The New York Times https://www.nytimes.com/2021/04/27/technology/daniel-kaminsky-dead.html

Daniel Kaminsky, Internet Security Savior, Dies at 42

If you are reading this obituary online, you owe your digital safety to him.

By Nicole Perlroth

Published April 27, 2021 Updated April 28, 2021

Daniel Kaminsky, a security researcher known for his discovery of a fundamental flaw in the fabric of the internet, died on Friday at his home in San Francisco. He was 42.

His aunt, Dr. Toby Maurer, said the cause was diabetic ketoacidosis, a condition that led to frequent hospitalizations in recent years.

In 2008, Mr. Kaminsky was widely hailed as a digital Paul Revere after he found a serious flaw in the internet's basic plumbing that could allow skilled coders to take over websites, siphon off bank credentials or even shut down the internet. Mr. Kaminsky alerted the Department of Homeland Security, executives at Microsoft and Cisco, and other internet security experts to the problem and helped spearhead a patch.

He was a respected practitioner of "penetration testing," the business of compromising the security of computer systems at the behest of owners who want to harden their systems from attack. It was a profession that his mother, Trudy Maurer, said he had first developed a knack for as a 4-year-old in San Francisco, after his father gave him a computer from Radio Shack. By age 5 he had taught himself to code.

His childhood paralleled the 1983 movie "War Games," in which a teenager, played by Matthew Broderick, unwittingly accesses a U.S. military supercomputer. When Daniel was 11, his mother said, she received an angry phone call from someone who identified himself as a network administrator for the Western United States. The administrator said someone at her residence was "monkeying around in territories where he shouldn't be monkeying around."

Without her knowledge, Daniel had been examining military websites. The administrator vowed to "punish" him by cutting off the family's internet access. Mrs. Maurer warned the administrator that if he made good on his threat, she would take out an advertisement in The San Francisco Chronicle denouncing the Pentagon's security.

"I will take out an ad that says, 'Your security is so crappy, even an 11-year-old can break it,'" she recalled telling the administrator, in an interview on Monday.

They settled on a compromise punishment: three days without internet.

Nearly two decades after he lost his access to the internet, Mr. Kaminsky wound up saving it. What Mr. Kaminsky discovered in 2008 was a problem with the internet's basic address system, known as the Domain Name System, or DNS, a dynamic phone book that converts human-friendly web addresses like NYTimes.com and Google.com into their machine-friendly numeric counterparts. He found a way that thieves or spies could covertly manipulate DNS traffic so that a person typing the website for a bank would instead be redirected to an impostor site that could steal the user's account number and password.

Mr. Kaminsky's first call was to Paul Vixie, a longtime steward of the internet's DNS system. The usually unflappable Mr. Vixie recalled that his panic grew as he listened to Mr. Kaminsky's explanation.

"I realized we were looking down the gun barrel of history," Mr. Vixie recalled. "It meant everything in the digital universe was going to have to get patched."

Mr. Kaminsky spoke at the annual Black Hat convention on hacking in Las Vegas in 2008. Jae C. Hong/Associated Press

Mr. Vixie asked Mr. Kaminsky if he had a fix in mind. “He said, ‘We are going to get all the makers of DNS software to coordinate a fix, implement it at the same time and keep it a secret until I present my findings at Black Hat,’” Mr. Vixie said, referring to an annual hacking conference in Las Vegas.

Mr. Kaminsky, then the director of penetration testing at IOActive, a security firm based in Seattle, had developed a close working relationship with Microsoft. He and Mr. Vixie persuaded Microsoft to host a secret convention of the world’s senior cybersecurity experts.

“I remember calling people and telling them, ‘I’m not at liberty to tell you what it is, but there’s this thing and you will need to get on a plane and meet us in this room at Microsoft on such-and-such date,’” Mr. Vixie said.

Over several days they cobbled together a solution in stealth, a fix that Mr. Vixie compared to dog excrement. But given the threat of internet apocalypse, he recalled it as being the best dog excrement “we could have ever come up with.”

By the time Mr. Kaminsky took the stage at Black Hat that August, the web had been spared. Mr. Kaminsky, who typically donned a T-shirt, shorts and flip flops, appeared onstage in a suit that his mother had bought for him. She had also requested that he wear closed-toed shoes. He complied, sort of — twirling onto the stage in roller skates.

