains practical recommendations and advice on how you can better protect yourself. In Chap. 7, myths and misunderstandings are first cleared up, so that it becomes clear to everyone where the true dangers lie and what solutions do not work at all. In Chap. 8 you will find a whole range of practical tips for everyone, from the simplest things ("Keep your software up-to-date") to some real surprises ("Disable your webcam" or—one of my favorites—"Media training for everyone!"). Chapter 9 addresses economic issues with a few more specific and sometimes technical tips.

Chapters 10 and 11 address the role that the state and media can play in tackling these dangers and whether they can succeed in doing so. In Chap. 12, I'll share with you my own ideas about the "Future of Malware" and how we can face future dangers.

As an author, I developed my vision of a distant future into a short story in Chap. 13, into which I have interwoven various predictions about cyberdangers in 2033.

Anyone who reads this book will sometimes face the dangers of the Internet, I am convinced. My dream is to make life a bit harder for cybercriminals and other "shady characters" on the Internet through my book—because the better informed Internet users are about their scams, the harder it will be for them to find innocent cyber victims in the future. It is important for me to know if I have succeeded, and I hope in any case that you enjoy reading it. A good thriller should never be lengthy, and I really hope that I have succeeded in this. Which reminds me: May I first introduce myself?

All Aboard?

Anyone who has ever taken part in an organized trip knows what I'm talking about: we want to get to know our travel guide. Who is he, where does he come from, and why does he, of all people, get to decide in the coming fortnight where we go, and

what we learn about our holiday destination and the wonderful things we encounter on the way? Only when I feel that I have gotten to know my travel guide a bit, am I willing to pay wholehearted attention to his stories.

That's why I think it would be a good idea to introduce myself to you. After all, we have agreed to go on a long journey together through the world of cyberdanger. After this introduction, you will hopefully trust me to bring you safely back from this journey. This adventure is designed to captivate and surprise you, to shock you from time to time, but in the end to make you smarter and more cautious.

My Youth and Technology

I grew up in Mechelen (Belgium), the son of a family of entrepreneurs. Our middle school was probably one of the first in Belgium to teach students computer science. The first lessons focused primarily on simple programming languages such as BASIC. Which was not spectacularly entertaining, but it was enough to arouse my interest.

Very shortly after, besides experimenting with electronics kits, chemistry projects, and amateur radio (then known as CB radio), I spent a lot of time programming, and I was fascinated by both the technical and the communications aspects of coding.

In 1980 computer science was a completely new field of study. The universities were still busy delivering the required academic training and apparently did not know how to handle this new science. First, I decided to study computer science at the Free University of Brussels, but I later switched to what is today called Erasmus College. The focus of my studies was learning programming languages like Pascal, Assembler, and Fortran, which was more of a pleasure than work for me.

During my studies I worked in radio as a technical assistant behind the scenes—a very interesting time during which I learned a lot about the importance of clear and transparent communication to a wide audience.

First Experiences, First PC

After graduating I immediately found employment as a programmer at a food wholesaler. My job was to write COBOL programs on a big machine from Bull. A nice experience, but soon the "user-friendliness" of the device annoyed me: in common with most central and mainframe computers and other servers at the time, it was accessed via a terminal with a black screen with green characters. In addition, these large devices were quite unwieldy: you could not even take them home! Imagine my enthusiasm when our company started using the first IBM PC: a "portable" device that could be used to program COBOL, equipped with a 5 MB hard drive. "How," I wondered then, "would it ever get full?" I immediately realized

the potential of these devices, but it took some time until my colleagues were convinced. Even then it was clear to me that my future would be aligned in some way in the future with these personal computers.

In 1987 I started looking for a new challenge and found what I was looking for, at what was then called Vaderlandsche Verzekeringen (a subsidiary of Nationale Nederlanden, now ING, a Dutch banking and financial services provider). There I had the opportunity to combine my two biggest passions: as a helpdesk specialist I had the great job of helping users solve their problems, but I was also allowed to develop software to improve the helpdesk function. At the same time, we were given the opportunity for self-study and for testing new programs, which I gratefully used to expand my software knowledge.

