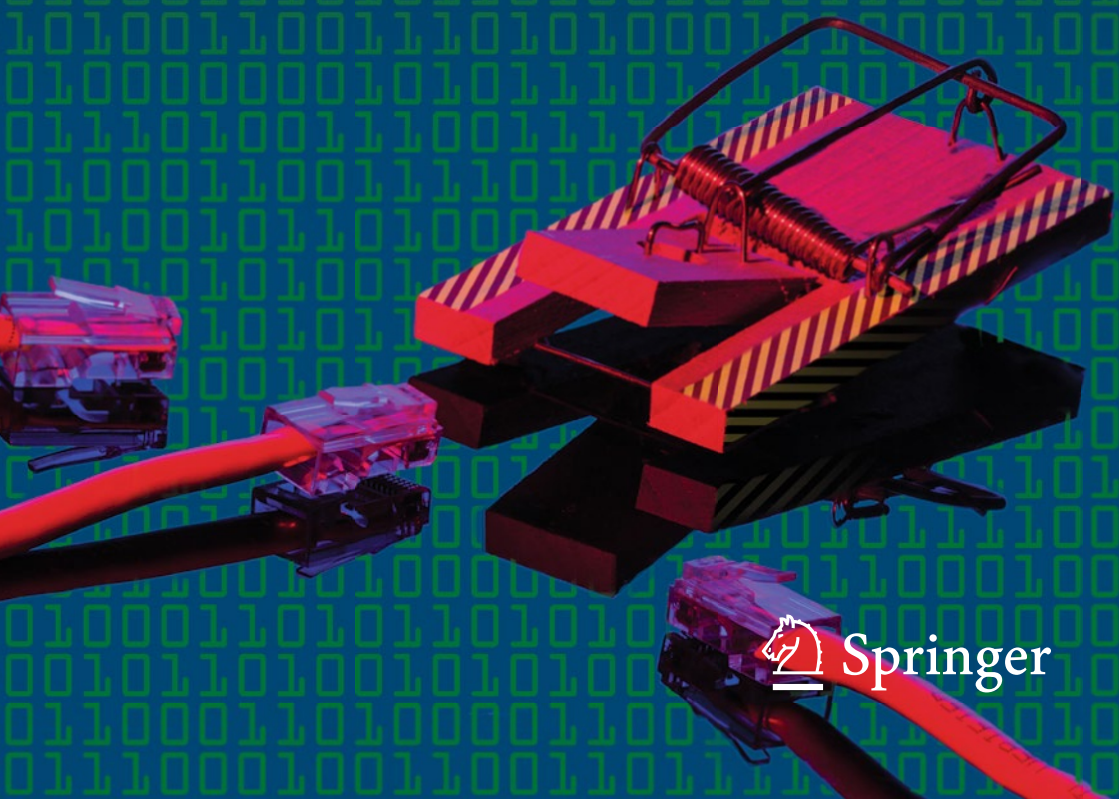
Eddy Willems

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.

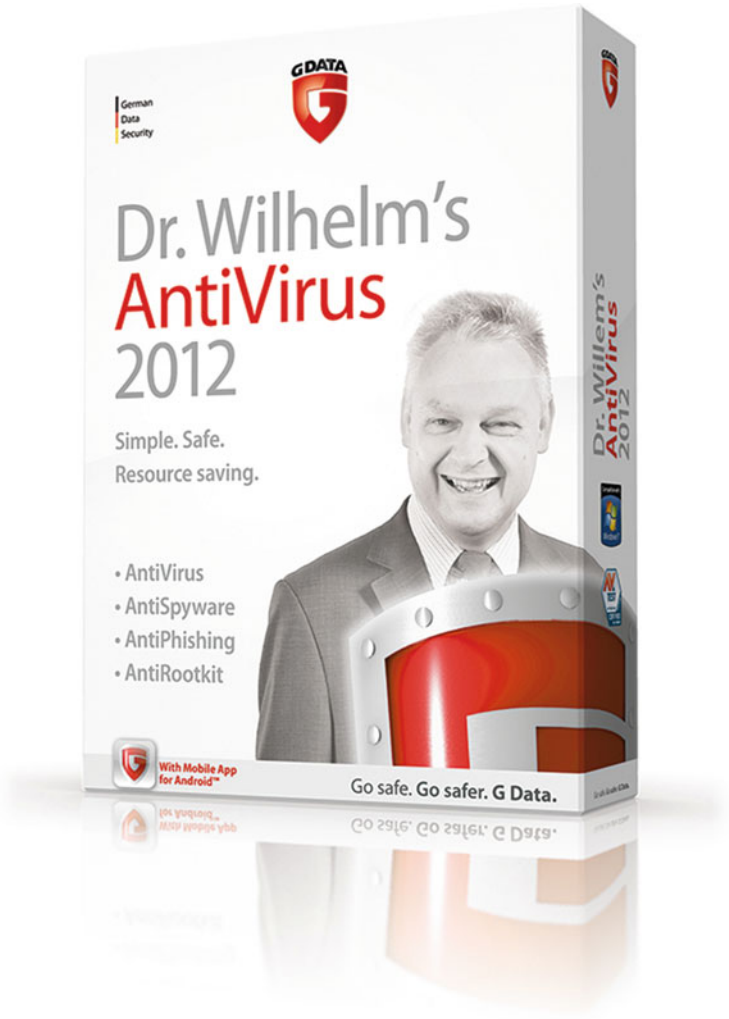
So, enough of the opening credits—now we will enter the captivating world of cyberdanger together. Follow the signposts, take good care, and do not get lost . . . because dangers lurk around every corner.

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

1 Thirty Years of Malware: A Short Outline 1
- 1.1 What Is Malware? 1
- 1.2 What Is a Virus? 1
- 1.3 The First Generation 3
- 1.4 Generation Internet 4
- 1.5 The Mobile Generation 9
- 1.6 Finally 10

2 Malware Author Profiles 13
- 2.1 The Graffiti Sprayer and Script Kiddies 13
- 2.2 Cybercriminals 13
- 2.3 Malicious by Ignorance, Not by Design 14
- 2.4 The Authorities and Government Departments 14
- 2.5 And What About the Hacktivists? 14
- 2.6 Gigabyte: Made in Belgium 15
- 2.7 Virus Developers and Virus Hunters 19

3 The Digital Underground Economy 23
- 3.1 How Is the Digital Underground Economy Organized? 25
- 3.2 Is *Everything* for Sale? 31
- 3.3 How a Mass Attack Works: Botnets and Their Structure 41
- 3.4 And What About the Victim? 41
- 3.5 Conclusion: E-crime Is on the Rise 44

4 From Cyberwar to Hacktivism 47
- 4.1 Cyberwar 47
  - 4.1.1 The Cloud as a Battlefield? 48
  - 4.1.2 Stuxnet 50
- 4.2 Cyberterrorism 51
- 4.3 Hacktivism 52

4.4 Cyberespionage . . . 54
4.4.1 Stuxnet's Relatives . . . 56
4.5 Last but Not Least . . . 58
4.6 Some (Final) Final Thoughts . . . 59

5 The Antivirus Companies . . . 65
5.1 The Manufacturer . . . 65
5.2 Nonprofit Organizations in the Fight Against Cybercrime . . . 71
5.2.1 CARO . . . 71
5.2.2 EICAR . . . 72
5.2.3 AMTSO . . . 75
5.2.4 The WildList . . . 79
5.2.5 Test Sites . . . 80
5.2.6 Other Organizations and Services . . . 80

6 Today's Threats . . . 85
6.1 Botnets . . . 85
6.2 Ransomware . . . 89
6.3 Social Networks . . . 91
6.4 Portable Media . . . 92
6.5 Attack . . . and This Time on Businesses! . . . 92
6.6 Mobile Targets . . . 95
6.7 Online Banking: Beware of the Man-in-the-Browser . . . 98
6.8 PUPs, PUS, and PUAs . . . 105
6.9 Cryptocurrency and Cryptojacking: Virtual Currency and Real Criminals . . . 107

7 Malware Myths . . . 111
7.1 Myth 1: If I Do Not Notice Anything Suspicious on My Computer, It Is Not Infected . . . 111
7.2 Myth 2: There Is Absolutely No Need for Expensive Security Software. There Are Free Programs That Are At Least as Good! . . . 112
7.3 Myth 3: Most Malicious Software Is Sent as an Email Attachment . . . 114
7.4 Myth 4: My PC or Network Cannot Be Harmed by My Visiting a Website, If I Don't Download Anything . . . 114
7.5 Myth 5: Malware Is Most Commonly Downloaded Through Peer-to-Peer and Torrent Sites . . . 116
7.6 Myth 6: Visiting a Porn Site Is More Likely to Result in Being Attacked by Malware than Looking at a Page About Equestrian Sport . . . 116
7.7 Myth 7: If I Do Not Open an Infected File, It Can't Do Any Harm . . . 117
7.8 Myth 8: Most Malicious Software Is Distributed via USB Sticks . . . 117

7.9 Myth 9: I Can Save Myself the Expense of Security Software or Hardware, Because I Know My Way Around and Only Visit Safe Websites . . . 118
7.10 Myth 10: My PC Holds No Valuable Data—So Why Would Anyone Attack It? . . . 119
7.11 Myth 11: My PC Doesn't Run Windows, So It Is Quite Safe . . . 119
7.12 Myth 12: Malware Is Written by Antivirus Vendors . . . 120

8 Tips for Consumers: How to Travel Safely on the Information Superhighway . . . 123
8.1 Invest in an Antivirus Program and Make Sure You Update It Regularly! . . . 123
8.2 You Also Need to Make Sure That Your Operating System and Other Programs Are Updated Regularly . . . 124
8.3 As a Matter of Routine, Power Your PC Down Properly . . . 125
8.4 Don't Make Your Passwords Easy to Guess . . . 125
8.5 Make Sure You Make Regular Backups . . . 129
8.6 Think Carefully About Where You Leave Your Personal Details on the Web . . . 130
8.7 On Principle, Don't Respond to Spam . . . 130
8.8 A Little Common Sense Goes a Long Way . . . 131
8.9 Staying Safe on Vacation . . . 131
8.10 Not Everything That *Can* Be Installed *Should* Be Installed . . . 133
8.11 Make Yourself Knowledgeable About Security Software . . . 134
8.12 If a File Looks Suspicious, Check It! . . . 135
8.13 Media Training for Everyone! . . . 136
8.14 Think About Your Privacy . . . 136
8.15 Uninstall Software That You Don't Use . . . 137
8.16 Watch Out for Hoaxes . . . 137
8.17 Keep Your Webcam Masked . . . 138
8.18 Back Up Your Smartphone, Too . . . 138
8.19 For Advanced Computer Users and Courageous Beginners: Encrypt Your Hard Drive . . . 139
8.20 Tip for Advanced Users: Use a VPN . . . 139
8.21 Tip for Advanced Users: Disable Java . . . 140
8.22 Tips for Advanced Users: Make Sure Your Device Locks Itself Automatically . . . 140

9 Tips for Companies: Surviving on the Internet . . . 145
9.1 A Good Security Policy Is the Bedrock of Corporate Security . . . 145
9.2 BYOD (Bring Your Own Device) or Not, You Must Ensure Good Security . . . 149
9.3 Take Care in the Cloud . . . 150
9.4 Beware of Social Engineering . . . 153

9.5 Patch Management: Put Some Plasters on Your Wounds! 154
9.6 The Greatest Danger Often Lurks Within Your Own Walls 157
9.7 Attend Security Conferences 158

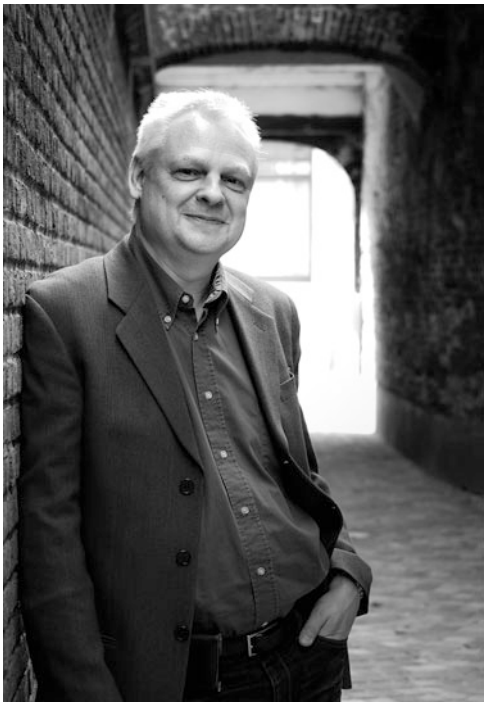
10 The Role of Government 161
10.1 Espionage and Privacy 161
10.2 Malware and Espionage 166
10.3 Knowledge, Ignorance, and Bad Practice 169
10.4 Legislation, Execution, and Punishment 170
10.5 CERTs, CSIRTS, and CCUs 174

11 The Media 179
11.1 The Media as an Ally 179
11.2 The Media as Influencer 180
11.3 The Media as Victim 183
11.4 News Sites and Malware 183

12 The Digital Future 185
12.1 The Shape of Things to Come 187
12.2 Sophisticated Malware 189

13 Awakening: A Short Story 201
13.1 A Possible Customer 201
13.2 The Meeting 203
13.3 The Dinner 205
13.4 What Happened? 206
13.5 The Interrogation 207
13.6 Bio Dynamics 208
13.7 Hacking NATO's Impregnable Network 209
13.8 Calling Dad! 211
13.9 The Team of Security Experts 212
13.10 The Attack Analyzed 213
13.11 Disabling the Malware 215
13.12 Larry Lane 216
13.13 Prevention 216
13.14 Where in the World Is Eddy Willems!?! 217

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.

In 1995 there was another milestone: the very first macro virus, called *Concept*. A macro virus was (to most people) a new type of virus that hid itself in a document file and was executed the moment the file was launched with the associated application. Macro viruses hid mainly in Word files—for one simple reason: Word documents are the files most frequently sent as email attachments. Integrating malicious code into Word files greatly increased virus writers' chances of success—at least as far as the spread of such viruses is concerned.

One of the worst viruses (at least before the millennium) was the *CIH* virus, also called the *Chernobyl* virus. This had nothing to do with innocent gadgetry or fun anymore: if it hit your PC—depending on the variant and the type of hardware on which it found itself—it might "flash" or overwrite your BIOS (an important part of the boot process), causing the PC to stop booting or the motherboard to become unresponsive. Or it might overwrite part of the hard disk so that you could still not start the PC. Malware that trashed firmware had not been seen until then so this brought us again to a new level of malice in cybercrime.

In 1999 we were visited by Melissa. This virus combined a macro-virus-like concept with understanding of the workings of the Outlook email app. As a result, the virus not only caused damage to the PC on which it was started, but it also scanned the PC for Outlook contacts and sent an infected attachment to the first 50 addresses in each address list. From this moment on, a global infection was no longer the vision of "paranoid virus hunters," it was bitter reality.

The "infection" trend continued in 2000 with *VBS.loveletter*, the virus that became known in the media as the "ILOVEYOU" virus, because that phrase was the subject of the email. I remember the first time I heard about this cursed "love letter." I was busy installing an antivirus system for a mail server with a customer when I was asked on the phone if I knew the "ILOVEYOU" virus. I quickly completed the installation and got to the office half an hour later. There I could hardly open my mailbox anymore, having in the meantime received so many messages as a result of this worm. Countless mail servers were blocked because they were hopelessly overloaded. This event was the direct trigger for setting up an anti-malware team at the highest state level (see Introduction). It was strange how many people opened this mail right away, even though they did not know the sender at all.

Even more efficient at self-dissemination than "ILOVEYOU," *SQL Slammer* (from 2003) was a worm that used SQL Server to spread itself. While it could take several days before a VBS.Loveletter infection became evident, it took SQL Slammer only a few hours to paralyze global Internet traffic. Slammer and its SQL Server worm brothers Sobig and Blaster had another thing in common: they were sent out into the world to coincide with major antivirus conferences. A provocation? A practical maneuver so as not to be exposed too quickly? We will never get to the bottom of this, but it has kept many of us away from conferences.

The speed record, however, was set by *Mydoom* in 2004, a worm that not only spread faster than all of its predecessors, but always returned—like a boomerang. A particularly unpleasant example of malware.

In 2005 a new dimension in the world of viruses opened up. Suddenly, multimedia content was also responsible for the spread of malware—at least that was true for

the rootkits on CDs manufactured by media giant Sony. These contained an effective copy-protection mechanism that prevented copying by means of software code. If PC users tried to burn copies of Sony CDs, they became automatically unreadable and therefore unusable. Sony received a lot of criticism for this step, among other things because it was particularly complicated to remove the software from the system as it was hardly noticeable. Furthermore, it was installed without authorization on the CD purchaser's system. (The EULA to which the purchaser agreed did not mention the software).

What Is a Rootkit? A rootkit is described by Wikipedia as "a collection of software tools" installed after intrusion into a software system to conceal future intrusions ("log-ins") by the intruder and to hide processes and files. The rootkit is deeply embedded in the operating system, which may make the operating system unstable.

Although Wikipedia suggests that the author is usually a hacker, a rootkit can even involve a business enterprise, as in the case of Sony. With their rootkit the company wanted to prevent their copyrighted material on (music) CDs being copied to other media. But even if a rootkit is intended only as copy protection (i.e., for Digital Rights Management), it may turn out to be multitalented, creating bugs that can be exploited for other purposes. Some rootkits can do whatever they want with the memory of a PC: read files or system data, changing or manipulating them in other ways. All without the user noticing.

My professional interest was aroused in particular by the *Anna Kournikova virus*. Not, of course because of the email promising photos of the attractive former tennis player, which a victim did not get to see at all. All it took for the worm to make its way into the Outlook contacts was to open the script. I was fascinated by the worm because it was the first malware that the *Emergency Response Team*, set up by the Belgian government (see Introduction), ever warned the public about on radio. Without these warnings, this hardworking virus might have spread much further throughout Belgium.

The first noteworthy virus developed to infect smartphones was called *Cabir*, dating back to 2004. This worm was developed for smartphones running the Symbian operating system and it spread via Bluetooth. It was therefore relatively easy to protect against it—simply by turning off Bluetooth—which made this a relatively harmless pest. The really dangerous thing about Cabir was its persistence: as long as smartphone owners were in the area of an infected device, they were asked to install software, no matter how many times they refused. Out of sheer frustration, many people followed this suggestion instead of simply taking a few steps out of the danger zone, which would have broken the Bluetooth connection to the infected device.

It's not just smartphones that have been increasingly targeted by malware developers over the years. Even the Apple community, previously largely spared such annoyances, would experience their malware Waterloo. In 2006, the *Leap* worm ended the myth that Apple's OS X (now macOS) would be malware-free for all eternity.

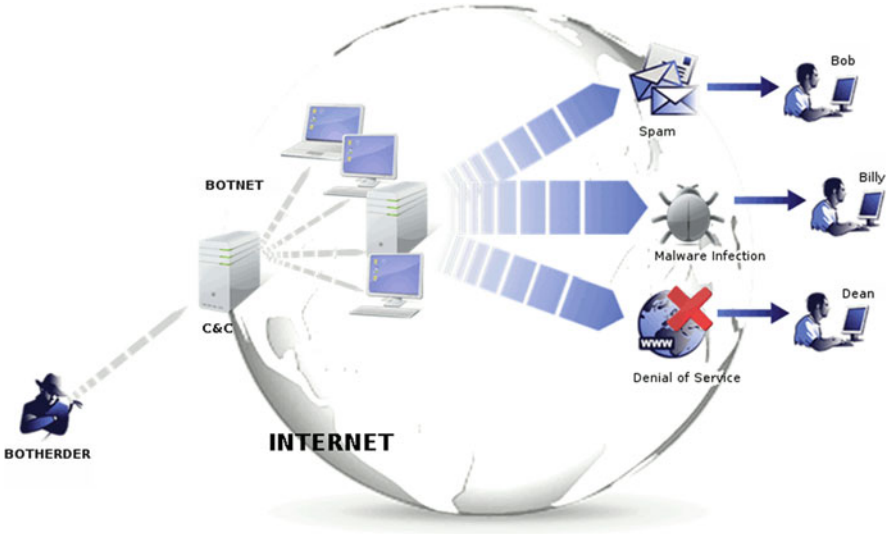


Fig. 1.1 Structure of a Botnet

In 2007 *Storm Worm* hit, the first worm to build itself a botnet. A botnet is a kind of zombie army: your PC will be one of many linked and used by cybercriminals without their owners' knowledge to attack other websites with a PC or to hack them (with thousands of simultaneous attempts at) or simply paralyze them. This is a kind of "website storm attack." The Storm Worm lived up to its name.

Botnets are used for a variety of purposes: to send out spam in massive quantities, to execute DDoS attacks (as defined below), and to infect other PCs with spyware, to name but a few. They are mostly controlled via a C&C (Command and Control) server or using a decentralized peer-to-peer protocol, but the real controller is the person who transmits the commands acted on by the individual bots. Sometimes this person is also referred to as a "bot herder" (Fig. 1.1), because he controls the botnet's zombies in the manner of a sheepdog herding sheep, steering them in a coordinated manner. For my part, I would have suggested a less peaceful term such as "bot sergeant." Indeed, we sometimes talk of malware-compromised systems being "recruited" into a botnet, so the military metaphor is appropriate.

What Is DDoS? "Distributed Denial of Service," DDoS for short, is aimed at a specific site or service with the intention of crippling it. In principle, "Denial of Service" is the result achieved with such an attack: the attacked site is unable to provide its services, as it simply cannot be reached anymore. "Distributed" means that the attack comes from many devices at once, so that it's more difficult—or impossible—to maintain service.

Almost all web servers are capable of processing hundreds of thousands of user requests. But even these services have their limits. If a server receives enough requests by more and more clients at the same time over an extended period, it will eventually collapse. The server will then "hang," so to speak. You can visualize this by comparing the effects of starting too many programs on your PC at the same time—eventually it will also "hang."

The process described here is called a Distributed Denial of Service (DDoS) attack, so-called when it's carried out by thousands or even more devices at the same time. Often, this is a single zombie network that is managed centrally. The hijacked computers—so-called zombie PCs—try, for example, at the same time to call the same web page at the same time and thus incapacitate it.

Social networks have also become victims of malware. Above all, Facebook's popularity has made it a focus of criminal activity. In 2008, the *Koobface* worm appeared—a truly original name indeed. Facebook users whose systems were infected with this worm unknowingly sent messages to friends with the message that they should download a specific program, such as a fake Adobe Flash Update. The download then also infected the friends' PCs and the worm continued to search for more victims. The infected PCs eventually became zombies in a botnet.

In 2008 there was one of the biggest malware attacks ever. *Conficker* infected the PCs of companies and of home users as well as those of various authorities—hardly anyone was spared. It was one of the busiest times antivirus vendors ever experienced. And the worm was long-lived and tough: according to the Conficker Working Group, there were still hundreds of thousands of PCs infected with Conficker as recently as 2016, although the number of unreported cases may be much higher. The compromised PCs were integrated into botnets which are now to all intents and purposes inactive, but it's probable that the malware is still present on many of those systems.

In 2010 the first malware for Android appeared, which was in a sense official confirmation that Android had grown to become the most popular smartphone platform in the world. This was the year when we were confronted with the first "banking Trojans" which targeted mobile banking customers.

The year 2010 will also be remembered by people who fight against malware as the year of *Stuxnet*, the most advanced malware program encountered. It is so "smart" that many consider that it cannot possibly be the work of simple cybercriminals, but must have been in some way state-sponsored. Perhaps because this worm probably had only one goal: the delay of the uranium enrichment program in an Iranian nuclear complex. More detail about this is given in Chap. 4.

In 2011 and 2012 there were further attacks with *Duqu* and *Flame*, where intelligence agencies were again suspected of having been responsible for their development. The age of progressive cyberattacks and espionage by nation states had officially begun.

By the beginning of 2014, experts from G DATA SecurityLabs had published their discovery of a highly complex espionage program with Russian roots: *Uroborus*. The malware executed the theft of highly sensitive and secret informationally high-value networks, such as government agencies, intelligence agencies, and large corporations.

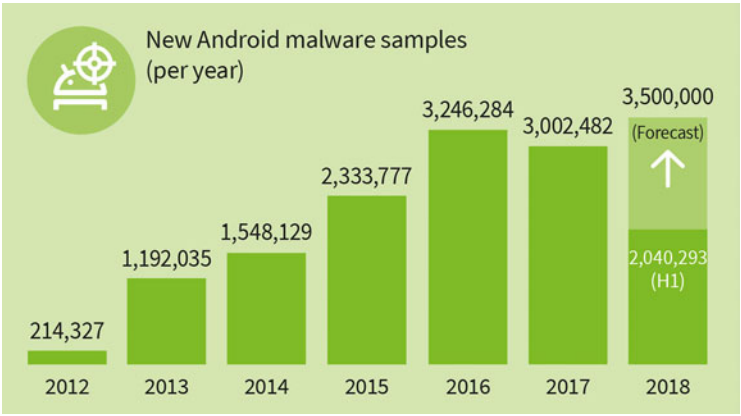


Fig. 1.2 Increase in the number of malware programs for Android—G Data Software AG

1.5 The Mobile Generation

We talked briefly earlier about malware on mobile devices. Since 2010, the number of Android malware programs has been growing exponentially (Fig. 1.2), and there is no end to this trend in sight. The number of victims continues to rise rapidly: millions of smartphones have already been compromised.

Android long ago exceeded macOS, other flavors of Linux, and other operating systems and not only in number of users: it is now the second largest platform in terms of malware volumes. For the time being, Windows leads the table with 99% of all malware. No one can say how this will develop over the next few years. But it's clear that malware on open platforms such as Android will increase exponentially in the coming years.

Apple's iOS is a bit different. iOS smartphones or tablets have no—or at least few—problems with malware for the time being, because the company strictly controls which apps are offered in its App Store. On the other hand, it does not allow any antivirus apps on the platform: only Apple can provide protection for its smartphones and tablets. It's true that this is not much of a problem at the moment (except in terms of adware), but one day there may be malware that secretly finds its way into iTunes. Then Apple itself will hopefully provide a solution. Since the Cupertino-based company has so far rejected the entire antivirus industry, we can only hope that any solution it develops becomes available faster than some global infection manages to spread.

It may surprise a few people but I'm sure about this: if Apple's iOS had as high a market share as Android, there would also be significantly more malware for the iPhone. Granted, it's harder to inject malware into the App Store, whereas Google Play Store is not the only source of Android apps. But that's not the issue that pushes malware writers toward Android. The stronger the market share, the greater the interest of cybercriminals. If Apple had 80% instead of 20% of market share today, cybercriminals would show far greater interest in it.

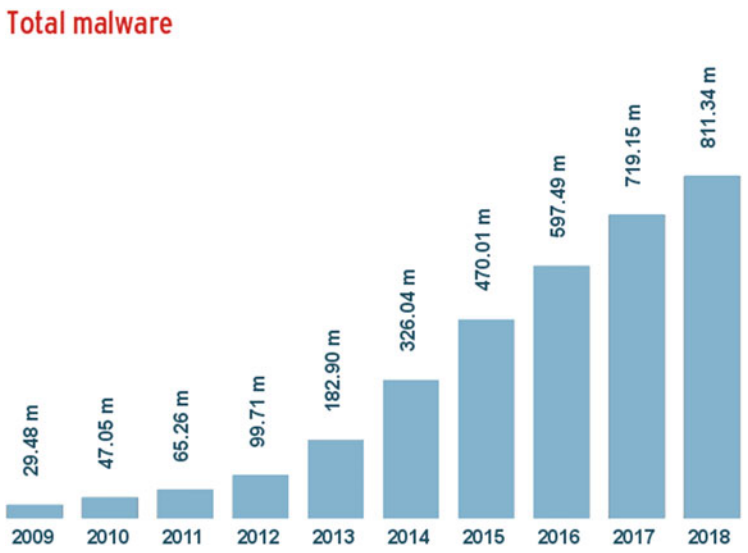


Fig. 1.3 Total malware per year—AV-TEST.org

1.6 Finally

Figure 1.3 says more than a thousand words. In recent years, the number of computer pests has risen spectacularly. Malware is everywhere, but is usually quickly detected and removed, as shown in the graphics.

Most antivirus vendors regularly publish statistics on malware that they have discovered and neutralized with their security solutions over the past few years. Conservative estimates seem to have gone out of fashion with some companies. Thus, according to their own reports and statistics, some manufacturers have found far more malware than their competitors. Apples from manufacturer A are easily compared with pears from manufacturer B—because some manufacturers only count malware families, while others count each respective mutation. This quickly results in seemingly different pictures of the situations as a result of different counting approaches. However, this does not automatically mean that one of the two numbers is wrong or that the manufacturer in question has been more or less successful at rendering the malware harmless.

What Can We Learn from History?

1. With VBS.loveletter, it's painfully clear: humans are often the weakest link in the defense chain when it comes to combating malware. It does not matter how often it is pointed out that people should be careful about emails from senders they do not know. All it takes is a simple message like "ILOVEYOU" to persuade people to simply ignore all previous warnings.

(continued)

As strong as the desire for love may be, do not fall into the trap of social engineering malware. (Malware that tricks the victim into executing malicious code using psychological manipulation).
2. Other human characteristics are also abused, as shown by the Symbian worm Cabir. For example, if an application or service pushes you to install an update often enough, many people will give in to this urge at some point just to be rid of the constant demands once and for all—ignoring or not caring what they are then actually installing.
3. "If I see nothing, there is nothing there." Wrong! As we have already seen several times in this chapter, viruses and worms are no longer just disgusting little beasts that directly attach themselves and can then be removed as soon as possible from the PC. The vast majority of malware embeds itself in PCs unnoticed and performs tasks in the background, some of which you may become aware of months or even years later, and sometimes not even then. Malware is mostly invisible, so you should not be tempted into a false sense of security because your PC does nothing (visibly) unusual. You will meet this advice again because it is so incredibly important. Be warned!

Did You Know . . .?

Netsky is currently perhaps the most popular Belgian dance act. The man behind Netsky is Boris Daenen, a former boy prodigy. Did you also know that he took his name from a 2004 worm that infected a huge number of computers worldwide over a period of about 2 years? Let's hope that our Belgian Netsky sticks to spreading catchy tunes.

Some Milestones

- 1983: Frederick Cohen and Len Adleman define and name the computer virus.
- 1986: *Brain*, the first PC virus emerges. The virus spreads by writing its code in the boot sector of floppy disks.
- 1987: Ralf Burger publishes the book *Computer Viruses: A High-Tech Disease*.
- 1988: The *Morris* worm infects approximately 10% of computers connected to the Internet (approximately 60,000 computers).
- 1989: *Ghostball* is the first multipartite virus.
- 1989: The *AIDS* virus is the first known ransomware.
- 1992: *Michelangelo* is the first virus to attract massive media attention.
- 1995: *Concept* is the first macro virus.
- 1999: Melissa heralds the era of mass-mailing malware, causing epidemics worldwide.
- 2000: *VBS.Loveletter*, an extremely rapidly spreading worm, also known as the "ILOVEYOU" virus.
- 2003: *SQL Slammer*, a fileless worm, is responsible for a worldwide epidemic.

(continued)

- 2004: *Cabir*, the first "proof-of-concept" for Symbian, is distributed via Bluetooth.
- 2006: *Leap* is the first significant malware for Mac OS X.
- 2007: *Storm Worm* is among the first to use fast flux DNS in combination with P2P distributed networking so that it can't be disabled by taking down C&C servers.
- 2008: *Koobface* is the first malware that attacks Facebook.
- 2008: *Conficker* infects companies, users, and government agencies, causing one of the biggest epidemics in history.
- 2010: *FakePlayer* is an SMS Trojan for Android.
- 2010: *Stuxnet* makes a targeted attack on an Iranian uranium enrichment center.
- 2011: *Duqu* is an advanced Trojan that collects information.
- 2012: *Flame* is a very advanced spy virus.
- 2014: *Uroborus* infiltrates the Belgian Ministry of Foreign Affairs and other European organizations (Fig. 1.4).
- 2015: *XcodeGhost* modifies Apple's Xcode development tools and results in thousands of compromised apps being found in the App Store.
- 2016: *Locky* ransomware is said to have attacked thousands of computers in Germany alone at its height, and affected millions worldwide.
- 2017: *WannaCry* ransomware brings services to a halt including parts of the UK's National Health Service, the Spanish telephone system, and many others worldwide.
- 2018: VPNFilter compromises a wide range of home routers and implements an effective Man-In-The-Middle attack on incoming web traffic.

Fig. 1.4 Uroborus Illustration by G Data Software AG

Chapter 2
Malware Author Profiles

Hackers and people who write malware are by no means always criminal geniuses. In fact, not all malware authors have, historically, intentionally set out to break the law, though nowadays most are quite happy to do so where there are high profits and low risks. Here we take a closer look at the psychology of the malware developer.

2.1 The Graffiti Sprayer and Script Kiddies

Many of the first viruses and worms were written by teenagers who just were curious to see how their creations would fare in the real world. They established the foundations of the approach before 2006, but actually they were responsible for only a small part of the malware flood that followed. However, they formed the largest group of malware writers in the late 1980s. But even in the early years, they were not the only ones: even then cybercriminals were active. The biologist Dr. Joseph Popp, who was identified as the author of the AIDS Trojan horse (Chap. 1), is a good example.

Although these teenage experimenters wanted to show off their technical talents, I still call them "Script Kiddies." At that time malware was often shared via copy and paste through scripts found on the Internet. This also explains their poor technical quality, and antivirus programs usually had few problems eliminating them. This type of malware is still found today, but it is not state of the art.

2.2 Cybercriminals

At the time of writing, this group is responsible for nearly all malware, and they write it for one reason only: to make money. In Chap. 3 we shall discuss the economy of the underworld further. The technical expertise of cybercriminals is improving constantly.

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_2

2.3 Malicious by Ignorance, Not by Design

There is a relatively small group of people wanting only to protect their programs and data, but they use software which in turn can be used by third parties with malevolent intentions. The Sony Rootkit from Chap. 1 illustrates this quite vividly, but some of the activities of various government ministries engaged in the fight against cybercriminality also fall into this category. I refer to this in Chap. 11.

2.4 The Authorities and Government Departments

Many nation states have established special agencies to ward off cyberattacks on their civilian or military IT infrastructure by other nations or by cyberterrorists. In the meantime, however, nobody doubts that most countries are also using malware to spy on other nations or to engage in targeted attacks on "enemy" targets. In Chap. 4 we will reveal these activities.

2.5 And What About the Hacktivists?

Here the situation is somewhat more complicated. Actually, hacktivists, as the word suggests, are hackers and not malware writers. To be a hacker, it is not enough to write only malicious code—quite different skills are required. Often the hacker is also a malware writer, but in principle these are people with differing skillsets who may work together in teams. Hackers specialize in the intrusion into and/or paralysis of websites and/or networks, while malware developers are focused on the distribution of their code. They may also be "activists" who want to use malware as part of working toward a "higher goal" or to announce some message to the world.

The Author of the Protovirus

The first PC virus, Brain (Chap. 1), dates back to 1986, but is it also from the first developer? Well, strictly speaking, of course, but this "invention" was preceded by several years of trials—the virus prehistory, so to speak. These are described in the excellent book *Vers & Virus* (*Worms and Viruses*) written by François Paget. Of course, I would not want to deprive you of some of the highlights.

The Hungarian-American scientist John von Neumann made many revolutionary contributions to science, but he is also known for his role in the Manhattan project which led to the first atomic bomb. His analysis of the structure of self-replicating organisms led indirectly to the discovery of the structure of DNA. However, he also contributed to the invention of the virus or worm in the sense of a digital organism which can self-reproduce.

(continued)

In 1971 we meet the first program that behaved like a worm. It was called Creeper: it could move from computer to computer, and it served almost as a proof-of-concept tool in research toward improvements to air traffic management. Whenever the program was inserted into a computer, the following appeared on the screen: "I'm Creeper! Catch me if you can!" Subsequent versions of Creeper could even reproduce. Later, Reaper (often referred to as the first antivirus) was developed to remove all versions of Creeper. It was a little like a cat-and-mouse game between worms and antivirus programs.

Last but not least I would like to mention the science fiction author David Gerrold, a contributor to the Star Trek series. In his novel *When HARLIE Was One*, HARLIE (Human Analogue Robot Life Input Equivalents) is described as a computer with highly developed artificial intelligence that can interact with other computers to reprogram them or change their data. To make contact, he uses a program that dials numbers by chance, hoping that the number belongs to another computer. Once a computer is found, the program is also loaded onto this computer. The name of the dialer? Quite simply: Virus.

2.6 Gigabyte: Made in Belgium

Even the "most public" message from a virus developer can sometimes be very personal. Let's take a look at the history of the very first—as far as we know—female malware developer in the world, with the "nom de plume" Gigabyte. This—believe it or not—Belgian had been experimenting with viruses for quite some time, when the well-known virus hunter Graham Cluley expressed himself in what she saw as an emphatic and arrogant manner about virus writers. Thereupon Gigabyte, in revenge, began to write viruses that contained special messages for Cluley.

Gigabyte was the prototype of a graffiti artist—at the height of her "career" she was about 18 years old—without any criminal intent. She never spread viruses, instead she put them on her website so that third parties could use them for distribution. Paradoxically, there was a warning on the page (Fig. 2.1) that stated that visitors were not allowed to download the viruses for criminal use.

Journalists of the online station TechTV (no longer active) pointed out the inconsistency in this statement: whoever makes a weapon available to others has to assume that someone will use it. Gigabyte just shrugged and blamed the users: "If they're so stupid . . ." Putting the blame on others was typical of her. For example, it was Microsoft's own fault that it was so easy to write viruses for the Windows platform. When Microsoft responded with *Trustworthy Computing*, she only saw a sneaky plan to bind more people to Microsoft's systems. "*Bill Gates is Satan*" she concluded triumphantly (Fig. 2.2).

And yet, as I established later, she was a timid and amiable young woman (see also the paragraph "Accidentally Unmasked" in Sect. 2.7) for whom the writing of viruses was, above all, her chosen form of self-expression, with no intention of harming or hurting others. She was arrested and interrogated and

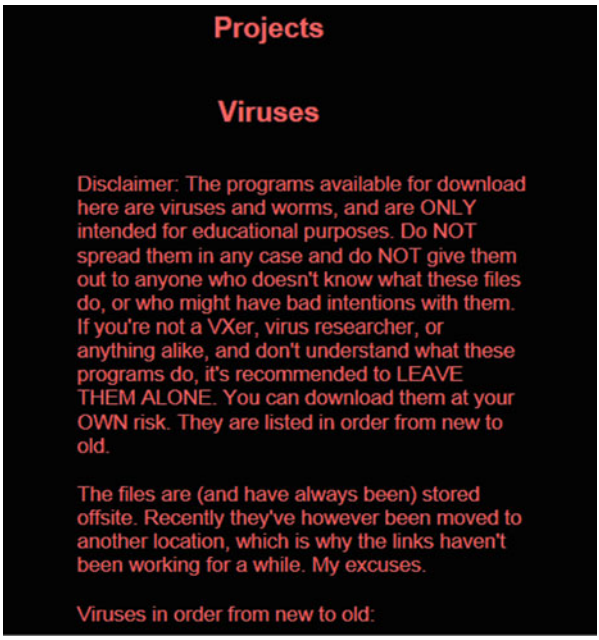


Fig. 2.1 Gigabyte disclaimer: "These viruses are NOT intended for distribution"

Fig. 2.2 From Gigabyte's Diary: "Bill Gates is Satan"

swore to never again write viruses or deal with malware. As far as I know, she kept her promise.

In the Words of . . .
Graham Cluley, Blogger, Researcher and Public Speaker
What a strange long trip we've been on.

It's approaching 30 years since I first set foot onto the world of computer security, and then found a job actually writing anti-virus software.

Software to hunt and kill other software. What a strange concept! But at the end of the day it was just a collection of bytes, a mishmash of subroutines. The only thing about computer viruses that made them different from other software was that they included code to replicate themselves, sometimes jumping on the back of other programs on your computer to help them spread.

A program can be analysed and disassembled. You can find out, if you have the time and perseverance, how to understand what it has been coded to do. It is, to some extent, predictable.

What isn't so predictable, however, is human behaviour. And, for me, that has always been one of the most interesting aspects of computer security—whether it's understanding the mistakes that people make and that allow their computers to be hacked and their companies to be breached, or the motivation for the person who codes the malware in the first place.

In the early days a stereotype quickly emerged. There was no money, really, to be made from writing a computer virus. So that couldn't be the motivation for those who chose to sit in their back bedrooms for hours and hours trying to write a virus that the latest and greatest anti-virus programs couldn't detect.

For many I think the motivation was "showing off to their mates". Those mates, quite often, were the result of electronic friendships that they had built up via bulletin boards and message forums with other likeminded computer enthusiasts with a penchant for "being naughty" and writing viral code.

What they had in common was that an immature sense of ethics and a lack of empathy. They failed to put themselves in the shoes of their victims, or (mostly) simply didn't care about the problems that their malware might cause on a user's computer. If they had taken the phone calls, as we did when working inside antivirus companies, from grannies who were scared to use their computer anymore, or the blind guy whose PC would no longer boot up, maybe they would have thought twice about the mayhem they were causing.

But they were just kids. Even the ones who were older seemed to display immaturity—like David L. Smith, the author of Melissa (W97M.Melissa.A), who was in his early thirties when he unleashed his notorious email-aware virus and chose to hang around on forums with people much younger than him, seemingly emboldened by his status in the group.

(continued)

They were just boys. And yes, I mean boys. With very few exceptions, in those early days viruses were testosterone-fuelled electronic graffiti, perhaps for the simple reason that the female of the species tends to be more empathic and fails to see the point of writing malware just to spread a childish message or wipe a stranger's hard drive.

But then things began to change. The rise of AOL and other services had seen a wave of newbies embrace the internet, less technically-savvy than those who had gone before them, and often careless with the security of the computer they now had in their home.

This change brought new incentive for malware creation. If you could write a Trojan that could steal a password, you could access the likes of AOL for free. Password-stealing Trojans weren't interested in spreading electronic graffiti or announcing their presence, as that would give them away.

And, inevitably, other criminals began to see opportunities. If malware could steal passwords for a dial-up internet connection it could also grab the passwords of online bank accounts, as home users got used to the idea of handling their finances via the computer.

Suddenly there was money to be made from malware, and criminals saw an opportunity. Money continues to be a primary motivation for most of the malware seen today—whether it's intended for gaining unauthorised access to systems, spying on communications, stealing data, or breaking into accounts.

It's not just a case of the bad guys growing up. Organized criminal gangs that already existed came to recognize the opportunities and benefits that cybercrime would bring them. Whereas 30 years ago you might have robbed a bank in person and then made your getaway, now you could try to rob a bank over the internet. . . and perhaps be on the opposite side of the world when you do it.

I never imagined 30 years ago that things would become so serious, and that malware would stop being the province of adolescent boys who I imagined would eventually grow out of it.

What is perhaps even a bigger shock is that malware and hacking has been embraced so seriously by governments and nation states—using their abilities to spy on their enemies and sometimes their own citizens.

In fact, if you're looking for a job in computer security, there are now state-run intelligence agencies who might even consider turning a blind eye to any murky hacking you may have committed in the past, if they think it would be to their advantage to have you working for them.

Should you take a job like that? That's up to you. Only you know if you could live with it or not. But it's certainly a better option than being a part of a criminal hacking gang.

(continued)

Graham Cluley is an award-winning security blogger, researcher, podcaster, and public speaker. He has been a well-known figure in the computer security industry since the early 1990s when he worked as a programmer, writing the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Since then he has been employed in senior roles at a number of security companies.

Graham Cluley has given talks about computer security for some of the world's largest companies, worked with law enforcement agencies on investigations into hacking groups, and regularly appears on TV and radio explaining computer security threats.

Graham Cluley was inducted into the InfoSecurity Europe Hall of Fame in 2011.

Follow him on Twitter at @gcluley, or listen to him on his weekly podcast "Smashing Security."

2.7 Virus Developers and Virus Hunters

Twenty years ago I would not have dared to write about those two groups in the same paragraph. For a long time it was absolutely frowned upon in the antivirus world to make contact with writers of viruses and malware. "To seek direct contact with the enemy is not acceptable" was the guiding principle then in force. And yet deep insight into the malware writer's psyche and way of thinking helps us to combat malware. Dr. Sarah Gordon has dealt with this subject in various articles (e.g., https://www.wired.com/1997/11/heartof/) for antivirus and other specialist journals. Her insights benefited from her contacts and she has made the following observations:

1. The typical virus writer doesn't exist! They are not all lonely nerds who want to prove their intelligence. However, the majority of virus writers were male at that time, between 13 and 26 years old, and had developed viruses for quite varied reasons.
2. The most important motivators for virus writers are (or were) the urge to be acknowledged, the technical challenge, the desire to belong to a particular group,

revenge, curiosity, and the satisfying feeling when one proves that a system is not watertight.
3. More stringent laws have minimal effect on dissuading virus writers from their activities, unless they really feel that these laws will be enforced consistently. If someone *is* arrested, but only after months or even years of creating malware, this leaves the virus-writing community quite cold. If you want to persuade them to adopt other ideas and hobbies, you have to convince them that viruses are not cool!
4. When virus writers are active, they don't usually consider themselves to be doing something bad. They take no responsibility for their actions and look for excuses in phrases such as "only for research purposes" and "liability for malware is excluded," blaming bad consequences on others and even on the victims.
5. The realization that you can cause considerable damage through one's actions comes with age. Sarah Gordon realized that unfortunately the age at which developers became aware of the consequences of their activities was rising—earlier this age had been 21, but at the time of her research it was 25. But please note I am talking about hobby virus writers, not the true cybercriminals. I will discuss the latter group in Chap. 3.

There are many misunderstandings about the complex relationship between virus writers and virus hunters. We will shed further light on this in Sect. 7.12.

From the Diary
Accidentally Unmasked
May 2002
Gigabyte's Homepage

To be honest, I am fascinated by the career of Belgian virus writer Gigabyte (Fig. 2.3). She was invited on television to talk about the motivation behind her virus writing. [The interview was shown on the TechTV, a San Francisco radio station I mentioned previously, that specialized in technology and the Internet, broadcast in 73 countries. It was later merged with G4.] In the program they showed photos of her school, which reminded me of my hometown, Mechelen. The frontage of her house was also shown. When I drove a few days later through a residential area in my neighborhood, I suddenly realized that Gigabyte must live there. So I had a chance to discover her identity. Sarah Gordon was very excited when she heard this, and she immediately asked me to establish contact between herself and Gigabyte. We organized a meeting between the two in a castle in Luxembourg, not far from where an EICAR conference had just taken place in 2004. It caused a huge stir in the antivirus world: many people wanted to know with whom Sarah had met, and there was greater astonishment when it became clear that this involved Gigabyte. Step by step, the antivirus world learned that it could be useful to know the enemy better and thus better understand them.

(continued)

But the fact is, this realization was only hesitantly reached, as had also been demonstrated in 1997 when a virus writer called "Stormbringer" gave a presentation at the Virus Bulletin antivirus conference. Admittedly, he was not lynched, but the atmosphere in the hall was extremely hostile, he was constantly confronted with accusations, and his lecture was anything but smooth. I still remember that he was trying to persuade the security industry that they should give him a job. I think the objections were mainly ethical: no mainstream antivirus vendor was going to employ former virus writers because they'd shown themselves to be ethically challenged. Furthermore, having written a few viruses wasn't considered a technically convincing preparation for the discipline of writing security software. David Harley, who helped me with the translation of this book (see Acknowledgments), wrote about some of these issues in the 2006 November edition of Virus Bulletin Magazine (https://www.virusbulletin.com/virusbulletin/2006/11/i-m-ok-you-re-not-ok).

Fig. 2.3 Gigabyte's homepage (2012 screenshot)

Chapter 3
The Digital Underground Economy

It could be suggested that the dangers we have encountered so far were relatively harmless. But now we dive deep into the underground and find the dark corners of the cyberworld where criminals thrive. Down there in the underworld, we no longer have to deal with amateur hackers boasting about how many websites they've accessed. Today's hackers boast about how many credit cards they steal with their botnets. Credit card data is worth cash.

In the digital underground you can now find everything that exists in a "real" business environment: manufacturers, retailers, suppliers, shady operators, and customers. For many, earning money in this shadow world is their springboard into organized crime, although (or perhaps because) they never have personal contact with their "business partners." I'll show you that cybercriminals are not a small, harmless minority but flourish in a milieu ruled by organized crime.

In the Words of. . .
Bob Burls, Director, Incident Response EMEA and APJ Symantec Cyber Security Services

Cybercrime has evolved dramatically in the almost two decades I have been investigating it. In the first 10 years of the twenty-first century cybercriminals were often more focused on attacking each other: the IRC wars waged and systems were owned because they could be. These emerging criminal types built their own tools and took unashamed advantage of each and every software vulnerability. As soon as a vulnerability was patched another would appear and be exploited, in a cat-and-mouse-like fashion. Remember the Unicode exploit used for directory traversal? How large and vulnerable the Internet was exposed as being when the network worms were released?

Then came the shift: the tipping point was reached with the growing realisation that botnets could be monetized. They had true value. Affiliate schemes evolved and banking Trojans were born.

(continued)

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_3

Money is the driving force behind today's cybercriminal, who benefits from a low-risk, high-yield model. Those responsible for designing and building modern malware are abusing the Internet in ways never imagined. Fast-flux botnets, domain generation algorithms and rootkit technologies all cluster to make the investigation of cybercrime more challenging. We now see collaboration between malicious actors: for example, the release of the Zeus source code and the growth of its offspring ICE IX and Citadel. Evasion tactics are clearly shared and developed in a would-be criminal cooperative.

Point-and-click technology, together with the development of crimeware kits and an uptick in underground services, has, I am certain, made it easier to become a cybercriminal; sometimes it is as simple as criminal hacking by numbers.

Bob Burls leads Symantec's Incident Response Services delivery operation in EMEA, helping organizations identify, contain, and eradicate the threat of increasingly sophisticated attack actors.

Before joining Symantec, Mr. Burls was an independent IT Security Consultant working extensively with UK law enforcement, in the role of Cyber Crime Advisor for the Metropolitan Police Service. He also worked with the European Law Association and a number of global IT Security companies. Mr. Burls is a recognized expert witness in the United Kingdom and has been engaged by the UK Crown Prosecution Service.

Prior to this Mr. Burls had a successful 25-year career as a detective in the UK Metropolitan Police. He had served on the New Scotland Yard Police Central e-Crime Unit since the creation of that unit and prior to that the Metropolitan Police Computer Crime Unit and the National Hi Tech Crime Unit. During this phase of his police career, Mr. Burls investigated a number of high profile international cyber-crime cases.

Mr. Burls hold a Master's Degree in IT Security and has co-authored a number of academic papers whilst undertaking post-graduate research at the Centre for Forensic Computing, Cranfield Defence and Security, the academic provider and partner to the Defence Academy of the United Kingdom.

3.1 How Is the Digital Underground Economy Organized?

For many cybercriminals their careers begin in "discussion forums," also called *boards*, which deal with topics such as botnets, spam, data theft, and other issues. There are boards for script kiddies who would like to present themselves as hackers, but also forums where credit card data, stolen goods, and other "wares" are publicly traded. We should make one thing clear: these are not forums for regular consumers who want to read film reviews or buy maternity clothes: rather they are meeting points and communication platforms for people who are clearly pursuing criminal goals. Therefore, it is unlikely that you will just happen upon such a site: these boards are not as open and accessible as the harmless forums and platforms already mentioned. And the more illegal the content of the forum is, the more intense is the owner's commitment to protecting himself from uninvited guests.

The structure of these boards is in most cases not significantly different from normal forums. Often there is also a private area reserved for the members who belong to the management team, or who have worked their way up the hierarchy through "special merit." Only the normal, public forum environment is available to all the other members. But even there, cybercrime novices get plenty of useful information.

There are, for example, guidelines for installing your first botnet—self-assembly instructions, so to speak—and also information on security holes in software and in operating systems (Fig. 3.1). Often, experienced members offer their support to newcomers, but only for a fee, as should be clear. What else would you expect?

The owners of these forums provide regular marketplaces, sometimes called *black markets*, where members can offer goods and/or services. From stolen credit card data via lists with email addresses to botnets (Sect. 6.1), everything is available. In addition, you can download pirated software from almost all boards.

The underworld economy is teeming with a variety of competing boards or forums that anyone can turn to. The competition among the operators is almost limitless. Often forums are "defaced" by competitors (i.e., the site is, for example, edited so that a link points to the wrong site), and sometimes there are even DDoS attacks. Sometimes a forum's databases are copied by rivals and published in other

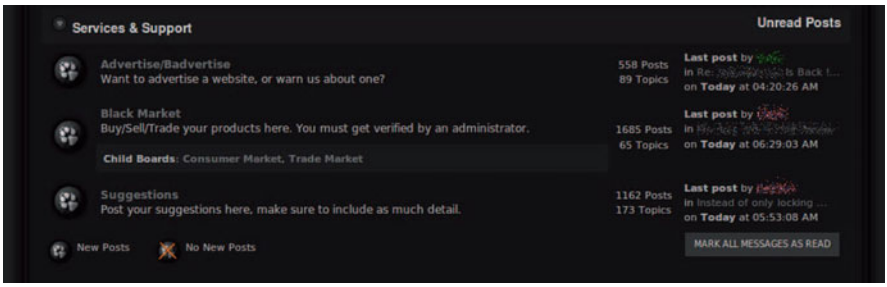


Fig. 3.1 Screenshot of a forum

forums. This is then seen as evidence of the cybercriminals' attack capabilities, for which they then gain considerable recognition in their own *community*. In addition, the hacker even leaves his mark somewhere on the website as proof that he hacked it. All this sounds like a crime novel—except that this drama plays out for real in the virtual world.

Within the community, in most cases the purchase and sale of the products offered is negotiated using chat programs such as Skype or ICQ. In particular, ICQ, which never really took off in the classic Internet world as most of us experience it, is the most widely used means of communication in these groups. So it's often the case that the supplier doesn't offer a form or an email address as a contact option but one or two ICQ numbers instead.

It's not uncommon for cybercriminals to use *private messaging* for initial contacts. This is a chat window that's only available to just two communicating persons. Such a function is available in almost all forums, which almost always use standard software, even if they occasionally modify it somewhat (Fig. 3.2).

Another frequently used service is *Internet Relay Chat* (IRC), a public chat room that resembles a pub with a colorful mix of many regulars, all sitting at a counter. The chat takes place almost in real time, and it happens quite often that several thousand users can interact in a single chat room, so it's quite easy to go unnoticed. That's why people often warn against making purchases using IRC, because of the risk of becoming a victim of "*scammers*." I will be talking about this threat.

Additionally, a large part of the trade in credit cards and access data, such as for PayPal or eBay accounts, is handled via forums. The sales are made in specially designed environments within the forums called black markets or simply markets.

