Examples of Malicious Computer Programs Part 2

Keywords

address, addresses, arrest, attachment, attack, attacks, author, authors, Bagle, Blaster, case, cases, code, computer, computers, consequences, conviction, court, crime, criminal, criminals, damage, email, e-mail, Goner, harm, harms, history, infect, infected, injury, injuries, internet, Jaschan, law, laws, legal, mail, malicious, Microsoft, MyDoom, Netsky, Parson, Pechman, perpetrator, program, programs, propagate, propagates, propagation, punish, punishment, restitution, Sasser, Slammer, SoBig, software, victim, victims, virus, viruses, worm, worms

Table of Contents

Introduction

my previous essay

In May 2002, I wrote my first essay about the harm done by malicious computer programs (i.e., computer viruses and computer worms). That essay, which is posted at http://www.rbs2.com/cvirus.htm , discussed fourteen examples of malicious computer programs:

1-5. five early examples, released during the years 1986 to 1994
6. the worm released into the Internet by Robert Tappan Morris in 1988
7. Melissa Virus, released in March 1999
8. ILOVEYOU Worm, released in May 2000
9. Anna Worm, released in February 2001
10. CodeRed, released in July 2001
11. Sircam, released in July 2001
12. Nimda, released in September 2001
13. BadTrans.B Worm, released in November 2001
14. Klez, most significant versions released in early 2002

In May 2002, despite the existence of approximately 60,000 different computer viruses and worms, the authors of *only five* malicious programs had been arrested and punished, which was an appalling failure of the criminal justice system, worldwide. My first essay concluded with the recommendations that (1) legislators enact criminal statutes against authors of computer viruses and worms, with punishment to reflect the damage done by those authors, and (2) legislators allocate more money to the police for finding and arresting the authors of malicious computer programs.

this present essay

This present essay discusses some examples of significant malicious computer programs since my first essay, with emphasis on the harm done and the continued nonexistent or weak punishment for authors of such malicious programs. I have also collected links to legal documents in the prosecution of some authors of malicious programs.

It is *not* my intention to provide information on threats by *current* malicious programs: this essay is only a historical document. You can find information on current threats at websites operated by vendors of anti-virus software, which are linked in my essay at http://www.rbs2.com/cvict.htm#anchor888888 .

This essay is intended only to present general information about an interesting topic in law and is *not* legal advice for your specific problem. See my disclaimer at http://www.rbs2.com/disclaim.htm .

I have not cited a source for each fact mentioned in this essay, because most of these facts have been reported at many different sources, and are well known to computer experts who are familiar with viruses and worms. Further, this essay is not a formal scholarly document, with numerous citations, but only an informative review intended for attorneys, legislators, the general public, students, businessmen, etc. Some general sources are mentioned in my first essay on this topic, at http://www.rbs2.com/cvirus.htm#anchor999950 . In this present essay, most of the technical description of the malicious programs comes from information at the Symantec Anti-Virus (http://www.symantec.com/avcenter/vinfodb.html) and F-Secure (http://www.europe.f-secure.com/virus-info/) websites. I have used Symantec's names for variants of worms. Some other anti-virus vendors may use a different letter to denote the same variant.

The many epidemics of new malicious programs in the year 2004, along with the arrests of perhaps a dozen authors of malicious programs worldwide during the year 2004, means that keeping this essay up-to-date is no longer possible in my spare time. Therefore, this essay will be updated only sporadically and only to include the most significant examples of malicious programs. (Frequent revisions and more comprehensive coverage could be done if there were long-term funding from either the U.S. Government or the computer industry to reimburse my time spent on this project.)

rapid propagation

As an indication of how bad the situation is, data[1] from February 2004 through July 2004 show that a new computer running Microsoft Windows XP will have an average survival time of less than twenty minutes on the Internet, before being infected by malicious software. Twenty minutes is *not* enough time to download and install the latest security patches from Microsoft, although it *might*[2] be enough time to download and install the latest anti-virus definitions. This rapid propagation of malicious programs via Internet (*not* via e-mail) is more than a threat to new computers — the rapid propagation means that all vulnerable computers that are connected to the Internet will be infected *before* anti-virus software vendors can identify a new malicious program, develop a virus definition of it, and upload the new virus definition to their website for users to download. Examples of worms that propagate via the Internet include Slammer, Blaster, and Sasser, each of which is discussed in this essay.

---

[1] Scott Granneman, "Infected in 20 minutes," *The Register,* 19 Aug 2004, http://www.theregister.co.uk/2004/08/19/infected_in20_minutes/ , citing data from SANS Institute, http://isc.sans.org/survivalhistory.php .

[2] If the anti-virus software were installed from a CD-ROM *before* the computer was first connected to the Internet.

Goner Worm

The Goner worm was released on 4 December 2001 in an attachment `Gone.scr` that was purportedly a screen saver, but was actually a worm. The worm did the following things on a victim's computer:

1. attempts to delete anti-virus software, including Norton Anti-Virus and McAfee anti-virus, which makes the victim's computer vulnerable to other malicious programs.
2. attempts to delete firewall software, including Zone Alarm.
3. looks for the address book in Microsoft Outlook, then it automatically sent the following e-mail to every address there, with text:

   Subject: Hi
   How are you? When I saw this screen saver, I immediately thought about you
   I am in a harry, I promise you will love it!
   Attachment: GONE.SCR
4. also sends itself to all friends who are connected to ICQ.
5. inserts scripts into victim's mIRC subdirectory, to enable the victim's computer to be used in denial of service attacks. When the victim starts the IRC program, the script connects to IRC via `twisted.ma.us.dal.net` , then joins the `#pentagonex` channel, without the victim's knowledge. (DALnet subsequently removed the `#pentagonex` channel that Goner used, so this exploit no longer functions.)

The Goner worm was written in Microsoft Visual Basic, using the source code for the Melissa virus as a starting point. News reports do not identify where the author of the Goner worm found the source code for the Melissa virus, but presumedly it was downloaded from a website.

