GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Morris Worm: How it Affected Computer Security and Lessons Learned by it
By Larry Boettger
December 24, 2000

On November 2, 1988 there was a major change in how computer professionals and the public viewed the security of the Internet. The event was known as the Morris Worm Incident or the Internet Worm. The worm is named after its creator and releaser, Robert Tappan Morris, Jr. At the time he was a graduate student in computer science at Cornell University. Robert's father was also in the computer field. Ironically, his father was the head of the National Security Agency. Some sources stated that Robert Jr. was trying to get away from his father's image and have one of his own. Other sources have stated that it was an accident intended only as an experiment and it wasn't intended to cause as many problems as it had. A mistake in the code caused it to do what it did.

Robert authored the self-replicating, self-propagating worm and then released it from an MIT and not Cornell. Some sources state the worm was intended to look like it came from Berkeley. It has been stated that he did not want anyone to know that the virus came from his own college. The worm took advantage of the exploits in Unix's sendmail, fingerd, rsh/rexec and weak passwords. It only affected DEC's VAX and Sun Microsystems's Sun 3 systems. It also wasn't coded to do any damage. There are two very good articles on the details of how the worm exploited these vulnerabilities by Bob Page titled "A Report on the Internet Worm" at http://www.ee.ryerson.ca:8080/~elf/hack/iworm.html and Donn Seeley titled "A Tour of the Worm" at http://kt-www.cs.titech.ac.jp/~natori/.../wormtour.html. The worm was intended to only put itself on the computer once and when it recognized that it was on the computer it was supposed to stop. It did not. It kept replicating itself on the computer hundreds and hundreds of times. This loop caused the computer's memories, drives, and processors to get filled up and cease working. Even a reboot didn't help because the drives were filled up. It required some work to get the computer back up and operational and then the worm had to be taken off the computer when the fix was available. Because the worm was self-propagating and self-replicating and it was using the connection capabilities on the Internet, it was able to spread to other computers. It spread so fast that no one had a chance to stop it. The only hope was to take your computers off the Internet if you hadn't been a victim yet. If you were a victim you would take yourself off the Internet and fix your computer and keep it off the Internet until there was a fix for it.

When Robert had realized what was happening he got help from some associates to try to stop the spread of the worm. Many programmers and computer experts worked on the solution. They were from many different institutions, such as, MIT, Berkeley and Purdue. By the time there was a fix it was estimated that about 6000 computers were victimized. At the time, this was about ten percent of the Internet. Along with the 6000 victims there were also the unreported amount of systems and networks that did have a chance to disconnect themselves from the Internet before they got victimized by the worm. These could also be called victims due to the loss in down time. (Fortunately, computers were not as revenue generating as they are today). By the time the incident was isolated it was too late. It was reported that 5-10 percent of the Internet computers were victimized. Estimates on the damage vary but it ranges in the area of $98 million. Most of it was related to man-hours to fix the problem.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

There were many first related to this incident. One of the firsts was the creation of the Computer Emergency Response Team (CERT). This organization was comprised of computer scientist from many different and similar industries gathered together to isolate the problem and prevent this sort of thing from happening again. CERT makes references to their existence on their web page due to this worm. Another organization was also created. It was the National Computer Security Center. Which was a part of the National Security Agency.

The other first was the trial of this case. This was the first conviction violating the 1986 US Federal Law Computer Fraud and Abuse Act (Title 18). After all of the appeals he was sentenced to three years probation, 400 hours of community service, a fine of $10,050 and the costs of his supervision. This sentence seemed light to the many people that had to work many hours to solve the problem and the many hours to fix their victimized machines. Others stated that he meant no harm and that the punishment was either OK or too harsh. Either way, it is reported that he his very successful today. One of his successes is that he had recently sold a start-up company that he had founded to Yahoo! Inc. for $49 Million.

