OWN YOUR SPACE

Compliments of Microsoft®

Know Your Villains

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

Edited by Linda McCarthy and Denise Weldon-Siviy

Publisher: Linda McCarthy
Editor in Chief: Denise Weldon-Siviy
Managing Editor: Linda McCarthy
Cover designer: Alan Clements
Cover artist: Nina Matsumoto
Interior artist: Heather Dixon
Web design: Eric Tindall and Ngenworks
Indexer: Joy Dean Lee
Interior design and composition: Kim Scott, Bumpy Design
Content distribution: Keith Watson

ISBN 978-0-615-37366-9
Library of Congress Cataloging-in-publication Data

McCarthy, Linda
Own your space : keep yourself and your stuff safe online / Linda McCarthy.
ISBN 978-0-615-37366-9 (electronic) 1. Computer security. 2. Computers and children. 3. Internet and teenagers. 4. Computer networks-Security measures. I. Title.

Visit us on the Web: www.100 pagepress.com

Download free electronic versions of the book from MySpace (http://www.myspace.com/ownyourspace) and Facebook (http://www.facebook.com/ownyourspace.net), and from Own Your Space (http://www.ownyourspace.net)

Chapter 2

Know Your Villains

Meet Eric, from Novato, California, a normal teen who likes to create web pages for his friends. Eric spends a lot of time on the Internet. He is a major gamer, visits a lot of different sites looking for ideas, and likes to download free software.

Before Eric got his own laptop, he used his mom's computer to surf the Net and download free stuff. Eventually, Eric's mom's computer became so slow that it took *forever* to download software. That's when Eric asked a friend what to do. That's also when Eric found out that he should have had a firewall and downloaded patches to prevent hackers from planting spyware on his system. Eric thought that antivirus software was all he needed and he hadn't even heard of drive-by malware.

Eric found out the hard way that a hacker had back-doored his system and had been sifting confidential information from it. Well, not really Eric's system. It was his mom's system and her confidential information. Oops... sorry, Mom. Now, Eric has his own laptop with a firewall, current patches, antivirus software, and spyware protection.

ISBN 978-0-615-37366-9

What happened to Eric? He simply didn't have the right protection to keep the bad guys out and to keep malware from getting in. Like most teens, he needed to know a lot more about security than he did. While virus protection is important, it's not the be-all and end-all of security. Malware can land on your system in *many* ways. You might simply have visited a website that was created specifically to download malware.

2.1 Why Does Malware Exist?

When you consider the work that goes into writing software, you have to ask why anyone would care that much about trashing a stranger's computer system. To understand why people write malware, it helps to look first at WHO is doing the writing.

A surprising number of teens write malware. According to Sarah Gordon, a research scientist, their most common feature is that they don't really have a lot in common. Sarah's research finds that malware writers "vary in age, income level, location, social/peer interaction, educational level, likes, dislikes and manner of communication."

While some teens write malware for the sheer challenge of it, others have heavy delusions of grandeur. That was certainly the goal of Sven Jaschan, an 18-year-old German teen sentenced in 2005 for creating Sasser.e, a variation on an earlier worm dubbed Netsky. Sasser literally bombarded machines worldwide with millions of junk emails. Jaschan's goal wasn't so much to disrupt Internet commerce as it was to make a name for himself. After his arrest, he told officials he'd only wanted to see his "creation" written about in all the world's papers. Jaschan told reporters, "It was just great how Netsky began to spread, and I was the hero of my class."

Is this admiration justified? Rarely. Consider the case of Jeffrey Lee Parson, of Minnesota, an 18-year-old arrested for releasing a variant of the Blaster virus. While his friends and neighbors were taken in, at least briefly, the world of computing professionals was not. Parson had simply copied the existing Blaster code, created a simple variant (no real skill there), then was almost immediately caught when he released it. Not a lot to admire.

The nature of malware writers has evolved with the technology they exploit. The very first self-replicating programs existed mostly as technical exercises. For the most part, these were generated by graduate school programmers, often as research for doctoral theses. Early on, the field expanded to include teens looking for a technical challenge as well as the stereotypical loner geeks—socially awkward teens using malware to make names for themselves. These writers not only didn't hide their viruses very well, many didn't hide them at all. Their goal was to make as many people as possible aware of what they'd done.

Not surprisingly, many of these malware writers were caught. Even today, some malware includes "authorship" information. In some cases, those really are the names of the malware writers or the groups they represent. In other cases, named authors are themselves additional victims.