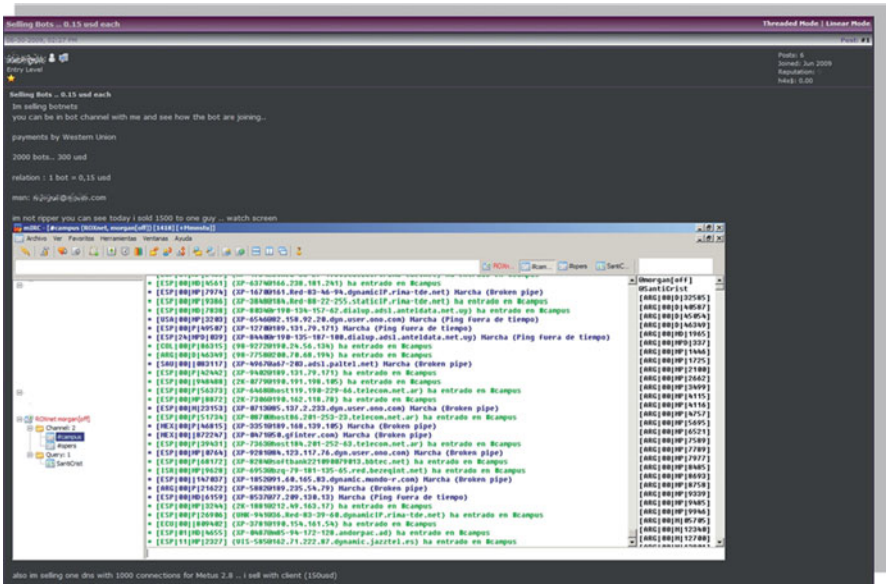


Fig. 3.2 Offer of bots in an underground forum

Fig. 3.3 Marketplace with offers from various sectors

There are even boards that consist only of market pages where nothing takes place other than trading in stolen goods.

The procedure is very simple: someone offers a product for sale, for example, several user IDs and passwords from eBay. He notes how much money he requires per account (per record, username, and password). Occasionally, the seller even offers volume discounts if the customer wants to buy all or several of the available records. In addition, the seller tells you which form of payment he prefers. The prospective customers then communicate their answer via the forum, or they contact the seller directly via the contact details given, in order to complete the purchase (Fig. 3.3).

Occasionally you can even find shops on the Web where you can source malware, much as you would order something in a regular online shop.

Is the stolen PayPal account disabled? Do cybercriminals need new credit card information? No problem! A shop like the one pictured in Fig. 3.4 can simply offer hundreds of other accounts. Payment is made via recognized or less well-known money transfer services such as Western Union, paysafecard, e-Gold, Bitcoin (Fig. 3.5), or other virtual currency.

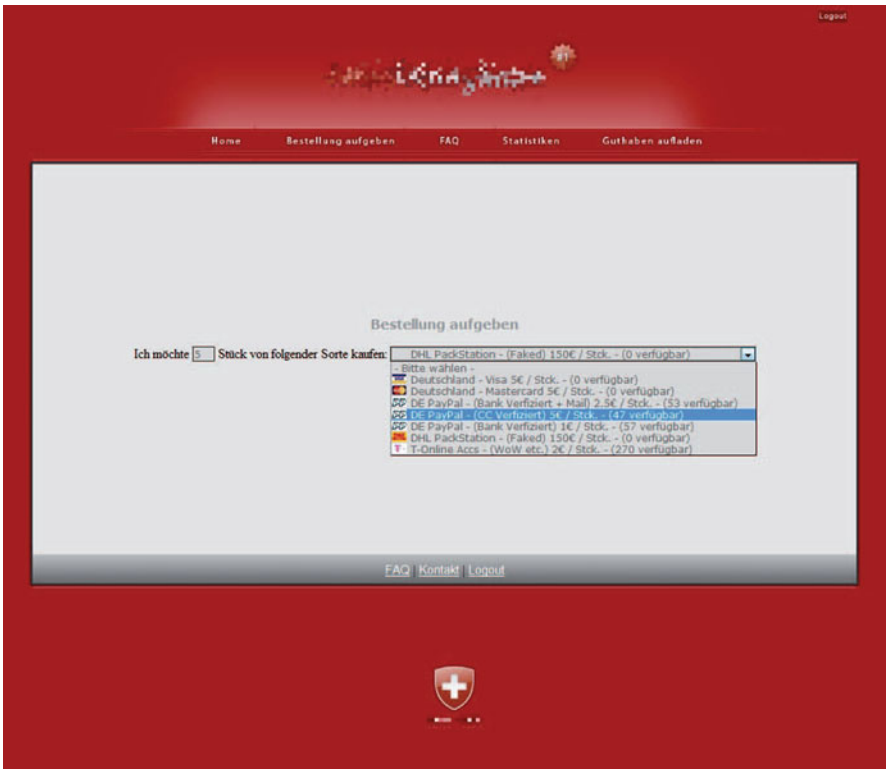


Fig. 3.4 Webshop selling account data

Fig. 3.5 Even in real life you can now pay using bitcoins

Bitcoin is now considered much more acceptable, along with all the other ways of making a payment. It's an online payment service that uses its own digital currency (or cryptocurrency). Bitcoin is thus the digital equivalent of a currency like the dollar or euro. The value of a bitcoin changes quickly. While this book was being written, a single bitcoin changed in value from $75 to $290 to over $14,000 at the time of this translation and is not expected to stabilize any time soon. The popularity of this virtual currency has grown impressively fast, so that even in the real world, it is now possible to pay with bitcoins. They are currently accepted as a valid form of payment at Café De Waag in Delft in The Netherlands and many similar venues.
Bitcoins are as precious as gold (and in 2017 actually reached a value higher than that of an ounce of gold) according to official sources. Working on data mining projects that use PCs to analyze large amounts of data was the original way to earn bitcoins. In a sense you were rewarded with bitcoins.
Since this money is completely independent of other currencies, but above all since the owners of bitcoins remain absolutely anonymous, this payment method is extremely attractive for cybercriminals who can make convenient use of it to launder their dirty money. They can also use the many zombie systems in their botnet for data mining projects, giving them the opportunity to earn even more bitcoins.

Meanwhile, there are of course suppliers who offer a complete infrastructure for such online shops, meaning not just the shop itself but also the "hosting" of the shop, the domain, and everything else that belongs to it. With such a complete package on offer, the seller just needs to put his stolen goods "in the shop window" (Fig. 3.6).

* * *

FAQ Page for Criminals
Yes, even cybercriminals have a resource with answers to frequently asked questions. So, let's see what this one looks like:

1. *What does *******.net do?*
   (a) *Domain registration*
   (b) *Free server and script updates*
   (c) *Free advice on implementing the concept of a shop*
   (d) *Server configuration (DDoS protection and full protection)*
   (e) *Taking over the advertising costs in known boards to increase sales*
   (f) *Creation of scripts (further information about the script under ******.net/products)*
   (g) *and much more . . .*
2. *How do I lease a shop?*

   A good reference: people must confirm their reliability.

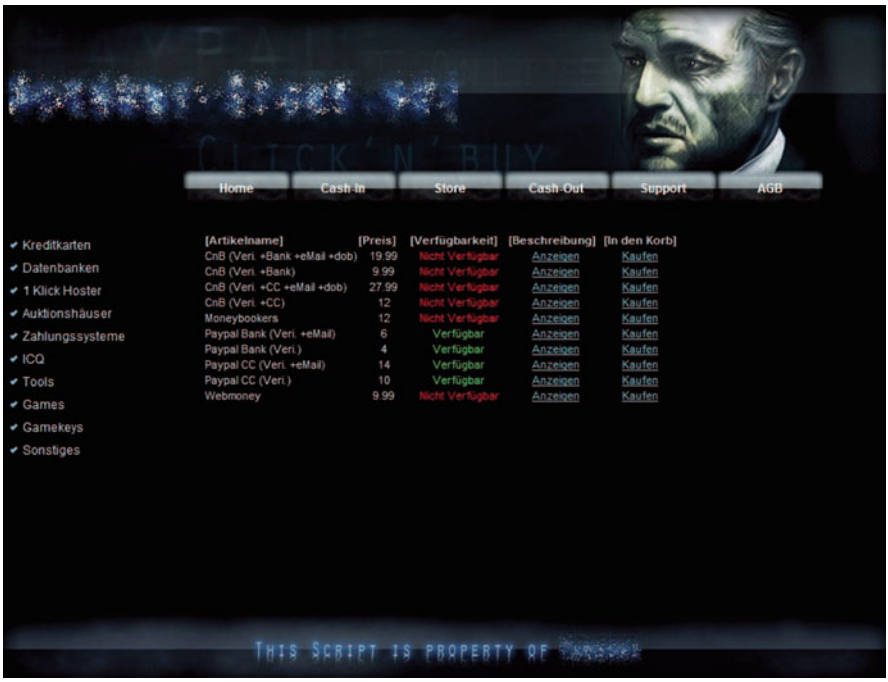


Fig. 3.6 Webshop for credit cards, PayPal accounts, and other stolen goods

Although this does not mean automatic acceptance, it is the basic prerequisite for a rental. Without such a recommendation, no shop can be opened.

3. *What does it cost me?*

Starting price:

$50—For setting up a header and footer as well as buttons

$100—Custom design, with different elements according to customer requirements (custom header and footer and buttons)

*$200—Complete "custom design," meaning the positioning of the elements (buttons, etc.) are not predefined, such as *******.cc or ******.net or ******.net or *****.net, and the design is completely individual.*

Selling prices:

$0–1000 per month: 33.33%

$1000–3000 per month: 30%

More than $3000 per month: 20%

The percentages are deducted from the total profit.

If the leaser has no other requirements, the payment will be made every 3 days, but at the earliest 24 hours after the last payment.

* * *

It is also interesting that the shops even give guarantees on the functionality of their goods. So if a set of credit card details fails to work, the buyer actually has the option to complain. He then gets either an amount credited to his account or "new goods." Here you can clearly see the professionalism in the fraudsters' approach to their "job." And the relationship between those who offer something analogous to real-world "fencing" services by helping the thieves to cash out and the thieves themselves is also clear: if the thief delivers bad goods, this also has negative consequences for the "fence" or intermediary. Because he is the one who must then deal with a bad reputation in the community and lose his customers if they move to other "fences."

At this point I would like to mention the *scammers*. They are, so to speak, the "the scammers who scam the scammers." To be sure, they act in the same way as the cybercriminals described above and offer data, goods, or services for sale, usually against advance payment. The only (but crucial) difference is that the buyer never receives these goods or services, and the scammer seems to disappear without trace.

However, it can also happen that the scammer's new customers initially get the goods they want, and in that way he gains their trust and makes a name for himself. And this sets the groundwork for him to squeeze larger sums of money out of his victims later. In many forums there are now evaluation/ratings systems for buyers and sellers, similar to those we know from legal web shops like eBay and Amazon. In this way it is possible to immediately recognize potential business partners as trustworthy—or not.

Most forums have long threads complaining of scammers, as shown in Fig. 3.7. But of course complaints threads are also open to abuse. Often, negative *posts* are used to make a (perhaps already unpopular) competitor look bad and drive them out of the market. Thus, screenshots and related evidence are required in many forums before board administrators will take action against certain users and perhaps block them.

3.2 Is *Everything* for Sale?

The underground economy offers various product groups and services. Most criminals have all kinds of information on their wish list that they can use to create accounts or take over identities.

1. Online stores trade in personal information such as names, signatures, and so on, as well as "database dumps," that hold data on thousands of users. Database dumps are copies of databases from online stores or forums that store user data. There are data that are offered free of charge in the marketplace, but this generosity is limited to databases of competing forums, because user data from "classic" online shops are simply too lucrative to share with "colleagues."
2. The addresses of so-called cardable shops are similarly in demand. These are web shops with poor controls where online shoppers can easily place orders using stolen credit cards. The more data a shop requests, the more data the scammers must capture or buy, which means the more complete the credit card record, the more valuable it is.

Fig. 3.7 Forum with messages about scammers

Proxy The English word "proxy" means someone who can act on behalf of a third party. In the IT sense the term "proxy" mainly relates to servers. For example, proxy servers are a company's surrogates for surfing and mailing.

Regardless of location or IP address, there are free "open" proxy servers that anyone can use. One can also use a for-fee proxy server, and this is often more reliable and faster than using a free alternative. Using malware, cybercriminals can even turn any computer into a proxy server so they can pass on all emails and websites visited via a hijacked PC. The intent is always the same: to make the IP address and identity of the mailer or surfer untraceable (Fig. 3.8).

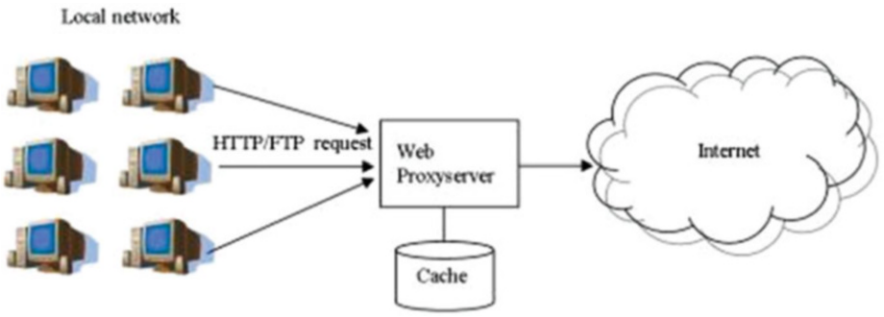


Fig. 3.8 Proxy servers switch between the user and the Internet to speed up activities on the Internet but also to hide user identities

3. It is extremely important for cybercriminals to encrypt all data that could reveal information about their true identities. Therefore, the use of proxy servers when visiting forums and websites in this environment is unavoidable, because only in this way can a cybercriminal make sure that his own IP address is not logged, or in the worst case stolen and published elsewhere.

If the user submits his requests via a proxy to a forum, the protocol of the forum shows only the IP of the proxy server, not that of the user. Thus, it is impossible to work out which IP address belongs to the user. This is very problematic when a crime is committed, because without the criminal's IP, the judicial authorities have no way to request the corresponding name and address from the relevant network providers via a court order.

Cybercriminals particularly like to use proxy servers abroad. For example, Eastern European criminals prefer to use proxies based in Germany, The Netherlands, and Switzerland, while German criminals prefer servers based in Poland, Russia, and the Ukraine for their schemes.

In this context, lists of information about free proxy servers are available on countless websites. But their performance is often not fast enough, which is why people resort to for-fee providers. Some for-fee providers are also part of this shady ecology and they therefore sell their proxy services directly. The offers range from the simple proxy, with which one can surf anonymously, to versions with where one can chat anonymously using services such as Instant Messenger, IRC, or Skype.

4. Even so-called infections or malware are sold. These are intended to compromise victim's computers in order to build a botnet or to commercially exploit the compromised computer with spyware or with adware (software that causes the Internet user to be bombarded with unsolicited advertising).

There are a variety of methods that can be used to install malware onto a PC. A popular option (for criminals) is the distribution of malware via offers of pornography. Another way is to distribute emails that contain links to dangerous

websites, or with which—as ever—malware is sent as an attachment. A careless mouse click is enough for the computer to be successfully attacked. Many Trojans are also distributed via file sharing platforms. Here they are disguised as desirable programs, games, and the like. Once the attack has been successfully effected, the Trojan loads the bot (short for "robot," a small program installed on the PC) over the Internet, and the PC is now part of the botnet. These examples make it abundantly clear how important it is to have a good antivirus program and to keep it up-to-date.

5. So-called outsourcing is also booming in the digital underworld. If you do not want to get your fingers dirty by infecting or otherwise attacking computers, you have the choice of a comprehensive range of service providers. On underground boards, infection with viruses is advertised as a service (Fig. 3.9). The prices depend on the countries where the victims live. Preference is given to compromised computers in Western Europe, North America, and Australia, as these regions maintain the best Internet infrastructures. However, the prices are correspondingly high. Meanwhile, there are bot dealers who pay per thousand bot-infested computers to expand their botnets.

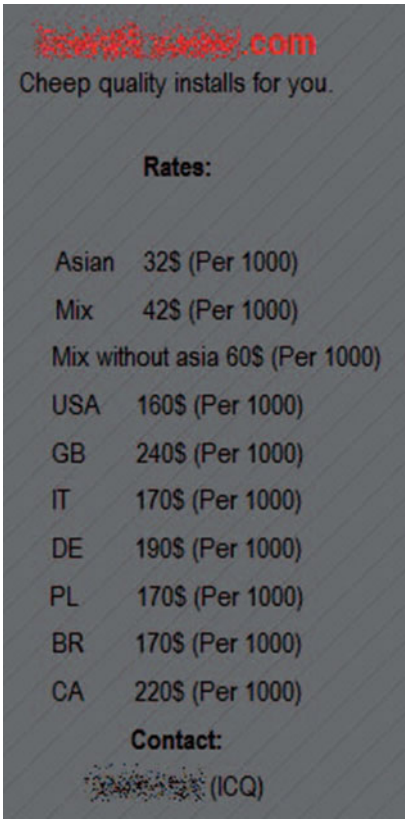


Fig. 3.9 Website that offers "viruses"

A compromised computer can make money in many ways. In most cases, the scenario is as follows: once the computer is infected, all the data stored on it that can be used to make money are copied and sold. Subsequently, all associated accounts are stolen and offered on the black market. Now that all usable data has been "used," the bot only serves for tasks such as sending spam or use in DDoS attacks.

6. Anyone who wishes to use servers in an environment protected from international crime-fighting access is well served by the "bulletproof hosting" suppliers. Typical examples of this are vendors of pirated software and child pornography.

Here one also finds people looking for "drop zones" for botnet data or people who manage illegal shops and the like. In this context drop zones are servers on which, for example, the spyware installed on a victim's computer can store the data collected. The bulletproof hosting product portfolio varies, as with any honest provider, from offering small corners on the server to virtual servers to entire server clusters, depending on the amount of "investment capital" available and the customer's feature requirements (Fig. 3.10).

The terms of use are usually very vague in these applications: the terms "forbidden or abuse" do not usually even appear. In this environment, however, it is well known which provider allows which services. Some only allow pirated software copies, others even allow the hosting of child pornography on their servers (Fig. 3.11).

Managed VPS Benefits:

- Dell PowerEdge 2950.
- 2 x Intel Xeon E5430 Quad Core Processors.
- 8GB DDR2 PC2-5300 Fully Buffered ECC Memory.
- Hot swap SAS disks with hardware RAID5 - Raid5 mirrors your data across multiple disks.
- RAID5 data synchronisation, garantued data security!
- Fully Managed! 24/ 7/ 365 Proactive Service Monitoring + Security Updates.
- Confixx Pro 3.x Licence included / RES / WEB - PHP5.
- 24/ 7/ 365 Support via Email, Forum and Ticket System.
- 2048 MB SWAP Memory - Full Power VPS.

Managed VPS location in Turkey / Ankara. Fast and Secure! MediaOn Fully Managed VPS - Overview:

VPS Disk Space	10 GB	20 GB	30 GB	40 GB	50 GB
RAID5	✔	✔	✔	✔	✔
Guaranteed RAM	256 MB	256 MB	384 MB	512 MB	1024 MB
Quad Core CPU	✔	✔	✔	✔	✔
Traffic & Bandwidth	100 GB	200 GB	300 GB	400 GB	600 GB
1 x PI-IP address	✔	✔	✔	✔	✔
Confixx Pro 3.x	✔	✔	✔	✔	✔
Host Unlmted Domains	✔	✔	✔	✔	✔
Period of payment	3 months	3 months	3 months	3 months	3 months
Monthly price	39 Euro	42 Euro	59 Euro	72 Euro	119 Euro
Setup	0 Euro	0 Euro	0 Euro	0 Euro	0 Euro
See all details:	details	details	details	details	details

Fig. 3.10 Overview of offers from a hosting provider

What can i host ?	Web Hosting	Semi Dedicated	Managed VPS	Managed Server	Bulk E-Mail Plans
Can i host toplists ?	✗	✓	✓	✓	✓
Can i host hate sites ?	✓	✓	✓	✓	✓
Can i host child porn ?	✗	✗	✗	✗	✗
Can i host adult sites ?	✓	✓	✓	✓	✓
Can i host warez sites ?	✗	✓	✓	✓	✓
Can i send bulk e-mails ?	✗	✗	✗	✗	✓
Can i host political sites ?	✓	✓	✓	✓	✓
Can i host hacking sites ?	✓	✓	✓	✓	✓
Can i host business sites ?	✓	✓	✓	✓	✓
Can i host gambling sites ?	✓	✓	✓	✓	✓
Can i host download sites ?	✗	✓	✓	✓	✓
Can i host fraudulent sites ?	✓	✓	✓	✓	✓
Can i host investment sites ?	✓	✓	✓	✓	✓
Can i host chat or shoutbox ?	✗	✓	✓	✓	✓
Can i host MUDs/RPGs/PPBGs ?	✓	✓	✓	✓	✓
Can i host pharmaceutical sites ?	✓	✓	✓	✓	✓
Can i host HYIP or related sites ?	✓	✓	✓	✓	✓
Can I host hundreds of pictures ?	✗	✓	✓	✓	✓
Can i host freedom of speech sites ?	✓	✓	✓	✓	✓
Can I host hundreds of big archives ?	✗	✓	✓	✓	✓
Can i host mail bombers/spam scripts ?	✗	✗	✗	✗	✓
Can i host autosurf/PTC/PTS/PPC sites ?	✗	✓	✓	✓	✓

Fig. 3.11 A list of the services allowed by a hosting provider

When it comes to providing these services, Russia, Turkey, and Panama are the countries most commonly mentioned, although it's not possible to say authoritatively where *all* these providers are. This is because unlike normal hosting service providers, cybercriminals do everything possible to hide their identity. And that applies also (maybe particularly) to bulletproof hosting providers. They use "straw men" to represent them situated in other parts of the world, preferably in Africa or Asia. This guarantees the protection of the identity of the users of a bulletproof hosting provider and thus also offers better protection against prosecution.

7. Probably the most important activity pursued by the digital underground is spamming, that is, the mass distribution of unwanted emails. In the e-crime milieu, this enjoys great popularity, if only because there's a lot of money to be made. For sending 1 million spam mails, a botnet owner might make $900 and more. Even with a relatively small botnet of about 20,000 bots, he only needs 25 seconds to complete this job at a rate of, say, two mails per second with the whole botnet active. This explains why botnet owners are so motivated to add more and more bots to their networks.

The customer may decide for himself to whom his spam mails will be sent. Many owners of botnets offer their customers a wide selection of countries. It is also possible to send the spam to specific interest groups, for example, only to people who play online games. It is not a problem at all to buy address lists in the shops of

most forums or via specialized spam service suppliers. Mostly, these are already customer-friendly and divided into different categories. Not infrequently, the salespeople explain earnestly that these addresses have not yet been sent as spam, but that only means that they have not sold these lists to someone else, not that the addresses on these lists have not been used by other spammers.

8. One of the worst scenarios for website owners is undoubtedly a DDoS attack. Protecting yourself from this type of intrusion is almost impossible if the attack is high-intensity, with a sufficient volume of PCs all attacking at the same time. Often the only option for the owners is to wait until the "storm" is over. Only then is their website or service accessible to the outside world again.

Implementing such an attack is of interest to the competition, for example. If a competitor's website becomes unreachable due to a DDoS attack, the likelihood of customers switching sites increases. If there is successful DDoS attack on an email provider, it will most likely result in a loss of reputation and trust among its customers, which will give its competitors much pleasure (Fig. 3.12).

Such DDoS attacks often target other sites and forums within the e-crime community, in order to displace them. Reasons for such actions include simple business considerations but may also include envy and simple dislike—common motivations even in the (legal) free market economy.

9. Counterfeit documents are becoming increasingly popular and profitable. In particular, driving licenses and student ID cards are increasingly in demand, as well as stolen passports and any other documents that can be used to hide a real identity or that may be accepted as genuine by a third party. In Russian forums especially, there is a flourishing trade in such documents.

Fig. 3.12 Banner for DDoS attacks that can be found on the Internet

Stolen or counterfeit documents are used to open bank accounts where the money for stolen goods is deposited. Or a criminal wishing to hide his true identity can log into online casinos or auction houses, which is usually not possible without some proof of identity.

Therefore I must advise you to report the loss of any personal documents to the police immediately. Otherwise, you may quickly face a Kafkaesque scenario where you have to try to prove that you are who you claim to be and that a third party is abusing your identity.

10. Credit card fraud is also still a lucrative business. When it comes to "*carding*," criminals use stolen or fake data to shop with—for example, in the already mentioned "cardable shops." Criminals get the necessary data using phishing Trojans on the computers of their victims (more on this in Chap. 6) or by hacking into the databases of web shops. Often the cards are simply copied when a customer makes a payment, without the card owner noticing. The offender quickly pulls the card through a second device, and seconds later he has all the necessary data. This scam is widespread, especially in tourist destinations. And then it's game over in terms of recovery, because with these data the crooks can shop to their heart's content at the expense of their victims.

Fortunately, if the affected customer reports the fraud immediately after receipt of the bill, the burden of proof that no fraud has taken place lies with the credit card companies. As with many other things, these data are widely used in various boards and shops (Fig. 3.13).

But even here the fun for cybercriminals doesn't stop. If you own a collection of apparently valid credit cards, you will be able to generate even more useful data. With a "credit card generator," which is easy to obtain in underground forums, new credit card numbers of various banks can be quickly and conveniently produced and

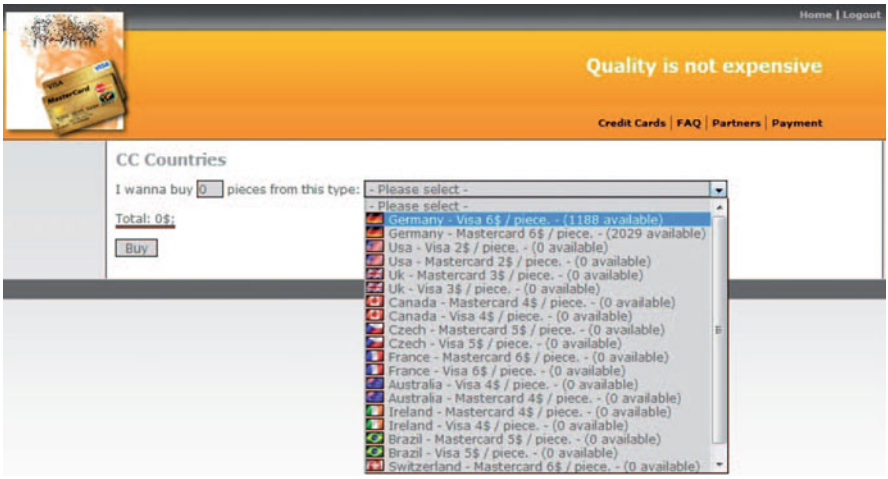


Fig. 3.13 Shop for credit card data

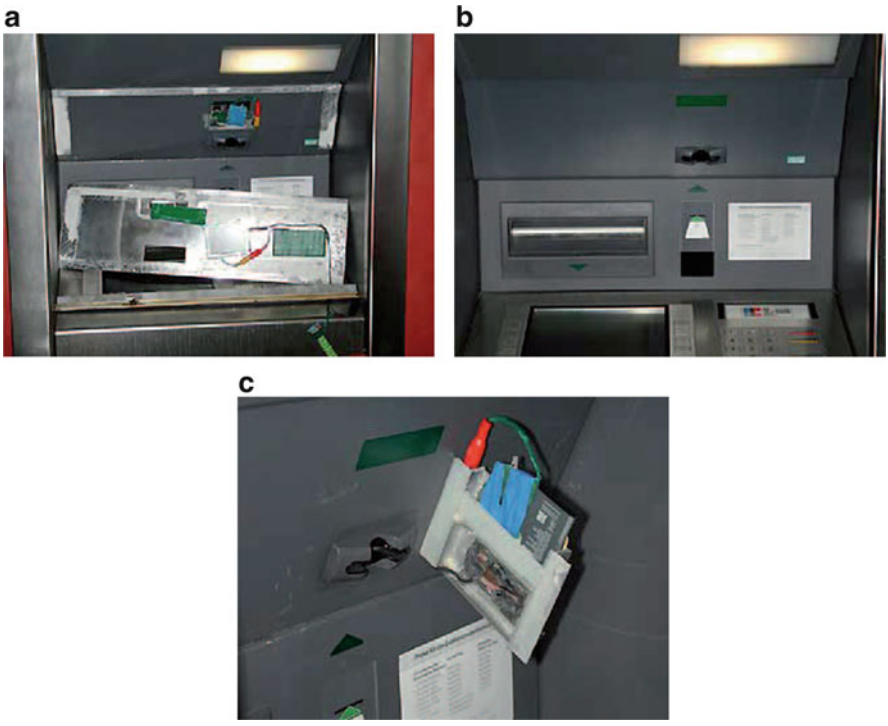


Fig. 3.14 A manipulated ATM

used for shopping on the Internet. This is possible because most providers use consecutive numbers when issuing cards and the method of calculating credit card check digits is publicly known.

It is important for the carder that the data are complete. The price therefore depends on the scope of the delivery: does the buyer receive only the number and expiration date of the credit card or are the other relevant data included? In the latter case, the buyer will have to pay a much higher amount per record.

11. The best camouflaged form of cybercrime is skimming, as the perpetrators must operate in the real world and be careful not to get caught. Skimming consists of attaching technical devices such as card readers and a camera to an ATM (Automated Teller Machine). (See Fig. 3.14.) The device reads the victim's card while the camera films the PIN (Personal Identification Number) as the victim types it in. Since these devices have to be installed in public and the risk of exposure is considerably higher than in the case of pure online fraud, this form of fraud, to our relief, is not widespread. The crime is complicated by the relatively high costs of the technical equipment: the hardware required costs several thousand euros in the relevant forums. In addition, the skimming devices can be detected and confiscated at any time. So the installation process is very dangerous for the offender because most ATMs are now monitored around the clock via video cameras.

Often the perpetrators come from abroad, in particular from Eastern Europe. In the past, many skimming devices were discovered by attentive customers and reported to the police or the bank. In the meantime, however, they have often become so well camouflaged that they are hardly recognizable to the layman. This is due, among other reasons, to the fact that criminals know the exact dimensions of the ATMs and can therefore adapt their devices perfectly.

12. Phishing is also a popular form of fraud. The bad news is that with this method the criminal can get almost all the data required for further fraud. First, he must have access to the bank details of his victims. He usually creates a fake bank site (phishing site). Then he sends large amounts of spam via his botnet with links to his phishing site, and then it's time to sit back and drink tea. Victims in this case are often people who reveal their bank details in all innocence and good faith on the fake site. This method "fishes" for all data that can somehow be turned into money: from user data for gaming sites, via credit card data, to accessing data for online banking or for packing stations, which are distribution centers for goods acquired as money laundering (see also Sect. 3.4).
13. Then there are the so-called data-stealers. As the name suggests, these are used for the theft of account data. Definitive protection is provided only by an excellent antivirus program that reliably monitors all access routes, for instance, by using an HTTP filter to monitor the browser or a mail scanner to check the email inbox.
14. Finally, there are the keyloggers: it would be remiss of me not to mention them. These small programs nest in the computers of their victims. Once they are anchored in the system, they read everything that the user enters via his keyboard. For a criminal, this is a very convenient way to get usernames and passwords when they are not stored anywhere in the system so that the user has to reenter them over and over again.

Also very popular are accounts for online betting or online casinos, as criminals can thus launder their earnings from other fraudulent schemes.

In the digital underworld, there is virtually nothing that is not available for the right price. Rummaging around in the relevant forums, you quickly come to the realization that even stolen Facebook, MySpace, and Twitter accounts are being traded. The purpose is to harvest as much personal detail as possible about prospective victims, because only then can fraudsters take over their identities and use them for their malicious purposes.

Marketing in the Underworld

In addition to the abovementioned resemblances between the underground economy and the "classic" business world, there are a few other striking similarities. Yes, underground dealers offer discount sales! If certain products are selling badly, they apply big discounts to generate sales during quiet periods.

Traders can also apply popular marketing tricks such as free offers. An offer of DDoS services, for example, often includes the selling point "The first ten minutes are free!"

15. Many people are recruited into service as "money mules." These aptly named people move the cybercriminals' illegally earned money around in much the same way as normal couriers and transfer services. The money is picked up at a from one bank account to another bank account mostly with several bank accounts in between making it harder to trace. Transferring a victim's money to a money mule account for subsequent transfer to the ultimate beneficiary's account is also part of the role, and for this the mule receives a small fee.

3.3 How a Mass Attack Works: Botnets and Their Structure

The invaders like to use "exploits"—weak points in the operating system or in the software (see also Chap. 8)—in order to install Trojans, for example, on the victim's computer. In order to avoid immediately alerting active anti-malware, the Trojans are encrypted with "cryptic codes," that is, their code is obscured. There are publicly available versions of these cryptic codes, but most of them cannot be reliably used for criminal purposes because owing to their large-scale distribution, they are immediately recognized by most anti-malware scanners. However, very expensive versions are available, which are considered "Fully Un-Detectable" (FUD)—they cannot be detected by virus scanners.

These Trojans download bots and install them on other PCs. Of course, very large bots are more expensive than simple, limited bots. The simple bots usually also have an Achilles heel, so it can happen that the botnet that you set up for yourself is taken over by a third party (Fig. 3.15).

For administration, the botnet administrator uses a web interface to make the data of the server user-manageable (Fig. 3.16). After entering the username and password, the customer will be taken directly to the administration control panel, where access to various functions can be found. In addition, statistics are available, indicating how many bots are online, how many are infected in total, or which operating systems they are running on. Also, updates can be carried out via the interface.

3.4 And What About the Victim?

Diverse as the tools and procedures may be, they all serve the same purpose: to make money! The bad news is that some of the biggest problems will not show until the fraudsters have already stolen money. There are different ways to "cash out." For example, you exchange your virtual money for real money, so that it's not possible to ascertain where the former came from. Often, stolen credit card data or virtual currency, which criminals have "earned" by sending spam, is used to pay for goods

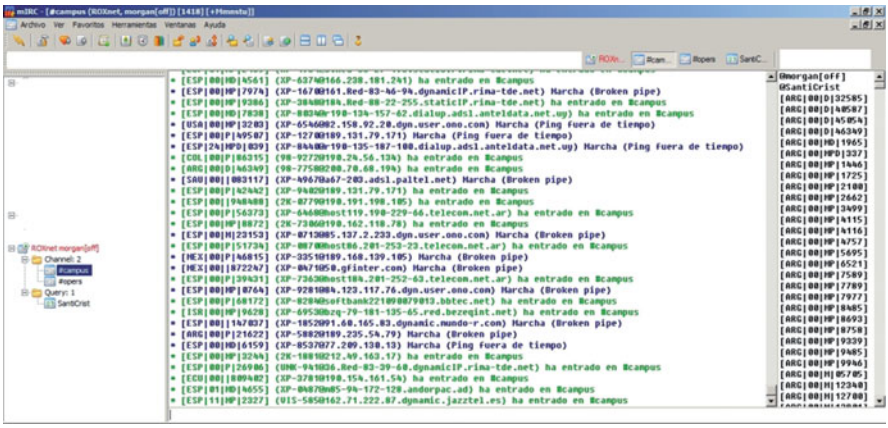


Fig. 3.15 Bots using IRC channels

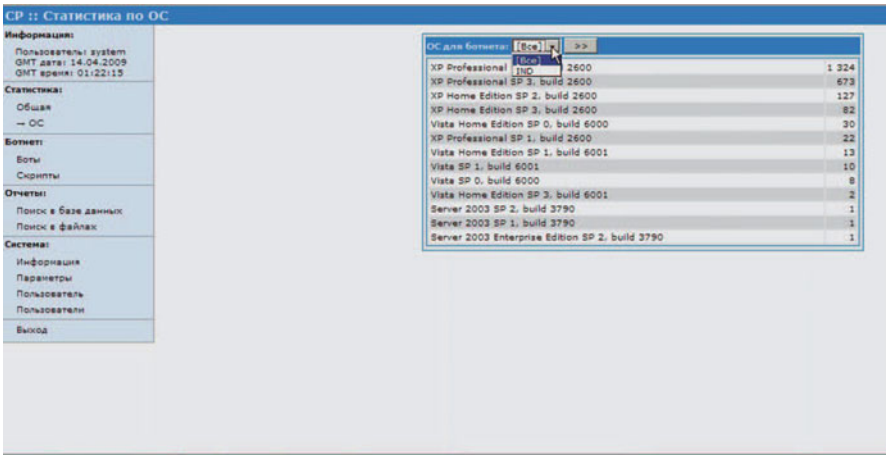


Fig. 3.16 Web interface of a botnet

on the Internet. In order not to be implicated in the subsequent delivery, the crooks ship the goods (this time physically) to so-called *drop zones*. Here straw men are paid to forward the goods immediately (Fig. 3.17).

Drop zones are extremely popular with criminals, which explains why they are so prevalent in underworld forums. The standard scenario is as follows: the ordered goods are shipped to an address in Russia (for instance). Here they are picked up by a straw man and forwarded to the address of the actual recipient. The straw man is nicely rewarded for his services, for example, by taking some of the ordered goods.

In the past, vacant houses and apartments were often used, and this was referred to as a "House Drop" in the underworld. You can also send all the mail from a bank, for example, to such an address.

Fig. 3.17 Offers for drop zones in a forum

The prerequisite, however, is to have the address of the victim changed at the bank. Obviously this can be done online, but an unscrupulous villain would not be afraid to go to the bank and ask the pleasant staff at the counter to make the change. He can get the fake documents that he needs for this via underworld forums. If he holds his nerve and he is persuasive when he visits the bank, there's nothing to stop an address being set up of as a house drop.

Another possibility for implementing money laundering takes the form of packing stations, to which goods ordered in web shops can be sent and then collected anonymously or pseudonymously. Criminals can buy stolen access data for the stations in forums or from shops in the underground market. Even with counterfeit

documents, one can collect goods from third parties at parcel delivery points relatively reliably and anonymously (Fig. 3.16).

Another method is to move money through online casinos. For example, the money can be used as a deposit at an online casino via a stolen PayPal account. Through reviews in the forums of this domain, one can quickly find out which casino or sports betting portals are best suited for criminal activities. Important factors here include what data are required to create an account, whether the authenticity of the data is carefully verified, and whether illegitimately manipulated proof of identity is accepted. For accounts that are already verified, cybercriminals are happy to pay considerable sums of money.

The money is passed on from the online casino account, preferably to a "bank drop"—an account to which one has access but which operates pseudonymously or anonymously. That is not so easy. Therefore, it is not surprising that advice on how to open anonymous accounts in this environment is sold for quite sizeable sums.

And there are also various combinations for cashing out. For example, a fraudster purchases goods via a *Cardable* shop on the Internet, which he then has sent to a packing station, for which he has stolen the access data from a third party who is unaware of what is going on. He then collects these goods and sells them through an auction house, and the money he gains is sent to his account. So who says cybercriminals are lazy?

3.5 Conclusion: E-crime Is on the Rise

The days when the hacker scene for the most part consisted of male adolescents who went on the Internet for fun and out of technical interest are long gone. In addition, using the term "hacker" for this new generation, which operates in a "digital underworld," is simply wrong. These people are nothing more than offenders who, like safecrackers or other criminals, have a certain amount of "expertise." In today's scene, everything revolves around money, with millions transferred every year, both through active theft and fraud. Often, the perpetrators are linked by a professional organizational structure, within which each has their own task.

For the user with a home PC, it is therefore increasingly important to protect that computer from such evil stratagems. Anyone who goes on the Internet today without proper protection is in constant danger of falling victim to this type of criminal. At a time when online auction houses and online banking are part of everyday life, this poses great dangers.

Another important topic is our handling of personal data. Many of us thoughtlessly put up a lot of personal data on our social networks, without considering that this plays almost directly into the hands of scammers. This is because even seemingly insignificant pieces of data, like your date of birth, can help to supplement information from other sources that may be enough to work out credit card details, for example.

More and more often, cybercriminals, after they have stolen the account data of their victims, also take advantage of their web pages, such as blogs, Facebook pages, and so on. If you know that there is malware on your PC, not only does your computer need to be scanned and cleaned up—you also need to check your website! Otherwise, an infection can have extremely unpleasant consequences: if the fraudsters have smuggled malware onto your website, you as the owner may be liable for any damage suffered by third parties.

What Have We Learned?

If you can't find personal documents, whether they were stolen or simply lost, you should report the loss to the police immediately. Because—faster than you would ever believe—your identity data can end up in the cyber underground and be used for online betting or other activities. Imagine what happens when you discover that in real life someone else is pretending to *be* you . . . then it's up to you to prove who you really are.

If your credit card is abused by criminals, it does not necessarily mean that you are going to lose all your money. In most cases the credit card company pays back the amount taken, but only if you report the fraud within 30 days of discovery. Be sure to remember this if you detect any irregularities on your credit card statement.

When using Internet services, you must be extremely careful with your data and carefully check where and through which channels you enter them. Common sense is needed here! Loud alarm bells should ring when you are asked on what seems to be an online banking website to keep supplying various confirmation codes or where there's no encryption of the data.

It is therefore always better to put the original URLs of the banks in your browser "favorites" and use only these links. It's also a good idea to check links in an email—even from seemingly authentic senders. A careless mouse click can quickly lead to a compromised page.

If you know or suspect that your PC is infected, check and clean not only your PC but also your website, which could also have been hacked.

Think carefully about what personal information you provide on social networks: This information can help cybercriminals; for example, to complete their credit card information in order to use it for further unpleasant schemes.

* * *

Chapter 4
From Cyberwar to Hacktivism

Chapter 3 showed us that behind the familiar facade of cyberspace lurks a dark and dangerous world. But that's not all. Even governments are not disinterested, neutral players: they use cyberweapons in a variety of ways to manipulate, spy on, and even fight against other nations. Therefore, we should not be surprised that government agencies taking action against other nation states have also discovered and deployed digital weapons. We are now going into the binary trenches to find out whether the digital James Bond likes his vodka martinis "shaken, not stirred."

4.1 Cyberwar

In recent years, we have heard the term "cyberwar" more and more frequently. But the term is (more or less) metaphorical. Why is it called cyberwar when there are no human victims? Not that physical casualties would be desirable, but as long as there are no dead and injured, the term "war" is, strictly speaking, inappropriate.

"Cyberattack" therefore seems to me to be the most suitable term. It remains to be seen, however, whether such attacks will be seen more often in the coming years in the context of real wars and if they will be part of the overall strategy used against potential enemies.

There is, by the way, another reason not to speak of a "cyberwar." In a real war, there are always at least two identifiable nations or regions involved (or ideologies, or religious, or even classes). By contrast, Internet attacks are usually attacks made by or on behalf of a party that cannot even be identified with absolute certainty.

The first examples of attacks that we saw referred to as cyberwar occurred in 2007 and 2008. In 2007, the Internet infrastructure of Estonia was under attack for weeks after the Estonian government had decided to remove a statue surviving from the Soviet era. These repeated DDoS attacks proved to be the work of more than a million computers apparently located in Russia, leading to total chaos. In Estonia, 97% of banking transactions are processed online. For this reason alone, the

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_4

unavailability of many Estonian websites hit the economy and the entire population particularly hard.

Nevertheless, even this event does not merit the term "cyberwarfare"; at most, one might speak of a remarkable experiment. Furthermore, it has not yet been established beyond doubt that the attacks bear the signature of the Russian authorities. According to the data available to us, the attack was organized by Nashi, a political youth movement in Russia. Strictly speaking, a hacking group was behind the event, and while the Nashi movement is tolerated and supported by the state, that still does not tell us whether the state actually instigated the attack.

It has not yet been proven whether disruption of the Georgian infrastructure, while Russian tanks were overrunning Georgian territory in 2008, was the work of the Russian authorities or the FSB, the Russian secret service. However, the timing suggests that the latter agency was involved.

Are the countries that suffered these assaults better prepared now to withstand similar attacks? Probably not. I am convinced that only a few countries are well-prepared. A targeted attack carried out today by a "pack" of zombies (PCs compromised by bots) would also paralyze many official websites. But would that be really bad? How many nation state websites have to be available day and night? Sites like the Belgian Tax-on-Web system, the Dutch tax declaration module, or the US Internal Revenue Service (IRS) probably do, or else taxpayers could unwittingly miss deadlines for online submission of tax returns. But for most official websites, some downtime (unavailability) is more annoying than traumatic, at least as I see it. Perhaps there are attacks that could disrupt a whole nation.

In the coming years, however, cyberattacks could lead to far greater problems. You do not need to be Nostradamus to predict that we will become much more dependent on online access to services provided by government authorities and the private sector in the near future. And at that time the impact of such attacks is likely to be more severe.

4.1.1 The Cloud as a Battlefield?

The "Cloud" is a collective term for all the software and infrastructural components offered by external parties (Fig. 4.1). Both Dropbox (for online data storage, sharing, and version control) and Google (for finding and storing data, and much more) are examples of cloud services. But companies also use cloud software in a wider range of contexts. Some vendors also offer cloud versions of their software. A usage fee is applied, which may benefit some users in terms of funding a wider range of options and services. In addition, this software is stored centrally and is therefore always available wherever you are, connectivity and bandwidth permitting. The disadvantage of this system is that you need to be sure that the appropriate online service is always accessible and that the servers on which the services run are protected against all possible attacks.

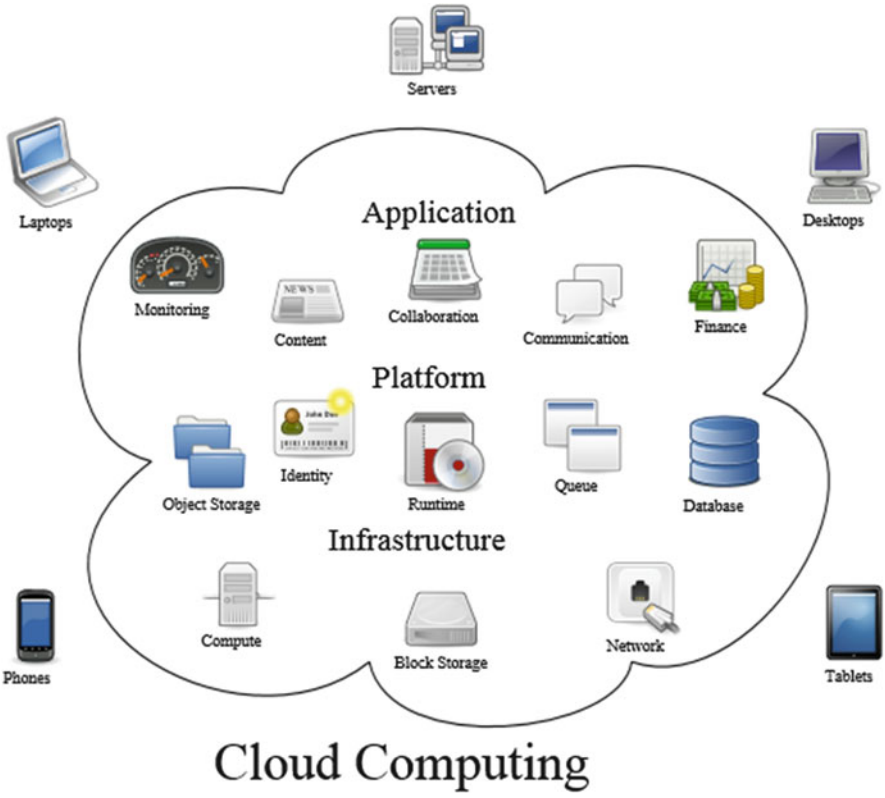


Fig. 4.1 The cloud

Admittedly, the Cloud is (or should be) better protected than the regular websites of private individuals and companies, but an attack on the cloud would enable the attacker to reach many victims at once, and the consequences of such an attack would be far-reaching. We must therefore be wary of the euphoria sometimes inspired by the vaunted potential of cloud computing. It may be better protected than it used to be, but the attendant risks are significantly greater than those entailed by local storage and processing. In addition, we should ask ourselves whether the cloud is always the better solution. Unfortunately, the bandwidth required for its use is still not universally available. Have you ever tried to download a file that is more than 1 MB in size over a mobile phone connection? Or have you ever wanted to send a tweet during a conference while many other attendees are competing for online access? Then you know from your own experience that the cloud is not always the fastest or most reliable option. Perhaps this will change as we adopt newer technologies, but at the moment, the effectiveness of cloud computing is often overstated and its benefits literally nebulous.

4.1.2 Stuxnet

Stuxnet is also often mentioned as an example of cyberwarfare, but I do not agree with that. Admittedly, Stuxnet was a highly sophisticated and complex worm that, among other things, provided access to the networks of energy companies. It managed to take control of some systems, temporarily delaying the production of a uranium-enrichment plant in Iran. An attack took place on the headquarters of a company said to have played an important role in the alleged plans to build an atomic bomb in Iran. This worm affected the development of the nuclear facilities, and this was considered sabotage of nuclear components. In my opinion the whole affair comes closer to being describable as cyber-sabotage. Luckily for the whole world, it was again a one-sided attack, with no human casualties.

This does not, of course, alter the fact that the trend is *toward* cyberwarfare. It's appropriate to speak of a cyberwar when the infrastructure of a country is in danger. If, for example, an attacker paralyzed the US electrical power grid, one could certainly regard it as an act of war. And this danger is quite real, because energy suppliers are often less well-prepared than you might think. Are you aware of the term SCADA (Supervisory Control And Data Acquisition), for example? Such computer systems monitor and control technical processes involving various machines in large industrial plants. SCADA software controls systems hardware that is (or should be!) generally well protected via the IT infrastructure. Suppliers and users of SCADA software often mistakenly underestimate the importance of a reliable security program. Because they consider the risk of compromise to be relatively low, they become careless and do not update their software regularly. Even where the utility administrators are security-savvy, their efforts may be constrained by poor practice on the part of hardware/software suppliers. In my opinion, this carelessness is a cause for concern, as Stuxnet settled down all too comfortably into such an environment.

It is also the case that, as a result of attacks such as Stuxnet, Flame, Duqu, and Gauss (Sect. 4.4 "Cyberespionage"), various authorities worldwide are developing concepts for cyber-strategies or cyber-oriented units. Agencies are even developing platforms for easier, less bureaucratic exchanges of information about this problem, so that they can better assess where attacks are coming from. However, cooperation between different nations is limited and is subject to the initiatives and political interests of individual countries. There is currently no global coordination of cyber-strategies, which is why we cannot expect comprehensive protection at this level. On the contrary, the danger is that when differing cyber-strategies come up against real cyber threats, they tend to create chaos rather than better protection. Designing cyberwar treaties between nations is likely to prove a hard nut to crack, arising from different approaches to cyber-strategy in different countries.

It may seem premature to deal with such strategies, especially since there are no signs that a cyberwar threatens. Not even close. But it is only reasonable to determine at an early stage how to act in the event of a cyberattack. If, for example, an attack is launched against a country's central water and electricity supplies, there

will actually be civilian casualties. There must be action plans in place to address a range of scenarios. This is the only way to save human lives and to prevent an inappropriate reaction to a possible attack. In short, good preparation for a cyberwar might even prevent it.

4.2 Cyberterrorism

In my opinion there is actually no such thing as cyberterrorism. We speak of "terrorism" when it comes to bloody attacks like 9/11 or those more recently seen in London or Madrid or Paris. But it has never been the same in cyberspace. Although we can find online communication related to the implementation of such attacks, and terrorists use the Internet for recruitment and for communication, we have not yet encountered true terrorism in cyberspace.

As with cyberwar, however, this does not mean that we should ignore the threat of cyberterrorism. Comprehensive protection is the watchword here, too. The potential dangers should—as far as possible—be worked out in detail and appropriate protective measures taken. I participated in the European "Clean IT" project, the results of which are available on the Internet (http://www.cleanitproject.eu/). There it was explicitly stated that there was still no cyberterrorism as such at that time, but that nevertheless, preventive measures must be taken proactively. Potentially, there are sensitive censorship issues, but if we ignore the danger completely, we anticipate that more people will be recruited into performing terrorist acts. For themes such as pornography and violence, there are already numerous filters at work, so the fight against terrorist threats on the Internet would simply be the next step. Would it not make sense to be able to identify terrorist pages at the touch of a button? In the case of the Clean IT project, the question was framed thus: What solutions and technologies are meaningful and, above all, possible?

It is of course extremely difficult to achieve cooperation and coordination between all the member states of the European Union, let alone across the globe. For me, however, this is a missed opportunity, because if we were to put all our knowledge together we could fight terrorism much more efficiently. There clearly *is* cooperation and communication between governments in the case of terrorist threats, but it's either restricted to small groups of countries or rather informal, which is not a soothing thought.

I would like to say once more that Stuxnet is *not* an example of cyberterrorism. Terrorism aims, among other things, to cause panic, while sabotage aims at destroying a particular target or service. In the case of Stuxnet, the intention was to delay work at a factory so that Iran would not be able to carry out its uranium-enrichment program. Scaring the population may have been seen as a desirable side-effect, but it wasn't the original motivation, which required a degree of covert action.

Thus, Stuxnet falls into the same category as the attack on Saudi Aramco, the state oil company of Saudi Arabia—the world's largest crude oil exporter. More than 30,000 computers were infected by Shamoon and temporarily disabled. The purpose

of the attack was to slow down or temporarily shut down the production of crude oil. This purpose was not achieved, in that production processes as such were not affected, but data was deleted and hard disks completely destroyed, causing severe disruption to business processes. Iran was blamed for the attack. It denied involvement, but for most observers the attack is still today considered a warning signal: it is postulated that Iran wanted to find out what would be possible in a real war. But it seems inappropriate to call this cyberterrorism.

I therefore advocate categorizing well-known attacks more accurately as, for example, cyberespionage or cyber-sabotage. As I said, the term "cyberterrorism" is not really appropriate. Admittedly, the term is sensational and exciting and can attract many readers to an article that uses the phrase. However, one should also make clear that sensationalist media coverage can frighten people unnecessarily, especially if this coverage contains terms that denote a nonexistent danger. Up to this point there has not been a single terrorist act on the Internet, even if the media want to believe—or want their audiences to believe—something different.

4.3 Hacktivism

The confusion regarding cyberterrorism is due to a large extent to hacktivists. Their actions are often referred to in the same breath as cyberterrorism or cyberwar, but hacktivists are not terrorists, and they certainly do not wage war. They use hacking and DDoS as a means to spread messages of a mostly political or ideological nature, which may have an intimidatory effect. Terrorists also have a political agenda and send an ideological message and may even intend to be intimidating, but their main tools are violence and *physical* intimidation.

I want to clarify once and for all: malware is not a type of hacking. Of course, malware and hacking have certain similarities: they are both undesirable, and techniques and code are often shared between criminal groups. But there is a substantial difference between the two. Malware, as you know, means any form of malicious software that can manipulate computing devices. Hacking does not necessarily involve malware. A hacker can simply try to penetrate a foreign system or access a webpage using the login data of a third party. However, he can also bypass the security of a system or website in other ways. Sometimes—but not always—malware is used.

The motives of hacktivists and their approaches to what they do could not be more different. Some want to denounce the authorities' lack of data protection by publishing confidential government data, as happened in Chile. Others attack the website of a news service or station because they are dissatisfied with its reporting. The American news channel CNN experienced this when it made critical comments about human rights in China during the Beijing Olympics. The hacktivists' weapons include the ability to disable websites or redirect visitors to their own pages, to steal information and to publish it elsewhere, to parody legitimate pages, and to use "typosquatting." [That is, a user who mistypes a URL may be redirected to a hacktivist's page.]

I've deliberately chosen the term "weapons" to make clear that hacktivism is a criminal offense and violates certain laws in most countries. It seems that many hackers are not aware of this. When hacktivists pursue noble goals we should always be able to acknowledge this. They don't usually resort to destruction. Anyone who leaves a positive message on his own website and ensures that users are redirected there is not doing anything morally wrong, or even unlawful. But destroying or "defacing" the website of a third party (changing the page, e.g., using slogans of a hacktivist group), stealing data, and publishing these data elsewhere are clearly criminal acts in jurisdictions where unauthorized access and unauthorized modification (according to frequently used terminology) are specifically outlawed! I always wonder what such people have in mind. If you want to point out to a company that it's not well-protected, you can simply say so, right?

Hacktivists have contributed to a situation where many see no difference between a hack as a statement and a hack with criminal intentions. And yet hacktivism is considered in a positive light, and hacktivists enjoy such a good reputation that even everyday computer users are starting to behave like hacktivists. In the meantime, a lot has happened in this domain, and many hacktivists have been arrested. Nevertheless, they have been able to benefit as a group from positive media interest for much too long.