Perpetrators of Goner Worm

The Goner worm was created by a 15-year old boy in Nahariya, Israel. On 4 Dec 2001, the author gave the Goner worm to three of his local friends, all of whom were between 15 and 16 years of age, to spread via the Internet. The four boys were arrested on 7 Dec 2001 and taken to jail, where they were interrogated by police for several days. All four confessed their roles in writing and distributing the Goner worm. At a hearing before a judge on 10 Dec 2001, the four were released to their parents and ordered to remain at home.

At the time of their arrest, police also seized the boys' computers, for forensic examination. However, three of the boys had already deleted relevant files from their computers. While the deletion of files frustrated the investigation, it also allowed the boys to be charged with the crime of destruction of evidence.

Because these four perpetrators are all juveniles (i.e., less than 18 years of age), their names can not be publicly disclosed, and all court proceedings involving them are closed to the public. Therefore, the available information on this legal case is limited.

On 18 July 2002, the Haifa District Attorney's office indicted five boys: the four who were arrested in Dec 2001, plus one 13-year old boy from a town near Haifa, Israel.
An English-language translation of the Indictment was posted at http://www.4law.co.il/350.pdf by Boaz Guttman, a former Israeli policeman and currently an attorney in Israel who specializes in computer crimes and fraud. The indictment mentions four distinct crimes:

1. creating a malicious computer program
2. distributing a malicious computer program
3. fraud (i.e., Goner was deceitfully presented to potential victims as a screensaver program)
4. destruction of evidence (i.e., deleting files from the perpetrators' computers)

Journalists apparently stopped reporting on this case a few days after the arrests. I can find no mention on the Internet of a trial, and no mention on the Internet of any punishment for these five accused perpetrators. My e-mail to the Israeli government has gone unanswered.

Slammer

On 25 January 2003 at about 05:30 UTC the Slammer worm appeared. This tiny worm, with a size of only 376 bytes, infects a computer and then continuously attempts to send a copy of itself to port 1434 at randomly selected IP addresses. Computers that run Microsoft SQL Server 2000 will be infected,[3] because of a defect in that Microsoft software. Because Slammer exploits a defect in SQL, Symantec called this worm SQLExp.

For users whose computers were *not* running Microsoft SQL Server 2000, the harm from Slammer came from the prolific amount of Internet traffic generated by Slammer. F-Secure reported that:

1. Immediately after its initial release, Slammer scanned all *four billion* IP addresses in less than 15 minutes, making it the most rapidly propagating worm, as of the year 2003.
2. Five of the thirteen Internet root nameservers crashed on 25 Jan 2003, owing to extraordinarily large number of requests from copies of Slammer.

For users running Microsoft SQL Server 2000, Slammer put their machine into an infinite loop. The Slammer worm could be cleared from memory simply by turning the infected computer off, then on. However, the computer would then be quickly reinfected, probably before

[3] This SQL Server software is embedded in Microsoft Data Engine 2000, which is installed by several dozen different applications from Microsoft or other vendors, so a user might inadvertently have SQL Server running on his/her computer.

the patch to SQL could be downloaded from the Microsoft website and installed to remove the defect that allowed infection. Many anti-virus programs fail to detect the Slammer worm, because the worm resides in random access memory, *not* on the hard disk. This means that careful users who *never* clicked on an attachment in e-mail could still have their computers infected by Slammer.

The Slammer worm was notable because it was the first of several significant malicious programs (i.e., Blaster and Sasser) that exploited a defect in Microsoft operating systems. These malicious programs spread automatically via the Internet, *not* via e-mail.

Slammer perpetrator

To the best of my knowledge, the author of the Slammer program was never identified, so there can be no legal consequences for him. F-Secure notes that the tiny size of the Slammer worm "suggests that it was written and hand optimized using the Assembly language."[4] This skillful use of assembly language suggests to me that the author of Slammer was a professional computer programmer.

SoBig

On 9 January 2003, the first version of the SoBig worm was found. Some anti-virus vendors called the early versions of SoBig by the names Palyh or Mankx. A variant, named SoBig.F, appeared on 18 Aug 2003 and caused the most harm of the SoBig family. SoBig is notable because it downloaded and installed a program on a victim's computer, which program provides a backdoor on the victim's computer that can be used by spammers to send spam e-mail.

propagation of SoBig.F

The SoBig.F worm arrives in an e-mail with the following characteristics:

To: [address found on victim's computer]
From: [address found on victim's computer]
Subject: [either] "Your details" [or] "Thank You!" [or] "Re: Details"
Body: [either] "See the attached file for details" [or] "Please see the attached file for details."
Attachment: [one of the following filenames]
your_document.pif
document_all.pif
thank_you.pif
your_details.pif
details.pif

---

[4] F-Secure, Slammer Description, http://www.f-secure.com/v-descs/mssqlm.shtml .

document_9446.pif
application.pif
wicked_scr.scr
movie0045.pif

SoBig.F scans files on the victim's computer with file types `.wab, .dbx, .htm, .html, .eml, .txt` and harvests e-mail addresses for the **To:** and **From:** lines of e-mail sent by the worm to propagate itself. Such a fraudulent **From:** address has been used by many previous malicious programs.

harms from SoBig

SoBig.A downloaded the Trojan Horse program Backdoor.Lala, which installed a backdoor on the victim's computer. This backdoor could be used to download and execute files, which could send spam e-mail. SoBig.A, which was discovered on 9 Jan 2003, is apparently the first worm to serve spammers, and, for that reason, SoBig is a landmark in the history of malicious computer programs.

SoBig.E and .F can download a file from a specified Internet address to the victim's computer at a specified time. The Symantec report on SoBig.E and .F tersely says "The author of the worm has used this functionality to steal confidential system information and to set up spam relay servers on infected computers."

The SoBig family of worms contains instructions to disable propagation of the worm after a certain date. For example, SoBig.F will not propagate after 9 Sep 2003 if the clock on the victim's computer is set correctly. However, an infected computer will continue after 9 Sep 2003 to download files from the Internet to the victim's computer, and the victim's computer can continue to serve as a relay for spam e-mail.

MessageLabs, an e-mail filtering service, reported that at the peak of the SoBig.F epidemic on 6 Sep 2003, one in every 17 e-mails (6%) contained SoBig.F.

