November 2, 2018

Twitter (https://twitter.com/intent/tweet?text=The%20Morris%20Worm&url=https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218) Facebook (https://www.facebook.com/sharer/sharer.php?u=https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218&t=The%20Morris%20Worm) Email (mailto:?Subject=%22The%20Morris%20Worm%22&body=https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218)

The Morris Worm

30 Years Since First Major Attack on the Internet

At around 8:30 p.m. on November 2, 1988, a maliciously clever program was unleashed on the Internet from a computer at the Massachusetts Institute of Technology (MIT).

This cyber worm was soon propagating at remarkable speed and grinding computers to a halt. “We are currently under attack,” wrote a concerned student at the University of California, Berkeley in an email later that night. Within 24 hours, an estimated 6,000 of the approximately 60,000 computers that were then connected to the Internet had been hit. Computer worms, unlike viruses, do not need a software host but can exist and propagate on their own.

Berkeley was far from the only victim. The rogue program had infected systems at a number of the prestigious colleges and public and private research centers that made up the early national electronic network. This was a year before the invention of the World Wide Web. Among the many casualties were Harvard, Princeton, Stanford, Johns Hopkins, NASA, and the Lawrence Livermore National Laboratory.

The worm only targeted computers running a specific version of the Unix operating system, but it spread widely because it featured multiple vectors of attack. For example, it exploited a backdoor in the Internet's electronic mail system and a bug in the "finger" program that identified network users. It was also designed to stay hidden.

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. The network community labored to figure out how the worm worked and how to remove it. Some institutions wiped their systems; others disconnected their computers from the network for as long as a week. The exact damages were difficult to quantify, but estimates started at $100,000 and soared into the millions.

As computer experts worked feverishly on a fix, the question of who was responsible became more urgent. Shortly after the attack, a dismayed programmer contacted two friends, admitting he'd launched the worm and despairing that it had spiraled dangerously out of control. He asked one friend to relay an anonymous message across the Internet on his behalf, with a brief apology and guidance for removing the program. Ironically, few received the message in time because the network had been so damaged by the worm.

Independently, the other friend made an anonymous call to *The New York Times*, which would soon splash news of the attack across its front pages. The friend told a reporter that he knew who built the program, saying it was meant as a harmless experiment and that its spread was the result of a programming error. In follow-up conversations with the reporter, the friend inadvertently referred to the worm's author by his initials, RTM. Using that information, *The Times* soon confirmed and publicly reported that the culprit was a 23-year-old Cornell University graduate student named Robert Tappan Morris.

This cyber worm was soon propagating at remarkable speed and grinding computers to a halt. “We are currently under attack,” wrote a concerned student at the University of California, Berkeley.

Morris was a talented computer scientist who had graduated from Harvard in June 1988. He had grown up immersed in computers thanks to his father, who was an early innovator at Bell Labs. At Harvard, Morris was known for his technological prowess, especially in Unix; he was also known as a prankster. After being accepted into Cornell that August, he began developing a program that could spread slowly and secretly across the Internet. To cover his tracks, he released it by hacking into an MIT computer from his Cornell terminal in Ithaca, New York.

After the incident became public, the FBI launched an investigation. Agents quickly confirmed that Morris was behind the attack and began interviewing him and his associates and decrypting his computer files, which yielded plenty of incriminating evidence.

But had Morris broken federal law? Turns out, he had. In 1986, Congress had passed the Computer Fraud and Abuse Act, outlawing unauthorized access to protected computers. Prosecutors indicted Morris in 1989. The following year, a jury found him guilty, making him the first person convicted under the 1986 law. Morris, however, was spared jail time, instead receiving a fine, probation, and an order to complete 400 hours of community service.

The episode had a huge impact on a nation just coming to grips with how important—and vulnerable—computers had become. The idea of cybersecurity became something computer users began to take more seriously. Just days after the attack, for example, the country’s first computer emergency response team was created in Pittsburgh at the direction of the Department of Defense. Developers also began creating much-needed computer intrusion detection software.

At the same time, the Morris Worm inspired a new generation of hackers and a wave of Internet-driven assaults that continue to plague our digital systems to this day. Whether accidental or not, the first Internet attack 30 years ago was a wake-up call for the country and the cyber age to come.