What is also noticeable to me is that hacktivists are often associated with cyberwar. Even in a broadcast by the renowned Flemish TV magazine Panorama, hacktivism was considered in the same breath as "cyberwar" and hacktivists were offered a platform. However, there was no counterbalancing discussion of how to fight hacktivism. I am consoled by the thought that even the best people sometimes make mistakes.

As a result, hacktivism is viewed by many as a nice, positive, and legal pastime. But anyone who is really concerned with the machinations of the hacktivists knows how wrong this sentiment is. What would these "fans" say if someone broke into their homes, stole their furniture, and hung their pictures somewhere else? The morality of hacktivists leaves something to be desired, and yet to say so seems to be taboo.

V for Vendetta

When the media talk about hacktivists, they usually accompany it with a photo of a Guy Fawkes mask.

Fawkes was an English soldier who lived from 1570 to 1606. Together with other Catholics, he was involved in a conspiracy to kill the Protestant King James I in a gigantic explosion in the Houses of Parliament. But Fawkes had already been compromised, and he was arrested and sentenced to death.

The failed attack is celebrated in England on 5 November (Bonfire Night) as Guy Fawkes effigies are burned. But even this man had his followers. When the 2005 film *V for Vendetta* appeared in movie theaters, the mask with

(continued)

Fawkes' face (Fig. 4.2) became a symbol of freedom of expression and the fight against the injustice of misuse of power by the State'. In particular, the hacktivist group Anonymous has used this symbol since 2008. As far back as 1994 there was a DDoS attack on Guy Fawkes Day by a hacktivist group with the rather cute name "the Zippies."

The masks from *V for Vendetta* are also very popular with security experts, and I even got a mask from a renowned security company. Surely this was all meant to be funny, but it boosted the positive image of hacking. I have expressed my dissatisfaction with this more than once, but my reservations have not always met with understanding—proof, in my opinion, of how sensitively this subject should be handled.

4.4 Cyberespionage

Cyberespionage is a reality, and it has been for a long time, as was clearly illustrated by the PRISM scandal of 2013. Edward Snowden told The Washington Post that the NSA and the FBI had for years accessed the personal data of suspects on social networks like Facebook and YouTube and accessed their communications using the software of Internet giants such as Microsoft, Google, Apple, and Yahoo. Snowden himself was a former CIA contractor; he worked as a systems administrator for the company Booz Allen Hamilton, which provided services for the National Security Agency (NSA). This collaboration was known as the PRISM program and served primarily to improve the monitoring of suspicious persons abroad. A clear case of

Fig. 4.2 A quote from the film *V for Vendetta*

cyberespionage. Perhaps the thing to remember is that this cooperation between government services and IT companies had already been launched by 2007.

This example of cyberespionage was discovered almost by chance and is primarily concerned with the intelligence services of the United States. But it's a safe bet that cyberespionage is also used in many other countries, even if we don't know the whole story. How much easier, safer, and cheaper it is to steal secrets from other countries (or, in the case of industrial espionage, from other companies) if you only need to work from behind a monitor in a protected environment, instead of spending years in the lion's den and spying on him when within reach of his paws.

In the Words of . . .
Guy Kindermans, ICT Journalist, Security Expert

You have nothing to hide, but everything to protect.

In Aalst, where I live, carnivals used to feature the custom of "indictment". A costumed merrymaker would read out a list of the 'sins' of the 'accused' in the presence of witnesses, usually his family. Nowadays you would think that the digital world traveler no longer needs anyone to do that for him as he is only too happy to release unbelievable amounts of information about himself, even unflattering details. Whether this is due to naivety or inexperience, and how—and to what extent—this information is distributed digitally, I would like to leave open for the time being. But everyone should be aware that information in digital form spreads like wildfire and that the Internet does not forget anything.

"And so what . . .?" I often hear, ". . .I have nothing to hide!" That may be true, but there is a principle everyone should know: "You have nothing to hide, but everything to protect!" Anything released in digital form can spread rapidly, even to those for whom it was not intended. Or this data makes its way to professional marketing companies that analyze it from top to bottom and then pass it on. Often this leads only to inoffensive advertising or discount campaigns, but you cannot exclude possible misuse of the data. For example, data you never intended to reach a prospective employer may be used as grounds for turning you down for a job—we're not even talking about information that became available somewhere without your consent, as we see from the revelations relating to the US security services.

In short, young (and even older) people would be better advised not to allow digital data to circulate if they don't want it to be seen by their parents or partners or acquaintances or colleagues. We all need to be aware that this morning's friend can become tomorrow's enemy. Even the European Union's privacy law—the General Data Protection Regulation (GDPR), reinforcing the "right to forget" power of data subjects—cannot guarantee that the data you share will not fall into the wrong hands. My advice is, therefore: never give away your personal information recklessly—protect it!

Guy Kindermans (born in 1956 in Aalst), a qualified translator and communication specialist, began his career with the computer science journal Data

(continued)

News. There he learned all he could about computers and their quirks. After a brief stint with the publications PCM Belgium and Schoolnetwerk, he worked full time at Data News, where he was a member of the editorial board for more than 27 years. During this time, he probably wrote about every conceivable aspect of IT—from silicon technology to company projects. However, the main focus of his work has for over 20 years been on security. In addition to all these tasks, he wrote the book "Wegwijs in de computerwereld." ("Finding your way in the World of Computers", 1988), and he regularly contributes on radio and television regarding IT topics. His hobbies are astronomy, space, and technology in general, but only if he is not deep into a science fiction novel.

Since cyberespionage usually uses extremely sophisticated technologies, it is not so easy to detect. If a case actually comes to light, as happened with Flame, Duqu, or Gauss (see "Stuxnet's Relatives" below), this is often regarded as an operation in a cyberwar. Basically, these computer programs were used as tools for cyberespionage with specific targets in the Middle East. The attacks could be compared to precision bombardment, with well-coordinated, targeted deployment, and the authors focusing only on areas in which they were particularly interested. Luckily there were no human casualties, and these aggressive activities were unilateral, so I prefer not to describe them as cyberwar, reprehensible though they were.

4.4.1 Stuxnet's Relatives

Although Stuxnet attracted the most attention, its "relatives" Flame, Duqu, and Gauss were also quite sophisticated and their programming suggests that they

were developed by the same team. Stuxnet became better known because it managed to temporarily paralyze an Iranian uranium-enrichment plant, but the others are very advanced malware, as they can register all the keystrokes and listen to and forward all calls routed via a computer. They were mostly used in the Middle East, and they managed to remain undetected for years. As far as we know, they do not drink vodka martinis, but they can be considered to rank with James Bond among the top spies.

Aurora was an equally modern and smart malicious program that triggered a series of attacks and even forced large, globally operating companies to their knees. The most famous victim was Google China, which publicly admitted its Aurora breach, sparking a controversial political discussion about censorship in China. Because of the political context, the most important aspect of Aurora was hardly noticed by the media: apart from Google, the hackers attacked around 30 other large companies, but their networks had obviously better protection. This reveals a lot about how clever the hackers were.

Aurora was able to penetrate the networks of large corporations because the malware used a previously unknown security problem, Internet Explorer's so-called "zero day" vulnerability (Sect. 6.1). Antivirus developers had not developed protection against this vulnerability. Also, the malware, which consisted of 12 different programs, was multiply encrypted, which is why it was not discovered until a long time after its insertion into the system.

The profit-oriented Aurora developers ensured that only certain decision-makers with system privileges suitable for exploitation were approached. To this end, emails with links to infected websites were sent to appropriate employees within the companies concerned. However, since many of these emails landed in spam folders, or were not taken seriously by the recipients, there was another very elaborate plan that took advantage of the popularity of social networks. The attackers did not set out to hack the accounts of the key figures of the company: instead they were intended to hack those figures' virtual friends. If successful, updates and reports from "friends" would be redirected to the actual goal—a tempting link to the infected website. A clever move, since a link posted by a friend appears to most people to be trustworthy and is likely to be clicked on. A single visit to the infected website was enough to download the malicious software in the background—completely unnoticed—to the PC.

Apparently the writers of Aurora had thought of everything. When the malicious software was detected after some time by the security software, the hackers had long since stolen the desired information from the company. After it was discovered, Aurora was described by safety experts as the "most advanced malicious software ever." But however unpleasant the consequences were for the businesses under attack, and possibly for their customers, the actual goal was industrial espionage. The general public had not suffered any damage, but the IT managers of the companies affected were certainly in the firing line in terms of criticism from their superiors and corporate heads.

Aurora illustrates what we call an advanced persistent threat (APT). As already stated, it used (for the time) state-of-the-art technologies, which is why the term "advanced" is appropriate. And the term "persistent" is appropriate because the malicious software was able to change its shape and remain undetected over a long period. APTs are, for now, mainly reserved for cyberespionage, because they require hackers with a particularly refined approach and a high degree of patience. It

is interesting to note that Aurora, despite all the skill and tenacity it involved, required a moment of weakness or inattention by an employee in order to achieve its goal. As with all other modern APTs, Aurora "impresses" us more because of its persistence than with its sophisticated technology.

4.5 Last but Not Least

The attacks using Aurora and Stuxnet allow us to reach some conclusions:

1. Malware is no longer restricted to script kiddies or petty criminals. Intelligent developers are also entering this market with considerable financial support from third parties, in some cases from the governments of various countries.
2. Cyberattacks are becoming more sophisticated. When a new attack is discovered, experts often wonder how it has been possible to develop it in just a few months, and yet it's a safe bet that a group of malware developers is working on a new project that will make the current attack seem like child's play. It is quite possible that the next "most advanced malicious software ever" has already penetrated all possible systems worldwide, without having been detected yet.
3. It appears that the targets of malicious software are also escalating in significance and profitability. If the cyberattackers were originally content to get a little money from those affected, business secrets and the like are now their (more profitable) prey. Apparently, their objectives nowadays are sabotage, extortion, complete control of industrial processes, destruction, and damage to the world at large.

In order to be able to ward off these exceptionally well-organized cyberattacks, much more is needed than just providing appropriate protective measures and raising awareness among personnel. Cooperation at the international level is indispensable. As in the case of nuclear weapon programs, the relevant ministries should adopt agreements regulating the participation of individual nations in the development and financing of weapons against cyberattacks. We need procedures that make it easier to find the people behind such attacks. Obviously, the organizations responsible for the attacks do everything they can to remain undetected and hide their tracks. Servers used for cyberattacks, for example, are regularly located in China or Russia, but that does not mean that the attackers are in these countries. Cross-border investigations are therefore an absolute must, and all countries should participate actively, or if they do not have their own experts, at least open the door to investigators from other countries. We need severe penalties for such attacks and uniform criminal laws in all countries. This is the only way to prevent cybercriminals operating out of jurisdictions that implement comparatively minor penalties.

It is not only a matter of politics: the police and the judiciary have to work hand in hand against this form of crime, but cooperation at the international level is more than justifiable in order to prevent cyberattacks. International companies need to be required to report all the (more or less) successful cyberattacks on their networks, even where this is, for various reasons, obviously not in their corporate interest. The stakes are too high for pursuing self-interest: there is no justification for failing to

share information that can help others. When information about cyberattacks is known at an early stage, other companies can take countermeasures. In business, full participation in all cybercrime investigations should become standard practice, even if this involves some disruption to business processes, and even if it means that some business secrets are revealed to investigators. The latter may seem a bitter pill to swallow, but the alternative is devastating: if you do nothing to address dangerous malicious code, then production may be completely suspended. Or those business secrets could be made available to *everyone*.

Allow me to make one last comment: the (possibly deliberate) misuse of terms such as "cyberwar" and "cyberterrorism" to create fear awakens memories of the 1960s and 1970s, the time of the Cold War. There was deep mutual distrust between the superpowers and a petrifying fear of a first strike. It is quite possible that in a few decades, we will look back on the present and call this "the cold cyberwar." A nice thought, since it would mean that the violence in cyber space won't have escalated into unequivocal conflict.

4.6 Some (Final) Final Thoughts

This is a dangerous and uncertain world, and while the Internet has brought many benefits, it has also brought dangers and disadvantages and made problems that already existed in some form in the physical world much, much worse. I could again mention here many examples of criminal behavior that have been translated to the online world—fraud, criminal damage, bullying, hoaxing, blackmail—but perhaps we should also think about attacks on a less personal level that nevertheless affect us all.

It doesn't seem so long ago that cyberwarfare seemed like the stuff of spy fiction or even science fiction, yet in recent years surveillance or disruption of infrastructure and services has become the subject of high-profile media stories, and speculation about government agencies using information technology as a tool for monitoring and disrupting the activities both of its own citizens, and of others perceived as potential enemies of the status quo, whether they be activist groups or other nation states. And, likewise, of means of disrupting services such as financial markets, and even the way that people think about (and even vote on) current issues.

So we've seen malware distributed with the intent of introducing keyloggers and other surveillance tools on the systems of political activists and/or potential terrorists and/or established politicians; we've seen malware (like BlackEnergy) intended to disrupt power utilities and other SCADA sites (and remember that by "critical infrastructure" we mean not only utilities like power and water but also financial institutions, emergency services, and healthcare); we've even seen reported instances of destructive malware (sometimes posing, like NotPetya, as ransomware). Other examples of ransomware that demands a ransom but tends not to provide decryption in return has, like these other attacks, often been attributed to nation states engaged in some form of cyberespionage.

While the media are always eager to know "whodunnit?", security researchers are generally wary of attributing malware to specific groups and nation states, because

it's sometimes very easy to introduce "false flags" into malicious code, which in any case is frequently shared between groups. Or it may be stolen/leaked—honor among thieves is not a given... Even now, there is no absolute proof of the origins of Stuxnet, for instance. Still, there is little doubt that a high proportion of cyberattacks originate with (or are sponsored by) government agencies.

Sadly, it's not just the sharing of malicious code among criminals and government agencies that contributes to the problem. While security companies have always made a point of not distributing malicious code and binaries, the comprehensive analysis of certain malware by anti-malware researchers (blog articles, white papers, conference papers, and presentations) inside and outside the security industry is monitored carefully by the "bad guys," with a view to improving the quality and effectiveness of their code. While ethical researchers will try not to be more helpful to the creators of APTs (advanced persistent threats) than to other researchers and security product vendors, and some information is only shared privately, it's sometimes not possible to disclose information publicly in the interest of the community as a whole without also enabling the people behind the malcode to address the very issues that the security community needs to know about.

In recent years, we've seen just about every modern country admitting to investing in some kind of military or governmental cyber-force engaged in "defensive" cybersecurity (perhaps in many cases too little, too late). It would be naïve, however, to think that these activities are not accompanied by offensive measures that may even attract significantly greater funding. Nowadays, the population of any country with a significant investment in information technology needs help and advice in its personal computing activities, while the technological infrastructure needs protection from cybercriminals and from hostile nation states. But, given that the IT industry in general has difficulty finding all the security experts it needs, even the wealthiest countries may be experiencing difficulties recruiting the right people. By "right" I mean not only the most technically knowledgeable people but also those best-equipped with knowledge of the social and ethical implications of their work. And in a politically unstable world, who can guarantee that such people will be deployed in roles that will work to the best advantage of the community as a whole?

What Have We Learned?

Wherever there is an Internet-connected device, there is a risk of it being compromised by a cyberattack. This applies to equipment used in industry, for instance, to control production processes and also to less obvious devices such as smart TVs in private households. At the moment, the risk is still relatively small, devices with key computing functionality being considered to be more clearly at risk, but sooner or later we will have to deal with this danger.

Thanks to its general availability, cloud computing can provide outstanding solutions to many problems, as mobile users have their data and applications available at all times. At the same time the cloud is also of great interest to cybercriminals, as it offers many potential victims. Which is why I keep sounding this warning: do not store your data *only* in the cloud, but also keep a local copy on your own computer, and make sure those data are

(continued)

regularly backed up to offline storage. You never know if and when a cloud-hosted service will be brought to its knees by an attack.

Even though you may not be aware of it, there is a real possibility that your PC has already mutated into a zombie used by hacktivists or other cybercriminals for DDoS and other attacks. As already explained, zombies in this sense are PCs that have become compromised due to insufficient protection, for example because there is no security software, or the program is no longer up-to-date. Nowadays, some hardware manufacturers offer free protection with regular updates every few months or even weeks, but as soon as the user has to pay for the service, it is no longer used. However, those who do not have the technical equipment or knowledge to protect themselves—that is, the majority of the population—are not, as a result, adequately protected from possible attacks. A program that updates itself, includes various perfectly integrated components, has proactive detection techniques, and provides professional support and a real help desk is a luxury, but a luxury that everyone should obtain.

Listen closely when cyberwarfare and cyberterrorism are discussed, and don't get infected by the panic that is occasionally spread. Are there dead people? Were buildings destroyed? Or has the damage been limited to a temporary loss of the Internet or the theft of identity data? No matter how long or massive the attacks were, to call them war or terrorism is simply wrong.

In the Words of . . .
Dr. Klaus Brunnstein

CyberWar: The Internet as a gateway for attacks on individuals, businesses, and the State

The reports are piling up: hackers attack companies, governments, and organizations, and they steal information and obtain unauthorized access to important data, as well as blocking computer systems and Internet connections. In addition to continuous bombardment with spam emails, people face massive damage from attacks on passwords and digital bank accounts. Due to illegal access to passwords and Internet accounts such attacks cause significant damage, currently estimated to be in tens of billions. Continuing advances in the networking of important service supply systems means we will see more attacks on so-called "critical infrastructure" such as logistics and traffic control systems, hospitals, and the like.

And all this terrible news is heard despite regular warnings and reminders to home and business users about safety-conscious behavior. This, despite allegedly sophisticated security systems, from antimalware programs devoted to the detection and destruction of malicious software to intruder detection systems, to supposedly unbreakable encryption techniques for securing stored and transmitted data. Moreover, many IT systems manufacturers claim that their

(continued)

countermeasures against such attacks, if not "safe" from the outset, should at least offer protection if used appropriately.

On the causes of today's unsecured IT procedures

So how can it be, despite these allegedly secure systems and protective procedures, that we experience such attacks and damage? The causes are immediately obvious when we look at the evolution of today's IT systems and processes: they're built on top of concepts created for completely different applications and deployments that didn't need secure procedures. Today's IT systems and applications merely seek to limit or resist, as much as possible, the symptoms of inherent IT insecurity, but with inadequate resources.

Here are three examples of how the development of today's important IT processes overlooked (or neglected) some IT security concepts that are required today.

First, the concept of a "safe" operating system: the operating system developed at Massachusetts Institute of Technology (MIT) in the 1960s contained several important security concepts, including the concept of guard rings in the "secure kernel". However, MULTICS exhibited significant storage and performance issues on the underperforming hardware then available. When Ken Thompson and Dennis Ritchie wanted to implement the program "Space Travel," which was primarily intended to perform arithmetic operations on a PDP-7 that didn't have its own operating system at the time, they developed the foundations of today's widespread UNIX systems and their descendants Linux, macOS and Android. Since the "Space Travel" task didn't address any security requirements, the authors—who by the way also developed the language C, which is unsuitable for programming reliable systems—renounced the security kernel incorporated in the well-known MULTICS concept: the decision can be illustrated with the formula

$$\text{UNIX} = \text{MULTICS} - \text{Security}$$

People attempted to mitigate this in later variants, trying to add security measures in shells around the kernel—a misguided attempt to cure a flaw in the original design. The consequences: almost daily reports of newly discovered vulnerabilities in Linux variants.

Second, the TCP/IP protocols underlying the Internet: Robert Kahn, Vint Cerf, and others developed the Internet Protocol (IP) and Transmission Control Protocol (TCP), so important for today's Internet, with financial contributions from the US Defense Agency ARPA, and particular emphasis was placed on fast connections and rapid transfer of data. However, important security requirements such as the identification of the transmitter and the receiver—as well as the protection of the transmitted data against eavesdropping—played no role in the specifications. This is all the more surprising, as this would have been important for the military applications associated with the financial backers of the program.

(continued)

The lack of reliable transmitter identification and the too-easy access to unprotected data is proving to be a major liability in secure Internet communications.

Third, the hypertext concepts underlying the "World Wide Web": when Tim Berners-Lee, then a physicist at the CERN research center in Geneva, submitted his proposal for "Information Management" in March 1989, he wanted various documents—containing ideas, essays, and comments—to be saved as "knowledge" and to be findable for anyone interested. For these "Hypertext" condensed documents, he developed the description language "HTML" (Hypertext Markup Language) and the communication protocol "HTTP" (Hypertext Transfer Protocol). Since the hypertexts at CERN were accessible to interested parties without any protection conditions—such as requesting an authorization, or protection against unauthorized modification—Berners-Lee likewise imposed no protection requirements in HTML and HTTP. So it is not surprising that the structure that was developed on top of his concept, today's dominant "World Wide Web," lacks intrinsic security requirements, and is a high-risk environment subject to numerous attacks: even security concepts added later, such as the encrypted variant HTTPS, have little impact on this problem.

The mystery of how the obvious shortcomings of these original concepts could have come about is simply explained: these pioneers developed their concepts for applications where the basic requirements for "securely controllable systems"—identification and authentication of sender and receiver, protection of the transfer procedures against denial of service and other misuse, ensuring the integrity of transmitted and stored data—were not important. On the contrary, the main focus was on simple implementation of the concepts, minimizing the storage and computational requirements (aka performance), and ensuring easy use by non-specialists, so today's problems were inevitable.

On the use of today's unsecured IT procedures

The security deficits of today's information & control systems, and the daily attacks and problems that arise in consequence, suggest the following adage: "You don't have to do everything that's technically possible!" Newer IT systems are characterized by a dangerously slavish devotion to feature creep ad absurdum.

With more than 4 billion Internet users by the beginning of 2018 (according to Internetworldstats.com), it is virtually impossible to introduce new inherently-secure methods and systems (for example, IPv6, the 1998 secure protocol, is still underutilized).

The poor security of transmission protocols is of particular benefit to criminals who use millions of malware-contaminated networked computers (botnets) that are hard to detect, thereby generating high criminal profits.

Many companies have made it their business policy to generate their own added value with large amounts of unprotected data from unsuspecting users, especially by manipulating search engines and so-called "social media."

(continued)

Many business models use insecure methods, to the detriment of traditional industries, as can be observed with Amazon: the business model its founder pursues "mercilessly"—the originally planned name for Amazon was "Relentless"—is to replace booksellers and publishers and even authors with itself as a monopoly.

A completely new dimension of risks and attacks is brought about by the rapidly increasing networking of highly secure systems—such as logistics and energy supply—via the Internet of Things (IoT).

What are the prospects for "secure" IT systems?

Dark though the future seems from today's perspective, with the inevitable and ongoing increase in attacks and accidents, some unpleasant incidents will lead us to a rethink, at least in some areas: in spite of the plans of European governments to network "critical infrastructures," serious accidents and blackouts will force us to decouple. However, the learning process for less critical infrastructures such as "smart cities," "smart homes," and "smart cars" may be longer, with correspondingly unpleasant experiences in store in the meantime for many consumers.

Dr. Klaus Brunnstein was a professor for computer science applications in the Department of Computer Science of the University of Hamburg. His specialties were data protection, IT security, and IT forensics. In 1990 he co-founded the Computer Antivirus Research Organization (CARO). He was a member of the German Gesellschaft für Informatik (Computer Science Society), in particular its specialist "Informatics & Society" group, and from 2002 to 2007 he was the President of the International Federation for Information Processing (IFIP). He passed away in May 2015, to the deep regret of many people in the security industry, as evidenced by comments at http://itsecurity.co.uk/2015/05/professor-klaus-brunnstein

Chapter 5
The Antivirus Companies

There's no denying that it is becoming increasingly difficult to combat cybercrime. The stakes are getting higher, the gangsters are getting more and more professional, and now there are cyberspies, cybersabotage, and threats of cyberwar to contend with. Malware is sprayed out into the world like buckshot.

5.1 The Manufacturer

But the virus hunters don't sleep, either. The manufacturers of anti-malware software are developing more and more professional, efficient, and sophisticated products. A complete list of all products, including their strengths and weaknesses, would be too long here. You can get a pretty good idea of what anti-malware products are available by checking out testing organizations such as those mentioned in Sect. 5.2.5 (Virus Bulletin, AV-TEST, and AV-Comparatives). One of the most important functions of these sites is to test these products, so you can also get some idea of how well they perform. However, product testing is a challenging exercise, and it's by no means a given that a test will give you the most appropriate results for your particular needs. Nonetheless, testing organizations and vendors that are members of the Anti-Malware Testing Standards Organization (AMTSO) are committed to raising the standard of testing across the board, so AMTSO provides a good indication of which testers and which products are worth your time and consideration. There is much more about AMTSO and testing in general later in this chapter.

However, I would not necessarily mean to discourage you from using programs by vendors that are not members of AMTSO, or not tested by testing organizations in AMTSO. Not every good product is included in every test, even by the best testing sites. But the reverse *is* true: if you choose one of the products from the products they test, you can always be reasonably sure that you have not purchased so-called scareware, because testers don't waste time on products that are not real security software. Scareware literally means software that is intended to frighten the user

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_5

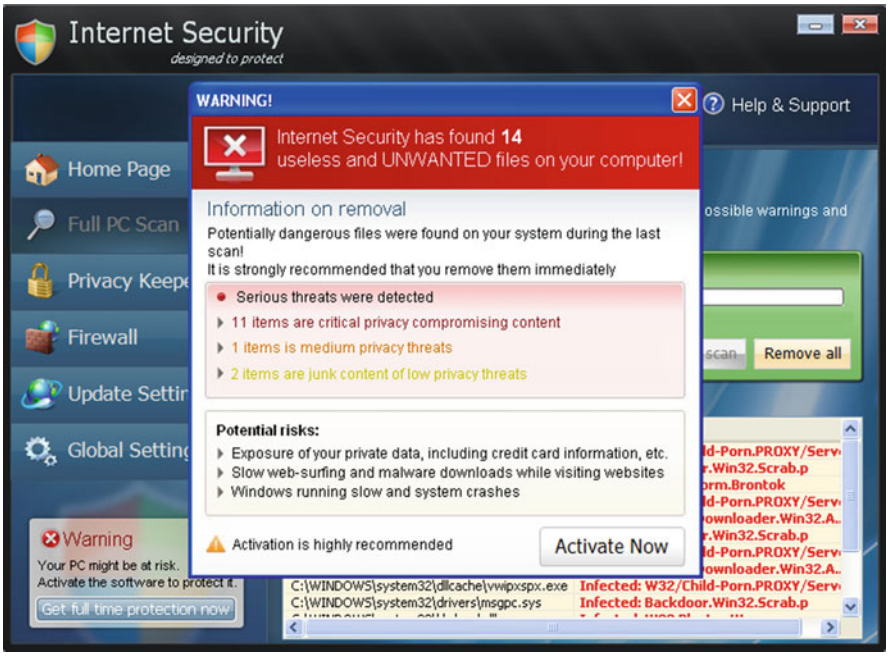


Fig. 5.1 This "scareware" pop-up, which warns of spyware, is nothing more than malicious software

inappropriately, using that fear as a selling point. The best-known examples of this type of FUD (fear, uncertainty, doubt) marketing are the pop-ups displaying a message claiming that the computer user's PC is full of viruses, so he should buy a specific virus scanner to remove them (Fig. 5.1). Scanners marketed in this way usually offer no protection and are likely to contain malicious software.

Purchasing Decisions Made Easy

Granted, some people may feel overwhelmed when choosing a particular antivirus program because the range of options is huge. Make sure that the following functions are offered:

- Real-time (on-access) protection: A kind of "condom" for your computer. This feature is automatically turned on whenever you go online, effectively providing a layer of protection that counters most attacks before they can do any damage to your PC, by monitoring programs and processes as they are executed. If this function is deactivated, there is no longer any "always on" protection. Frequently, so-called "behavior monitoring" is integrated into this function as well as detection of known malware. This type of scanning looks for suspicious behavior, such as when files are being downloaded that can inappropriately access system data. These are usually filtered out as a precautionary measure.

- On-demand scanning: In addition to real-time scanning, most programs offer the option of performing a virus scan of individual files, folders, or media if you explicitly want to: that is, you would normally start this process manually. However, many manufacturers make sure that a complete all-folder virus scan is started automatically if the computer is not used for some time, for example, if the user takes a break so that the processor is near-idle.
- On-demand scanning does much the same as a real-time scanner, but—depending on how (and how effectively) it is implemented—may provide even more protection, in that it may be able to inspect a program or process more thoroughly without introducing a noticeable delay in PC performance when it *is* deployed. Let's take the case where your PC is infected by malware that isn't yet recognized by the on-access scanner. (I.e., it had not yet been included as a detection of known, specific malware at the time the file was downloaded and run.) Even when the real-time scanner is updated so that it *will* now recognize the malware when it attempts to execute, it will not scour your entire hard drive for malware that has already been downloaded. In this case, a virus that has already executed may not be rendered harmless until on-demand scanning is performed, even though the on-access scanner will now pick up known malware (but only when it tries to execute). Scheduled scanning is done automatically by some programs. If your chosen program does not do this, you should do a thorough hard disk scan at least once a week, preferably using some form of automatic scheduling. This is especially true if you are worried about catching malware, as you should be. If you're not worried about malware, you probably don't have anti-malware protection. Unless, maybe, it's a legal or organizational requirement.

  After an on-demand scan, a restart may be required if malicious software has been removed. This feature is especially helpful where the presence of a rootkit or bootkit has been detected, because without restarting you will find it almost impossible get rid of this very annoying type of malware.
- Behavior blocking: Most antivirus programs can recognize viruses and other malicious software based on certain other characteristics (see below). Behavior-blocking technology looks for suspicious behavior typical of a malicious program. Once detected, the suspected malware is isolated unless the user confirms that the file is safe and is allowed to access it.

The Elements of Malware Detection

What is a signature? No writer of malicious software will sign his "artwork," because that would make it far too easy for the people hunting him and his creations. And a signature is not usually part of a filename, as you might think. While in the early days of email worms, for instance, it was possible to perform limited mail-filtering by filename alone; identifying malware by filename was always a limiting and easily bypassed approach to accurate detection,

In a sense, program code resembles human DNA, the carrier of our genetic information. Each of us has unique DNA that can now be completely decrypted. And certain sequences of this DNA are shared with our blood relatives. A virus scanner can store a "DNA strand" of a virus—that is a specific sequence of zeros and

ones—in the database, and the software can detect a single virus using this sequence, i.e., not by using the file name, but by finding a characteristic "signature" within the code. This was the primary detection technique used by early "known virus" scanners but has been augmented and often superseded by more sophisticated techniques over the years (Though the myth that mainstream anti-malware products detect only malware that has been analyzed by its researchers continues to haunt the media, encouraged by some purveyors of alternative technologies, often misleadingly hyped as "next generation").

* * *

In the Words of . . .
David Harley, Former Research Fellow, ESET

Anti-Malware: Technology, Mythology and Detection

Established security vendors nowadays often prefer to avoid using the term 'signature' altogether because it harks back to simplistic detection techniques that are rarely relied upon nowadays. Part of their dislike of the term derives from the way in which so-called next-gen security marketroids often misuse this association with prehistoric simple string scanning to suggest that this is *all* that 'first-generation' scanners do, in order to 'prove' the superiority of their own products.

Ironically, next-gen products often focus on just one or two of the many technical approaches of which longer-established vendors are likely to make fuller use. This doesn't mean that newer products are useless: they may be very effective in some contexts. However, older products may have an advantage over the complete range of existing malware, having a multilayered approach to detection and blocking based on decades of experience.

While an exhaustive essay on the history of malware detection is beyond the scope of this chapter, it's worth an overview of the more common detection techniques in order to dispel some of the confusion generated by misapplied terminology,

At one time, Virus Bulletin, at that time a monthly printed magazine, used to publish lists of hexadecimal sequences that could be used as search strings to detect the presence of malware, and would include such sequences or strings in virus analysis articles, but stopped doing so in 1999 or thereabouts. Most of the back issues of Virus Bulletin can still be found at https://www.virusbulletin.com/virusbulletin/archive/ and are still well worth reading if you're interested in the history of malware.

As malware became more sophisticated, string searching also became more sophisticated. Early scanners learned to incorporate regular expressions, including wildcards, to identify strings even in (early) encrypted and polymorphic viruses. This permitted a fairly basic scanner to detect other members of a particular family of malware: that is, new malware that is generated by a similar process and thus have characteristics that may be identified as

(continued)

resembling a program known to be malicious. This is sometimes known as a generic signature.

However, modern security programs do not rely on signatures in the form of static sequences or 'strings', but use a wide range of much more sophisticated algorithms to identify suspicious characteristics and behavior. There are various forms of code and behavior analysis that not only make it possible to detect malware that hasn't been seen and analyzed before, but also to establish family connections between malware samples, making it easier to identify and categorize new variants from existing families.

Algorithmic detection covers a wide range of approaches. (Technically, searching a file for a static signature is itself an algorithm, if a fairly simplistic one.) The term 'heuristic' is another highly generic term, and has been applied very successfully to malware detection technology since the 1990s. The term as used in anti-malware essentially describes 'rules of thumb' compiled as a sort of expert system and used to evaluate the likelihood that the object being analyzed is malicious. When an extensive and well-founded and well-balanced set of rules is used, the risk of a 'false positive' (where an innocent file is flagged as malicious) is surprisingly low. Of course, a 'false negative', where a malicious program evades detection, is still possible.

Behavioral heuristics are augmented by sandboxing and similar techniques, where the suspicious program is executed in an isolated or virtual environment, so that its behavior can be analyzed without endangering the system. There are variations on this theme that can address specific forms of malware: for example, a program that appears to make one or more copies of itself may be a 'true' virus; a program that makes changes to a series of local could easily be ransomware applying encryption to a victim's data. And so on.

Other (more generic) techniques are also used. Detection of known malware is an example of blacklisting. However, whitelisting is a technique whereby a program known to be safe is not considered to need exhaustive analysis, which improves performance in terms of speed. Whitelisting is most often associated with checking for reputational information held in the cloud, which is likely to be more up to date than information held locally.

Whitelisting is also one of the techniques that can be used to speed up sample analysis in security labs. Such techniques are essential because of the huge volumes of samples that are now generated every day. While so-called next-generation products often make heavy use in their marketing of their use something vaguely described as 'Artificial Intelligence' or 'Machine Learning', AI (or ML) are indeed made use of by many mainstream products in order to reduce the number of samples that need to be analyzed 'by hand'. Perhaps the main point of contention is that mainstream labs see AI not as a magic bullet, but as a way to whittle down the hundreds of thousands of samples seen daily, so that the number of samples that require manual analysis is made manageable.

(continued)

David Harley is an independent security researcher, author and editor who until 2019 held the position of Senior Research Fellow at ESET—a security company with headquarters in Slovakia—with whom he had worked as a consultant since 2006. He previously worked for the UK's National Health Service, where he ran the Threat Assessment Centre, and before that for Imperial Cancer Research Fund (now Cancer Research UK) in a variety of IT security, systems administration and support roles. His academic background is in social sciences and computer science. He has written or co-written a number of books, including 'Viruses Revealed' and 'The AVIEN Malware Defense Guide'. He lives in the UK with his wife and rather a lot of guitars.

* * *

- *Web protection*: All Internet traffic is checked for potentially damaging behavior before it is displayed in the browser.
- *Phishing protection*: Based on cloud technology, websites known to carry fraudulent messages, malware, or masquerading as legitimate sites are automatically blocked and not allowed to be displayed in the browser.
- *Firewall*: Although Microsoft Windows already offers a firewall by default, Internet security packages with their own firewalls and other layers of protection such as intrusion detection are recommended.
- *Exploit protection*: Many successful malicious code infections are based on software vulnerabilities that are actively used by so-called exploits. Good security packages have anti-exploit modules/capabilities that help protect against this danger. Further details on exploits can be found in Chaps. 6 and 8. However, a great deal of malware relies mostly or completely on tricking the user into executing. This is an example of "social engineering" or psychological manipulation of one or many potential victims.

No question, for the layman many of the virus protection programs on the market seem to differ only in minimal ways. But again here the devil is in the details; one should pay attention to special functions and proactive protection technologies. For

example, in its solutions with BankGuard technology, G Data offers automatic protection against so-called "man-in-the-browser" attacks during online banking (Chap. 6). There is a variety of such programs on the market. Consumer protection organizations can help with the selection of such programs. However, they may make the selection easier by narrowing the range of selections to some well-known names that aren't necessarily the most appropriate to the needs of the reader.

5.2 Nonprofit Organizations in the Fight Against Cybercrime

There's one more thing. Happily, the malware hunter community is a very close-knit community whose members freely share information about threats, doing everything in their power to warn the general public about all dangers. This is particularly noticeable at conferences, but also in direct contact between virus/malware hunters. It's striking how many nonprofit organizations have set themselves the goal of fighting cybergangsters by all legitimate means. I would like to introduce you to the most important ones.

5.2.1 CARO

CARO (Computer Antivirus Research Organization) was founded in 1990 by individuals who could be described as powerhouses of the industry, most notably Dr. Alan Solomon (UK)—the developer of the eponymous antivirus program subsequently absorbed by McAfee, Vesselin Bontchev (Sofia), Klaus Brunnstein (Hamburg), Christoph Fischer (Karlsruhe), Friðrik Skúlason (Reykjavik), Morton Swimmer (Hamburg), and Michael Weiner (Vienna)—all well-trained academics—working together intensively in the search for and fight against viruses.

There are now many more members of CARO, but their names are not publicly revealed. It's a fair bet that the most influential figures in the world of anti-malware are among them. However, CARO is keen to be known as a free association of experts—more than that is not revealed, and even the CARO website is noticeably light on content.

This does not mean that CARO has not been actively involved in the fight against viruses and malware. On the contrary! Each member has been very committed to the cause from the very beginning, and nothing has changed since. Most of the current members of CARO occupy leading positions among manufacturers of anti-malware software. As I said, CARO emphasizes informality, with as little bureaucracy as possible. In practice, therefore, all meetings take place behind closed doors, and the results of these meetings are not immediately passed on to the media, as there is a risk that the information could be abused. However, the group continues to take practical steps to encourage the sharing of information between trusted researchers far beyond the walls of the CARO boardroom.

CARO became known in particular through the "Virus Naming Convention" (http://www.caro.org/articles/naming.html), where agreements were made regarding the formal naming of malware. For example, malware should not be named after its creator, or according to its author's wishes, and naming should conform to a fairly complex syntax. Sadly, this convention has proved less effective than hoped, due to a number of factors:

- The shift away from "real" viruses to a wide range of other forms of malware and the impact of the huge increase in volume of malicious programs in recent years.
- The widening range of security vendors who were to some extent involved in the analysis and detection of malware, but did not feel obliged to align with older-established vendors and the practices they had evolved. Even the WildList Organization (Sect. 5.2.4) has, in recent years, moved away from the CARO convention to a method of cataloguing that is more sample-specific.
- The fact that the media tends to prefer "soundbyte" names that are brief and grab the nontechnical reader's attention.

5.2.2 EICAR

However, the members of CARO had a problem. Although they could quietly discuss important things without the walls having ears, how could they share their findings with the whole antivirus community? Or the whole world?

For this reason, CARO decided in 1991 to create another organization whose mission was to disseminate information and insights. Thus EICAR (European Institute for Computer Anti-Virus Research) was founded in Brussels. Most of its workforce also worked for CARO, but there were other members as well, such as myself. EICAR serves primarily as an independent and impartial platform for the exchange of information about the protection of computers, networks, and telephony. One of the ways to promote this exchange of information is the annual(-ish) EICAR conference, listening to expert presentations by security experts or engaging in heated discussions. More information about EICAR can be found at https://www.eicar.org.

* * *

In the Words of . . .
Rainer Fahs, Chairman of EICAR

Back in the early 1990s, when viruses started to work to the disadvantage of business processes in industry, an attempt to unite efforts against this new nuisance resulted in the founding of the European Institute for Computer Anti- Virus Research (EICAR) where most of the contemporary anti-virus (AV) vendors participated in joint efforts against the ever-increasing spreading of viral code.

(continued)

While virus proliferation reached exponential growth rates and new variants appeared in parallel with new computing technologies, only a handful of AV engines have ever been developed, all based on a similar technical approach, which was reactive scanning for known viruses based on signature files.

Around these core AV engines a new industry developed, trying to keep abreast of the ever-increasing number of viruses and the later explosion in Trojan Horses and other malicious code. Newly-appearing malicious codes and their distribution techniques required more subtle technologies (cyclic redundancy checking, behavior checking, and heuristics) in the AV products (AV is used as a synonym for all "anti" products), creating diversity in industry and products but, unfortunately, no standardized technology. The dramatic increase in virus numbers and the ever-increasing speed of infections all across the world in a reactive scanning environment created a problem with sharing of validated samples of viral code. Unfortunately, first discovery and analysis of a new virus created also a business advantage for the vendor of an AV product and thus no centralized sample verification and distribution across national and business boundaries has ever been created. This situation was (and still is) fostering a business driven approach controlled by the AV industry.

However, active participation in the fight against malware and willingness to share information has become essential to the business success of vendors. New developments or advancements in AV technology are not so often the result of collaborative scientific research as of internal industrial, limiting the extent to which detailed information is shared between birds of a feather.

Nonetheless, AV products are on the market and they are doing a fairly good job. Though they differ from each other in minor respects, their quality relies on clever marketing than rather than on verifiable quality control based on scientific foundations. Because of the diversity of the different AV products and the non-standardization of technical approaches, testing of AV products remains a delicate field. It is EICAR's view that testing should be:

- based on agreed standard methodologies, within standardized test environments against clearly-established criteria, making test results less susceptible to inconsistencies of interpretation,
- transparent and repeatable.
- developed and performed by an independent organization with involvement of all stakeholders
- based on scientific research.

From an academic—and EICAR—point of view, it is very unfortunate that industry and the average home user in principle counters the AV problem by simply selecting an AV product from a market where the range of options is driven by marketing and not based on transparent and agreed standards.

(continued)

This will leave the user totally dependent on product vendors. It is EICAR's view that scientific research and applied industrial research must come together to put products on the market that counter actual threats and are developed in a standardized, verifiable way.

Predicated on the actual situation with clandestine surveillance and stealthy access via the manipulation of security products (i.e., "Third Party Access, Bundestrojaner") we believe that trust in security products has been unsustainably damaged.

No transparency in relation to minimum security requirements for IT security products is available to the consumer. EICAR accepted the challenge to provide clarification and to move industry in the direction of defined minimum standards with the noble aim of providing enhanced and sustainable trust in IT Security products. The current EICAR standard addresses anti-malware products and other IT security products (that is, routers, firewalls, and Intrusion Detection).

The EICAR Minimum Standard represents minimal requirements for IT Security Products.

The overall goal is to provide:

- Compliance to Data Protection (Privacy) regulations
- Transparency in communication between the user and the provider
- Affirmation that products are only doing what they are designed for and not manipulated with any hidden functionality.

EICAR will follow its philosophy of uniting efforts and will continue to bring together all disciplines—technical, legal and organizational—to establish an environment where academic research is the foundation for applied research and the development of new AV products, in response to state-of-the-art technology and the ever-changing environment.

(continued)

Rainer Fahs
Chairman of the EICAR Board

Rainer Fahs is a recently retired NATO Security expert. He spent 21 years in NATO organizations, most of the time (17 years) in the Air Command & Control Systems Management Agency (NACMA) in Brussels (BE). As Senior Information Systems Security Engineer he was responsible for the planning, co-ordination and implementation and quality control of computer and communications security measures in the NATO Air Command & Control Systems (ACCS) project and the agencies' networks, as well as for the development and enforcement of a coherent security policy throughout the systems.

As Chairman of the ACCS Security Accreditation Board, he was also responsible for the security accreditation of the system in accordance with NATO security policy. As representative of his agency he was involved in the NATO committees supporting NATO and the participating nations in the development of Computer and Communications Security, later dubbed Information Security (INFOSEC) and now Cybersecurity or Cyberdefense. His interest in INFOSEC and all aspects of malicious code brought him in contact with the European Institute for Computer Anti-virus Research (EICAR) in the early '90s and since 1996 he has been the Chairman of the Board.

Rainer has been married to Patricia, a Scottish lassie, for over 25 years. They have spent a great portion of their lives on international assignments in Germany, Portugal and Belgium and they do enjoy a game of golf together.

* * *

5.2.3 AMTSO

Product tests are not child's play. It must be clear without any doubt that actual malicious software is being used for any detection test. We often observe the following pattern: Trade magazines talk about malware that is not recognized by specific security software, and this is interpreted as a failure on the part of the program under test. Often a more detailed analysis shows that what the testers used was not actually malicious software at all. In another common scenario, a test set includes programs often classified as Possibly Unwanted: for historical reasons, security programs approach these in different ways, so detection of that class of program is not necessarily switched on by default. If the test doesn't allow for differences in configuration and behavior—for example, by installing and testing programs "out of the box" without adjusting configuration to suit the test set—the test audience may get a false impression of the relative capabilities of each product. As is so often the case here, apples are compared with oranges. In another scenario, a product designed for industrial use may be compared to one intended for private users, even though the two should be judged on completely different criteria. For example, a program detected incorrectly as malicious (a "false positive") may be a

much less serious issue for a home user than it is for a commercial or governmental organization.

During a CARO workshop, the idea was born to set up a neutral organization to develop objective and consistent criteria, which sparked the establishment of AMTSO, the Anti-Malware Testing Standards Organization. Its members come mostly from the anti-malware product industry, but testers themselves are represented as well as some independent researchers. With real enthusiasm, these experts cover everything from research to field testing to documenting their experience in countering malware (which feeds into their software). It's not always easy to prevent product testing from being done the wrong way, but following the recommendations hammered out by AMTSO, members can certainly reduce the risk of making silly and damaging errors. Allow me to say that smartphones are not tested by someone driving over them.

AMTSO has created guidelines for conducting field tests that will be readily available to future testers. If industry and business require that testers to stick to these, this will be the only way to ensure that the results have a common basis. That isn't to say that there aren't other valid approaches to testing, but all that experience and discussion shouldn't be discounted. AMTSO has published several guidelines documents [https://www.amtso.org/documents/] addressing various types of test and methodology, but perhaps its most important from the consumer's point of view is the document "Fundamental Principles of Testing." Below is a summary of that document, under the heading "The Nine Commandments for Testers."

* * *

In the Words of . . .
Denis Batchelder, President of AMTSO

As Eddy explains in *Cyberdanger*, picking an appropriate security provider is an important decision for you to make. But to make a good decision, you need trusted sources who present product comparisons fairly and objectively.

Unfortunately, it isn't easy to compare security products, because potential conflicts abound. This is especially true in anti-malware product tests, where both the malware expertise and the most up-to-date malware samples come from the same vendors whose products are being tested. Vendors may pay to be included in a test, and vendors may commission tests against their competitors. Without any testing standards, there is huge potential for testers to produce comparisons that won't be helpful to you.

The Anti-Malware Testing Standards Organization (AMTSO) is an industry trade organization dedicated to making security product tests relevant to you. Over 50 of the largest anti-malware vendors, testers, and other industry players spent 2 years nailing down the AMTSO Testing Protocol Standard, and tests run following the Standard as well as using AMTSO's published

(continued)

guidelines can be trusted by analysts, reporters, and you. You can use the test results to help lead you to better decisions as you choose your security provider.

Eddy has been contributing to AMTSO as a both a member and as one of its Directors since its start in 2008. As you might imagine, discussions of standards and guidelines between industry experts who work for competitors can get quite heated; AMTSO benefits from Eddy's calming presence.

More information about AMTSO can be found at www.amtso.org.

Dennis Batchelder is the current President of the Anti-Malware Testing Standards Organization (AMTSO). He's also the President of AppEsteem Corporation, where he's eradicating unwanted software while helping the software monetization industry thrive. He spent 8 years at Microsoft, where he led their antimalware efforts to protect billions of customers through real-time antimalware products and services, industry partnerships, and continuous analysis of threat intelligence using machine learning and the cloud. Prior to Microsoft, Dennis managed the threat and security information management product lines as a Senior Vice President at Computer Associates, which he joined after founding, running, and selling them a network security product company. Dennis has worked for more than 25 years in the security industry, holding various leadership roles in the US and India. He lives in Seattle, Washington. Dennis is the author of the Soul Identity series of techno-thriller novels.

* * *

The Nine Commandments for Testers

AMTSO has created several elementary guidelines to ensure once and for all that testing of malware programs is consistent, useful, and efficient. Detailed information about these principles can be found at www.amtso.org. Here is my summary, which I would like to share with you:

Principle 1: Testing must not endanger the public.

Tests must not be dangerous. Testers are strongly discouraged from writing new malicious software with which to test anti-malware products.

Principle 2: Testing must be unbiased.

Tests must be conducted neutrally and objectively. Each product should be treated equally, and not in a way that favors a given product unfairly.

Principle 3: Testing should be reasonably open and transparent.

Tests must be transparent so that you can easily determine what has been tested, and how.

Principle 4: The effectiveness and performance of anti-malware products must be measured in a balanced way.

Tests of the effectiveness and efficiency of anti-malware products should provide enough information to avoid misleading the reader. For example, a product that detects and isolates all malicious software but also identifies many harmless files as malware (which is called a "false positive") is not fundamentally better than a product that does not detect all malware but does not create "false positives."

Principle 5: Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent, or invalid.

Test files and test scenarios should correctly, objectively, and comprehensibly be classified as malicious, harmless, or invalid. This is a particular concern where a test is conducted including (or making sole use of) samples provided by a vendor, whether or not that vendor's product is one of the products under test.

Principle 6: Testing methodology must be consistent with the testing purpose.

The testing methodology must be appropriate to the test. The same test criteria are not, for instance, necessarily appropriate both for business solutions and for programs designed for use at home.

Principle 7: The conclusions of a test must be based on the test results.

Often a test is used as a basis for national and international publications, which may cause the starting point for the test to be lost in the various edits of the article. (We have, for instance, seen examples where the same test results were used by different periodicals with startlingly different conclusions). Or it creates completely meaningless and even wrong conclusions if a tester makes assertions about a product's effectiveness that are based on preconceptions rather than on the test data.

Principle 8: Test results should be statistically valid.

Test results must be statistically usable. In other words, test programs must be extensive enough to provide representative results.

Principle 9: Vendors, testers and publishers must have an active contact point for testing related correspondence.

Manufacturers, testers, and IT magazines must be able to contact a person who will handle all correspondence relating to the test. This is a starting point for ensuring that the tester can be held accountable for the accuracy of their testing.

If a test meets all of the above criteria, you can be confident that a product that does well in that test will perform well in the real world, at least in the context of the

test's objective. A product that does well where the test accurately assesses "whole product" effectiveness is a good prospect, but some tests are more specialized and measure only certain aspects of product functionality. Such tests can be very useful indeed, as long as the reader recognizes their limited scope.

AMTSO is also likely to be of direct interest to you, dear reader. We've developed a series of tests for users that can be used to verify that a security program is working properly. I highly recommend that you check these tests out. However, these are not tests of a product's performance in detecting malware: rather, they demonstrate that specific functions within the product are enabled. In other words, they are checks of configuration, not performance. I will come back to this in Chap. 8, "Tips for Single Users."

5.2.4 The WildList

The WildList Organization International, often called WildList or WLO for short, was founded in 1993 by Joe Wells. He wanted to create a directory of all the malware that can be encountered "in the wild," i.e., in real life. The term "in the wild" (sometimes capitalized as "In the Wild" or abbreviated to ItW) has been defined by Paul Ducklin as "spreading as a result of normal day-to-day operations on and between the computer of unsuspecting users." Wells brought experienced people like me to the project, people who deal with malware on a daily basis and are called "*reporters*." Based on our monthly reports, Wells and his team provided a monthly overview of the most commonly detected viruses.

This WildList enjoyed incredible popularity. It didn't take long until some 60–70 people were continuously sending in samples of malicious software to add to the list. Many testers decided which viruses they wanted to test on the basis of the WildList. The reason for this is obvious: if a vendor could neutralize at least the "Top 100 Viruses," it could be proud of itself. Or at least claim to be meeting baseline requirements for demonstrating reasonable competence, which is why WildList testing has survived for so long as a tool for certification testing. Comparative tests aim to determine which products perform best out of a group of tested products, whereas certification testing just determines which products meet an acceptable level of confidence.

Subsequently, the WildList faced strong criticism, not least due to the incredible speed with which viruses were now spreading and the later decline of viruses as a significant proportion of the totality of malware. In the past, a monthly update was more than enough, but with malware mushrooming, it's nowhere near enough. A similar development has also happened with news bulletins: where once you saw the news on television once a day, today you may want to be kept informed right up to the minute about current events, so that you don't miss anything important. With AMTSO this trend is reflected in the so-called real-time threat list, where listed malware is detected immediately after its first appearance, subject to validation of

samples. Incidentally, the name of this list should be taken literally, because AMTSO knows that even a day later is too late for some users.

5.2.5 Test Sites

Virus Bulletin, based in the UK, was possibly the first periodical to focus primarily on malware and is certainly the longest lived publication that does so, though it has ceased to be distributed as a print magazine, becoming fully digital in 2006, and since 2014 only publishes standalone articles on its website, rather than at monthly intervals. But it has always been (and remains) much more than a magazine. While it's still a go-to resource for security-related technical articles, it accurately describes itself as a security information portal and testing and certification body. It's well worth reading its exhaustive reviews of anti-malware products, and it has been running yearly conferences since 1991, an essential highlight of an anti-malware researcher's year (See https://www.virusbulletin.com/).

AV-TEST (https://www.av-test.org/en/), based in Germany, and AV-Comparatives (https://www.av-comparatives.org/), based in Austria, are experienced specialists in product testing, both comparative and certification, and among the best-known names in the field. Like Virus Bulletin (Fig. 5.2), they are prominent members of AMTSO. While some vendors have taken to expressing doubts about the competence and impartiality of third-party testers, I suggest that it's better to look to an experienced testing organization for information on the effectiveness of products than to the vendors behind tested products or to testers who are too closely linked with a specific vendor.

5.2.6 Other Organizations and Services

Some organizations, such as the *Anti-Phishing Working Group* and the *Anti-Spyware Coalition*, played a particularly important role in countering phishing and spyware, at a time when no one knew exactly what devilishly complicated issues needed to be resolved. Today, for most good anti-malware programs, it is standard practice to detect spyware and phishing sites. The *Conficker Working Group* also had to come to terms with a lack of demand for its services, as many manufacturers were able to easily face this threat once the botnet controller ceased to maintain it. The fact that Conficker is still prevalent, however, demonstrates that there is still work to do in persuading computer users to protect their systems properly.

AVIEN (Anti-Virus Information Exchange Network) has meanwhile also lost importance. However, the idea behind this association was excellent: it was a user group, that is, an interest group representing the interests of large client organizations in communication with manufacturers of antivirus software and exchanging best corporate practices in the fight against malware. While vendors were specifically

Fig. 5.2 Screenshot of Virus Bulletin's magazine archive which goes back to 1989

excluded from AVIEN membership, its sister organization *AVIEWS* (Anti-Virus Early Warning System) not only acted as a means of sharing prompt information about malware epidemics, but also as a forum in which vendors and security-proficient customers could share and discuss. In due course AVIEN incorporated AVIEWS and stopped discriminating between customers and vendors. AVIEN launched a number of cooperative projects, the most successful being a couple of online conferences and a major book for Syngress/Elsevier, *The AVIEN Malware Defense Guide for the Enterprise*. However, the group declined in importance as an early warning system as vendors got better at countering fast-burning malware attacks, and after the publication of the book, there was less enthusiasm for another major project. Since the group was totally reliant on volunteers, its mailing list fell gradually into disuse. The AVIEN website survived as a blog largely focused on a number of specialist resources maintained by David Harley. These included pages devoted to news and commentary concerning technical support scams, the Spectre

and Meltdown breaches (which have a far-reaching influence on hardware and software security), "anti-social media," GDPR, the Internet of Things, cryptocurrency and cryptomining, and various aspects of the ransomware problem.

