Global Information Assurance Certification Paper

Virus Writers 360^{o}

An analysis of virus writers

Julie S. Newberry

GSEC certification
Practical Assignment v1.4b
Option 1

Submitted: August 2, 2004

Abstract

To comprehend the personal motivations of a virus writer investigating the technical angle presents only a small part of the puzzle. There is a significant gap between what is known about viruses/worms and our understanding of the virus writer. After pouring through volumes of technical documentation, there remains only limited information about the individual who chooses to write viruses.

The objective herein, is to communicate a 360^{o} view of the virus writer that will include a sociological and psychological perspective, a summary of their intellectual makeup, and an examination of the ethical implications involved. On a visceral level, questions will be explored that will determine what virus writers have in common as well as how they differ. Their educational background will be examined and stereotypical behaviors identified.

Background

Today's viruses have reached new heights of sophistication, with the ability to take computers out of service, leave networks in disarray, and bring companies to their knees. New generations of virus writers attack from all angles and return home through multiple paths. To use an Internet-enabled computer today, is to be directly or indirectly affected by viruses. Thieves have capitalized on the freedom of the Internet that has awarded them a wealth of confidential information available for the taking.

A number of statistics support this theory:

- According to a recent study by the Department of Trade and Industry in the United Kingdom, "93 percent of smaller companies and 99 percent of large companies said they use antivirus software, and close to 60 percent of firms update their antivirus software automatically to keep up with new virus threats. […However,] computer viruses still managed to hit 50 percent of the smaller firms and infect 68 percent of the larger companies' networks in 2003" [1].

- "The number of attacks seems to have increased from previous years, with the largest growth occurring in the 1-5 incidents per respondent range (47%, up from 38%). It is interesting, however, to note that the source of attacks is roughly equal[ly distributed] with 70% originating from external sources (usually Internet) and 66% coming from internal ones" [2].

- "80 percent of the viruses were spread through e-mail and mass mailers and 90 percent of the companies surveyed had been infected with worms or viruses" [3].

These statistics underline the fact that viruses are a major problem and that viruses are not going away. Not only is the complexity of network threats growing but the time in which it takes a virus to spread is decreasing. Viruses used to take days or weeks to spread. Now, they take only minutes. It is predicted that it will only take seconds to propagate in the next generation. At this rate, the fifth generation will take milliseconds to proliferate [4].

To comprehend the personal motivations of a virus writer investigating the technical angle presents only a small part of the puzzle. There is a significant gap between what is known about viruses/worms and our understanding of the virus writer. After pouring through volumes of technical documentation, there remains only limited information about the individual who chooses to write viruses.

