

The Changing Face of Computer Crime

By Ira Winkler

The Early Days

I remember meeting someone at a HOPE (Hackers on Planet Earth) conference in New York City about seven years ago. We got into a "discussion" about some nebulous point, and parted ways. A few months later, I received an e-mail message through an anonymous e-mail from someone claiming to be a criminal hacker and telling me that my first book, *Corporate Espionage*, and many of my articles helped him to hone his criminal skills. I exchanged a couple of e-mails and soon realized that this was the person I met at HOPE.

Back then, it was no surprise that I would meet a criminal at a HOPE conference. The fact of the matter is that since the early 1980s, there have been computer hackers who live off their criminal actions. I don't think that anyone actually started out to be a criminal when they started hacking. Before computers were widespread, there was little information available to anyone wanting to learn about computers. Computers had little documentation, and there were definitely no library books that could be used as a reference for legitimately interested people.

These people did break into computers, looked around, and likely committed a variety of criminal acts. Most of the crimes were benign. Some of them malicious. Inevitably, many of these

hackers found ways to make money off of their actions. Their professionalism varied, though. Their profitability varied by their actions. The majority of these criminals did things like break into credit reporting agencies and other information stores to steal information for unscrupulous private investigators. The more professional criminals were able to break into banks and align themselves with more established criminal organizations. These people were smart enough to keep their egos in check and quietly commit their acts without getting caught.

Script Kiddies

Over time, computers began to proliferate, as did computer criminals. At this point though, information about computers was readily available. People who wanted to learn about computers only had to go to the library or the Internet. Information about how to break into computers and commit other computer crimes was now easy to get. Programs or scripts for breaking into computers were widely available, and people needed no actual skills to break into computers. They just needed the scripts, which is where the term script kiddies came from.

These script kiddies were mostly known for their malicious acts, such as vandalizing Web sites. Their actions seemed legendary, however the legendary acts were more a result a negligence on the part of the victim than any skills of the attackers. While almost all of the crimes involved ego, some script kiddies started committing their acts for profit. Again, it takes little skill to break into poorly protected computers for any reason.

There were always people who performed criminal acts, however they were generally a relatively small group compared to the general number of computer users, and the losses were small compared to other crimes in general.

Electronic Theft

Over time though, organized criminals started experimenting with electronic theft. By 1997, General Marsh, who was then chairman of the President's Commission on Critical Infrastructure Protection, stated that banks lose billions a year due to electronic theft, aka computer hacking. Those losses seem staggering, but they are relatively small to the financial sector as a whole. Computer crime was an established method for doing business.

Soon after that, we started seeing extortion against large financial institutions around the world. It is likely that many of these crimes were committed by organized crime rings of various sizes, due to the ability of the organizations to effectively launder the money. It is important to remember that the hard part of stealing money from a bank is not stealing it, but laundering it.

Some of the mentioned crimes were likely committed by "hackers" who turned professional criminal. The ability to launder the money was the key factor for those who were able to get away with major thefts and extortion attempts.

At the same time, there were a variety of people using IRC and other online resources to buy, sell and trade credit card information, as well as other items of information we now associate with identity thefts. Generally, this wasn't widespread.

Spamming and Phishing

Also during this time, spam began to grow on the Internet. By this point, I believe that spammers are worse than other computer criminals.

Spammers became the most aggressive in studying computer technologies and ways to abuse them. They refined their techniques to cover their tracks, and ironically were met with more aggressive countermeasures and tactics than typical computer criminals were. That is because organizations like AOL and Microsoft started going after them.

The profit for spam continued to grow. Prosecution was extremely rare, so spammers flourished. At the same time, the more technically savvy computer criminals began to experiment with combining spams with fraud. When I interviewed Alexei Ivanov, a member of an early Russian cybercartel, for my book, *Spies Among Us*, he mentioned that in the early 2000s, he experimented by searching eBay for likely PayPal account holders, and he sent a spam to 150 people offering them \$50 to go to a site to fill out a survey. 125 people provided him with the information requested.