AVAR (Association of Anti-Virus Asia Researchers) continues to play a significant role. The Asian equivalent to EICAR enjoys the same success that EICAR has enjoyed in Europe. As a result, Asian virus hunters do not need to travel to Europe or to the United States for every conference, and it is also the case that malware-related problems in Asia often differ greatly from those in the West. However, the conference remains well-attended by researchers from the United States and from Europe.

The main focus of MAAWG (Messaging Anti-Abuse Working Group) is the fight against spam. This too is nothing new, but the focus has shifted to spam problems in smartphones and mobile phones.

VirusTotal (http://www.virustotal.com) is a site that uses multiple anti-malware products to examine files and URLs for viruses and other malware. Its value to the everyday user lies in its potential for checking suspicious files and links. If such an object is found to be flagged by some of those engines as malicious, there's a good chance it is malicious. While detection by one product may be a false positive, detection by several is much likelier to be correct. However, the fact that no product flags an object as malicious is not a guarantee that it is benign. VirusTotal is often used as a sort of pseudo-testing resource: however, the site itself has itself been anxious to point out that it is entirely unsuitable for assessing the comparative performance of products because it doesn't make use of all the levels of detection and blocking that are used nowadays by mainstream security products. Nevertheless, it is valued by the security industry for a number of reasons, such as an additional means of sharing malicious samples.

There are other sites that offer similar services, but they tend not to have such a good relationship with the security industry: indeed, sites even exist that are intended specifically for the benefit of the bad guys, not the everyday computer user. These latter sites offer a means by which malware authors and distributors can test their programs against a range of products. Such sites do not, of course, have the blessing of security product providers, and in fact not all the multi-scanner sites with *good* intentions are authorized to make use of the engines they employ. Apart from the fact that this isn't exactly honest or legal, it means that they aren't able to cooperate with vendors to ensure that the latest versions and best configurations of specific products are being used. Still, the security industry is not going to complain if malware writers aren't getting the best possible service.☺

One thing malware writers and malware hunters have in common is that they love forums about everything. One particular forum, where about 80 anti-malware experts (including members of CARO and other representatives of the companies to which they are affiliated) regularly exchange views on all sorts of interesting topics from the world of malware, is very popular. Topics include gaps in certain programs, sensational interviews in trade journals, or the retirement or recruitment of top experts in the anti-malware industry. In this way, we virus hunters always have our fingers on the pulse, even if we otherwise move in a quite self-contained world.

What Have We Learned?

Without doubt, there are areas where everyone is on their own. But when it comes to fighting viruses and malware, it's clear that together we're better equipped to tackle (most of) the threats that we face in the digital world. The entire industry communicates company to company, shares its experiences, and unites in its fight against evil.

Anyone who thinks that "Us Against Microsoft" is the right slogan is wrong. Granted, Microsoft does not have the best reputation for the security of its programs. I believe this is unfair, for two reasons. Since Microsoft sells by far the most popular operating system, it is not surprising that Windows systems are the ones most frequently affected by malware. And to make matters worse, its cooperation with the manufacturers of antivirus programs has in the past left much to be desired. Nowadays, though, communication between Microsoft and the specialist security community is much better. Year after year we have a roundtable discussion with Microsoft, and we focus on the programs they will bring to the market in the coming months. We are forming a strong community, prepared to face the malware writers in the years to come.

Good cooperation between the various manufacturers of antimalware technology is the prerequisite for successfully countering new malware, and the more established companies have shared samples in various forums for many years, putting the safety of the community ahead of the competitive advantage that some might think would result from not sharing. In fact, this isn't the case: because no single vendor is likely to pick up all the malware that's around at any one time, and sharing samples means that participating vendors are less likely to miss prevalent malware. So the differences between major vendors are not so much in terms of what they detect, as in the way in which they implement their detection.

And that is precisely why organizations like EICAR, CARO, and AMTSO are indispensable: only by pooling our strengths and expertise can we put the cyberthreat in its place, as we already do more successfully than we are given credit for. No question, we are and remain competitors, and we all have our own trump cards in our hands to convince customers to purchase our own products. But when it comes down to it, we're working together to pursue the same goal: to protect cyberspace as far as possible from risks and dangers.

This common goal brings us together on a regular basis; for example, at different conferences, where frequently real friendships can be made, because it does not matter that we work for different companies. In my close circle of friends I have counted Righard Zwienenberg, a Senior Research Fellow at ESET and an active CARO member, for some years, even though our employers are competitors. We can rely on each other when it comes to product-independent mutual support, and we never lack the opportunity to talk to each other when we meet at conferences or as part of our activities at AMTSO, which to my delight happens regularly.

* * *

Chapter 6
Today's Threats

Now that we have looked closely at the battlefield, we know who the good guys are and who the bad guys are, and we can therefore easily judge what is at stake, and so we can address the most important issue. What is in store for us? What terrible cyberthreats are waiting out there for you, dear reader? What kind of cybercrime will you face, sooner or later?

6.1 Botnets

At the top of the list of the biggest past and future threats are botnets. First of all, because they are still a huge threat to computers. Secondly, because malware can now invade almost any system unnoticed. It's possible that your computer has been part of a botnet for months or even years without your noticing it. Third, there are still many misunderstandings and myths pertaining to this topic.

Let me summarize briefly: if your PC becomes compromised in this way, a so-called bot will be installed on your computer: that is, a program that regularly contacts the server from which it was downloaded. This server then has nothing to do but send commands that will quickly cause the bot on your PC to take some action, along with the bots on countless other infected computers. These actions include the mass generation and forwarding of spam, involvement in DDoS attacks, massive phishing campaigns, and so on. While there have been botnets built and used legitimately, nowadays most botnets are nothing more than a network of bot-infested computers used for (almost exclusively criminal) acts.

Bots are hard to identify because often they aren't installed onto a PC in a single operation. First, a Trojan is inserted into the PC, which hides so well that this malicious program is simply not discovered. It may happen that only after hours or days does the Trojan contact the "mothership," the server that drives the botnet, and then installs the "bot" on the PC.

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_6

And now, briefly, we move on to the biggest misconception of our time: a considerable number of users are still convinced that a computer can only be infected by opening email attachments. In a later chapter I will clear up this misunderstanding.

Basically, even visiting a website can be enough to infect or compromise a PC, by a process that is called a "drive-by download." This term is meant to remind us of an order at a fast-food restaurant—but instead it should remind us of how easy it is to install malware onto a computer. All you have to do is visit a website without paying enough attention, and it will happen before you have time to blink.

"No problem," you may think, "I don't visit suspicious sites and so I'm spared this nonsense." Quite simply, this is unfortunately not the case. Even popular, presumed harmless, legitimate pages can be the cause of harm to a visitor's system if hacked by cybergangsters. For example, if there is a bad banner ad that redirects the unsuspecting surfer to an infected page, or if the infected page pops up by itself. In the recent past, various BBC sites have been abused to circulate malicious software. Even the website of the renowned New York Times was abused for this purpose. It's difficult to say exactly how many pages have been compromised in these ways, as many were cleaned up immediately after it was discovered that malicious code had manipulated visiting systems. One study came to the frightening conclusion that around 30,000 webpages are compromised every day. In other words, a new page is infected every 3 seconds—so we definitely can't say there's no danger.

Should one avoid surfing? Probably that would be an effective solution to our problems on the Internet, but whether that's feasible or desirable is an open question. One small consolation might be that the browsers we use (Internet Explorer, Google Chrome, Firefox, and the like) are basically fairly well-protected, as is much of the third-party software we access that enhances our surfing enjoyment and is used by almost everyone. Just think of Adobe Flash for playing videos or Java for running many games and other mini applications. Basically, these are useful applications, but they too will sooner or later have vulnerabilities that malware writers might use to invade a PC.

Although most software vendors can quickly update their software to close such gaps, these updates must first be installed by the user. I can only offer you this advice: install all updates from a verified, reliable source and restart your PC regularly. If you do not adhere to this golden rule, you run the risk of getting your PC infected, however safe you think you are.

The fact that many users do not heed this simple tip can be attributed to the iPad mentality: Everyone wants to get started immediately—as is possible with tablets—and no one feels like waiting through a long startup process; we don't have the patience to press a button and then find that even after a coffee and a chat with colleagues we are still waiting for the process to complete. That's why countless users simply close the lid of their notebooks or put their computers on standby, because then the startup process is limited to a few seconds.

If you regularly install updates and restart the PC, the danger is still not completely ruled out, but the risk of infection or compromise is much lower. So, basically, as far as exploitation of security vulnerabilities in programs is concerned,

the machine is only susceptible to "zero-day exploits." When attacks use this vector, online criminals exploit the period between the discovery and exploitation by attackers of a software vulnerability, and the development and deployment of a vendor's update. One thing must be clear: There is no 100% protection against viruses and other malicious software and probably never will be. But that *cannot* be a reason not to bother to take steps to reduce one's personal risk to a minimum.

In the Words of. . .
Peter Kruse, Director of the CSIS eCrime Unit and CTO of the CSIS Security Group

When I started analyzing malware back in the late 1990s, there was very little in the way of complex code. You could basically tell what the program was meant to do, by reading the code directly with an ordinary hex editor or even a regular text-editing program. Since then, the threat landscape has changed in threat volume, attack vectors and complexity. The code has generally become a lot more sophisticated and most of the time is wrapped in packers (programs that compress the code until it's run) and crypters (programs that obfuscate or encrypt code) to make it even more annoying and complicated to analyze and detect at runtime. Nowadays, the majority of endpoint developers have to rely on multiple technologies such as signature, heuristics and behavior checking, file integrity checking and HIPS, sandboxing, and traffic filtering as well as additional functionalities on top of all that, like patching 3rd party software, password managers and browser add-ons in order to prevent malicious code from being executed and planted on the system. Despite all these efforts, we have witnessed large-scale disruptions and outbreaks costing businesses millions of dollars and euros.

Apart from these obvious changes, it is striking how much more professional and well-structured the underground economy has become over the past 2–3 years. We are not only dealing with opportunistic lone wolves seeking fame or financial gain, but also with clearly organized groups providing well-crafted and well-managed crime-as-a-service. These groups have a vetting process for new members that is similar to the one we have established in the security industry and matured over decades of networking and data sharing. It is scary to see criminal organizations doing exactly the same and having the same awareness of the importance of good operational trust.

From my point of view, we are dealing with four different types of attackers. We have the script kiddies, who oftentimes have very poor operational security and even expose their identities to researchers. Then we have attackers capable of larger volume attacks, who control thousands of bots at the same time and maintain a stable infrastructure. This group of attackers is by far the largest, with a business structure resembling that of legitimate companies, with different functions and tasks and providing support and SLAs (Service Level Agreements) to other criminals.

(continued)

The third group consists of state-sponsored malware developers performing targeted attacks against different countries and sectors. These operations are financed by a nation state, which adds an additional level to the complexity of the dynamic threat landscape. As this group is funded by and working for a state entity, little can be done from a law enforcement point of view. As long as the criminals do not travel abroad, the chances of getting them imprisoned or otherwise punished for their crimes are low. We have a constantly growing amount of data and intelligence directly related to what many security companies describe as APTs (Advanced Persistent Threats), and the number of these attacks is likely to increase with the growing tendency for nation states to invest in offensive and defensive digital assets to fuel the concept of cyberwarfare.

Last but not least, there are individuals or companies that on a daily basis develop commercial surveillance software and sell bundled licenses to any buyer willing to pay the price. A good example of such a company was "HackingTeam". In the past year, we have witnessed an increase in legitimate and tax-paying companies developing malware in order to infect targets of the buyer's choice. The service is provided for almost all operating systems ranging from Windows through MacOS and Linux to Android and iOS.

To sum up: in my opinion, we have a vast array of challenges ahead of us. Potential attackers within all four groups described above are growing in both numbers and sophistication. The underground economy is maturing and generating new ransomware, crypto malware, RATs (Remote Access Trojans) and data stealers. Several countries have more or less accepted that the use of digital defense and, even worse, digital offensive weapons is now legitimately approved and funded. If you ask me, we are in for a bumpy ride.

Peter Kruse co-founded the Danish IT-security company CSIS in 2003 and currently leads the eCrime department, which provides services mainly aimed at the financial sector. His ability to combine a keen appreciation of business needs and a profound technical understanding of malware has made CSIS a valued partner of clients not only in Scandinavia but also in the rest of Europe.

(continued)

Today, Peter is by far the most quoted IT-security expert in Denmark and considered among the most recognized in Europe. He has a long history of active participation in several of the top closed and vetted IT-security communities and has numerous international connections in the antivirus and banking industries, law enforcement and higher education institutions.

6.2 Ransomware

One of the most significant criminal activities for which botnets are used is, as already mentioned, extortion. Originating from the term ransom, meaning "payment for the release of something or someone held captive," ransomware refers to a kidnapping case on the Internet: a PC or the data it contains is "kidnapped" or, in other words, rendered useless by cybergangsters until the ransom is paid. As already mentioned, the AIDS diskette Trojan of 1989 is considered to be the first ransomware seen worldwide. Granted, it was not the most effective example of ransomware ever, but it worked on the principle of withholding access to a system and its data until a ransom was paid.

Nowadays, there are countless, very professionally constructed examples of ransomware that occasionally hide behind ostensibly legitimate warnings or reprimands from law enforcement agencies. An example of this is the well-known eCops malware.

Figure 6.1 illustrates the inventiveness of criminals—a prime example of extortion. However, this can be seen as a small deviation from the norm, because this is not a "kidnapping" of data. An on-screen message is displayed claiming that the user has done something forbidden and thus violated applicable laws (e.g., a site with pornographic content or the like has been visited) and therefore has to pay a fine as punishment for his offense. And to make the whole thing even more believable, the screen shows nicely imitated logos and background illustrations that really do appear on the official law enforcement websites like the United States Department of Justice. In other countries we find similar fabrications with variations specific to those countries.

The payment of the "fine" is made via voucher services like Ukash, which are available online and at certain retail outlets. For payment to be made, only the number of the voucher needs to be entered. Everything, of course, is completely anonymous. Not a few victims think they have gotten off lightly, because they have some reason to be ashamed. Often, it is claimed that they have visited pornographic or other sites of dubious reputation. Even those who know with complete certainty that they have never visited such sites cannot be sure that their colleagues and friends would believe them to be innocent. So cybercriminals can often assume that their victims will stay silent out of shame or fear of damage to their reputations.

The criminals who developed this particular family of ransomware have now been arrested, but at time of writing the malware and other programs like it are still in circulation. The malcode buzzes around the Internet and is adapted and redistributed

Fig. 6.1 eCops in the United States

by other criminals, which explains why this ghost refuses to be exorcized. That's why there are warnings about this ransomware on various police websites, as well as hints on how to remove it and what you can do to get your money back.

Unfortunately, there is no light at the end of the tunnel. Other ransomware families such as Locky, Petra, and TeslaCrypt encrypt all data and demand bitcoin or other means of virtual payment. Only after receipt of payment is a key sent to the victim, with which the data is decrypted and made usable again. At least, the victims are made to believe that. But once the ransom is paid, there is no guarantee that a key will be transmitted, and in fact it seems that the crooks are becoming less likely to honor any promise that it *will* be. A report (https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf) from early 2018 by CyberEdge including data on ransomware in general stated that out of 1200 survey respondents, 38.7% paid up. However, only 19.1% of those surveyed were able to recover their data subsequently, whereas 19.6% were *not* able to recover data despite paying up.

There is even a related group of malware we sometimes call "wipers": malicious programs that are primarily or solely intended to wipe a victim's hard drive. Sometimes the difference between a wiper and true ransomware is—deliberately or not—hard to establish. It's not clear whether *anyone* who paid for the recovery of data mangled by the malware usually identified as WannaCry or WannaCryptor (Fig. 6.2)—or the "copycat" malware that is sometimes referred to as Fakecry—ever got it back, but the Petya-like NotPetya demanded ransom even though the criminals had no way of effecting recovery for victims who paid up. There have, of course, been logic bombs and destructive malware like Shamoon for decades, but fake ransomware like NotPetya adds insult to injury.

Conclusion: paying for the recovery of your data is no guarantee that they are not already irrevocably lost. Incidentally, this can also apply to data stored in the cloud,

Fig. 6.2 WannaCry malware

such as in Dropbox, Google Drive, or OneDrive. Without regular backups to media that aren't easily accessed by malware, your data will be easy prey and you will be left bereft.

6.3 Social Networks

Facebook, Twitter, Pinterest . . . we now spend a large part of our free time in front of the computer and playing around in social networks. See Eddy Willems' first law, below, which explains exactly why it was no wonder that malware appeared on Facebook, YouTube, and Twitter soon after they became popular.

> **Willems' First Law**
> *The more popular a platform is, the more malicious software will be created for it.*

With malware for social networks, the situation is mostly the same as with email: readers and users (or, in this case, followers and friends) are encouraged to open attachments or click on specific pages. Done and dusted? Too bad, because one or two clicks later, the malware is installed on the PC in question and the misuse of the

data can begin. Again, the bald truth that every PC user should face is that most attacks would never be successful without the users' cooperation! A simple double-click on an email attachment, clicking on a link to a page *you just have to see*—yes, it's made very easy! But often there are early warning signals, to which people should pay attention. For example, if a good friend who normally posts in fluent German suddenly starts posting videos with some highly impersonal commentary in English, then all alarm bells should be ringing straightaway.

Willems' Second Law
$CSP = TF \times MF$

where CSP stands for a cybersecurity problem, TF for the technological factor, and MF for the human factor.

In other words, almost any cybersecurity issue is a direct result of a combination of technological and human factors. Most malware would not stand a chance without naivety, curiosity, or other human weaknesses.

6.4 Portable Media

Malware writers shamelessly exploit human weaknesses such as gullibility and curiosity, but also carelessness. The way the dreaded Conficker worm knew—and still knows—how to spread was relatively simple. If you plugged an infected USB stick into the computer, a screen was displayed as shown in Fig. 6.3.

If you paid careful attention to a screen like this, however, you should not be led astray by this wonderful example of deception. Among the options displayed, a folder can be opened just as we are used to seeing. However, in this case, another option for opening a folder will be displayed. The two differences are the top option is under the heading "*Install or run program*" instead of under "*General options*" as usual and in the top line under "*Open folder to view files*" we see "*Publisher not specified*" where normally there should be "*Using Windows Explorer*."

An experienced user should be aware that something is wrong with the option and should guess that he is probably in danger of installing malicious software. However, because we see windows like this every day and—this is an important factor—the message suggesting malicious software is above the window with the apparent option to open a folder, most users will click on the malicious software because it's convenient and they're not in any case paying attention.

6.5 Attack . . . and This Time on Businesses!

In recent years, cybercriminals' focus has shifted away from the end user and home computer to the systems of entire companies.

* * *

Fig. 6.3 Distribution of the Conficker worm via a USB stick

Companies Under Attack

Aurora—This attack, which we discussed earlier, occurred in the second half of 2009. The main objective of the attack was to gain access to high-tech and security companies working for the military and then to compromise their source code. Victims of this targeted attack included Adobe, Juniper, Google, and Yahoo.

Stuxnet—This Windows computer worm was discovered in July 2010. Since the target was an Iranian nuclear facility, Stuxnet should be included in this list. It caused disruption to the Iranian nuclear program.

German Emissions Trading Authority (DEHSt, Deutsche Emissionshandelsstelle)—This EU emissions allowance authority (which, among other things, oversees related trading) was the victim of phishing attacks in January 2010. The perpetrators sent an email to contact persons outside the organization pretending to be employees of the DEHSt. The hackers showed a sense of humor—admittedly quite idiosyncratic—in their email, where they asked people to log into a fake website to better protect against hacker attacks. With the stolen access data, they were then able to sell various emission allowances worth around €3 million to companies abroad, especially in the Netherlands and the United Kingdom.

RSA—A well-known and highly respected security company that specializes in identity and access management technology. Hackers managed to get information from this company in 2011 without any visible consequences.

(continued)

There was a rumor circulating that a Chinese group might have been behind the attack.

Epsilon—This US-based online marketing firm has millions of email addresses from employees in large and global corporations in its database. In April 2011, hackers stole countless names and email addresses from the database. Among the most famous victims were Citibank, Verizon, and Disney.

Target—Although a breach was announced in 2013, its effects continued into 2014. According to Target, sales in the US declined significantly after data theft of details of over 110 million credit cards became known.

eBay—In the course of a major attack, hackers captured over 145 million private files of active users of the service in 2014—including log-in data, email addresses, and postal addresses.

JPMorgan—Also in 2014, the largest US bank announced data theft affecting 76 million households and 7 million business customers: in other words, 83 million sets of email and address details were stolen.

Home Depot —The US DIY chain announced the theft of 56 million customers' credit cards in 2014, and it turned out later that 53 million email addresses had also been stolen.

Sony—In 2014, hackers gained access to Sony's network and published 47,000 documents with personal information, salaries, and home addresses, including private email traffic between well-known Hollywood celebrities.

A German Steel Producer—A cyberattack in late 2014 on the company network caused massive damage to a blast furnace. Infected emails were used to steal log-in data that allowed access to the control system. This bypassed certain features and meant that the blast furnace could not shut down normally. This attack is one of the few known to have caused damage to an industrial system. The most famous example of such an attack is Stuxnet.

Anthem—In early 2015, more than 80 million social security numbers, email addresses, and home addresses were stolen. According to Bloomberg News sources close to the investigation, this theft had the hallmarks of a state-initiated attack.

If anything, attacks seem to be proliferating. In early 2017 it was claimed that "...there was a monthly average of 500 threatening cyber attacks last year against NATO infrastructure that required intensive intervention from our experts..." (https://phys.org/news/2017-01-nato-sharp-state-backed-cyber-stoltenberg.html#jCp), while the organizers of the Pyeongchang Games in 2018 and the International Olympic Committee declined to comment on the source of the Winter Olympic attacks—"We know the cause of the problem but that kind of issues occurs frequently during the Games. We decided with the IOC we are not going to reveal the source (of the attack)" (https://www.reuters.com/article/us-olympics-2018-cyber/games-organizers-confirm-cyber-attack-wont-reveal-source-idUSKBN1FV036).

* * *

All these attacks had one thing in common: they were believed to be the result of an APT (*advanced persistent threat*, see Chap. 4, Cyber Espionage); only because they had a good deal of perseverance and were able to combine different attack technologies did the hackers succeed ultimately in destroying the defenses of the attacked company.

But their motives were very different. In the case of Stuxnet it was all about sabotage; with the DEHSt hack the underlying motivation was financial. In any case, it is clear that some targets are so valuable to criminals that they are willing to invest months and even years in order to penetrate a company's system.

People who work for a small business may think they will never be confronted with such advanced and intensive attacks. Unfortunately, that's not true: it's not just large corporations that are attacked; even small companies are of interest to cybercriminals for the following four reasons.

First, even a small business can have valuable information, such as email addresses, that allows criminals to gain quick access to big companies.

Second, it doesn't require a sustained, bleeding-edge attack to get a small business into serious trouble. If a hacktivist succeeds in bringing a website or online shop down for a few hours, for example, this can have serious consequences for sales and reputation at a small company. To make matters worse, the victim may only discover the full consequences of a frozen webpage or the installation of malicious software after months or even years.

Third, the number of corporate attacks will continue to grow in the coming years, and this will mean that a wider spread of companies of various sizes is likelier to be targeted. For this reason alone, we should hope that more will be done in terms of protection and security in small- and medium-sized companies as well as the biggest players.

Fourth, even the smallest company is a more rewarding target than a private individual. After all, a business account usually has a higher credit balance, and in most cases, larger transactions are allowed.

6.6 Mobile Targets

What is it they say: everything was easier in the past? You worked in the office all day long, leaving your data and records there for the next working day, and protecting them was quite simple: the IT manager put a large digital moat around the virtual factory walls and positioned a few guards who could deter intruders with digital bows and arrows. In simpler terms, if all the data could be stored centrally, it was much easier to protect it from external attacks.

Nowadays it is perfectly normal to work from home or just to use your notebook on the road. In addition, more and more companies allow their employees to use their own notebooks, tablets, and/or smartphones. At first glance this sounds good, because it is quite simple and allows the individual employee maximum flexibility. But what about protecting the data? There is no way to dig a ditch around any mobile

device. And what can be done if a device is lost? Can it be turned off by remote control? In that case, what happens to the owner's business and private data?

In short, a company's defenses are being completely torn down at the digital level, with all the resulting implications and consequences for security. Just think of all the devices that are constantly logged into the corporate network and thus are connected to the Internet for long periods. And one more thing: most people who work on mobile devices have only one preoccupation—usability: a real nightmare situation for any security expert. For cybercriminals, on the other hand, it's a true gateway to paradise!

Just as with desktop and notebook operating systems, cybercriminals focus primarily on the platform with the largest share of the market—and this is currently Android, as shown in Fig. 6.4.

Conclusion: the consequences are easy to guess, a spectacular increase in mobile malware for Android systems. In 2011, around 1800 mobile malware threats were detected, of which 95% targeted Android devices, and in 2012 this figure was exactly 99% with approximately 100,000 threats. In early 2015, it was subjected to 3,000,000 attacks. As you can see from Fig. 1.2, the number of attacks is increasing dramatically: by the time you read these lines, it may already be several millions more, perhaps six or more new malicious samples each minute.

Things get even more complicated with the many different versions of the Android operating system that are on the market today: some devices run with Version 2.2, others with 3.0, and others with 4.1 and higher (Fig. 6.5) (At the time of writing, the latest version, Pie, is 9.0.)

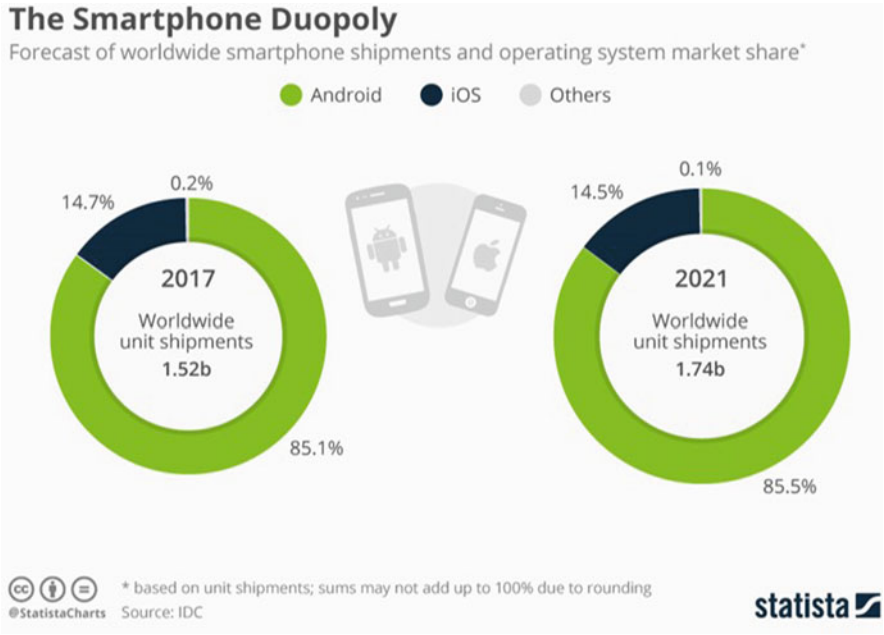


Fig. 6.4 Worldwide sales of smartphones (Statista)

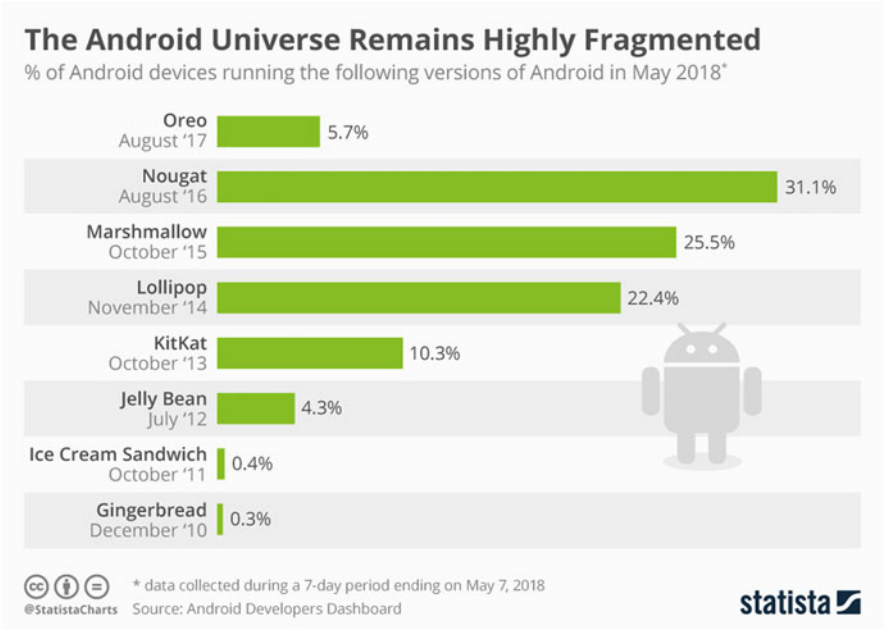


Fig. 6.5 Distribution of various Android versions (Statista)

Due to its numerous versions, Android has experienced tremendous development in terms of security. Unfortunately, there was a lack of consistent implementation of these various security standards in terms of operating system updates. Therefore, the security status of many mobile devices is catastrophically low where individual vendors have failed to apply available patches, and this is shamelessly exploited by the current mobile malicious software.

It's not only the general popularity of mobile devices—especially when running Android—and the well-known security problems that cause me disquiet. Add to this the almost careless handling of smartphones and tablets. The user is the biggest "vulnerability" in any security strategy for PCs, but even more so when it comes to mobile devices. Basically, the protection systems for these platforms are not bad. Every time an app is installed, the device user is explicitly asked for "permission" (the term used on most devices). Typically, however, the user is only too happy to grant this, because after all he wants this app now. I wonder if he would also give permission to have his house burned down if this was necessary to install an app. How else can we explain the fact that there are people who explicitly allow an app on their tablet to automatically send text messages, even though they only want their children to be able to use their tablets for painting?

Have a look at Figs. 6.6 and 6.7—do you notice something common to both?

Both screenshots are similar to the Google Malware Removal Tool, an app developed a few years ago for removing specific malware for Android. In the spirit of better disclosure, one of the two apps really *is* a tool for removing malicious code, while the other one merely claims to be, but is in reality a malicious app in its own

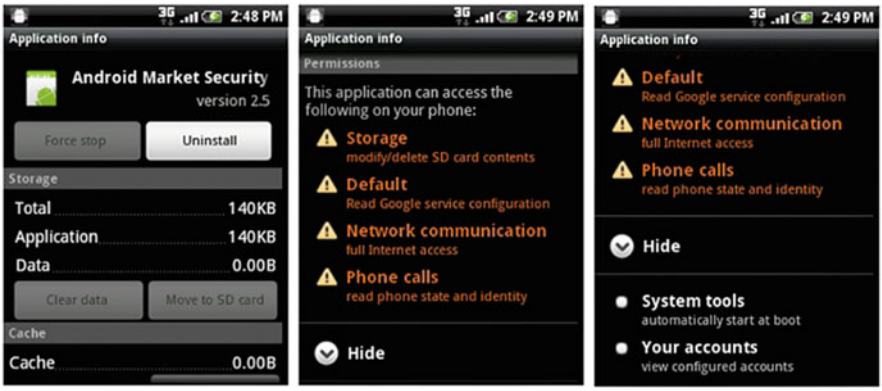


Fig. 6.6 Google Malware Removal Tool, version A

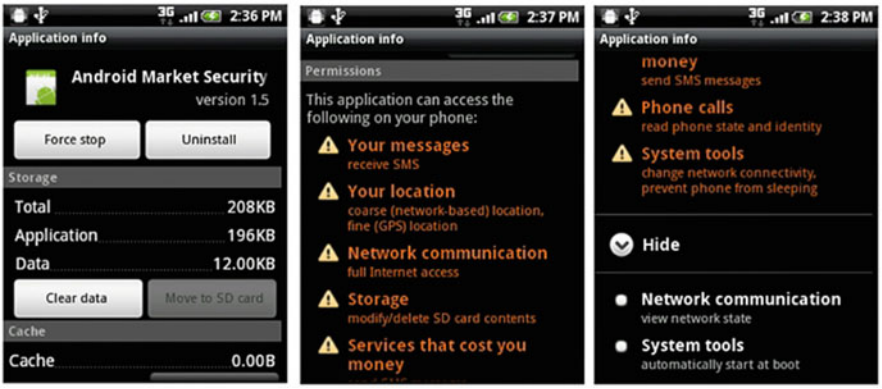


Fig. 6.7 Google Malware Removal Tool, version B

right. Can you tell which screenshot is the malware and give me reasons for your decision? The answer can be found below.

Version B is the malicious software, as can be seen by the types of traffic that the app wants to use. There is the option "send SMS messages" under "services that cost you money." The attentive reader must realize that for such an app to be able to send an SMS is completely superfluous. From this we can conclude that where such an option is included, distrust is absolutely appropriate.

6.7 Online Banking: Beware of the Man-in-the-Browser

There are only a few countries in which online banking is more popular than it is in the Netherlands. In 2012, around 11 million Dutch people used this service, or 79% of all Dutch adults. The Netherlands is number one in the world when it comes to

Internet banking. But more than half of the population also use online banking in Germany, Belgium, the United Kingdom, and France (Fig. 6.8).

Is it really the case that the more popular online banking becomes, the bigger the risk? Apparently, the harm to users of online banking is not (yet) great, but many countries do not disclose the exact amount of known damage. The Netherlands is an exception: in 2012, 10,900 offenses related to online banking were reported. The total damage amounted to 34.8 million €, an average of almost €3200 per case. One can assume similar behavior in other countries, although often no statistics are available. The more popular online banking is in a country, the more interesting it becomes to cybergangsters. You could say that cybercriminals follow the money trail. Luckily for most of their customers, virtually all banks are aware of the risks and have taken appropriate security measures. In most cases, the banks reimburse customers' losses, but, unfortunately, not always. This is handled differently from case to case, bank to bank, and country to country.

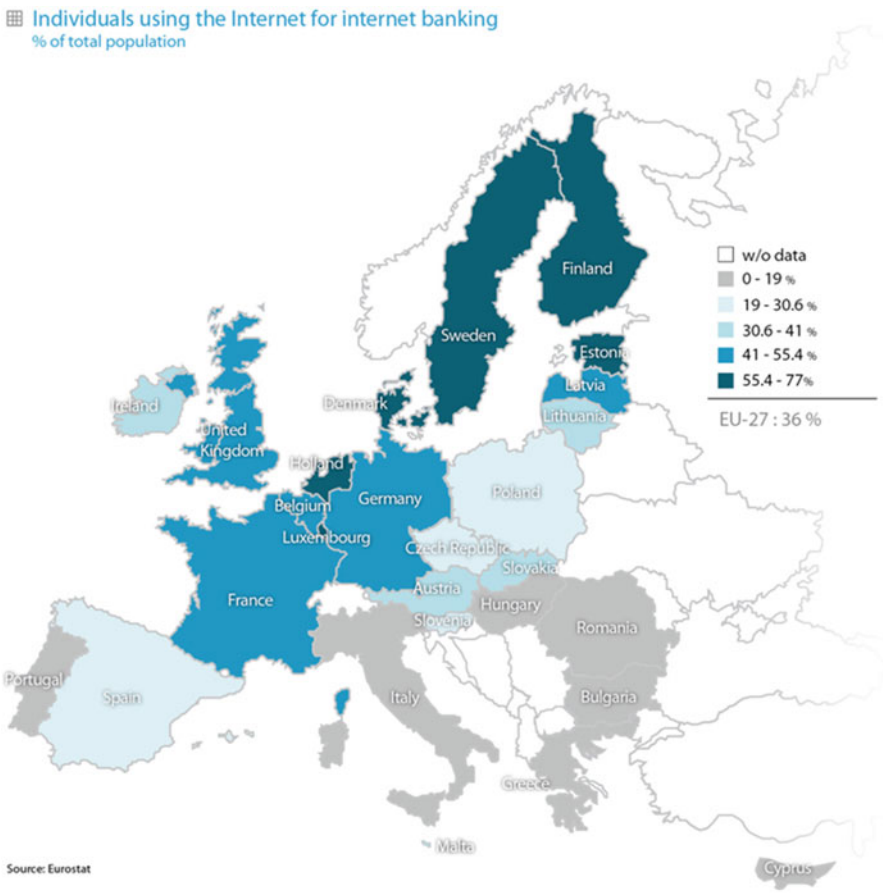


Fig. 6.8 Online banking users in Europe

What dangers lurk in online banking? First of all, as already mentioned, *phishing*. By this we mean that an attacker tries to get the login data of a customer via a phone call or an email that appears to originate from a bank. Phishing is—and will continue to be—a major threat on the Internet, although there has been a slight dip in the numbers of these scams in some years. According to the Anti-Phishing Working Group (APWG), the number of unique phishing reports it received during the third quarter of 2017 was 296,208 (http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf.) A Symantec report stated that in July 2017 one in 1968 messages was a phishing message, the highest it had been in 12 months. Social networks are being abused more and more frequently for the capture of personal data. Luckily there is a clear improvement in the situation, which is likely to be due to better, more up-to-date security measures. But around 66% of all phishing attacks are directed against banks and their customers, because that's where the money is, as Willy Sutton may or may not have said.

I'll bet that all of us have found phishing mails in our mailboxes like those shown in Fig. 6.9a, luring us to websites like the one shown in Fig. 6.9b.

Some are quite professional and hardly distinguishable from real emails from your bank. It is therefore almost inevitable that many people become victims of this trickery.

Fortunately, the data that cybercriminals get from phishing are in many cases no longer enough to allow them to make bank transactions on behalf of their victims. This mitigation comes thanks to dual authentication, where a code is generated by a so-called TAN (Transaction Authentication Number) generator, so the perpetrator cannot directly access the account associated with the data obtained via the email.

What is a TAN generator? Almost all banks in Belgium and the Netherlands—but also in other countries such as Germany—use TAN generators to make registration procedures and banking services more secure. The TAN generator was developed by the Belgian security company Vasco under the name DIGIPASS. The device has a number and keypad, and the EC debit card is inserted into the side. For newer devices, a scanner is used for additional protection, by scanning optical data (a type of barcode). The PIN of the debit card and the code generated by the TAN generator provide access control. Since authentication is based on two factors, this is called double or two-factor authentication (2FA). There are different models of the TAN generator: some have only one button. Depending on the country and bank, older or newer versions (with better security techniques) are used.

A far greater problem is telephone phishing, in which the caller pretends to be a bank employee. The person called is asked to reveal the TAN generated. When calling "your" bank, you should therefore play it safe and offer to call back. Be sure to use a phone number *known* to be genuine, rather than one offered by the caller, and make sure that the phone connection has been broken before dialing the legitimate number (there are ways in which the caller may be able to keep the

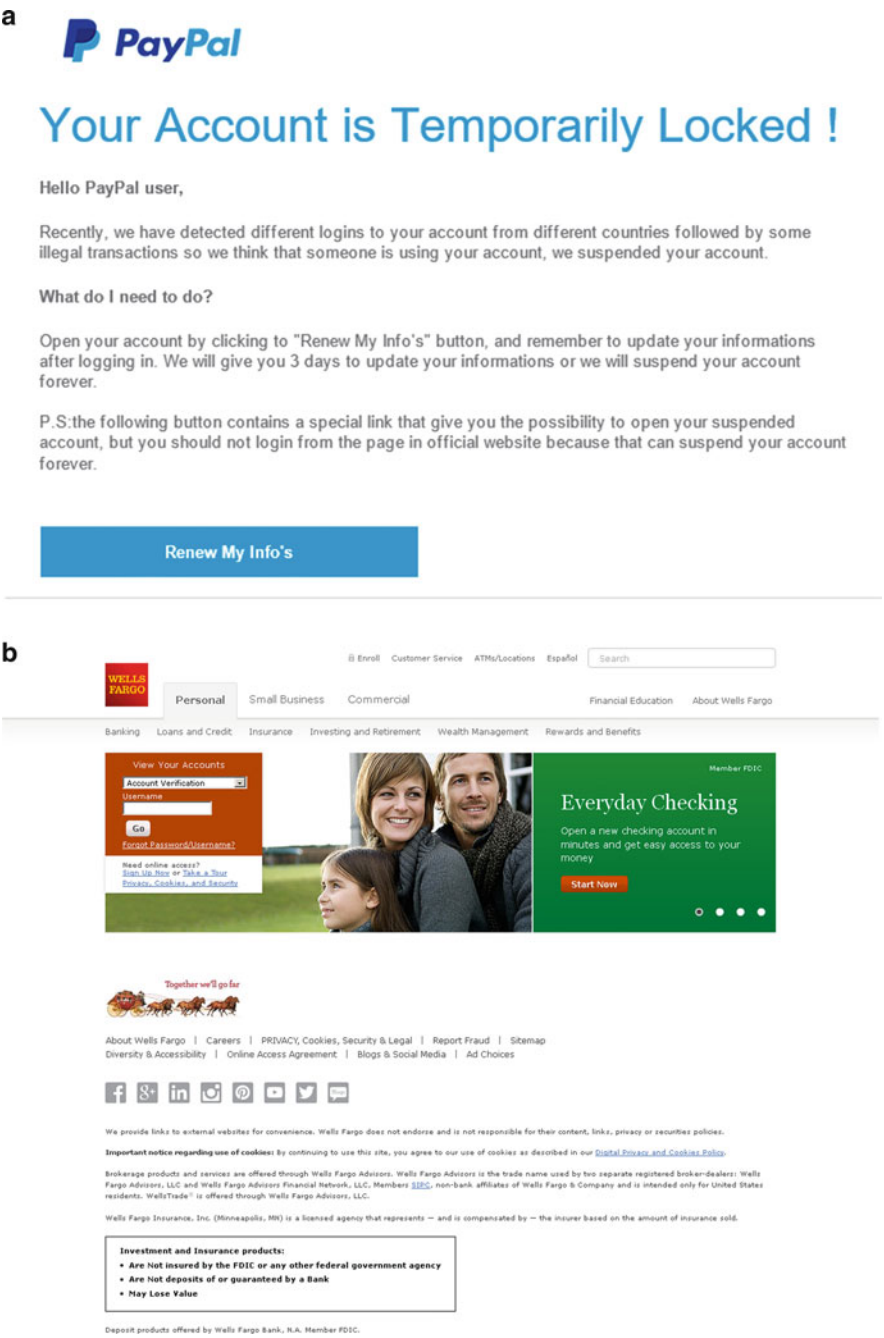


Fig. 6.9 (**a**) Example of data phishing in online banking (fake PayPal email) and (**b**) example of data phishing in online banking (fake Wells Fargo website)

connection alive even after the victim puts the phone down and may even play a counterfeit dial tone so that the victim is fooled into thinking that the connection has been broken). Be sure to get the name of the caller. Maybe this will prevent more damage.

But even "traditional" types of malicious software—such as keyloggers and spyware—are trying to get hold of sensitive information (e.g., online banking credentials) in order to forward them to cybercriminals. This form of malicious software is usually detected and blocked by the relevant security software, provided that the software is up-to-date. Most banks advise their customers on how to protect themselves against such malware. The good news is that due to two-factor authentication, bank fraud is usually prevented, as the data stolen are not enough to allow the scammer to hijack someone else's online banking.

Something banks are reluctant to acknowledge is the third major online banking threat: the banking Trojan. Credit institutions do not like to admit to a problem for which they don't have solutions. At present, banking Trojans are a major problem worldwide. The sole purpose of this malware is to abuse online banking for nefarious purposes. Unfortunately, this fraud cannot always be prevented by two-factor authentication. To make matters worse, Trojans are may be recognized by virus scanners very late in their lifecycle if at all. Actual numbers will follow later in this chapter.

A banking Trojan can enter a system completely unnoticed and refresh itself at regular intervals. With this trick, it remains unrecognized and can wait patiently until the customer starts online banking. At that moment, the Trojan starts a "*man-in-the-browser*" attack, which almost always goes unnoticed. What does that mean? As you know, any Web address is either *http* or *https*. The former stands for *hypertext transfer protocol*, i.e., the protocol with which data is sent to and from the relevant page. The latter basically means the same, but the "s" at the end stands for "*secure*," meaning there is a secure connection between the browser and the page to be accessed. The data are transmitted encrypted so that they cannot be read by anyone who gains unauthorized access.

Of course, bank transactions should always run over such encrypted connections. Most users are convinced that online banking is completely secure, due to the two-factor authentication method and the expectation of an encrypted connection. But customers may not realize that the biggest danger is that the data will be intercepted *before* the encrypted connection is made. To achieve this, the malware must access the data as it is input via the keyboard. If this succeeds, the "man-in-the-browser" attack has succeeded (Fig. 6.10).

Once data is entered for a transfer, it is available to the "man-in-the-browser," who then ensures that a *simulated* transaction screen is displayed that is nearly identical to the *legitimate* one with which the customer is familiar. Now, if further transfer data is entered, the "man-in-the-browser" sends another amount to a different account. Note that he does this using the session started by the unsuspecting user. The bank then sends an authentication request, which is intercepted by the "man-in-the-browser" and answered with the data entered by the user. The customer then only needs to give the final approval for the transfer he intends to make, and the scammer's work is done.

Figures 6.11 and 6.12 show schematic representations of a normal transfer.

In this scenario, the transfer is made, and the customer does not suspect that his money has gone somewhere else entirely. Even the bank isn't suspicious: after all, a bank transfer is an everyday business event. And the winner is? No question, the cybercriminal, who gets a lot of money by this means without anyone noticing at the time.

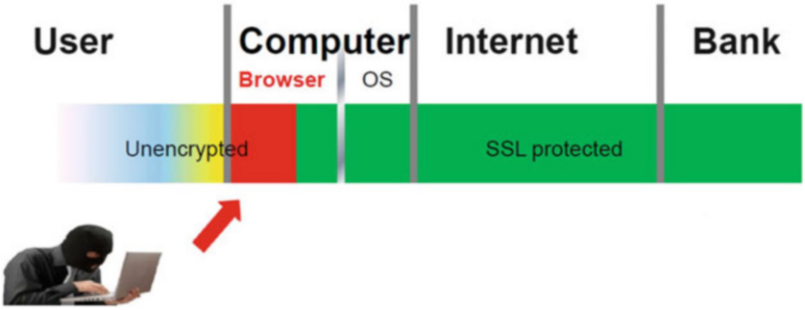


Fig. 6.10 The "man-in-the-browser" malware registers the data input via the keyboard

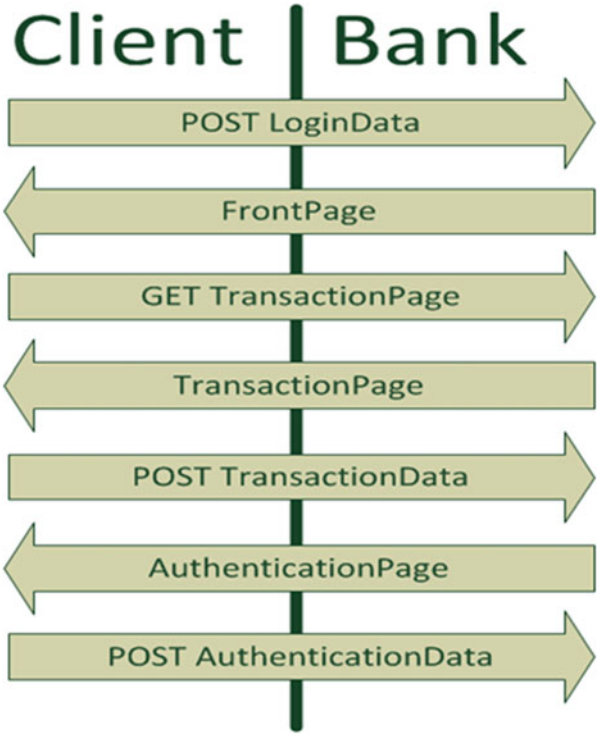


Fig. 6.11 A normal bank transfer via online banking

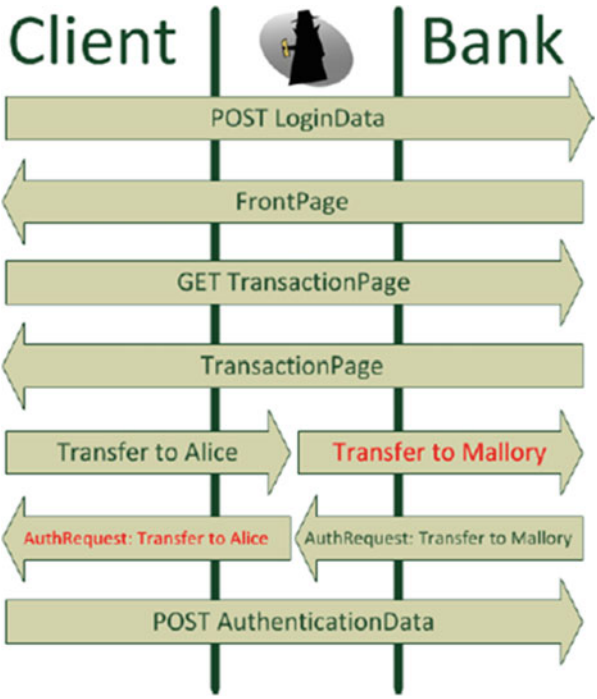


Fig. 6.12 A transfer when a "man-in-the-browser" intervenes

Fortunately for most banks in Germany and Belgium, this problem was solved using a special form of dual authentication. The transaction data (the account number and amount) is converted into a unique code for each transaction. If an account number and/or amount is changed by the "man-in-the-browser," the transaction will not be executed because the code generated for the transfer is incorrect.

In many countries, the code required to complete the transaction is tied to the amount or account number of the transaction in certain banks—this applies usually only to larger amounts.

In countries where two factor authentication is not standard for online banking, the risk is thus disproportionately higher: an SMS code is normally used, which of course can be intercepted by the "man-in-the-browser." Fortunately, most Trojans are detected by an antimalware scanner after some time and made harmless. However, from white papers written by security experts in science and industry, we know that the discovery rate leaves something to be desired. Only 27% of Trojans are detected within 24 hours (Fig. 6.13), and it may take several weeks for all common antivirus programs to detect and eliminate this type of malware.

But then again, new Trojans or variants may have been developed to launch new attacks in the interim. The risk is thus completely real. However, there is software that recognizes banking Trojans based on system information and behavioral analysis rather than the name of the file or a static signature.

Despite two-factor authentication, online banking is unfortunately not completely safe, because there is still the vulnerability introduced by human naivety or error.

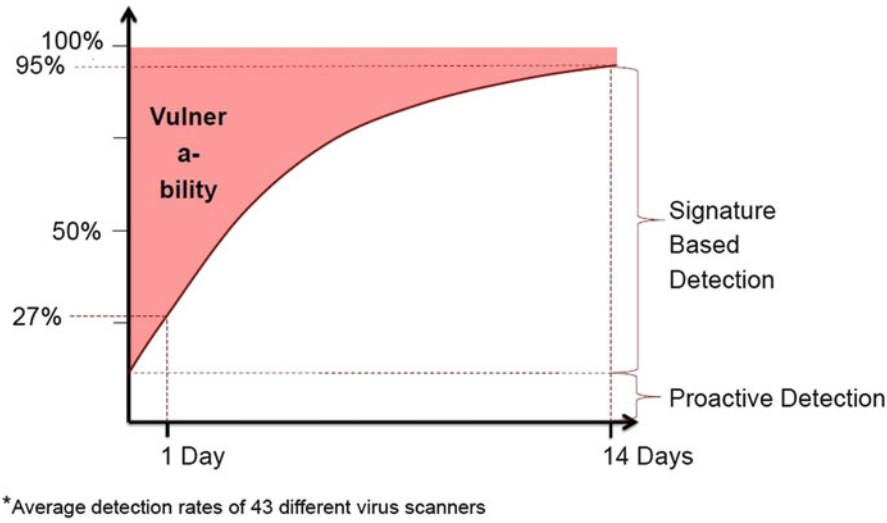


Fig. 6.13 Only 27% of these Trojans are detected within 24 hours, only after another 2 weeks does the proportion reach 95%. (From: Buescher A., Leder F., Siebert T. (2011) Banksafe Information Stealer Detection Inside the Web Browser. In: Sommer R., Balzarotti D., Maier G. (eds) Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, vol 6961. Springer, Berlin, Heidelberg)

There is the "man-in-the-browser" who is trying to pass on a bank account number as the transfer destination that isn't the one entered by the customer but (obviously) that of the cybercriminal or one of his associates. If all the numbers are not checked carefully before a transaction is confirmed, it can happen that the fraudulent action is executed well before a code is generated by the TAN generator. There is some small consolation, though: this method is very labor-intensive for the offender, which in most cases discourages him from taking this approach.

As I said, criminals also have no fear of getting at coveted data via the phone. In this attack, an attempt is being made to elicit transfer data and TANs from the person being called, under the pretext that the software for online banking is temporarily out of order. Victims who are taken in come to harm because there is no protection mechanism that works reliably against a victim's blind and undeserved trust!

6.8 PUPs, PUS, and PUAs

There are unequivocally malicious programs, and then there are programs you probably don't want. These are usually referred to as PUPs (Possibly Unwanted Programs), PUS (Possibly Unwanted Software), or PUAs (Possibly Unwanted Applications). As you might gather from these names, the security industry is not fond of this type of nuisance, for reasons I'll explain shortly. But they're certainly a

problem for the everyday user. An application that (for instance) showers you with advertisements that you don't want, and didn't sign up for, is not just a nuisance but an invasion of privacy, and in many jurisdictions contravenes legislation relating to unauthorized access and unauthorized modification of the victim's devices and systems. There have been instances where adware has imposed such a load on a system that it becomes effectively unusable. Sometimes these are referred to as adware Trojans. Some apps include clearly undesirable functionality, such as restricting the ability of the device/computer user to access *any* sites but the ones considered advantageous to the advertiser, or are associated with unequivocally malicious functionality such as the distribution of spam and malware.

But it's easy to take action against such clearly inappropriate apps, surely?

Well, no, sadly. Even such an apparently straightforward case presents problems. Anti-malware vendors have often found themselves entangled in threatened lawsuits that gobbled time and other resources even where the legality of the plaintiff's software was highly dubious. And the border between legitimate and unwanted can be paper-thin. A PUA may come equipped with some functionality that might just be considered useful. For example, a case was recently reported of 35 Android apps that appeared to be security apps, but whose primary purpose was to display adware, while the implementation of their "security technology" was so poor as to offer little more than a sense of false security. In one common scenario the PUA installation is required as the trade-off against the installation of another, more desirable program. In such circumstances, the user might not be aware of the intrusive activities of the PUA: even if the app is relatively "honest" about what it does. The description of its functionality is likely to be buried deep in a EULA (End User License Agreement) where few end users will find or notice it. Or they might even be prepared to accept those activities if the other package is considered desirable enough.

Sometimes we're told that a message isn't spam if it's something someone *wants* to receive. Which is probably true, as long as it isn't deceptive, fraudulent, or concealing malicious functionality that that someone wouldn't want if they knew it was there. Similarly, if a PUA has functionality that some people will find desirable, a security company is reluctant to categorize it as malware: instead, many companies categorize it as a PUP (or whatever) and leave it to the end user to decide whether to allow programs so categorized to run. Often, this is an "all or nothing" decision: either you allow your security application to detect and block all PUAs, or you don't.