SoBig perpetrator

To the best of my knowledge, the author of the SoBig program was never identified, so there can be no legal consequences for him.

Blaster

On 11 August 2003, the first version of the Blaster worm (also called MSBlast or Lovsan) was found. Subsequently, many variants of this worm appeared. This worm is notable for three reasons:

1. Unlike most previous worms that required the victim to click on an attachment in e-mail, Blaster generated random IP addresses and automatically attempted to contact and then infect computers with a defective operating system (i.e., Microsoft Windows 2000 and Windows XP) that were connected to the Internet. The Blaster worm did *not* send e-mail.
2. Blaster apparently inspired Microsoft, on 5 Nov 2003, to announce it was setting aside five million dollars as a reward fund for people who informed police of the identities of authors of malicious programs. Microsoft specifically offered US$ 250,000 for information leading to the arrest and conviction of the author(s) of the original Blaster worm.
3. Authors of several variants of Blaster were arrested.

The Symantec description of the original Blaster worm tersely says "The worm also attempts to perform a Denial of Service (DoS) on the Microsoft Windows Update Web server (windowsupdate.com). This is an attempt to prevent you from applying a patch on your computer against the DCOM RPC vulnerability." The code for Blaster contains the following comment:

```
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money
and fix your software!!
```

One can see why Blaster irritated Microsoft enough to begin its reward program for reporting the author(s) of Blaster and other malicious programs.

Microsoft developed a software tool to remove the Blaster worm from an infected computer. By 2 April 2004, the tool had been downloaded about eight million times, which suggests that at least eight million computers were infected with Blaster. I say "at least", because some infected computers may have been cleaned with removal tools available from various anti-virus vendors' websites, and other infected computers may have simply had their hard disk reformatted and all software freshly installed.

Perpetrators of Blaster

To the best of my knowledge, the author of the original Blaster program (i.e., Blaster.A) was never identified, so there can be no legal consequences for him.

On 19 August 2003, federal agents searched the house of Jeffrey Lee Parson of Hopkins Minnesota on suspicion that he wrote the Blaster.B worm, which was initially released on 13 Aug 2003. Federal agents found him quickly, because the code for his Blaster.B program sent reports of infection to the `www.t33kid.com` website, which was registered to Parson. Further,

he changed the Blaster filename from the original `MSBlast.exe` to `teekids.exe`, which referred to his online identity. During the search on 19 Aug, Parson admitted to the federal agents that he was responsible for the Blaster.B worm. Parson was arrested on 29 Aug 2003.

Because one of the harms of this worm was a denial-of-service attack on the Microsoft website, prosecution of the case was transferred to U.S. District Court in Seattle, near the Microsoft headquarters. Although Parson owned seven computers, he could not afford an attorney, so a federal public defender was appointed to represent him. At the time Parson released Blaster.B, he was several weeks past his 18th birthday, which qualified him to be treated as an adult by the courts. He was arraigned on 17 Sep 2003, where he initially pled "not guilty". On 11 Aug 2004, Parson pled guilty and he agreed to a prison sentence between 18 and 37 months.

Parson's principal modification of Blaster.A was to add a backdoor to the original worm, so that Parson could access victims' computers. He apparently found the code for the backdoor at a hacker website.

At the court hearing where Parson pled guilty, newspapers reported some remarks by his public defender:

> One of Parson's lawyers, Carol Koller, said that Parson was young when he committed the attacks and that being arrested made him realize the seriousness of his crime.
>
> "He has been exemplary," she said. "He has not touched a computer since the day of his arrest."

Gene Johnson, Associated Press, "Man Pleads Guilty to Sending Out 'Blaster' Worm," *The Washington Post,* p. E05, 12 August 2004.

I'm sorry to need to say this, but society can not excuse felons who need to be arrested and charged in court *before* those felons learn to avoid *un*lawful conduct that harms other people. Parson was *not* accused of unlawful conduct *after* his arrest, so his attorney's remarks are irrelevant.

While it was appropriate that Parson be arrested and punished for his crime, it is also important that we keep him in proper perspective. Parson was an amateur who made a few minor modifications in Blaster.A, which was written by an *un*known criminal. At his guilty plea, federal prosecutors stated that Parson's worm, Blaster.B, had infected "more than 48,000 computers", which is a trivial fraction of the total of more than eight million infections by the Blaster.A and other variants.

On 28 Jan 2005, Parson was sentenced by Judge Marsha Pechman in U.S. District Court in Seattle to:

- 18 months in prison
- 3 years of supervised release after prison, including mandatory testing for illicit drugs and mental-health treatment. Parson will be forbidden to use Internet chat rooms and video games.
- 100 hours of community service, which can include classes taken in a classroom with face-to-face contact with people, but not classes via the Internet
- pay restitution in an amount to be determined at a future hearing (see page 12, below)

The prison sentence was the *minimum* allowed by Parson's plea bargain (which had a range of 18 to 37 months in prison), because the judge:

(1) blamed his parents for his problems,
(2) believed that Parson was less mature than his 18 y age at the time of his crime, and
(3) repeated some vague allegations that Parson had an *un*specified "mental illness".

The judge's remarks at Parson's sentencing, as reported by journalists, are interesting:

> U.S. District Judge Marsha Pechman said Jeffrey Lee Parson's neglectful parents were to blame for the psychological troubles that led to his actions in the summer of 2003.
>
> The Internet "has created a dark hole, a dungeon if you will, for people who have mental illnesses or people who are lonely," Pechman said. "I didn't see any parent standing there saying, 'It's not a healthy thing to lock yourself in a room and create your own reality.'"
>
> ....
>
> Pechman said she was sentencing him at the low end of the range because although he was 18 at the time of the attack, his maturity level was much younger than that.
>
> ....
>
> "What you've done is a terrible thing," Pechman told him. "Aside from injuring individuals and their computers you shook the foundation of the system."
>
> "I learned a lot about you," she added. "Many of the mental-health problems from the household you grew up in contributed to this problem."