In 1989 I was asked to test the usability of a program for our company, something that happened quite often. So I was handed a floppy disk, which was attached to a computer science booklet. With the program stored on it, one was supposed to be able to determine whether one belonged to the at-risk group of people who could develop AIDS. The software proved a total failure and I found it very annoying that such a thing should be tested at all.

The next day there was chaos in my office. I started my PC and nothing happened, nothing at all. The screen only displayed a window requesting that I transfer money to a specific account. I restarted the PC, whereupon *nothing* happened anymore. I assumed this was some sort of bug. I started the PC via the system diskette and immediately saw where the "error" lay: the path had been changed and encrypted. Without realizing it, I was just getting acquainted with the first known "ransomware," malicious programs designed to "kidnap" PCs and release them only after paying a ransom. But I managed to fix the problem after a few minutes and then continue to work unhindered.

I was really surprised when, 2 days later, during a broadcast by the national news broadcaster VTM, I heard that this ransomware was spreading uncontrollably and "not a single company had a solution yet." I beg your pardon? Not a single company? But I had solved the problem yesterday. Without further ado, I called the VTM program and talked about my success, which I had achieved without much effort. The next day two camera crews were at my door and the recording was broadcast the same evening.

The Malware Train Had Left the Station

To stay with the terminology of malware: the "virus" had infected me. (Technically, it was a Trojan, and it had compromised my PC rather than "infecting" it, but I'll go into all that further on.) It suddenly dawned on me that this was a huge opportunity for me to do what I always wanted: detect and analyze computer viruses and develop a suitable antidote. I began searching the relevant bulletin boards for the experts and companies involved in viruses. That's how I inevitably came across company names

like McAfee and Dr. Solomon but also interesting personalities in research like Dr. Sarah Gordon (Sect. 2.7).

In 1991 I was invited to a conference on antivirus activities in Brussels where all the important personalities from around the world were gathered: Dr. Solomon himself, Vesselin Bontchev, and many others. I was sure that this would turn out to be more than just a hobby; this was nothing less than my professional future. EICAR[1] was founded during the conference, and so I am proud today to call myself a founding member of this organization.

Fortunately, De Vaderlandsche appreciated my interest in viruses and my experience as a programmer, so my passion for the subject was useful in my job. In the meantime, bulletin boards had been replaced by emails and webpages. That said, it was anything but easy at the beginning: after finally finding the right browsing software—and configuring it correctly after hours of struggle—I was finally at the finish line and able to surf . . . to immediately discover that there was still a gaping emptiness online!

At that time one could find absolutely nothing about viruses and other forms of malware on the Internet. Even companies like McAfee did not have an online presence in 1994. So I decided without further ado to develop my own website with information on viruses and related issues: www.wavci.com. Here, visitors could find many links to IT security sites. My goal was to create a kind of antivirus encyclopedia. This project immediately attracted the attention of many security experts. Within a short time I received many invitations to IT events—including the Virus Bulletin Conference in Brighton in 1996. There I met Harry De Smedt. Harry was a manager at Data Alert, a department of Unit 4 specializing in security software. Data Alert distributed Dr. Solomon's Antivirus Toolkit, at the time one of the most renowned antivirus programs. Harry De Smedt already knew me relatively well through my activities on the Internet, and before I knew it I already had a job offer.

So on January 1, 1997 I joined the security services provider Data Alert. Since then I have participated in almost all the antivirus conferences. However, one event is still at the top of my list: Virus Bulletin! Everyone who counts meets there, and for me there is no better place to inform yourself about the latest developments and to expand your network. The EICAR and CARO[2] conferences are also highly recommended. If I had to restrict myself to a few conferences a year, it would be these three.

After a few years (and acquisitions) Data Alert evolved into NOXS, the security division within Unit 4 Agresso, which is still one of the most important IT suppliers in the market under the name UNIT4. It was no coincidence that during this time I got to know the biggest personalities of the antivirus world: Sarah Gordon, Righard Zwienenberg, Dr. Solomon, Mikko Hyppönen, and others. And I became a member

[1]European Institute for Antivirus Research (Sect. 5.2.2)

[2]Computer Antivirus Research Organization (Sect. 5.2.1)

of the Vforum, an exclusive (invitation only) community of virus experts. All the major players in the anti-malware domain were represented there.