While this approach has to some extent mitigated the impact of threatened lawsuits from PUA vendors in the past, recently those vendors have been more active in trying to force security vendors to remove their apps from that category. If you're not sure whether your security application is configured to detect PUAs, AMTSO has a page (https://www.amtso.org/feature-settings-check-potentially-unwanted-applications/) that tests that functionality. If your vendor supports the test, you can download a harmless program to see whether it is detected as a PUA or not. If it isn't, PUA detection is not enabled. ESET's Aryeh Goretsky has published a more-than-usually comprehensive document about PUA issues which also addresses

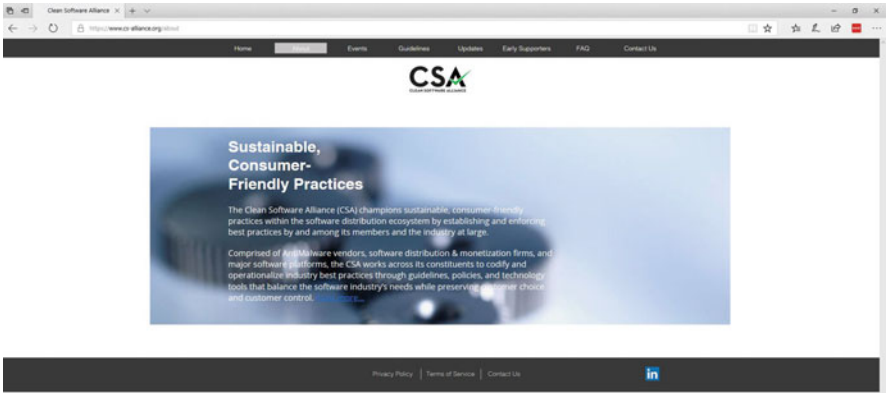


Fig. 6.14 Clean Software Alliance Website screenshot

the issues around what ESET calls potentially unsafe applications (https://www.welivesecurity.com/media_files/white-papers/Problematic-Unloved-Argumentative.pdf). These are legitimate applications which may, however, be misused by cybercriminals. Unfortunately, there is less industry-wide standardization when it comes to handling such apps.

There have been a number of initiatives in recent years that have attempted to address the growing problem of PUAs. That ball is currently in the court of the Clean Software Alliance (https://cleansoftware.net/), which mediates between security vendors, platform providers, and software distributors/monetizers. The Alliance (Fig. 6.14) has published a guidelines document which addresses such issues as:

- Deceptive versus honest advertising
- Transparent installation processes
- Transparency of functionality
- The need for a straightforward deinstallation process

6.9 Cryptocurrency and Cryptojacking: Virtual Currency and Real Criminals

There is a story transcribed by the Brothers Grimm (but probably far, far older) as *Rumpelstiltskin* (or Rumpelstilzchen) about an imp who helps a miller's daughter by spinning straw into gold. Long before Harry Potter, and even before medieval alchemy, the quest for transmutation of base metals into gold and other noble metals by means of the Philosopher's Stone constantly recurs in the search for philosophical and scientific knowledge. The scientific method and the goals of the scientist may have changed, but the search for money for nothing (or at any rate for something of

comparatively little intrinsic value) continues. Nowadays, the Philosopher's Stone has been replaced by the magic blockchain and the rise of the cryptocurrency, spearheaded in 2009 by Bitcoin.

Cryptocurrencies have attracted much enthusiasm of the "you need to get involved with this" variety and considerable skepticism, with some comparing cryptocurrency mania to Ponzi schemes, pyramid schemes, and the South Sea Bubble. A cryptocurrency has several distinctive features.

- Unlike some other forms of digital currency, it isn't just a token or representation of an existing physical currency, but a currency in its own right that exists as a digital object rather than as a physical entity such as gold. Another way of putting it is that Bitcoin and its peers are "fiduciary": they have no value in themselves but derive value because there is agreement between their users that they are acceptable as a means of carrying out a transaction.
- The file is intended to be protected from counterfeiting by the blockchain, which authenticates the ownership of a token and facilitates its use in a transaction.
- Despite its fiduciary nature, a virtual currency can intersect with "real money," and that in itself attracts bad actors (crooks, not thespians!). Hence attacks on virtual worlds and gaming sites, harvesting (for example) tools and weapons, or tokens such as Linden dollars, that can be cashed out in the real(-ish) world. More recently, we have seen the use of Bitcoin and Monero as a means of extracting money from victims of phishing and ransomware, for example. And, of course, they can also be used to buy illegal goods and services (fairly) anonymously.
- It isn't state-backed, so it can't be regulated or diluted/inflated by political activity such as the intervention of some such body as the Federal Reserve, the World Bank, the Bank of England, and so on. It says here. . . So where does the "money" come from? Is it, in fact, spun from straw? Well, no, but cryptomining does derive from the bits and bytes of a virtual transaction, validated by the "work" of "miners." These are not, however, the seven dwarves, though, nor an example of the barter system where goods and services are exchanged directly for other goods and services without the use of tokens/currency. A "miner" is a node that can propose the addition of a transaction to the blockchain, deriving its own authority and value from its ability to solve a mathematical problem, and thereby derives another (growing) problem. Indeed, some now regard this as a bigger problem than ransomware, asserting that cybercrooks are making more money this way.

Where does all the energy and computing power required to feed a cryptominer (Fig. 6.15)—and reward it for its exertions with cryptocurrency—come from? After all, bitcoin mining takes more resources than your laptop can offer (though other cryptocurrencies are less demanding). Sometimes a service may offer you the opportunity to trade some of your machine's cycles for mining, in return for use of that service, as an alternative or in addition to the ads that it serves to you by way of monetization. Some junkware offers you the "opportunity" to contribute in this way without making it clear that it's the miner that profits from your cycles, not you. "Cryptojacking" takes this a step further by stealing your cycles (and, perhaps more

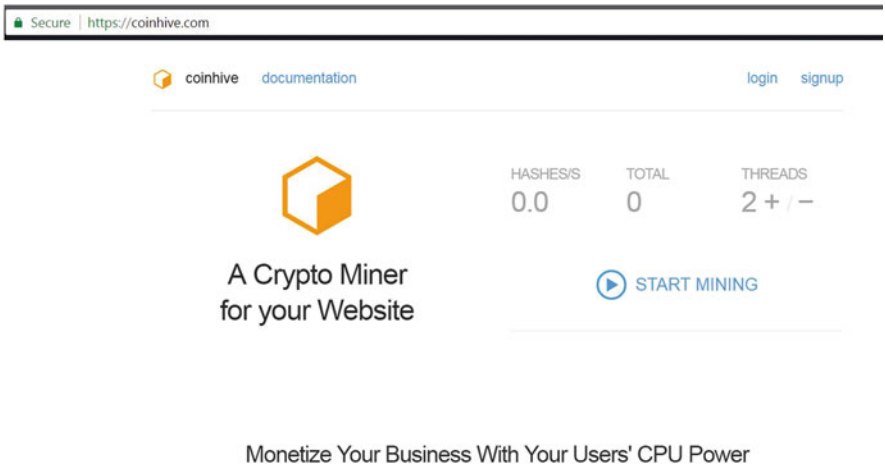


Fig. 6.15 Coinhive cryptominer website screenshot

dramatically—I nearly said shockingly—your electricity) without asking your permission. There are a number of ways in which this might be done, including on-scripts run when you access certain websites and malware installed on your system. Security software may cover both those vectors, but for the former you should consider additional measures such as a reputable script blocker like NoScript or one of those ad blockers that monetizers have been learning to loathe.

If you want a comprehensive explanation of how cryptocurrencies and the blockchain are supposed to work, I recommend Princeton University's *Bitcoin and Cryptocurrency Technologies by* Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, though it's a long read and not particularly cheap (And, ironically, you can't buy it with bitcoin). This four-page primer is rather less daunting: (https://www.cs.princeton.edu/courses/archive/fall14/cos109/bitcoin.primer.pdf.)

Andy Greenberg's 2013 summary for Forbes is still a reasonable encapsulation, taking in the essential points about Bitcoin in particular: (https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#15f17ac353ee).

* * *

What Did We Learn?
If your bank contacts you because of an (alleged) problem with the software for your online banking, you should insist on calling that employee back on a known legitimate number. Only then can you be sure that you are connected to the right contact person. As a rule, you should know the name and extension of your advisor.

(continued)

You want to load an app but find that it requires approval to take inappropriate and intrusive action? Trust your gut feeling, and do without this app instead!

When you connect a USB stick or other external storage device to your PC, first check that the "open folder" message is actually from Windows Explorer and not from an unknown vendor.

Always shut down your PC before you leave your office, even if that means you need a little more time in the morning before you can start work. Regular updating of programs such as Adobe Reader or Java is a must, because vulnerabilities in these commonly used and commonly attacked programs are very dangerous.

There's a demand for payment of a fine in your inbox, because you allegedly visited a porn site or some other illegal site? This should elicit only a weary smile, because that's probably the only fine you need to pay under such circumstances. If you wish, you can contact the police, and perhaps they can make use of your information and stop these crooks.

* * *

Chapter 7
Malware Myths

If this book was an elaborate banquet, we would now have reached a point between courses where we can enjoy a small and easily digested snack that gives us the best possible preparation for all the courses still to come. I am devoting this chapter to identifying the most common malware-related misconceptions and will explain why they belong to the world of "myths and fables." You'll be amazed at how many myths have arisen around the topic of malware.

Several years ago, my employer, G Data, conducted a large-scale survey with 16,000 participants from 11 countries (The Netherlands, Belgium, Germany, Switzerland, Austria, the United Kingdom, Russia, Spain, Italy, Poland, and the United States), in order to find out how well Internet users understand potential dangers. The first ten myths examined here were drawn from the results of that investigation.

7.1 Myth 1: If I Do Not Notice Anything Suspicious on My Computer, It Is Not Infected

G Data's researchers found it hard to believe what came out of this study. A staggering 93% of all participants believed that this first myth was factual! In other words, the misconception stubbornly persists that a PC is OK unless there is some conspicuous and unexpected visual or auditory effect. There have, in fact, been times when malicious software was mostly aimed at making a splash and attracting attention (though even in those early days, some of the most damaging malware was designed to work invisibly). That was the time when most wannabe hackers were script kiddies who stepped onto the stage with only one thing in mind: seeing and being seen, and by as large an audience as possible.

Nonetheless, since you've read my book up to this point, you already know that nowadays cybercriminals are working very hard to ensure that a computer they have infiltrated doesn't show signs of being compromised. When malware is installed

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_7

onto a PC, it does not necessarily mean that screens start to flicker or life-sized skulls are displayed, whatever Hollywood so often tries to tell us. The longer malware goes undetected, the more useful it is to the criminals who can continue to use it (for instance) as part of a botnet. As part of such a network, there are lots of "useful" tasks a PC can perform: send spam, assist in industrial espionage, launch a DDoS attack. . . Without a doubt, delegating such tasks to a network of compromised PCs saves evildoers a lot of work.

7.2 Myth 2: There Is Absolutely No Need for Expensive Security Software. There Are Free Programs That Are At Least as Good!

This is another misconception that we see time and time again: 83% of the survey population believed this statement to be correct. But it's a fairy tale! Clearly, you *can* use a free antivirus program instead of a for-fee package: however, to do so safely requires more in-depth knowledge and a willingness and ability to use other technical tools. If a competent antivirus program is carefully matched to a firewall, perhaps the one supplied with the operating system, and combined with other security software, a level of security is possible that is quite comparable to that of a paid-for security suite. However, I'd recommend that you leave this DIY option to the technically savvy minority of "nerds." And even nerds may not know enough to protect themselves adequately: people whose main focus is on other areas of security often overestimate their own understanding of malware.

For most free virus programs, there is also a for-fee and feature-rich counterpart. Can you give me one good reason why manufacturers would do this if the free version provided equally good protection?

At the time of writing, Microsoft are going to some lengths to emphasize the increased detection capabilities of Windows Defender, the utility that replaces the built-in Microsoft Essentials utility in recent Windows versions. And, indeed, independent testing suggests that its functionality is much greater than that of the much earlier product (also called Windows Defender), which detected only adware and spyware. It certainly beats the long-gone Microsoft Antivirus (MSAV), which was infamous for its inability to cope with polymorphic viruses. It seems to hold its own against other free products in detection performance, though it doesn't have the sophistication of most full-blown commercial products. (Nor has it succeeded in driving commercial security software out of business, despite the gloomy prognostications of so many journalists.)

However, those who rely solely on free antivirus protection take significantly greater risks than someone who has paid for sound anti-malware protection. The difference starts with the update cycle: Sometimes, free antivirus programs are updated once a day using a database containing detection algorithms for the most recently discovered malware and in some cases some known vulnerabilities in the operating system and other software, whereas most commercial programs update

their databases every hour or even more frequently. (Though the frequency of updates isn't always a dependable indicator of how good a security program is.) Nevertheless, if the free version of a product takes much longer to receive an update to detect a newly discovered malicious program than the for-fee version, this means that the free version provides an expanded window of opportunity for the cybercriminal and therefore significantly less protection. This is because the nature of the threat is such that by the time an update is received, malware may have already used that expanded window to infiltrate the PC, having had more time to find its way in. (In general, products that don't have a for-fee counterpart are outside the framework of the mainstream security community and don't have the same benefits of cooperation between competing vendors and their research labs.)

Often, free antivirus programs still include little in the way of proactive technologies for fighting malware. Or to put it another way, there is no technology included that enables malicious programs to be detected based on system information, rather than on some sort of detection of specific malicious code. As a result, such security software is less capable of detecting the very latest malware *before* it has been identified by a company's labs so that detection for the specific malware can be incorporated. Multilayered security software is capable of detecting many threats even though the malware has not yet been seen in the research lab. Often, malicious programs don't reach the labs until they're forwarded automatically by security software, having been recognized as exhibiting malicious behavior or characteristics when they first reach a customer's system. For many people who use security software, this is an important difference in functionality between free and for-fee products: What's more, free programs do not provide a helpdesk or, in some cases, any other type of support in case of problems. In some cases, there will be some sort of forum where users of the software can ask for and offer advice, but for obvious reasons such advice will be of variable quality, compared to the advice you would expect from a suitably qualified and knowledgeable member of staff.

Make sure you buy reputable security software, from an official source: otherwise you run the risk of falling for scareware, or worse. Many of these so-called antivirus programs do nothing but install spyware, adware, and other malware and forward data to a third party, without the knowledge or permission of the system's owner. Many have fallen victim to this kind of scam, which in many cases entail a significant cost. To be on the safe side, buy your anti-malware from a reputable manufacturer: a sound commercial program should detect a wide range of malware, not just viruses, which are only a small proportion of today's malware. Contrary to what some sources claim, modern mainstream "antivirus" software detects a wide range of malware, not just viruses. It also offers several layers of protection, not just simple-minded signature protection, more like a security suite than a simple antivirus program (What's more, good anti-malware programs use far more sophisticated algorithms than the "signatures" of the early 1990s, whatever the media and competitors in other sectors may tell you). In any case, it's well worth any additional cost to invest in a multi-functional security suite that incorporates extra functionality, such as a personal firewall.

7.3 Myth 3: Most Malicious Software Is Sent as an Email Attachment

About 54% of the survey respondents were still locked into this conviction. They believe that a PC is predominantly infected or otherwise compromised by malicious email. It's hard to believe that this myth persists so stubbornly, because email attachments are really responsible for only a small percentage of all infections nowadays. It's more often the case that a malicious email message contains a link to another page (or a series of redirections to other pages) ending up where the malware is already lying in wait. That's right, we are talking about a drive-by download, such as you already met in Chap. 6.

Social networks are responsible for a persistent deluge of infections and other security breaches. Every fan of Facebook and Friends is likely to have seen the links that point to a video seemingly sent by a friend and accompanied by terse comments, mostly in English, urging you to "*Check this out!*" or telling you that "*You gotta see this!*" And this scam seems to work all too well. The study also raised questions about how respondents deal with social networking sites. Forty-six percent of respondents said they had never visited unknown sites, while 35% would only click on links sent by their friends. At least 19% admitted to clicking without hesitation on all links that are sent to them via social networks. The younger generation is particularly likely to do this without any hesitation, while women think longer and more carefully than men before clicking. The conclusion? The average user easily falls victim to abuse of social networks.

7.4 Myth 4: My PC or Network Cannot Be Harmed by My Visiting a Website, If I Don't Download Anything

Do you see it as remotely possible to gently teach the 48% of respondents who happily subscribe to this myth that they are seriously deceiving themselves? I don't, which is why I am pinning my hopes on this statement for its shock effect: *If you* are *surfing the Internet, dear reader, all the data on your PC is potentially exposed the whole time you are online.* Consider all the contents of a website, text, frames, and images. And much more: Flash plug-ins and all those other small applications, needed to watch a video or listen to an audio file, have the sort of access to your system that criminals crave. And all of that happens behind your back, without you having to agree. (Even all those pop-up messages that have accompanied the onset of GDPR often offered the simple choice of "accept all our requirements or do without us. . .") And it's a safe bet that malware is not going to ask for your consent.

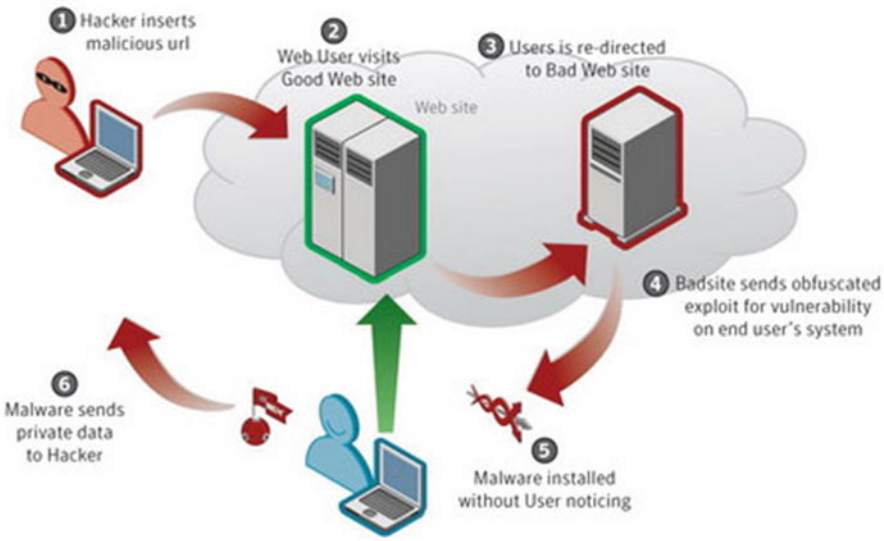


Fig. 7.1 Schematic representation of a drive-by-download

How does a "drive-by download" work? It's beyond all doubt that drive-by downloads currently represent the greatest security risk. The times when you had to click on "Accept" to allow a program or an update to install and expose your system to infection or compromise are definitely well in the past. Nowadays all it takes is to visit a compromised page—hence the term "drive-by"—for harmful code to latch onto your system.

In such cases, download and installation take place in the background, without asking permission and completely unnoticed by the victim. This is only made possible because the initial program is usually very small and thus can be downloaded and installed very quickly. After all, it is only there to contact a server from which the actual malware is downloaded and installed. Most drive-by-downloads are just the first step in an extensive infection process (Fig. 7.1), making it even more difficult to discover what's happening.

Web pages that host such drive-by downloads usually come across as being quite harmless and show a cute photo or video that will hold the viewer's attention long enough for them to stay on the site while the malicious code is installed. Such pages often contain a variety of types of code, so that different vulnerabilities in the browser or other software are sought and exploited from one visit to the next. Popular websites are especially likely to be hacked so as to generate these attacks, because not only do they attract the most visitors, but they are also the sites on which victims are likely to linger longest.

(continued)

Manufacturers of antimalware solutions fight these drive-by downloads on two distinct fronts. On the one hand, they maintain a list of suspicious URLs (web addresses and all links to these URLs are automatically blocked). On the other hand, so-called crawlers (programs that automatically scour the entire Internet) search for the sites from which malware is being spread.
See also Peter Kruse's explanation in the Chap. 6.

7.5 Myth 5: Malware Is Most Commonly Downloaded Through Peer-to-Peer and Torrent Sites

Peer-to-peer (P2P), torrent . . . if these terms mean nothing to you, then it's probably a very good thing, in that you are better protected than those who work day in, day out to gain the benefits of these services. Peer-to-peer networks are networks whose users may make their own files available for download in exchange for data made available by others. This is a cheap way to get tons of software, music, and movies, but mostly illegal, since the files made available are often copyrighted material that the P2P participants are not entitled to share. There is no question that malware writers like to use such platforms to transfer their viruses and Trojans—passed off as, for instance, the current version of Microsoft Office—to the unsuspecting and incautious. Incidentally, the term "torrent site" is often used as a synonym for a peer-to-peer site. But basically, torrent refers to one specific protocol that makes peer-to-peer networking possible. There are others, some of which are used *only* by malware.

The download of data is, therefore, basically a risky endeavor, especially if it involves the illegal sharing of games and other software. Yet it is still not the main source of infection by malware, as was mistakenly assumed by about half of the participants in our study. Compared to the impact of "drive-by downloads," the number of infections on peer-to-peer and torrent sites is relatively low.

7.6 Myth 6: Visiting a Porn Site Is More Likely to Result in Being Attacked by Malware than Looking at a Page About Equestrian Sport

Thirty-seven percent of the participants in the survey felt safe because they did not visit "adult" sites. It's not unreasonable to suppose that a page about equestrian sport puts the visitor at much less risk of infection than does one that advertises "unprotected sex." And yes, it is quite true that malware writers sometimes use sites hosting

erotic content to spread malicious software. This is probably because the victim often stays silent, being ashamed to acknowledge where the infection came from, and this in turn significantly prolongs the life of the malware.

Professionally designed erotic sites, however, are often far better protected than most hobby pages, as they are often programmed and maintained by people who are equipped with enough knowledge to provide adequate safeguarding of web pages. Professional erotic sites are therefore much safer than many sites—such as smaller sports clubs and other recreational sites—which are often quickly created by amateurs, perhaps using templates supplied by vendors who may or may not be well informed in terms of security. In addition, erotic sites are mostly dependent for their cash flow on returning visitors, which makes it even more important for the site owners to protect their site from malware.

Personally, I have come to the conclusion that *any* website, professionally designed and implemented or not, and whether pornographic or about some innocuous topic such as butterflies, nevertheless carries a risk.

Even the pages owned by major news channels have not been spared, and I'm afraid they will not be the only victims. Caution is therefore essential!

7.7 Myth 7: If I Do Not Open an Infected File, It Can't Do Any Harm

First, the good news: just 22% of the people who responded to the survey believed this statement to be true. In fact, it's far from the truth! The times are long gone when a file only got to be opened (or executed) if the user chose to open it. The fact is, a file can be opened or executed without any intervention by the user.

In fact, this *has* to be so in the context of a modern operating system: consider, for example, the automatic updating and patching of security software, system utilities, and so on. But for a long time it has been entirely possible technically to write malware so that both the download and the execution of the relevant files go completely unnoticed. In plain language, this means that this myth will be with us for a while yet, because at first glance it seems that nothing has happened: no file appears to have been downloaded or opened! And that's the way in which the victim can be deceived. . .

7.8 Myth 8: Most Malicious Software Is Distributed via USB Sticks

USB sticks have, in fact, been a frequent source of infection and infestation. The best-known example might be the Conficker worm, which was mainly able to spread initially via USB sticks.

At various security conferences that I have attended, it was established that some PCs belonging to attendees had been infected by USB sticks distributed by the organizers or exhibitors—yes, at *security conferences*, no less! Nevertheless, the danger is relatively low, not least because major vendors have taken steps to reduce the possibility of software being silently and automatically executed from a USB-connected device. In fact, in comparison to drive-by downloads, the risk is almost ridiculously low.

7.9 Myth 9: I Can Save Myself the Expense of Security Software or Hardware, Because I Know My Way Around and Only Visit Safe Websites

This claim, to which 13% of the respondents of the study subscribed, should really be put into the "total nonsense category." First of all, nobody can say absolutely without contradiction which pages are definitely safe and which are not. Secondly, even a safe and secure site can be hacked and infected at some point, even if the compromise is effective only for a few hours. Thirdly, even an otherwise perfectly secure website can carry infected advertising material.

The fact is, there is fraud at all times and everywhere, in private as well as in professional life, and there are people who are working in the background to mislead and misdirect their fellow human beings: sometimes in a very clumsy and obvious way, but sometimes using extremely sophisticated techniques. It would totally disrupt the framework of this book if I were to list all the tricks that are used to lure victims into unhappy situations. In fact, examples of professional malware technique are being combined with each other in increasingly cunning ways. Also, so-called "*social engineering*" plays a part. This is a term applied to various types of psychological trickery used to take unsuspecting victims by surprise: the social engineer relies on the victims' curiosity or susceptibility to sensationalized content, or else on their failing to read the fine print or to think before clicking. Not to mention the ways in which criminals try to misuse data from social networks. I do not think it is possible to live life without ever encountering malware. Not even if you avoid the Internet like the devil avoids holy water, because it's only a matter of time before most of or all our home appliances are connected to the Internet (the so-called Internet of Things or Internet of Everything). And then what?

Only those who protect their computer with reliable security software can enjoy a long-term carefree life on the net. Anyone who considers security software to be superfluous will, in all likelihood, sooner or later have to pay the price for this attitude, which is likely to far exceed the cost of good security technology.

7.10 Myth 10: My PC Holds No Valuable Data—So Why Would Anyone Attack It?

The answer to that is as easy as can be: take another look at the section about the Underground Economy in Chap. 3 in this book (Sect. 3.1).

We can therefore assert that all personal and other data in anyone's computers (and that includes mobile devices!!) constitute information of value to criminals. Almost all data such as email addresses, user IDs, passwords (for online banking, for social networks, for corporate networks and so on), credit card information, and all content from corporate databases, customers, and suppliers can be abused and misused, whether on a small or large scale. This list could probably be continued endlessly.

But even if no such data is located on your own PC, that doesn't mean it can't be used for criminal purposes. It could be used as part of a botnet in order to spread spam and malware, allowing it to earn heaps of money for the criminals from the black economy (Fig. 7.2). Criminals can even rent PCs by the hour that have been compromised by being recruited into a criminal botnet (Fig. 7.3).

Never forget that even *your* PC, however little valuable data you think it holds, can be of enormous value to criminals great and small. Its security must, therefore, be as important to you as its *lack* of security is to a criminal!

7.11 Myth 11: My PC Doesn't Run Windows, So It Is Quite Safe

Windows 95 dominated the PC market for many years, which is why it is not surprising that malware was, over that period, developed almost exclusively for that platform. This is also one reason why Mac owners for years looked down on Windows users. But little malware was developed for the Mac operating system because the number of potential victims was simply too small. However, as the popularity of Apple computers increased, so malware writers grew more interested

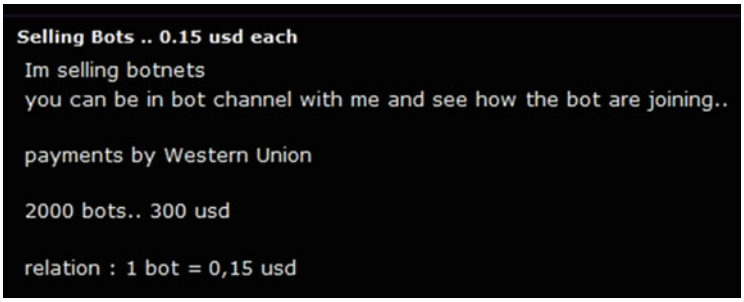


Fig. 7.2 Sale of PCs in botnets

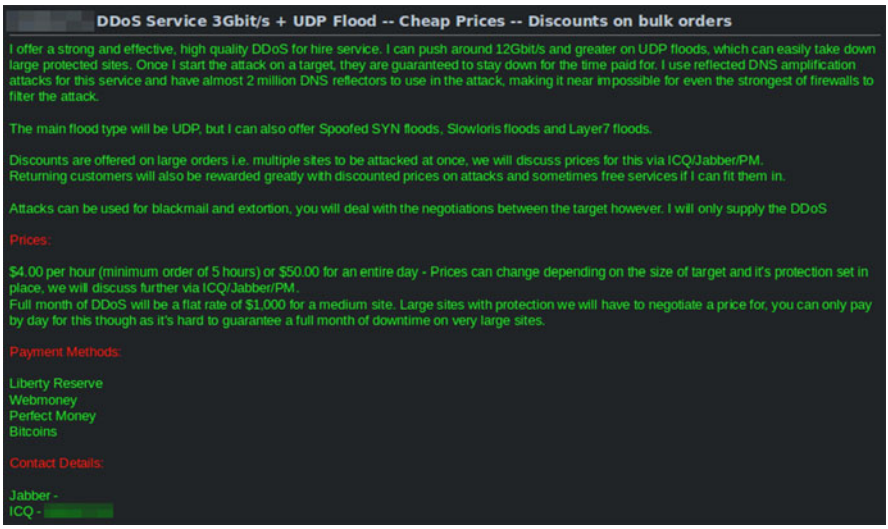


Fig. 7.3 Rental of PCs in botnets

in attacking it. The Flashback Trojan, which succeeded in attacking the systems of more than 800,000 OS X users, is considered the prime example of this increasing interest. While Apple's iOS operating system for phones and other mobile devices has not experienced such a dramatic attack, there is a constant stream of attempts to attack iOS users with smaller-scale threats such as adware.

And while Google has made strenuous attempts to play down the impact of malware on Android, the most popular operating system for smartphones and tablets, it is also considered the most insecure mobile operating system and has to fight more and more against malicious software (see Chap. 1, Sect. 1.5, "The Mobile Generation," and Chap. 6, Sect. 6.6, "Mobile Targets").

7.12 Myth 12: Malware Is Written by Antivirus Vendors

One thing I have to clarify once and for all: all the experts I know fight against viruses and all the other types of malicious software and adhere strictly to some kind of Code of Ethics to which they have committed themselves wholeheartedly. For them, writing and circulating viruses is completely taboo. This also applies when it comes to the recruiting process: anyone who is known ever to have written malware is already filtered out ahead of any interview process.

Writing viruses requires very different talents from those needed for discovering and dealing with them. Although I can only speak for myself, I am sure that my colleagues would agree with me: we are so intensively involved in the fight against malware, that we wouldn't even be able to find time to write malware. At the time of

writing, more than 450,000 new malware samples were being fired at us every day: that's more than one per second! And there are just a few dozen manufacturers who have declared war on malware. We do not need any more enemies to fight against, we are more than fully occupied!

By the way, our moral values have nothing in common with those of malware authors, nothing at all. The purpose of a security company is to combat viruses, while virus writers ... What can I say? You know the answer to that already. Anyway, for that reason alone, we are extremely cautious in the way in which we advertise job openings. If it comes to light that an applicant has played about writing malware, then his chances of joining the industry are out of the window. And this is not just a matter of morality. Just imagine the following scenario: suppose it becomes known that a reputable security company is employing one or more former virus writers? Despite the myth that you have to be some sort of virus writer to detect malware, the chances are that its share price would tumble: not so much through the roof as through the cellar into the bottomless pit. And imagine how much negative publicity competitors would generate from it. (David Harley wrote at some length on these matters for Virus Bulletin here: https://www.virusbulletin.com/virusbulletin/2006/11/i-m-ok-you-re-not-ok.) So, to be absolutely clear, we—the manufacturers of security software—want to have the good guys in our ranks and not the (former) bad guys. Not only do our moral concepts diverge by miles, but we also use very different methods and tools. After all, we just want to analyze malware, not to write it.

Maybe you are now thinking "Yes, but if you'd written even one virus, would it not give you a better understanding of how viruses are constructed?" No way! Malware can be understood and analyzed perfectly well by someone who has never been active in malware creation. Probably the opposite is true: as an outsider, I have a much better understanding of what someone has coded ineptly than someone whose experience is, after all, primarily based on his own malware-authoring methodology. In the end it comes down to the danger of not being able to see the wood for the trees.

It *is* the case that within the security industry in general, there are plenty of poachers turned gamekeepers: sometimes, former hackers can now be found working as consultants and testing the security of a client company's website. Well, you should know that the antivirus community is something of a special case within the larger security industry. There are much stricter moral precepts in play, and—I have to speak plainly here—a good thing too!

I very much hope that I have managed to convince you that—in view of the tsunami of malware that rolls over us day in, day out—we have no time, need or desire to write malware ourselves.

And in my opinion, there is nothing more to say.

Chapter 8
Tips for Consumers: How to Travel Safely on the Information Superhighway

There are many hazards on the Information Superhighway: not just the potholes and tailbacks that hamper our digital communications, but the unwelcome attention of highwaymen and snoopers. Here are some tips and tools to make your Internet journey smoother and safer.

8.1 Invest in an Antivirus Program and Make Sure You Update It Regularly!

Buying a good security program that deals with all kinds of viruses and malware—and making sure it's updated whenever an update is available—is the bare minimum, nuts-and-bolts precaution that every PC user needs to take. But how do you recognize that an antivirus program is *good*? At first glance, this question may sound quite simple, but—believe me—it is anything but straightforward to answer. The functional requirements that any good antivirus software should meet have already been described in detail in Chap. 5, but every manufacturer has its own ways of approaching those requirements. So two comparable programs may focus on completely different aspects of security, and even among experts, there's no absolute conviction as to which are the very best programs. However, you can get a pretty good idea of which manufacturers are reliable by seeing which vendors are members of the Anti-Malware Testing Standards Organization (AMTSO) and checking out the tests conducted by reliable test sites such as Virus Bulletin, AV-Comparatives, and AV-TEST (see the section in Chap. 5 on AMTSO and test sites). And that, dear reader, is a big step toward choosing the right program to suit your needs.

Just as important as purchasing the right program, however, is the regular and frequent updating of detection—and, quite frankly, I cannot offer a 100% recommendation of free antivirus programs in this respect (as discussed in Chap. 7). However, for-fee programs must also be kept up-to-date. In general, the whole

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_8

process runs like this: most users, full of good intentions, acquire an appropriate program, usually with a license for 1 year. When the time comes to renew the license, lots of people skip this very, very important step and settle for the protection offered by Microsoft's built-in security utilities, like Windows Defender, or free antivirus from a third party. Better than nothing, you may be thinking, and I can only agree with that, but if something does not work as it should, most users rely on the extra protection and support that commercial, for-fee software offers and which they probably mistakenly believe to be there in the free product.

By the way, this tip also applies to desktop machines and laptops running MacOS or Linux, even though devotees of these systems are apt to believe in their mythical immunity to malware. And even more to mobile devices, even those that are *not* running Windows. Smartphones, tablets… Do you know anyone who can do without at least one mobile device? And that's why such devices are also of great interest to malware writers. Android is often (quite rightly) compared to Windows because of the sheer volume of malware that targets it. But at least it's possible to get security apps for Android from reputable vendors. While iOS is much less frequently targeted by seriously damaging malware, the iron control exerted by Apple in order to keep malware to a minimum also prevents legitimate security vendors creating apps that might help with those malicious apps that *do* manage to get through.

Now I have one more point to make to you: a good security program whose database is constantly being updated with detection for the latest in malicious software is not a luxury item, but a necessity. So, what are you waiting for?

8.2 You Also Need to Make Sure That Your Operating System and Other Programs Are Updated Regularly

As you know, cybercriminals make much use of currently unknown (0-day or zero-day) vulnerabilities in order to infiltrate the PCs of unsuspecting users. Sometimes it takes a while for the publishers of antivirus programs or the operating system in use on the PC to become aware of such holes in the safety net. In such a case, swift action is needed, and most manufacturers do provide a fix ("*patch*") without delay in order to plug the "leak." But what good are even the best updates if they are not installed? Actually, we all know what needs to be done, but—hand on heart—who hasn't seen a message pop up onscreen prompting them to update a program or the system and reboot at a time that is woefully inconvenient? And then just clicked for the prompt to go away and then forgotten all about it? At the risk of repeating myself, *don't do it!* Why not? Because introducing even a short delay in updating could make the small but important difference between a PC that is infected and a PC that is "clean." Many cybercriminals pay close attention to announcements of new patches and then go searching for the vulnerabilities they're intended to deal with. Unfortunately, this strategy often pays off for them. But you know what you can do about it!

Microsoft, in particular, has gone to some lengths with its latest operating systems to make it more difficult to avoid installing updates as soon as Windows Update has noticed that they're available. I know this can be annoying, but it is safer for the home user. (For businesses, the situation might be more complicated, since the IT team may have a formal update management process in place.)

8.3 As a Matter of Routine, Power Your PC Down Properly

It's a familiar situation. We arrive at the office full of beans and bubbling over with good humor, and the first thing we do is boot up the PC. And then? The PC takes forever to get going.

Most of us have firsthand knowledge of how poorly the average PC compares in terms of startup time to an iPad or other tablet, which is almost immediately ready for use when powered up. Many users lose patience and simply do not want to wait for the usual boot process to finish. There is a commonly used, simple way round this: close the lid of the notebook or laptop, or put your desktop PC or workstation into standby or energy-saving mode when you leave the office. When you come back the next day or even after the lunch break, everything will get going much more quickly and you don't have to sit around waiting for your system to boot up. But let's be clear about this: if you never completely shut down your PC and/or restart, the updates I talked about in the previous tip may not have been installed. If so, your PC remains extremely vulnerable to malware that exploits the vulnerabilities those updates are meant to address. In the same way, if you have security software that doesn't update automatically (though I'd expect any good anti-malware to do so nowadays), you need to make sure it is updated as soon as new updates are available.

Here's an easy way to stay safe and trick your PC into getting on with its wake-up routine without putting you into a rage or a coma. Switch it on and then go and find yourself a cup of coffee. By the time you get back to your workstation, your PC should be well on the way to being fully protected and ready to welcome you to a day's work. If you can't leave your PC to boot (perhaps for reasons of privacy/security), take the coffee in with you: at least you'll have something to do while you wait for the hamster wheel to stop turning.

8.4 Don't Make Your Passwords Easy to Guess

In the late 1980s, a hacker found it easy to crack the password of the then Belgian Prime Minister Martens—"Tindemans1" after a former Prime Minister of Belgium. In the Spring of 2013, the drama was repeated with the cracking of the password of Elio Di Rupo, the Belgian Prime Minister at that time, although one would have thought that the lesson had been learned from the earlier breach and the password better protected. And what can you learn from this miserable example of unlearned

lessons and self-repeating history? Make it as hard as possible for the attackers and let your imagination run wild when creating passwords. Keep away from things like the name or date of birth of your partner or your children, but also avoid personal data like street names or house numbers where you live, even your license plate number, because all this information is relatively easy to get for a moderately knowledgeable hacker. Not even the name of your pet is safe. Paris Hilton had to learn this unhappy lesson when her account was hacked, since the attacker knew—as did the rest of the world—that her Chihuahua was called *Tinkerbell*.

How do you create a password that offers optimal protection? In my opinion, the only safe password is one that meets at least one—and preferably several—of the following criteria:

- It must be at least 12 characters long.
- Ideally, it will contain a colorful mix of numbers, letters and special characters such as punctuation marks, hash symbols, and the like.
- A combination of uppercase and lowercase letters also improves security.
- It is different from the passwords that you use for other accounts, so that if one of your accounts is compromised, it doesn't mean that the cracker can now get into all the others.
- You should also change your passwords regularly, preferably every three months. At that moment, you're sure to think, "Oh, what's the point of that? I only change my password if my account has been cracked or my PC has been hacked." But how do you *know* that this happened? Maybe your PC will only be used to read and capture your emails and Facebook data. And I guarantee that there is no way you can be sure that such a breach has not happened. For this reason you should change all your passwords regularly—without exception!

Quite honestly, it's child's play for a creative hacker to get into all your accounts if you always use the same password. First of all, cybercriminals try their luck on the least protected websites, and if they're successful, try the same credentials on all other interesting accounts (Facebook, Twitter, and, of course, online banking or other financial services). Are you unable to remember more than one password? Then simply create an encrypted file containing all your passwords or use a so-called virtual password safe or password manager, a program that runs invisibly in the background of a computer and can supply you with your password for various services. It may even be able to automatically log in or generate credentials on the fly, and such programs often include a utility for generating a difficult-to-crack password. There's nothing for you to do once your password management system is set up except when you need to add, change, or remove the credentials for a particular service, but you *will* need to remember the password you use to lock and unlock your "safe." Among the best known password managers are LastPass, KeePass, and 1Password. Sometimes you also can find a good one included with your favorite security product.

Some passwords are easier to crack than others. The following is a list that compares the ease with which a common, stereotype password (like "password") can be cracked to the comparative difficulty of a more complex format. (Estimates

taken from a password strength meter page, though its accuracy shouldn't be taken for granted.)

Password	Cracked in . . .
Password	0.0001 seconds
12345678	0.0002 seconds
Pasw00rt	53.9 seconds
Klammeraffe	5 months
Kl @ lways @ ffe	10 months
$ Kl @ lways @ ffe $	895 years

Do you want to know how secure your password is? There are quite a few "password strength meter" sites that offer to check passwords for their effectiveness and resistance to password cracking or guessing, but their effectiveness as a gauge of password strength is at best variable. However, caution should also be exercised here: do not enter a password that you actually use, just a similar one. In this way, you can learn how to come up with a simple but hard-to-crack password. You may also find that when there is—as happens all too often—a major leak of passwords, sites spring up offering to check whether your password is among those leaked. Some of those sites are genuine and well-meant: others are simply looking for a shortcut to your password. Rather than try to guess which is which, it's better to simply assume that your password is compromised and change it as fast as you can.

In the Words of
Luis Corrons, Security Evangelist, Avast

Our adversaries in the cyberworld have changed since the first days of the Internet. Hobbyists—or people who wanted to show off and gain fame—created the majority of viruses in the early '90s. Now, it is the large groups representing organized crime that create today's malware, for financial gain, to the point where they even offer malware as a service, meaning that they provide malicious code, financial incentive and support for other cybercriminals to spread the malware.

While the motives driving hackers have changed over the years, one thing has remained the same: people need to carry out basic security best practices to protect themselves and their data. Unfortunately, not everyone sticks to best practice in security as they mistakenly believe that because they are sitting in front of a screen in the comfort of their own home or office, that they are safe. This false sense of security makes people act recklessly, not realizing that with just a few clicks they can take risks equivalent to behavior in which they wouldn't dare to engage in real life.

The most important step people should take is to install antivirus, whether it be on their mobile, Mac or PC. Antivirus acts as a safety net, protecting even

(continued)

the most carefree users. Updating software should also be a top priority. Regardless of whether it's operating system or application software, users should update all software as soon as updates are made available. Keeping software up-to-date can prevent hackers from exploiting software vulnerabilities, and thus keep hackers from accessing users' systems and data.

One critical security measure that is certainly best practice, but which is often challenging for users, is using strong and unique passwords for each online account and changing them all on a regular basis. Data breaches are not always detected by companies right away, meaning that cybercriminals can get their hands on login credentials without anyone realizing it, making it vital for users to change their passwords regularly. Furthermore, leaked login credentials from data breaches can be misused either by the threat actors who stole them or by cybercriminals who purchase the information from the darknet. Cybercriminals are well aware that many people use the same username and password for more than one account, so the first thing they do after obtaining login credentials is to attempt to access other accounts. Users should create unique, long passwords that contain a mixture of letters, numbers and special characters, one for each of their online accounts. Most users have more than 20 online accounts, making it difficult for them to create and remember strong and unique passwords for each of them. In such a case, a password manager tool is helpful for consumers, as it can generate strong passwords and change them instantly. With a password manager, the user only has to remember one master password.

Cybercriminals excel at deception: they use social engineering techniques to fool users into infecting their own devices or giving away their personal data. A user who has never seen an attack using social engineering is especially at risk of falling into the trap. It is therefore also advisable to stay informed about the latest security threats, as well as following best practice. That doesn't mean getting a master's degree in security, but just reading the news, while following a few of those security companies and cyber-oriented law enforcement agencies that provide advice and give tips on social networks on how to recognize the latest attacks going around: this can help a great deal.

Last but not least, people should remain cautious and alert online, thinking twice before downloading attachments or apps and other programs, and before clicking on links from untrusted sources. The bad guys in today's cyber-world are professionals. They look for the best return on investment when setting up their traps, and they are fully aware that the most vulnerable people are the ones who do not take the most basic precautions.

(continued)

Luis Corrons has been working in the security industry since 1999, specifically in the anti-malware field. In 2018 he signed up with Avast as their Security Evangelist. Previously he was the Technical Director at PandaLabs, the malware research lab at Panda Security. Luis has been always involved in malware investigations, such as the shutdown of the Mariposa botnet, and Operation Oil Tanker. Luis is a top-rated industry speaker, speaking at events like HackInTheBox, APWG (Anti-Phishing Working Group), AVAR (Association of anti-Virus Asia Researchers), Virus Bulletin, and Security BSides. In addition to being Avast's Security Evangelist, Luis is a WildList reporter, a member of the Board of Directors at AMTSO (Anti-Malware Testing Standards Organization) and a member of the Board of Directors at MUTE (Malicious URLs Tracking and Exchange).

8.5 Make Sure You Make Regular Backups

Despite all precautions, you may sooner or later find yourself among the victims of cybercrime. You also need to be prepared for the worst-case scenario in which your system and/or data sustain damage.

So here's the next tip for you: back up your data frequently—daily, if possible. No doubt in the evening you are exhausted after a hard day's work, and looking forward to an evening's relaxation: is that really the best time to launch a backup? Yes, absolutely, because the very idea that all of your data might fall victim overnight to a criminal's cyberattack should send shivers down your spine, and with good reason. Effective data backups do not require much effort—there are many tools available that carry out backups automatically, as soon as the computer's shutdown process is initiated. This brings us full circle with tip 8.3, because this only works if the PC is actually shut down and not just put into standby mode.

One more thing: Do not rely exclusively on cloud services for your backups, because these too can be hacked! (This even applies to attacks such as corruption of data by ransomware: some such malware goes to some lengths to encrypt data in the cloud at the same time as it encrypts it on the machine under attack.)

Creating your backups at home is a good place to start. It is even better if you also provide for an "off-site backup." For example, copying all your photos from your computer's hard disk to an external hard drive is a good beginning, but maybe you could also copy them to your parents' computer, or that of your parents-in-law. In that way, you kill two birds with one stone, because the happy grandparents will be happy to have access to all those photos of their grandchildren.

But there are other options. There are hard drives containing several terabytes of storage space that you can take anywhere. It is also advisable to encrypt your backups, because if, despite all the care you've taken, your data fall into the hands of a third party, that party will not be able to read them. This tip applies, by the way, to *all* secure content. From the incident with PRISM (Chap. 4) we finally learned that you never know *who* is peeping over your shoulder.

8.6 Think Carefully About Where You Leave Your Personal Details on the Web

Every day we are inundated by a veritable tidal wave of contests and the tantalizing prospect of great prizes, such as cruises, boxes of high-priced wines, cars, and more. Participation is a breeze: just enter your own email address and answer two easy questions. I do not know if you are one of the lucky ones who have won some cruise or other, but I guess that most of my readers do not belong to this illustrious circle. Let's be clear on one thing, though. When you submit your email address, as is always required when entering such a competition, there's one thing you always win: Lots of spam—month after month and day after day.

Do you want to take part in some such competition despite my advice? Then I suggest the following: acquire a second email address and use it just for contests. In this way you can avoid having your "real" mailbox gradually silted up with junk mail. And check the other mailbox to see if you can start packing your bags ready for that cruise.

8.7 On Principle, Don't Respond to Spam

The worst thing you can do with spam is to respond to such emails. Most spam has at the bottom of the message a notice telling you that you can unsubscribe from the distributor's mailing list via the link included there. Of course, you can also contact the sender directly with a few choice words (supplemented with numerous

exclamation marks!!!) asking for your email address to be removed from their database, but the bad news is that nine times out ten, all this will make no difference, none at all. Most of the time, all you've achieved is to ensure that the spammer now knows that your email address is being actively used. And as a result, you will most likely find yourself receiving even more spam and then even more as the lists to which you've been added are sold on to other spammers. In addition, it's common for cybercriminals to make it look as though the email address you've confirmed as active is itself sending spam or phishing emails. In other words, such innocent addresses are inserted into the message headers to make it look as if you, the innocent third party, are the sender of the spam. This procedure is called *spoofing*. In the worst case, this takes place by way of an infected PC belonging to an unsuspecting user. But if someone receives spam messages that you didn't send, then that doesn't mean that *your* PC must have been infected or infested with malware. It's perfectly possible that cybercriminals have got your email address from data provided by or stolen from a third party and are now spoofing it for spamming purposes. Note, though, that we're only discussing spam here that you didn't spread or ask for, and of which you are not the author. In the case of legitimate newsletters, things are different: In that case, if you registered your address to receive such newsletters, you can of course, unsubscribe again whenever you choose. This should not be a problem.

To sum up, I can only say that if you acquire a good spam filter of your own and follow the tips above, you should be very well protected from spam.

8.8 A Little Common Sense Goes a Long Way

You will certainly remember that I have already advised you to pay attention to your gut feeling when it comes to security. Ask yourself these basic questions for each email: What is likely to happen, if I answer it? Why am I receiving this email at all? Is there something odd or suspicious about it? Why should (good) friends in my native Belgium suddenly send me English-language Facebook messages? People who don't "turn off" their common sense are already pretty effectively self-protected from such attacks.

8.9 Staying Safe on Vacation

After a wonderfully relaxed day under the Spanish sun, the evening is a very good time to post your latest beach photos on Facebook so as to share them straightaway with family and friends. This can quickly become an expensive pleasure when using a smartphone with high foreign tariffs. There is a convenient alternative, though: take a short detour to the nearest Internet café and you're ready to go—and all for a few cents.

Not such a good idea after all, though... Because in most cases, these Internet connections are not particularly secure. In this case, "unsafe" doesn't just mean that no credentials are needed to use them. Rather, it means that uploaded data can easily be intercepted. At the free hotspots in popular resorts there are countless cybercriminals enjoying themselves, precisely because the free networks are generally so inadequately secured, allowing them to steal all sorts of potentially valuable data in no time at all. Before you can count up to three, your credit card information, your passwords, and other sensitive information have been acquired! My tip is this: only connect to the Internet over protected links, even if you have to pay a few dollars for the connection.

Do you believe that a properly secured network will protect you from all attacks by hackers and cybercriminals? That is definitely not the case! But you do significantly lower the risk that way of falling victim to such criminal activities. I am reminded of quite a different unpleasantness we are particularly likely to encounter on vacation: sunburn! Without the protection of sun cream, the chances are you'll return from the beach to your hotel in the evening with your skin a fetching shade of lobster red. What's more, your personal susceptibility to developing skin cancer is increased. If you use a sunscreen with a sun protection factor (SPF) of five, you reduce this risk, but you're not immune to sunburn. Clearly, an SPF of 50 offers better protection: on the other hand, a lower SPF is still better than no protection at all. Don't you agree?

Speaking of protection factors, did you know that web-surfing and emailing over a 3G or 4G connection is more secure than using a protected Wi-Fi network? With the former, all data are always encrypted and you can be reasonably sure that no unauthorized person gets access to your data (if you trust the government of that country and can be reasonably sure there is no "überhacker" in the vicinity). However, the main disadvantage of this type of network connection is that you have to dig deeper into your pocket. For many holidaymakers, the sheer cost of Internet surfing on a 3G or 4G network in a foreign country can spoil the memories of a holiday destination long after they return from their vacation.

My advice is to pay attention to the following, especially while you're on vacation:

- Check before departure that you're running the latest version and updates to the operating system and other software—especially your browser—on your laptop (and other devices). In this way you can reduce the risk of falling victim to attacks that exploit known vulnerabilities.
- Set yourself up with an anti-theft utility: not just a hardware device like a Kensington lock for a laptop—though that certainly might be a good investment—but software that prevents a thief from gaining access to data on a protected laptop or tablet. Such programs often provide another advantage: devices protected in this way may be easy to locate using GPS.
- Set up a dedicated email address that you use only when traveling: If your data are stolen, it's better to include an email address that can easily be renounced and abandoned.

- Use a firewall to protect your personal information from unwanted intruders trying to break into your system (by the way, this tip applies all the time, not just during the holiday season).
- Secure your smartphone with a security app, too, especially if you own an Android device.
- Switch off Bluetooth if and when you aren't using it. If you are using it, switch to "non-discoverable" mode. Make sure your PIN isn't something obvious like 0000 or 1234.
- Make a note of the serial number of your smartphone and keep it somewhere safe, because if it is stolen or lost it is better to have it readily available. You can probably find this number on iPhones under "Information/General/Info" (but check with Apple's site), while on Android devices it's likely to be under "Settings/System/About phone/Status" (but check with the vendor).
- Make a note of this useful information before you travel, too: the phone number that will allow you to lock your mobile phone with your wireless service provider, as well as the phone numbers of your credit card company and your Bank.
- Keep the exact dates of your vacation to yourself (or at any rate don't give the information to people who don't need it, especially on social networks). Or do you actually want to tempt potential burglars into foolish ideas?
- Make sure that your children are alerted to all the dangers associated with the Internet and mobile telephony. What is the best protection for your children when they are surfing and emailing without a care? Is it to let them leave the front door wide open to any passerby?
- Online banking is best protected by restricting your banking activity to times when you're at home and connecting over a reliable and suitably protected home network, rather than risking sensitive transactions over an unprotected network outside the home. By using an unprotected network you risk having your user ID and your password stolen, so that your dream holiday quickly turns into a nightmare.

8.10 Not Everything That *Can* Be Installed *Should* Be Installed

Some apps for Android devices are incredibly tempting at first glance, as they promise fun, excitement, and games, or even to make your life easier in some practical way. Nevertheless, I earnestly advise you to look before you install. What permissions do these apps want you to grant them? (Yes, we have already spoken about that in Chap. 7.) Try to find out how often they have been downloaded. Every time a new app is published, there's always going to be someone who wants to be the first to download it, and, to my great astonishment, a great many people sometimes download malware. Still, the fewer followers and downloads an app has, the more likely it is that something is not right. Be aware, though, that publishers of

dubious and downright malicious apps may go to some lengths to make it look as though those apps have been downloaded by an improbably high number of people. Recently we've seen apps misusing developer names to give the impression that they've been downloaded more than 5,000,000,000 times—at this time, even apps like Google Play, Facebook, Skype and so forth only fall into the 1,000,000,000+ category.

8.11 Make Yourself Knowledgeable About Security Software

Are you looking for a good anti-malware package? Excellent! It is best to contact a dealer in the area you live in. Or you can purchase the same program that your employer uses, for example. Or you can find out about comparative evaluation articles in IT journals or online consumer tests. No matter how you choose to try to make sensible choices in this area, I am pleased that you are dealing with the subject conscientiously and critically.

However, your information resources need to be checked. What do you know about the publisher of the antivirus program you are considering? How comprehensive and reliable are the experiences of other users? Has the software been thoroughly tested according to objective criteria or by independent testers? Was malware used as the basis for the tests? Of course, these and other questions are of vital importance when it comes to selecting the right product. Consider your choice carefully. After all, you do not want to buy a mediocre product, just because it happened to do well in just one test.

In the worst case, it's possible that the tester has published misleading results because of a poor choice of malware with which to conduct the test or even because by some coincidence the recommended vendor happened to have sponsored the test. To prevent such arbitrary and distorted results, some excellent initiatives have been launched in recent years, such as AMTSO (www.amtso.org), the Anti-Malware Testing Standards Organization, as was already discussed in Chap. 5. You can also check for yourself on the AMTSO site whether the package you are using now works properly when it comes to detecting different types of malware. At the time of writing there are five types of protection that can be tested here (https://www.amtso.org/security-features-check/):

- Check whether protection against the manual download of malware is enabled.
- Check whether protection against drive-by downloads of malware is enabled.
- Check whether protection against the download of compressed malware is enabled.
- Check whether protection against the downloading of Potentially Unwanted Applications (PUAs)—e.g., software that could be abused by malware writers or which doesn't exactly fit a category of out-and-out malware—is enabled.
- Check whether protection against phishing pages is enabled.
- Check whether cloud protection is enabled.