Gene Johnson, Associated Press, "Judge takes pity on defendant in Internet worm case, blames parents", *Seattle Post-Intelligencer,* 28 Jan 2005, 16:11 PST.

Another reporter in Seattle wrote:

> A federal judge gave Jeffrey Lee Parson the minimum sentence of 18 months in prison yesterday for releasing a version of the Blaster computer worm into the Internet in 2003.
>
> U.S. District Judge Marsha Pechman could have sentenced Parson to as many as 37 months — the maximum end of the range agreed to by lawyers on both sides of the case.
>
> Instead, she said she was swayed to a more lenient sentence because of Parson's history of mental-health problems and because his home life "sounds grimmer than many prison camps I've visited."

....

Pechman wondered aloud in court how much of Microsoft's damages Parson should pay for. In the real world, she said, if a home's front door was left open and a television was stolen, should the thief have to replace the television, pay for the front door to be nailed shut and pay for a home-security system?

....

No one in Parson's family was in court yesterday. Parson's lawyer, Nancy Tenney, said in court that he never received the attention, guidance and parenting that children require. By the time he entered junior high, he suffered from a mental illness that was so severe he was afraid to leave his own home, she said.

The computer became an escape for Parson, and online he was able to become part of a group of friends without having to leave the house, Tenney said.

"These positive influences that Jeff found in this community clouded his vision," she said, "clouded his common sense."

Many details about Parson's home life were sealed from public access. After reviewing them, Pechman said that if she had known what his circumstances were, she might have suggested removing him from the home earlier.

Kim Peterson, "Blaster Hacker Receives 18-month Sentence," *Seattle Times,* 29 Jan 2005.

And a third reporter in Seattle wrote:

Before sentencing Parson, Pechman told the young hacker he had done "a terrible thing. You shook the foundation of the system" by damaging trust in the Internet. But the judge noted that Parson had just turned 18 when he launched his attack and that his psychological evaluation indicates that he had the maturity of someone much younger.

"The Internet is a wonderful thing," said the judge. "But it has created a dark hole, a dungeon if you will, for people who have mental illnesses or people who are lonely."

And Pechman — who said Parson's home "sounds much grimmer than some prison camps I know of" — asserted that Parson's father led him into that hole.

His parents were not at the sentencing, Tenney said. "Jeff's parents are unable to provide guidance and support," she said.

....

Once Parson gets out, he will be put under the supervision of a probation officer who will require that he get mental-health treatment.

Pechman also ordered him to perform 100 hours of community service, in part as a way to force the young man to have as much contact with other people as possible.

She also barred Parson from using computers for video games or chat rooms. Only educational or business computer use will be allowed.

"We're not going to have imaginary friends," said Pechman. "I want you to have real friends."

Paul Shukovsky, "Blaster worm attacker gets 18 months," *Seattle Post-Intelligencer,* 29 Jan 2005.

restitution

The hearing to determine the amount of restitution that Parson would pay was originally scheduled for 10 Feb 2005, but was postponed until 4 Apr 2005, as attorneys for Parson negotiated with both Microsoft and the Assistant U.S. Attorney who prosecuted the criminal case. Journalists reported that Microsoft and the prosecutor were initially seeking restitution of more than one million dollars. Finally, Microsoft and the prosecutor agreed on 29 Mar 2005 that Parson owed only $ 497,546 to Microsoft. In the same agreement, Microsoft agreed to accept a total of 225 hours of community service following his imprisonment, instead of monetary restitution. The following sentence from the agreement was also included in the Amendment Judgment by Judge Pechman:

> These hours are not to be performed in an area dealing with computers or the Internet, and instead are to be performed working with less fortunate members of the defendant's community.

Note that Judge Pechman's Amended Judgment on 4 April 2005 — while intended only to specify the amount of restitution that Parson would pay — also deleted her initial sentence of 100 hours of community service "that involves direct contact with people" and replaced that requirement with 225 hours of community service, as agreed between Microsoft Corp. and Parson.[5]

my comments on Parson's sentence and restitution

I find appalling Judge Pechman's speculation on 28 Jan 2005 that Parson should not need to pay for Microsoft's *entire* cost of investigating and repairing the damage caused by Blaster.B. We do not blame rape victims for wearing clothing that allegedly provoked their rape. We don't blame elderly people for walking to a grocery store with money for groceries, although they are an easy target for robbery. A victim's imprudent act(s) that made them an easy target for a criminal is *not* a legitimate justification for the crime, nor should it reduce the amount that the guilty criminal must pay to the victim in restitution.

Judge Pechman appears to believe that Parson avoided face-to-face human contact and concentrated his relationships with people in chat rooms, who were a bad influence on Parson. But Judge Pechman ignores the possibility that, if Parson had avoided computers and had face-to-face relationships with local people, Parson might have chosen friends who were anarchists, rebellious, criminals, or gang members. So blaming Parson's crimes on his self-imposed isolation and his indulgence in online chat rooms is *not* justified. And, despite Judge Pechman's remarks, people are "real", regardless of whether one meets them face-to-face or in an online chat

---

[5] Compare item 13, page 4 of the 28 Jan 2005 Judgment at http://www.rbs2.com/parson1.html with the same "additional supervised release" item of the 4 April 2005 Amended Judgment at http://www.rbs2.com/parson2.html .

room. One wonders if Judge Pechman's career in law, which involves intensive face-to-face contract with people, influenced her opinion. Some other careers (e.g., computer programming, research in physics, etc.) are essentially solitary endeavors.

As for Parson's alleged mental health problems, many computer programmers who I know spend more time alone with their computers than in face-to-face social settings. But that does not make these programmers either criminals or insane, and neither should Parson's self-imposed isolation mitigate his responsibility for his crimes. Note that Parson pled guilty, which includes an admission that he was sane at the time of his criminal act(s). In effect, he admitted that he knew that his acts were wrong and harmful to people.

Although not part of the criminal indictment, prosecutors noted that Parsons *also* had engaged in attacking websites of the Recording Industry of America and motion picture companies.[6] Furthermore, Parson was *not* charged with installing and using a "backdoor" to access approximately fifty computers. According to his plea agreement, Parson used these fifty computers to release the first wave of Blaster.B worms. Parson's *un*authorized access of these fifty computers should have constituted a separate crime (perhaps under a state statute) from the harm caused by his Blaster.B program.

