

# Twenty years later

## Morris' legacy

Evandro Curvelo Hora  
evandro@tempest.com.br  
Recife/2008

 **Tempest**  
Security Intelligence



# Do you remember ?

11-9wic.mpg

 **Tempest**  
Security Intelligence

# What's going on ?

*“There may be a virus loose on the internet.”*

Andy Sudduth (of Harvard)  
34 minutes after midnight, Nov. 3, 1988.



# Virus X Worm

- **Primary difference between worms and other illicit computer programs (often referred to as viruses):**
  - The method of operation the programs use in order to reproduce and spread.
  - **Virus :**
    - Alters a system file, or some other convenient file, which is likely to be used sometime in the near future;
    - The alteration to this file usually is the addition of commands that will activate the virus wherever it is on the computer;
    - Until the user (inadvertently) activates the virus, the virus is dormant on the computer;
    - Until the altered file is called, the virus is unable to do any activity;
    - A virus needs to be carried from one computer to another.
  - **Worm :**
    - A worm gains access to a computer (usually by breaking into it over the internet) it launches a program which searches for other internet locations, infecting them if it can;
    - At no time does the worm need user assistance (accidental or not) in order to operate its programming;
    - The worm travels over the internet, so all machines attached to an infected machine are at risk of attack;
    - Worms can spread with no assistance (as opposed to viruses which must literally be carried from one machine to another). Once the worm discovers an internet connection, all that it must do is download a copy of itself to that location, and continue running as normal.



# Internet Worm

- Robert Tappan Morris, a 23 year old student at Cornell University;
- A small C (99 lines, not including object files) program;
- 6.000 computers crashed, only in USA, in a 24 h tour;
- Rises a question: are the networks vulnerable ?



## What worm did to systems ?

- Explored *sendmail* and *fingerd* servers vulnerabilities:
  - sendmail: exploring a *project feature*;
  - fingerd: exploring a *software bug*.
- Explored *trust relationships*:
  - rexec
  - rsh
- Explored users *weakness*
  - *Passwords cracking*

## What worm didn't do to systems ?

- The worm didn't alter or destroy files;
- The worm didn't save or transmit the passwords which it cracked;
- The worm didn't make special attempts to gain root or superuser access in a system (and didn't utilize the privileges if it managed to get them);
- The worm didn't place copies of itself or other programs into memory to be executed at a later time. Such programs are commonly referred to as timebombs.
- The worm didn't attack machines other than Sun 3 systems and VAX computers running 4 BSD Unix (or equivalent).
- The worm didn't attack machines that were not attached to the internet. In other words, no computers that didn't have an internet address were attacked. Modems do not count as internet connectors in this respect.
- The worm didn't travel from machine to machine except via network functionality.
- The worm didn't cause physical damage to computer systems.

## Worm's main.c (1 of 4)



```
#include <stdio.h>
#include <signal.h>
#include <string.h>
#include <sys/resource.h>
long current_time;
struct rlimit no_core = {0,0};

int

main (argc, argv)
    int argc;
    char *argv[];
{
    int n;
    int parent = 0;
    int okay = 0;
        /* change calling name to "sh" */
    strcpy(argv[0], "sh");
        /* prevent core files by setting limit to 0 */
    setrlimit(RLIMIT_CORE, no_core);
    current_time = time(0);
```

## Worm's main.c (2 of 4)

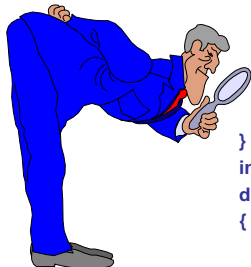


```
/* seed random number generator with time */
srand48(current_time);
n = 1;
while (argv[n]) {
    /* save process id of parent */
    if (!strcmp(argv[n], "-p", 2)) {
        parent = atoi(argv[++n]);
        n++;
    }
    else {
        /* check for 1l.c in argument list */
        if (!strcmp(argv[n], "1l.c", 4))
            okay = 1;

        /* load an object file into memory */
        load_object(argv[n]);
        /* clean up by unlinking file */
        if (parent)
            unlink(argv[n]);
        /* and removing object file name */
        strcpy(argv[++n], "");
    }
}
```

