



[Email this Document!](#)

Tracking a Computer Hacker

Daniel A. Morris
Assistant United States Attorney
Computer and Telecommunications Coordinator
District of Nebraska

A report written near the start of the Information Age warned that America's computers were at risk from hackers. It said that computers that "control [our] power delivery, communications, aviation and financial services [and] store vital information, from medical records to business plans, to criminal records," were vulnerable from many sources, including deliberate attack. "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." National Research Council, "Computers at Risk," 1991.

To see what computer hackers are doing today, take a look at www.attrition.org. This is one of the places on the Internet where hackers receive "credit" for their attacks. If the operator of this website verifies that a computer system has been invaded, a "mirror" of the damage, often a defaced web page, is posted on the website along with a link to the undamaged website. More importantly to the person or group claiming credit, the online nickname of the responsible hacker (HaXoBuGz, databoy and HACKWEISER being examples) is included next to the published description of the intrusion. This fleeting notoriety is what motivates many hackers. Other hackers cause even greater damage and try to avoid notice, much less notoriety.

Information about some of the Department of Justice's successes in prosecuting hackers can be found on the Department's website at www.cybercrime.gov. This site includes manuals for searching and seizing computers, policy statements, useful background material, and press releases regarding hacker prosecutions. It is one of the first places prosecutors should go when called upon to assist investigators looking into computer intrusions.

Hacker Tools Available Online

Some websites on the Internet provide both novice and expert computer hackers with programs, sometimes called "exploits," needed to conduct attacks. These sites may provide services to computer security experts and even advise hackers that they should not use the posted exploits to hack into another computer. Anybody, including some very destructive people, can download the hacker tools or "scripts" coded by experienced hackers, along with instructions for their use. See, e.g., <http://www.securityfocus.com> and its "bugtraq" service.

Hackers who find exploits on these websites may use them to do more than just deface webpages. Novices, sometimes referred to in hacker circles as "script-kiddies," who download hacker scripts may gain "root" access to a computer system, giving them the same power over a computer system as a trusted systems manager -- such as the power to create or delete files and e-mails and to modify security features.

Hackers who gain such unauthorized root access sometimes speak of this as "owning" the system they hack. If they want to cause damage they may do so immediately, or they may plant viruses or time bombs in a system. Sometimes they configure the system to work for them in later "denial of

services" attacks on other computers.

Some websites that post hacker tools also post known fixes, or patches. They advise systems administrators and network operators to download and install these patches so their systems will no longer be vulnerable to the listed attacks. But hackers know that, with persistence and help from other readily available computer programs, they can find computer systems vulnerable to the listed exploits. Hackers frequently launch their attacks against these unprotected systems.

It is commonly believed that many systems operators do not share information when they are victimized by hackers. They don't contact law enforcement officers when their computer systems are invaded, preferring instead to fix the damage and take action to keep hackers from gaining access again -- with as little public attention as possible.

Protected Computers

Federal law enforcement officers may be called in to track a hacker if the hacker gains unauthorized access to a Federal Government computer or to a computer system protected by federal law. Protected computers are any computer used in interstate or foreign commerce or communications, which includes any computer connected to the Internet. 18 U.S.C. § 1030(e)(2)(B).

Tracking a hacker may call for a combination of Internet research skills, subpoenas, court orders, search warrants, electronic surveillance and traditional investigative techniques. At least one Assistant United States Attorney (AUSA) in every district has been trained as a Computer and Telecommunications Coordinator (CTC) to assist law enforcement officers and other AUSAs in this effort. CTCs can obtain guidance from attorneys in the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS)(pronounced See-sips). CCIPS attorneys deal with these issues daily.

Clues of a Cybercrime

Clues to the identity of a hacker often exist in cyberspace and in the real world if the investigator knows where to look.

Computer systems of interest to hackers usually keep track of all authorized and unauthorized access attempts. Records, called computer logs, provide useful and often critical clues that a trained agent or computer specialist can use as the starting point to trace the route taken from computer to computer through the worldwide web, to discover the one computer out of the millions in the world from which an intrusion was conducted.

All computers using the Internet are assigned a different numeric Internet Protocol (IP) address while online, similar to country, city, street, and number addresses for houses. Unless the hacker alters the victim's logs once he or she gains unauthorized access, the victim's logs should list the precise computer address from which unauthorized access was gained. That address may not be the hacker's own computer, but instead another computer that the hacker has hijacked or an account that he owns on a third party's computer, as discussed in more detail below.

Lookup tools are available online to identify the owner of the network through which an attack was launched. To see how this works, see www.arin.net, operated by the American Registry of Internet Numbers.

Obstacles to Identifying the Hacker

Because of the make-up of the Internet, it is sometimes difficult for law enforcement officers to discover the identity of a hacker.

