THE POLICE HOW-TO GUIDES

HOW TO INVESTIGATE CYBERCRIME

by David Griffith
POLICE MAGAZINE

www.PoliceMag.com

HOW TO INVESTIGATE CYBERCRIME

Tracking bad guys on the Net takes the experience of a detective and the know-how of a tech head

Back when the term “computer” meant mainframes and reel-to-reel tape drives, computer criminals were masterminds who used their programming talents to glean millions of dollars from banks and corporations. These crooks were so ingenious in their schemes that many banks and corporations cut deals to hire them as security consultants rather than send them to prison.

Today, the average desktop workstation has all the computing power of one of those old mainframes, the average American home has at least one computer, and computer criminals are no longer masterminds, just crooks and creeps doing what crooks and creeps do. Today and every day, thousands of people worldwide are being victimized by computer crime. That’s why just about every major municipal or county law enforcement agency in the United States now has a new breed of detective: the computer crime or “cybercrime” investigator.

It’s easy to pinpoint the reason why cybercrime has statistically exploded since the mid-1990s. Just about every computer on Earth is now connected via a once obscure research tool called the Internet. Once derided as a passing fad and the CB radio of the ‘90s, the Internet and its graphic component the Worldwide Web have become so prevalent since 1995 that they have altered almost all fields of human endeavor, including crime.

If it were possible to murder someone by sending computer code across the Internet, people would do it. After all, they commit just about every other type of crime via the computer. Name a form of theft, fraud, or exploitation, and it is probably now being perpetrated or abetted by computer. The computer crime hit parade includes distribution of child pornography, credit card fraud, industrial espionage, harassment, breaking and entering (hacking), solicitation of prostitution, conspiracy, child molestation (“traveler” cases), malicious mischief, and property destruction (viruses), and that barely scratches the surface.

THE POLICE HOW-TO GUIDES

HOW TO INVESTIGATE CYBERCRIME

"I can teach a good detective how to investigate computer crime much faster than I can teach a computer guy to become a good detective"

So the need for cybercrime investigators is indisputable. But how do you go about transforming yourself into a cybersleuth?

Getting Started

Contrary to public perception, most cybercrime investigators are not propeller head geeks who spend all of their time on the Net, nor are they black-suited guys in sunglasses whose first name seems to be "special" and last name "agent." A lot of the best cybercrime investigators are just local detectives who have branched into a new field.

Slomo Koenig, a detective with the Rockland County (N.Y.) Sheriff's Department, has been working as a cybersleuth and computer forensics expert since 1997, and he believes any experienced investigator who is not afraid of technology can become an excellent computer crimes detective.

"I can teach a good detective how to investigate computer crime much faster than I can teach a computer guy to become a good detective," explains Koenig. "If you already have good investigative skills, then all I have to teach you is what is considered evidence in the digital world, how you can contaminate that evidence, and how you preserve that evidence. But if you don't understand what evidence is or how to go about conducting an investigation, then that makes the job a lot harder."

Koenig's comment shouldn't be construed as a license for detectives without special training to start working cybercrimes. There are some basic skill sets you will need before you can start chasing evildoers on the Internet.

"You have to have a thorough understanding of how the technology works," says Sgt. Ronald Levine of the Foothill-DeAnza College District Police Department in Los Altos Hills, Calif. "If an officer or deputy doesn't have computer skills, they're going to have to come up to speed and understand how the technology works before he or she can become an effective investigator," adds Levine, who has been involved in computer crime investigation since the early 1980s.

HOW TO INVESTIGATE CYBERCRIME

What most people, including many crooks and cops, don't know is that ISPs have records of everything a subscriber does on the Internet

Going After 'Em

The typical cybercrime investigation begins like most other investigations with a citizen complaint. Perhaps a local individual has been defrauded of several thousand dollars on an Internet auction site, and he or she contacts your agency.

Your first step in such an investigation is to find the Internet protocol (IP) address of the individual who defrauded the citizen who filed the complaint. An IP address is a series of numbers and letters that is attached to every piece of data that moves on the Internet. When the auction crook set up his or her auction, that code was registered with the auction company.

Big dot-com companies like Web auction sites have their own security specialists. So once you have identified the host of the auction site, you will probably work with the company's security people to gain access to the IP address of the Internet Service Provider (ISP) used by the person who set up the bad auction. They may cooperate fully, or you may need a subpoena, warrant, or court order just for the IP address.

Anyone who has an Internet account knows that the ISP is a subscription service that grants the user access to the Internet. What most people, including many crooks and cops, don't know is that ISPs have records of everything a subscriber does on the Internet.

That's the good news for investigators. The bad news is that the records are digital information with a very finite existence. In other words, if you're investigating a cybercrime involving the Internet, you better move fast.

How fast depends on the policy of the ISP in question. Large ISPs often keep their data for as much as 30 days, but that's not true in all cases. Data storage is a major cost center for ISPs, and some save money by dumping the data very quickly.

"Most agencies in the United States don't have anyone who is even remotely on top of what needs to be done to investigate these cases"

"There's no law that requires people to maintain the data," says Koenig. "Once we sent a subpoena to an ISP, requesting their records, and their answer was, 'Sorry. We only keep our records for 30 minutes.'"

Because ISPs would rather dump data than store it, Koenig says one of the most important weapons in a cybercrime investigator's arsenal is a letter requesting that the ISP preserve the data until the investigator can secure a subpoena, warrant, or court order requiring the ISP to turn over its records.

The preservation letter does not legally require the ISP to turn over its records. But many ISPs will cooperate with a request to preserve data.