Tempest  
Security Intelligence

## Worm's main.c (3 of 4)



```
/* if 1l.c was not in argument list, quit */
if (!okay)
    exit(0);
/* reset process group */
setpgrp(getpid());
/* kill parent shell if parent is set */
if (parent)
    kill(parent, SIGHUP);
/* scan for network interfaces */
if_init();
/* collect list of gateways from netstat */
rt_init();
/* start main loop */
doit();
}
int
doit()
{
    current_time = time(0);
    /* seed random number generator (again) */
    srand48(current_time);
    /* attack gateways, local nets, remote nets */
    attack_hosts();
}
```

Tempest  
Security Intelligence

## Worm's main.c (4 of 4)

```

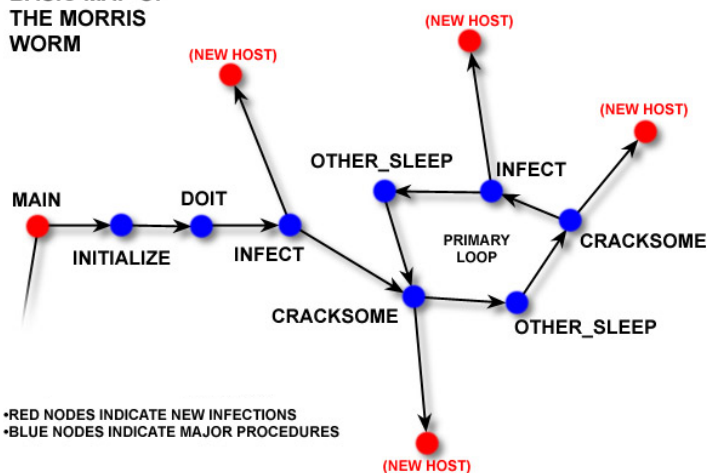
/* check for a "listening" worm */
check_other ()
/* attempt to send byte to "ernie" */
send_message ()
for (;;) {
/* crack some passwords */
crack_some ();
/* sleep or listen for other worms */
other_sleep (30); crack_some ();
/* switch process id's */
if (fork())
/* parent exits, new worm continues */
exit (0);
/* attack gateways, known hosts */
attack_hosts(); other_sleep(120);
/* if 12 hours have passed, reset hosts */
if(time (0) == current_time + (3600*12)) {
reset_hosts();
current_time = time(0); }
/* quit if pleasequit is set, and nextw>10
if (pleasequit && nextw > 10)
exit (0);
}
    
```