1. A hacker might hide or "spoof" his Internet Protocol (IP) address, or might intentionally bounce his communications through many intermediate computers scattered throughout the world before arriving at a target computer. The investigator must then identify all the bounce points to find the location of the hacker, but usually can only trace the hacker back one bounce point at a time. Subpoenas and court orders to each bounce point may be necessary to identify the hacker.
2. Some victims don't keep logs or don't discover a hacker's activities until it is too late to obtain records from the hacker's Internet Service Provider (ISP). A victim who has no record of the IP address of the computer from which unauthorized access was gained limits law enforcement officers to traditional investigative techniques, which alone may be inadequate to identify the hacker.
3. Some ISP's don't keep records or don't keep them long enough to be of help to law enforcement officers. As explained below, when the investigator determines the identity of an ISP from which records will be needed, the prosecutor should send a retention letter under 18 U.S.C. § 2703(f) requiring the ISP to preserve the records while a court order or other process is being obtained.
4. Some computer hackers alter the logs upon gaining unauthorized access, thereby hiding the evidence of their crimes.
5. Some leads go through foreign countries, not all of which consider hacking a crime. Treaties, conventions, and agreements are in place with some countries, and there are "24/7" contacts in dozens of countries around the world who can be contacted for help. When a lead points to a foreign country, the investigator should contact a CTC or CCIPS attorney.

Electronic Communications Privacy Act

Some of the information investigators need to track a hacker might be readily available to the general public on the Internet. No special restrictions apply to an investigator's access to and use of such information -- in the same way that information available in a public library can be used by investigators without special authorization. Common search engines such as www.dogpile.com, www.lycos.com, www.excite.com, or www.netscape.com may be used to find information about a username or nickname of the person or group claiming credit for a computer intrusion.

Other information, such as the content of e-mails, is available to law enforcement officers only if they comply with the provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-11. ECPA creates statutory rights for customers and subscribers of computer network service providers. The details of this Act are beyond the scope of this article, but an excellent guide to the Act is provided by CCIPS in print and on its webpage. See Computer Crime and Intellectual Property Section, Department of Justice, [Prosecuting Intellectual Property Crimes Manual](#).

Section 2703 of ECPA provides investigators with five mechanisms for compelling an Internet Service Provider to disclose information that might be useful in an investigation of a hacker.

The mechanisms, in ascending order of the threshold showing required, are described below:

1. Subpoenas can be used by an investigator to obtain basic subscriber information from an Internet Service Provider, including "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of such service and the types of service the subscriber or customer utilized." 18 U.S.C. § 2703(c)(1)(C).
2. Subpoenas also can be used to obtain opened e-mails, but only under certain conditions relating to notice to the subscriber. See 18 U.S.C. § 2703(b)(1)(B). Notice may be delayed under Section 2705 for successive 90-day periods. Subpoenas may be issued for e-mails that have been opened, but a search warrant is generally needed for unopened e-mails.

3. Court orders under 18 U.S.C. § 2703(d) can be obtained by investigators for account logs and transactional records. Such orders are available if the agent can provide "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.*

The government must offer facts, rather than conclusory statements, in an application for a 2703(d) order. A one to three-page factual summary usually is sufficient for this purpose. The standard for issuing such an order is not as high as for a search warrant.

4. Investigators who obtain a court order under 18 U.S.C. § 2703(d) can obtain the full contents of a subscriber's account (except for unopened e-mail stored with an ISP for 180 days or less and voice-mail), if the order complies with a notice provision in the statute. 18 U.S.C. § 2703(b)(1)(B)(ii) and (b)(2). Notice to the subscriber can be delayed for up to ninety days when notice would seriously jeopardize the investigation. 18 U.S.C. § 2705(a).

5. Search warrants obtained under Rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant can be used to obtain the full contents of an account, except for voice-mail in electronic storage (which requires a Title III order). The ECPA does not require notification to the subscriber when the government obtains information from a provider using a search warrant.

Warrants for information regarding evidence of a computer intrusion are usually obtained like all other search warrants but are served like subpoenas. That is, the agents serving the warrants on an ISP ordinarily do not search through the providers computers. Instead, they serve the warrants on the provider and the provider produces the material described in it.

Voluntary Disclosures

Investigators can obtain the contents of a hacker's communications stored on the victim system without first obtaining an order or a subpoena, pursuant to 18 U.S.C. § 2702(b). For example, a hacker's victim may voluntarily disclose the contents of internal e-mails relevant to the attack.

Voluntary disclosure by a provider whose services are available to the public is forbidden unless certain exceptions apply. These exceptions include disclosures "incident to the rendition of the service or the protection of the rights of property of the provider of the service." 18 U.S.C. § 2702(b)(5). See 18 U.S.C. §§ 2702(b)(1)-(4),(6)(A)-(B) for other exceptions.