When his talk was complete, Mr. Kaminsky was approached by a stranger in the crowd. It was the administrator who had kicked Mr. Kaminsky off the internet years earlier. Now he wanted to thank Mr. Kaminsky and to ask for an introduction to “the meanest mother he ever met.”

Daniel Kaminsky was born in San Francisco on Feb. 7, 1979. His mother, now retired, was the chief executive of a medical company. His father, Marshall Kaminsky, is a retired accountant in Chicago. (The parents’ marriage ended in divorce.) His stepfather, Randy Howell, was a data engineer consultant for the computer security software company McAfee, based in Santa Clara.

Daniel attended St. Ignatius High School in San Francisco and Santa Clara University and afterward worked for the tech companies Cisco and Avaya in addition to IOActive.

While the DNS fix was Mr. Kaminsky’s most celebrated contribution to internet security, it was hardly his only one. In 2005, after researchers discovered Sony BMG was covertly installing software on PCs to combat music piracy, Sony executives played down the move. Mr. Kaminsky forced the issue into public awareness after discovering that Sony’s software had infected more than 568,000 computers.

“He did things because they were the right thing to do, not because they would elicit financial gain,” his mother, Mrs. Maurer, said.

(When a reporter asked Mr. Kaminsky why he did not exploit the DNS flaw to become immensely wealthy, he said that doing so would have been morally wrong, and that he did not want his mother to have to visit him in prison.)

Silicon Valley’s giants sought Mr. Kaminsky’s expertise and often tried to recruit him with lucrative offers to serve as their chief information security officer. He politely declined, preferring the quiet yeoman’s work of internet security.

Mr. Kaminsky in 2005. “He did things because they were the right thing to do, not because they would elicit financial gain,” his mother said. Kevin P. Casey for The New York Times

In a community known for its biting, sometimes misogynistic discourse on Twitter, Mr. Kaminsky stood out for his empathy. He disdained Twitter pile-ons and served as a mentor to journalists and aspiring hackers. He would often foot a hotel or travel bill to Black Hat for those who could not afford it. When one protégé broke up with her boyfriend, Mr. Kaminsky bought her a plane ticket to go see the young man, believing they were meant to be. (They married.)

He was outspoken when privacy and security were on the line. After the F.B.I. tried to force Apple, in federal court, to weaken the encryption of its iPhones in 2015, James B. Comey, who was then the F.B.I. director, testified to Congress in 2016 that he was not asking for a backdoor, but for Apple to “take the vicious guard dog away and let us pick the lock.”

“I am that vicious guard dog, and that used to be a compliment,” Mr. Kaminsky told The New York Times at the time. “The question for Mr. Comey is: What is the policy of the United States right now? Is it to make things more secure or to make them less secure?”

The Electronic Frontier Foundation, a group that promotes civil liberties, said in a tweet on Saturday that Mr. Kaminsky had been a “friend of freedom and embodiment of the true hacker spirit.” Jeff Moss, the founder of the DefCon and Black Hat hacking conferences, suggested that Mr. Kaminsky be inducted into the Internet Hall of Fame.

Mr. Kaminsky’s generosity extended to his many side projects. When a friend struggled with color blindness, he developed the DanKam, a mobile app that uses a phone’s camera to decipher colors otherwise indecipherable to the colorblind. When his grandmother Raia Maurer, now 97, experienced hearing loss, he refocused his efforts on hearing-aid technology.

And when his aunt, a dermatologist, told him that she could no longer treat under-resourced patients for AIDS-related skin diseases in sub-Saharan Africa and Rohingya refugee camps, Mr. Kaminsky helped develop telemedicine tools for the National Institutes of Health and AMPATH, a health project led by Indiana University that he sought to bring to San Francisco during the coronavirus pandemic.

In addition to his mother, father and grandmother, Mr. Kaminsky is survived by his sister, Angie Roberts, and his stepfather.

Security was always Mr. Kaminsky’s lifework, most recently as the chief scientist at White Ops, a security company he helped found; it was recently renamed HUMAN. He was not above criticizing his own industry. In a 2016 keynote address at Black Hat, he said the industry had fallen far short of expectations. “Everybody looks busy, but the house still burns,” he said, before pitching the cyber equivalent of the Manhattan Project.

“The internet was never designed to be secure,” Mr. Kaminsky recalled in a 2016 interview. “The internet was designed to move pictures of cats. We are very good at moving pictures of cats.” But, he added: “We didn’t think you’d be moving trillions of dollars onto this. What are we going to do? And here’s the answer: Some of us got to go out and fix it.”