This worm has been called a virus even to this day. The difference between a worm and a virus is that worms can self-propagate to other machines by themselves. They need no assistance from other sources. A virus needs to be propagated by another source to get to another computer. A source can be a floppy disk or another software program. There seems to be many gray areas lately on the definitions of many variances of how computers are getting victimized. Trojans, viruses, and worms are affecting computers more and more. The one thing that they all have in common is that they cause problems for computer users and the people that support computers. Some of these problems are minor annoyances and some are very malicious and cause companies millions of dollars a year for lost data, and lost hours to recover the data.

Many computer experts believe that the worm incident caused by Morris was newsworthy for not what the worm did but for what it could have done. It is very concerning to imagine what could have happened if Morris was a malicious coder out to damage as many computers as he could. He could have altered the code to go after more than just the machines that he did. He could have purposely started the running of the worm from many different sources worldwide to spread the worm faster before it could get stopped. He could have coded the worm to erase data from the systems. He could have done many things to hide the worm for longer than he did. The worm also brought attention to the New World of the Internet. It only had about 60,000 systems on the Internet then. Today there are millions. The incident surfaced to the computer professionals that security on the Internet was in need of higher security practices for protecting critical data.

Could an incident like this occur today? If so, how much damage could it cause? The answer is unfortunately, yes it could happen today. And, if a coder wants to be malicious the worm, Trojan or virus could be catastrophic to data on the Internet and the cost of losing and recovering the data. It would have a greater impact today for two reasons. One, there are millions more computers than there was in '88. Two, Some companies rely solely on the Internet for generating revenue. Imagine if a company could not generate revenue for an extended period of time.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Have we been good in the information security field at stopping this kind of occurrence from happening or have we been lucky that someone as smart as Morris has not come along with destructive code and the intelligence, motivation and the resources to implement the code? Morris' worm had only three exploits that it focused on within basically one operating system, Unix. What if someone tried to exploit more than one OS and more than three exploits on the operating systems within a small code? Could the information security professionals and the companies they work for be vulnerable to this kind of attack? Most recently, two viruses/worms penetrated many companies. The 'Melissa' and the 'iloveyou' virus/worm (Again, there is a question as to terminology as to what to define these works of code. And again, they still caused data loss regardless of the terminology). These works of code only affected less important files and data. By the time new code was created using variances of these codes to do even more malicious tasks the public was aware of what these programs were doing and they had fixes and awareness of them. Were companies and the computer professionals working for them lucky that the worse code didn't come first?

If we look at what could have been done to prevent the Morris worm incident could we use that knowledge to guard against new more dangerous issues to come in the future? We cannot change the fact that intelligent people will be able to code malicious programs. They will always be around. The coders will only change in what motivates them to attack systems.

Two of the exploits, sendmail and fingerd, were targeted at the OS. The operating system and software programmers will always be under deadlines to get their product to market. Software companies and their customers have been willing to sacrifice security for functionality. This may be able to be changed with security awareness and hopefully the security awareness will motivate the software vendor's customers to force the software vendors to create secure code. Of course, Unix and Linux are open source so they don't follow under the issue of deadlines to market but some of the programs that are designed for them do. Another way to prevent this from occurring is using security software programs to supplement weak OS and software coding. A structured IDS solution with firewalls, network and host based solutions may have been able to circumvent the code from coming into the network. Or, if it made it into the network an IDS solution could have prevented it from migrating from machine to machine within the network.

One of the exploits with the Morris worm was that users and some computer professionals were using weak passwords. This still seems to be the fact today. Again, this can change with user awareness or the administrators at these companies to force and monitor strong passwords. If stronger passwords had been used in 1988 the worm would not have been able to use one of its three exploits. Again, an IDS solution may also have prevented this from happening.