More recently, professionals are joining the loop. Mikko Hypponen of the Finnish security firm F-Secure, notes, "We used to be fighting kids and teenagers writing viruses just for kicks. Now most of the big outbreaks are professional operations." They're looking for cash, not infamy.

People still write malware for the challenge or to become famous, but they also write malware to steal intellectual property from corporations, destroy corporate data, promote fraudulent activity, spy on other countries, create networks of compromised systems, and so on. Malware writers know that millions of computer systems are vulnerable and they're determined to exploit those vulnerabilities. Does this mean that all those teen users are turning into computer criminals? No. It simply means that with widespread Internet access, more people are using the Internet to commit crimes.

Wanted Dead or Alive!

Reminiscent of old West bounties, a few malware victims have struck back by offering substantial awards for the capture and conviction of worm and virus writers. Microsoft began the trend, offering $250,000 bounties, and then upping the ante to $500,000 on the Blaster and SoBig authors. Preparing for future attacks, on November 5, 2003 Microsoft funded the Anti-Virus Reward Program with $5 million in seed money to help law enforcement agencies round up malware writers. That approach continues today. In February 2009, Microsoft offered a $250,000 reward for information leading to the arrest and conviction of those responsible for the Conficker worm.

More information than ever is now stored on computers, and that information has a lot of value. You may not realize it, but your computer and your data are at higher risk than ever before. Even if your machine contains NO personal information, NO financial data, and nothing that could be of the slightest interest to anyone, your computer could still be used to attack someone else's. As Justin, a 16-year-old from Atherton, California said, "It's just not right that someone can take over my machine and use it."

2.2 Viruses

A computer virus is a set of computer instructions that self replicate. A virus can be a complete program (a file to itself) or a piece of code—just part of a computer program file. In its most basic form, a virus makes copies of itself.

Virus Number 1

Fred Cohen, then a doctoral student at the University of Southern California, wrote the first documented computer virus in 1983 as an experiment to study computer security. Officials were so concerned, they banned similar projects!

Some viruses are designed to spread only in certain circumstances, like on a certain date, or if the machine belongs to a certain domain.

Some viruses also carry a payload. The payload tells the virus to do damage like delete files or attack other systems. We'll talk more about payloads in the next section.

Even a virus without a payload can cause major problems. Just through the process of making copies of itself, a virus can quickly use up all available memory in your computer. This can slow your computer down to a pathetic crawl and sometimes prevent other programs from running altogether.

A **computer virus** is very much like a biological virus. The flu is a good example of a biological virus that can be transmitted from one person to another. Just how sick you get depends on the type of flu and whether you've been vaccinated. Once you're infected with the flu, you can also spread that virus to every person you come in contact with.

In the worst-case scenario, you could be another Typhoid Mary. As you probably know, Mary Mallon was an immigrant cook working in New York at the turn

of the 20th century. Apparently healthy herself, from 1900 to 1915 Mary spread typhoid fever around town along with her signature peach desserts. Records tell us that she infected between 25 and 50 people and probably caused at least 3 deaths. After the 3rd death, "Typhoid Mary" was placed in quarantine for the rest of her life. In the computer world, carriers have a much larger reach. While Typhoid Mary infected a mere 50 people during a span of 15 years, computer viruses and worms can infect thousands of other systems in just minutes. When Code Red was unleashed in 2001, it infected more than 250,000 systems in only 9 hours.

Virus A piece of code that makes copies of itself. A virus sometimes also includes a destructive payload.

Once a single computer is infected with a virus, it can infect hundreds of thousands of other computers. Just how much damage occurs depends on two things: (1) whether each computer in the chain is protected with current antivirus software, and (2) whether the virus carries a payload. If the virus carries a payload, it may perform harmful requests such as deleting all your data; if it does this, it can't continue to replicate because there are no programs for it to infect. Most viruses don't contain a payload; they simply replicate. While this sounds harmless enough, the copying process uses memory and disk space. This leaves affected computers running slowly, and sometimes not at all.

2.2.1 How Viruses Replicate

Most viruses require human intervention to start replicating. You may inadvertently trigger a virus to begin replicating when you click on an infected email attachment. Once a virus is activated, it can create and distribute copies of itself through email or other programs.

Your machine can be infected by a virus if you:

- Share infected CDs
- Download and run infected software from the Internet
- Open infected email attachments
- Open infected files on a USB drive

Just as the flu reappears each winter with just enough variations to negate last year's flu shot, computer viruses keep coming back as new variants. Often, just a few simple tweaks to the code creates a new variant of the virus. The more variants that are created, the more opportunities a virus can have to get access to your system. McAfee reports that over 200 new viruses, Trojans, and other threats emerge *every day*.

