CS 526: Information Security - Fall 2017

Following the Morris Worm

Phil Van Every

December 1, 2017

Abstract

On November 2, 1988, a Cornell graduate student named Robert Tappan Morris unleashed one of the first ever computer worms on the fledgling internet. It quickly spread to thousands of connected computers, causing crashes, performance degradation, and panic until it was contained and eradicated. This unprecedented crisis elicited both immediate and long term responses spanning multiple disciplines. The research community responded with the formation of new security emergency diagnosis and response protocols and organizations, including the CERT at CMU. Law enforcement responded by making Robert Morris the first felon convicted under the Computer Fraud and Abuse Act of 1986. The public at large began to appreciate the potential impact of internet security, or a lack thereof.

This paper explores the Morris Worm and its overall impact. It details the events surrounding the Morris Worm crisis and the inner workings of the worm itself. It goes on to trace the worm's influence on cyber security legislation, cyber security research, and other cyber attacks over the past several decades. Finally, it draws conclusions about the quality of the worm's overall impact. A jarring and devastating nuisance, the Morris Worm ultimately spread awareness of the gravity of computer security to both legitimate and malevolent users.

Contents

Incubation

The Internet's massive size and popularity today make it hard to imagine its humble beginning. What we now know as the Internet began as a research project sponsored by the Defense Advanced Research Project Agency (DARPA) called the Arpanet. On the day of its birth in December, 1969, the Arpanet consisted of only four connected nodes: UCLA, SRI, UCSB, and the University of Utah. Lines of communication between these nodes were "two million times slower than today's fastest networks" [Strawn(2014)].

The Arpanet opened the door for a flurry of new research projects. New ideas grew into numerous applications like file sharing, remote logon, and email. Soon, more nodes and networks were added. By the mid 1980s, the growth and success of the Arpanet prompted the National Science Foundation to build a network to connect research universities to some of its newly built supercomputer centers. This new network came to be known as the NSFnet. It made internetworking ubiquitous amongst universities and researchers, eventually connecting "more than 2,000 universities and colleges and a number of high tech companies" [Strawn(2014)]. Ultimately, the 1990s would see the NSFnet becoming commercialized into the Internet that we know today, but not without some growing pains. This paper focuses on one of the earliest and most vehement growing pains the developing internet[1] would face, known initially as the "Internet Worm" and later as the "Morris Worm".

An important detail in the internet's conception and early life is the attitude of its creators. This internet was developed by researchers focused on optimizing its efficiency, not its security. Some security measures were built in as an afterthought, but security was not woven into the core fabric of the internet or its applications. As the internet grew, researchers who used and designed it were generally assumed to have good intentions. According to [Lee(2013)], "...the Internet was like a small town where people thought little of leaving their doors unlocked. Internet security was seen as a mostly theoretical problem, and software vendors treated security flaws as a low priority." The same article

[1]The above summary of the birth of the Internet used the names "Arpanet", "NSFnet", and "Internet" for various stages in a growth of a widely connected network of computers. For simplicity, the rest of this paper will collectively refer to all of these stages as the "internet".

quotes the sentiments of Dr. Eugene Spafford [2]:

> The majority of people had some tie to computation for their jobs. I wouldn't say that we trusted each other, but there was more a community sense of caring for the stability and appropriate use of the computing systems... There was no such thing as a firewall back then. You didn't have people who were vandals or anarchists or criminals as much.

Thus, there was no perceived need for strong security. This very lack of security would ultimately provide a temperate environment for the incubation of a virulent infection: the Morris Worm.

The remainder of this paper tunnels through the worm hole in history that the Morris Worm has left behind. First, it covers *what* happened during the worm's outbreak and eradication. Second, it recounts the discoveries that were made by researchers about *how* the worm works upon its dissection. Third, it discusses the *immediate impact* that the worm had on the research community and the general public as they convalesced from the infection. Fourth, it traces the worm's *long term influence* on the evolution of future worms and shifting cyber-security perspectives. Finally, the paper provides a post mortem synthesis on the quality and depth of the worm's overall impact on the history of computer security.

[2] Dr. Spafford is a computer security researcher and professor at Purdue University. He is also executive director of the Purdue's Center for Education and Research in Information Assurance and Security and an internationally recognized expert in computer security.

Outbreak

Black Thursday

Many works covering the Morris Worm begin with some variation of the phrase "On the evening of November 2^{nd}, 1988...". This section will do the same:

On the evening of Wednesday November 2^{nd}, 1988, Robert Tappan Morris, a first year graduate student at Cornell University, released a worm onto the internet. The worm was released at around 6 pm at MIT. Spreading rapidly, by 11 pm it had infected machines at the University of Pittsburgh, RAND Corporation in Santa Monica, UC Berkely, the University of Maryland, the University of Utah, Stanford, the University of Minnesota, and the University of North Carolina [Seeley(1989)] [Spafford(1989c)].

