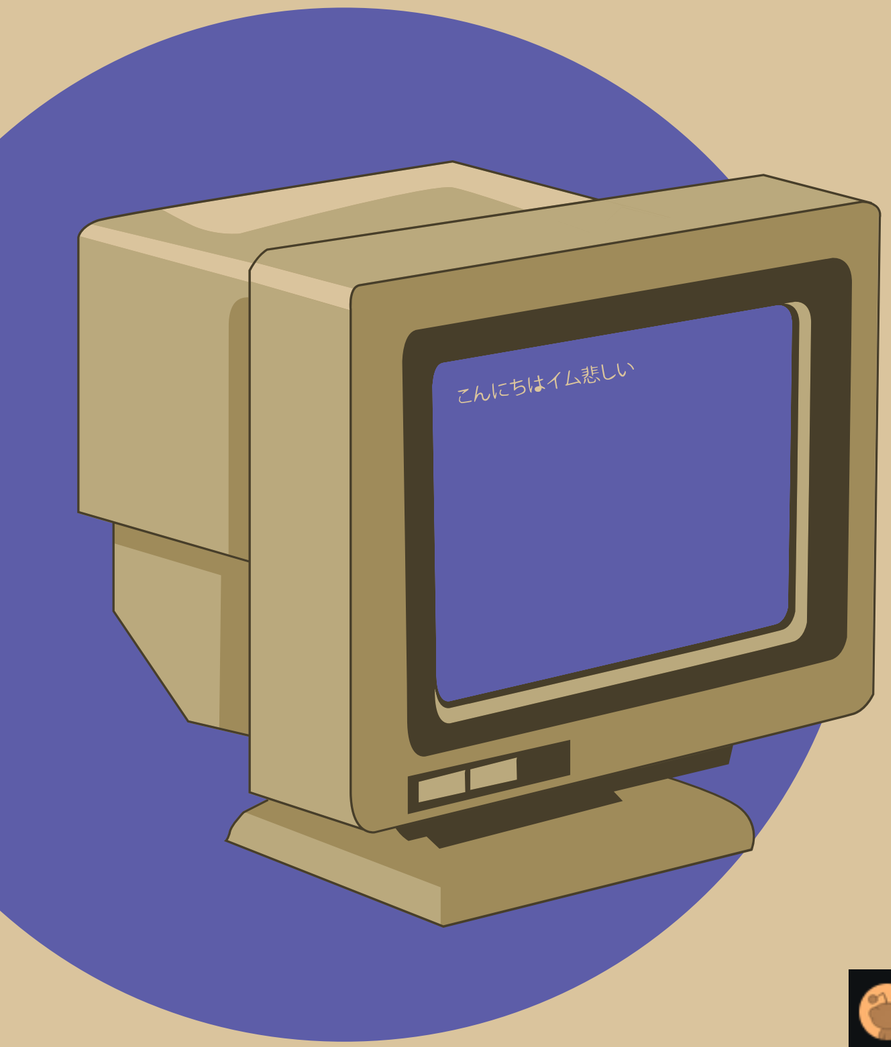
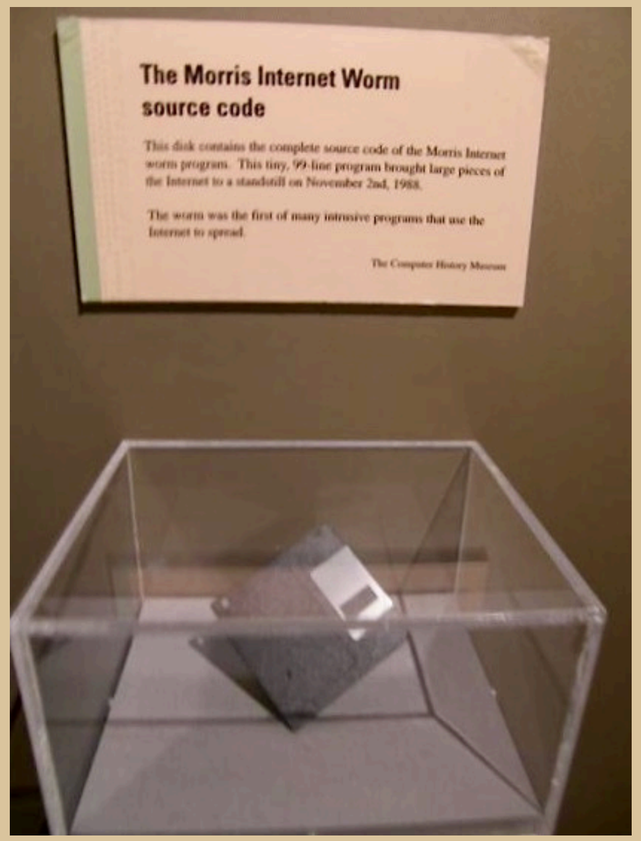
CS7NS5-202425 SECURITY AND PRIVACY