The anti-malware community is a very close group because antivirus vendors show solidarity with each other and like to share their knowledge about malware. I too did my utmost to analyze viruses, if only because it enabled me to detect malware at a number of companies.

My role within NOXS was mainly in research, consulting, and customer training. NOXS, which later became Westcon Security, developed into a big company and enjoyed an excellent reputation. I was deployed to more than 1000 companies, from very small entities to very big corporations, including ministries and government agencies. I also had responsibility for international projects (more on this later—see the "No problem in Saudi Arabia" episode at the end of this chapter). If there was a problem that I could not solve, I just pulled out my "little red book," which contained the contact details of numerous colleagues who worked for the largest software manufacturers and who were available to me day and night to offer help and advice. The "human" network is at least as important in the cybersecurity world as any specific knowledge about malware.

In 2000, at the time of the "Loveletter" virus, the Belgian Telecommunications Minister Rik Daems decided to set up a kind of anti-malware network "in close collaboration with the people." When I heard this message on television in the evening, I could not believe my ears. Why was there talk of close involvement with the Belgian people, even though, as far as I knew, not a single Belgian had been consulted? So with anger I turned once more to VTM, who were very receptive to my criticism, and this led not only to my second appearance on the channel but also to a concrete collaboration with the Belgian government. I worked on a network for the ministry responsible for combating malware, a predecessor to today's Computer Emergency Response Team (CERT). At the beginning of this project, there were occasional warnings about dangerous viruses and other computer threats via public radio stations, in a sense digital traffic news: "We advise caution: there is a new virus . . ." Nobody wanted to spread panic, but caution was imperative. Incidentally, this still applies today.

During this time I occasionally appeared as the official spokesman for the group and gave numerous interviews. In addition, I acted as a consultant on computer pests: Was the virus dangerous or a hoax (Chap. 8, Sect. 8.16)? Did the population need to be warned? I have to say that we were very active at that time and much more committed than today's CERT in Belgium.

My Years as an Evangelist

Over the years NOXS put together a strong team of security experts, most of whom still hold high positions in the security world today. It was a great pleasure for me to fight cybercrime for years in this team. But every story, beautiful as it may be, comes to an end. In late 2007, I switched to Kaspersky Labs, a well-known maker of anti-

malware software. I decided to change jobs because there I was allowed not only to engage in research but also to act as an "anti-malware ambassador," educating people about cyberdangers. So I became a Kaspersky evangelist and part of the Kaspersky expert team. I knew exactly where their competitors were failing, and at the same time I could inform the general public about the importance of IT security.

This task was very much to my liking.

A few years later I had the opportunity to join the German antivirus company G Data Software AG. I could not and would not refuse this offer, because it was an excellent opportunity to learn more and keep my finger on the pulse of the times. And so, in early 2010 I dared to make the change—a decision that I have not regretted for a moment. Here, despite the hard work, there is a fantastic working atmosphere and lots of people laughing together.

Since March 2001 I have sat on the board of the antivirus organization EICAR and hold the post of Director of Security Industry Relationships. Because of my work for EICAR and AMTSO (an international IT security organization; I will comment on both EICAR and AMTSO in more detail later in the book) on the one hand and my job at G Data on the other, I have achieved everything that I set out to achieve in my career. I enjoy a great amount of leeway on a technical level, but also freedom on the human side, and not least the very personal realization that my work helps people. My greatest wish is that this book will help you and save you a lot of trouble.

Disclaimer

One more thing, before we dive deeper into the content. Although I have been active internationally for many years, individual examples or anecdotes may be colored "Belgian." Of course, I give examples that are also relevant to readers from other countries. My starting point always is this: what gets the reader interested in cyberdanger, regardless of his nationality or where he lives?

