Profiling a Hacker

In 1990, Kevin Poulsen took over all the telephone lines going into a Los Angeles radio station to win an automobile in a call-in contest. In 1999, David Smith launched the Melissa Worm that caused more than $80 million dollars worth of damage to businesses. What do these people and millions more have in common? They are all hackers.

According to William Tafoya, professor in the national security graduate program at the University of New Haven, cyber-crime profiling is defined as “the investigation, analysis, assessment and reconstruction of data from a behavioral or psychological perspective extracted from computer systems, networks and the humans committing the crimes.” Profiling a hacker is both valuable and dangerous. Identifying a range of characteristics such as motivations and skills, knowledge, resources and access can be very useful in profiling a hacker. The danger is that people will rely on the average profile of a hacker to try and determine an identity. Knowing the motivations of hackers provides assistance in understanding their behaviors and thus can help companies protect their networks better. Identifying the common and unique characteristics of hackers can provide you valuable information that can be used to safeguard your system and further increase your knowledge and forensic practices. It is very important to try to profile a hacker because companies are losing large amounts of money because of security breaches. In 1998, the Computer Security Institute estimated that intrusions cost
corporations $236 million in damage (Marcus Rogers, Wired News, 01/20/99). A big problem today though is that there are many different kinds of hackers; some good, some bad, some curious, and some malicious.

Before the age of computers and hackers, a hacker was simply defined as someone who made furniture with an axe. That is not the case today. There are many definitions of a hacker but they are commonly defined as people who enjoy exploring the details of programmable systems and how to stretch their capabilities, as opposed to a normal user, who would rather learn only the minimum necessary. A hacker is consumed with curiosity of anything technical and share the belief that things only have meaning if people know how they work and operate. Hackers tend to consider themselves something of an elite status; a meritocracy based on one’s ability. There is a certain ego satisfaction to identify yourself as a hacker, but if you claim to a hacker and are not, you will more than likely be labeled as a fake. Your role or status in the “hacker community” depends on how good your abilities are. Hackers normally think of themselves as a group of information seekers who are adept at exploring computer systems and networks. Even though hacking into these systems is illegal, hackers find it to be ethically acceptable as long as he or she does not commit theft, vandalism or breach any confidentiality. This is also called the hacker code of ethics that was developed by traditional hackers of the 1970’s. Hackers also believe that all information should be available to everyone and that things should be allowed to be improved and made perfect. A lot of times hackers think their responsibility is to hack into these systems to find security holes so that the systems administrators can patch up these holes. Hackers place a high value on freedom of inquiry and hostility towards secrecy. They view
information-sharing as both an ideal and a practical strategy. Conversely, there are hackers that do not follow the so-called code of ethics. These hackers break into systems with the intention to cause damage. These types of hackers are known as crackers. This title was created to separate the ethical hackers from the unethical hackers. Crackers, most times, lack the skills and abilities of hackers, but are still considered a major threat because of their reckless use of very powerful software. Most of today’s hackers fall into one of three categories; black hat, grey hat or a white hat hackers. A black hat hacker does not use a code of ethics and uses his abilities strictly for immoral purposes. A grey hat hacker is one with unclear ethics and borderline legality. White hat hackers are the ones that follow a code of ethics and try to help security administrators repair the holes they may have in their system. They accomplish this by leaving notes behind after having breached the security boundaries to assist the administrators address the problem(s). These kinds of hackers perform the task as “bugspotters.” The fact that hackers are able to penetrate computer systems magnifies software weaknesses.

Hackers have many different patterns of behavior. They act quickly and precisely to make their activities harder to detect. They stick around until noticed and make few or no mistakes. Using hidden software such as Trojan horse, they leave back doors open for re-entry to a system.

A number of hackers underachieve in school. This is usually blamed on the teachers not catering to their interests. One hacker, who goes by the alias “mosthated,” says “A lot of people drop out because there’s really nothing you can learn in school. They only had two computer classes being taught at my school.” The hackers that do stay in school are usually near the top of the class in academics.
Marcus Rogers, an associate professor at Purdue University who has a doctorate in forensic psychology and worked as a detective in a computer crimes unit in Canada, has developed his own “Hacker Taxonomy.” He has identified eight different types of cyber-criminals, separated by their skill levels and motivations. The types are novice, cyber-punks, internals such as disgruntled or ex-employees and petty thieves, coders, old guard hackers, professional criminals and cyber-terrorists. The novice type has limited computer and programming skills and look for the media’s attention. Cyber-punks are capable of writing their own software and often brag about what they did. A disgruntled or ex-employee poses the largest security problem because of the knowledge of the system they possess. Petty thieves are motivated by greed or necessity to pay off addictions such as drugs or gambling. Coders are dangerous because they have hidden agendas and are motivated by a sense of power and prestige. Old guard hackers appear to have no criminal intent but have very little respect for personal property. Professional criminals are basically guns for hire. They are highly motivated, highly trained and have access to high-tech equipment. Finally, cyber-terrorists are well-funded and often engage in hacktivism, which is the utilization of technology to announce a political message (Ann Bednarz, Network world, 2004).