Incidentally, the first two protection checks were provided using a utility provided by **EICAR** (another very important organization in the struggle against malware, also mentioned in Chap. 5). Similar functional tests are also available on the **EICAR** website at www.eicar.org.

These tests make use of the so-called EICAR test file, a file that by convention is treated (more or less) like malware by most anti-malware products but does not contain malicious software. This can be used to test the response of your software without having to use real malware. You can also compress or archive the file and see if your package can also recognize the test file in that form.

8.12 If a File Looks Suspicious, Check It!

What can you do if you suspect that a specific file on your PC might be malware? Hopefully, you have already taken my advice from the previous tips and already have a good—and, above all, up-to-date—security program installed. Nevertheless it is possible, that some malware might have evaded detection by your antivirus program. How can you find out whether this is the case?

One option is to visit VirusTotal (www.virustotal.com) or a similar site such as Jotti (virusscan.jotti.org) or Metascan (metadefender.opswat.com). Here we take VirusTotal as an example. You can upload your file to this site and have it scanned by a number of scanning engines, made available by participating suppliers (and the best known and most reliable ones are included), and you will be notified of the result. If any participating product identifies it as malware, all other participating anti-malware vendors will also be notified immediately, and they can add detection to their products if necessary.

Be aware that online scanners using multiple scanning engines are only there to check certain files for viruses and other malware, but are certainly not suitable for evaluating and comparing the performance of various malware detection utilities.

If the file is recognized by some vendors as malware, but not by yours, that does not mean that you have made a bad choice. It's by no means impossible that one or more products has fallen victim to a "false positive" (FP), meaning that an innocent file has been incorrectly identified as malware. Even when malware is correctly identified:

- Updates to detect a specific example of malware are not sent by every vendor at exactly the same time. Furthermore, reports on multi-scanner sites about which products do or don't detect a sample as malicious tend not to be generated in real time, so may be hours or even days out of date.
- Multi-scanner sites do not use all the functionality that is available in the full-blown product, so a particular engine may be shown as missing a malware sample by VirusTotal, yet the sample will actually be detected by other layers of technology in the real world (though this can vary according to how the product is configured). Failure to identify a specific piece of malware is not always a good reason to write off your security package.

These online scanners can therefore only be used as a check for specific files, but are certainly not a reliable guide the effectiveness of the different participating packages. And, of course, the converse applies. The fact that no scanning engine detects a file or URL as malicious is not conclusive proof that it is harmless.

8.13 Media Training for Everyone!

The recent fuss about PRISM (see also Chap. 4), and the indignation about all the information that all governments hold about us, continues to amaze me. Because in most cases the information those governments have about us (apart from that held legitimately by government agencies such as healthcare services) is no more than what we have put online ourselves. Those who do not want the government to know that they own a convertible should not post photos of it on Facebook. This is why I advocate compulsory media training for everyone, starting in childhood. If everyone realized that all their embarrassing statements, photos, and videos may continue to haunt them for a lifetime, we might all start thinking a bit more carefully about what we post on all social networks. Moreover, being more discriminating about what we post can only benefit the quality of the content we find on social media.

8.14 Think About Your Privacy

Is it important for you to make a clear distinction between information that you're happy to share with the public at large and private information that you would only want to share with (close) friends? Then you should take into account the following points about personal privacy:

- Read the privacy policy of every social network (or other resource) that collects personal information from you. In particular, take note of what information they will share with third parties and how. This way you already know what information about yourself will be distributed without your having any control over it. You can then decide whether you want to be part of such a network. In principle, any product or service that wants to do business with anyone in the European Union should, since the implementation of GDPR (the General Data Protection Regulation), be notifying you of your rights: hence the barrage of notification emails and web pop-ups that assaulted so many of us in 2018. That said, many of these notifications have missed the point by blocking traffic with European countries or putting up notices saying "click here to accept our terms and cookies or else do without this service," or simply ignoring the whole issue.
- Turn on cookie notifications in your browser. This way, you can monitor all cookies that find their way onto your computer/device and, if necessary, block them.
- Finally: be choosy with your online "friends." Only admit people you know and trust to your circle of virtual friends.

8.15 Uninstall Software That You Don't Use

This is a tip from my esteemed colleague Ralf Benzmüller.

Unfortunately, leveraging vulnerabilities and gaps in software has become a real and much-used business model in the cybercrime industry. Cybercriminals have access to an enormous range of "*exploit kits*" featuring a wide selection of exploits. Some of the vulnerabilities that underlie these exploits were already patched years ago, but unfortunately these toolkits are continually updated with new exploits, usually very soon after the discovery of a vulnerability.

Because software is complex and in principle may always contain unnoticed weaknesses, I recommend that all computer users keep the number of installed software programs they install as low as possible. Many people install all kinds of tools, games, and applications as soon as they become available, without thinking too much about it. Apparently, they are not aware that this indiscriminate "pack rat" behavior increases the risk of their becoming victims of cybercrime, since every program installed also increases the (theoretical) possibility of an attacker invading the system without authorization.

If you only install the software you really need, your system is less vulnerable. A good way to decide whether or not to install a certain program is to consider whether you would be willing to install updates for this software on a weekly basis if that were to prove necessary. Do you still want to install it, or have you changed your mind?

But there is another reason to delete unused software: most software developers eventually cease to support older versions of their products (this applies to both free and paid software and affects individuals and businesses equally). As a matter of principle, do not use any software that is no longer supported by the manufacturer, because if new vulnerabilities are discovered, patches will not normally be developed to fix them. Some tools may be able to recognize such outdated software on a computer system. Try replacing the old software with a new version or an alternative brand that is still supported, because the availability and quality of support is an essential measure of a program's value.

What Is An Exploit?
The term "exploit" may sound very technical, but it is literally what the name suggests: a way to "exploit" a weakness in software or in an operating system. Thus, if a security hole is detected in Windows (for example) through which malware can sneak in, then you can be sure that days (or even hours) later malware will already be circulating that uses exploits to enter the system through this vulnerability.

8.16 Watch Out for Hoaxes

Even if you do not know exactly what a hoax is, you have probably already encountered hundreds of them. On the Internet, a type of hoax still often seen consists of warnings concerning dangerous viruses and other malware. The subject

lines of hoax messages are often all uppercase, besprinkled with exclamation marks to emphasize the "importance" of the message. Then they continue along the lines of "Important!!! This is not a joke!!!," after which some nonexistent virus is described.

I would like to say it once again very clearly: it's not normal or reliable for the public to be warned by email—especially electronic chain letters—about dangerous viruses! You already know that you should be careful about opening mails sent by unknown senders—and even more so about attachments to unexpected messages. If you trust your own common sense and regularly update your antivirus protection, you are already well protected.

And above all: do not forward these messages yourself, that is, absolutely useless, and may even expose your friends and acquaintances to unnecessary risks.

8.17 Keep Your Webcam Masked

It seems a bit paranoid, but sometimes it pays to cover your webcam. Doing so prevents uninvited guests from getting an inappropriate view of your office or bedroom, and even of taking advantage of that view, for example, by capturing images as potential material for blackmail, with sneaked photographs of your private life buzzing around the web and discoverable by search engines. Or they might be able to get more information about you as a basis for social engineering (also see the tips for companies in Chap. 9). There are even known cases of hackers who, by using facial recognition on the webcam, managed to log in to someone else's PC.

Nowadays, some webcams already have small flaps to cover the lens, making it child's play to protect against unwelcome guests, not to mention Peeping Toms. But if your webcam does not have that feature, I would recommend that you cover it with masking tape or something similar except when you need to use it.

Alternatively, companies should consider device management solutions that allow, for example, the disabling of USB webcams.

8.18 Back Up Your Smartphone, Too

Just as there are for desktops and laptops, there are various ways to make backups of smartphones and other mobile devices, either to a local external hard drive or to the cloud. Anyone who does more with his smartphone than just phone calls, web-surfing, chatting, and texting would be well advised to consider one of those options. If there is information on that device that you do not store anywhere else, you could lose it completely in the event of the loss or theft of the device, or a system crash.

Get into the habit of synchronizing your smartphone with your PC on a regular basis—do not worry, it's not difficult—perhaps in combination with a cloud solution like Dropbox when you're out and about. This will save you a great deal of trouble.

8.19 For Advanced Computer Users and Courageous Beginners: Encrypt Your Hard Drive

If you are not afraid to take a deeper dive into protecting your computer or mobile device, I can also offer you some further tips. They are, admittedly, a bit more complicated to implement than the others and require careful attention in order to configure things properly, but they are definitely worth the effort!

Probably you think that only highly sensitive corporate data needs to be encrypted and protected with passwords against unauthorized access. But you are wrong! Your personal PC also contains a great deal of data that should not be allowed to get into the wrong hands. Just think about information that would allow a criminal to access your credentials for online banking. In particular, I would like to urge all users who frequently use their laptop or notebook PC on the move to encrypt their data on the hard drive as well as traffic exchanged with websites.

This is not difficult for users of some devices with Windows Vista or a later operating system from Microsoft. From Windows Vista onwards, Microsoft offers its own disk encryption software, BitLocker, though it is not available on *all* versions of those more recent operating systems. Many systems do not have the TPM (Trusted Platform Module) that BitLocker requires as standard. However, a small adjustment in the policy may be sufficient to circumvent this problem.

Adjust the "Group Policy" of your PC as follows. Run "gpedit.msc," and navigate to Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives. Open the setting "Require additional authentication at startup." By checking "Allow BitLocker without a compatible TPM" and applying the policy by clicking "OK" or "Apply," it is possible to go through the BitLocker drive encryption wizard and to encrypt the entire disk. There are also other solutions available for the less adventurous user.

If you are now convinced that hard disk encryption would be of use to you, but you are finding this all a little overwhelming, there's no reason to tear your hair out. With luck, your local computer store will be able to put you in touch with experts who will be happy to help you with implementing safe data encryption of your hard drive. If you only want to encrypt individual folders, security companies (including those who offer security suites incorporating malware detection) often offer solutions that already include an appropriate encryption tool.

8.20 Tip for Advanced Users: Use a VPN

Anyone who frequently has to send reasonably confidential information over the Internet should consider using a virtual private network (VPN). A VPN sends and receives all data over an encrypted connection to lessen the risk of unauthorized interception. If you want to purchase VPN services from Internet service providers or more specialized providers, it would be better to check whether all traffic is fully

anonymous and that your data are not inappropriately stored and exposed. And to keep the risk of interception as low as possible, it's best to use a VPN in combination with other techniques such as end-to-end encryption of emails.

8.21 Tip for Advanced Users: Disable Java

Java is very popular among malware writers: Java's vulnerabilities sometimes make it very easy for them to bypass your firewall if they can persuade the victim to click on the "right" links and files. As soon as these hurdles have successfully been cleared, they can tunnel from the inside out to the Internet, something the firewall often does not consider suspicious, whereas inbound traffic is carefully inspected.

Those who do not use Java all the time, and are prepared to switch Java on and off manually before and after using Java-powered software, contribute significantly to their own security. Information on how to do this is available here: https://www.java.com/en/download/help/disable_browser.xml.

8.22 Tips for Advanced Users: Make Sure Your Device Locks Itself Automatically

The very thought that they might lose their beloved smartphone, or that it could be stolen, makes most cell phone owners go green around the gills. I can only advise you to keep the damage to a minimum by using the automatic locking features of your smartphone, so that the device locks itself after a few minutes and can only be accessed by a password, passcode, or similar authentication feature such as pattern matching or fingerprint scanning. At least then the data stored there will be protected against access by unauthorized persons.

Similar functionality is also available for tablets and laptops. If such functionality is enabled, thieves or other dishonest people who find a mislaid device cannot do anything with it, even if it's not possible to destroy your data with a remote deletion utility. Set your smartphone or mobile device to lock automatically after two to three minutes of inactivity to minimize the risk of potential data loss.

For a device running iOS, you'll probably find the relevant functionality under Settings > General > Automatic lock: for an Android device look for Settings > Security Screen Lock or Auto Lock.

For a PC or laptop you can usually configure the PC to be reactivated with a password when the screen saver is active or the PC comes out of sleep mode. I advise you not to set the number of minutes after which the PC goes to sleep too high. You should, of course, also ensure that the PC will not give access when powered up or rebooted without a password and/or other authentication.

It may seem a nuisance when you do not use your PC for a short while and then realize that the screen saver has kicked in so that you need to enter your password

again to continue working. But believe you me, the day you leave your notebook somewhere, or it gets stolen while you nip outside for a cup of coffee, you will be very grateful for this data-preserving functionality and will not regret requiring the minimal effort needed to enter a password. Minimal, that is, for you as the legitimate owner. Hopefully, you'll have made it very much harder for a thief or the less-than-honorable finder of a mislaid notebook to get access to your data.

Since there's no harm in repeating good advice, here's an opinion piece that summarizes much of the advice given in this chapter and elsewhere in this book.

In the Words of
Jeannette Jarvis, Director of Product Marketing, Fortinet

The Internet has radically changed our lives. Mostly for the better. Having access to an unprecedented amount of information now available at our fingertips, being able to shop online 24 × 7, engaging with family and friends around the world, attending university from the comfort of your home, joining online communities around our interests, and much more: this is all good. But cybercrime continues to be a great threat to each one of us. The Internet, while a great place to socialize, shop, and learn, has a dark side. On the Internet you don't always know who is good and who is bad, what is fact and what is fiction, which website is legitimate and which site has been hacked. Cybercriminals are constantly evolving their tactics and techniques so as to evade detection and to exploit you. What is an individual user to do? How can you stay safe online as you traverse cyberspace? You need to take precautions, and below I spell out some suggestions to help keep you safe while browsing

Operating System Updates—New vulnerabilities and weaknesses in operating systems and applications are always being discovered. Ensure you are keeping your system up-to-date with the latest patches that are designed to address these concerns. Home users are advised to turn on automatic updates, ensuring that your computer is always updated with the current patches.

Security Tools—Make sure you are using reputable firewall and antivirus software, and that it is kept current with the latest detection signatures and updates. Your security software should include antivirus, firewall, web security, and vulnerability scanning tools, at a minimum. Utilizing a suite of security tools that can detect known and emerging malicious threats is a must.

Passwords—Don't fall into the trap of using the same passwords across multiple accounts: this only makes it easier for you to be exploited even more, should one of your accounts be attacked. It isn't easy to think of new passwords but there are some easy tactics you can adopt. Use phrases that are easy to remember—the longer the better. Add a number or more within the phrase as well as special characters/symbols. Misspell words intentionally and add capitalization within the password, not just at the beginning. Your password doesn't have to be logical—make it senseless and silly, but long. Never share your passwords and if you must write them down, don't store them in an

(continued)

easy to find location. If you can use a multi-factor authentication process, do. Many banks are now offering this service—use it!

Secret Questions—When creating many of your online accounts, you will be asked to create special questions and answers for account and password recovery purposes. Realize that you do not need to create questions and answers that are truthful or make sense. Never use your mother's real maiden name, or your dog's name. You are under no obligation to tell the truth here. Instead use something funny and rooted in fantasy.

Be Wary—There are a lot of 'bad' sites on the Internet, and phishing emails continue to be a successful way to exploit you. Be careful. As sad as it sounds, you should take the attitude of Zero Trust and always validate the legitimacy of a website or email. Web sites are easily spoofed to look genuine, and hackers are quite good at ensuring that the counterfeit sites look authentic. Ensure, if you are on a financial site, that you typed in the URL yourself. Financial websites should include 'https' to ensure that it is using encryption and that your communication is secure. Don't click on unsolicited links in your emails, ever. Be leery of any site asking for personal information. Scams are abundant. Be on guard at all times. Stop and think first before sharing anything. And for what it is worth, you are not obligated to share anything!

Public Computers—Never use a public computer to access personal or financial websites. You never know what is being tracked and logged. It is highly likely that the computer has already been compromised with malicious software, such as with a keylogger that tracks all your information as you type. Use a virtual private network (VPN) so your data is encrypted and kept private. Be on guard at all times.

Back Up Your Data—How upsetting it would be to lose all your data and pictures due to a cyberattack, or even computer malfunction. You can easily back up your data using an external hard drive (store it in a safe place). Back up your data often. There are legitimate cloud service sites to help store your data too, but do validate their legitimacy before using them.

Internet of Things—Many home devices are now being directly connected to the Internet. Most common are your home media devices like smart TVs, home-monitoring cameras, home thermostats and lighting, digital voice assistants, and more. All these devices are vulnerable to exploitation. If you don't need the device connected to the Internet, disable that feature (ask for help if you don't know how). The last thing you want is your private information, conversations or videos being sent across the Internet without your knowledge. You can update your IoT devices by going to the hardware vendor's website and getting a firmware update: again, ask for help if needed. These devices often have default passwords installed, so do change these where possible: don't make it easy for the hackers. Above all else, secure your home network. Make sure your home router is kept up-to-date with the latest updates, and that you have changed the default password.

(continued)

Fact Check—Don't get caught believing a dubious story on social media. There is a useful service—snopes.com—that fact-checks many stories for their legitimacy. Bad actors play on web users' vulnerability and emotion and create stories that are not correct in order to cause disruption, confusion and promote ideology. It is always best to fact-check before forwarding or posting any story.

The Internet is a wonderful thing: it has altered our life like nothing before. With a few precautions you can be protected and secure, but it takes proactive steps on your part. Don't be lax: be guarded, be safe.

Jeannette Jarvis is Director of Product Marketing for Fortinet, focusing on FortiGuard Labs, their research and threat intelligence organization. Previously she served as Director of Product Management at McAfee and Intel Security. She has also held senior leadership roles in computer security organizations at Microsoft and Boeing. Jeannette is on the advisory board for Virus Bulletin, an international organization covering the global threat landscape. Jeannette was selected by SC Magazine as one of eight IT Women to Watch in 2017.

Chapter 9
Tips for Companies: Surviving on the Internet

All the tips that we discussed in Chap. 8 also apply to companies. Here too, general principles apply, such as regularly updating software (including security software) and operating systems. Indeed, they are even more important in the corporate context, not only because more computers and system users are affected locally in the event of a successful attack or other damage, but also because the impact of malicious software and/or a possible corruption or loss of data can be far more far-reaching. But there are statutes and regulations that apply specifically to companies, or at any rate are less applicable to private individuals. That is why we consider these tips in a separate chapter.

9.1 A Good Security Policy Is the Bedrock of Corporate Security

Information security in the enterprise starts by implementing the security of the basic infrastructure of ICT: the networks and computer systems. But that's just the start. There are many other aspects of security that need to be addressed: technical, organizational, physical, and procedural. It is therefore extremely important to develop a good security policy because it is one of the pillars of safe computing, foundational to almost every company. The starting points for an effective security policy are always the same. Here are the most important:

- Ease of use and information security are both considered desirable, but they lie at opposite ends of the spectrum. A security policy is usually a compromise between these two objectives.
- Information security is usually the last budgetary element to be considered, if at all, when estimating costs. For many projects it is not taken into account as an integral component at the planning stage. Security (and the need for security) is

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_9

often unseen by the unpracticed eye, but it is complex and has a correspondingly substantial price tag.
- A security strategy is only as strong as the weakest of its components.
- Good information security is set up layer by layer, not as a single solution.
- Trust is the worst basis for security and safety.
- Security has a strong operational component. You must be constantly alert and take appropriate precautions: the Internet is a great resource for a hacker looking to obtain up-to-date information and set up organized attacks.
- Attacks from within the organization are potentially the most successful, yet receive much less attention than attacks from the outside, to the detriment of the organization's security. However, it's not just deliberate malicious action from insiders that is responsible for successful attacks. Often, it's just poor practice or user errors enabling attacks from the outside, or causing problems that aren't directly caused by an intentional assault.
- Another (related) problem in information security is an awareness of the *importance* of security. This is still neglected in most companies. Only by ensuring such awareness throughout an organization can an effective security posture be achieved.

Based on recognition of these (sometimes sobering) conclusions, security policies can be drawn up for all aspects of the information architecture. Here I am going to be a bit more technical, so as to provide a sketch of the issues that a good and complete security policy must address. However, it's the responsibility of every organization to paint the full picture most appropriate to its own needs.

Server Security describes a standard that every server must meet before it is put into service. Such a security standard includes the local security policy, and a comprehensive consideration of correct configuration, but also the local hardening of the systems parts that can be isolated from the rest of the infrastructure. Testing a server can be done manually, but in real life that is often forgotten or simply skipped. However, there are good remote audit tools that can help with this task. It is important that logs are created and regularly monitored within this framework. A commitment to a timely update and patching process is an indispensable component of every company's security policy.

Numerous components are defined as integral to *Network Security*. Usually, people see this as being just the firewall, but there is a lot more than that to sound network security, of course. Several security vendors also have internal IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) that can be deployed and configured at certain strategic locations. How these are configured and where they are placed on the network must also be clearly described in the policy. In addition to firewalls, switches, and IPS/IDS systems, configurations and setup for components such as scanners, printers, and proxy servers must also be defined. *Client Security* describes what criteria a PC must meet before it can be used. For example, it states whether security requirements must be met before the client (the end user device) is to be permitted onto the network. Many companies do not even use the standard compatibility tests often included with antivirus packages, and in fact there are even workstations or portable devices such as laptops and tablets where no anti-malware protection is installed.

Endpoint security (security of the devices used by end users) stands and falls nowadays according to whether or not USB sticks and other portable media are permitted. It is not happenstance that Conficker is still circulating on several networks: it is precisely because people have forgotten to "lock the back door": in other words, to restrict or prevent USB access. All too often we have already found that on far too many networks, this risky behavior has led to major disruption.

A respect in which companies often go wrong with anti-malware packages is *fine tuning*: this means modifying the standard (default) settings of the package to meet the requirements of the organization's security policy and thus fit the organization's specific needs. A security specialist who does not *know* a company should nevertheless be able to deduce key aspects of the client's security policy from the settings of the anti-malware package and other security management and remediation tools. In fact, such a management toolkit is more or less the beating heart of corporate security and underlies the organization's security policy, and therefore a company must have calibrated this toolkit with precision to meet its own needs. The problem is that many companies fail in this area and do not even manage to document the nature and configuration of the tools in use.

Here, too, the problem of updates or patches arises. Every company needs to describe clearly in its security policy how updates should be handled. This is not only about keeping the operating system up-to-date but also about installing newer versions of (and updates to) other applications. For example, Adobe Acrobat Reader and Flash Player, and Java, have become two of the most vulnerable and frequently attacked packages in recent years. If you do not patch these, and do not have good security on your endpoints and gateways, you can expect to fall victim to malware attacks and data theft sooner or later. (See also Sect. 9.5.)

Gateway Security (security of the gateways allowing access to and from the Internet) is in general fairly well addressed by many companies. However, there are still too many that rely on the strong security of their gateways but totally forget that there are still potentially serious vulnerabilities and security issues associated with end user devices (especially notebooks). Malware can then enter by this back door and leak certain business-critical data (Or worse!).

Nor should companies forget to strictly regulate the browsing and email behavior of their staff. Are employees allowed to visit all Internet sites and/or open all email? And if that is not the case, are these restrictions configured and monitored correctly on the proxy and/or email server? If that isn't done, we must face facts. We simply cannot know what is and what is not dangerous at any time of any day. By implementing good policies, we can at least make users aware of the consequences that can arise as a result of reckless behavior.

Sadly, end users are usually the weakest link, with reckless behavior being observed all the way up the worker/management hierarchy. For this reason, companies need to address this specific issue and should not underestimate the importance of *Security Awareness*. There are certainly companies that make praiseworthy efforts in this area, but experience shows that many are still too lax and unhealthily complacent. Otherwise, it would long ago have been standard practice for them to give regular training to their staff in security, with regard to both internal and global

networks. Such regular educational practices are largely restricted to some banks, insurance companies, and major multinational corporations, and that's about as far as it goes.

There is no doubt that it is not easy to design and implement a good security policy. What are the most important points that should be considered in formulating such a policy?

1. The whole management team must support the policy. You may as well save yourself the effort of formulating a policy if there are no sanctions attached to it. An effective sanction in most cases is a formal warning to the user who does not behave according to the rules, with a note placed in his or her file. If such a note is taken into account in regular performance evaluations, then it can work very well.
2. Employees must be made aware of the current corporate policies, especially those relating to data protection and network security, and should be encouraged to review it regularly, for example, via the intranet, but they must also receive it in writing at home.
3. Developing a security policy is best left to experts. Often a company leaves the job to a layman who overlooks crucial elements, and that can sometimes lead to even worse consequences than when *no* security policy has been drawn up, because it gives a false sense of security. A company should consider hiring a specialized consultant to design or at least have input into and review the policy.
4. The company should define responsibilities, define appropriate processes, and name employees who are responsible for adhering to the IT security policy in the company. Internally, a team including representatives from the HR and ICT departments must bear primary responsibility for ensuring compliance.
5. Auditing tools (software to analyze the robustness of the company's security) should be purchased, though security software already purchased may include up-to-date monitoring and auditing capabilities that can be used as the basis for ensuring corporate privacy and security.
6. Finally, the policy must also be thought through in terms of content. This is not the place for a vague description of a general security objective and how the company intends to realize it. Even a brief but incoherent description of security objectives and the resources planned for meeting them is guaranteed *not* to be read by *any* employee, let alone acted upon. Not even if the policy is a model of conciseness, and even if these documents are printed on handmade paper and bound in leather.

To my regret and astonishment, few top managers are interested in security policy. Adherence to strict regulations (as per standards formulated by ISO, for instance) with little obvious Return On Investment (ROI) are not glamorous enough to attract bonuses at C-level. But that is precisely why the security policy fails to be aligned with the overall corporate policy. Yet as soon as a major incident occurs, the house of cards collapses, and everyone looks bewildered, staring at each other and wondering how this could happen and who is to blame, "because we had a policy and we invested tons of cash into it." It goes without saying that investing in an infrastructure for security does not generate an immediate and visible return, which

is why security is not addressed as a function of routine company policy and company interests. Yet a good security policy is indispensable here. It needs to be made clear to the decision-makers that they can only successfully protect their company if IT security is holistically addressed and becomes part of the corporate culture. A quality security policy is not implemented in isolation.

Let's take a look behind the scenes and ask ourselves how an IT security policy is usually designed. First of all, the company's assets are classified as data, systems, and applications: then you think about what could go wrong with them. Then you pick out the most likely scenario and base your countermeasures and policies on that. You think that is a good starting point? But it is not—at least not always! After all, how does the author of a security document or even the system administrator know what a hacker thinks and predict what data will be of interest to him? Many administrators consider a system secure because it is protected by a firewall and because they believe it holds nothing of interest to a hacker. (Of course, many home users have similar misconceptions.) They assume (incorrectly) that they only need to protect against spyware and other malware. But data that the legitimate user believes to be of no value to others can turn out to be valuable information for a cybercriminal. It is difficult for policymakers and security administrators to determine what an attacker might be after and to think like a hacker, spy, or spammer.

That is why the starting point for policy makers should be that they need to protect against attacks that they do *not* know about. In order to develop an adequate security policy, it is therefore important for a company to keep itself continuously well-informed about what can go wrong, the possible consequences of a successful attack, and, above all, how the company policy needs to evolve. Too often, no security experts with in-depth knowledge of the potential hazards are brought in to consider these factors, and the policymakers themselves do not know enough about the possible dangers. And then all those precious dollars spent on security might just as well be spent on the office Christmas party.

If all this sounds too much to take on, ISO/IEC 27001 offers guidance on and a standard for the implementation of a comprehensive Information Security Management System (ISMS) that can be independently verified by audit.

9.2 BYOD (Bring Your Own Device) or Not, You Must Ensure Good Security

It gets harder all the time to distinguish between work and private life, not least in that almost everyone has a mobile phone—nowadays even more smartphones are sold than "ordinary" handsets for landlines—and they tend to be used to some extent for both personal and business use. Even those of us with two separate telephones have difficulty keeping their use for home life versus work life perfectly separate. What's more, almost everyone stores a lot of information on their smartphones and tablets. The devices are overflowing with personal information, working documents, emails, text messages, contact information, and appointments.

No wonder these mobile terminals are of such interest to cybercriminals, being such a valuable source of information. Nor is it at all surprising that since 2010, volumes of mobile malware have increasing exponentially. And the most important victim is Android, the mobile operating system that is more popular than Apple's iOS, but unfortunately much less secure. Compared to iOS, the operating system used for iPhones and iPads, there is much less control exerted over apps for Android. In addition, the distribution of updates is not as smooth and systematic, since Android doesn't have much control over their distribution to any hardware other than its own (though Google claims to be attempting to address that problem). In addition, it's often not possible to apply current upgrades to older models of smartphones. This certainly does not benefit the security of Android devices (though it's also an issue with Apple devices). In addition to vulnerabilities in the operating system, there is another major problem, as I've already mentioned several times: namely, the human factor. The permissions required for the installation of apps are readily granted by users, often without reading the small print. This opens the way for applications to collect information, call expensive pay-as-you-go numbers, send the geolocation of the user to a server, and much more.

> Regardless of whether a company has a "Bring Your Own Device" (BYOD) policy or prohibits the use by its staff of their own devices for work purposes, it is hopelessly optimistic to think that employees will maintain complete separation between the private use and business use of their mobile devices. The chances that an employee will install malware on his phone or tablet grow month by month. Mobile devices are getting more and more attention from cybercriminals even as the number of mobile device owners increases. Which is why the development of new malware will continue to accelerate.

To make matters worse, the possible uses for smartphones are far from exhausted. New technologies are constantly being developed—and with them, new vulnerabilities. Therefore, it should be clear to anyone that Android devices, like our traditional PCs, need to be protected against malicious software and other attacks. Regardless of whether or not you insist on maintaining a BYOD strategy in the workplace, all devices must be protected against unauthorized access by third parties—and other attacks—whenever they contain company data. This is the case irrespective of who actually owns the device, or whose responsibility it is to meet the cost of this protection.

9.3 Take Care in the Cloud

The "Cloud" is the collective term for all forms of outsourcing of software, development platforms, data storage, and even the entire ICT infrastructure to somewhere outside the organization's own perimeter. The best-known form is Software as a

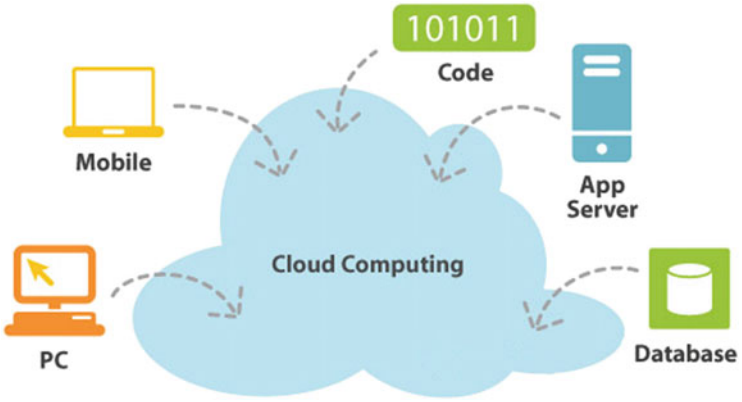


Fig. 9.1 Cloud computing graphic

Service (SaaS), where software is no longer hosted on its own company server or end user PC but is offered to the end user from the supplier's server via the Internet. This may be business software such as Salesforce.com but could also be pay-per-use or free software or unpaid services such as basic Gmail (as opposed to G Suite). One characteristic of cloud software is that—if you *have* to pay—you pay for each time the software is used or for the period of time specified in the license, instead of purchasing the software. In addition, you can quickly increase or decrease the number of users at need.

The cloud (Fig. 9.1), as a logical development of outsourcing, is seen by many as the ultimate computing model of the future. And I am myself convinced that it is the best solution for many applications. But as a security expert, I also cannot permit myself to gloss over the dangers of this new model. That is why, some time ago, together with Righard Zwienenberg (see also Chap. 5), I wrote a conference paper ("Attacks from the inside," Virus Bulletin, 2010) with an overview of the dangers threatening the cloud at the security level. The following nine threats are the main ones we described (https://www.virusbulletin.com/conference/vb2010/abstracts/attacks-inside/):

1. *Identity management*. You never know for certain who's who in the cloud, or under it. Attackers can steal your identity. The cloud does not know who you are. If an attacker infiltrates your corporate network, perhaps via your smartphone or tablet, and starts communicating with the cloud from there, the cloud still assumes that this is a reliable source within the company. This allows the attacker to intercept a great deal of information or to feed the cloud server with incorrect information. A "man-in-the-middle" scenario is also not inconceivable here, where the attacker finds a way to position himself between the company and the cloud.
2. *Abuse of services*. The atomic bomb has provided conclusive proof that every technology, like those based on nuclear physics, can be used both for good and

for evil. It's the same with cloud computing. The cloud makes it easy for companies to quickly launch a program or service, without suffering too much hassle in terms of management and administration, since much of it happens elsewhere, and is someone else's responsibility. But this is also good news for cybercriminals, of course. For example, cloud services have already been used for different botnets—such as Zeus (see also Chap. 10)—and malware downloads. Since simple registration with a cloud service also increases anonymity, the cloud is a popular platform among criminals, especially since the likelihood that cloud suppliers will detect fraud is usually not great.

3. *The hijacking of accounts and services*. If your account is hijacked in the cloud—as happens regularly on Twitter—this is annoying for both the cloud service and the user. It is not always clear who is responsible for the leak that made the hijacking possible. But whether it is the cloud service or the user, the latter will always be blamed (or at least held partly responsible), because it is in his name and that of the company that the breach has taken place.
4. *Financial distributed denial of service*. This term refers to the widespread misuse of (or attacks against) cloud services that can have a serious financial impact. The most obvious example is where the cybercriminal gets hold of someone else's account information and executes large transactions for his own profit or in order to harm the other party. This can, in the worst case, lead to a company's bankruptcy. A criminal can also abuse your company's account for personal use, for example, by using servers you hire monthly for his own—usually criminal—activities. Worst of all, you can also be accused of these criminal activities, with all the damage that entails. Finally, the cybercriminal can also attack your cloud service from the outside, for example, with a targeted DDoS attack, so that the resources to which you are entitled according to your cloud contract are completely used up.
5. *Leaking and losing data*. Suppose you are using an antivirus service in the cloud, and a confidential document is sent to the cloud for checking, for example, because it is not "whitelisted" (meaning that it is not on the list of authorized documents). But what happens to your documents up there in the clouds? And who is *behind* the cloud? You can still see what goes on outside your company, but do you know what happens to content when it is scanned in the cloud? For example, a document incorrectly labeled as malware can be quarantined in the cloud forever, even without your being aware of it. Maybe that's just a harmless statistic, but do you want to take that risk?
6. *Unknown risks*. Are you aware of all the risks of using the cloud, or a specific cloud service? The basic agreements about security are usually laid down, but is it also stated in the contract which of the supplier's representatives have access to your information? And what happens in the event of a vulnerability? Or—not unimportantly in today's world of surveillance and espionage—what obligations does the cloud supplier have in relation to its own government? If you cannot accurately identify and assess these risks, it's best to think twice about whether you really want to use the cloud and its services. Such a decision may involve a lot of problems with business partners or even with government agencies, as they quite reasonably expect you to have full control over all your applications and data.

7. *Hidden logs / burglary attempts*. You can detect a targeted attack on your own network based on your own log files. On the other hand, if an attacker targets your data and applications in the cloud, he can intercept all reports about the attack sent to you, and you'll lose out—since you have no cloud administrator rights, you can do nothing to remediate the situation.
8. *Abuse by insiders*. The biggest threats to any ICT architecture are more and more to be found behind the company's own walls (I'll come back to that later). In the majority of cases, an organization's own employees are responsible for data loss and theft. That is a point in favor of the cloud, you might think, because if that's where your data are, your own employees are no longer in danger of attack or temptation. But if that *is* your expectation, you are forgetting one important factor: the cloud provider also has its own employees, and they are all the more interesting to cybercriminals because they have inside information about dozens, hundreds, or even thousands of companies. The security rules will have to be adjusted accordingly, but it will be necessary because attempts by cybercriminals to use cloud workers—willingly or unwillingly, consciously or unconsciously—will only increase. There is a small consolation: Cloud providers usually update their security rules in a timely manner, and that is sorely needed, because the number of attempts by cybercriminals to persuade cloud employees to do their nefarious work for them is increasing daily.
9. *Centralized authentication, authorization, and accounting (AAA)*. Everything that concerns access to cloud resources, the imposition of security policy and auditing and invoicing of customer usage, is kept centrally by the cloud provider. Of course, this has enormous security implications if the integrity of this centralized AAA cannot be guaranteed. Be aware that the consequences of your account being misappropriated must, in principle, be borne by you, regardless of what it may say in your contract.

As cloud services become increasingly popular, many private individuals and companies are eager to follow this trend, usually without having given due consideration to the associated risks and issues. I hope that with the list above every manager, but also every private individual, looks at cloud services a bit more critically and signs up only when they've thoroughly considered its ramifications.

9.4 Beware of Social Engineering

There is no firewall or other advanced security software that offers much in the way of protection against social engineering. That's because the point of this kind of hack is that the intruder infiltrates a company with the unsuspecting help of a user and thus bypasses (potentially) all IT security. Thanks to the worldwide use of the Internet, more and more personal data are served up on a silver platter, and *Social Engineers* can use those data to pretend that they know their victim or to pose as, for instance, a senior manager within their company. The possibility of such imposture makes it

advisable for staff always to check first with their own direct supervisor whether a person making unusual demands really exists, and whether their making direct contact actually makes sense. Contact from social engineers is mostly by telephone or email, but they do not always shy away from personal contact. Here are some tips to prevent a company or organization from falling victim to such an attack.

On the Internet you can prevent a lot of mischief by checking URLs you are sent: just mouse over the link and check whether the URL that appears in the pop-up is the same as the one you are supposed to click through. An alternative is to enter the URL you *know* to be correct in your browser yourself, rather than clicking on the URL you're not sure of. Even with emails from unknown senders, you need to pay careful attention, before you answer this person or strangers, and be sure of their bona fides before you reveal confidential information.

Critically, keep your passwords to yourself. Don't share them for work purposes, even with people you trust. And certainly not in personal conversation or via email or the telephone. Bear in mind that your IT unit has administrator privileges and should never need to ask you for your password—if they do, there is something wrong.

Physical access and contact must also not take place within (large) companies without appropriate caution. Companies must provide access passes for all employees, and all visitors to the company must identify themselves upon entry before they are provided with a temporary access pass. It is also important to ensure the necessary awareness among all employees—especially those who have the most contact with the outside world—because they are a potential target. And last but not least, companies must ensure that business information is not left physically exposed outside the company walls, for example, documents in paper containers or hard disks in scrap metal containers awaiting disposal. In one case I heard about, an organization sent its paperwork to an outside company for shredding. However, it was left in the forecourt on Friday evening to be picked up early on Monday. . .

All of a company's employees must always be wary of strangers, wherever they are.

The entire workforce should be made aware that they should never give company data to unknown persons, either at the company's own front door or in the pub, in front of the PC, or in the conference room. Even if you think I'm paranoid, I can only advise you that a little too much trust can cause a great deal of damage.

9.5 Patch Management: Put Some Plasters on Your Wounds!

We have already talked about the importance of patches and updates to all computer users, but I'd still like to pass on this tip from my colleague Jan Van Haver (please see also blogit.nl).

If you regularly pay attention to current IT news, you know that not a week goes by without a big news story being reported somewhere about newly discovered

vulnerabilities in commonly used software. Everyone (experts and laymen alike) fears these so-called *zero-days*. The term refers to the time that elapses between the discovery of a leak or vulnerability and the availability of a patch that fixes the problem. Such issues are feared because it is assumed that cybercriminals are more likely to write malware that exploits the leaks before the software vendor can come up with a patch. That is, of course, a realistic scenario that should indeed make you nervous. But zero-days are far from being the biggest problem.

For cybercriminals, information about security vulnerabilities in computer programs is highly sought after. If they succeed in spreading computer malware that exploits a specific gap in system defenses before the affected software vendors can counter this with an update, the chances for a successful attack or a PC malware pandemic are much greater. However, such malware may be caught by anti-malware programs before the affected vendor is able to issue a patch. In fact, anti-malware vendors may be able to detect unknown malware using that vulnerability before a patch is released, since it's sometimes easier and quicker to detect the presence of an exploit than it is to generate an effective and thoroughly tested patch in the affected software. This is, of course, by no means criticism of affected vendors: it's just how things are in the world of programming. Some coding tasks are more time-consuming than others. And it's still essential that you install a patch when it becomes available, rather than rely on detection of malware. It's rather like the difference between applying an emergency splint to a broken limb and resetting the bone under hospital conditions.

But here's the thing. Research has shown that 90 percent of successful attacks on business networks have made use of security breaches for which at the time of the attack there is already a perfectly adequate mitigation to the leak in question—a so-called *patch*, the software equivalent of the patch used to seal a leak in an inner tube—available from the manufacturer of the software. The big security problem is therefore not that there are no solutions available, but that such patches are not installed as soon as is practicable after they become available. Ironically, cybercriminals take advantage of patches: by analyzing the patches made available by the software producers, they get exactly the knowledge to make malware that exploits those vulnerabilities. Then they unleash their malware onto the world, in the hope (and certainty) that many companies have not yet rolled out these patches.

The fact that patches are not always properly or promptly installed on corporate network is understandable. The IT administrator often has no idea which software is used by all the company's employees, and it's even less certain that he has a good overview of exactly which software versions are running on which machines. Moreover, it happens quite often that patches conflict with certain (less common) programs that are used by companies or that a patch disables—intentionally or as a side-effect—certain functionalities that are important to some users, so it may be easier just to skip the patch. After all, as we often say in IT circles, why fix what isn't broken? But the patches described here are intended to fix something that *is* broken, and all companies should realize how important it is to roll out security patches as soon as possible.

A proper patch policy is an essential component of a sound security strategy, defined as a so-called UPMS (*Update/Patch Management System*). Such a procedure should consist of the following steps:

1. *Updating the inventory of software and hardware*. The company needs to be aware of all programs and devices used within the network.
2. *Information gathering*. Before every rollout of software or hardware, the IT administrator has to be made aware of the version to be installed, and to have investigated possible problems, such as known bugs and vulnerabilities, and whether updates and patches are already available.
3. *Planning and implementation of a strategy*. It's not always necessary to roll out all patches over the entire network. Factors that should play an important role when planning a rollout include the seriousness of the vulnerability, the degree of awareness of the leak, how easily and extensively the leak can be abused by cybercriminals, the likely impact of a breach, and whether the patch might be dependent on previous patches that might not yet have been installed.
4. *Testing patches*. This is a crucial phase that can prevent many problems. Testing must be done where possible on systems that simulate all systems within the network in terms of configuration. It is often *not* possible to implement a physical test setup that completely meets this requirement. In such a case, it is possible to use virtual machines, even though they do not provide a realistic picture in *all* respects of the physical problems that might occur, such as problems with bandwidth and lack of disk space.
5. *Planning the rollout*. Many patches cannot be performed on a system while it is in use, or may require a reboot of the system, in which case it is advisable to roll out patches outside office hours. (This is a particular problem on SCADA sites such as power utilities, where there isn't always a way of mitigating the impact of a loss of service even by load sharing or switching to a backup system.) An exception can be made in the event of very severe or very urgent vulnerabilities. It is in all cases advisable to warn users in advance that an update will be installed, because an unanticipated issue could affect the functionality of programs in use, or might even cause a malfunction that results in an inability to continue working. It is also wise to make a backup of the pre-patch configuration and software before installing an update, so that it's possible to roll back to the previous state of the system if there are compatibility problems.
6. *Rolling out the patches*. This is not always just a matter of distributing patches to servers and end user devices. Often it is wise to do a full antivirus scan before deployment to avoid problems. The authenticity and integrity of the patch must also be checked in order to be sure that no error occurred during the download of the update.
7. *Verification and logging*. Do not blindly assume that the installation of the patch onto all systems went smoothly. It is a good idea to check that the version number of the patched software has indeed changed and, indeed, that the vulnerabilities are no longer present. Also, to check afterwards whether problems have occurred when rolling out the software. Involve the end users in the evaluation, too. Can

they still carry out their work properly after the update? And could anything have been done to make the process smoother and more efficient?

After the seventh step is completed, it's time to start immediately with the first step again. Patching is more than just a one-off process, it is a continuous cycle. Fortunately, it's one that can, to a large extent, be automated with the right software.

9.6 The Greatest Danger Often Lurks Within Your Own Walls

A company may spend millions on protecting its network from outside attacks, yet even then it may be anything but safe. Unfortunately, many risks to the IT infrastructure and to corporate data still emanate from our own employees and those of third parties who may have access to the internal network. . . No doubt there isn't an IT or security manager in the world who isn't concerned about the risks from "attackers from the inside" and asking themselves the question: how can I protect my company? A complicated issue, but one that must always be taken into account.

To protect your corporate network effectively, you first need to know the potential risks. In general, insider threats can be roughly divided into two categories: On the one hand, unfortunately there may be unscrupulous data thieves among your own employees, who could deliberately abuse and sabotage the company's internal infrastructure. And on the other, there are those who might unsuspectingly give assistance to attackers. There are some technical defenses available against the first category, making as much use as possible of monitoring and logging tools and strict security practices. But people belonging to the second category are at least as dangerous, their innocence notwithstanding, and they are much more numerous.

Anyone at all might, sooner or later, be involuntarily drawn into taking part in a malicious attack. Perhaps by opening an email that looks normal but contains a link that sends you off to an infected site. Perhaps by providing (through email) confidential information to someone they think they know, but who later turns out to be someone else. Perhaps through some other form of social engineering (see above), whereby the attackers accumulated, piece by piece, enough information about an employee and his working environment to gain his trust. Sometimes this takes weeks or months, and they can compile a complete "dossier" based on their own research, perhaps with the unsuspecting assistance of colleagues and loved ones. As the proverb says, patience pays dividends. In this way they push open the door an inch at a time until it is wide open. For sure, it's just a matter of time before these criminals strike and make use of the information they've gathered for their unsavory purposes.

A company can protect itself only if a solid and comprehensive security policy is implemented (see Sect. 9.1) in combination with an active process of raising awareness across the entire company about security issues that may affect staff.

By doing so, you can ensure that everyone can understand why certain restrictions apply, for example, as regards data traffic or Internet access (see Sects. 9.1, 9.3, and 9.5). Incidentally, this educational process must be repeated regularly, because nothing is forgotten as quickly as a message that you really do not want to hear.

9.7 Attend Security Conferences

There is no better way of keeping yourself informed about all aspects of cybersecurity than a good security conference. For someone who is not occupied with security issues day in and day out, this advice may seem a little over the top, but believe me, it's really worth the effort to ensure that someone is tasked with attending a conference, sharing all the information they've gathered, and maybe helping to initiate actions based on what has been learned. In just a few hours you may get insight into all the security topics that are relevant to you, learning about all the current serious threats and all technologies and methods available to combat them. In addition, these events provide a wonderful opportunity to expand your personal network of experts that you can turn to when you need help and advice.

Which conferences are suitable for laymen as well as for experts? Probably the most important and interesting conference is the one organized every year by Virus Bulletin (www.virusbtn.com). The organizers manage like no one else to build a bridge over the yawning chasm between technology geeks and management, which is why the conference appeals to a very broad audience.

The RSA Conference (www.rsaconference.com) is also suitable for everyone from geek-level to C-level and is in consequence attended by huge numbers of people. The only drawback is that lots of events take place at the same time, so it can be quite painful to choose between them. However, you may be able to catch up with videos of some of the more major presentations later in the event, or even on the Internet.

The EICAR conference (www.eicar.org) is somewhat more exclusive and also somewhat smaller but also lends itself to more in-depth discussions. EICAR therefore has a slightly more academic image. While EICAR is only holding small workshops at time of writing (the last full-blown conference was in 2016), the Board has stated that there are plans to relaunch a refurbished version of the conference in the future. Finally, if it makes sense for you to combine such a conference with a business or personal trip to the (Far) East, I can definitely recommend a conference (www.aavar.org), organized by the Association of anti-Virus Asia Researchers (AVAR), the Asian equivalent to EICAR. Black Hat also deserves a mention, as a conference where malware hunters and *"ethical hackers"* meet, with offshoots in other parts of the world if you can't get to Las Vegas. Though you might want to consider keeping your laptop turned off while you're there. ☺ CARO holds a yearly and highly technical workshop intended for the sharing of information between legitimate researchers. The press is not invited, and public discussion of content, for instance, on social media or industry blogs, is not

permitted. However, it's an excellent source of information for those with sufficient technical knowledge.

I should also mention Infosecurity Europe, which brings together many security providers and experts and includes many theater and booth presentations. This trade fair, originally mostly UK-focused, has now also become a fixture in the Netherlands and Belgium, among other venues.

Chapter 10
The Role of Government

In the struggle against terrorists, cybercrime, and crime in general, governments and state agencies often rely on intelligence in the form of espionage. And more and more espionage (and counter-espionage) takes place online, as I have already extensively demonstrated in Chap. 4. In this chapter we'll look at how espionage works on both sides of the divide between Good and Evil, embodying both sides of a single coin: Espionage can be associated with a cyberattack (and that may be what you first think of in terms of cyberespionage), but it's also part of the way we defend against such attacks. This is not the least of good reasons that the role of espionage in both attack and defense will always give rise to controversy.

10.1 Espionage and Privacy

The so-called NSA affair (also referred to as the PRISM affair), emerging at the time when I was writing the first edition of this book, left many people open-mouthed. The revelations of Edward Snowden, a former employee of the CIA and contractor for the NSA, made it public that the NSA and FBI had agreements with companies such as Google, Apple, and Microsoft, who cooperated by allowing the security agencies to search their databases in order to detect and thwart possible plans for terrorist attacks. The spectacular announcement that the US government was seeking information from giants in the world of the media and information, in its search for enemies of the state, caused a commotion all over the world. The "whistleblower" Edward Snowden's flight to safety was followed with enormous interest across the world.

Much of this excitement was completely overblown, in my view! For me it has always been clear that the US government—like all other nation states with the contacts and capabilities—would be making use of these resources. What's more, it would be very surprising if cooperation between the US government and corporations was limited to the nine most often mentioned (in addition to those already

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_10

referred to above, these are Facebook, Yahoo, Dropbox, AOL, and Skype). It's to be expected that other companies are cooperating in this way, as has indeed been confirmed in subsequent Snowden revelations.

Just try googling for information about a certain person yourself, or via another regular search engine: by doing so you launch a simple data mining program, and from that you may also learn more than you expect, though privacy regulations in Europe have had some impact worldwide on the (lack of) privacy free-for-all. Datamining software is technology that allows you to delve into a mountain of information for specific information or for connections between specific data items that enable you to pick out trends. Using simple and publicly available software, you can obtain large volumes of data on celebrities, but also on mere mortals like the rest of us. It's safe to assume that the state still has very different and far more modern and effective means to screen and monitor its citizens. The insights gained in this way can certainly cause you to see someone in a very different light.

You may well find this regrettable and oppressive and wonder whether it doesn't violate privacy principles and regulations—such as European data protection legislation like GDPR—and the citizen's privacy rights. But espionage has been around for centuries, and privacy concerns have never been a priority for those who initiate it. It is sometimes argued that espionage should *not* take privacy into account, because otherwise the government will never be able to meet its security obligations efficiently and effectively. The American security service, the NSA, has gone so far as to state that without the information it has acquired covertly, it could never have prevented many of the attacks that they claim to have stymied. "What do you prefer," asks the NSA, "to protect the privacy of people under suspicion, or to protect the lives of innocent civilians?" Furthermore, privacy legislation varies from country to country, but spying knows no borders, so privacy and espionage will always be in conflict with each other (Fig. 10.1).

Perhaps the truth of the matter is this: rather than being a stark choice between privacy (as espoused by fervent libertarians) and the paternalistic advocacy of state-managed surveillance (as preferred by so many politicians), the answer lies on a spectrum between the two extremes, even if that means perpetual controversy and continuous calibration to ensure the best possible outcomes for the population in general.

Apart from the abstract ethical and philosophical aspects of this case, we should ask ourselves the question "what can we do about this *ourselves*?" You can find the answer to that question in Chap. 8, offering tips for individual users on achieving a safer online existence, but it can be tersely summarized as follows: if there are things you do not want the government (or others) to know about you, it is better not to talk about them online. In that chapter, I also advocate media training for everyone: I hope you agree that we could all profit from a training and awareness course that explains what happens when we do post something online, how it can continue to haunt us for the rest of our lives, and—in certain very specific cases—how you can be more aware of how and why the government takes so much interest in you.

The choice is yours: the only important thing is that you make a very considered and informed decision, after you have thought carefully about everything.

Fig. 10.1 Child to Obama: "My dad says you can look at my computer." Obama: "He isn't your dad."

Granted, it's very tempting to take advantage of the opportunities offered by the Internet to express our opinions to a wider audience, in blogs, in forums, or on social networks. It's one thing to comment on the latest headlines, but you can also make your private life very public with thousands of photos and movies on Instagram, YouTube, or Pinterest. In these ways, anyone can easily become a "media star." But are we really ready for that? In my opinion, 99.9999% of the population cannot begin to handle the role of a public person or media darling, and they do not realize what impact their words or images can have, not only on other people's lives, but also on their own. Even people working in the security sector sometimes have problems correctly assessing their actions on the Internet. Recently, I learned that the employee of a security company posted a photo of his car on Facebook, where the license plate was clearly readable. Such carelessness is not conducive to protection of privacy: to me, this seems like an open invitation to misuse personal information. If even so-called security experts can make such serious errors, you can imagine how easy it is for the rest of the Internet-using population to slip up.

In summary: privacy is a great asset, will always exist as a desirable aim, and is worth fighting for. But if you consider it important to protect your precious data, you must do the bulk of the job yourself: nobody else can do it all for you. Be discreet in what you post online, and careful with regard to what technology you use. For example, Google makes it possible to have your house blurred on photographs that

can be seen on Google Street View. If your privacy is important to you, you should take advantage of this offer. Others may see things differently and might consider it to be important for would-be burglars to see through this medium that their houses are well protected because they have a modern alarm system. Criminals may then think twice about whether they want to risk carrying out a burglary there. The choice is yours, dear reader, but I think you should be fully aware of the pros and cons when you make that decision.

In the Words of
Richard Ford, Chief Scientist, Forcepoint

Personal Data, Cybersecurity, and the death of Privacy. . .

When we think of our own personal data, we tend to think of it as present, controlled by us, shared carefully and thoughtfully with a few friends. However, in today's computing ecosystem, nothing could be further from the truth. Each click we make is analyzed, each website we visit logged. Data aggregators look carefully at our activities for various purposes, ranging from the benign ("I think Richard would really be interested in this advertisement") to the malicious ("Knowing what I know, I think I can spear-phish Richard with this custom-made email"). And all because our data is out there, more widely distributed than we could ever imagine.

You might be wondering what this has to do with cybersecurity—isn't this purely a privacy issue? I would argue that these topics are closely related, though the fact that we don't see them as such is actually a symptom in and of itself. For better or worse, when we think about security, be it commercial, government, or personal, we tend to forget that security is a means to an end: we want our data to be confidential (keeping our secrets secret), available (there when we need it), and to have integrity (that is, what's stored is what we meant to store, not modified artificially and without authorization). When we forget that end, we lose sight of *why* we do what we do with respect to protection—and the breadth of the threats from which we need to protect ourselves.

To that end, one of the biggest challenges I see today with respect to the digital ecosystem is the astonishing amount of personal data that is available about anyone, anywhere. Astonishing because while some of it has made its way into the public domain because of a breach, much of it was knowingly given away by the data owner (you!), in exchange for browsing the web, sending a free email, or playing a game on your mobile device. We can't think about personal data without recognizing that the problem is broader than just a security issue—it's also an opt-in and ecosystem issue, whether you know it or not.