When physicians check for a physical virus, they rely on a set of symptoms that together indicate the presence of that virus. Some antivirus programs use a signature to identify known viruses. You can think of the signature as a fingerprint. When crime scene investigators (CSIs) want to know whether a particular criminal's been on the scene, they check for that person's fingerprints. When antivirus software wants to know whether your machine's been infected with a particular virus, it looks for that virus **signature**.

Signature A unique pattern of bits that antivirus software uses to identify a virus.

2.2.2 Malicious Payloads

All viruses are annoying. Some also have a destructive payload. A payload is a subset of instructions that usually does something nasty to your computer system—or someone else's. The payload may destroy or change your data, change your system settings, or send out your confidential information. The damage can be costly.

Where Do Viruses Come From?

Geographically, viruses are awfully diverse. Some of the more well-known malware actually originated in some pretty unexpected places:

- Brain originated in Pakistan.
- Chernobyl, while referring to a Ukrainian city, originated in Taiwan.
- Michelangelo began in Sweden, not Italy.
- Tequila sounds Mexican, but originated in Switzerland.
- Yankee Doodle, surprisingly, really is an American virus!

When the Chernobyl virus payload was first triggered in 1999, nearly a million computers were affected in Korea alone, costing Korean users an estimated quarter of a *billion* dollars!

A payload commonly used today initiates a denial of service (DoS) attack. This type of attack is usually aimed at a third-party website and attempts to prevent legitimate users from gaining access to that website by literally flooding the site with bogus connections from infected machines. MyDoom.F is a good example of a piece of malware with a destructive payload. MyDoom.F carries a payload that initiates a denial of service attack AND deletes picture files and documents from your PC. More damaging payloads can modify data without even being detected. By the time the deadly payload has been discovered—it's simply too late.

While we tend to think of viruses as attacking programs, they most often infect documents or data files. Unlike programs, which users rarely share indiscriminately, documents travel far and wide. During the writing of this book, the document that contains this chapter traveled between Linda, Denise, the publisher, reviewers, and typesetting. Other documents are FAR more widely traveled. Job seekers may distribute hundreds of resumes via email or upload in search of that perfect position.

2.2.3 Virus Hall of Shame

There are literally tens of thousands of computer viruses. Some are nasty, others funny, still more just annoying. Of the field, we found these viruses to be worthy of note:

Famous Viruses

Virus Name	Release Date	Significance
Stoned	1987	If political activism were a category of virus, Stoned would be its first member. Usually benign, it displayed the message: "Your PC is now stoned! LEGALIZE MARIJUANA!"
Yankee Doodle	1989	This virus serenaded its victims by sending part of the tune "Yankee Doodle" to the system speakers every day at 5 pm.

continues

Famous Viruses *continued*

Virus Name	Release Date	Significance
Michelangelo	1991	This was the disaster that never happened. This virus was designed to delete user data on the trigger date, March 6—Michelangelo's birthday. WIDELY reported in the press, doom-sayers prepped the world for up to 5 million affected machines. March 6 came and went with fewer than 10,000 incidents. What Michelangelo actually accomplished was to make the average computer user aware of computer viruses and to spur massive sales of antivirus software.
Concept	1995	Spread through word processing documents, this virus was one of the first to work on multiple operating systems.
Marburg	1998	Named after Marburg hemorrhagic fever, a nasty form of the Ebola virus that causes bleeding from the eyes and other body openings. The Marburg virus triggered three months (to the hour) after it infected a machine. Random operating system errors followed. Marburg also compromised antivirus products, putting the victim at risk from other viruses.
CH1	1998	Named for the Ukrainian nuclear reactor that imploded in 1986, this family of viruses actually originated in South-East Asia. When the virus triggered on the 26th of the month, it rendered the PC unable to boot AND overwrote the hard drive with garbage characters.
Waledec	2009	Also known as the Valentine's Day virus, targets receive an email from a "secret admirer" with a link to a "Valentine" site. That site actually downloads a program that not only co-opts the target's address list to replicate itself, but installs a bogus antivirus program calling itself MS AntiSpyware 2009. The rogue antivirus program issues repeated warnings that the user's computer is being used to send SPAM, then demands that the user register and purchase the latest version to remove the "virus."

