# Morris Worm: the First Buffer Overflow Vulnerability

History

- Released at 8:30pm, 2 November 1988 by Robert Tappan Morris, a graduate student at Cornell University
- Launched from the computer system of MIT, trying to confuse the public that this is written by MIT students, not Cornell.
- Buffer overflow in sendmail, fingerd network protocol, rsh/rexec, etc.

Impact

- ~6,000 UNIX machines infected (10% of computers in Internet)
- Cost: $100,000 - $10,000,000
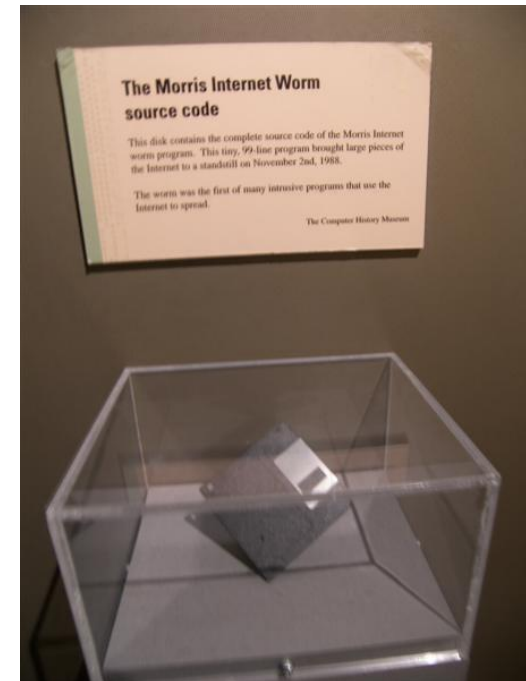
loppy disk containing the source code for the Morris Worm, at the Computer History Museum

Robert Tappan Morris

What happens after Morris Worm

▸ Tried and convicted of violation of 1986 Computer Fraud and Abuse Act. This is the first felony conviction of this law.

▸ Sentenced to three years' probation, 400 hours of community service, and a fine of $10,050 (equivalent to $22,000 in 2023).

▸ Had to quit PhD at Cornell. Completed PhD in 1999 at Harvard.

▸ Cofounded Y Combinator in 2005

▸ Became a tenured professor at MIT in 2006. Elected to the National Academy of Engineering in 2019.

Robert Tappan Morris, Entrepreneur, professor at MIT

Following Morris Worm

Code Red
Targeting Microsoft's IIS web server. Affected 359,000 machines in 14 hours

Sasser
Targeting LSASS in Windows XP and 2000. Affected around 500,000 machines. Author: 18-year-old German Sven Jaschan. Received 21-month suspended sentence

Stuxnet
Targeting industrial control systems, and responsible for causing substantial damage to the nuclear program of Iran

There are more…

2001   2003   2005   2008   2010   2012

SQL Slammer
Targeting Microsoft's SQL Server and Desktop Engine database. Affected 75,000 victims in 10 minutes

Conficker
Targeting Windows RPC. Affected around 10 million machines

Flame
Targeting cyber espionage in Middle Eastern countries