As for the restitution accepted by Microsoft, a total of 225 hours of community service has an effective value of $497,547, which is equivalent to an outrageous $2211/hour. I say "outrageous", because Microsoft's agreement overvalues Parson's time[7] by a factor of at least 220.

Equally troubling is the restitution to be paid to the eight individual victims of Blaster.B. Their victim impact statements show a total of $ 3487 in remediation expenses, for an average of $ 436/victim. Because some of the victims had replaced their computers, instead of having a technician remove the Blaster.B infection, so the judge allowed a maximum of only $ 150 in restitution per infected computer. The plea agreement[8] declares that *more* than fifty computers were infected with Blaster.B, while journalists[9] mention approximately fifty thousand computers. Therefore, a fair estimate of the damage inflicted by Parson on *un*identified computer owners is more than $ 7500 and probably closer to $ 7.5 million. While Parson's attorneys quibbled over

---

[6] These websites were probably targeted because of their litigation against people who infringed their copyrights. Copyright infringers often attempt to portray themselves as victims, instead of admitting their wrongful conduct.

[7] Parson, who is a 20 y old high-school graduate with no college classes, has a fair market value of his time of less than $ 10/hour. On the other end of the scale, a computer scientist with an earned doctoral degree and substantial professional experience is worth about $70/hour.

[8] Plea Agreement, http://www.rbs2.com/parson0.html , Fact j, page 6 (11 Aug 2004).

[9] Leslie Brooks Suzukamo, "Microsoft settles with virus creator," *Pioneer Press,* 30 Mar 2005.

payment of $ 100/victim vs. an average of $ 436/victim to the eight identified victims, no one noticed that *most* of Parson's victims would *never* be compensated.

It is a basic principle of criminal law in the USA *not* to impose fines or restitution that the defendant can not reasonably be expected to pay. Suppose Parson works for forty years at a salary of $30,000/year, and he pays 10% of his salary as restitution without interest. With these assumptions, Parson can pay only $120,000 in restitution during his lifetime. Regardless of whether the proper restitution is a half-million dollars or more than eight million dollars, Parson can *not* feasibly pay full restitution for the damage that he caused.

In conclusion, given the multi-million dollar damages caused by Parson's Blaster.B worm, a mere 18 months imprisonment plus a total of 225 hours of community service[10] is a remarkably lenient punishment. Judge Pechman's gratuitous comments about the lack of parental supervision, Parson's avoiding face-to-face contact with people, and Parson's alleged mental illness, should all be irrelevant to his sentence.

The leniency of Parson's sentence is apparent from comparing it to the sentence in another federal case, approximately two weeks later. William Jensen Cottrell was sentenced to 100 months in federal prison and ordered to pay $ 3,583,544 in restitution for arsons and vandalism at four automobile dealerships in the Los Angeles area.[11] Cottrell was 22 y old at the time he committed his crimes, just 4 years older than Parson. Cottrell's crimes arguably caused almost five million dollars of damage, *less* than the eight million dollars of damage arguably caused by Parson's worms. Cottrell had two assistants (both of whom were fugitives from justice at the time of Cottrell's trial) while Parson worked alone — so one might argue that Cottrell alone was responsible for 1/3 of five million dollars of damage, which is only 20% of the damage that can be attributed to Parson. Despite the fact that Cottrell arguably did *less* damage than Parson, Cottrell received a prison sentence that was more than five times longer than Parson, and Cottrell was ordered to pay more than seven times[12] as much restitution as Parson. One reason for the disparity in the punishment of Cottrell and Parson is that it is easy to prove the amount of damage caused by destroying automobiles and buildings, while most of the victims of a computer worm (and their remediation expenses) remain unknown to the court.

---

[10] Recognize that 225 hours is slightly less than six weeks of working 8 hours/day, 5 days/week.

[11] *U.S. v. Cottrell,* 04-cr-00279 (C.D.Calif. 18 April 2005); David Rosenzweig, "Student Sentenced in SUV Firebombings," *Los Angeles Times,* (18 April 2005).

[12] Comparing $ 3.58 million for Cottrell to $ 0.504 million for Parson, assuming Parson chooses to pay restitution to Microsoft.

links to *U.S. v. Parson* documents

The following documents about Parson's crime are available on the Internet:

- 28 Aug 2003 arrest warrant
  http://news.corporate.findlaw.com/hdocs/docs/cyberlaw/usparson82803cmp.pdf

- 29 Aug 2003 press release from U.S. Department of Justice about arrest:
  http://www.usdoj.gov/criminal/cybercrime/parsonArrest.htm

- 29 Aug 2003 press release from FBI in Minneapolis about arrest:
  http://www.fbi.gov/fieldnews/august/doj082903.htm

- 10 Sep 2003 Indictment by grand jury:
  http://news.corporate.findlaw.com/hdocs/docs/cyberlaw/usparson91003ind.pdf

- 11 Aug 2004 press release from U.S. Department of Justice about guilty plea:
  http://www.usdoj.gov/usao/waw/press_room/2004/aug/parson.htm
  Adobe PDF copy of Plea Agreement:
  http://www.usdoj.gov/usao/waw/press_room/2004/aug/pdf_files/cr03-379p_plea.pdf

- I posted an HTML version of the 11 Aug 2004 Plea Agreement:
  http://www.rbs2.com/parson0.html

- 28 Jan 2005 press release from U.S. Attorney in Seattle about sentence:
  http://www.usdoj.gov/usao/waw/press_room/2005/jan/parson.htm
  http://www.usdoj.gov:80/criminal/cybercrime/parsonSent.htm

- I posted an HTML version of the 28 Jan 2005 Judgment:
  http://www.rbs2.com/parson1.html

- I posted an HTML version of the 29 March 2005 agreement between Microsoft and Parson:
  http://www.rbs2.com/parson3.html