From a threat perspective, it seems that the rapid evolution of analytics and personalization of content has set security on a collision course with privacy, and is forcing us all to think more holistically about who owns our personal

(continued)

data, how it is stored, who can access it today, and, perhaps most importantly, who should be able to access it in the future. It's this explosion of personal data that I consider to be one of the biggest long-term threats we face in today's world—and that has significant implications for cybersecurity.

First, data holders are slowly coming to the realization that data is both an asset and a liability. An asset, because it can be used in a myriad of ways and has considerable value. A liability, because there is a cost associated with holding it, protecting it, and (as we see in breaches) losing it. Thus, for data aggregators, protecting the data they hold from unauthorized eyes is the Number One Job. That's one of the most important parts of their security stance, and doing this is expensive—it's a more data-centric (rather than threat-centric) way of looking at the world so it is a new approach for some defenders. GDPR has helped shed light on the strange world of data for most companies, but compliance is just a starting point here, not the conclusion.

Second, more focus on the question of who owns data can lead to security problems, too. For example, security researchers rely on a large amount of end-users' information (telemetry) pulled from the field. The average security researcher has no interest in a particular user or the websites that she visits, for example, but the same data is incredibly useful for detecting new threats. Thus, there's a tension between enabling privacy and security here. We have already seen researchers struggling with changes to how information about domain registration is released as a side effect of GDPR. We'll likely see more impacts on security research due to a tighter rein being kept on data sharing, and while on the one hand it's good that we're being more mindful, it's important that we don't inadvertently make life easier for the attackers. It's very much a question of balance.

Third, we need to open our eyes to the fact that some of the most damaging breaches are those carried out by a malicious insider. Thus, protecting the privacy of the *many* causes a potential impact on the privacy of the *few*, as the best way to detect and mitigate insider threats can have privacy implications for those who operate on the data. Balancing the global good here will be difficult, and we are going to have to innovate to really comprehend how best to achieve it.

When we put this all together, we see a significant reckoning coming—where data that is already shared begins to have larger impacts. While we will continue to see laws such as GDPR provide a legislative framework for privacy and ownership of personal information, the situation remains very fluid—and will likely be addressed more by societal mores than in the court room. However, when we think of our privacy, we must remember the story we began with above: the data we share today will still be around tomorrow, and the implications of that are very unclear indeed.

(continued)

Dr. Richard Ford is the chief scientist for Forcepoint, overseeing technical direction and innovation throughout the business. He brings over 25 years' experience in computer security, with knowledge in both offensive and defensive technology solutions. During his career, Ford has held positions with Virus Bulletin, IBM Research, Command Software Systems and NTT Verio. He has also worked in Academia, having held an endowed chair in Computer Security, and worked as Head of the Computer Sciences and Cybersecurity Department at the Florida Institute of Technology. He holds a Bachelor's, Master's and D.Phil in Physics from the University of Oxford.

10.2 Malware and Espionage

Of course, it is quite another matter when malware is used to spy on (harmless?) citizens on the pretext (or even with the sincere intention) of combating crime. Over the past few years, there have been repeated reports of covert online searches and surveillance of the public, where it's clear that government agencies had some involvement.

In fact, we have already seen a whole series of espionage activities that we know to have been executed by—or on behalf of—a government: for example, it became known that the German police, with the approval of the courts, used the so-called *Federal Trojan* or *Bundestrojaner* (Trojans commissioned by the German government) to spy on computers used by suspected criminals. Subsequently, it was revealed that the Germans had also ordered spyware Trojans from the British software builder Gamma Group, and the technical and legal ramifications were much discussed at various conferences, some including representatives of the Belgian and Dutch police.

This spyware was called FinSpy or FinFisher, and research from early 2013 shows that this package was already active at that time, in the form of C&C (Command and Control) servers in more than 35 countries. The most striking

Fig. 10.2 Gamma Group website promoting FinFisher

thing is that Gamma Group makes little effort to conceal its activities, as you can see on their homepage: FinFisher is openly offered as part of their product portfolio (Fig. 10.2).

Let's face it: the state and the surveillance sector of the security industry rely on spyware. It says a lot about how governments and the industry in question look at espionage software: as a legitimate and necessary evil with which to fight the enemy, in the same category as tanks and other military weapons. And, as you might expect, in the meantime FinSpy/FinFisher is also being used by less democratic states to spy on dissidents, as revealed in investigations from security experts and seen, for example, in Bahrain.

All known cases where FinFisher has been used have two elements in common. Firstly, the government concerned makes no secret of the fact that it is using the software because it is operating within its own legal framework. Second, mainstream anti-malware detects and removes FinFisher and similar packages. Those of us working in the antivirus industry cannot distinguish between malware created and used by cybercriminals and malware developed "legitimately" on behalf of the state, even if we considered it appropriate to treat them differently. If we did, then before you could count up to three, that "legitimate" software would be misused by other parties to develop malware with criminal intent, and for all our good intentions it might then be able to slip past our defenses via security vulnerabilities or the naivety of some computer users.

We therefore consider it our duty to detect and intercept malware even if it's "legitimate." For example, do American anti-malware vendors not run the risk of their government asking them to turn a blind eye to malware built for American intelligence and law enforcement agencies? Hopefully not, because such malware is by definition international, and antivirus companies outside the United States will cheerfully report this malware if they detect it, and if that happens the American anti-malware suppliers will sustain a black mark against their reputations. Will other governments try to control how suppliers in their own countries detect government spyware? I have never seen evidence of this in all the years that I've worked for the anti-malware industry. Sadly, such actions cannot be altogether ruled out. In the United States, for example, since the introduction of the so-called Patriot Act, it might be used to force US security companies to cooperate with their intelligence services in case of doubt. Consider, after all, the controversial and ongoing legal tussles between law enforcement and providers over access to passworded cell phones.

In other countries, such draconian measures might be taken as a matter of course. Or, at any rate, assumed to be the norm. In 2018, we've seen such assumptions made about Kaspersky Labs, to the point where other governments have stopped their own agencies and departments from using their products. This mistrust has even spread to the private sector. Late in 2017, for example, Barclays stopped offering free use of Kaspersky software to its customers as a "precautionary decision" (see https://www.bbc.co.uk/news/uk).

While the mainstream anti-malware industry sees this sort of speculative mistrust as largely misplaced and ill-informed, other sectors of the security industry added fuel to the controversy in the wake of the Snowden revelations in 2013. A somewhat presumptuous open letter to the industry required antivirus companies to respond in order to meet an arbitrary deadline. Several major companies did so, fairly politely considering the illogical and somewhat biased tone of the letter hinting that a non-response would be seen as an indicator of government interference. In general, the responses could be summed up as:

- Yes, we've detected surveillance software alleged to have been distributed by government agencies, though it's not usually possible to attribute the source of malware definitively.
- No, no government has asked us to give certain malware a "free pass" by not detecting it or by not flagging it to our users.
- No, we can't give details of such requests since we haven't received any.
- No, we wouldn't comply with such a request if it was made.

Some companies went to some lengths to explain (with good reason) why it would make more sense for a government agency to *avoid* asking for special treatment. However, it's likely that many people looked at these responses in terms of "Well, they would say that, wouldn't they?" Which is one of the reasons the open letter was never likely to be really helpful. It's likely that some companies only responded because if they didn't, they would have expected to be assumed to be collaborating inappropriately with government agencies.

10.3 Knowledge, Ignorance, and Bad Practice

Sometimes, legitimate messages and software are delivered using characteristics normally associated with malware: indeed, it's the bad practice sometimes used in the banking industry that makes phishing so effective—sometimes a badly executed but genuine message is indistinguishable from a phishing message. On the other hand, it's also not uncommon for legitimate agencies to use the same techniques and patterns that the bad guys use. This is illustrated by the following story from a few years ago. . . I was approached by the Dutch High-Tech Crime Unit (the government body specifically tasked with fighting cybercrime) to investigate the so-called Shadowbot, a newly discovered botnet. This looked like becoming an interesting collaboration between government and industry, until it came to what they were planning to do with this botnet: they intended to pop up a message on all contaminated devices indicating that they were indeed infected and posting a link to a place where they could complain, register, and download a file at the same time to get rid of the infection. Very noble in intent, perhaps, but to combat the evil, they used the same means as the malware writers themselves: displaying unsolicited messages on a device, blocking the system until they had performed a certain action which could easily have involved accessing a dubious site. In many jurisdictions, these actions would be prohibited by law as constituting "unauthorized access" and "unauthorized modification." That was the first time I saw this happening, but certainly not the last. Recently, the FBI called on Microsoft to fight the Citadel botnet in a similar way. In this case, even IP addresses were modified so that they sent the user to a Microsoft security site instead of to Facebook.com.

This approach chills me to the marrow, because I wonder what consequences this approach might have. Is it really justified to use the enemy's weapons to fight him? Where do we draw the line? Is it permissible to break into someone's house and even take them hostage in order to save them from a "real" criminal? To put it bluntly, how can one differentiate between good and evil?

How *do* you tell the difference between a real hostage taker and a government agency? Do you think this is a hypothesis too far, or that I'm exaggerating the risks and implications? Then think back to the eCops ransomware that I described in detail in Chap. 5. This malware used exactly the same procedure to persuade unsuspecting victims to pay up, blocking access to the victim's computer with a screen that popped up and explained how to get that blocking reversed. The only difference was that the ransomware demanded a payment, whereas in the Shadowbot incident, the victim was forced to pay a visit to a security site. But for the unsuspecting user, that difference is not always clear. Instead of making use of the same techniques as are used by malware, the government could make better use of its resources by doing a better job circulating the necessary information to the population in general to enable them to take better self-protective measures. Breaking into a computer to perform such activities, however well meant, is not only unethical, it is also punishable by law in many instances, depending on which country you are in.

10.4 Legislation, Execution, and Punishment

Sometimes a government also shows its positive side, taking effective and legitimate action against cyberthreats and the criminals behind them. Despite breaches of privacy and the use of malware to protect state interests, less controversial overt actions against cyber-hazards are also being taken. An example of this is the European Union directive 2013/40/EU on the harsher punishment of hackers. Since the directive came into effect, offenders can expect at least 2 years imprisonment if convicted. Companies that hire hackers to bring down a competitor's website or IT infrastructure can not only be fined but might even be closed down. Bot herders and botnet operators can expect sentences of not less than 3 years in prison. Damage to a country's critical infrastructure or corporate systems can carry a penalty of up to 5 years. These recommendations show that we are on the right track. Nevertheless, as long as corresponding laws are not implemented worldwide, there will still be scope for cybercriminals to operate almost unhindered, believing that low penalties make for low risks.

The directive even goes one step further: every EU country is required to be able to respond to requests for help from other member states in the event of national cyberattacks within 8 hours. This demonstrates that the EU is preparing itself for all eventualities in a spirit of international cooperation. However, it will take several years for these good intentions to be translated into concrete legal measures in all countries. Unfortunately, community-wide (let alone worldwide) enactment continues to be a slow and laborious process.

In the Netherlands, a bill was passed on the immediate reporting of industrial harassment, whereby every company that is hacked must immediately report the incident. If a company fails to do so, it can be fined up to 450,000 euros. There is also a similar initiative at the European level. Telecommunications companies are required to report data breaches within 24 hours, and the details of these breaches will then have to be made available within 3 days. Unfortunately, these praiseworthy advances fail to take two essential issues into account. The first is that a hack is not always visible, so a company can be hacked without realizing it. It may therefore be a bit excessive—unjust, even—for an organization to be fined under such circumstances. The second is that the fine may, for large companies, have less impact than the damage they incur by reporting a hack—bad publicity and reputational damage, loss of revenue when customers migrate to the competition, and so on.

It's different when the law pursues real cybercriminals. But even here, before fines or even imprisonment can usefully be imposed, every single case must be thoroughly investigated so that arrests can be made. Here, too, we have seen positive signs. The media have already reported on cases where investigators have scored successes against individual cybercriminals or groups. Consider, for example, the arrest of a hacker who hacked into Canadian singer Carly Rae Jepsen's account, hoping to be able to find nude photos of her to sell to the tabloids. Or the action taken against the operator of the Zeus botnet, who made about US$20 million through his schemes. Another spectacular case concerned the arrest and conviction of Dutch cybercriminal David Benjamin Schrooten, better known in hacking circles as Fortezza. He was sentenced to 12 years behind bars when convicted of identity

theft and credit card fraud involving the theft of more than 100,000 credit card numbers. Schrooten was arrested in Romania and extradited to the United States.

The requirement for appropriate sentencing and the punishment eventually imposed can sometimes diverge widely between individual legal systems. Thus, the prosecutor in a US court demanded a prison sentence of 105 years for a cybersex offender. "Gary" Kazaryan, as he called himself, had not been out for monetary gain. He blocked the accounts of his victims, then went in search of nude photos or other incriminating or embarrassing material, then demanded that his victims do a striptease in front of their webcam. After he pleaded guilty, he was sentenced to 5 years in prison.

Hacktivists are no longer safe from the judiciary, now that courts are often empowered to pass much harsher sentences. Two British hacktivists involved with the Anonymous hacking group received respective sentences of 7 and 18 months in prison for their DDoS attacks on PayPal, MasterCard, Visa, and others. Some considered this a relatively harsh punishment, considering their relatively innocuous motive was dissatisfaction with the way in which these sites made it difficult to raise money for WikiLeaks. The makers of the Spanish version of the eCops ransomware were also arrested after using their malicious software to loot around 1 million euros, which is about equivalent to 100 euros per victim.

The hacker who stole and published nude photos of—among others—Scarlett Johansson also received a hefty punishment: 10 years in prison, even though the public prosecutor had only demanded 6 years. A striking detail of this case is that he was able to get hold of the account information of more than 50 celebrities simply by clicking the "forgot password" button and answering some simple questions with information easily found with a little help from Google.

In 2016, the co-authors of SpyEye, sophisticated malware said to have been used to steal around US$100 million (https://www.bbc.co.uk/news/technology-36101078), were sentenced to 9½ and 15 years in prison, respectively.

Scan4You was a sort of "anti-antivirus" service: it worked in much the same way as legitimate multi-scanning sites like VirusTotal, but instead of sharing its data with security companies, Scan4You enabled malware distributors to tweak their creations until they were no longer detected by anti-malware products. According to the US Department of Justice, parts of its functionality were even incorporated into the Citadel malware toolkit. As of September 2018, one of the people behind it is about to face a sentence of up to 35 years.

From the Diary: Meeting with the State Security (2 May 2008)
Even before I started working for a manufacturer of antivirus software, I had regular informal contact with the Belgian State Security Service. A short time later I began working for Kaspersky Labs, whereupon that contact lapsed for a while. Since you never know when such contacts may come in useful in the future, I decided to arrange a casual meeting. Over a pizza I once again got to hear about the state of affairs in the world of security and offered my counterpart the opportunity to discuss some important current issues. Among

(continued)

other things, I was asked if I knew who was responsible for certain attacks on offices and authorities in Belgium. I agreed that it could well be China, although there was no tangible evidence of that.

Just two weeks later, on the 2nd of May 2008, I heard on the morning news that State Security had publicly stated that China was certainly responsible for these attacks. Apparently, my opinion was enough to substantiate the agency's guesswork. To me this seemed a very slapdash way of working, and in conversations with the media, I made it clear that I could not confirm this accusation, that the position was not as clear as State Security had suggested, and that they might have overstated their case. Since then my opinions have not been of interest to this particular authority.

In the Words of . . .
Nikolaus Forgó, Professor of IT Law and Legal Informatics and Head of the IRI

What James Bond teaches us about IT security law

James Bond films are a good example of a particular film genre: The hero is in a foreign country—at best indifferent, often hostile—and once there must take arms against a sea of troubles in order to track down ruthless criminals who want to bring about the end of the world, or bring about some other unpleasantness. It is only reasonable in such extreme circumstances that James need not be squeamish in his choice of weapons and should not be required to stop for too long to consider the question of whether the use of an agent on the scene is permitted. Where would we be if, every time the agent wants to use a flamethrower or one of Q's Wonder Weapons, he has first to debate whether he is allowed to have such a thing in his possession. The next scene would be endangered or indefinitely postponed because the hero is trapped in bureaucratic insanity (who wants to see Sean Connery filling in forms?) or dead. It does not matter that James is not hassled with these unpleasant details, because he has unquestioned, limitless authority to act on behalf of his homeland, including (of course) his 'license to kill'. This concept of limitless authorization is an essential subtext to the films: it allows the agent to assert his own values and overcome all resistance—even in countries that are hostile or indifferent or just too incompetent to do the Right Thing—and thus promotes the sense of survival of the fittest, and the right of the technologically superior Good to overcome Evil. At the final credits everything is fine ("turned out nice again") and his country is once more top of the heap.

The Edward Snowden affair reminds us of the very simple insight that James Bond exists in real life and can be found everywhere, though (presumably) agents usually lead a less glamorous, less sexually active and in general

(continued)

much less exciting everyday life. However, what they have in common with James Bond is that—hopefully—they are committed to abiding by the norms of their country of origin, but not necessarily to those of the state in which they carry out their activities. Secret services are *called* secret services because their actions are required to be secret and unhindered by legal conflicts. Proceedings against their own secret agents are rare occurrences in Western democracies.

James Bond thus illustrates a problem intrinsic to the legal system: norms can only formulate commandments, in the sense of moral or quasi-moral imperatives; create behavioural requirements; and threaten sanctions in the event of their non-observance. They can (ethically speaking) appeal to what is perceived to be good, threaten (in religion) with eternal damnation or (in law) provide compensation to the victim or impose penalties on the criminal. But those who consider themselves to be outside the reach of the law do not feel the need to obey. All too often, they are all too justified in thinking that the risk of getting caught is not great.

Law can never be the complete answer to the disastrous issues and weaknesses in IT security, which Snowden (again) made so obvious to us. The usual knee-jerk reaction is to call for more and stricter norms, but these will be ineffective unless mechanisms are created to help enforce those norms. Increase of penalties, creation of a new offense, rewritten IT security law and similar (symbolic) legal policy activities are not sufficient, because all these legal instruments do not in themselves provide protection from who choose to disregard them.

The answer must be a combination of measures, including raising awareness with education; technical, organizational, political and ethical measures that take into account non-compliance as a risk; and evaluating and responding to that risk accordingly. The prerequisite for an effective array of countermeasures is a realistic analysis of the situation, not an unthinking, reflexive call for legislation which is more symbolic than actually useful.

(continued)

Professor Doctor Nikolaus Forgó was born 1968 in Vienna, Austria, and studied law in Vienna and Paris. Between 1990 and 2000 he worked as an assistant at the Institute of Roman Studies in Law, and as IT instructor in the Faculty of Jurisprudence at the University of Vienna. Since 2000 he has been Professor of IT Law and Legal Informatics at the University of Hannover; since 2007 he has been the head of the Institute for Legal Informatics (www.iri.uni-hannover.de); and since 2011 he has also been a member of the L3S Research Center (www.l3s.de). Nikolaus researches, teaches and advises on all IT-related legal matters, with a focus on data protection and data security. He regularly advises public institutions such as the European Commission, the Austrian Parliament, the German Ethics Council and various Austrian and German ministries on IT issues.

10.5 CERTs, CSIRTS, and CCUs

I would like to finish this chapter with a few words about professional cybercrime hunters like CERTs *(Computer Emergency Response Teams)*. **CERTs** are necessary, useful, and do a good job. They keep track of the cyberthreats seen in everyday life and try to respond swiftly to violations of the security of computers and networks. Their goal is to prevent crime and minimize possible damage. However, a CERT does not *only* act when cybercrime has already occurred but also acts in the area of prevention. CERTs owe their name and inspiration to the CERT Coordination Center at the Carnegie Mellon University's Software Engineering Institute in Pittsburgh. Sometimes we speak of Incident Response Teams, which are often labeled as CSIRTs *(Computer Security Incident Response Teams)*. Originally, CSIRTs were more focused on incident response and less on prevention, but the two terms are now used more or less interchangeably. Figure 10.3 shows current CERTs and CSIRTs in Europe, as of 2013. But they are also to be found in the rest of the world, notably US-Cert and CERT/CC in the United States, CanCERT (Canada), CERT-In (India), and AusCert (Australia) (See also the interactive map of CSIRTs and CERTs at https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map).

Worth mentioning in this context is the **European Agency for Network and Information Security Agency (ENISA)**, the source of the interactive map mentioned in the last paragraph. The task of this collaborative initiative is to ensure that information networks, and the data sent over them, are protected from unauthorized access by third parties. This is of enormous importance for all citizens, businesses, and governmental institutions in Europe. In fact, you might see this as a transnational body of European CERTs.

We should also consider the "cyber-police" or more properly the "High-Tech Crime Units"—or, for short, "CCUs" (Cyber Crime Units or Computer Crime Units). By now there are CCUs in nearly all countries, but some work more efficiently than

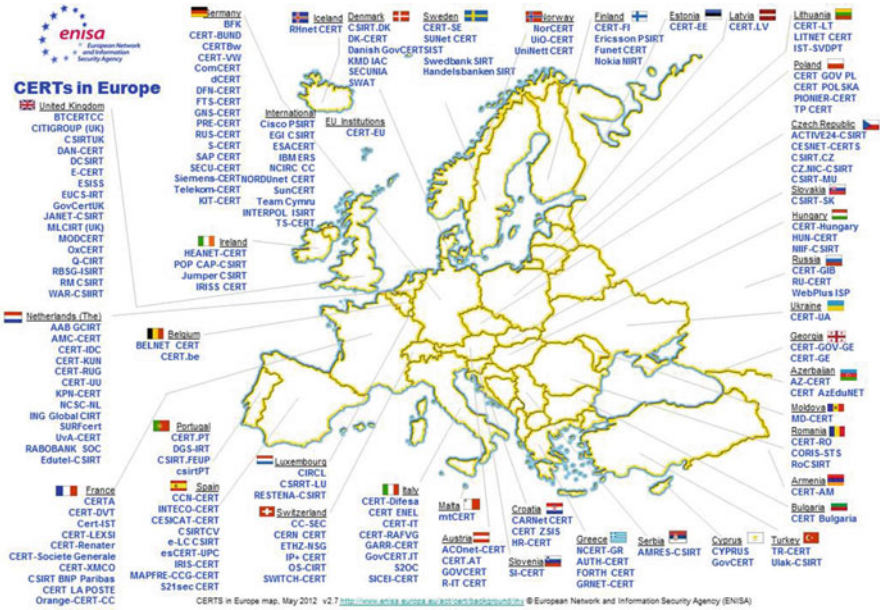


Fig. 10.3 CERTs in Europe

others: not all are fully resourced with qualified (and specialized) staff. Examples of very professional units performing well in the fight against cybercrime are the US Federal Bureau of Investigation (FBI), the Dutch National High Tech Crime Unit (NHTCU), the UK's National Cyber Crime Unit (NCCU), and the German Bundeskriminalamt (BKA), who are all already arresting as many cyber criminals as they can lay hands on.

In the meantime, many countries have moved to a national cyber-strategy, which is primarily intended to protect their own infrastructure from possible cyberattacks. Some countries implement the appropriate measures in an exemplary manner, but unfortunately there are other countries still encountering difficulties in getting it right. In early 2013, the European Commission (EC) launched its European Cyber Strategy. Smooth cooperation between member states is crucial, especially in the fight against cybercrime. This is because if a country is attacked via the Internet, rescue is often only possible through solid alliances and with the support of neighboring countries. It will, however, take years for this strategy to be harmonized and for all Member States of the European Union to cooperate in countering attacks.

Fighting against cybercriminals is only one aspect of a comprehensive strategy to protect cyberspace, though it's by no means unimportant. The protection of cyberspace itself is the other task that is inextricably linked to cybersecurity and protection of the community. You don't leave your automobile parked with the doors open, in the expectation that the police will catch anyone who might intend to steal it. But, having locked the doors and done your best to protect the vehicle, you *do* expect the

police to try to track down and punish criminals if they *do* manage to break into it, and so you should. It's the same with cyberspace: of course you should take all reasonable steps to protect yourself, your family, and your property. But that doesn't mean that the State—or its appointed representatives in law enforcement—has no part to play: it is there to seize and punish offenders.

I'd like to end this section with a few words about the need all countries have for specialized cybercrime fighters, such as the CERT (Computer Emergency Response Team) in Belgium, and the NCSC (National Cyber Security Center) in the Netherlands. Both organizations are necessary, useful, and do a good job, just as similar and higher-profiled organizations in larger nations do. It's a sign of the times that in general, budgets for such initiatives are being increased in the larger countries. While it might reflect a societal malaise, at least the willingness to address the issue is healthy, given the increase in cybercrime.

- NATO leaders adopted a Cyber Defense Pledge at the NATO Summit in Warsaw in July 2016, as a way of underlining their commitment to strengthening national infrastructures and networks (https://www.nato.int/docu/review/2017/also-in-2017/nato-priority-spending-success-cyber-defence/en/index.htm).
- In May 2018, the UK government announced that it was investing £1.9 billion in cybersecurity as part of its Cyber Security Export Strategy, expecting the size of UK cybersecurity exports to rise from £750 million in 2017 to £2.6 billion by 2021 (https://www.newstatesman.com/spotlight/cyber/2018/05/why-uk-investing-19bn-cyber-security and https://www.infosecurity-magazine.com/opinions/government-policy-regulation/).
- In February 2018 the US government proposed to spend US$80 billion in IT and cybersecurity spending for federal agencies and US$45.8billion for civilian agencies (https://fcw.com/articles/2018/02/12/budget-johnson-overview.aspx). It's good to know that cyberspace security will be getting some money, and not just the space force.

Even if they can't match these big budgets, smaller countries like Belgium and the Netherlands need to react to the threat as effectively and efficiently as possible.

But where will it all end? Will even the largest investments be enough to stop everything that threatens us? I doubt it, but that's not a good reason to avoid doing whatever is practical to reduce the impact of all those threats.

In the Words of
Righard Zwienenberg, Senior Research Fellow, ESET

The threat today and the role of the government

It is old news that the greatest emerging threat today is from the world of the IoT: the Internet of Things. Interconnected devices are to be found everywhere. If you haven't heard of the IoT or any of its problems, most likely you have not been online in the last year, nor did you follow the news.

(continued)

Cybercriminals are exploiting these IoT devices right now. There are massive botnets comprised of these devices that have been surreptitiously harnessed for various tasks, such as stealing credentials, performing DDoS attacks, or the many other undesirable acts the authors want to accomplish. And since security vendors have hardly any access to (or worse, no insight into) these devices, securing them (if that is possible at all, given how cheaply they are designed and produced) is usually limited to external protection on the wire, trying to stop inappropriate communications. In the worst case—but as most commonly happens—there is no way to truly eradicate the malware from the device. Usually a device reboot (or setting it back to factory settings) will do the job in the short term, but as there is often no possibility of properly securing the devices against the attack, they are bound to be reinfected, in the same way that when an infected operating system is restored from a backup without also immediately applying available security updates, reinfection is almost inevitable.

We are in need of regulation here. Governments around the world have created (tax) laws for (or against) cryptocurrencies and offshore online stores (as these affected their income streams) and are creating laws about net neutrality to ensure the consumer has freedom of choice. However, there is a lack of legislation protecting those same consumers from the threats emerging from the proliferation of devices connected to the internet and the welcome given to net neutrality.

In mid-2018 we know of a few governments that have independently started to create laws around IoT devices and the security thereof. These laws, however, are not unified. If that is not addressed—and soon—we will end up lost in a maze of laws where a device, or misuse of a device, or the lack of adequate security functionality on a device, is prohibited by law in one country while it is completely legal in others.

Why is it important for governments to create unified rules in relation to these devices? Apart from the ease of enforcing these rules across international borders, as already hinted, all governments are in the same boat, increasingly susceptible to cyberthreats as more and more control systems for their critical infrastructure come either directly connected *to*, or indirectly accessible *via* the internet. Unified laws specifying what is allowed and what isn't allowed, and requirements for a minimum-security model would, as an additional bonus, safeguard against the threat of (rogue) devices.

We need to create proper protocols and proper (unified) legislation to make the world better-protected against today's threats *and* tomorrow's. We have to move to a world where the term IoT has a new meaning: Internet of Trust. "Why?" is obvious, but it won't happen until the majority starts to believe it and understand it.

The internet gave us access to almost everything, but it also gave almost every connected device access to "us".

(continued)

Righard Zwienenberg started dealing with computer viruses in 1988 after encountering the first virus problems at the Technical University of Delft. His interest thus kindled, Zwienenberg has studied virus behavior, and presented solutions and detection schemes, ever since. Initially he started as an independent consultant, and in 1991 he co-founded CSE Ltd. where he was the Research and Development Manager. In October 1995, Zwienenberg left CSE and one month later he joined the Research and Development department of ThunderBYTE. In 1998, Norman Data Defense Systems acquired ThunderBYTE and Zwienenberg joined the Norman Development team to work on the scanner engine. In 2005 Zwienenberg took the role of Chief Research Officer at Norman. After AMTSO—the Anti Malware Testing Standards Organization—was formed, Zwienenberg was elected as president. He serves as a Vice-President of AVAR and on the Technical Overview Board of the WildList. Zwienenberg left Norman in 2011 looking for new opportunities, and joined ESET spol. s r.o. as a Senior Research Fellow. In April 2012 Zwienenberg stepped down as President of AMTSO to take the role as CTO and later as CEO. In 2016 he rejoined the board for another 2-year run. He is also the Vice Chair of the Executive Committee of IEEE ICSG. In 2018, Zwienenberg joined the Europol European Cyber Crime Center (EC3) Advisory Group representing ESET.

Zwienenberg has been a member of CARO since late 1991. He is a frequent speaker at conferences—among these Virus Bulletin, EICAR, AVAR, RSA, InfoSec, SANS, CFET, ISOI, SANS Security Summits, IP Expo, Government Symposia, SCADA seminars, and so on—and general security seminars. His interests are not limited to malicious code but have broadened to include general cybersecurity issues and encryption technologies in recent years.

Chapter 11
The Media

In a world where communication can be instantaneous and truth is sometimes buried under data, it is more important than ever to be able to distinguish between the 24-carat gold of reliable information from professional sources and the fool's gold of misinformation and fake news. In this chapter, we look at the roles and risks of the media in Internet security.

11.1 The Media as an Ally

In Chap. 10 I dealt with one of the State's most important responsibilities: namely, to provide the populace with comprehensive information about all the dangers lurking in cyberspace. It is therefore essential that the media are on board with this agenda, and journalists play an extremely important part in the fight against cybercrime. After all, it is they who collect relevant news and information, prepare it for public consumption, and understand the need to warn against the ubiquitous dangers on the Internet.

For myself, I can look back on decades of intensive cooperation with the media—in every shape and form. After all, it doesn't matter to me whether I educate people directly about safely navigating the internet, or by talking to journalists through the media of print, audiovisual media, or online. My first consideration is always to inform and educate individuals and communities as effectively as possible, irrespective of which media channel and which editor carries the message. Nevertheless, it makes me feel a little proud to have collaborated with well-known newspaper publishers such as the New York Times, Agencia EFE, Deutsche Welle, *De Standaard*, *El Pais*, *Gazet van Antwerpen*, *Axel Springer*, and *De Telegraaf*, as well as renowned radio and television broadcasters such as the BBC World Service, CNN, Al-Jazeera, and, locally, VRT, VTM, and RTL.

The media are indispensable partners for the IT security industry. They themselves have already taken the initiative and taken on this educative role. For example,

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_11

in Belgium, Radio 2's Inspector Decaluwé—the lunchtime program aired on weekdays, offering all sorts of tips for an easier life—organized a whole week of topics on "online safety" in the spring of 2013. During that week, security and privacy experts—among them Yours Truly—participated each day in Question and Answer sessions on topics such as buying and selling on the Internet, problems with privacy in social networks, and much more. I think this is a significant initiative that could usefully be repeated as often as possible in the media worldwide.

The significance of the online media as a channel of information should not be underestimated. Thanks to their speed of delivery and their potential effectiveness at staying up-to-date, online media are able to warn Internet users very quickly about current cybersecurity-related threats. The countless blogs that have sprung up like mushrooms, as well as the social networks and traditional media that have jumped onto the online bandwagon, play a special role. Blogs are an effective way to spread messages. In the past years, I have expressed my opinion and made recommendations on security issues both on our company blog (blog.gdatasoftware.com) and on my own anti-malware page (www.anti-malware.info). Many of the views I hold, and practical tips as expressed in this book, were drawn from these blogs. What can I say? I'm in good company with that: here's a good list of some of the most interesting cybersecurity news and blogs: https://heimdalsecurity.com/blog/best-internet-security-blogs/.

11.2 The Media as Influencer

When it comes to assessing the role of the media, I am occasionally ambivalent: on the one hand we have to be grateful to the media in that they can keep us updated and warn us of potential hazards on the Internet. On the other hand, they can also manipulate our knowledge and opinions in ways that do us more harm than good. Should we allow the media to be guided by our love of the sensational and to focus on circulation figures rather than on useful information content? That is indeed a bitter pill to swallow. So it's no wonder that it often turns out that certain facts and information have been misrepresented or simply withheld.

The principle applies in particular to the media: the more up-to-date the reporting, the more valuable it is to you. Dramas that unfold right in front of our noses are always more interesting than anything that happens in distant places like Los Angeles or Singapore. But there's a downside to this immediacy: the closer you are to what has happened, the greater the risk that the wrong conclusions are drawn or that reporting is not as objective as it should be. The following story vividly illustrates this problem.

On March 27, 2013, BBC Online reported that "The internet around the world has been slowed down in what security experts are describing as the biggest cyber-attack of its kind in history." These attacks impacted on the traffic rate from online services as Netflix but also those of BBC. The actual target of this attack was Spamhaus, a nonprofit organization that helps email providers to keep their customers' mailboxes

free from spam and other undesirable emails. Such companies use so-called *blocklists* provided by organizations like Spamhaus: databases listing the addresses of servers, from which messages known to be used for harmful purposes are known to be sent or relayed.

At the beginning of that month, CyberBunker had been added to the Spamhaus list, being a web host that claimed to host everything except child pornography and terrorist material. CyberBunker spokesman Sven Olaf Kamphuis emphasized that Spamhaus "Does not have the right to decide who has access to the Internet and who does not." Perhaps CyberBunker wanted to emphasize this message by claiming the same privilege.

Spamhaus was completely paralyzed by a hitherto highly unusual DDoS attack that lasted more than a week, with attack speeds six times greater than those achieved by an average DDoS attack at that time; this one reportedly peaked at 300 gigabits per second. And since Spamhaus managed a considerable number of domains, these sites were also victims of the attack.

The BBC site was obviously "on the same stretch of the Internet Superhighway" as Spamhaus, as can be seen from the immediate impact of the attack on the BBC service. As a result, it suffered delays in Internet traffic, especially in terms of incredibly slow response times. As many companies (probably in London), with whom the BBC was in contact were also suffering similar delays; the BBC concluded that the entire Internet was probably affected by the DDoS attack. But that was not the truth of the matter! Unfortunately, the BBC compromised its own reputation for accurate reporting by prematurely claiming that the issue was a worldwide slowdown in internet traffic.

You should therefore always be extremely skeptical if the media claims to report the "biggest ever cyberattack." While your own experiences may lead to misunderstandings and misleading information, it can also happen that the media may be similarly misled, owing to lack of time and resources to investigate the situation properly, with the result that fiction may become widely read as fact.

In the Words of. . .
Guy Kindermans, Journalist Specializing in ICT Security

The Internet—even journalists both love and hate it

For journalists, the Internet is a wonderful source of information, facilitating any amount of research on people, companies, products and any current or historical events. This is especially true when there is no restriction on what may and may not be published. Of course, we also use information from social networks like LinkedIn or services like Twitter. The icing on the cake for us is that all these data are available to us with just a few clicks.

Nevertheless, the Internet is also a source of danger for us as journalists. This applies in particular to countries or areas in which news and information are neither freely available, nor permitted to be distributed uncensored. Search queries, reports, communication . . . Everything is registered and monitored

(continued)

continuously. Maybe you have heard of the DigiNotar débâcle? This Dutch certification authority specialized in services for notaries. At the beginning of September 2011, it became known that an attacker had issued unauthorized certificates for various domains (including google.com). These have been proven to have been used for interception attacks against Iranian citizens. The affected certificates were then deleted by some browser and operating system vendors from their systems. As a result, even legitimate DigiNotar certificates were no longer valid, which had serious consequences for their IT infrastructure, particularly as certificates from DigiNotar were also used for the Dutch government's Public Key Infrastructure. On the 20th September 2011, DigiNotar was declared bankrupt. Their carelessness in terms of security enabled the generation of fake security certificates, which put journalists and activists at risk because they mistakenly relied on a protection that did not exist.

There are services that allow anonymous searches on the Internet. In addition, you can encrypt stored data and messages. In principle, this does not provide 100 percent protection either. Governmental security organizations such as the NSA, with 'convenient' and ample 'access and storage' resources, simply store everything. Behind that strategy lies a simple principle: "If we can't crack the data today, maybe we can succeed tomorrow." In a nutshell: for us journalists, the Internet and digital information are gifts from heaven, but for our colleagues in less liberal and democratic countries they can become very dangerous and have diabolical side effects ...

There is more about Guy Kindermans in Chap. 4. 'You have nothing to hide, but everything to protect.'

11.3 The Media as Victim

In recent years, the media have themselves been the frequent target of cyberattacks. In particular, the Twitter accounts of broadcasters, magazines, and well-known journalists have regularly been hacked so as to send false messages to the world under their names. The perpetrators are mostly motivated by the buzz of short-term celebrity: everyone halfway interested might well ask themselves who is behind the hacker attacks or false tweets and how it was done. Answering the latter question is usually a breeze: Most accounts are hacked because someone fell for a simple phishing email, this still being the most effective way of exploiting the human weakness for indulging one's curiosity.

11.4 News Sites and Malware

Finally, I would like to point out that there are also compromised media websites which are themselves responsible for drive-by downloads. We saw this done in the case of flair.be and nu.nl. After a successful attack these media websites even spread—unintentionally—malicious software. By virtue of their popularity, these websites became a frequent target for cyberattacks, both by notorious hackers and by criminals who had only one thing in mind: to make as much money as possible. That's why it's all the more important to the media to achieve comprehensive self-protection from cyberattacks and social engineering attacks in all shapes and forms. So much for the theory. Unfortunately, in practice the situation is completely different. Even malicious advertisements all too often find their way onto news portals available on newspaper websites, showing that moderation and control of those sites leave much to be desired. Recently, malware was even found on *Google News*, even though Google should actually be expected to adopt a scrupulous approach to security.

The most notable example—at least in Belgium—of such an unintentional spread of malware was the story of Radio Brussels, Michael Jackson, and the organized attack on South Korea. Let's take a "Moonwalk" back to that time.

In July 2009, Internet traffic in South Korea was seriously disrupted. Government websites were affected as well as financial sites, but many other portals and popular search engines were also difficult or impossible to reach. The conclusion of the Korean news service after a few days was that this must be the (diabolical) work of some large organization or of another country. And, of course, at that time it was inevitable that fingers would be pointed northward to the archenemy, North Korea. However, this could never be proved, because the DDoS attacks came from all sorts of other countries, and North Korea was not one of them. A few of the computers involved were even located in South Korea, and others were noted in Japan, the United States, Great Britain, and even Belgium. Nobody knows exactly how many Belgian PCs were part of the zombie network that attacked South Korea. However, we do know that these PCs had been recruited into a gigantic network (botnet).

Two weeks earlier, Michael Jackson, one of the biggest stars in pop history, had died. To commemorate his art, the Belgian rock station Studio Brussels dedicated its own website—eternalmoonwalk.com. The aim was that each visitor could offer to the site his own interpretation of the "Moonwalk"—Michael Jackson's legendary dance, in which his leg movements appeared to indicate that he was running forward, while the dancer was actually moving backwards. The idea was to fit all these emotional interpretations later into one endless Moonwalk. At first it was mainly video clips from Belgium that were uploaded, but it wasn't long before Jackson fans from the rest of the world were joining in, and so eventually an hour-long video was compiled. What a huge success for Studio Brussels!

Unfortunately, the story didn't end there. As it turned out later, the site was compromised. A vulnerability in the Adobe Flash Video Software caused tens of thousands of computers to be compromised in their turn and recruited into a kind of zombie army, that army then being mobilized to help implement the DDoS attacks targeting the South Korean websites. It is, of course, possible that the malware responsible came from North Korea, or was controlled by cybercriminals hired by North Korea, but in the end it does not matter. The most important lesson we can and should learn from this is that each and every website, well known or less well known, is a potential target for cybercriminals and saboteurs. Since the web pages of famous media companies enjoy enormous popularity, there is a significant danger that other online media will also unintentionally spread malicious software in the future.

We should not underestimate the value of the media as partners in the fight against cybercrime, but they can also, unintentionally, become part of the problem.

In the first place, newspaper websites, specialized publications, or news channels are popular targets for—and victims of—hackers and other cybercriminals and are misused for the distribution of various kinds of malware.

In addition, though, agency reports or short messages (for example) are not necessarily suitable channels to convey explanations of complex technical relationships to audiences whose knowledge and understanding varies widely. It is understandable that it's not possible for everyone—or even every journalist—to be an IT security expert, and there is often not enough time available for lengthy research in this age of rapid exchanges of information. Unfortunately, it is often not a priority to ensure that important aspects of an issue are made clear to the reader.

It remains a challenge to bridge the gap between security experts and the general public. Personally, I will continue to use all my knowledge to help media and journalists master this challenge.

Chapter 12
The Digital Future

If you ask me what all the malware and other cyberdangers will bring us in the future, I can answer in one word: MORE. In essence, what we'll be seeing is more of what we already have, though we can expect changes in format and even platform. Not only a continuation but an increase, both in the number of attacks and the potential for damage. Surely no one is so naïve as to seriously believe that cybercrime or cyberespionage will suddenly tail off because individual criminals or state-sponsored attackers have been identified? On the contrary: the number of those who turn their hands to malware and hacking will grow steadily. That's why I believe that potential victims and malware hunters have ever greater challenges to face. And yet I am sure that we will always find solutions, even for future cyberdangers.

In the Words of . . .
Ralf Benzmüller, Founder of G DATA Security Labs

In the last decades our world has embraced so much technological progress, and is still digitally transforming into a virtual environment that closely maps to reality. This extra dimension is completely populated by computing devices that continually become both smaller and more powerful. We are surrounded by smart gadgets that are permanently connected to the Internet and are capable of making our lives more convenient and interesting. But our businesses are also optimized by computers. High-frequency trading on the stock exchange, mining cryptocurrencies, and optimizing logistics or energy consumption are just a few examples of how much money is made with computers. But there is more to come. Autonomous cars to take you to your home, which you can manage remotely from your mobile. Most of the shopping you do will be virtual, you will pay through a consistent, standardized payment mechanism, and you will get your items delivered to wherever you are at the moment.

(continued)

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_12

The food you eat will be optimized for the soil it is grown in and harvested by machines that are directed via satellite. In short, all our lives will be dependent on computing devices.

The early computer viruses were just annoying, in most cases. And even the bad ones only bricked one machine at a time. Today, malware outbreaks like WannaCry and NotPetya bring down the production lines of companies, or a country's airports, hospitals or power plants. The potential damage that misused or abused computing devices can inflict is immense. That's why the fight against malware is becoming more and more important. And that's why computing devices should be created with security in mind—especially if they are used in long-term contexts like cars, buildings and industrial production lines. Eddy makes good points in his book about how we can safeguard our future

Ralf Benzmüller has headed the G DATA Security Labs in Bochum since 2004. In this role, he has been responsible for the development of proactive detection technologies, and the design of the automatic malware analysis system. In his current position he coordinates G DATA's research activities. He is regarded in the industry as one of the foremost experts in the field of malware and online crime. Ralf Benzmüller has established his reputation at many national and international conferences and trade fairs. In addition to his activities as head of G Data's Security Labs, he has published many articles on current computer threats and has given seminars on malware research at various universities. Ralf Benzmüller is a member of EICAR and AMTSO.

12.1 The Shape of Things to Come

In the coming years I see the following developments coming our way:

We can expect ever more (and ever more innovative) mobile malware. The number of viruses and Trojans for mobile devices (smartphones, tablets, iPads and iPods, and whatever else is available on mobile platforms) will increase systematically. Right now, the majority of mobile malware is aimed at Android devices. Remember my first law (Chap. 6)? It is therefore perfectly possible that in the coming years an increasing number of malware authors will target iOS or perhaps some other operating system whose market share is currently minimal, or perhaps even one that hasn't yet reached the market. The degree of interest shown by malware authors depends on a number of factors—not least, how easy the system is to subvert—but mostly on the success and market penetration of an operating system.

Currently, the developer of mobile malware still has to contend with a number of practical problems: for example, apps require approval before they can be downloaded to a smartphone or tablet, which should, of course, be refused in the case of known malware. But the malware author has possible solutions to hand: malware can be packaged as an update to a popular software package. How many people carefully read every requirement made by a software update? For most users, all that matters is that software should hit the ground running: the quicker they are to accede to its demands for access privileges and other requirements, the sooner they'll be able to use the app. Another approach we often see nowadays is for the downloaded app to be just a downloader in its own right: it seems harmless enough when scanned by the software repository, but then it downloads components that may be far from harmless.

Another worrying development had already been identified by my colleagues at G Data back in 2014: smartphones that are already contaminated with malware at the factory. Further discoveries like this are to be expected, since spyware embedded within the firmware, and other attacks inserted into the supply chain before the device ever reaches the retailer's shelf, are notoriously difficult to detect.

I'm pretty sure there will be a future generation of malware that does not require explicit user approval. I'm thinking along the lines of a kind of drive-by malware for mobile devices: that is to say, smartphone or tablet owners will only need to visit a certain website in order to infect their devices, without having—to their own knowledge—executed or opened any programs at all. We don't hear a lot about this kind of attack, but it's already out there, while Android ransomware kits continue to command premium prices even as cryptomining malware takes center stage on desktops and laptops.

Globalization of malware: I am also convinced that types of malware currently found mainly on PC platforms will continue to have increasing impact on other platforms such as Android, iOS, and macOS in the future. As an example, I'd like to cite Android.Fakedefender, the first ransomware for mobile devices. There is a longstanding type of malware that locks smartphones because, allegedly, the device owner viewed naked images, and only unlocks the device after a "fine" has been

paid, while a variation on the theme demands that a certain amount of money be paid to "install an antivirus update." This type of malware has also penetrated into the world of mobile malware. The DoubleLocker malware not only locks the legitimate user out of the device by changing the PIN to a random value but also encrypts all the files in the devices primary storage area, demonstrating that mobile ransomware has evolved well beyond simple screen-locking.

Another trend convinces me that the number of botnets comprising zombified mobile devices (not to mention IoT devices) will continue to increase rapidly. Initially, the spread of such malware was limited, because approval still has to be issued for each function, which severely limits the range of action available to a zombie device. But by 2017, the WireX Android botnet had quickly grown to comprise tens of thousands (or more) of zombified nodes, spread through some 300 apps that had managed to slither onto the Google Play Store, and were used to implement Distributed Denial of Service (DDoS) attacks.

Botnets can also target 64-bit versions of Windows 8.x and upward. Currently, they are a serious threat to *all* Windows platforms and they will continue to be developed. Before long, bot herders will be able to take advantage of the capabilities of 64-bit Windows platforms as well as 32-bit Windows 8.x/10 in order to build botnets. Indeed, a 64-bit, Tor-enabled Zeus variant was seen in the wild as far back as 2013.

More "Man-in-the-middle" Attacks: In Chap. 6 (under "Online Banking: Beware of the Man-in-the-Browser"), you learned what to do in the event of a Man-in-the-Browser (MitB) attack. In principle, a Man-in-the-Middle (MitM) attack is exactly the same and serves the same purpose: to siphon off data before it is encrypted and/or sent to the cloud (Fig. 12.1). Man-in-the-middle attacks are likely to be incorporated into more malware including Windows 10, macOS, and Android.

More social engineering: because defense mechanisms against malicious software have significantly improved and continue to develop, attack methods will, of course, also become more sophisticated in the future. Inevitably, this means that weaknesses in defensive strategy will be eagerly sought. And so we are reminded once again of the weakest link in the security chain: the poorly informed end user. Or to put it another way, I fear that cybercriminals will rely more and more on social

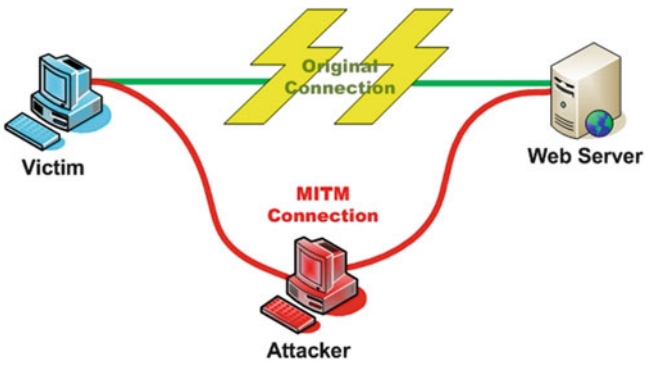


Fig. 12.1 Man-in-the-middle

engineering and on looking for personal data that will give them the key to accessing a computer and/or a corporate network, or to acquiring social networking credentials. But the list of potential prizes for an accomplished social engineer is endless.

More cross infectors: a *cross infector* is malware that has every advantage because it works across platforms, not just on one vulnerable type of system. Malware that manages to jump effortlessly from Windows to Android and back will probably be particularly successful.

More botnets: make no mistake, security experts are not sleeping on the job and will continue to uncover botnets in the future. We will be more successful at detecting and punishing the culprits, for sure, as happened with the Citadel botnet. But behind each botnet discovered the next is already lurking. In addition, existing botnets are not always totally isolated from each other, which means that hijacked computers that continue to be infected with malware may be easily integrated into a new botnet.

12.2 Sophisticated Malware

There are undoubtedly sophisticated malicious programs arising from intelligence sources. The Snowden revelations are certainly just the tip of the iceberg and have, quite rightly, caused worldwide outrage. But what impact do these high-end cyber weapons have on our day-to-day security as we navigate the Internet? Like many other experts I have become aware of a worrying trend: the authors of routine criminal malware have learned to analyze state-sponsored spyware programs, and are using the sophisticated techniques they discover there to improve and develop new malicious attacks to use against the computers used by businesses and home users.

More cyberespionage and cybersabotage: I am sure that there will be a continuing increase in the number of targeted attacks on companies, in order to gain access to their databases or paralyze their infrastructure. And these will not be just the preserve of foreign secret services or news agencies. The majority of the attacks will, instead, probably come from (or be launched on behalf of) direct competitors of the companies targeted.

More hacked SME (Small- to Medium-sized Enterprise) websites: SMEs/SMBs (Small- and Medium-sized Businesses) are likely to succumb in the coming years to the misconception that their networks and websites are safe because they are not worth hacking. But they are wrong, because hackers have come to understand that these businesses also offer them the opportunity to make a quick buck and therefore have turned their attention to that sector. My fear is that the number of hacked SME websites will skyrocket and then serve as a platform for spreading malicious software. This trend will continue until, like everyone else, small- and medium-sized enterprises come to understand that their operations are just as interesting to cybercriminals as their big brothers and that they have just as much need to take appropriate countermeasures. For this reason, if for no other: small organizations often have information at hand about those larger enterprises that will make a cybercriminal's life easier.

In the Words of . . .
Natalya Kaspersky, CEO of InfoWatch Group of Companies, co-founder of Kaspersky Lab

1. **What do you see as the biggest threats in cyberspace, in the near and distant future?**

I have been working in IT security for 23 years, and have witnessed how technology has grown, developed and changed our lives. Unfortunately, together with all their benefits and advantages, new technologies bring new threats to the world.

Today, the whole world community is discussing a new digital economy based on Big Data, the Internet of Things, Industry 4.0 (the current trend of automation and data exchange in manufacturing industries, blockchain (records linked cryptographically) and so on. However, while implementing these new ways of working and living, we need to analyze the risks associated with them and consider how we can reduce those risks.

Let's take as example the Internet of Things (IoT). Innumerable new connected devices appear daily. Thousands of IoT developers use their own protocols and firmware, resulting in a continuing increase in the number of vulnerable IoT devices appearing around the world, mainly in the US, China, Germany, France, India, UK, Russia, South Korea, Brazil, and Japan. As you can see, these are major economies and BRICS countries (the five major national economies, i.e. Brazil, Russia, India, China and South Africa). Tens of thousands of unprotected devices are being connected to the Internet every day.

IoT may cause two types of risk.

1. First, misuse of unprotected devices for attacks on normal computer infrastructure. For instance, the Mirai malware attack in 2016 was organized through vulnerable IoT devices and created a successful DDoS-attack on the biggest American service provider company, DYN. DYN hosts, by the way, many major global websites and portals, such as the New York Times, eBay, Twitter, and so on. Another IoT botnet, known as Reaper, borrowed some of Mirai's source code, but, unlike Mirai, it used several vulnerabilities at once. Reaper had the potential to incorporate millions of IP addresses and thus become more destructive than its predecessor.
2. The second risk is that of a hacker attack on IoT devices themselves. In March 2107 FDA reported a vulnerability in cardiac devices from St. Jude. "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in control, they could deplete the battery or administer incorrect pacing or shocks", the FDA said. The devices, such as pacemakers and defibrillators, are used to monitor and control patients' heart functions and prevent heart

(continued)

attacks. Another example is the famously successful Jeep hack, when a team of researchers was able to take total control of a Jeep SUV using the vehicle's CAN bus.

The situation is worsening when it applies to the Industrial Internet of Things (IIoT). In March 2018 the Ponemon Institute published research about IoT security (https://sharedassessments.org/iot-new-era2/). Researchers asked more than 600 respondents about their perception of IoT risks and third-party risk management programs, as well as the strategies being employed by their organizations to defend against IoT-related cyberattacks. 97 percent of respondents said an attack related to unsecured IoT devices could be catastrophic for their organization and 60 percent were concerned that the IoT ecosystem is vulnerable to a ransomware attack.

Unfortunately, the majority of manufacturing enterprises that use IIoT do not understand what's going on in their own infrastructure. Indeed, industrial sites may be those at the highest risk of suffering damage from cybersecurity incidents. In the above-mentioned report, only nine percent of respondents say they are fully aware of all the physical objects on their sites connected to the Internet. We must assume that the others aren't.

2. **Will the anti-malware industry be able to keep up with the cybercriminals?**

For the global information security market, the traditional approach, whereby you build a threat model and then monitor incidents as they occur, is becoming out of date. Today the market is shifting towards incident prevention and the assessment of corporate cybersecurity risks. As all modern systems are IT-addicted, corporations are exposed to specific IT risks. This changes the game entirely for information security: it is no longer a department-specific job but a business-critical function.

Both businesses and government have to ensure end-to-end protection against multiple threats. They need a cyber shield against a cyber sword. Unfortunately, cyber criminals constantly invest in new attack weapons, thus forcing their potential victims to spend more resources and money on protective measures.

3. **Do you see anything that could seriously reduce cybercrime or increase the efficiency of cybercrime fighters, on any level (personal, vendor, government,** . . .**)?**

Ideally, I would say that governments, businesses, and individual users should ensure cybersecurity at their own level. Thus, vendors need to quickly respond to incidents and continuously improve their existing protection tools, no matter how hard it may get. Businesses should strive to find ways to

(continued)

implement integrated security solutions and always keep them up to date. End users should install—at a minimum—antivirus software and follow simple cyber hygiene rules, while government has to tackle the extremely difficult problem of protecting both people and businesses against potential cyber threats and continuously fortifying the security of mission-critical infrastructure sites. The perfect solution would be a local IT infrastructure, but that is a very expensive asset to own and maintain.

In any case, nobody can guarantee absolute safety.

