CS 526: Information Security - Fall 2017

Following the Morris Worm

Phil Van Every

November 30, 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 began to realize the importance of internet security.

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 and importance of computer security to both legitimate and malevolent users.

Contents

Incubation

- background/context
  - birth and growth of the internet
  - early internet use and perception
  - beginnings of research into viruses and worms
  - exploration of vulnerabilities, particularly in unix
  - technical and characteristic unpreparedness for large-scale Morris Worm type attack ***(transition)
- layout rest of paper
  - What is theme of this paper? How the Morris Worm helped bring us from point A (above) to point B (today)
  - What sections are in it?
  - What does each of these sections illustrate?

Outbreak

Black Thursday

- intro
- Nov 1988 - release/discovery [Spafford(1989a)]
- symptoms
- how many infected
- Morris' friend anonymous email

Vaccination

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

Anatomy

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

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

[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, Gries, Hartmanis, Holcomb, Lynn, and Santoro] Ted Eisenberg, David Gries, Juris Hartmanis, Don Holcomb, M. Stuart Lynn, and Thomas Santoro. The Cornell commission: on Morris and the worm. *Communications of the ACM*, 32(6):706–709, 1989.

[Fisher(2002)] Dennis Fisher. LIVING WITH WORMS, VIRUSES AND DAILY SECURITY ALERTS. (cover story). *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.

[Hinden et al.(1983)Hinden, Haverty, and Sheltzer] R. Hinden, J. Haverty, and A. Sheltzer. The DARPA Internet: Interconnecting Heterogeneous Computer Networks with Gateways. *Computer*, 16(9):38–48, September 1983. ISSN 0018-9162. doi: 10.1109/MC.1983.1654494.

[Kelty(2010)] Christopher Kelty. The Morris Worm. *Limn*, December 2010.

[Lee(2013)] Timothy B. Lee. How a grad student trying to build the first botnet brought the Internet to its knees. *Washington Post*, November 2013. ISSN 0190-8286.

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

[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)] George Strawn. Masterminds of the Arpanet. *IT Professional*, 16(3): 66–68, 2014.