- I posted an HTML version of the 30 Mar 2005 Memorandum by the U.S. Attorney about the amount of proper restitution to individuals:
  http://www.rbs2.com/parson4.html

- I posted an HTML version of the 4 Apr 2005 Amended Judgment:
  http://www.rbs2.com/parson2.html

Bagle

On 18 January 2004, the first version of the Bagle worm, called Beagle by Symantec, appeared. This worm is notable for:

1. After Bagle infected a victim's computer, Bagle downloaded the Mitglieder Trojan Horse program from a website to the victim's machine. Mitglieder installed a backdoor on the victim's computer that could be used by spammers to send spam e-mail. (Earlier, SoBig.E and .F has installed a similar backdoor for use by spammers.)
2. In Bagle.H and some later variants, the attachment containing the worm was compressed as a ZIP file *and* password protected. A password protected compressed file is more difficult for anti-virus scanners to inspect, since the scanner does not know the password used to compress the file. The password was contained in the body of the e-mail that propagated the worm.
3. Bagle.J through Bagle.O sent a deceptive e-mail that pretends to come from management at the recipient's domain and instructed recipients to click on the attachment, which caused the recipient to become a victim of the worm. The deceptive e-mail, which is described in detail below, was an advance in the art of persuading recipients to become victims.

Propagation of Bagle

Most versions of Bagle propagated by sending e-mail containing the worm as an attachment, although a few versions also attempted to spread via file-sharing networks (e.g., Kazaa and iMesh). According to Symantec, the e-mail sent by Bagle.J has the following characteristics, where `<domain>` is the domain name of the recipient's e-mail address (i.e., if your e-mail address is `joe@abc.com`, then `<domain>` is `abc.com`):

From: [One of the following]

- `management@<domain>`
- `administration@<domain>`
- `staff@<domain>`
- `noreply@<domain>`
- `support@<domain>`

Subject: [One of the following]

- `E-mail account disabling warning.`
- `E-mail account security warning.`
- `Email account utilization warning.`
- `Important notify about your e-mail account.`
- `Notify about using the e-mail account.`
- `Notify about your e-mail account utilization.`
- `Warning about your e-mail account.`

There are a large number of possible messages, the following are six examples that I constructed using text at Symantec's description of Bagle.J:

```
(1)Dear user of <domain>,
   Your e-mail account has been temporary disabled because of
   unauthorized access.
   For more information see the attached file.
   The <domain> team                              http://www.<domain>
   The Management,

(2)Dear user of <domain> gateway e-mail server,
   Our main mailing server will be temporary unavaible for next
   two days, to continue receiving mail in these days you have to
   configure our free auto-forwarding service.
   For more information see the attached file.
   The <domain> team                              http://www.<domain>
   The Management,

(3)Dear user of e-mail server "<domain>",
   Your e-mail account will be disabled because of improper using
   in next three days, if you are still wishing to use it, please,
   resign your account information.
   Further details can be obtained from attached file.
   The <domain> team                              http://www.<domain>
   The Management,

(4)Hello user of <domain> e-mail server,
   We warn you about some attacks on your e-mail account.
   Your computer may contain viruses, in order to keep your
   computer and e-mail account safe, please, follow the
   instructions.
   Further details can be obtained from attached file.
   The <domain> team                              http://www.<domain>
   Have a good day,

(5)Dear user of "<domain>" mailing system,
   Our antivirus software has detected a large ammount of viruses
   outgoing from your email account, you may use our free
   anti-virus tool to clean up your computer software.
   Please, read the attach for further details.
   The <domain> team                              http://www.<domain>
   Have a good day,
```

```
(6)Dear user, the management of <domain> mailing system wants to
   let you know that, some of our clients complained about the
   spam (negative e-mail content) outgoing from your e-mail
   account.  Probably, you have been infected by a proxy-relay
   trojan server.  In order to keep your computer safe, follow the
   instructions.  Pay attention on attached file.
   The <domain> team                              http://www.<domain>
   The Management,
```

As you can see, the above message is likely to convince someone to click on the attachment, in order to either continue using their e-mail account (messages 1-3 above), or to remove the alleged virus from their computer (messages 4-6 above). The clever design of these fraudulent messages is an indication that the author of this worm *intended* to convince the victim to click on the attachment and become infected.

In my first essay on malicious programs at http://www.rbs2.com/cvirus.htm#anchor555220 , I observed that grammar errors, punctuation errors, and spelling errors in a message apparently from a native speaker of English is suggestive that the message has a forged `From:` address and the attachment may contain a malicious program. This observation is correct again for Bagle.J, as shown by the above-quoted e-mail sent by that worm.

The e-mail contains an attachment in ZIP format, which is password protected to make it more difficult for anti-virus software to detect the worm in the attachment. Also a knowledgeable recipient is more likely to click on an attachment with a file type (e.g., a wordprocessing document or `.zip`) that is common in nonmalicious e-mail, than to click on an executable file type (e.g., `.exe` `.pif` or `.scr`) that could be a virus or worm. According to Symantec, the e-mail contains one of the following sentences or something similar:

- `For security reasons attached file is password protected. The password is "<password>".`
- `In order to read the attach you have to use the following password: <password>.`

Bagle perpetrator

To the best of my knowledge, the author of the Bagle program was never identified, so there can be no legal consequences for him.

MyDoom

On 26 Jan 2004, the first version of the MyDoom worm, also called Novarg, appeared and did the following harms:

1. Like SoBig.E and .F, and like some variants of Bagle, MyDoom installed a backdoor on a victim's computer, which could be used by spammers to send junk e-mail.
2. MyDoom.A executed a distributed denial-of-service attack on the SCO website between 1 Feb and 12 Feb 2004. Because the clocks were set to the wrong date on many victims' computers, the SCO website remained offline until about 5 March 2004. The SCO website was apparently chosen for attack because SCO had filed litigation seeking royalties for use of Unix software that is owned by SCO.
3. MyDoom.F performed a denial of service attack on websites of Microsoft and RIAA, and also deleted randomly chosen files from the victim's disk drives, including document files.
4. MyDoom.M appeared on 26 July 2004 and caused a novel kind of harm. MyDoom.M searched a victim's hard disk to find domain names, then used search engines to find e-mail addresses at those domains. MyDoom sent a copy of itself to the e-mail addresses constructed in this way. As a result of a flood of searches, the Google search engine was *un*available to legitimate users for part of Monday 26 July 2004.