You'll note that many of these viruses are more historic than current. If you're wondering whether viruses are out of vogue, hardly! What's actually happened is that malware has advanced with technology. Old viruses evolve into new viruses (called variants or mutations), and new viruses are being created every day. Many of those viruses now include features of worms, Trojans, and other forms of more advanced malware. The viruses are still there—they're just playing with meaner friends.

You'll also notice that much of the last table is written in past tense. We talk about these viruses as if they no longer exist. That's not technically true. Viruses are a bit like socks that get lost in the washing machine. They have a way of reappearing. Most of these viruses still exist in the wild corners of cyberspace. They're just no longer major threats. That's partly because some of these viruses target technology that's no longer in use. A bigger factor, however, is that antivirus software now routinely searches for them. The truly dangerous viruses at any moment are the ones we don't yet know about.

2.3 Worms

Often people refer to viruses and worms as the same things. However, there are two major distinctions: the ability to travel alone and the ability to stand alone as separate programs.

Viruses require human intervention to start replicating. That is NOT true of worms. A **worm** can make copies of itself on a network or move by itself using email without any human intervention.

Worm A standalone malware program that copies itself across networks.

A worm is also usually a standalone program. A worm *transmits itself* between machines across a network. A virus *attaches itself* to files. When a virus copies itself, it is copying itself to other files on the same machine. (A virus spreads to another machine when one of the infected files is moved to another machine, in most cases by a user who does not realize that her files have been infected.) A worm copies itself to another machine rather than another file on the same machine.

The end result of all that copying is usually denied service. Someone, somewhere who wants to use a network resource can't get to it because the worm is taking up so much disk space or bandwidth. Often, worms initiate a denial of service (DoS) attack against a specific website. Code Red targeted the White House website.

Other worms send out so much garbage data that substantial parts of the Internet stop responding. Financially, this can be devastating. When Slammer brought the

Net to its knees, Continental Airlines had to cancel flights from Newark, New Jersey, because it couldn't process tickets. Slammer also brought down emergency services. Outside Seattle, 911 dispatchers lost access to their call centers. While no deaths were directly reported from this outage, fate could easily have taken another turn.

Worm Number 1

In the early 1980s, Xerox researchers John Shoch and Jon Hupp designed an application to automate installing and updating software across a network. When that application hit a bug, it distributed the bug as well. Shoch and Hupp noted, "The embarrassing results were left for all to see: 100 dead machines scattered about the building." They had unwittingly created the first network worm.

Our society relies on computer networks for a lot more than banking and education. The Sasser outbreak was widely believed to have crashed a train radio network, leaving 300,000 train travelers stranded in Sydney, Australia. Of course, computer networks link more than just our transportation systems. They also link our hospitals and ambulances. Many traffic lights are also computer-controlled. It may only be a matter of time until those pranks prove deadly.

Worms have many ways of getting into your system without your knowledge. They can make their way into your computer from the Internet through a security flaw. You might run a cool game on your computer, but it is really a worm that tricked you into running it by making you think it was only a game. Sometimes, you don't need to do anything. Some of the more devastating worms, Code Red and Slammer, actually spread with NO action required by the user at all.

Worms are also designed to be *fast*. The speed at which they are released once a security flaw is found but before a patch is released is amazingly fast. To make matters worse, **script kiddies** start releasing variants.

Script kiddie A low-talent hacker (often an immature teen) who uses easy, well-known techniques to exploit Internet security vulnerabilities. In the hacker community, being called a script kiddie is a major insult.

One infamous script kiddie was Jeffrey Lee Parson. While still in high school, he released a variant on the Blaster worm. The real malware writer—the person who wrote the original Blaster worm—was never found. Parson was just a copycat. Like Parson, almost anyone can make minor alterations to code. It doesn't require the same skill or creativity that you would need to actually create a worm or virus. Still, the effects of minor alterations can be devastating. Mere weeks after Parson unleashed his Blaster variant, experts estimated that the worm had infected 500,000 computers worldwide. Even that wasn't all his own work. Parson's Blaster variant only infected 7,000 computers. After that, variants on his variant created by still other script kiddies took over.

As worms continue to become more complex and evolved, it isn't just the rate of variant creation that's speeding up. Infection speeds have also dramatically increased. During the Code Red attack in 2001, the number of machines infected doubled every 37 minutes. At the peak of the Slammer attack, the number doubled every 8.5 seconds!

2.3.1 Especially Wicked Worms

Like viruses, worms exist in many shapes and forms. These are some of the more notable worms.

