U.S. Department of Justice
Executive Office for United States Attorneys
United States Attorneys' USA Bulletin
March 2001 Vol. 49, No.2

Working with Victims of Computer Network Hacks

Richard P. Salgado

USA Bulletin

(March 2001)

Richard P. Salgado
Trial Attorney
Computer Crime and Intellectual
Property Section

In our ten years' experience in detecting, locating, and prosecuting network intruders (hackers) we have seen that, as with many offline crimes, robust law enforcement alone cannot solve the network intruder problem. To be effective, any overall strategy must include the owners and operators of the nation's computer networks. They are the first line of defense and have the responsibility to take reasonable measures to ensure that their systems are secure. They are also in the best position to detect intrusions and take the first critical steps to respond. At the most basic level, we rely on network operators to report to us when their systems are hacked. Intrusion victims, however, are often even more reluctant to call law enforcement than other business victims. This reluctance has been reflected in the surveys conducted jointly by the Computer Security Institute and the FBI. In the year 2000 survey, for example, only 25% of the respondents who experienced computer intrusions reported the incidents to law enforcement. To better understand why and to learn how we can promote reporting, the Department of Justice has undertaken a concerted effort to reach out to the operators of our nation's computer networks.

As part of this effort, the Department, through the Computer Crime and Intellectual Property Section, has participated with the Information Technology Association of America in several industry-government summits this past year. The first two summits (held in Palo Alto, California, and Herndon, Virginia, respectively) were national in scope. Several regional summits followed, with more in the planning. The discussions in the summits concentrated on how law enforcement and victims of computer intrusions could work better together. Although several larger themes common to all the summits became apparent, one theme of particular concern was that private victims of computer network intrusions are reluctant to report the crimes to law enforcement.

The reluctance of intrusion victims to report poses a significant problem to the development of networked computers generally, and the Internet in particular. Although, upon finding a hacker

in his or her system, a system administrator may be content to close the intruder's account and fix the vulnerability (essentially kicking the hacker out and locking the door), this provides little true security. Not only is the hacker free to try the exploit on another company's network, the hacker may have left behind back doors through which he or she can return to the computer undetected. In addition, through the hacker community, others may learn of the exploit and, emboldened by the lack of any law enforcement response, join in compromising computer systems. It is folly to believe that any particular hacker is motivated by the desire to show-off computing prowess with no real intent to damage, steal, or defraud. What may appear to be a simple hack with no real risk of damage can, in fact, be a part of a larger scheme to launch a very destructive attack against other highly sensitive machines. Intruders may compromise many systems, collecting them like baseball cards. Some hackers use the "stolen" computers to launch attacks against other computers, shutting down the next victim, taking information from the systems, and using the stolen data in extortion schemes, or to engage in innumerable other types of illegal conduct. With each compromise, the security of our nation's networks diminishes. Without reporting by victims, law enforcement cannot provide an effective and appropriate response.

Myths and Misunderstandings

During the summits, some of the industry participants claimed a wide variety of reasons for the reluctance to report hacks. The perception on the part of some businesses is that there is little upside to reporting network intrusions. The perceived rationale for not reporting an intrusion include the following:

• The victim company does not know which law enforcement entity to call. Surely, the victim reasons, the local or state police will not be able to comprehend the crime and the FBI and Secret Service would have no interest in my system.
• If the victim company does report the intrusion to an appropriate agency, law enforcement will not act. Instead, the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions.
• If law enforcement does act on the report and conducts an investigation, law enforcement will not find the intruder. In the process, however, the company will lose control of the investigation. Law enforcement agents will seize critical data, and perhaps entire computers, damage equipment and files, compromise private information belonging to customers and vendors, and seriously jeopardize the normal operations of the company. Only competitors will benefit as customers flee and stock value drops.
• If law enforcement finds the intruder, the intruder likely will be a juvenile, reside in a foreign country, or both, and the prosecutor will decline or be unable to pursue the case.
• If the intruder is not a minor, the prosecutor will conclude that the amount of damage inflicted by the intruder is too small to justify prosecution.
• If law enforcement successfully prosecutes the intruder, the intruder will receive probation or at most insignificant jail time, only to use his or her hacker experience to find fame and a lucrative job in network security.

As formidable as the list of excuses may appear, these deterrents to reporting can be overcome by better-informed computer network owners and operators, and skillful investigatory and prosecutorial practice. Further, the risk presented by failing to report intrusions is tremendous. For the foreseeable future, our nation's networks are only going to get more complex, more interconnected and thus more vulnerable to intrusions. Networks are also going to be more important to our private lives, the nation's defense, and our world's economy. If there was a single clear mandate from the summits, it was that we must get the word out explaining why victims should report intrusions.

The Case for Reporting

Law enforcement needs to debunk the myths that have developed about the dangers of reporting intrusions and to sharpen our investigatory and prosecutorial practices. We also need to make an affirmative case for reporting to large network computer operators, focusing on the value to the company of reporting. In the course of the summits, it became clear that the message to operators and owners of computer networks is best delivered before a crises arises, when relationships can be built without the pressure of an ongoing investigation.