Another item that could have prevented the worm from occurring is security awareness or concern of data security in general. It seemed like there was an open trust between everyone on the Internet at the time. It appeared as if not too many computer professionals were really into protecting the data. It seemed to be the exact opposite. Data was there to be shared. Unfortunately, the data was also unprotected so a worm such as this exploited the overall trust on the Internet. Security awareness entails having the necessary computer security resources to do auditing of the security tools.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Because there wasn't a major concern for protecting data there certainly was not a concern for having trained computer security professionals working in companies and other institutions. Had there been more security professionals using the information security tools to monitor the IDS software, data traffic, user logon times and access to servers then this incident may have had less of an impact that it did have. Today, more companies are using the Internet for financial and customer support issues. If ten percent of these companies were to be disconnected from the Internet it could be financially catastrophic for the economy. There are more information security professionals trained than there were in '88 that are using many of the information security tools to assist them in their daily task. Companies are relying on these people to assist them to prevent such attacks from occurring.

Are enough companies relying on these professionals and are there enough of these professionals to prevent an incident like the Morris worm? With all of the new malicious codes and cracker attempts that have generated media attention has there been any that would have been considered catastrophic? Not really, most of them have been annoyances. Have the crackers given their best attempt at exploiting weaknesses and is information security overrated? There are many more tools that the malicious coders and crackers can use here and in the near future. Cable modems and home users that have no security training are projected to be the next victims and they could be used as tools for the crackers to get to other more important targets to exploit. Were there enough trained information security professionals working for Microsoft when it was reported that they were hacked on October 27, 2000? With the rise of Ecommerce, home users, reliance on the Internet for critical information, and more intelligent, motivated, and resource strong coders and crackers it appears like there is a strong need for information security experts.

Are US Federal and Local laws strong enough and are they enforced to prevent these kinds of occurrences? In '88 the law was relatively new and it hadn't been tried. Would Morris have created and implemented his code had the laws been used and had stronger penalties that had been enforced? There are many famous crackers that have been caught and prosecuted only to get probation or a little jail time and then come out and make more money than they had before they got caught. As information security professionals are trained in how to deal with computer crime evidence we should see more prosecutions occur. After the malicious person is prosecuted the sentence is equally important. If the malicious people are better off for having gotten caught then the punishment does not fit the crime. Should our laws be changed to prevent this from happening?

Hopefully the Morris Worm of 1988 has not been forgotten. Sometimes the public forgets about the history and history repeats itself. The worm incident had brought many good things to light. It brought focus to data security on the Internet. It led to the creation of CERT, National Computer Security Center, and other organizations to attempt to prevent these and worse occurrences from happening. It led to public awareness about information security and the vulnerabilities of the Internet and computers in relation to security. It did not cause irreparable damage to data or systems. The laws were tried that had an impact on the prevention of computer crime. Overall the Morris Worm can be an indicator of other more vital exploits that may be coming. The information security field and the companies that it protects need to be prepared for the next time something like this incident occurs.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sources

1. Brenton, Chris, "Mastering Network Security", Sybex Network Press, 1151 Marina Village Parkway Alameda, CA 94501. Copy write 1999, Page 365

2. Byte Magazine Online "Noted and Notorious Hacker Feats" (September, 95) URL: http://www.byte.com/art/9509/sec7/art25.htm

3. Sullivan, Bob, MSNBC "Remembering the Net Crash of '88" URL: http://www.msnbc.com/news/209745.asp

4. Page, Bob, "A Report on the Internet Worm", November 7, 2000 URL: http://www.ee.ryerson.ca:8080/~elf/hack/iworm.html

5. Markoff, John, The New York Times Late Edition – Final Section 1 National Desk Page 1 "Computer Intruder is Put On Probation and Fined $10,000", URL: http://cs.nyu.edu/ms_students/cera7013/class/worm.htm

6. "The Internet Worm" URL: http://rhet.agri.umn.edu/Rhetoric/misc/dfrank/worminfo

7. "The CERT Coordination Center FAQ", (October 27, 2000) URL: http://www.cert.org/faq/cert_faq.html

8. Kehoe, Brendan P., "Zen and the Art of the Internet: A beginners Guide to the Internet, First Edition, January 1992, Section: The Internet Worm URL: http://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91

9. Seeley, Don, "A Tour of the Worm", URL: http://kt-www.cs.titech.ac.jp/~natori/…/wormtour.html

© SANS Institute 2000 - 2002 Author retains full rights.