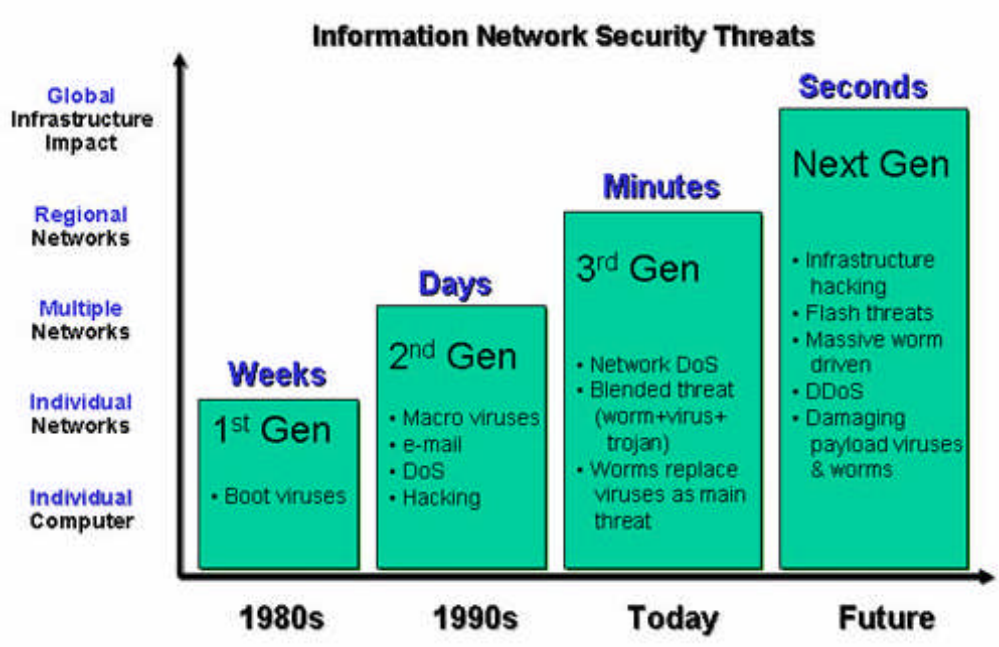

Figure 1: The growing Complexity of Network Threats
Source: "Securing the Corporate Information Network - Balancing Protection and Productivity."
URL: http://newsroom.cisco.com/dlls/tln/newsletter/2004/february/part1.html

The rise of new technologies has extended network boundaries to cafes, coffee shops, and carpools making them difficult to protect [4]. Today's virus writers can attack companies through these new exterior boundaries, like remote connections and wireless devices, that are often more difficult to maintain when compared to a computer within a company's walls. Analyzing this growth rate can help put future infection rates in perspective.

Studying charts and graphs of projected threats will assist in preparing for future attacks but knowing more about the virus writer themselves will help us comprehend why they continue to write. Generally speaking, a computer user's

personal behavior is indicative of their needs. In turn, their needs dictate their behavior. This fact is often used by the virus writer to fool the user into installing their program, via normal email usage or an inadvertent click on a lurid link. Utilizing this concept in reverse can help predict the virus writer's future behavior.

Many experts consider virus writers to be a class of hackers. The term hacker has evolved through the years. Hacker used to mean someone who was inquisitive about how computers function [5]. Today the word hacker tends to mean someone who gains unauthorized access to a computer or network. Hacking requires a more advanced set of skills than virus writing [6]. A hacker requires system knowledge, is popular in today's counterculture, and is considered a loner in society [7]. Some hackers have enough knowledge to spread virus attacks capable of damaging global economies.

Hackers have been grouped into four categories including script kiddies, professional criminals or crackers, code and virus writers, and old school hackers. Script kiddies (or cyber-punks) ages range from 12-30. They tend to be primarily Anglo, males with about a twelfth grade high school education. School does not hold their attention but they are very proficient with modern technology. Script kiddies do not think twice about downloading scripts to launch or hacking into a computer. Professional criminals or crackers tend to make a living exploiting information for profit. People in this group might be involved with government espionage or criminal organizations. There seems to be less research about code and virus writers. They have an elitist attitude. They enjoy writing code but to not launch it in the wild themselves. They have their own experimental networks called zoos where they test their code to satisfy their intellectual curiosity. They let others write the viruses based on their code. Lastly, there is the old school hacker who has been described as a seasoned programmer from Stanford or MIT who is intrigued by analyzing code. Typically they are not involved with criminal activities [8].

Virus writers are a subset of hackers but they are different in many ways. Virus writers tend to be socially adept unlike hackers [6]. They often ride piggyback on the technological brilliance of hackers, tweaking their code or writing a virus on the hackers exposed vulnerabilities. The hacker cracks a code and the script kiddy spreads this malevolent code often using psychology to ensure their success [8].

A social perspective

This section will address the sociological and stereotypical makeup of the virus writer. An overview of the research will be used to illustrate the types of people who write viruses along with the behaviors they share. The amazing social engineering techniques used by the virus writer will also be examined.

"There has been no systematic analysis of the effectiveness of social engineering techniques in spreading viruses and worms" [3]. However, we can draw some conclusions about the social make up of a virus writer from their

demonstrated actions and techniques. More research is necessary as the future brings more severe risks requiring more vigilance.

The work of a virus writer fulfills a variety of social needs. Many will look to their peers for acceptance of their actions. Their peers might even cheer them on. Virus writers feel they play an important role in society, securing the world of computers. They believe it is their responsibility to inform people their personal computer is vulnerable. Some virus writers make headline news and the national coverage is considered a victory, giving them a sense of accomplishment and fulfillment.

A stereotype is a social perspective or ideal applied to groups of people. According to popular belief, the stereotypical virus writer is a computer-obsessed, teenage to young adult male, whose ages range from 14 to 34, hiding in their basement. The fact is however, many veterans are created by their twentieth birthday. Intellectually, virus writers are compulsively drawn to writing self-replicating codes [9]. They enjoy messing around with code and will release a virus to see if it works. Typically, they lack a girlfriend [10]. "They do not connect the impact of what they do on the computer with the impact" it will have on others [7]. They do not conceive that their actions can affect the wider world and appear disconnected from reality.