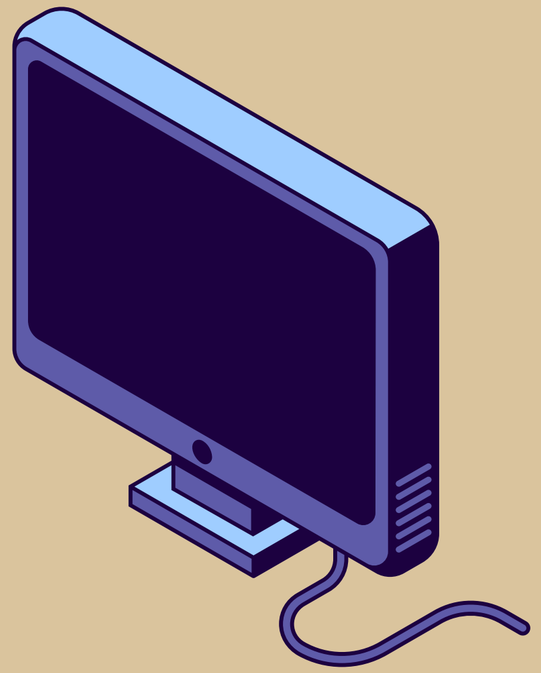


MORRIS WORM

~ KARTHIK VENKATESH NAGARAJ

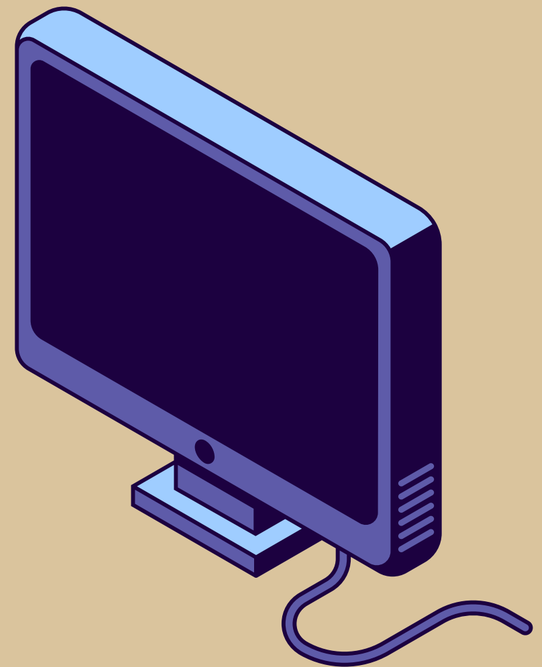
WHAT IS A WORM?

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through.



IN 1988,

- Robert Tappan Morris, launched a worm that took advantage of C2 infrastructure from a machine at Cornell University, targeting other machines that ran a specific version of the UNIX operating system.
- Due to a design flaw in the script, the worm ended up replicating itself a lot more times than originally intended.
- This ended up reaching around 6,000 (out of 60,000 total back then) different systems across various different universities in the USA.
- The worm did not damage or destroy files, but it still packed a punch. Vital military and university functions slowed to a crawl. Emails were delayed for days.