Perhaps the worm spread faster than even Morris had anticipated. Around 11 pm and again at around 11:30 pm, he contacted Andrew Sudduth and Paul Graham [3] to tell them that he had released the worm and steps that could be taken to stop it. Furthermore, Morris requested that Andrew Sudduth alert the research community of the presence of the worm and how it might be stopped, which Sudduth did anonymously via email to a widely used internet research mailing list, called TCP-IP shortly thereafter. Unfortunately, by that time system administrators had already noticed the worm and had shut off internet gateways in an effort to quarantine the infection; thereby blocking Sudduth's email for several days [Lee(2013)][Eisenberg et al.(1989)].

The worm continued to spread throughout the night. By early Thursday morning, the infection had spread to the University of Arizona, Princeton University, Lawrence Livermore Labs, UCLA, Purdue University, Georgia Tech, Dartmouth, the Army Ballistics Research Lab, and the University of Chicago, amongst others. By this point many system administrators were aware of the spreading infection, and Peter Yee of UC Berkeley and NASA Ames Research Center had posted a message to the TCP-IP mailing, stating "We are under attack". Eventually, Thursday November 11^{th} would come to be known as "Black Thursday" [Seeley(1989)] [Spafford(1989c)].

[3] Andrew Sudduth was a friend of Morris'. He and Paul Graham were both members of the technical staff at Harvard University's Aiken Computational Laboratory [Lee(2013)]

At its peak, the infection is estimated to have spread to around 6,000 machines. That is 10% of the approximately 60,000 computers connected to the internet at that time[Eichin and Rochlis(1989)][Marsan(2008)]. Syptoms of infection included blah blah blah TODO:**********

Fortunately, the research community had not only noticed the worm by early Thursday morning, they had already begun to combat it.

Vaccination

- what researchers did to stop it
  - sh soln.
  - software patches
  - mailing list
  - quarantined email solutions
  - disassembly and analysis ***(transition into next section)

Dissection

Self Preservation

- Camouflage
  - disk clean up
  - encrypted image
  - name change to sh
  - fork() for new pid
- magic number authentication
- persistence (1 in 7 becomes unkillable)

Reproduction

- rsh/rexec exploit
- fingerd exploit
- sendmail exploit

Password Cracking

- common words and permutations
- unix dictionary
- other stuff

Maladaptive Traits

- detecting itself / coinflip for self termination and immortality bug
- no checks for good return values

- pass struct instead of pointer to struct
- joke about bug fixes in worm
- other stuff pointed out by Spaf

Vestigial Organs

- UDP to ernie over TCP connection, never sent
- accidental leftover files in /tmp (of compilation too slow?)
- unused functions and dead code
- unused file structure entries
- unused features- could have been much worse... ***(transition into next section)

Convalescence

The phase after illness caused by an infectious disease is called *convalescence*. This section addresses the recovery and response of the computing community in the wake of the worm.

Awareness and Perception

- of the research community
  - virus vs. worm terminology (taxonomy)
  - need for better passwords
  - hashing algorithm
  - this was too easy and it could have been much worse
- of the general public
  - Internet becomes widely know technology
  - cybercrime becomes more well known (at the same time... what a coincidence)
  - Genius computer whiz?
    - researchers: NO
    - public: Yes
  - Is Morris a criminal?
    - yes, fire and brimstone (some researchers)
    - yes, but don't punish too harshly (Cornell Commission and others)
    - no, just a mistaken experiment
    - no, he's a hero for demonstrating security flaws (transition to next section: blaming the victim)
    - the real question - should accidents/experiments be considered crimes?
  - Who is at fault: administrators vs. vendors... beginning of "blame the victim" mentality

Immune System Growth

  - computer security as a legitimate field
    * tons of publications
    * questions about security design principles (like least privilege)
    * questions about ethics and law ***(transition to next section)

- prosecution under CFAA
  - Morris' claim that it was unintentional... "knowingly" vs "intentionally" .. accident
  - Morris' claim that he didn't gain ungranted access because he had access to Cornell computers
  - Precedent: the internet falls under CFAA
  - Question: what if worm hadn't infected government computer?
- crisis response protocol
  - formation of CERT at CMU
  - phage mailing list

Evolution

The Morris Worm and subsequent decompiled and analyzed code provided ancestral concrete examples of several attack vectors, like. . . :

- email as a spread mechanism
- scanning as a spread mechanism
- attacking weak passwords
- concept of use to spread other attacks

Descendants

- Code Red
- Slammer
- Probably others... Nimbda, Stuxnet? etc... (I found mention but no substantive, concrete comparison)

Evolved Awareness and Perception

- long term influence on perception
  - new vulnerabilities and attacks on same old vectors for same old reasons ***(transition)
  - with new worms, people still saying the same thing in the aftermath
  - there isn't much question now: cybercriminals are criminals, not admirable geniuses or heros
  - there isn't much question now: we blame the victim... both of them. Admins and vendors point fingers at eachother, following the Morris Worm trend
- Long term influence in formal cyber security and cyber crime
  - CFAA still being expanded to deal with criminals like Morris

