Nervous System #37: The 414s

BY DAVID KALAT

With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have been with us longer than we remember.

Nervous System *is a bimonthly blog that approaches issues of data privacy and cyber security from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.*

On the evening of May 9, 1983, an employee of Los Alamos National Laboratory ("LANL") was working from home. Just as it does today, "working from home" in 1983 meant remotely connecting to the organization's computer network using the TCP/IP network connections that today constitute the modern Internet. And this employee, John F. Davis, started getting communications from a user who was logged on as "DEMO." Those communications seemed very odd. For one thing, "DEMO" seemed unsure what system he was on, which was unnerving because the system in question was one of the nation's most sensitive nuclear weapons research facilities. Furthermore, "DEMO" seemed preoccupied with figuring out what games he could play on the system, and impatient with Davis' explanations that NANL was not storing any computer games on the research computers used by atomic scientists.

Davis had no way to know this at the time, but he had encountered one of a soon-to-be-notorious gang of cybercriminals whose rampage through America's computer networks would expose the shocking lack of computer security and the growing menace of online hackers... or, put another way, Davis had just had an awkward encounter with a teenage kid.

On September 26, 1983, one of those kids, Neal Patrick, stood before the House Committee on Science and Technology to give his testimony on the issue of computer crime. His fellow witness on that first day of hearings was Jim McCleary, NAL's Division Leader of Operational Security and Safeguards—there to sheepishly explain how the seventeen year-old fan of the movie *War Games* had bypassed all of McCleary's operational security and safeguards in hopes of playing video games using Los Alamos' computer network.

Patrick's invasion of Los Alamos was not achieved alone—he was part of a group of computer enthusiasts in Milwaukee who had taken to using dial-up modems to explore supposedly "secure" computer networks for fun. Their explorations required only modest computer skills. Patrick and his friends discovered that many computer network administrators had never changed the default logins and passwords published in the system's instruction manuals. In other cases, the administrators' selection of custom logins and passwords left a lot to be desired.

Patrick and his friends were inspired by the way that Milwaukee street gangs named themselves after the numbered streets they commanded. As Patrick later explained, he'd see graffiti identifying the "1-9s" who ran 19th Street, or the "2-7s" who controlled 27th Street. The hackers were like a gang, too, but their turf was a patch of cyberspace they accessed through the telephone lines. So, they took to calling themselves the "414s," for Milwaukee's area code.

The 414s had little interest in taking corporate secrets or confidential information from the computers they roamed. Instead, they were primarily motivated to seek out computer games and earn the top scores. When prompted to enter their initials to log those scores, they gleefully entered "414."

That is not to say that their antics were entirely benign. On June 3, 1983 (as it happened, opening day for War Games' American release), the 414s accessed the computer network of the Sloan-Kettering Cancer Center in New York. The system administrators at Sloan-Kettering had protected their network with the username "test" and password "test." Once inside, the kids discovered that the system was logging their activity. Hoping to cover their tracks, they attempted to delete the logs, but ended up accidentally deleting the company's payment records. The damage was estimated at $1,500—a fairly minor loss to an institution of Sloan-Kettering's size, but it naturally attracted more attention than merely recording the high score on a game. Sloan-Kettering called the FBI.

The FBI planted a Star Trek game on the Sloan-Kettering system and waited for the 414 gang to come back and play it. When they did, the agents traced the activity back to the teenagers' respective bedrooms in Milwaukee. Then, the agents put physical wiretaps on their phones to monitor their activity and build up a case...

Except, as Patrick's testimony before Congress was ultimately used to illustrate, in 1983 the actions of the 414s were not self-evidently illegal. Law enforcement had to creatively bend existing laws around otherwise minor facets of the facts in hand to come up with substantive charges. Even then, Patrick's age placed him beyond serious prosecution, and his family's lawyer successfully negotiated an immunity deal for him.

The problem with cybersecurity in the early 1980s was that the skills and technology available to potentially malicious actors were fast outstripping society's ability to cope. The First Session of the 98th Congress convened a series of several days' worth of testimony and debate to try to rectify that gap. Of the six bills that were proposed in the wake of the hearings, none made it into law, but the various ideas and concerns they reflected were worked into the Comprehensive Crime Control Act of 1984, which was amended in 1986 to become the Computer Fraud and Abuse Act. The law made it illegal to intentionally access a computer without authorization or in excess of authorization. This gave law enforcement some of the tools they had been lacking in the battle against hacking, but also opened up new avenues of controversy and dispute—which we will explore next month.

Legaltech news

This article was originally published in Legaltech News on February 8, 2021.