Famous Worms

Worm Name	Release Date	Significance
Morris worm	1988	Robert Morris, Jr., a Cornell graduate student was responsible for what is generally considered to be the first worm released to the Internet. This worm affected 6,000 to 9,000 major Unix machines and shut down a good bit of the Internet as it existed at that time. Morris himself became the first worm writer arrested for his exploits.
Melissa	1999	Melissa was a blended threat that included a virus that attacked Microsoft Word documents. When users opened an infected document, Melissa accessed the user's email address book and mailed itself to up to 50 people.

continues

Famous Worms *continued*

Worm Name	Release Date	Significance
I Love You	2000	The I Love You worm arrived in the form of emails having the Subject: line "I love you" and carrying the attachment, Love-Letter-For-You.txt.vbs. Readers who opened that attachment had their PCs searched for passwords which were emailed back to a website in the Philippines. The worm then re-sent itself to every contact in the reader's Outlook Express address book. This worm makes the list for using social engineering to create a message that even readers who knew better simply HAD to read.
Code Red	2001	Code Red attacked websites rather than PCs. First, Code Red defaced infected sites with the message: `Hello! Welcome to http://www.worm.com! Hacked By Chinese!` At the trigger time, midnight July 19th, infected servers stopped infecting other servers and initiated a massive DoS attack against the White House website. This attack failed only because experts identified the target—on the 18th—and moved the White House website to a different Internet address.
Slammer	2003	Known as "the worm that crashed the Internet in 15 minutes." Slammer *literally* slammed into the Internet at full speed. Within 10 minutes, Slammer had infected 90% of its targets. Within 15 minutes, important parts of the Internet became unusable.
Sasser	2004	Unlike many other worms, Sasser was NOT a mass-mailer. Instead, it attacked via operating system security holes and spread without user intervention.
Conficker	2008	Conficker used a variety of malware techniques to take control of infected remote systems. First detected in November 2008, by January 2009 Conficker had gained control of between 9 and 15 million PCs in nearly 200 countries.
SillyFDC	2009	By late 2010, this worm had gained substantial ground compromising infected machines by downloading and installing additional security threats.

2.3.2 Variants and Mutations

While a single worm or virus is bad enough, few pieces of malware remain in their initial states for long. The original authors, as well as other malware writers, continuously produce new variations on old attacks. The MyTob worm gave rise to 12

additional mutations by month's end. Netsky, in its first six months in the wild, evolved into 29 variants.

Got a minute?

At top speed, Code Red infected over 2,000 servers a minute!

With a biological virus, a single tiny mutation in the virus can mean that the vaccine no longer works. With a computer virus, a tiny variation in the code can prevent antivirus software from identifying the virus. Virus writers know that once someone creates a new virus, they can simply add a few tweaks and get their **variant** past the antivirus engine. Some viruses are even polymorphic and can alter themselves.

Fortunately, antivirus software can detect many new variants through the use of heuristics. Still, variants and mutations continue to cause problems. This is why your antivirus software must be up-to-date. If your virus software hasn't been updated since last week, you don't have the new signatures. And last week's signatures might identify last week's viruses, but not this week's new viruses and mutations. Most mutations are changed just enough to render the last virus signature invalid.

Variant A mutated form of a virus or worm. Variants are usually just different enough that the original virus signature won't match.

To avoid getting slammed by last week's news, always make sure your antivirus software is configured to download updates *automatically* from your antivirus vendor. Don't forget—anti-virus software is only one piece of the security puzzle. Firewalls and intrusion detection/prevention systems can also detect various worms and can be used to prevent unwanted connections. Intrusion prevention software is often bundled into firewall software—software that allows you to detect and sometimes block known attacks from getting into your network.

2.4 Trojan Horses

The name "Trojan horse" derives from Greek mythology. In an exploit reported by the epic poet Virgil in the *Aeneid*, the Greeks gained entrance to the city of Troy by presenting the Trojans with a gift of a giant wooden horse. Delighted by

the gift, the Trojans took the horse beyond the gates and into the city. Overnight, scores of Greek soldiers who had hidden inside the wooden horse emerged. They slew the Trojans in their sleep and opened the gates of their city.

In computer terms, a Trojan horse has a similar objective: to camouflage itself as something harmless or desirable, then to open the door and let attackers in. Just as the ancients learned to "Beware of Greeks bearing gifts," you should always question the motives and real purposes behind free software.

The idea with any Trojan is that it needs to be enticing enough that users will want to run it. In reality, the real purpose of many Trojans is to open a "backdoor" to your computer that allows for easy re-entry. The backdoor allows someone else to control your computer system or access your files without your permission or knowledge. This allows the attacker to return later and steal your confidential information or even use your machine to attack someone else's.