There are many different motivational factors for hackers. Motivations among today’s hackers range from money to gaining peer acceptance. According to Marcus Rogers, most computer criminals are motivated by status, money, or revenge. Max Kilger has developed a motivation profile for hackers that he calls MEECES, standing for money, ego, entertainment, cause, entrance into social groups and status. These are the reasons why Mr. Kilger thinks people hack. For many hackers, it’s an addiction. They
become obsessed and can spend hours upon hours each day dedicated to the pursuit of access of information. Steven Branigan, president of security company CyanLine, states that “My experience has been that those who get into computers first, and then start hacking, are more motivated by curiosity. Those who have criminal tendencies to begin with, when they learn about using computers, simply apply that to their trade.” He also adds that “The people I’ve found to be the most dangerous are the ones seeking revenge.”

People have many preconceived notions about what hackers look and act like. Marcus Rogers believes that the most common computer cracker is an obsessive middle-class white male, between the ages of 12 and 28, with few social skills and a potential history of physical and sexual abuse (Wired News, 1999). Donn Parker, Max Kilger, Terry Gudaitis, Marcus Rogers and Eric Shaw have come up with their responses to seven common myths about criminal hackers:

1. Computer criminals are motivated by greed or achieving a high standard of living. “These people are motivated by a huge range of factors, but generally, on average, they are motivated by intense personal problems and not by greed or high living.” –Donn Parker

2. Computer criminals don’t like to talk. “Among 200 convicts that I interviewed, most of them told me they were willing to cooperate with me because they were willing to do whatever they could to keep other people from getting into the situation they were in.” –Donn Parker

3. The hacker culture is chaotic, with no clear hierarchy or social controls. “It just looks like chaos to people, but if you look behind it with a trained eye of a social scientist, the social structure is very clear, very strong and very organized. It’s a meritocracy.” –Max Kilger

4. Hackers are all young males who drink too much Mountain Dew and eat too much pizza. “The more dangerous hackers are more sophisticated, older, insiders at a company and may be involved in organized crime.” –Terry Gudaitis

5. Computer criminals tend to be better educated. “A recent study of computer crime in Canada during the last five years suggests no socio-demographic differences between people found guilty of computer crimes and those convicted
of similar offenses, such as assault and burglary. That includes education levels.”
–Marcus Rogers

6. Computer criminals lack social skills. “The same study of 132 Canadian criminals found no significant difference between the number of convicts who were married or single.” “Their marital status indicates they may not be as socially dysfunctional as we thought.” –Marcus Rogers

7. The threat from insider and outsider attacks is very different, and information security professionals should plan accordingly. “In fact, many insiders want to make their attacks look like outside hacks to protect their identity. They may also seek outsiders to work through. Many outside hackers operate in “tribes” based on shared interests and professional and personal background. Through these groups, outside hackers may have access to insiders to aid them in their attacks.”
–Eric Shaw

A hacker myth that I found amusing was that hackers dream not of scoring on prom night but of getting to the finals of the General Electric Science Fair competition. Basically, hackers can be anyone, from the adolescent joy rider who gets thrills from outsmarting the adults of the world to the very disturbed person determined to use other people’s computer systems for his own malicious purposes. Some hackers try to disrupt an organization’s operations as a way to bring society to its knees. Other hacker’s objectives are to steal money or seek revenge on a former employer.

Hackers can be any age. They can look and act like an everyday person would. The number of computer criminals successfully captured and prosecuted is very low. This is in large part due to people’s failure to report the crimes. The main goal is that people should never, ever underestimate the creativity and the ability of any of the computer criminals in the world. We need to stop stereotyping hackers as nerds who don’t leave their houses because of their supposed lack of social skills. Hackers cost businesses and corporations millions of dollars every year. It is imperative that we make
a general profile of a hacker in order to cut down on the financial losses of the companies and make them safer as a whole.
References:

Network World

Http://infosecuritymag.techtarget.com/articles/june01/features_hacker_psychology.shtml

Http://www.wired.com/news/technology/0,1282,17427,00.html


Http://en.wikipedia.org/wiki/Hacker_culture

Http://feed.proteinos.com/item/453

Http://en.wikipedia.org/wiki/Hacker_ethic

Http://www.stanford.edu/~aafurman/PWR2/classifications.htm

Http://en.wikipedia.org/wiki/Hacker_definition_controversy

Http://www.pbs.org/newshour/bb/cyberspace/jan-june98/hacker_profile.html