It is truly chilling that authors of worms will attack websites of companies with whom the authors disagree — such attacks are censorship, repression, and self-appointed vigilantism. If the U.S. Government attempted to censor the Internet, one could file litigation in federal court challenging such censorship, and – indeed – many past court challenges of this type have been successful. In contrast, censorship of the Internet by criminals hiding under a cloak of anonymity, and who get innocent victims' computers to do their dirty work, is probably beyond the reach of the law in the USA, partly because the perpetrators are unknown and partly because they may live and work outside the USA.

propagation of MyDoom

MyDoom propagates via an attachment in e-mail. MyDoom looks on a victim's hard drive for domain names, then adds a first name (e.g., joe, bob, james, etc.) from a list contained in MyDoom.A to generate fictitious From: and To: addresses. There are a variety of possible Subject lines and messages, of which the following three are examples used by MyDoom.A:

```
(1) Subject: Mail Transaction Failed
    The message cannot be represented in 7-bit ASCII encoding and has been
    sent as a binary attachment.

(2) Subject: test
    The message contains Unicode characters and has been sent as a binary
    attachment.
```

```
(3) Subject: Error
    Mail transaction failed.  Partial message is available.
```

The copy of MyDoom.A is in an attachment that has a name chosen from a list of nine filenames and six filetypes (e.g., `document.zip`). When the recipient clicks on the attachment to read the message, MyDoom infects the recipient's computer.

MyDoom perpetrator

To the best of my knowledge, the author of the MyDoom worm was never identified, so there can be no legal consequences for him.

MessageLabs, an e-mail filtering service, reported that at the peak of the MyDoom.A epidemic on 8 Feb 2004, one in every 9 e-mails (11%) contained MyDoom.A. On 30 April 2004, F-Secure reported that MyDoom.A accounted for about half of infected computers in the first four months of 2004.

Netsky

On 16 February 2004, the first version of the Netsky worm appeared, followed by approximately thirty variants discovered before 4 May 2004. The worm spread by e-mailing itself to addresses that it found in files on a victim's hard drive. Netsky did less harm to victims than some other malicious programs, it is included in this essay because some versions propagated prolifically and because its author was arrested.

MessageLabs, an e-mail filtering service, reported the following incidence of Netsky variants at the peak of their epidemic:

	date	peak incidence
Netsky.B	23 Feb 2004	one in every 48 e-mails (2%)
Netsky.D	3 Mar 2004	one in every 19 e-mails (5%)
Netsky.P	21 June 2004	one in every 12 e-mails (8%)
Netsky.Z	21 June 2004	one in every 20 e-mails (5%)

The anti-virus vendor F-Secure reported[13] that "Netsky.P possessed the 'most common virus in the world' title for over four months, from early April 2004" until 17 Aug 2004. This is despite intense competition from variants of MyDoom and Bagle.

[13] http://www.f-secure.com/weblog/archives/archive-082004.html#00000265 (18 Aug 2004).

The author of the original Netsky worm, as well as the author of most of the Netsky variants, was Sven Jaschan, who is discussed below, beginning at page 22. Jaschan claimed he created the original Netsky worm to fight the MyDoom and Bagle worms.

Some variants of Netsky worms caused denial-of-service attacks against several websites. For example, Netsky.Q attacked several file-sharing websites:

www.Kazaa.com
E-mule-project.net and
Edonkey2000.com.

For unknown reasons, Netsky.X, Netsky.Y, and Netsky.Z attacked three education websites during either 28-30 April 2004 or 2-5 May 2004:

www.nibis.de	Niedersächsischer Bildungsserver
www.medinfo.ufl.edu	University of Florida Medical School
www.educa.ch	Der Schweizerische Bildungsserver

propagation of Netsky

Netsky propagates by sending e-mail. This worm uses a long list of possible Subject: lines and a long list of possible messages. I received a many copies of Netsky.Q in e-mails with the following characteristics:

```
Subject:  Mail Delivery (failure userid@domain.com)
To:  userid@domain.com

If the message will not displayed automatically, follow the
link to read the delivered message.

Received message is available at:
www.domain.com/inbox/userid/read.php?sessionid-18295

The following document was sent as an embedded object but not
referenced by the email above:
Attachment converted: message.scr
```

What appears to be a link to the recipient's website is actually a MHTML CID command that executes the attachment. Apparently the worm's author hoped that the recipient will be more trusting of a document at their own website. Clicking on the attachment will also infect the recipient's computer, if that computer runs a 32-bit version of the Microsoft Windows operating system.

Some versions of Netsky.O and Netsky.P sent e-mail that fraudulently claims that the e-mail and attachment was scanned by a named anti-virus program (e.g., F-Secure, Symantec, McAfee, etc.) and found to contain "no virus". For example, the e-mail sent by Netsky might say:

```
+++ Attachment: No Virus found
+++ F-Secure AntiVirus - You are protected
+++ www.f-secure.com
```

or

```
+++ Attachment: No Virus found
+++ Norton AntiVirus - You are protected
+++ www.symantec.de
```

The use of the German-language Symantec website (instead of the main website at `www.symantec.com`) is a clue that the author of Netsky is German.

Sasser

On 30 April 2004, the first version of the Sasser worm appeared. Like Slammer and Blaster, Sasser spread automatically via the Internet to computers that used a defective (euphemistically called a "vulnerable") version of either the Microsoft Windows 2000 or Windows XP operating system. The defect exploited by Sasser was in Microsoft's "Local Security Authority Subsystem Service (LSASS)", which caused the worm to be called Sasser.

Computers infected by Sasser frequently do a restart (i.e., shut down then reboot), which is an annoyance and disrupts a user's work. The frequent restarts complicates the process of removing the Sasser worm.