The same applies to graphics, figures, and numbers that have been included in the book. Fortunately, G Data provides me with a wealth of relevant data and statistics. This allows me to correctly assess and evaluate the current threat situation at all times.

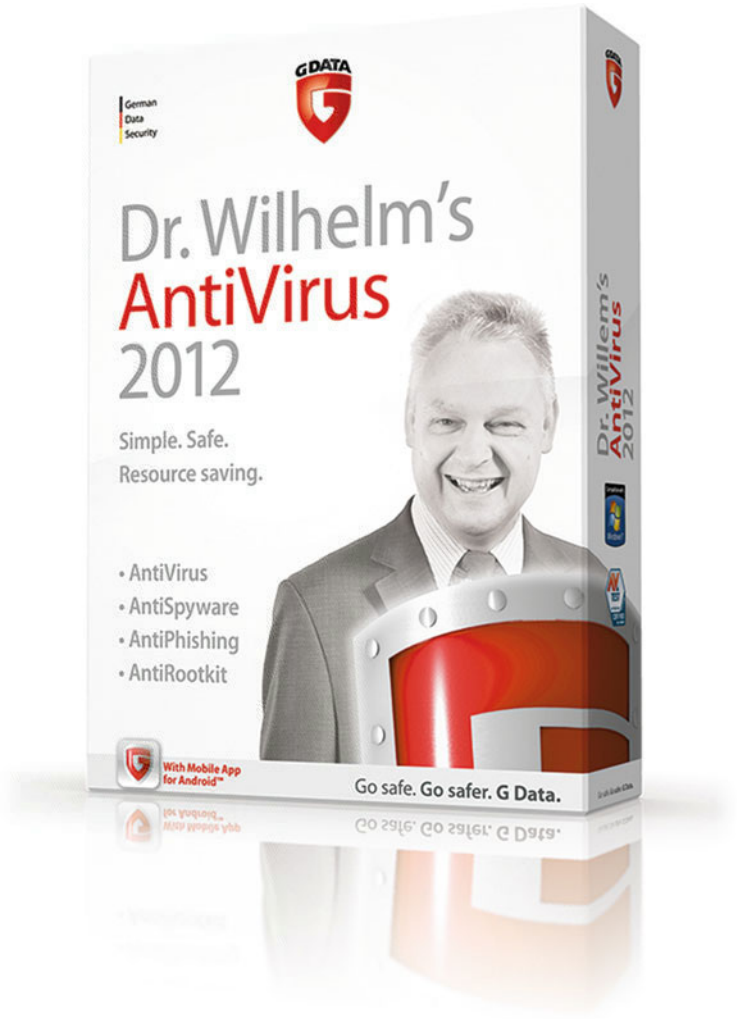
So, enough of the opening credits—now we will enter the captivating world of cyberdanger together. Follow the signposts, take good care, and do not get lost . . . because dangers lurk around every corner.

From My Diary
"No Problem in Saudi Arabia"
October 2001

Sometimes we encounter unexpected situations that turn our lives upside down. Immediately after the September 11 attacks, it was relatively complicated for Americans to travel to Arab countries, and companies like McAfee had real difficulty finding people willing to go on assignments in these regions. For this reason, many companies went in search of Europeans who were competent and adventurous—or crazy enough, some might say– to take on these projects. Right, I'm talking about people like me. So I flew to Saudi Arabia to manage some security projects on behalf of Saudi Aramco, the world's largest oil company.

After a long flight, I landed at about half past ten in the evening, with a strong feeling that this would be a long evening. The wait at the passport control had already taken what felt like an eternity. But then I was asked to wait in a shorter queue. What luck, I thought, until it was my turn. My Notebook bag underwent an extensive investigation and a customs officer's gaze fell on a stack of floppy disks that I had stashed in my pocket. These floppy disks contained a few recent "captured" viruses. However, the officer suspected pornography or other illegal data and confiscated the disks as well as my passport. Although I urgently warned them that loading these diskettes might infect their systems, the customs officials could not be deterred from examining the diskettes more closely. Each of my warnings was received with a terse "No problem, sir." I was deliberately ignored. I could see the warnings appearing on the computer screens, each following the other at breakneck speed, and no trace of a virus scanner. A little later I was allowed to leave the airport with my passport and the diskettes. I seriously doubt that these officials still had "no problem" after that.