The methods used to trick recipients into installing the Trojan vary. One underhanded approach in 2009 was the Swine Flu Trojan. In this attack, users received an email spoofed to make it look like it came from the Centers for Disease Control and Prevention. The emails, carrying Subject lines such as "Governmental registration program on the H1N1 vaccination" or "Your personal vaccination profile", directed users to create an online profile for their state's H1N1 vaccination program. Users who clicked the provided link installed a Trojan instead.

You can run a Trojan program without actually knowing that you are doing so. Undetected Trojans are lethal and when mixed with a **zero day** attack, they have the potential to cause mass destruction.

A zero day attack is an attack based on a security hole that the experts don't know about. Thus, there's no easy remedy to stop the attack. The Aurora attack was a zero day attack mixed with a Trojan that was used to siphon out confidential information. By the time McAfee Labs discovered the attack on January 14, 2010, the damage had already been done to Google and a reported 34 other companies.

Zero Day attack An attack that takes advantage of a security hole for which there is no current patch.

At first glance, that probably sounds strange. Aren't ALL attacks based on a security hole we don't know about? Surprisingly, no. Most attacks take advantage of fairly well-known vulnerabilities. Those attacks succeed mostly because users don't do a good job of applying updates and patches to fix those vulnerabilities.

Zero day attacks are problematic because there really isn't a good way to protect yourself from a problem that the experts don't know about yet. The Aurora attack is believed to have begun in late 2009, running undiscovered by most victims until mid-January 2010. The Aurora attack was incredibly sophisticated. It used a combination of malware programs, some of which used multiple layers of encryption to hide their activities. The attack was aimed at Google's mail system (Gmail) as well as dozens of other companies involved in technology, finance, media, chemicals, and defense. Because the Gmail attack targeted the accounts of Chinese dissidents, some pundits suggested potential Chinese government involvement.

While Aurora was used mostly to steal source code and other intellectual property from corporations, other Trojans are created specifically to collect information from teens and consumers. For example, Trojan Win32/PSW targets online gamers. This Trojan installs a keyboard logger that captures gamer logins. Thieves use those logins to steal gaming avatars, virtual cash, and treasures.

Sometimes, running a Trojan can also unleash a computer virus or a worm. This combination of nasty code operating together is called a **blended threat**. By attacking in several ways simultaneously, blended threats—even those that aren't zero day attacks—can spread rapidly and cause widespread damage.

Blended threat A form of malware that includes more than just one attack. A blended threat could include a virus, a worm, a Trojan horse, and a DoS attack all in one attack.

2.5 Bot Networks

The Zombie Machine

Tabitha, a junior at Gettysburg Area High School, got off the school bus and ran home to check her email. Because she has friends (real and virtual) spread around much of the world, this is something she did at least 3 times a day. No Internet. Three hours later, still no Internet. And no Internet still later that evening.

Assuming there was a problem with her service, Tabitha had her father brave the rounds of "Please hold" and recorded ads to actually talk to her cable company. What they learned was unexpected and pretty frightening. Earlier that day, her cable company had tracked hundreds of emails coming from her connection. Seeing the massive outflow of email, the cable company cut off her service. Unfortunately, they didn't tell her.

Tabitha was clueless. Like a growing number of home users, Tabitha's parents had networked their home. A simple router (under $50 at Staples) split her Internet cable allowing access from both her computer and her parent's machine. Apparently, her computer had been the victim of a BOT network attack that gotten past the router firewall. Someone else had taken control and was using her PC to launch attacks against other computers. The attacker had literally turned her computer into a "zombie".

This teenager's computer had become part of a bot network. A **bot** network is a collection of compromised machines often called zombies. Each **zombie** machine is under the command and control of the malware writer or hacker—almost always without the knowledge of the machine's rightful owner. The owner of the botnet can issue instructions from a central location, and all of the zombies will carry out these instructions, often to attack more hosts. Tabitha certainly had no idea that her PC had been enlisted in a bot army. Likewise, Tabitha had no idea who took over her machine. She didn't even know what website they were trying to attack. If her father hadn't called the cable company, she may never have even known that her PC had been hijacked. What she did know was that losing her own service, however temporarily, was incredibly frustrating. She also found the idea of having some stranger control her computer just plain creepy.

Zombie or Bot A computer that's been compromised by a piece of code that allows it to be controlled remotely without the computer owner's knowledge.

