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.

Outline

1. Abstract
2. Introduction
   - background/context
     - birth and growth of internet
     - early internet use and perception
     - resulting emergent cyber threats
   - layout rest of paper
3. Outbreak
   - intro
   - Nov 1988 - release/discovery
   - symptoms
   - how many infected
   - Morris' friend anonymous email
   - what researchers did to stop it
     - sh soln.
     - software patches
     - mailing list
     - quarantined email solutions
     - disassembly and analysis ***(transition into next section)
4. Anatomy
   - Defense
     - 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
      - detecting itself
      - coinflip for self termination and immortality
   - password cracking
      - common words and permutations
      - unix dictionary
      - other stuff
   - bugs, mistakes, omissions
      - checks for good return values
      - pass struct instead of pointer to struct
      - UDP to ernie over TCP connection, never sent
      - accidental leftover files in /tmp (of compilation too slow?)
      - joke about bug fixes in worm
      - other stuff pointed out by Spaf
   - unused features- could have been much worse... ***(transition into next section)
   - conclusion

5. Aftermath

- intro
- Perception and awareness
  - of the research community
    - virus vs. worm terminology
    - 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
  - 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
   - conclusion

6. Influence
   - intro
   - other demonstrations of exploits
     - email as a spread mechanism
     - attacking weak passwords
     - concept of use to spread other attacks
   - Other worms it inspired and how
     - Code Red
     - Slammer
     - Probably others... Nimbda, Stuxnet? etc... (I found mention but no substantive, concrete comparison)
   - 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
    a) CFAA still being expanded to deal with criminals like Morris
    b) CERT still handling real crises, like the newer ones mentioned above
    c) CIRT is a commonly studied and applied topic
  - conclusion

7. Conclusion
   - 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

1. **Introduction**

   This section will provide some background. In particular, it will briefly address the birth and growth of the internet, how it was used and perceived early on, and resulting emergent cyber threats. This section will then introduce the Morris Worm and map out the rest of the paper.

2. **Outbreak**

   This section will walk the reader through the outbreak of the worm. It will relate *what* actually happened. It will discuss the release and discovery of the worm, symptoms of infected machines, rate and size of the infection, and finally, the containment and eradication of the worm. Accounts of immediate crisis response tactics employed by the research community will seed discussion about the worm's impact in later sections.

3. **Anatomy**

   This section will dissect the worm and analyze its anatomy. It will relate *how* the worm worked. Discussion topics will include target host machines and their vulnerabilities, exploits used by the worm to spread itself, the worm's life cycle and activities, its intended behavior, and unanticipated behaviors that lead to the crisis. The Morris Worm's anatomy will be exhibited in enough detail to spur a discussion of its influence on future worms and cyber attacks in subsequent sections.

4. **Aftermath**

   This section will discuss the short to mid term impact of the Morris Worm crisis. Discussion topics will include software vulnerability patches, cyber security legislation, resulting research and publications, the formation of the CERT at CMU, and general public perception and awareness of cyber crime. It will point out groundbreaking events that occurred during or immediately after the Morris Worm crisis, including Robert Morris' prosecution under the Computer Fraud and Abuse Act and the formation of the CERT at CMU.

5. **Influence**

   This section will discuss mid to long term impacts of the Morris Worm. Discussion topics may include other worms and exploits inspired by the Morris Worm, software security principles influenced by the Morris Worm, longterm drift in cyber security awareness and perception, and continued research and legislation.

6. **Conclusion**

   This section will briefly recapitulate the topics and theme of the paper. It will then further discuss the impact of the Morris Worm. Questions addressed may include:

   a) Was the overall impact positive, negative, or neutral?

   b) Are Morris and others like him brilliant? deviant? both?

   c) How have worm driven cyber attacks evolved over time? A lot? Not much?

   d) How has public perception of cyber attacks changed over time? A lot? Not much?

   e) How has public perception of the Morris Worm incident changed over time?

   f) How has public perception of Robert Morris changed over time?

   g) How has prosecution of cyber crime changed over time? A lot? Not much?

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

- Nov 1988 - release/discovery
- symptoms
- how many infected
- what it was meant to do
- what it actually did

Anatomy

Reproduction

- fingerd exploit
- other replication exploit
- detecting itself
- coinflip for self termination and immortality

Password Cracking

Unused Features

(botnet stuff etc)

Convalescence

Legislation

1. first felony prosecution under CFAA

2. resulting new legislation (if any)

Research and Publications

CERT at CMU

Evolution

Public Awareness

- initially researchers trusted APRAnet
- now, the internet is assumed to be dangerous
- how public perceives cybercrime and computer "whiz"

Daughter Worms

1. worm A
2. worm B
3. etc.

Other Exploits

- email as a spread mechanism
- attacking weak passwords
- concept of a botnet

Post Mortem

TODO: Write an summary here...

1. what this paper covered
   - What is theme of this paper again?
   - What sections were in it?
   - What did each of these sections illustrate?
2. synthesize/speculate
   - what else could have happened?
   - if not for this worm, would something else have taken its place?
   - was the overall impact positive, negative, or neutral?

References