GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Scott Moss
January 4, 2001

Kevin Mitnick: Criminal or Conspiracy Victim?

Kevin Mitnick is arguably the most famous hacker in history. Kevin said his fascination with technology began at age 11 when he swept the floors and did inventory at Radio Shack in exchange for getting to tinker with their HAM radios. "I always carried my HAM radio with me," he said. "I wasn't much into social relationships. As a kid, I was overweight. I didn't make friends easy and one of the ways I could talk to people was over the radio. Even today, I still use HAM radio." Kevin began his hacker habits when he was a teenager, and his skills gained vigor during his days at Pierce College. For the next 15 years, Kevin would break into computers and curiously snoop around and steal information. He never did an extreme amount of damage, but people noticed his visitations and tried to stop him. This only made Kevin vengeful and he took actions such as tampering with victim's phone service, electronic mail, credit records, and job records. Kevin never stopped even though he was arrested for digital trespassing five times. Kevin's obsessive breaking and entering made him a legend, both in the underground world of hackers and in the headlines of The New York Times. New York Times reporter John Markoff followed Kevin's every move and featured Kevin in a book called *Cyberpunk* in which Kevin was one of the main characters. Markoff then wrote a front-page story for the *Times* on July 4, 1994 that portrayed Kevin as a superhacker who could wreak cyberhavoc if not caught.

Kevin has an uncanny ability to hack any system. From a military computer to FBI and DMV records, Kevin could weasel his way into nearly any network's core according to an article on the Daily News website. Kevin was technically dull, for he achieved most of his conquests through superb social engineering, "imitating a lineman's jargon, impersonating a superior, sifting through trash, conning unsuspecting employees out of their field manuals, exploiting his knowledge of a phone company's organizational chart." With all this mischief, Kevin turned into the FBI's most-wanted hacker. He was recently released from prison after serving four years for the crime of illegally copying proprietary software belonging to major companies including Motorola, Nokia and Sun. Kevin and his numerous supporters claim he has been set up to be an example of the harsh punishment hackers would receive. The majority of the populace at the time believe the sentence to be fair but Kevin and his loyal supporters believe the case was a conspiracy.

Kevin Mitnick vs. Tsutomu Shimomura

When Kevin was on the run for his illegal activity from the FBI, he made the mistake of angering a fellow cyber-genius, Tsutomu Shimomura, which allowed him to be caught. The following passage is taken from *Wired* magazine, which sets up the series of events that lead to the chase and capture of Kevin:

"Several years ago, Kevin cleverly figured out that if he could hack cellular phones

© SANS Institute 2000 - 2005 Author retains full rights.

with the same ease as ordinary phones, he could start from a mobile handset and thread his labyrinthine way to any computer in the world, virtually untraceably. Since he didn't do code, he needed to find someone who did; someone who had custom, turbocharged cellular phone software, and then social-engineer the goods away from him or her. After several unsuccessful attempts to con code from some likely candidates, Kevin eventually targeted Tsutomu Shimomura as the guy with the tools. It was a bold move, because Shimomura was a respected security expert and a character almost as complex as Kevin. A 30-year-old science geek, Shimomura was also a Japanese citizen, a ski bum, a longhaired computational physicist, and a hacker himself. But unlike Kevin, every time Shimomura's explorations uncovered security holes, he reported them to security authorities, not to hackers. On Christmas Day of 1994, Kevin launched a sophisticated "IP spoofing attack" against Tsutomu Shimomura's computers in San Diego. The attack was launched from toad.com in San Francisco, the Toad Hall computer owned by John Gilmore, a founding employee of Sun Microsystems. When Shimomura notice someone had attacked his computers, he took it as a personal challenge to find out who it was. When the trail led to Kevin, Shimomura became a cybersleuth, on a mission to catch him. Shimomura's pursuit of the hacker led to computers in Marin County where Shimomura's stolen files were found on the Well, Denver, San Jose and finally to Kevin Mitnick, the fugitive hacker, in Raleigh, North Carolina."

After a famous intensive two-week electronic manhunt, law enforcement agents closed in on Kevin's apartment in Raleigh, North Carolina on February 15, 1995. Under a plea bargain, Kevin pleaded guilty to various computer crimes and was sentenced to 68 months in jail and ordered to pay $4,525 in restitution and assessments.

Possible Conspiracy?

Kevin said the government claims that he caused companies hundreds of millions of dollars in damage were based on the costs of research and development for the software he downloaded. He insists this is not true. The consensus of Kevin and his supporters believe "the U.S. Government has grossly exaggerated and continues to exaggerate the 'losses' caused by Mr. Mitnick's alleged computer hacking and copying of source code." The government has stated that the losses in his case are in excess of $80 million dollars for Motorola, Fujitsu Nokia, Sun, Novell, and NEC. Kevin believes the government is alleging fictitious losses in his case to make an example out of him.

The most important condition of the alleged conspiracy is that none of the companies ever reported any material losses to their stockholders or the SEC. These entities are considered 12-G corporations under SEC regulations and is required by law to report any material loss to their stockholders and to the SEC. Failure to report such loss violates federal law and can subject the entity to civil penalties and a lawsuit by their shareholders. The question that Kevin and his supporters want answered is if any losses have been reported to the SEC or the entity's shareholders of their losses. The government continues to refuse to release any evidence of the alleged losses by these companies to Mr. Mitnick or his attorney.

© SANS Institute 2000 - 2005 Author retains full rights.