A **bot network** is a collection of computers that have been infected by a worm or Trojan which installs code (known as a bot) that allows the attacker to launch remote commands and use the systems for future attacks. The "bot" code opens a backdoor that allows the hacker to control the machine and initiate commands remotely.

Bot network A collection of remotely controlled bots. Hackers often use bot networks to launch attacks against other computers.

Once a hacker has assembled a bunch of machines compromised with bots, what he has is literally an army of "bots" that can be used to attack other machines. Frequently, the bots execute a denial of service (**DoS**) attack where so many compromised machines try to connect to a single website that the site itself crashes. In this type of attack, the goal is to flood the target machine with data packets. The data transmitted is usually harmless itself, but the large amount of traffic consumes the target machine's bandwidth. It uses up the Internet resources available to the target machine, keeping it from being able to communicate properly.

The end result is the same in all cases. Legitimate users are denied service because of all the bogus traffic.

DoS A denial of service attack. In a DoS attack, the victim is flooded with so much Internet traffic that legitimate users can't get through.

In recent years, bot networks have been used to attack some of the biggest names in the computing and corporate worlds. Because bot networks are assembled randomly across the World Wide Web, a single command can launch a DoS attack by bot networks at any time, from any place in the world. Or even many places in the world simultaneously. March 2009 saw the identification of a major bot network dubbed "Ghostnet" that included over 1,200 compromised machines in 103 countries.

The majority of machines compromised by bots are outside the United States. By mid-2009, the U.S. held only 18% of bot-controlled machines. Still, that's a huge number of compromised machines. From mid-2008 to 2009, the number of bot-infected machines jumped 50%. McAfee Avert Labs found 12 million new bots just in the first quarter of 2009.

If the threats have been growing, so have the attacks. In a single attack in June of 2004, a massive bot army of compromised home computers managed to shut down the websites of Apple Computer, Google, Microsoft and Yahoo! for a full two hours. How could a single attack kill the websites of four major computer firms at one time? In this case, by focusing on a fifth firm, Akamai. Akamai runs domain name servers that translate domain names, such as www.microsoft.com, into the numerical addresses used by the Internet. Basically, Akamai controls the address book that takes Internet users to certain websites. It so happened that Apple Computer, Google, Microsoft and Yahoo! were all Akamai clients.

So what can you do to keep your machine from attacking other computers? It would seem that the logical solution is to patch your machine. You need to make sure that you've applied all the current patches to your operating system and web browser. However, the real question is how to protect yourself from bad bots (i.e. zombie makers). The first step, as in almost all computer security issues, is to make sure that your antivirus software is installed correctly and ALWAYS up-to-date. It must include anti-spyware and anti-adware detection and removal capabilities. And you should make sure that your PC is sitting behind a very well-defined firewall.

2.6 Social Engineering

Nasty code has been around for over 20 years now. We all know that opening attachments is dangerous, and sharing files can leave you without valid files of your own. Still, every year millions of users fall victim to malware.

A common reason is the use of **social engineering**. Social engineering involves understanding human nature and using that understanding to take advantage of users. It allows malware writers to trick users into breaking their own security

rules. Sarah Granger, writing for *Security Focus*, put it well when she defined social engineering as, "a hacker's clever manipulation of the natural human tendency to trust."

Social engineering Using general knowledge of human behavior to trick users into breaking their own security rules.

A good example of the use of social engineering to spread malware was seen in the Love Bug attack. Most people who opened this virus did so for one of three reasons—all related to basic human psychology:

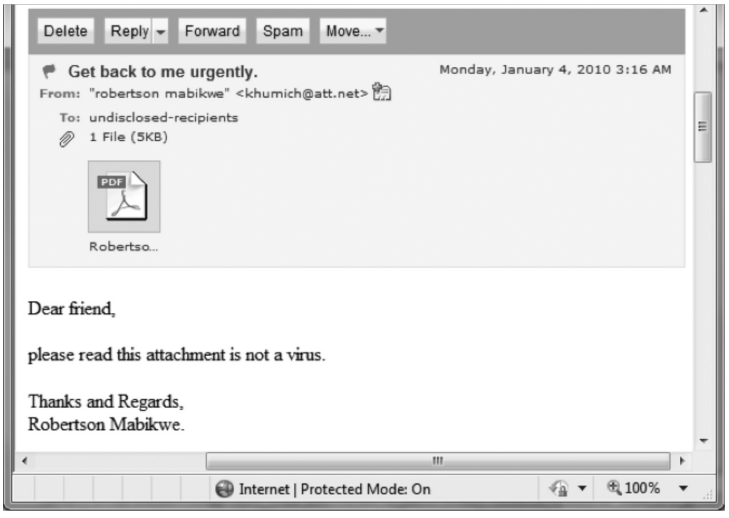
1. The email came from someone they knew and trusted—a colleague, a spouse, an old friend. Someone who might possibly really love them.
2. They thought the email was a joke. Millions of jokes (some much worse than others) circulate the Internet each day. For home users, these humorous anecdotes account for a good percentage of email usage.
3. They just couldn't help themselves. "I love you" messages from distant colleagues, regardless of how unlikely and bizarre, simply jolt the recipient's curiosity.