– CERT still handling real crises, like the newer ones mentioned above

– CIRT is a commonly studied and applied topic

– Cyber Security is a more popular and relevant field than ever

Post Mortem

- what this paper covered
- synthesize/speculate
  - what else could have happened?
  - if not for this worm, would something else have taken its place? probably, and it could have been meaner
  - was the overall impact positive, negative, or neutral?... neutral to positive
  - are Morris and other's like him brilliant? Not even in his day, and definitely not today... kiddies
  - How have worm driven attacks evolved? (not by much honestly, they just spread faster)
  - How has public perception of attacks shifted? - as far as blame, not much. as far as idolozing, very much
  - How has prosecution of cybercrime changed over time? - still a cat and mouse came between technology and legislation

References

[Adams(1996)] Jo-Ann M. Adams. Controlling cyberspace: applying the computer fraud and abuse act to the internet. *Santa Clara Computer & High Tech. LJ*, 12:403, 1996.

[Bailey et al.(2005)Bailey, Cooke, Jahanian, and Watson] M. Bailey, E. Cooke, F. Jahanian, and D. Watson. The Blaster Worm: Then and Now. *IEEE Security Privacy*, 3 (4):26–31, July 2005. ISSN 1540-7993. doi: 10.1109/MSP.2005.106.

[Berghel(2001)] Hal Berghel. The code red worm. *Communications of the ACM*, 44(12): 15–19, 2001.

[Coffin(2003)] B. Coffin. Slammer worm exploits risk management lapses. *Risk Reporter*, 2003.

[Eichin and Rochlis(1989)] Mark W. Eichin and Jon A. Rochlis. With microscope and tweezers: An analysis of the internet virus of november 1988. In *Security and Privacy, 1989. Proceedings., 1989 IEEE Symposium on*, pages 326–343. IEEE, 1989.

[Eisenberg et al.(1989)] Eisenberg et al. The Cornell commission: on Morris and the worm. *Communications of the ACM*, 32(6):706–709, 1989.

[Fisher(2001)] Dennis Fisher. Code Red worm exposes security flaws. *eWeek*, 18(29):1, July 2001. ISSN 15306283.

[Fisher(2002)] Dennis Fisher. Living with worms, viruses, and daily security alerts. *eWeek*, 19(6):20, February 2002. ISSN 15306283.

[Fithen and Fraser(1994)] Katherine Fithen and Barbara Fraser. CERT incident response and the Internet. *Communications of the ACM*, 37(8):108–113, 1994.

[Gardner(1989)] Phillip E. Gardner. The internet worm: What was said and when. *Computers & Security*, 8(4):305–316, June 1989. ISSN 0167-4048. doi: 10.1016/0167-4048(89)90092-8.

[Lee(2013)] T. Lee. How a grad student trying to build the first botnet brought the Internet to its knees - The Washington Post. *The Washington Post*, 2013.

[Marsan(2008)] Carolyn Duffy Marsan. Morris worm turns 20: Look what it's done. *Network World*, October 2008.

[Moore(2001)] Cathleen Moore. CM targets Web services. *InfoWorld*, 23(32):18, August 2001. ISSN 01996649.

[Moore et al.(2003)Moore, Paxson, Savage, Shannon, Staniford, and Weaver] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. Inside the Slammer worm. *IEEE Security Privacy*, 1(4):33–39, July 2003. ISSN 1540-7993. doi: 10.1109/MSECP.2003.1219056.

[Panko(2003)] Raymond R. Panko. Slammer: The first blitz worm. *Communications of the Association for Information Systems*, 11(1):12, 2003.

[Schultz(2003)] Eugene Schultz. Security views. *Computers & Security*, 22(3):176–187, April 2003. ISSN 0167-4048. doi: 10.1016/S0167-4048(03)00302-X.

[Seeley(1989)] Donn Seeley. A Tour of the Worm. In *Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February*, 1989.

[Spafford(1989a)] Eugene H. Spafford. Crisis and aftermath. *Communications of the ACM*, 32(6):678–687, 1989a.

[Spafford(1989b)] Eugene H. Spafford. The Internet worm program: An analysis. *ACM SIGCOMM Computer Communication Review*, 19(1):17–57, 1989b.

[Spafford(1989c)] Eugene H. Spafford. The internet worm incident. In *European Software Engineering Conference*, pages 446–468. Springer, 1989c.

[Strawn(2014)] G. Strawn. Masterminds of the Arpanet. *IT Professional*, 16(3):66–68, May 2014. ISSN 1520-9202. doi: 10.1109/MITP.2014.32.

[Tynan(2003)] Daniel Tynan. Dawn of the Superworm. *PCWorld*, 21(5):26, May 2003. ISSN 07378939.