Some speculators for Kevin claim a different conspiracy, which entails the reporter Markoff setting up Kevin for financial gain. They state that, "Markoff's friend, Tsutomu Shimomura, claimed that Kevin had hacked his home computer on Christmas Day, 1994, and went after him, with Markoff following. When Shimomura tracked Kevin down in North Carolina, Markoff was there for the kill. However, according to Dale Coddington and Brian Martin, both of whom were hired by the defense to comb through the 9 gigabytes of electronic evidence amassed against Kevin, there is no proof that Mitnick hacked Shimomura." Markoff and Shimomura shared a $750,000 advance to write a book called *Takedown*, which is a detailed account of the search and capture of Kevin. A movie based on the book is expected to be released soon.

The media coverage has also had a profound impact on Kevin's case. The following passage is from an article in *Forbes* focusing on Kevin's depiction to the world:

The media supposedly portrayed Mitnick as a "dark side" hacker intent on toppling civilization; a criminal who as a teenager penetrated computers at NORAD, inspiring the hit flick War Games; a phone phreaker who, just by whistling three tones into a telephone receiver, could launch World War III; and a computer hacker who, merely armed with a computer sans modem, could wreak cyberhavoc from his jail cell.

When asked in prison of the media and John Markoff's impact on his legal proceedings, Kevin had the following comments:

"Markoff has single-handedly created "The Myth of Kevin Mitnick," which everyone is using to advance their own agendas. I wasn't a hacker for the publicity. I never hacked for personal gain. If I was some unknown hacker, accused of copying programs from cell phone companies, I wouldn't be here. Markoff's printing false and defamatory material about me on the front page of The New York Times had a substantial effect on my case and reputation. He's the main reason I'm still in custody."

Supporters for Kevin

The supposed injustice of Kevin has rallied thousands of supporters. When in prison, he had his fans, who staged protests at federal courts around the country, sported "Free Kevin" bumper stickers and sent him letters of encouragement, magazines and money to buy items in the prison store. A standout event was on September 13, 1998, when hackers identifying themselves as HFG ("Hacking For Girlies"), hacked into the New York Times website explaining Kevin's plight. When asked his thoughts on this event and other hacks done in his name, Kevin had the following comments:

"I don't condone anyone causing damage in my name, or doing anything malicious in support of my plight. There are more productive ways to help me. As a hacker myself, I never

© SANS Institute 2000 - 2005 Author retains full rights.

intentionally damaged anything."

New websites are also popping up everywhere on the Internet in support for Kevin's freedom. Many of these sites offer conspiracy theories of the government against Kevin and procedures for new Kevin supporters on how to get involved.

What Kevin Says About Himself

"I broke into computers for the fun, the thrill and the intellectual challenge fed my ego. That's one of the reasons I did it -- for the ego boost. It made me feel good."

The threat of a cyber-genius out causing havoc on all the world's computer systems creates a persona that people naturally fear and call strange. When asked how he would describe himself, Kevin states, "When I read about myself in the media even I don't recognize me. The myth of Kevin Mitnick is much more interesting than the reality of Kevin Mitnick. If they told the reality, no one would care." Kevin also addressed his attacks on government systems and how he handled sensitive information: "…I never attempted to access anything considered to be classified government systems."

In an interview from *Forbes,* Kevin addressed his ambition for hacking. He says that he is not an addict and is not tempted to hack anymore.

"It's weird. I've kind of grown out of it. I'm not saying prison rehabilitated me. That's a crock. All prison is is punishment. I'm 36 years old now. Hackers tend to grow out of it in their early 30s."

What Kevin is Doing Now

Just several months out of prison, Kevin insists he's kicked his hacking addiction and wants to help rid the world of digital criminals. He states, "I'll never intentionally violate the law…I'm trying to use my background and expertise in helping others prevent computer break-ins." This will prove difficult, however, since Kevin is barred from touching computers as part of his probation.

"The requirements mandating I can't touch a computer or cell or cordless phone are akin to telling a forger not to use a pen or paper. There is no way I can earn a living when I get out. I couldn't even work at McDonald's. All I could do is something like gardening."

Even though he is prohibited from operating computers, he has job offers ranging in a broad spectrum as an online columnist for the e-business venture "Contentville", a job as the host of a Los Angeles radio talk show and as a consultant for a cyber-crime movie. Even the television show "America's Most Wanted" asked him to appear as an expert on computer hacking. He was also paid to write an article for Time magazine. Eventually he wants to become

© SANS Institute 2000 - 2005 Author retains full rights.

an independent computer security consultant. However, Kevin won't be allowed to travel outside the Southern California area or touch a computer until his probation ends in 2003.

"Kevin Mitnick is a recreational hacker with a compulsive-obsessive relationship to information" states a columnist for *Wired*. "He hoarded information, never sold it, and wouldn't even share it with his friends." It seems that Kevin Mitnick is not the dangerous cyber-criminal the media portrayed him to be, but only time will tell.

Works Cited

Andersen, Troy. "Mitnick Wants to Save Others From Hackers." Daily News. 3 July 2000. URL: http://www.dailynews.com/archives/2000/07/03/new02.asp (2 January 2001).

Gulker, Chris. "The Kevin Mitnick/Tsutomu Shimomura affair." Random Access. 21 Jan 2000. URL: http://www.gulker.com/ra/hack/ (2 January 2001).

Penenberg, Adam L. "Mitnick Speaks!" Forbes. 5 April 1999. URL: http://www.forbes.com/1999/04/05/feat.html;$sessionid$1YCF41YAACMTJQFIAGWCFFA (2 January 2001).

Shimomura, Tsutomu. "Catching Kevin." *Wired*. 4.02 Febuary 1996.

Unkown. "Kevin Mitnick Commentary." Kevin Mitnick Website. URL: http://www.kevinmitnick.com/cory.html (28 December 2000).

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.