Social inadequacy and the lack of a social life are characteristics of a virus writer [9]. They are often involved with an underground community of programmers, showing off their skills while trying to impress their peers [11]. Female virus writers do exist but this is a predominately male culture [6].

One distinguished authority on the subject is Sarah Gorden who is a senior research fellow at Symantec's Security Response unit, and previously was a researcher for the antivirus research and development team at IBM's Thomas J. Watson Research Center. Her work is based on a research study where she distributed a survey of questions to virus writers and then analyzed the results from the replies. They gained insight on questions answered and questions left unanswered. As a result of her research, she described them in four categories. Gorden's classification is similar to the hacking groups mentioned earlier which include the adolescent; the college student; the adult or professionally employed; and the ex-virus writer as shown below [12].

The Adolescent

> Virus writers aged 13-17; has written at least one computer virus; has distributed at least one computer virus into the wild.

The College Student

> Virus writer aged 18-24; has written at least one computer virus; has distributed at least one computer virus into the wild. Student in the university or university level classes.

The Adult & Professionally Employed

> Post-college or adult, professionally employed; has written at least one virus; has distributed at least one virus into the wild.

The Ex-Virus Writer

> Virus writer who has written and distributed one or more computer viruses. The viruses must have been found in the wild; the author must have supplied sufficient proof to enable determination that he did indeed write the virus; there must be no evidence that he has written or continued to write viruses for a period of at least 6 months prior to commencement of this research [12].

These categories are simply a guide, not an all inclusive categorical description of virus writers. Take into consideration that these groups can not be interpreted by age alone. For example, adolescence has been known to extend past the teenage years and sometimes well into the young adult years. For clarification, the descriptive hacker categories of the adolescent and the college student mentioned earlier, are very similar to Sarah Gorden's script kiddy category.

Virus writers sometimes accomplish their goal of virus infection by combining their technical skills with their social skills (or lack thereof). They will continue to write code and exploit it until they are discovered. They use these skills to their own benefit and take advantage of people who are unaware of the danger behind a link, an attachment or an open file share. Virus writers do not have to be very creative. Some of their success is the result of unoriginal work. They use "good old-fashioned social engineering" in addition to flaws in software to propagate their work [13]. User's keep falling for the same old tricks or have left holes while attempting to implement their system's defense strategy.

A spate of reports has underlined the fact that social engineering is escalating. Social engineering is one of the virus writer's favorite techniques. They "manipulate users into letting down their guard" [14]. Some have explained the success of social engineering by "casting aspersions on the intelligence of the victims, calling them ignorant or suggesting that they needed to apply common sense" [3]. Social engineering has proven to be an effective technique which is prevalent in today's society and has repeated itself through our history.

> "The Trojan horses we encounter today, along with the computer viruses and worms that bear them seem far more complex and sophisticated than the Trojan horse of legend. Yet the virus and worm makers often show that they are as capable as the ancient Greeks of influencing people to open their computers and networks to malicious code or even mistakenly to destroy their own data" [3].

Viruses of decades past were not as complex as the viruses of today. The

viruses that format hard drives and delete files are throw backs to the 1980's. Virus writers today are preoccupied with the challenge of conning users into clicking on a link or attachment [10]. They also depend on society's "flawed office culture as much as technical innovation" and viruses are written in a manner that will entice the user to click on the attachment or link [15]. The creators of MyDoom for example used brilliant psychological maneuvering by writing a pseudo-technical email message instead of a poorly written message "appearing to be a failed e-mail transmission, with the diagnostic of the problem contained in the attached text file. Users were lulled into a state of false security, and then the worm took full advantage of that dropped guard" [16].

A psychological perspective

The Internet is today's playground where virus writers can play creatively, developing and arbitrarily using their skills on the populace as pawns. The underlying psyche of the criminal virus writer could be a deep sense of inferiority. Their comprehension of computer technology and their ability to use it, overcomes their inferiority, giving them a sense of power. Writing a self-replicating virus and distributing it to the world can give them a feeling of adventure. The virus writer's "technological brilliance is matched by their psychological" appraisal of a situation, giving them an edge [15]. Their methods can lure a user from their regular practices, convincing them to click and disregard rules, regulations or best practices, without thinking.