When I was writing an article about this incident for the journal Virus Bulletin, I deliberately left unanswered the question of whether the airport's computer system had been infected with my viruses. Actually, I knew with absolute certainty that they had been infected, and only a few days later came the official confirmation when I read in the newspaper that the airport had been the victim of a serious virus attack. For me, a rather unusual premiere, because usually I'm part of the solution, but in this case I was part of the problem. As I said then, "No problem, sir" may have been the understatement of the year.

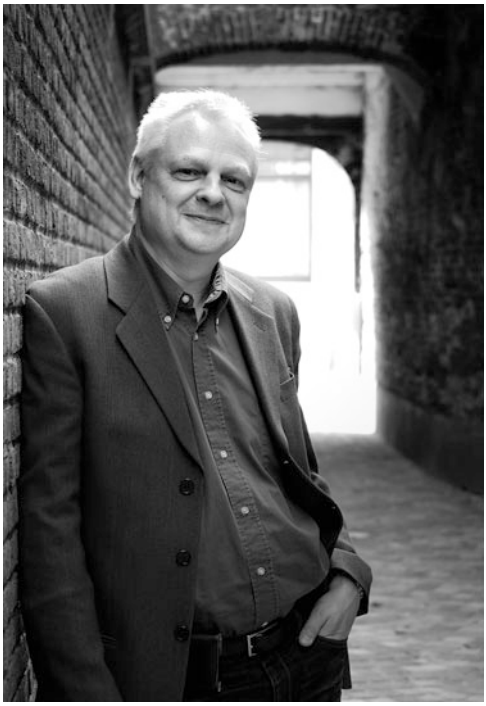


Funny joke with a G Data security box

Elewijt, Belgium Eddy Willems

Contents

About the Author



Author photo by Peter Van de Kerckhove

Malware Expert Eddy Willems, born in Belgium in 1962, has been working closely with the most important organizations in IT security for over 30 years. He sees his role as Global Security Officer and Security Evangelist at G Data Software AG as mediating between the geeks in the security labs and the less-jargon-obsessed everyday computer user. He advises companies, gives presentations and seminars all over the world, and is in constant demand as a speaker at international conferences.

After studying computer science at IHB and VUB, Willems began his career in 1984 as a systems analyst. He first became interested in computer viruses in 1989, and in 1991 was a founding member of EICAR, one of the first European IT security organizations. In the last 25–30 years, Willems has been actively engaged as a member or as a consultant with various CERTs and police forces, WildList Organization International, and commercial companies such as NOXS and Kaspersky Lab. He is a Board

member of AMTSO (Anti-Malware Testing Standards Organization), EICAR (European Institute for Computer Antivirus Research), and LSEC (Leaders in Security).

On G Data's behalf he gives advice to enterprises and governments and gives talks worldwide. Various press agencies and news media such as CNN regularly publish his commentary and security advice. In October of 2013, he published his first book in Belgium and the Netherlands, titled *Cyberdanger* (Cybergevaar). In December 2015 an updated and translated version of his book titled *Cybergefahr* (Springer Spektrum) was published in the German speaking countries, and now this English translation brings this book up to date.

Cyberdanger website:
www.cyber-danger.com
Twitter: @EddyWillems

Chapter 1
Thirty Years of Malware: A Short Outline

First, a warning: people with lively imaginations might find this chapter rather unpleasant. Why? Because it is full of viruses, worms, and other uninvited guests such as Trojans. And yet you *should* deal with the various forms of malware, the unwanted software in your system and on your hard drive, rather than trying not to think about them. As a small compensation you will learn interesting things about Anna Kournikova and even enjoy a declaration of love.

I would first like to explain a few of the most important terms that occur in this book, despite the risk that you already understand them all.