Once you get the records from the ISP, you're probably in business. In order to subscribe to the service, the auction thief had to give personal information like his or her physical address. Yes, they can use false information and fake credit cards, but even that information can be valuable.

Here or There

When you have an address and a name for the suspect, your investigation is likely to involve another agency. Cybercrimes are not like in-person physical crimes. The victim is often in another state from the suspect. And that means you may work for the Dallas Police Department and suddenly need to serve a warrant in Reno.

Experienced cyber police say that jurisdictional disputes are rare occurrences during cybercrime cases and that other agencies are likely to cooperate with your investigation.

"Most agencies in the United States don't have anyone who is even remotely on top of what needs to be done to investigate these cases," says Det. Mark Kelly of the San Diego Sheriff's Department who serves on a multiagency cybercrime task force. "They're often glad to hear that we're going to take the case. We tell them, 'We have the expertise and we have the willingness to prosecute. All you have to do is take a report or serve a warrant.' Most of the agencies that we have worked with have no problem doing that."

Computer forensic specialists are the real computer experts among cybercrime investigators, and their work is extremely specialized

Bit by Bit

After a suspect's computer and various hard drives have been seized, it's time for the computer forensic specialists to go to work. These folks are the real computer experts among cybercrime investigators, and their work is extremely specialized. It's so specialized that many agencies that have cybercrime detectives farm out forensic examination to federal agencies or multiagency task forces.

Koenig says computer forensics is a matter of knowing what you're looking for and knowing how to find it. "People think we look at the entire hard drive, but it doesn't work that way. If you come to me and say, 'find everything on a computer,' I'll tell you that I'll retire before I complete that job. If you printed out every piece of data on a 120GB hard drive you'd have enough paper to fill up a football stadium with stacks 8 feet high and you'd still be printing."

For this reason, among others, Koenig cautions against computer "fishing expeditions." Such attempts at trolling for evidence are even more complicated by the fact that computer crime cases often involve multiple machines.

"We worked a school hack that involved 500 computers," says Koenig. "But we knew specifically what we were looking for and we seized only two computers."

Once the computers are in police custody, a forensic specialist makes what's called a "true copy" of its hard drive. A "true copy" is made by using software to create a bit-by-bit image of the drive. If the investigator merely made a standard copy of the drive through a backup program or by dragging and dropping the drive, the copy would not include deleted files, temporary files, and other normally superfluous data that could prove critical to the investigation.

"You can't do anything online without leaving a trail … on the Internet there's always a trail"

The true copy of the data can be examined using a number of computer forensics software programs. And while Koenig says these are essential tools for cybercrime investigators, he's not a big fan of what he calls "plug-and-play forensics," arguing that computer forensic examiners need to know much more about what they are doing than just how to use a software application.

This is one reason why many agencies and even cybercrime task forces send their forensics work to outside experts. Another reason is that computer forensics requires money for hardware.

For example, if you take down a child pornography ring selling high-res video and images, you're going to need a fast computer with lots of memory and imaging software to catalog all of the evidence. Also, you can't just have one type of computer. Your agency may have only Windows platform systems, but if you are investigating a credit card fraud suspect who uses a Macintosh, you're going to need a comparable Mac and Mac software to examine his or her hard drive.

Foreign Connections

Despite the challenges presented by cybercrime and a public perception that most computer criminals never get caught, cybercrime investigators say they have more success than people might think.

Koenig argues that Internet crime can sometimes be easier to track than actual physical crime. "If you take a false check into a bank and the security camera is not pointing at you when you pass it, then there's no trail to you. But you can't do anything online without leaving a trail. You can try to spoof that trail and make it harder for me to track you, but on the Internet there's always a trail," he explains.

Unfortunately, the Internet is a global communications system and often the trail of a cybercriminal leads to Russia, a former Soviet Republic, or to Africa. And that complicates an investigation.

But it doesn't make it impossible. Levine says many cases have been successfully prosecuted overseas, especially in Russia. "Russia has actually been very good at cooperating on cybercrime cases," he says.

Other overseas havens for cybercriminals have been less cooperative. "We are less likely to see cases come to successful resolution when they do end up in an African country or one of the former Soviet republics," Levine admits. "But we are seeing increased awareness and cooperation."

And that cooperation with Nigeria and Belarus may not be as critical as some people think. Koenig argues that the majority of cybercrime is really made in the U.S.A., regardless of the perpetrator's country code.

"The majority of the bandwidth is still in the United States," explains Koenig. "Let's say you want to set up a site that sells child porn. You can go to Kosovo or Belarus and hide from the law, but they have very few Internet connections, and what they do have is very expensive and not very fast. It's hard to hide like that and be in business."

Stone Walls

Because of help from foreign governments and because foreign investigations often curve back to the United States, an investigation that leads overseas is not a dead-end. But there are some cases that run smack into a stone wall.

Cybercrime investigators are understandably hesitant to tell people how to get away with criminal acts on the Internet. But they will divulge that the best way to get away with a computer crime is to be lucky enough to have the evidence of your act disappear.

"If the ISP logs are there, then 99 percent of the time I will get you"

"The only time I come up against a stone wall and have no place to go is when the ISP logs have expired," says Koenig. "But if the logs are there, then 99 percent of the time I will get you."

It is, of course, the other one percent of cases that fascinates the public and is the stuff of movies and TV. But do supersmart cybercriminals really exist?

Absolutely, says Kelly. "If a suspect is really smart and knows the Internet and knows the various ways around being identified, it makes it extremely difficult and, in some cases, impossible to catch him."

Kelly quickly adds, however, that such cases are extremely rare. "There are not that many people out there who are technically savvy enough to know the ins and outs of covering up the trail," he says.