The virus writer may feel a sense of anonymity in a virtual world that provides an environment where people are more willing to take chances. Many virus writers, much like common criminals, believe they will never get caught. With the track record so far, it would appear that they are correct in this assessment. Virus writers tend to diminish or "misconstrue the consequences of their activities, rationalizing that their behavior is really performing a service to society. Some researchers call this the Robin Hood Syndrome. They […] tend to dehumanize and blame the victim sites they attack" [8].

They are very competitive amongst themselves often trying to make a point amongst their peers. It is not uncommon for a virus writer to stake a claim on an unsuspecting user's computer during a competition or gang war.

Virus writers feel that it is their right to exploit any computer that is left unprotected or uses vulnerable software. Once the virus writer has entered a user's computer, they will often leave telltale signs letting the user know of their presence. This differs from the behavior of the common thief who is unlikely to make their intrusion known, in an attempt to see themselves on the evening news. Having to prove yourself in this manner demonstrates a sign of the virus writer's immaturity.

Malicious code is compiled and released for reasons varying from a desire for profit, anger, curiosity, or a need to make a political statement to name a few [11]. Some may operate out of several or all of these motives simultaneously.

The majority of viruses are written by those who like to tinker with technology to explore known boundaries and release it as a sign of protest. Of course, it must be painful because they cannot brag too much about their accomplishments out of fear of getting caught [7].

As mentioned earlier, virus writers compete amongst themselves to claim a vulnerable computer or network as their own. Often, virus writers have been known to leave root kits and backdoors behind. Trojans are often installed without the user's awareness and are considered trophies. Virus writers have formed computer gangs and started wars against each other. Viruses will use a backdoor left by a competitor, search the infected computer for their competitor's files and disable it so that the competition can not get back in without taking further steps. In the mean time they are leaving their own back door and claiming new ownership over the box. Virus writers have been known to brag about the number of computers under their control.

Malicious code has also been used as a political platform. For example, viruses have targeted specific companies with a denial of service (DoS) attack. This fills the need to have a voice, to make a statement and be heard. The Internet is also vulnerable to terrorist threats. Even though "politically-motivated viruses are on the rise, they are unlikely to spread as far as those that rely on the psychology of sex," e.g. sexual images [17]. Others are driven to write viruses by ideological motives, concerning the ideal that information is free and should not be restricted in anyway.

Virus writers are occasionally financially motivated. Conclusive research has not been completed but it has been speculated that virus writers are involved with some of the spamming or pirating of credit cards. Virus writers have become extremely advanced in organized, high tech, criminal activities including an increasing number of viruses being released and stealing credit card or bank information [7].

An intellectual perspective

Viruses are written by some because they are intrigued by the workings of the computers and want to test their newly developed code. It is this same level of curiosity that leads the hacker to test the boundaries of software and discover vulnerabilities. They enjoy the mental challenge used to exploit code and attempt to spread their creation across the world. Virus writers are constantly finding new methods of infection and targeting vulnerable operating systems.

The real problem is that effective virus writing is not rocket science, brain surgery nor does it require a PhD. in Computer Science. A teenager can use existing code or pick up a virus writing kit to exploit pre-existing vulnerabilities. The more experienced hackers discover the vulnerabilities. Once a virus is written to exploit that vulnerability, a slight alteration of the code can trick today's antivirus software and slip through the signature-based application.

Reverse engineering involves disassembling a product to determine how it works with the intention of replicating pieces or the entirety of its functions. Script kiddies have often used this technique on the service packs and security updates distributed by the vender themselves. As a result, the decision about when to notify users of a new vulnerability is a controversial topic. Software vendors take two distinct approaches when notifying users about security vulnerabilities. Three out of four vendors notify the general public of vulnerabilities immediately before a fix is available [18]. Choosing to notify the user without delay or waiting until the fix is available both have benefits and pitfalls. Some believe that notifying the user promptly can give them a chance to administer temporary measures until the permanent fix is available. Others delay early notification because it hands the script kiddies a blueprint to work with. The first group feels the "idea that they should refrain from publishing their research in order to keep us safe is fundamentally flawed" [19]. Regardless of how the vendor chooses to respond, the Internet community continues to distribute information about these flaws via Bugtraq and other security focused mailing lists.