1.1 What Is Malware?

Malware (the portmanteau word used generally as an abbreviation for *Malicious Software*) is a collective term for all types of software that have been written with malicious intent. Viruses, worms, Trojans, spyware, and all other forms of malicious and potentially damaging software fall under the generic term "malware." Interestingly, this term was invented many years after the emergence of the first viruses and worms, when so many types of malware were appearing within a short time that we had to find a collective term for them.

1.2 What Is a Virus?

In biology, a virus is an organism that becomes implanted in a host, for example, in the human body, spreads in it, and often even results in the death of the host. A *computer virus* is so called, because in principle it is roughly the same and thus inserts itself into an application program or the operating system. It's a program that modifies other programs to contain a (possibly altered) version of itself (to use

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_1

Dr. Fred Cohen's informal definition). In the best case, it only takes up space in the main memory and steals CPU cycles. In the worst case, however, the virus causes so much damage to a PC as to make it completely unusable. In such attacks many data can be irretrievably lost: in the worst case, even all the data on the hard disk.

Nowadays, the malware loosely described as computer viruses is different: real self-replicating viruses represent quite a small proportion of all the malware that security programs detect. Most malware, however, consists of files that are installed so as to allow criminals to use the PC remotely for their evil machinations. This will be discussed in more detail in the following chapters.

A so-called *worm* is another form of malware. Again, a file is installed on the computer that tries to spread to other computers. The main difference is that a virus attaches itself in some way to executable code (thus including companion viruses and overwriters) but a worm self-replicates without "infecting" in that sense.

Spyware is another nasty form of malware, which is nowadays used more and more often. Spyware hides on a PC and tracks the user's entire activity. In particular, information relating to surfing behavior is registered and later sold to third parties. Even *keyloggers* that register what is typed via the keyboard are a form of spyware.

Finally, an absolute "treat": the Trojan horse. Often shortened in security circles to the *Trojan*. You certainly know of the Trojan horse from Greek mythology, though most of the story as we know it comes from the later *Aeneid* by the Roman poet Virgil rather than from Homer, even though it's alluded to in *The Odyssey*. Toward the end of their prolonged siege of Troy, the Greek warriors decide to defeat their enemy using a cunning ploy. They pretend to sail away, leaving behind the Trojans a huge wooden horse as an apparent gesture of reconciliation and an offering to Athena. The Trojans happily accept the gift because they believe the war is over. But at night the Greek warriors hiding in the horse climb out and open the gates of Troy, so the Greeks finally get past the city's defenses and march into Troy. A *Trojan* in a PC works in a similar way. So you can imagine what it can do. Once it has settled in the system by pretending to be something useful or desirable, it opens the gates for criminals who can then use the compromised PC for their own purposes, without restriction. The difference is that this is not a gate in the true sense, but rather a kind of backdoor, because often the user does not notice the breach. It may take a long time for the damage to be noticed. Nowadays, more and more Trojans are being created in a variety of forms. For instance, they ensure that a PC can be recruited into a botnet. I will come back to that later in the book (Sect. 1.4). There is a big difference between viruses, worms, and Trojans: the latter do not automatically spread (self-replicate) to other machines.

Note To circulate a computer virus is a criminal offense almost everywhere in the world. If you still want to experiment with a computer virus anyway ... well, I warned you!

1.3 The First Generation

Experts do not agree on which virus came first. For some it is *Elk Cloner* from 1982, though this may not have been the first malware to target the Apple II. Most consider that it was the worm *Creeper*, an experimental computer program from 1971. Most experts consider the *Brain* virus of 1986 to be the first PC-specific culprit. Both Elk Cloner and Creeper more or less conform to the definition of a virus established by the scientist Frederick Cohen in 1983 and later adopted generally. However, he did not write down this definition using the term "virus" until 1983. That's one of the reasons why Elk Cloner was not widely considered to be a virus for a long time—still the case for many people. Another reason may be that it was relatively quiet on the virus front for a few years and the age of the active virus was heralded by the subsequent appearance of Brain. Both viewpoints are valid, but Brain was certainly the first (PC) virus to appear after Cohen introduced the term.