Tempest  
Security Intelligence

## Worm's modus operandi

### BASIC MAP OF THE MORRIS WORM



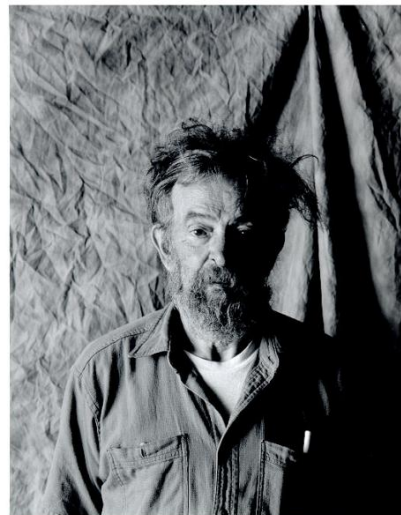
Tempest  
Security Intelligence

*Morris Jr no dia do julgamento...*



Tempest  
Security Intelligence

*Creator & creature...*



Tempest  
Security Intelligence

***... and if you think  
information security  
people are strange  
people...***

**Tempest**  
Security Intelligence

***... so try Dan Farmer...***



**Tempest**  
Security Intelligence

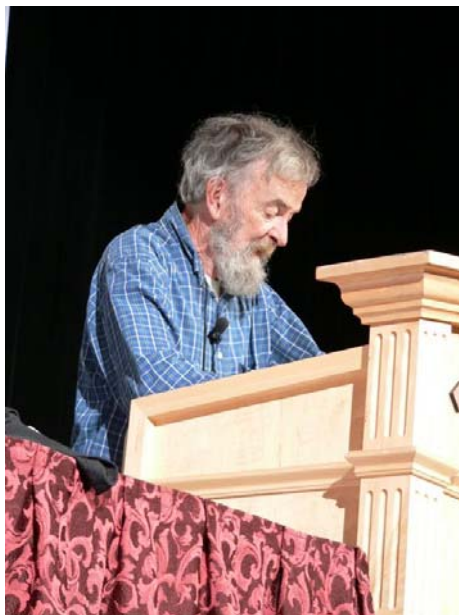


*... or even the Tempest crew!*

**Censured!**  
**;-)**

 Tempest  
Security Intelligence

*Bob Morris speaking*



 Tempest  
Security Intelligence

## Maybe a normal person...



Tempest  
Security Intelligence


## Today he is an associated professor at MIT...

CSAIL Biography - Windows Internet Explorer


http://www.csail.mit.edu/biographies/PeopleID=301

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

CSAIL Biography



### Robert Morris



Position: Associate Professor  
Office: 32-G972  
Phone: 253-5983  
E-mail: [rm@csail.mit.edu](mailto:rm@csail.mit.edu)  
Research Director(s): Systems

URL: <http://www.pdos.csail.mit.edu/~rm/>

**Biography:**

Robert Morris is an assistant professor in MIT's EECS department and a member of the Computer Science and Artificial Intelligence Laboratory. He received a PhD from Harvard University for work on modeling and controlling networks with large numbers of competing connections. As a graduate student he helped design and build an ARPANET-funded ATM switch with per-circuit hop-by-hop flow control. He led a mobile communication project which won a best student paper award from USENIX. He cofounded Viewns, an e-commerce hosting service. His current interests include modular software-based routers, analysis of the aggregation behavior of Internet traffic, and scalable ad-hoc routing.

**Recent and/or Significant Publications:**

Jinyang Li, John Jannotti, Douglas S. J. De Couto, David R. Karger, Robert Morris, IA Scalable Location Service for Geographic Ad Hoc Routing, ACM Mobicom 2000, Boston, MA.

R. Morris, E. Kohler, J. Jannotti, M. Frans Kaashoek, IThe Click Modular Router, In the Proceedings of the 17th ACM Symposium on Operating Systems Principles (SOSP '00), Kiawah Island, South Carolina, December 1999, pages 217-231

Home  
About CSAIL  
Lab Organization  
Directory  
Faculty  
Research Activities  
Events  
News  
Awards  
Outreach  
Joining CSAIL  
Member Resources  
Contact Us  
CSAIL Publications

## *Why celebrate an attack ?*

- **History is a huge and useful pack of human experience...**
- **If you are smart people, you learn with others mistakes!**

 Tempest  
Security Intelligence

*I have seen really worse celebrations...*



 Tempest  
Security Intelligence

## Lessons

- Access to certain files should be only granted to those who need said access.
- Heterogeneous networks as an advantage.
- A slightly less technical nature is that the sharing of research on something such as the worm (as MIT and Berkeley did in their attempts to decompile the program) is immensely helpful;
- Network security was shown to be incapable of defending from such attacks. Instead of concentrating on this area, many believe that the only real way to keep security tight is to have the defenses at the host, or computer, level.
- Beware of reflex reactions to computer problems. When system administrators discovered that the Worm was using sendmail to penetrate their systems, many of the responded by shutting down their mail server. This proved to be a cure that was worse than the disease. The worm had a number of other attack methods, and so was not really hampered by the loss of the mail utility. The only real result of the loss of the mail systems was the fact that mail describing how to defeat the worm and fix the bugs was delayed in reaching some sites.
- Logging information is vital in discovering the source of infections such as the Worm.
- In conclusion, the Worm made the internet community better prepared to handle and repel another such attack. However, the fact is that security is often a trade off with convenience, and for most day-to-day users, convenience ranks pretty highly.