Elegant and sophisticated techniques are more often employed by the virus writer as the average computer user becomes more savvy. Additionally, predators are growing minimally at an equal rate and possibly at a faster rate [16]. Exploitation can include writing simple code to very elaborate. Some of the less technically complicated viruses have proven to be detrimental despite their simplicity.

Hybrid attacks have become increasingly popular. The practice of attacking the same computer with multiple vulnerabilities is referred to as chaining. Furthermore, there seems to be an increasing trend that virus writers are adopting spyware and adware techniques into their bag of tricks, blurring the lines between them. Multi-threading techniques allow computers to execute several commands at once, adding to the level of complexity. These techniques consume computer resources which can eventually lead to a total DoS on workstations or servers. The randomization of file names, subject lines, and the body of email messages, make malicious code progressively more difficult to detect. This is a similar tactic to the one that spammers use to avoid being detected from spam filters. Virus writers also use a variety of protocols to spread and to report back to their point of origin.

Virus writers target a wide audience in order to guarantee results from their efforts. Their desire is to reach the maximum number of people while exerting minimal effort. Writers tend to focus their attention on popular software instead of targeting less popular operating systems and applications. From the writer's perspective, why would they write a program that only affects a small percentage of users?

Virus writers want to make a big impression on this vast Internet audience. They have the attitude that the world would be less secure without them. They force users to address their security issues by exploiting them. The virus writer forces society to tackle security issues that real criminals could capitalize on.

They rationalize that vender flaws might otherwise never be corrected [10].

An ethical perspective

Virus infections force businesses into down time resulting in a loss of productivity and large economic losses worldwide. For example, MyDoom.A created an estimated 38.5 billion dollars of lost productivity [20]. Hackers who discover the exploit may have altruistic intentions, operating from a higher ethical ground despite the financial or other disruption they cause to the user. They believe they are using their skills toward the greater good.

The individual exploiting the code is demonstrating a lack of personal values. Some virus writers feel they are providing a service to society. They appear inwardly focused and believe they are helping to secure the world. Virus writers are disconnected from the results of their actions and feel they are making people aware of security flaws by giving them a virus. Someone with this mindset believes that they are operating at a superior level of thinking that they are above it all. Once the virus writer has been caught, he typically denies any mal intent [11].

In reality, writers are often acting in their own self-interest to the point of narcissism. There is a fine ethical line between finding software flaws and exploiting them. "The common thread [among writers] is that there's a lack of serious intent by these people. This is the moral equivalency of graffiti," according to Trend Micro's David Perry, global director of education [11].

Conclusion

Defending networks from viruses today has become increasingly difficult. Their numbers will continue to increase. One dimensionally analyzing the technical side of the virus writer, does not utilize all resources available to the information security community. A 360^{o} analysis of the virus writer, of his or her motives, abilities, and experience, is necessary to understand and better defend against the crippling viruses experienced by an Internet-driven society. Understanding behavior and the needs that drive the behaviors, will assist in truly knowing the enemy, quickening the response time to avert total shutdown. The constantly changing state of the Internet has left many ways for virus writers to compromise a computer or network, leaving a significant security risk.

As mentioned earlier, viruses are projected to only take seconds to propagate in the fourth generation and could spread in milliseconds in the fifth generation if the Internet community continues its present growth rate. The risk and repercussions of viruses can affect the critical infrastructure of airports, banks, hospitals, universities, defense systems and even governments.

Several insights became apparent while constructing this paper including how virus writers believe it is their role in society to let people know about computer security by launching viruses, and feel justified in their actions. In

addition the connectedness of script kiddies and hackers who discover the exploit is fascinating. They have developed a symbiotic relationship. Lastly, virus writers have utilized many resources available to them. Adware and spyware techniques have been very successful and will likely be intergraded into their bag of tricks.

The motivations and characteristics of the virus writer are broad. The groups identified are helpful. However, there are "too many observable differences to categorize them into a generic construct" [12]. Virus writers will likely broaden their horizons in the future and prey on other mobile devices like cell phones and hand held devices.

The Internet does not provide the physical interaction experienced in a meeting face-to-face, complete with body language, voice inflections, and eye contact. The bad guy cannot always be recognized when knocking at the computer's door.

What happens, in the home, when a doorbell rings? The natural reaction is to look and see who's there. Then the decision is made whether or not to open the door. No one knowingly will allow a stranger into their home. No one would leave a window unsecured for an intruder to slip inside. Computer security is to be treated like home security protecting the valuables kept within.