Of course, social engineering touches more than users' romantic lives. Some common uses of social engineering in malware include guessing passwords, spoofing emails to appear to come from acquaintances, masquerading as authority figures, and never underestimating the human capacity for greed.

Don't I know you?

People love keeping in touch with each other. Spammers rely on this, generating `Subject:` lines that trick the user into believing she might know the message sender. Love Bug relied heavily on this factor to entice users to open the attachment. How easy would it be to trick you into opening an infected PDF someone sent you?

Would you fall for this one?



This example, like many attacks in the last quarter of 2009, exploits a vulnerability in the Adobe Reader program that your computer needs to display PDFs. Like most attacks, this is not a zero day attack. The security hole being targeted was identified and patched some time ago. Yet, these type of attacks succeed because so many users haven't installed the newer versions of Adobe Reader or applied the security fixes.

2.7 Avoiding Malware

Avoiding malware is getting to be a lot more complicated than it used to be. In the past, users could protect themselves fairly well simply by not sharing documents and not opening email attachments from people they didn't know. Today, that's just not enough. Today's user needs to know what to do as well as what not to do.

The first step to protecting yourself from nasty code is to be proactive as well as reactive. Make sure you have the basics covered:

- Install a top-rated antivirus package. No excuses here about not being able to afford it. Microsoft Security Essentials provides free antivirus protection that helps protect your computer against viruses, spyware, and other malware. AVG and Symantec also have free antivirus software (Symantec if you are a Comcast user).

- Use the automatic update option on your antivirus software. Remember that new mutations appear continuously. Automatic updates will help to keep your virus signatures current.
- Be sure to install patches to ALL the software you use. That includes browsers, plug-ins (like Adobe Flash Player), and utility programs like Adobe Acrobat and Adobe Reader.
- Download software only from first-party websites. If you need a new version of Adobe Flash Player, go to the Adobe website. Don't click links in pop-up windows.
- Be very careful about any "free" downloads. Remember that malware often masquerades as freeware.
- Be wary of email from people you don't know. Never open attachments to emails of unknown origin.
- Also be wary of email from people you do know. Some attacks appear to come from someone you know. Also, many worms resend themselves to every person in a victim's online address book. Think long and hard before opening an attachment that you weren't expecting. Call or email the sender first, just to be sure.

OWN YOUR SPACE

KEEP YOURSELF AND YOUR STUFF SAFE ONLINE

THE BOOK FOR TEENS THAT EVERY PARENT SHOULD READ!

A collaborative project to provide free security learning to teens and families online, made available under the Creative Commons Licensing, and made possible by the support of individual and corporate sponsors.

Every day, millions of American school children log on or log in and make decisions that can compromise their safety, security, and privacy. We've all heard the horror stories of stolen identities, cyber stalking, and perverts on the Internet. Kids need to know how to stay safe online and how to use the Internet in ways that won't jeopardize their privacy or damage their reputations for years to come.

Learn how to

- Kill viruses, worms, Trojans, and spyware
- Deal with cyberbullies
- Give SPAM the curb and smash web bugs
- Understand just how public your "private" blogs are
- Keep wireless freeloaders off your network
- Prevent sexting from ruining your life

About the team

Linda McCarthy, the former Senior Director of Internet Safety at Symantec, wrote the first edition of *Own Your Space*. With 20+ years experience in the industry, Linda has been hired to test security on corporate networks around the world. For the 2010 edition, Linda's expertise is backed up by a full team to provide the best security experience possible for teens and families online. That team includes security experts, design experts, anime artists, and parent reviewers, as well as a dedicated group of teen reviewers, web designers, and test readers.

General Computing

ISBN 978-0-615-37366-9

51999>

9 780615 373669

$19.99 US / $24.99 CAN

Cover design: Alan Clements
Cover artist: Nina Matsumoto

www.100pagepress.com

page press
Smart Books for Smart People®