Sven Jaschan: author of Netsky and Sasser

As a result of US$ 250,000 reward offered by Microsoft, informants tipped police in Germany that Sven Jaschan had written the Sasser worm. Police arrested Sven Jaschan at his home in Waffensen, near Rotenburg, Germany on 7 May 2004. Jaschan confessed to being the author of Sasser, as well as the author of the Netsky worm. Because Jaschan had his 18th birthday on 29 April 2004, he was a juvenile when he wrote and released most of his worms. Jaschan released the fifth version of Sasser (called Sasser.E) just before he was arrested, so he could be tried as an adult for that release. If tried as an adult, German law specifies a maximum punishment of only five years in prison for the crime of "computer sabotage".

On 29 July 2004, the anti-virus company Sophos reported[14] that "70% of the virus activity in the first half of 2004 can be linked to one man," Sven Jaschan.

---

[14] http://www.sophos.com/virusinfo/articles/oneman.html (29 July 2004).

The trial of Jaschan began on 5 July 2005 and lasted three days. He was tried as a juvenile, because he was 17 y old when he created most of the worms.[15] For that reason, his trial was *not* public and published information is limited to what was released by a court spokeswoman. On the first day of his trial, Sven Jaschan admitted in court that he created the Sasser and Netsky worms. However, only minimal evidence of damage caused by his worms was presented in court.[16] The German prosecutors asked the judge to impose a two-year jail sentence, which sentence would be suspended during a three-year period of probation — meaning he would *not* be imprisoned, plus order Jaschan to perform 200 hours of community service during his probation.[17]

The BBC neatly captured the significance of Sven Jaschan's crimes: "Anti-virus firm Sophos estimates that 70% of all the virus infections in the first half of 2004 could be blamed on Mr Jaschan's creations."[18] Journalists reported estimates that one million computers worldwide had been infected with one of Jaschan's worms. If the cost of removing each of these worms was a mere US$ 100, that would indicate damages of the order of US$ 10^8. Adding the consequential damages from infected business computers would push the total worldwide damages even higher. Despite the immense importance of his crimes, his trial received terse coverage from journalists on 5 July, and even less coverage on 6-7 July. In remarking on the 8 July 2005 verdict, Mikko Hyppönen, director of anti-virus research at a major anti-virus software company, F-Secure, said: "One of Jaschan's viruses, Netsky.P, is still number four in our virus statistics today, almost 16 months after it was released."[19]

Friday, 8 July 2005, a judge in Germany found Jaschan guilty of computer sabotage and illegally altering data and gave Jaschan a 21 month suspended sentence, plus ordering him to perform a total of 30 hours of community service at a hospital, nursing home, or home for elderly people. There seem to be four reasons for this lenient sentence:

1. He was a child (less than 18 y of age) at the time he committed most of his crimes.
2. There was no evidence presented in court of the enormous worldwide damage caused by his worms.
3. His motive was *not* financial gain.

---

[15] Jaschan released a few of his worms after his 18th birthday, a fact that seems to be ignored by both prosecutors and journalists.

[16] Reuters reported that prosecutors claimed damages of only 130,000 Euros (US$ 155,000), while it was estimated that one million computers systems were infected with one of Jaschan's creations. Reuters, "Sasser Computer Worm Author Confesses in Trial," (5 July 2005).

[17] Reuters, "Prosecution Urges Probation for Sasser Author," (7 July 2005).

[18] BBC, "German Admits Creating Sasser," (5 July 2005).

[19] http://www.f-secure.com/weblog/archives/archive-072005.html#00000594 .

4. Germany, like many European nations, does *not* routinely use long prison sentences that are common for criminals in the USA.

I comment that the first reason is a legal fiction: maturity is a *continuous* process, so there is nothing magic about a person's 18th birthday. Jaschan's level of moral development was essentially the same during the few months that he created his series of worms, and he released a few *after* his 18th birthday. The second reason is also bogus: one does *not* need a precise numerical value of the damage attributable to his worms to understand that he did an immense amount of damage. In fact, it is pointless to precisely quantify the amount of damage, because the total is obviously far beyond his capacity to pay restitution. The third reason is also suspect. He is reported to have created and released the worms to receive recognition for his programming skills, which recognition did —in fact — land him a job at a German software company. For a professional, there is a relationship between one's technical skills and one's income, so his motive was, at least indirectly, financial gain.

Conclusion

There are two worrisome trends since my first essay on malicious computer programs in May 2002:

1. Malicious programs have evolved from vandalism (e.g., deleting files on the victim's hard drive) to performing a service for the author of the malicious program (e.g., sending confidential information from the victim to the author, sending spam e-mail from the victim's computer).
2. Some programs spread very rapidly via the Internet (*not* via e-mail), so that all vulnerable computers connected to the Internet will be infected in approximately twenty minutes. (See above at page 3.) Such rapid propagation will defeat both anti-virus programs and attempts to repair defects in operating systems.

Some computer worms (e.g. SoBig.E and .F, Bagle, MyDoom) have evolved to opening backdoors on victim's computers, so that those computers can be used by others to send spam e-mail. Law enforcement apparently pays little attention to malicious programs that install backdoors on victims' computers, allowing those computer to be used to send spam e-mail and downloading confidential information from such computers.

There was a massive epidemic of computer worms on the Internet, beginning with Bagle and MyDoom in January 2004, continuing with many variants of Netsky from February through April 2004, and continuing with Sasser in early May 2004.

The Blaster worm in the Fall of 2003 motivated Microsoft to begin paying a bounty for information leading to the arrest and conviction of authors of malicious computer programs. Such a bounty is likely to be successful in finding children and amateurs (e.g., Sven Jaschan) who write worms, but *not* likely to be successful in finding professional computer criminals. It is the same with other kinds of professional criminals: for example, a US$ 25,000,000 reward for the capture of Osama bin Laden produced no results since June 1999.

This document is at **www.rbs2.com/cvirus2.pdf**
revised 9 Jul 2005

go to my first essay on Malicious Computer Programs at http://www.rbs2.com/cvirus.htm

go to my essay on Computer Crime at http://www.rbs2.com/ccrime.htm

return to my homepage at http://www.rbs2.com/