HOW DID THE WORM WORK?

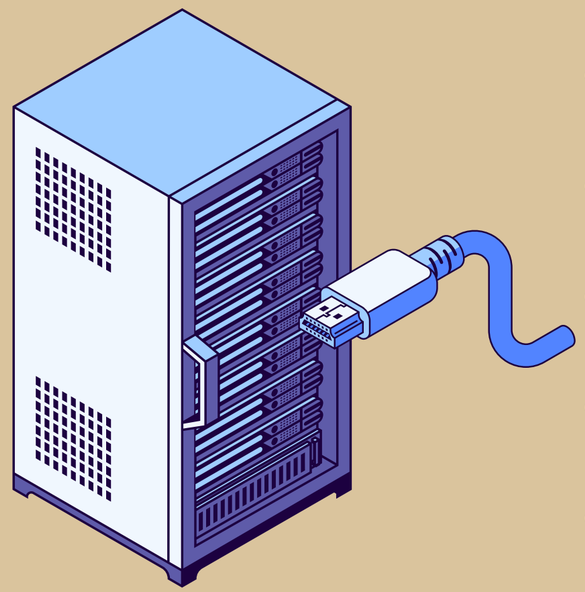
3 main channels of attack that the Morris worm employed:

- **SENDMAIL Attack:** the worm opens a TCP connection to another machine's sendmail (the SMTP port), invokes debug mode, and sends a RCPT TO that requests its data be piped through a shell. This data containing code scripts is then ran on the target computer, thus exploiting the system looking for more vulnerable targets.

- **FINGERD Attack:** In the fingerd attack, it tries to infiltrate systems via a bug in fingerd, the finger daemon. When fingerd is connected to, it reads its arguments from a pipe, but doesn't limit how much it reads. After the stack is a command to be executed ("/usr/ucb/finger") that actually does the work. On a VAX computer, the worm knew how much further from the stack it had to clobber to get to this command, which it replaced with the command "/bin/sh" (the bourne shell). So, a shell that has access to the network socket was started with no arguments thus making it able to bring over files the same was as the previos attack.

- **RSH/REXEC Attack:** get into systems was via the .rhosts and /etc/hosts.equiv files to determine 'trusted' hosts where it might be able to migrate to. To use the .rhosts feature, it needed to actually get into people's accounts which it did so by employing password cracking mechanisms.

CONSEQUENCES OF THE WORM



- Estimated damages from $100,000 up to a couple million dollars. [1]
- FBI launch an investigation and quickly identify Robert Tappan Morris as the culprit.
- Robert becomes the first person to be convicted under the US Computer Fraud and Abuse Act in 1989.
- Robert was sentenced to 3 years of probation, 400 hours of community service as well as a $10,050 fine.
- Cybersecurity and internet safety awareness became a top priority for users.
- But at the same time, the Morris worm inspired a multiple generations of ethical/unethical hackers to come.
- Robert completed his PhD at Harvard in 1999, and is now a dot com millionaire and a computer science professor at MIT.

MODERN WORMS SIMILAR TO THE MORRIS WORM

STUXNET - 2010

A sophisticated cyberattack discovered in 2010 that targeted the Iranian nuclear program. It was one of the earliest instances of malware using C2 infrastructure to infect and control target systems.

NOTPETYA- 2017

A destructive malware attack that impacted organizations worldwide in 2017. It initially spread through a software supply chain attack, infecting a Ukrainian accounting software called MEDoc with the malware, affecting everyone who installed it.

OPERATION AURORA - 2010

An espionage campaign that targeted companies in the technology, defense and financial sectors, among others. The attackers used C2 infrastructure to remotely control and exfiltrate sensitive data from targeted organizations.

WANNACRY - 2017

A highly virulent ransomware attack that affected over 200,000 computers in 150 countries in 2017. The virus spread by using a vulnerability in the Microsoft Windows operating system.

SOURCE