Did You Know . . .**?** For years, the Apple fanbase looked down on the Windows platform because almost all viruses were found on Windows, which is why, in their view, Windows was the source of all evil. But Elk Cloner, the first "virus *avant la lettre*" was written specifically for AppleDOS 3.3 (which preceded the better known Mac operating system). With the evolution of the Internet, this type of malware has created a precedent for the development of Rootkits, Bootkits, and AutoRun worms on USB sticks: more on that later.

In the months following Brain, more and more viruses appeared, many in the form of programs on floppy disks copied to the boot sector. In principle this was not very dangerous—it was more like a game where people could make fools of themselves—but it was not the aim to threaten data or programs. But there were exceptions: the *Christmas Tree* (CHRISTMAS EXEC) worm (not a boot sector infector and ran on IBM VM/CMS mainframes, not PCs) not only generated a Christmas tree without sparkling lights on the screen, it also completely paralyzed many networks through its massive distribution.

With the publication of Ralf Burger's book *Computer Viruses: A High-Tech Disease* in 1987, the situation changed fundamentally. This book became the bible for the people who wrote almost all the viruses in years that followed. Another example of well-known malware from this period is the *Morris worm* or *Internet worm* of 1988, which infected a staggering 10% or so of all computers connected to the Internet—which was 60,000 PCs. That may sound ridiculously small, but please remember that most people at the time did not even know about the existence of the Internet. As we now know, Morris was the first big Internet worm known at that time, but certainly not the last one.

Malware has kept evolving, with ever more features and capabilities. For example, *Ghostball*, the first multipartite virus, appeared in 1989. Multi-what? Well,

"multipartite" actually means that the virus has more than one infection vector (ways to infect a victim's systems). The Ghostball virus was contained in both executable files and the viral code for the boot sector, whereas in the past just files or only the boot sector had been targeted. This feature made finding out how it worked more of a detective mystery for virus hunters, because the virus was able to change its infection method, and it was thus difficult to trace its modus operandi. While malware that uses more than one way onto a victim's system is still common, the "file and boot" type of multipartite virus proved less effective at that time than might have been expected.

But 1989 was also the year that brought us the *AIDS* diskette, which I mentioned in the introduction. Historically, this could be considered an even more important threat than Ghostball, because it was so-called Ransomware, malware that could "kidnap" the computer system so that the owner of the PC would have to pay ransom to buy the "freedom" of his computer and regain access to its programs and data.

In 1990 Ralf Burger—yes, him again!—created the first polymorphic virus, a virus that takes on a different appearance after each copy while the underlying algorithm remains unchanged. This also makes it a lot harder for the virus hunters: software intended to detect malware must now recognize any new form of the virus. Some pessimists saw this as the beginning of the end, but luckily solutions to this problem were finally found. Though not before several B-list antivirus products had proved unequal to the challenge and were simply discontinued.

In 1992 Michelangelo appeared, the first virus to enjoy widespread media interest. All the computers that it infected ran normally—until March 6, Michelangelo's birthday. Then the first 100 characters of the boot sector were overwritten with zeros, which meant that the computer could not boot anymore. The virus caused tremendous panic both in the media and among users. According to expert opinion, millions of PCs would be infected with this virus, so it was generally recommended not to start up PCs on March 6 (As opposed, presumably, to simply using antivirus software to remove it! Well, why miss the chance of a day off?). It is believed that several thousand computers eventually became unusable (short of reinitializing the hard disk, but that meant losing the data and applications previously located there) due to the virus. One thing is certain: the virus triggered a true mass panic way out of proportion to the number of instances where it actually caused damage.

1.4 Generation Internet

The worst, however, was still ahead of us, because until the mid-1990s viruses spread at snail's pace from diskette to floppy disk, and, in the worst case, they entered an intranet. Of course, many viruses could no more spread over a local network than they could through the Internet. But others spread considerably faster as we moved into the Internet age—and the extent of the possible damage also grew rapidly! While in the past we had talked about a maximum of several thousand computers infected by a single virus, by 1995 cases of hundreds of thousands of infected computers were considered to be almost normal, or at least feasible.