More people decided to experiment with this, and now phishing attacks are rampant. The first phishing scams were clearly amateurish, containing poor grammar and other clear signs that the message wasn't actually from the claimed sender. Within two years, the phishing messages looked better than legitimate messages from the organizations.

The increased success of phishing, combined with the proliferation of Web sites that incompetently secure credit card numbers and the resulting hacking, created a tremendous increase in the profit potential for online crime. Organized crime started to step in to take their piece.

Rampant Crime

As this knowledge proliferated into the former Soviet Union, even computer-savvy people who were otherwise law-abiding citizens started forming their cybercartels. They specialize in crimes involving identity theft and cyberextortion. The lack of laws criminalizing these actions helped protect and encourage these actions.

As a result of how rampant these crimes have become, these computer criminals have set up an infrastructure to support their activities. There are now sites that facilitate the sale and barter of stolen identities and credit card information. Other sites facilitate the phishing and cyberextortion attacks by renting out zombie networks, aka botnets.

E-commerce and PC proliferation have made the crimes widespread. The fact of the matter is that this is just an evolution of crime, not the revolution that people believe. As my friend from the HOPE conference demonstrated a long time ago, there is always a criminal willing to use computers for criminal purposes. We are now entering an age where we are facilitating many more criminals, as well as victims.

Addressing the Problem

I tend to sound like a broken record when I say that the success of the criminals does not depend on their technical abilities, but the lack of technical abilities on the part of their victims. A frequent quote from Scott Charney during his tenure as Section Chief of the Department of Justice's Computer Crime and Intellectual Property Unit was, "At any point in time 3% of the general population will commit a crime given the opportunity." I am not that cynical, and think that the percentage is much smaller. Either way, even if only .1% of Internet users are willing to commit crimes, that is still a really large number of people.

The fact is that we have to make it more difficult to commit crimes. Poorly protected e-commerce sites give people opportunity. Ivanov used Google to find thousands of potentially vulnerable systems with very simple searches. That is how easy it is for criminals to commit identity theft and some forms of cyberextortion. Sites that adhere to a variety of

standards, such as Visa and Mastercard's new security standard, tend to be more difficult to compromise.

There are also a variety of third parties that are even more useful to criminals. These people are those who house zombie computers. While some ISPs have an unstated policy that they will cut off zombies from their network, ISPs generally claim that they are not responsible for policing systems on their network and allow attacks to continue unabated. If this occurred in the physical world, the terms reckless endangerment and aiding and abetting would be used in criminal charges. ISPs are in a unique position to cut off attacks at the enabling systems, but tend to refuse to do so.


Denial of service traffic is pretty easy to identify. Unfortunately, it falls to the people who host the victim Web sites to absorb the attack. That's too late, and the providers tend to drop the victims as customers. Making prevention a part of the infrastructure is the only way to be proactive to attacks.

Likewise spam, which enables phishing and other crimes related to identity theft, can be stopped by ISPs. An individual sending out hundreds or thousands of messages a minute is easy to spot and stop at the source.

The above solutions do not mean we can accept basic incompetence on the part of users and administrators in protecting their own systems. Everyone responsible for a computer system is a potential enabler for criminal acts.

Summary

So to sum it up best, the face of computer crime has not changed much. Computer crime is growing and will continue to grow. As Willy Sutton said about 100 years ago when asked why he robs banks, "That's where the money is." Today computers and the Internet are where the money is. Not only that, it is easy money. We have to accept that and act upon it.

Computer criminals, as all criminals, are opportunists who cross the criminal line where other people won't. They might have more technical skill than their victims, but that isn't required. The more skilled people will likely get away with just about all of their crimes, but the sad fact is that even the most inept criminals are getting away with more because of sheer volume. 

Ira Winkler, CISSP, CISM, is president of the Internet Security Advisors Group. He has held a variety of positions in the industry, including performing an array of functions within the National Security Agency and supporting a mix of other intelligence and defense agencies in the US and throughout the world. He is also author of the new book, Spies Among Us.