Natalya Kaspersky is President at InfoWatch Group, Kaspersky Lab co-founder;

Head of the Information Security Working Group, "Digital Economy of the Russian Federation program".

Born in Moscow in 1966, Natalya Kaspersky graduated from the Moscow Institute of Electronics and Mathematics with a Diploma in Applied Mathematics.

In 1997, Natalya, together with Eugene Kaspersky, founded Kaspersky Lab and became its CEO. During 10 years under Natalya's supervision, the Kaspersky Lab startup turned into a remarkable leader in the global IT market, boasting $126 million in annual revenue.

In 2007, Natalya left Kaspersky Lab to head InfoWatch, which offers software for enterprise data protection. InfoWatch now dominates the Russian IT market, and is actively developing its positioning in the global markets.

Natalya holds multiple awards in Russian and International Business and IT:

- *"Entrepreneur of the Year 2016" in Russia and a participant in a global competition of entrepreneurs organized by the company EY*

(continued)

- *"Russian Business Leader of the Year 2012" award, honoring her remarkable contribution to the progress of the Russian IT community, according to Horasis, the Global visions community*
- *Leader of "Top-1000 highest Russian managers of 2014" in IT according to Kommersant, the leading Russian business daily, and the Association of Russian managers*
- *Best Technology Business Entrepreneur, Women in Technology MEA 2014 awards, Dubai*
- *Nominee as "The most influential person from Russia Q1 2015" for input in the IT-industry by BRIC Magazine, UK*
- *Leader of "Best.ru" rating in Telecom/IT in 2017*
- *Named as one of "The 30 most inspirational leaders in business" by Insights Success Magazine.*

Any technical device may, sooner or later, be the target of a cyberattack. Nowadays there is talk in security circles of compromised refrigerators, televisions, watches, or spectacles . . . anything that connects to the Internet leaves the victim open to a potential attack from cybercriminals. This applies even more to devices with their own IP address and connected to a corporate network and/or the wider Internet, as these can be misused to infect the rest of the network. But even equipment with a purely local connection such as Bluetooth or RFID (Radio Frequency Identification) poses a risk of exposure to cyberattack. Such a highly targeted attack is by no means out of the question and therefore not excluded from discussion here.

In my blog article for G Data—"IoT: The Internet of Things. . . ehm. . . Trouble"—I warned that:

> The Internet of Things (IoT) gives everything an IP address so that everything can communicate with more or less anything and anyone else. The benefits and possibilities are almost infinite. But aren't these technological developments evolving rapidly, maybe too rapidly? Smart TVs, gaming consoles, tablets, smartphones, and cars can eavesdrop on us. Cameras in your laptop, smartphone, and smart TV can watch us when we don't want them to. Samsung is amending its user agreements to reassure people about the voice control on its smart TVs. BMW is rolling out a software update for the ConnectedDrive system in 2.2 million cars to prevent hackers easily being able to open the doors of the cars. These are the first signs that possibly too much has been started without reflection.

(https://www.gdatasoftware.com/blog/2015/03/24275-iot-the-Internet-of-things-ehm-trouble) And, incidentally, this is where I coined the phrase *Internet of Trouble (=IoT).*

And, sure enough, we've seen enough of these issues since that article to add some more predictions:

- Botnets related to IoT devices will continue to grow (see Mirai, VPNFilter, etc.), and a combination of DDoS attacks and ransomware through these devices is likely.

- Android will be misused to target IoT devices and ultimately the home and company network.
- I expect to see cyberattacks spreading into the Industrial IoT. The convergence of informational technology and operational technology is making environments more vulnerable. These environments often run legacy systems for which patches are either not available or simply not installed.
- Even more IoT devices will become part of bigger botnets (for example CCTV's, weather stations, thermostats, doorbells, and so on).
- IoT-targeted malware will show up by infecting portable devices like smartwatches, fitness-tracking devices, and so on, spreading with their ultimate target being the home PC or the company network. We can expect to see enterprise breaches that originate on mobile devices becoming a more significant corporate security concern.

More attacks on the worldwide infrastructure: by infrastructure I mean what is sometimes called the critical national infrastructure (CNI): indispensable organizational units, such as gas and electric utilities, public transport, healthcare, finance, and water utilities. In my opinion, skirmishes and wars will, in future, take place in cyberspace in parallel to real battlefields in the real world. Thus, the rallying cry of a future war may well be along the lines of "we shall fight in the fields and in the streets, we shall fight on the beaches, we shall fight in the air and we shall fight on the Internet."

There will be increased volumes of attacks on critical infrastructure to world-leading countries like the United States, the United Kingdom, Germany, and France. We will see more threats related to critical infrastructure with attack methods consistent with multiple potential threat actors, including nation states, terrorism, and organized crime. Worldwide data breaches and hacks of big companies and organizations will continue to appear, and locally based (country-specific) data breaches on smaller companies will increase.

More attacks on the infrastructure of companies. As I said, I'm focusing more on attacks on one country's infrastructure by another, but I believe that the infrastructure of large companies will frequently become the target of cyberattacks. After all, there are several reasons why an attacker might be interested in damaging or completely disabling an organization's entire IT infrastructure.

"Real" danger and cyberdangers go hand in hand. Until fairly recently, it was quite simple: there were dangers in the real world and dangers in the digital world. Where a crime was committed, such as armed bank robberies, the perpetrators were, once found, punished accordingly. And then there were online bank robberies, incorporating man-in-the-browser attacks, social engineering, or other means of obtaining banking information from individuals or businesses by theft.

However, cybercrime and "normal" crime will converge more and more to the point where there is often no meaningful way to distinguish between them. Consider, for example, the example noted below of criminals who hacked into the access system of a port terminal, changed cargo numbers, stole cargo containers containing drugs, and so on. Similarly, "old-school" crime will be further integrated into

cybercrime: for example, more cyberattackers will aim to make a quick buck (or several) by targeting banks or companies with low security hosted in less aware countries)

But since 2013, it should already have become clear to everyone that these two worlds are converging: online crime and old-school crime go hand in hand. In the spring of 2013, there was a large-scale raid in the port of Antwerp, where customs officials and police seized the largest quantities of heroin ever found there. At first glance, it was a classic real-world crime. But only until the investigators established a connection between a burglary carried out in advance of the drug smuggling. The burglars had, among other things, put in place keyloggers and prepared multiple connections with the IT systems belonging to companies at European ports. In this way they were able to get screenshots of monitors, access to operators' keystrokes, and access to internal systems. As a result, they knew at all times which containers where located were and had the data and credentials that enabled them to pick up containers. Unsuspecting drivers, who assumed that they were carrying harmless goods like bananas, thus became unwitting drug couriers.

It is now known that two very gifted Belgian programmers, who were at the start of a promising career in the IT sector, were behind the digital intrusion. Both were known up to then as "*Ethical hackers"*—which proved to be a significant misnomer.

There was an additional example in 2013 of the convergence between traditional criminal behavior and cybercrime: in an international "attack" on ATMs around the world, around USD 40m were stolen in just a few hours. This astounding operation was preceded by a long period spent implementing the theft of digital data, with credit card details and stolen PINs being loaded onto counterfeit credit cards. In addition, these cards were manipulated in such a way, that it was possible to use them to withdraw unlimited cash. The only limitation on how much could be stolen was how much money was available in the targeted accounts. In Germany, too, large sums of money were stolen in this way.

The SWIFT messaging system, used by financial systems worldwide to transfer funds, has been attacked a number of times in recent years in order to steal money. In 2016, around US$81 million was stolen from Bangladesh Bank. If another attempted transfer had been successful, the total haul would have been nearly a billion dollars. The theft is reported to have been effected by injecting malware into the bank's inadequately protected SWIFT terminal (https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC). In 2017, malware was used to steal US$60 million from the Far Eastern International Bank in Taiwan by gaining access to the bank's SWIFT terminal (https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/). SWIFT has been quick to claim that these attacks are against the banks concerned and don't represent a problem with the SWIFT infrastructure.

A report by the UK's National Crime Agency—*National Strategic Assessment of Serious and Organised Crime for 2018*—forecasts that "Developments in technology will continue to transform the future crime landscape . . . The use of technologies such as the dark web, encryption, virtual private networks (VPN) and virtual

currencies will support fast, 'secure' and anonymous operating environments, facilitating all levels of criminality. . ."

The report goes on to predict that technology in crime is likely to continue its "complex and global spread" and even suggests the possibility that cybercriminals will locate their activities within "'safe havens' in more hard-to-reach firewalled and 'siloed' jurisdictions. . ." It's hard to disagree with the conclusion that technologically driven change in a technology-dependent society will increasingly be reflected in both intentional and inadvertent criminal behavior.

(http://www.nationalcrimeagency.gov.uk/publications/905-national-strategic-assessment-for-soc-2018/file)

Cybercrime as a Service (CAAS) is becoming a standard, in the same way that organized crime has benefited from criminal versions of legal and financial services. Indeed, it's impossible to separate such services from the technology that provides them with a marketplace. And the fact that data now drives cybercrime means that data will drive an increase in the use of spyware, even more than has been seen in recent years.

A "smart" device can still be vulnerable. One of my passions is the enormous pleasure I get from smart devices, such as Internet-enabled televisions and refrigerators able to reorder via the Internet when food is running out, but also game consoles and the fad-of-the-moment consumer magnets: Google Glass (spectacles that supplied you with digital information and the means of verbal communication with the Internet, rather than just the visual information everyone else has) and of course smartwatches from Sony, Apple, or Samsung. They all have some degree of artificial intelligence and an operating system, processor, and memory. They all have Internet access, but the danger there is that malicious software might be developed on a grand scale for them too. Which devices attract the attention of the malware "developer", like that of the legitimate software developer, will depend solely on their market share. At the moment, for example, network printers are the most vulnerable component of the overwhelming majority of corporate networks. Defensive measures in this area are very sparse, but then so is malicious software that targets it, right now. And yet sooner or later I expect it to become extremely appealing, for those engaged in industrial espionage, to develop ways to observe from a safe distance what has been printed and scanned over a network.

The rise of "digital flu." Looking further into the future, I imagine that the human body will be more susceptible to attack from digital viruses as well as the biological variety. Infection will also be spread by family and friends. The development of microchips, lenses, and other artificial implants in various implementations is ongoing. So it is already possible today to monitor and control blood pressure or the administration of medication digitally. But it's not just in the realm of biomedical research and therapeutics that impressive progress is being made. Progress is also being made in quite mundane and even profane areas. In Barcelona, the trendy Baja Beach Club discotheque is using RFID chips that are injected under the skin by way of authorizing admittance to their VIP area, and even for the processing of orders. It shouldn't be too long before a system is invented whereby in order to get access to an event a pill has to be swallowed. Forget the usual wristband or the stamp applied to

the back of your hand. At the entrance control point it will be easy for the bouncer to scan and see from the monitor that you have paid for admission. But alongside the practical and ethical considerations, there are also safety concerns with all these new technologies. Because, as already pointed out, anything controlled by a microprocessor might also fall victim to malware.

More undiscovered malware. Spectacular though the examples already given may be, they convince me that cybercriminals, cyberspies, and cybersaboteurs are becoming more and more dedicated to the task of protecting their malware from the rest of us. In the long term, hackers and other cybercriminals are better off if their malware goes undetected for a long time rather than causing obvious damage that immediately indicates the presence of malware. The good news is that you may never feel your digital flu. The bad thing is that just the presence of a subclinical digital infection can mean a hefty bill for you, somewhere down the line.

Ransomware and, more recently, illicit cryptomining have become the malware breaches to make the most headlines in recent years. There has also been an increasing amount of "pseudo-ransomware" such as NotPetya and BadRabbit which may show ransomware-like messages but have (even) more destructive intent, like the "wipers" that have simply destroyed data rather than render data inaccessible by encryption. Ransomware and wipers have attacked—intentionally or otherwise—organizations as well as individuals. Indeed, SamSam, for instance, seems very much focused on extorting large sums from organizations rather than small amounts from individuals. Increasingly, though, we're seeing wipers used to attack nation states. We're also seeing malware that incorporates both ransomware and cryptomining as alternative payloads. Windows malware techniques have been increasingly implemented on the Android platform: not only ransomware but even (less successfully, so far) cryptocurrency mining.

There will also be a rise in ransomware attacks impacting cloud-based data centers. As more organizations embrace the cloud, these types of attacks will start finding their way into this new infrastructure, either through encrypted files spreading cloud to cloud, or by hackers using the cloud as a volume multiplier. Cryptomining via scripts on different websites stealing capacity from visiting computers has become almost routine since 2017.

Fake news will get worse in the coming years: perhaps this will restore a certain amount of trust in traditional newspapers and news agencies, though it gets harder to distinguish between well-resourced propaganda outlets and more-or-less independent news outlets. Even among long-established newspapers and news sites, independence is often overwhelmed by a blatant political agenda. However, these issues are further exacerbated when filtered through social media that are reluctant to penalize profitable propaganda outlets, while confused individuals uncritically exchange misinformation, all of which will turn social media into an even bigger mess than we're seeing now. We will also see more targeted attacks intended to influence or silence an organization, with "legitimate" actors launching such attacks. For example, the 2016 US Presidential campaign seems all too likely to serve as a precedent and template for future campaigns.

GDPR will be chaotic in the next years and drive privacy agencies to stronger control measures in the next years. With the regulatory responses to data breaches increasing, organizations will build new data frameworks, but there will be a long period of adjustment while organizations try to demonstrate compliance without necessarily understanding or achieving it.

Technical improvements to malware developed by/for cybercrime because of the examples shown by state agencies (Chap. 11). For example, expect to see increased quantities of fileless malware (memory malware) in all devices.

Backdoors in the Cloud: as enterprises are using the cloud more these days, more backdoors will be found by hackers, and an attack intended to disrupt some major cloud providers will also happen very soon. DDoS attacks will increase in prevalence compared to 2016 and will have triple the bandwidth of today's attacks. They may be used as a means to impact a specific competitor, who would be one of many affected, making it difficult to determine motive.

Smart Cities will become targeted cities in the end …. Here's a report that indicates the amount of spending that Smart Cities are attracting, but how much of that spend is going on security? "IDC Forecasts Smart Cities Spending to Reach $158 billion in 2022, with Singapore, Tokyo, and New York City Among Top Spenders": https://www.idc.com/getdoc.jsp?containerId=prUS44159418.

More defensive effort: if the cybercrime scenarios described above are robbing you of your sleep, I can prescribe a little calming information. Security vendors, governments, and other institutions have an ever-increasing arsenal of defensive weapons with which to counter offensive moves taken by cybercriminals and other villains in the never-ending game of Security Chess. And this will continue to be the case in the future.

How will the struggle develop in the next 20 years between malware authors and other cybercriminals on one side, and the forces arrayed *against* malicious software and cybercrime on the other? Nobody can know that with any certainty. Nevertheless, I have taken a look into my crystal ball and written a story in which I've incorporated my past experiences, my knowledge, and my opinions. It is, of course, a work of fiction, even if I have to say in all honesty that some resemblances to real events, people, and technologies are not entirely coincidental, though the names of real people you might identify in this story have only been used with their permission…

Have fun while reading!

Fig. 12.2 QR Code: link to a page at www.cyber-danger.com

If you are looking for more information on the subject of cyberdanger and would like to be kept informed about current threats and countermeasures, I recommend the website that we have designed especially for this book. Simply scan the QR code (Fig. 12.2) and you'll have plenty of additional information.

Chapter 13
Awakening: A Short Story

The intention of this story is to outline my vision of what the digital world might look like in the year 2033, and what cyberdangers that year might bring. What might really happen in the near future? Will we have learned from our mistakes?

Disclaimer: Although several people mentioned in this short story really exist, the story is completely fictitious. My thanks to Mikko Hyppönen, Righard Zwienenberg, Luis Corrons (Fig. 13.1), and of course my wife Nadine Van Grunderbeeck and my son Frank Willems for letting me use their names. All the events described here and statements and actions attributed to those real people are purely the products of my imagination. I really enjoyed writing this story, but to avoid any misunderstandings let me assure you that I don't know anyone called Lien Sander, Meredith Weston, Helen Dench, Anthony Dice, or, of course, Larry Lane. Any resemblance to real people with any of those names is purely coincidental.

* * *

13.1 A Possible Customer

Lien Sanders has no idea what's going on anymore. Just now she is in the conference room at the offices of her client Bio Dynamics, when she suddenly feels a sharp stinging in the eyes, caused by the smart contact lenses she is wearing. Her eyes are dry and the contact lenses rub like sandpaper against the cornea. She has no choice but to take out the lenses and give her eyes a break.

Frank Willems, Managing Director of the *Frank Talking* Communications Agency, sees his colleague's discomfort and laughs: "You must have another ocular virus," he suggests. Lien does not find it funny. She often calls her boss "Mac Malware," since he immediately suspects malware to be the problem when things go wrong. Apparently, he has acquired this habit from his father, now retired but formerly a well-known virus expert. Fortunately, you can also talk to Frank about

E. Willems, *Cyberdanger*, https://doi.org/10.1007/978-3-030-04531-9_13

Fig. 13.1 Righard, Luis, and Eddy (often known as the Three Amigos in the security industry) in 2018

other topics. And that's just as well, because he is now responsible for more than 100 communications companies. Tomorrow, the agency will even be acting for NATO for the first time.

NATO: who would have thought it?!? Obviously, the organization believes that the time has come for a change after several "communications breakdowns and stumbling blocks," as the Secretary General puts it. This is a verbose but carefully neutral way of expressing concern about the power wielded by the new superpowers, the Philippines and Zimbabwe, in trying to make their public image more palatable.

However, Lien is not at all amused: She spent a great deal of money on these lenses only recently. It will be annoying, to say the least, if she has to take them back to the dealer. After all, the new Lenovo lenses are unusually practical, in theory: They offer so-called *enhanced reality* with lots of relevant information, readily available and readable beyond the limits of her field of vision. That is an area in which Apple still has much to learn. An inflammation of the eyes would be fatal, she would hate to have to wear conspicuous smart glasses like Frank's.

Lien puts the lenses on the small table next to her. The table in the conference room, which is also used as a virtual conference table, is a no-go area, because all smartphones, tablets, and other devices used by participants in the conference have been placed there. That's *no* place for her new lenses. So far, she has only saved private files onto these lenses, such as the photos from last night's wild party. These photos are definitely not for the eyes of Frank and the other male participants.

"Ah, that's much better," Lien says enthusiastically, glad to be relieved of the irritation caused by the lenses. "Good to know," replies Frank. "We have to get down to some serious work now. We still don't know enough about the customer, what he expects from us or how he wants to position himself in terms of communication. We need to understand all that before we can develop an action plan." He has good reasons for not yet sharing with her some of his other thoughts. He suspects that this

customer, Bio Dynamics, is especially interested in *Frank Talking*, because it has heard that the agency is to take over all NATO's communications with the outside world. Bio Dynamics has a broad portfolio that they hope one day to be able to sell to NATO. Every contact that brings Bio Dynamics a little closer to the Big Cheeses in Brussels is therefore considered worth its weight in bitcoin. Frank is sure that Lien is expecting great things from her career with *Frank Talking*—after all, she is a decidedly intelligent woman with an incredible talent for communicating positive and negative messages. Besides, he wants to see whether she, too, understands why Bio Dynamics is so interested in them. Lien does not seem to suspect anything: she applies her eye drops again and puts her lenses back in.

Before the crew from Bio Dynamics enters the conference room, she discreetly checks out her photo album from the evening before.

"Well, what a waste of time that was!" Lien remarks after the meeting. "They must have known how complex the services you offer are and would have done better looking for someone with experience in their own sector. I wonder why they came to us? They didn't even give us enough time to present ourselves properly and explain how we work. That felt to me like an exercise in deploying a hidden agenda. And what's that about, inviting us and all our colleagues and customers to their company party? But they've completely miscalculated: I wouldn't dream of taking anyone from NATO along. Who do they think they are? That wouldn't be an option even if that old crooner Justin Timberlake *is* giving a private concert. I'll just take our marketing assistant."

Frank gives her a satisfied look. Yes, he knows his colleague well—he wasn't wrong about her intelligence and intuition.

13.2 The Meeting

The next day, at NATO, Frank and Lien find themselves at the center of an unaccustomed burst of activity, and they don't understand why. It all starts with the incredibly strict security controls they have to undergo on entering the building. First, they have to go through a metal detector in the lobby, and then their briefcases are thoroughly searched. In addition, all of their electronic devices are turned on and checked painstakingly for malware. This is an annoying procedure that seems to take forever as Frank carries about 20 devices that are capable of connecting to the Internet. Lien only has 15, but each one has to be examined individually.

Finally, it's done, and at last they can focus properly on their communications strategy, carefully formulated in accordance with the wishes of the highest-ranking representatives of NATO. Everyone participating in the meeting is clear that the number one priority is to make the most of all the positive news to have come out of NATO in the last few years. The media must be flattered and coaxed into forgetting all the communication problems of the past.

Frank and Lien are convinced that this is the strategy that will succeed. In the end, it is all about communicating plenty of positive messages. For example, there is the

message that, for the first time in NATO history, a woman has been appointed Secretary General. Frank still finds it amusing that she is addressed as a "general secretary," but, fortunately, only remarks on it today when he is alone with Lien, who looks daggers at him. As the next step, it needs to be pointed out that NATO has, the recent past, done its utmost to make the world safer. That could only be achieved through stricter controls, but as we now know all too well, that's the price of security.

There is a short break, during which everyone checks their video mails. Frank and Lien make the most of the opportunity to admire the conference room in all its glory. On the wall facing the floor-to-ceiling windows are a variety of screens that broadcast live what is happening in the most important places in the world. These include places of strategic and military importance, such as the White House and the Kremlin, but also tourist destinations like Times Square in New York and the Champs Élysées in Paris. The screens are strung together like pearls on a string, and the wall resembles an oversized poster that clearly conveys the message at the heart of NATO: "Everything is under control." *Frank Talking* also wants to put this slogan to use by communicating the pleasing aspects of current world events in accordance with this motto. There are no more bomb attacks, no cases of cyberespionage, only a few regrettable incidents in remote regions.

Up to then, recalls Frank, there has been a great deal of resistance to overcome. Innumerable nations and companies had, initially, strenuously resisted the attempts by NATO, the G12, and the European Community to establish a presence in cyberspace, to improve their monitoring of Internet traffic and, if necessary, have the ability to take immediate remedial action.

In the end, NATO got its supervisory mandate and has been controlling the internet for about 5 years now. Since then, there have been few significant cases of cybercrime—a major turning point in digital history. Of course, this meant making some significant adjustments. Russia and China were also given a seat in NATO as were most Asian and African countries. And that, of course, initially led to heated discussions between the world's various archenemies. But after a few years, all ideological obstacles were finally taken off the table and at last the digital control offensive was given the green light.

"The message is clear," says Meredith Weston, NATO's communications strategist. "NATO has everything under control. Control is a good thing. The world is now a peaceful place, and we owe that to NATO."

"For a dove of peace, she packages her message quite aggressively," thinks Frank, but keeps that thought to himself. Then he sits down with Lien and Meredith at the conference table and they start developing various concepts. They let the peaceful pictures that flicker across the screens in the background inspire them as they start the brainstorming. It is no easy matter to sell the idea to the rest of the world that NATO's control of Internet traffic and even road traffic is a major contribution to world peace. (For example, NATO can control traffic lights and other dynamic traffic management systems in and around its headquarters, if a terrorist threat makes it necessary.) But if there is an agency that is up to this task, then Frank is convinced that *Frank Talking* is the one.

13.3 The Dinner

Over an excellent restaurant dinner, Frank shares his thoughts with Lien. She agrees that things went much better in the afternoon than at the disappointing Bio Dynamics meeting the day before. Yet they are not entirely clear as to which media should convey their message. "Facebook is something for seniors," Meredith had said. "But a hologram in the room with a message about security would probably be too much of a good thing," Lien countered. "We could advertise a competition, where you can submit a song about NATO," Frank interrupted with a grin, and began to softly sing "N-A-T-O" to the tune of the Village People's "YMCA." The two women looked puzzled—they were too young to know that hoary old hit.

Now Frank and Lien review the day's discussions once more and seize upon the idea of the song contest again. "We could get the finalists from all the countries to play together and organize the biggest jam session of all time," says Frank, expanding on his idea. Lien prefers the idea of "*crowdwriting*," in which every citizen of the world is called upon to write a chapter of the greatest story ever written. "If all the citizens of this safe new world are not only online but also emotionally connected with each other, anything and everything is possible. And that's exactly what we want to do with the campaign," Lien sums up. Frank is excited by Lien's concept and they decide to put their heads together to put it into action.

Pleased with this decision, they devote their attention to dessert and talking about the impression the NATO building has made on them. "I am astonished by the sophisticated technical potential of this complex," says Lien admiringly.

"I can see that, but after all, it houses one of the most important and powerful organizations in the world. And businessmen, especially those who appreciate good food, have now understood and responded accordingly," says Frank, as he takes in the restaurant's furnishings and facilities and takes note at the delicious food that real waiters are carrying past their table. There is no digital menu here, and the diner's order is not forwarded digitally to the kitchen, as with most other restaurants, but a flesh and blood person takes care of the customer's wellbeing. For the first time, he realizes the value of this personal contact. Anyway, today was more than successful, Frank notes with satisfaction. After a delectable nonalcoholic cocktail for Lien and a 10-year-old whiskey for Frank, they decide to bring the evening to a close and go to their hotel rooms. Frank thought it would be a good idea to stay over in Brussels and start the next day at seven with a brainstorming breakfast. "So much has changed in the past few years, but one thing hasn't. It's mostly the Americans who like to swap ideas around a sociable meal," laughs Frank, and says goodnight to Lien. In his room he decides that he would like to be woken up with impressions of nature: an alpine landscape with the lapping of a stream and the sound of a few cowbells. . . This will be a good start to the day.

Minutes later, he is already sound asleep. But it is neither the tinkle of cowbells nor the splashing of a stream that wakes him, but the shrill beep of his smartwatch. Still half-asleep, he looks at his watch and immediately recognizes the caller. "Dammit, Lien, it's half past four in the morning," he croaks, holding the watch to

his ear. “I hope you have a good reason for disturbing me in the middle of the night!” And indeed she does. At first, he barely understands what she’s saying because she’s sobbing so bitterly, but gradually her words start to make sense. “Frank, I think I’ve brought the whole of NATO to a standstill.”

13.4 What Happened?

“So tell me, what happened?” asks Frank impatiently in the car that takes them to NATO headquarters. “With the best will in the world, I didn’t really understand what you were trying to tell me through all the crying. I’ve never known you to be so emotional.” “Well, let me explain,” replies Lien, who seems to have regained her customary composure. Like yesterday, she is wearing the sort of highly professional outfit favored by successful businesswomen, except that she has replaced her smart lenses with Google spectacles. For the first time, it occurs to Frank that Lien has blue-gray eyes, and not greeny-brown, as he has always thought. Apparently, her lenses not only store information but also distort it. He surprises even himself by being distracted at such a moment by such a trivial issue. Then he pulls himself together and eagerly listens to her extraordinary story.

“I was fast asleep, and then someone started banging on my door. My first thought was that there was a fire, so I leapt out of bed and opened the door. I’d hardly got it open before two strong-arm types in tailored suits stormed into my room, followed by two other suits, lighter guys who were probably in their 50s. They pushed me into a chair and demanded that I hand over my lenses immediately. But before I did that I wanted to know who they were, and why they’d got me out of bed in the middle of the night. When I put my glasses on, I immediately recognized the smaller of the two older men: It was Anthony Dice, Head of NATO Security, and then I realized how serious the situation was. After I gave him my lenses, Mr. Dice explained the reason for his “unannounced visit.” Shortly after 22.00, NATO’s computer systems began to go crazy. The traffic lights around the building started switching from red to green in five-second cycles. Heads of state all round the world got an ecard from the Secretary General with a highly suggestive message and “Greetings from the Brussels district of Evere.” That was by no means all, but I’ll save the details for later. NATO immediately called in all the available analysts and computer experts to work out what was going on. It was clear that some sort of malware was responsible, but knowing that wasn’t enough to reverse its effects. That’s why they were under pressure to find the culprit immediately. And after a few hours, they had the answer: my lenses. . .”

“That’s impossible!” Frank interjects. “First of all, there’s no way you would do something like that. And anyway, what about the security check? I’ve never experienced as thorough a scan as the one we went through yesterday, physically or digitally.”

“But that’s how it is,” sighs Lien, “and besides that, they were convinced that I’d deliberately smuggled the virus in. I was interrogated for three hours solid. They

wanted to know to the very last detail what I've been doing in recent years. Why did I take a holiday in Iran and was it really a private trip? "Because it's a beautiful country," I said, and it really was the most beautiful vacation of my life. Then they wanted to know about everyone I'd ever worked with, when I worked for the Russian aircraft manufacturers MIG Citizen Corporate. And did I know that MIG used to produce fighter aircraft? Uh, hello? *Of course* I know that: I was actually assigned to communicate their radical change of course to the outside world. Obviously, I succeeded in that, because tonight was the first time in ages that anyone has ever mentioned MIG's past history and activities. It looks as if they have been watching me for a while and knew almost everything about me. Fortunately, they seem to have missed my Chinese boyfriend from university, otherwise I would probably have had to face another half hour of questioning. Thankfully, I've never mentioned him on social media and Chinese social networking is a law unto itself."

"Did they also ask about Bio Dynamics?"

"Yes," replies Lien, "they wanted to know which members of staff I visited in the past few days and who I'd talked to on the phone. Why do you ask?"

"Just wondering," replies Frank, trying to sound casual, but he knows for sure that something isn't right. All at once he feels uneasy, but he isn't sure why.

13.5 The Interrogation

When Frank and Lien arrive at NATO headquarters, they are checked even more thoroughly than they were last time. Not surprisingly—after all, Lien is officially considered the prime suspect, and Frank, as her business partner, is also under suspicion. "I have a shrewd suspicion that we will not be talking today about our new campaign," he whispers to Lien.

She does not reply, but guiltily lowers her eyes. Frank didn't mean his comment reproachfully, because he is convinced that this is something that could have happened to anyone, and he is still hoping that this whole problem can be fixed today.

As soon as the security check is completed, over, they are taken to a room far away from the one they used the day before. Here, there are no video screens or attractive pictures of far-flung corners of the earth. Three of the walls are painted white, and there is a mirror stretching the entire length of the other wall: no doubt a one-way mirror. It occurs to Lien that she's in for more endless hours of interrogation, perhaps with an unhealthy dose of the "Good Cop, Bad Cop" routine. But it turns out better than expected. Along with Meredith and Anthony Dice, there is just the one guard in the corner. Frank sees this as a good sign: perhaps they already know that Lien didn't deliberately infect the NATO systems.

"As you can imagine, we want to resolve the matter as quickly as possible, without letting any cats out of the bag, let alone out of this building," says Anthony Dice calmly. "You, Ms Sanders, have brought this virus in here, which is why you are our best chance of finding out who is responsible for this chaos. And, yes, chaos

is exactly the right word," he adds with a sour expression. "Our systems are completely out of control. So far, the effects have been fairly innocuous, and the culprit has chosen to restrict his actions to pranks, but that might change at any time. Since last night, the air conditioning has already been increased twice to the maximum permissible value of 28 degrees Celsius, and once turned back to the permitted minimum, fourteen degrees. Ten times more sandwiches than usual were ordered today. The video stream to the White House is running *Die Hard 3* and the volume is turned right up on all the 'Yippee Ki Yays.'"

Frank, Lien, and Meredith can hardly suppress a grin: whoever the culprit may be, he has a sense of humor!

Just for a moment, Anthony Dice turns his face away from them. (Maybe to hide his anger? Or because even he has to hide a smile?) And then he continues: "Our systems do what they want, and do not respond to any of our commands. We can't just stand by helplessly and watch the offenders manipulate the system. Yes, the *offenders*—this can hardly be the work of an individual. And quite honestly, I have had more than enough of this. So, Ms Sanders, you will tell us immediately where your lenses might have been infected." And with those final words, Dice looms menacingly over Lien, probably to demonstrate to her how serious he is.

But Lien has by now recovered her composure and counters: "I would certainly have told you long ago if I knew from where I got this virus. And please do not talk as if I'm responsible for all this. I'm not as careless with my lenses as you suggest, especially when they're brand-new and very expensive." Lien actually wants to say more, but then she breaks off abruptly, suddenly remembering something. "Come to think of it, I did take out my lenses for a moment the day before yesterday at Bio Dynamics, because the air suddenly became incredibly dry. And right after it got really humid, almost like it is here. Could it be that . . .?"

Anthony Dice does not let her finish her sentence. "Inform the police immediately," he snaps at the guard in the corner of the room, "they should move in on Bio Dynamics right away. Tell them they need as many officers as possible." Then he asks Frank and Lien for the company's address. Frank checks the GPS on his watch and calls: "2 Solar Panel Street, in Diegem. A skyscraper. Twelfth floor." He notices how quick and staccato his own speech is. It seems that he, like Anthony, is caught up with the excitement of the chase.

13.6 Bio Dynamics

Soon after, five police wagons, each with two officers and two robots on board, are heading for Diegem. All the NATO staff, along with representatives of Belgian State Security, as well as some foreign experts who have been flown in to work together to find a solution, are assembled in the large cinema hall so that they can track the police raid live. Everyone is terribly excited, chewing their nails, rubbing their hands nervously, and fidgeting backwards and forwards on the cinema chairs. They watch every move on the big screen with rapt attention, caught up in the mad rush across

Brussels: the men, women, and robots swarming around and into the Bio Dynamics building; the sprint up the stairs (wisely, they didn't take the elevator, since the enemy is obviously technically skilled). They watch intently as the officers pound on the close office door, demanding that the occupants open up. Breathlessly, they wait for the laser apparatus burn a huge hole in the door and see the officers climb through it. But then they see the stunned expressions of those same officers as they realize that they're standing in a completely empty office.

Suddenly the live broadcast picture changes: instead of the empty office in Diegem, they see a man in closeup, and Frank recognizes the goatee beard and turtleneck sweater of the CEO of Bio Dynamics, Larry Lane. It's a look that dates back to the last century, but the technology he is using is bang up-to-date, and his grin is menacing.

"How nice that you could arrange to meet there in one room," he says. "That's a great help, because now I only need to explain myself once, and I can be sure that you all get the message. You all have the dubious pleasure of being the victim of the greatest ransomware attack of all time. Your systems have all been disabled by my people. If you want to get access to them again you will need to pay me the biggest ransom in history, but you've probably already realized that. I want to make it clear that I am neither a religious fanatic nor a nationalist extremist. The only thing that interests me is money. Lots of money. What is your organization worth?"

He strokes his beard theatrically, while pretending to think about the price. "How much money does the richest person in the world have? 750 billion dollars? How about if we just round it up? One trillion is a nice, round figure. Just think about it: I'll contact you again in one hour.

13.7 Hacking NATO's Impregnable Network

Everyone stares blankly at the movie screen, now empty. Was that real? Or have they somehow been just hallucinating? How did this happen? The team leaders are pulled into a videoconference with key heads of state and their security experts, in order to discuss the situation. Two questions are inevitably raised. First, how did Larry Lane manage to crack NATO's seemingly impregnable system? And secondly—and far more importantly—what do they do now? Do they have to meet the demands of this terrorist? Or should they get down to looking for a solution? But a solution to what problem, exactly?

The IT team that will analyze the infection has taken Lien and Frank to a different room. For the umpteenth time, they are asked all the same questions. Why did they visit Bio Dynamics? Who did they meet there? What was discussed? Did Lien feel somehow differently when she put the lenses back on? Frank shakes his head in disbelief at the last question: you don't physically feel a digital virus as you would feel the first symptoms of flu slowly spreading in the body. But his father always says, "You cannot imagine how many myths about malware are still around today."

Suddenly Frank has an overwhelming urge to call his father and tell him about the predicament he and Lien are in.

Meanwhile, the IT team has come to a further decision. Almost an hour has passed since Lane's video message, so the Chief of Staff decides to ask for a postponement of the deadline. He will say that in such a short time it was not possible to contact all the stakeholders and decision-makers. Given that extra time, he hopes that they will be able to find a solution to the problem.

Exactly an hour after his previous appearance, Lane is back onscreen in the movie theater. "So? Have you been able to reach a decision? Are you going to make me both the richest and the happiest man in the world? Or do you intend to bring the rest of the world to ruin?"

Helen Dench, Secretary General of NATO, has just arrived at NATO headquarters after a short flight in her HeliCar, a brand-new "amphibious vehicle" that can also be driven like a normal car and is also capable of short flights like a helicopter: indeed, she only left it a few minutes ago on the roof of the headquarters building. So now she takes the floor.

She asks Lane urgently for another 24 hours, in order to reach a consensus and get the ransom together.

Lane seems to have anticipated this request, because he grins broadly and sneers, "That's nonsense and you know it. You just want to spend time searching for a cheaper solution for your little problem. What you're asking for is an insult to my intelligence. But I've no wish to be unpleasant about this: I'm miles ahead of you technologically, so I don't have anything to lose by granting your request. But let's be clear: I have the whip hand here, and I set the conditions. But as a gesture of good faith, I'll even tell you a secret for free: there are now thousands and thousands of infected computer systems under my control. For every malicious program you remove, ten more viruses will instantly swarm and infect the next system in the chain. What's more, you cannot get access to your own systems, whatever you try to do," chuckles Lane mischievously. But all at once his tone of voice turns serious: "Okay, you get your 24 hours respite. But this is my first and last warning to you, not to lie to me again."

Suddenly the screen splits. In the left-hand frame is Lane's sneering face, and on the right, they see the road that connects NATO with the center of Brussels and what used to be Belgium's national airport. Since the price war between various airlines in 2025 resulted in many flights moving to other airports, Ostend and Charleroi share this role. Nowadays, Brussels Airport is reserved for the use of military transport and private flights by the President and other key figures such as NATO leaders. There is usually relatively little traffic on this street. Lane continues: "As you may have noticed, I'm now the one who controls the traffic lights around the NATO access roads. Presumably you can still remember the day it was decided that NATO would take control of road vehicles?" Some Chiefs of staff glance meaningfully at each other. Yes, that had been seen as a breakthrough. But all of a sudden, the screen shows one of the driverless vehicles accelerating and running at full speed into the car in front. Every face in the room is with distorted with shock at the sight: this is the first accident involving a driverless car in 5 years!

"What none of you considered, obviously, is that driverless vehicles constantly interact with smart traffic lights. Not with the intention of controlling the car, but just to exchange information. While the car advertises its location, the traffic light tracks its current position. The only reason traffic lights are not allowed to control the car's actual movement is that so many countries had moral and ethical concerns. But morality is not my problem." As if to underline his words, another vehicle leaves the queue in front of the traffic light, turns the wrong way, and after turning several somersaults finishes up in the middle of the street.

"One more thing: did you realize that I've also taken control of the air traffic control center next door to you at Eurocontrol?" asks Lane, and his mocking undertone causes everyone in the room to break into a sweat. "That's right, that's the great thing about the world today. Humans, animals, inanimate objects: they're all interconnected. We used to say that all roads lead to Rome, but now we should really be saying that all roads lead to each other. Except that when it comes to the road to fortune, following the money only leads to me!" He gives one last diabolical grin (which he undoubtedly copied from some action movie), then the screen turns black. The faces of everyone present reflect the same panic and despair.

Fortunately, Helen Dench is still present, and immediately takes the floor again. "There's no question that the situation is serious, but our IT and security departments are working hard to find a solution so that we can regain access to our systems." At that precise moment Frank's smartwatch beeps, and he hurries out of the hall.

13.8 Calling Dad!

"Hello, son, what's all this I'm hearing?"

Frank is overjoyed. It's years since he's been so happy to hear his father's voice.

"Dad! Have you heard what's going on here?"

"Yeah, sure, you evidently don't know where I am right now—I'm in Barcelona at the Virus Bulletin conference. There's going to be a sort of end-of-career party to celebrate my retirement. But the only thing anyone here wants to talk about is what's going on right now in Brussels."

"I've never come across anything quite like this," sighs Frank.

"What exactly happened? There are three different versions of the story circulating at the conference."

Frank tells him the whole story and when he is done, his father says, almost admiringly, "Oh yes, ransomware!"

"Excuse me?!? Could you temper your enthusiasm in the face of this crisis? This could be a worldwide catastrophe—or do you see it differently?"

"Oh, I am well aware of the danger. After all, son, you'll remember me telling you time and time again in the past how dangerous cloud services and global networking are. You'll have to excuse me if I can't quite resist an 'I-told-you-so'. But it's incredible that I am now celebrating the end of my career—well, after the end of my

career, but that's another story—fighting a potentially catastrophic case of ransomware. That's how my career in security started, remember?"

Frank still remembers all too well: after all, he has heard the story of the "AIDS floppy disk" more than 20 times, till it is literally burned into his memory.

"But let's get to the point, my boy: can we help you at all? After all, just about every antivirus expert in the world is here with me in Barcelona. Everyone who is anyone in security is right here!

It takes Frank a moment to realize all the implications of what his father has just said. He is right in the middle of what is probably the biggest cyberattack of all time, and at the same time his father is sitting with the cream of malware researchers and fighters against cybercrime in Barcelona. If the situation were not so dangerous, one might say, "Too good to be true!"

"Hang on a minute, Dad, and I'll call you back right away."

"Okay, Frank, but don't take too long. In an hour I'm going with some friends to eat at the El Bulli tavern. I've been looking forward to it for weeks!"

Frank hurries over to Anthony Dice and consults briefly with him and several other Chiefs of Staff, and then picks up his phone again. "Dad, you're not going to El Bulli! Grab the best guys you know and get to the airport. There'll be a NATO jet there waiting for you."

13.9 The Team of Security Experts

"Won't your father be unhappy at having to miss out on El Bulli?" asks Lien anxiously. "He must have made those arrangements ages ago."

"No chance!" laughs Frank, "He would hate it if he missed out on fighting the biggest cyberattack of all time. That will appeal to him much more than all the tapas El Bulli can put on the table. And as it happens, it sounds as if the food on the plane will be quite tasty, too. Not that they'll have much time to eat: they'll be landing at Brussels airport in about half an hour."

About an hour later, Eddy Willems comes into the NATO building with Mikko Hyppönen, still a ridiculously busy security expert and an experienced keynote speaker who has lectured at innumerable security conferences. Also in the group are Righard Zwienenberg and Luis Corrons—both good friends of Eddy's and renowned IT professionals who have worked in the industry for several decades. Anthony Dice is not sure whether to breathe a sigh of relief or sigh with anxiety. Sure, these men have years of experience, but do they also keep up-to-date with the latest malware techniques and trends? The fact that they have all come straight from the Virus Bulletin conference does reassure him a little. It's probably because of his job that he's basically cautious rather than optimistic.

13.10 The Attack Analyzed

As Lien already feared, she now has to tell her story for the fifth time. The only good thing is that this time she doesn't forget anything. With the other interrogations, she always found that there were a few significant details that she only remembered afterwards, but now every last detail is readily retrieved from her conscious memory.

Eddy and his colleagues are actually impressed by how perfectly planned Larry Lane's attack is. Immoral though it was, the way in which he engaged with *Frank Talking* and misused the agency in order to achieve his own ends was skillfully executed. Phase one, the preparation of the infection, was almost perfect. And then there's the way in which he then penetrated the system and used an ingenious combination of backdoors and vulnerabilities that they cannot help but admire. "I have to say, Lane has done his job with extraordinary efficiency. I have never seen an APT like this," says Righard Zwienenberg. "Yes, he really seems to have thought of everything. I think it's more A than P", agrees Eddy Willems. Frank and Lien look at each other quizzically, because they have no idea what the experts are talking about. Anthony Dice interprets their expressions correctly and starts to explain, seeing a good opportunity to prove his own expertise. "APT stands for *Advanced Persistent Threat*, meaning a sophisticated and ongoing threat. Your father is saying that this attack was launched using the most advanced technologies. After such thorough preparation, it was dead easy for Lane to penetrate the system. Is that right, Eddy?"

"I couldn't have put it better myself," Eddy replies. "And it's gratifying to know that NATO still employs people who are familiar with the basics of classic malware technology. Today the jargon used is *targetware* as a way of covering every possible targeted attack, but sometimes it's useful to apply a more specific term in order to understand exactly what's going on."

"What I still don't understand," says Anthony Dice, getting back to the point, "Is how this malware could be smuggled past all the malware protection programs that we used when Mr. Willems and Ms. Sanders were admitted to NATO headquarters?"

"I suspect that the actual malware had yet to be activated," replies Mikko Hyppönen. "I'm convinced that either a timer or the scan on entry to the building launched the malware. Since there was a gap of just a few hours between your leaving for dinner and the discovery of the malware, I'd guess the latter."

"That wouldn't surprise me with malware as tricky as this," Eddy tells him, "But the most important question is: how do we turn it off?"

The four participants in the Virus Bulletin conference are now working together with NATO's security experts on this problem. Fortunately, the whole room is kept isolated from the main systems, and so is secured against eavesdropping. "Lucky that I insisted on that precaution," thinks Anthony Dice.

They brainstorm furiously, running through all sorts of potential risks and problems (which takes quite a long time, because they must take into account *all* the systems to which NATO has access) and also review what NATO's security experts have tried to do so far in order to turn off the ransomware. That takes quite a

while, since a long list of countermeasures have been tried, even though none of them have worked. Finally, they think about what measures they can still attempt.

"Have you tried all the available virus sniffers?" asks Mikko Hyppönen. By this he means small programs that are routed through the network in order to track down malware. Some of these are not only good at tracking but are also capable of analyzing malware, and sometimes they already contain enough information to solve a malware management problem. "In this case, it would be very nice if they could relieve us of the need to analyze the malware directly: we can do the rest ourselves."

"But we can't get into our own network, so how can we send out sniffers?" asks Dice.

"Maybe we can also find this same malware in another network and can try it out there. If it works, we can do it again with the critical systems."

"Good idea!" everyone responds, and one of the security experts is sent to another team so that this idea can be put into effect.

An hour later, Anthony Dice receives a call. He picks up, listens, and takes a deep breath. "Our expert has tried everything, but he just isn't getting anywhere near the malware. Although he *has* found some satellite malware programs, which seem to be used to monitor activity, but they're really too well protected against analysis. What should we do now?"

"We could also try to get into the network system of a driverless car," Luis Corrons interjects forcefully. "Since the traffic lights send commands to the cars, it's possible that it would work the other way round."

"That sounds like a good idea: I'll get someone on it right away. Perhaps we should try it with a Chinese car? They are definitely well equipped and always carry the most technically sophisticated and up-to-date equipment. And since China and NATO are such good friends, they certainly won't object," says Dice, desperately trying to be witty.

Only 15 minutes later, the phone rings again and his face turns even more thunderous than the last time. "Dammit, he managed to get the sniffer into the traffic control system, but then our man tried to get deeper into the system from there, and before he knew what was happening, the car was propelled 50 yards further on into a concrete wall."

"Oh, heck. . . our own weapons are being turned against us," sighs Anthony Dice. "It could take days to write our own malware and insert it into the system. And we don't have that much time."

"Besides, we do *not* want to fix this by developing malware," chime in all four of the Virus Bulletin Musketeers as one, "that just wouldn't be ethical!"

"What else can we do, then?" Dice asks desperately. Everyone stares as if spellbound at the electronic whiteboard, on which all the options, risks, and technical specifications for the malware have been listed.

Eddy rubs his chin and almost casually asks, "Have you ever thought of trying to turn the systems off and on again? That's one of the biggest problems at the present time: All systems, large or small, from the mainframe to the smart lens, run 24 hours a day, 365 days a year. Everyone wants it that way. And of course, cybercriminals

also assume that's how everything works. And maybe that's exactly the point at which we can hook in our own processes."

"I don't understand," says Anthony hesitantly and a little bit anxiously. "Just in case you forgot, Lane is in control of our systems, not us. Which means that we can't perform a remote shutdown."

"Sure, but have you ever tried just turning the system off by hand? We just pull every plug we can find, and then we reboot the system. Maybe that's enough in itself for us to regain control."

"Is that even possible?" one of the security experts wants to know. "Can we access all our internal and external server systems at all? I guess all the doors to the server rooms were closed by our systems when the malware was triggered."

"No, that might actually work," says Anthony Dice enthusiastically. "When the doors to the server rooms were closed, there were a few guys from the IT team still in there, trying to recover the systems via the administration consoles. Presumably they're still trapped in there.

"A stroke of luck for those lads," Luis laughs. "Now they have the opportunity to be the heroes who save the day, if everything works out!"

13.11 Disabling the Malware

The only question to answer now is how they get into to the server suite to tell the IT team. Then someone suggests that they write the message with a good old-fashioned felt-tip on a whiteboard and hold it up to the window. The technicians look pretty puzzled at first. In all the years they've worked there they have never pulled a plug out or turned off a device by hand. On the contrary: turning off a server (unless there's a legitimate need to disconnect it) is punished with a hefty fine. The culprit is expected to invite the whole IT team to dinner in the most expensive five-star restaurant in Brussels! But then it dawns on them that this is their last chance. They agree that they must switch off all devices as fast as they can, so that Lane and his team don't notice what's happening.

Nerves stretched to breaking point, the entire NATO team, plus the four Virus Bulletin veterans, watch as the server team—fortunately, all very athletic guys in their 20s—sprint along the line of servers, turning off every device. Everyone is anxious, and only now does Frank realize that Lien has been squeezing his hand painfully hard. It all takes just 20 seconds. "And that," says Lien, sighing with relief, "is how to get into the *Guinness Book of Records* for 2034, if only because they've just invented synchronized server powerdown."

And it immediately becomes obvious that at least one success has been achieved: the server suite doors open and out comes the IT team, cheering. Without a moment's hesitation the lads start hugging all the onlookers. But now there is an even trickier task to undertake: the first system has to be rebooted and brought under control before the malware can be reactivated.

A tense silence falls as the security and IT experts watch the system administrator, who must start the system from external boot media, so that the malware cannot be triggered again. After a few minutes he gives them the thumbs-up, earning rapturous applause. Now the system has been recovered, the ransomware is disabled!

13.12 Larry Lane

Amid all the hubbub and cheering, Frank hears the ringing of his smartwatch. And now he sees that five missed calls have been flagged on the display, all from the same number. He suddenly realizes who is trying to contact him. His number is probably the only one that Larry Lane knows that he is able to dial directly. Now that NATO has control of its own telephone systems again, it's easy to block his calls. When he accepts the call, he hears the unmistakable, angry voice of Larry Lane. "Give me the Secretary General!"

"If I'm not mistaken, you're no longer in any position to make demands," grins Frank. "Why not try asking nicely? Anyway, I'll gladly pass you on, and I'll enjoy hearing how you get on."

Helen Dench immediately turns the watch onto speaker so that everyone can listen to the conversation. "Mr. Lane," she says mockingly, "instead of billions of dollars perhaps you'll accept our offer of food and lodging for at least 25 years?" "The game is not over yet," threatens Lane. "I'll find another way into your systems, and then you will know what a catastrophe really is!" His last few words have hardly been uttered when everyone hears a deafening noise at the other end of the line. They hear shots and a loud crash as a door falls to the floor. Excitement mounts as they hear Lane and his men being overpowered by the Security Service. The newest generation of tracking robots has found them in no time, and then it is child's play to reel them in without bloodshed. "In cyberspace, Larry Lane was a genius, but in real life he's a complete loser," murmurs Anthony Dice.

13.13 Prevention

After the cheering dies down, it's back to work for the whole group. Eddy and his Friends discuss with the NATO experts how such malware attacks can be prevented in the future. "Do *not* forget the off switch," Eddy says again, his whole face one big grin. Frank and Lien sit down at the conference table again with Communications Strategist Meredith Weston and discuss how best to set about limiting the damage the incident has done to NATO's public image. Perhaps they can tailor the message to focus on how successfully everyone involved cooperated in order to solve the problem? After all, experts in communications are not only capable of repairing reputational damage but of spinning the story so successfully that those involved are actually better-regarded than they were before. In this case, though, they face a

tremendous challenge, which is why Secretary General Helen Dench is also taking part in this meeting. "This is about more than just communication, this is about the whole strategy of NATO for the coming years," she says, explaining why she is there.

A drinks reception is being organized for that evening, with everyone present at NATO Headquarters invited—including Eddy and his friends—as a way of thanking everyone who helped to reach a satisfactory conclusion to this unfortunate incident. And so this unforgettable day is coming to a happy end, but Frank is still in the mood to celebrate. He and Lien ask the four security experts whether they would like to join them for a slap-up evening meal in a nearby restaurant. "Obviously we'd love you to join us: after all, you've probably saved not only the whole world, but also my contract with NATO!"

"With pleasure," replies Eddy. "But before that, I would like to satisfy my curiosity about something. Down in the basement they keep the server backups, and I'd like to take a look at all the system data and log files. Maybe then I'll understand how the malware actually worked. After all, fighting malware is not just about how to react when a virus strikes and repairing the damage: it's also about preventing similar incidents in the future. What do they say? 'An ounce of prevention is worth a pound of cure?'"

"Isn't that typical of my dad," laughs Frank. "Even now when he's drawing his pension, he just can't resist a security puzzle. Everyone else wants to party, and what does he want to do instead? Analyze viruses. OK, but make it quick, and in the meantime, we'll book a table."

"We'll come down with you," say Luis and Righard in unison. They too want to get to the bottom of this malware, but unlike Eddy, they hadn't dared to ask the NATO bosses if they could investigate further. On the other hand, they *were* basically the ones who have saved NATO and the rest of the world.

13.14 Where in the World Is Eddy Willems!?!

"Here we are again!" Luis and Righard are back after only half an hour or so. "For the moment, we just skimmed the data, because investigating the whole thing is probably going to keep us busy for a while. The NATO experts promised to let us have all the relevant information for my talk at the Virus Bulletin conference in Barcelona tomorrow night. That's going to blow everyone's socks off," says Righard and rubs his hands in sheer anticipation. "And what about my father? What's he still doing down there?" asks Frank.

"What?!?! He was right behind us when we left the basement." Only now do Luis and Righard notice that Eddy hasn't followed them into the conference room. "Hang on a minute," says Luis. "I'll go back and get him or he'll be spending the whole night down there." Less than five minutes later he's back. "There's no sign of Eddy, and the guards didn't see him either. They told me that Eddy was not behind us when the door that connects the basement with the offices was locked."

"That's odd," says Anthony Dice. "I hate it when people go missing round here."

"He can't have disappeared: it's just that we've managed to lose sight of him," Meredith Weston exclaims, grinning. "I'll just ask in the ballroom if anyone has seen him there."

"Good idea," say Frank and Lien, and go in with her.

A short time later, they learn that no one has seen Eddy since he went down to the basement. Anthony Dice checks the surveillance recordings. He finds nothing—no sign of Eddy anywhere in the building. When they try to ring him, they get an answerphone message. Frank says, slightly worried, "All I get from his smartphone is an 'I can't answer the phone right now' message."

"I *really* hate it, when someone goes missing round here," Dice says a second time, and this time Meredith does not contradict him.

"Maybe it was all too much for him and he quietly went home. I'll call my mother," says Frank, holding his smartwatch to his ear and giving the command "Call mom." A few seconds she answers.

"Mom, have you seen Dad tonight, or heard from him?"

"No, my boy. He's supposed to be with you: why are you asking?"

"Because we can't find him. Nobody saw where he went and he isn't answering his phone. Something must be wrong, because normally he *never* turns off his cellphone."

"That's true. If he contacts me, I'll let you know immediately," says his worried mother. "Best to get the NATO security services on the case right away. In the meantime, I'll contact my colleagues in the police. Is there anything else I can do? If he shows up, call me, okay?"

"I will," says Frank, and his smartwatch disconnects from the call. He looks in alarm at Lien and says, "Cancel the table at the restaurant: I'm afraid this is the beginning of a completely different story."