An inexperienced Internet community will leave computer systems unprotected in both the corporate and private sectors. Without the appropriate protection, they leave themselves prey to the virus writers, script kiddies and other computer criminals yet undiscovered.

References

1. Delio, Michelle. “Cashing In on Virus Infections.” Wired. 18 Mar. 2004. URL: http://www.globalsecurity.org/org/news/2004/040318-cash-virus.htm (31 Mar. 2004).

2. Bourgue, Lyne. “2004 CSI/FBI Survey Dissected, Part 2.” 27 July, 2004. URL: http://www.enterpriseitplanet.com/security/features/article.php/3386871 (1 Aug. 2004).

3. Rusch, Jonathan J. “The Social Psychology of Computer Viruses and Worms.” INET. 21 June 2002. URL: http://inet2002.org/CD-ROM/lu65rw2n/papers/g10-c.pdf (28 Mar. 2004).

4. Felton, Jim & Gleichauf, Robert. “Securing the Corporate Information Network - Balancing Protection and Productivity.” Executive Thought Leadership Newsletter. 17 Feb. 2004. URL: http://newsroom.cisco.com/dlls/tln/newsletter/2004/february/part1.html (2 June 2004).

5. “Just what is a hacker?” Kaspersky Lab. URL: http://www.kaspersky.com/hackerinfo.html (28 Mar. 2004).

6. “Studying the psychology of virus writers and hackers – an interview with researcher sarah gordon.” Frontline. URL: http://pbs.org/wgbh/pages/frontline/shows/hackers/whoare/psycho.html (27 Mar. 2004).

7. Twist, Jo. “Why people write computer viruses.” BBC News. 23 Aug. 2003 URL: http://news.bbc.co.uk/1/hi/technology/3172967.stm (28 Mar. 2004).

8. Quitter, Jeremy. “Hacker Psych 101.” URL: http://tlc.discovery.com/convergence/hackers/articles/psych.html (28 Mar. 2004).

9. Slade, Kent. “The Internet Guru.” Logan Library. 19 Mar. 2003. URL: http://associates.ucr.edu/csla304.htm (28 Mar. 2004).

10. “Looking Into the mind of a virus writer.” CNN. 19 Mar. 2003. URL: http://www.cnn.com/2003/TECH/internet/03/19/virus.writers.reut (31 Mar. 2004).

11. Lewis, Katherine R. “Changing Motives of Virus Writers Make Them Harder to Catch, Experts Say.” 27 Aug. 2003. URL: http://www.newhouse.com/archive/lewis082803.html (28 Mar. 2004).

12. Gorden, Sarah. “The Generic Virus Writer.” Sept. 1994.
URL: http://www.research.ibm.com/antivirus/SciPapers/Gordon/GVWII.html
(27 Mar. 2004).

13. Vamosi, Robert. “Could you get caught in a virus gang war?” 10 Mar. 2004.
URL: http://reviews.cnet.com/4520-3513_7-5125006-1.html (15 Mar. 2004).

14. “Topic 1 – Recent News.” Federal Information Systems Security Awareness.
URL: http://www.navo.hpc.mil/FISSA/text_only/module1/topic1.htm
(28 Mar. 2004).

15. Rose, Heidi. “Human weakness causes virus spread. (Industry Trend or Event).” Computer Weekly. 3 Aug. 2000.
URL: http://www.findarticles.com/cf_dls/m0COW/2000_August_3/64147842/pl/article.jhtml (3 Mar. 2004).

16. “Deconstructing MyDoom.” 15 Feb. 2004.
URL: http://pub.cyberlogic.net/news.php?NID=624 (28 Mar. 2004).

17. Sir Lankan virus spreads political message. 18 May 2001
URL: http://www.sophos.com/virusinfo/articles/mawanella.html
(28 Mar. 2004).

18. “Early Notification: Vendors have different policies concerning when to notify users of security problems.” Informationweek 5 July 2004 (2004): 21.

19. Doctorow, Cory. “Virus writers profiled.” 7 Feb. 2004.
URL: http://boingboing.net/2004/02/07/virus_writers_profil.html
(27 Mar. 2004).

20. “Mydoom.A: Timeline of an Epidemic.” 2 Mar. 2004.
URL: http://www.net-security.org/virus_news.php?id=359 (2 Aug. 2004).