Early Communication with ISPs

Investigators should contact a network service provider as soon as possible to request that the ISP retain records that may be relevant to an investigation. This is often done through the AUSA who is assisting the agent in the investigation. The AUSA should send a letter to the ISP directing it to freeze stored records, communications, and other evidence pending the issuance of a court order or other process. 18 U.S.C. § 2703(f).

If the investigator wants to be sure the ISP does not disclose that the ISP has been asked for information pursuant to a subpoena, order or warrant, an order not to disclose can be obtained under 18 U.S.C. § 2705(b).

Electronic Surveillance

Investigators tracking down hackers often want to monitor a hacker as he breaks into a victim's computer system. The two basic statutes governing real-time electronic surveillance in other federal criminal investigations also apply in this context.

The first is the wiretap statute, 18 U.S.C. §§ 2510-22, generally known as a Title III order.

The second statute relates to pen registers and trap and trace devices. 18 U.S.C. §§ 3121-27.

DOJ's manual for obtaining evidence of this type, says "In general, the Pen/Trap statute regulates the collection of addressing information for wire and electronic communications. Title III regulates the collection of actual content for wire and electronic communications." Computer Crime and Intellectual Property Section, Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation 71 (2001) *available at* <http://www.cybercrime.gov/searchmanual.pdf>.

A warrant is suggested, at a minimum, when an investigator wants to obtain access to opened voice mail, but the requirements of Title III apply if the investigator wants access to voice mail messages not yet retrieved by a subscriber or customer.

Nationwide Scope of Tools Used in Hacker Investigations

18 U.S.C. § 2703(d) orders are nationwide in scope, as are subpoenas. Other tools used in hacker investigations contain express geographic limitations. Search warrants under Fed.R. Crim.P. 41(a), Title III orders permitting the interception of communications, and 18 U.S.C. § 3123(a) orders authorizing the installation of pen registers and trap and trace devices all apply only within the jurisdiction of the court.

Search Warrants

Search warrants may be obtained to gain access to the premises where the hacker is believed to have evidence of the crime. Such evidence would include the computer used to commit the crime, as well as the software used to gain unauthorized access and other evidence of the crime. Suggested language for a search warrant for evidence of this type is available in the online manual prepared by CCIPS.

Analyzing Evidence from a Hacker's Computer

A seized computer may be examined by a forensic computer examiner to determine what evidence of the crime exists on the computer. The court order should specifically authorize this search. Many federal agencies have trained personnel on staff who are able to prepare a mirror image of everything in the memory of a seized computer -- often including the memory of things the computer owner thought had been erased. The computer examiner will prepare a detailed report regarding the information on the computer and should be able to testify as an expert at trial.

The Use of Traditional Investigative Techniques

Information obtained through the methods described above may reveal the subscriber or customer whose computer was used to conduct an intrusion. If it does, traditional investigative techniques may then be needed to determine who actually used the identified computer to commit the crime.

Due to the anonymity provided by the Internet, a suspected hacker may claim that someone else used his computer and assumed his identity at the time of the attack. It may be difficult to prove otherwise. For example, in a case charged in the District of Nebraska, the identity of the suspected hacker who defaced a newspaper's webpage by adding a bogus story was obtained even though computer logs showing the IP address of the hacker came to a dead-end because the hacker had used an ISP that provided anonymous access to the Internet. *United States v. Lynch*, 8:00CR344 (D. Neb. indictment filed Dec. 14, 2000). The now-defunct www.worldspy.com, kept no records of its users. Similar services still exist, such as www.anonymizer.com.

In the Nebraska case, calls to people in the community with the same last name as the person who was the subject of the unflattering article led authorities to the subject of the article, and that person led the FBI to the suspected hacker. Using tools available to obtain evidence of cybercrimes, including traditional investigative techniques such as this, federal law enforcement officers will continue to track down hackers and bring them to justice.

ABOUT THE AUTHOR

Daniel A. Morris is an Assistant United States Attorney (AUSA) in the District of Nebraska and is the Computer and Telecommunications Coordinator (CTC).

Mr. Morris has been an AUSA since 1987. Before that he was a Senior Corporate Counsel for the Mutual of Omaha Companies.

Mr. Morris is the author of two books, the *Nebraska Trial Handbook* and *Federal Tort Claims*, both published by West Publishing Company. He has published articles in the *Creighton Law Review* and for several years, was a regular contributor to *Case and Comment*, a magazine for lawyers.

Mr. Morris thanks CCIPS attorney Richard Downing for his comments and suggestions regarding this article and also thanks Patrick DeWall, a law clerk for the District of Nebraska for his assistance.

- [More information on: Computer Crime](#)
- [More information on: Computer Crime Guidance](#)
- [More information on: Cybercrime Documents](#)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page May 03, 2005

usdoj-crm/mis/sj