Tempest  
Security Intelligence

## Lessons ? Are you sure ?

- Why...
  - ...new worms and other malwares pops up every day ?
  - ... functionalities and/or bugs continues to be a huge vulnerability source ?
  - ... we still choose weak passwords ?
  - ... deny of service attacks happens today ?
  - ... buffer overruns/overflows still happens today ?
  - ... we insist in use of network trusted domains/realms ?
  - ... our strong beliefs in eradicate security problems only using technology ?



Tempest  
Security Intelligence

## ***Some things we are doing right now***

- **Market & trends demands...**
  - Improving our capacity to offer/provide security services (ethical hacking, managed security services, risk management) by:
    - **Head hunting:**
      - Hacking/cracking is like art... is not an usual expertise;
        - » Some basic expertise and skills are a true *gift*;
        - » Code breaking expertise, users psychology, philosophy, deception strategies and techniques skills, ethos, strong discipline... are not commodities.
- **Processes/tests/techniques (creation/tuning):**
  - Web applications cracking techniques;
  - Emerging technologies (cell phones, mobile computing etc);
  - General cracking shortcuts.

 Tempest  
Security Intelligence

## ***Some things we doing right now***

- **We think/believe we are not wasting our time with:**
  - TCP/IP layers using harassment approaching;
  - Security Information Doctrine;
  - Classical War Strategy, Assimetric War, Wargames (Sun Tzu, Hannibal, Alexander, Frederik II, Napoleon I, Clausewitz, Lee, Shermann, Mahan, Arnold, Moltke, Guderian, Rommel, Liddell-Hart, Mao, Guevara, Mitchell...)
  - Math: games theory, topology;
  - Quantum computing sideeffects;
  - Foundations: math, computing and philosophy.
    - » Gödel, Church, Turing, von Neumann, Kleenan, Shannon, Shorr, Riemann, Hilbert, Knut, Dijkstra, Bertrand Russel, Popper, Penrose...

 Tempest  
Security Intelligence

## Some stuff to read...

- [Cyberpunk](#) by Katie Hafner and John Markoff, Touchstone Books, New York. 1991.
- CA-89:04 CERT Advisory, "WANK" Worm in SPAN Network October 17, 1989 (cert@cert.org).
- FAQ written by Rober Gasch (rgasch@nl.oracle.com), September 23, 1992.
- *United States General Accounting Office report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce House of Representatives: Computer Security- Virus highlights need for improved Internet management*, June 1989.
- *"With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988*, by Mark Eichen (eichen@athena.mit.edu) and Jon Rochlis (jon@bitsy.mit.edu), Massachusetts Institute of Technology, Boston. 1988.
- March 7, 1991 United States Court of Appeals, Second Circuit. Decision on Morris's appeal of his conviction.
- *The Helminthiasis of the Internet* (RFC 1135) by J. Reynolds (JKREY@ISI.EDU), Network Working Group, December 1989.
- *Improving the Security of your Unix System* by David A. Curry April 1990.
- *A Tour of the Worm* by Donn Seeley.
- *The Internet Worm Program: An Analysis* by Eugene H. Spafford (spaf@cs.purdue.edu), November 29, 1988; revised december 8, 1988.
- *The Internet Worm Incident: Technical Report CSD-TR-933* by Eugene H. Spafford (spaf@cs.purdue.edu), September 19, 1991.
- *A Report on the Internet Worm* by Bob Page, November 7, 1988.
- Open mail message from Keith Bostic (bostic@OKEEFFE.BERKELEY.EDU), November 4, 1988, *Virus posting #3*.



## Thank you!

Any questions ?

evandro@tempest.com.br