Debunking the Myths and Explaining the Basics

Perhaps the most basic piece of information to convey to victims concerns to whom the victim should report. Law enforcement agencies at all levels have developed some familiarity with computer crime investigations in the recent years, and if they are not equipped to handle complex computer intrusion cases, they are at least able to promptly refer reports to agencies that are. We need to ensure that large computer network operators know the law enforcement agencies in their area that have the necessary forensic and prosecutorial expertise and resources. Victims also need to understand that law enforcement does view intrusions as important and will respond appropriately.

Publicity that may follow reporting was also a concern that pervaded the summits. As a rule, agents and prosecutors need to ensure that they handle business information with a great deal of discretion. Similarly, law enforcement has to be sensitive to victims' concerns arising from the seizure of data from internal corporate networks. Most of the industry participants in the summits thought that law enforcement investigators would remove the servers, proceed without any victim input, that it would disrupt the normal operations of the company for weeks at a time, and that law enforcement's involvement would mean that the company could not take steps to secure the system or conduct its own investigation. Contrary to this belief, many investigations actually require input from the victim's system operator for technical operations. Communication with potential victims prior to any investigation would likely go a long way to address these concerns. Similarly, during investigations, law enforcement can work with the victims to ensure that the investigation remains confidential.

Certainly every investigation poses its own unique challenges, and there is no way to predict, with certainty, how any particular investigation will proceed. We have seen, and undoubtedly will see again, instances where a victim wants to take measures that are in conflict with the investigative strategy. For example, where there is a series of intrusions into a victim's network,

the victim may want to shut the intruder out of the system and patch the vulnerability. Law enforcement may prefer that the company leave the system open so that the hacker will not know he or she has been detected, and the agents can monitor the hacker's activity and track the hacker's origins. If there is a cooperative and trusting relationship between law enforcement and the victim that predates the intrusion, the agents and the company are more likely to find a resolution that works for both. In this example, the agents and system operator may be able to configure the network such that it is secure against future exploits, but appears to the hacker to remain open. Law enforcement can both protect the victim and pursue the intruder.

Many of the industry representatives expressed doubt about the ability of law enforcement to find the culprits. Certainly, tracking intruders is a very challenging task for a variety of reasons. Industry representatives readily acknowledged, however, that intruders will not be caught if the victim does not report. In any event, law enforcement has become much more sophisticated at tracking communications in recent years and even juvenile intruders are not immune from prosecution. Even if the juvenile is outside the United States, many foreign countries have been willing to prosecute.

Highlighting the Value of Reporting

There are also business reasons for companies to report intrusions cases. The two primary values to victims in calling law enforcement come from the deterrence that prosecution provides and potential restitution to the victim.

Specific deterrence is perhaps one of the most compelling reasons for a company to report an intrusion. When law enforcement catches and successfully prosecutes an intruder, that intruder is deterred from future assaults on the victim. This is a result that no technical fix to the network can duplicate with the same effectiveness. Intrusion victims may try to block out an intruder by fixing the exploited vulnerability, only to find that the intruder has built in a back door and is able to access the system at will. There have been instances in which a system operator, believing he or she is locking the intruder out for good, expends a great deal of time and effort to completely rebuild the network using backup media, only to find that the exploit was present in the backup and was simply reintroduced. Of course, a victim could initiate its own investigation to find the intruder. If successful, the victim may be able to initiate a civil suit for damages. In many (if not most) cases, however, the victim is at a substantial disadvantage relative to law enforcement in this effort. Law enforcement is able to obtain wiretap, pen/trap and trace orders, enforceable data preservation requests and other criminal process unavailable to a private party. Further, a monetary award is unlikely to serve as the same deterrent as a jail sentence or even probation. The general deterrence that criminal law enforcement provides also benefits victims and potential victims in the long run.

Restitution is also an attractive motive for victim reporting. Being a victim of intrusion is almost always an expensive proposition. A responsible victim must survey the system to determine whether any data was taken or damaged, and if so must repair the damage. The victim must analyze the network to determine if there are any remaining holes in the system, check the integrity of the logs, identify the means by which the intruder accessed the system, and patch the vulnerability. The costs can be very high, and can grow when the victim includes the loss of

business and the lost productivity of the technical staff dedicated to the intrusion. The victim may be able to recoup some or all of the expenses through restitution.

Reporting a criminal computer intrusion to law enforcement may also help the victim recover under insurance policies for damage to its system or damage inflicted on a third party resulting from the intrusion. Director and Officer insurance policies, for example, may exclude coverage if as a result of the victim's decision not to report the intrusion to law enforcement, the intruder inflicted additional damage to the victim system or attacked another's network using the victim's system. By reporting the intrusion in the first instance, however, the victim decreases the risk that the carrier could deny a claim made.

Similarly, where a victim's network is compromised and used to attack another system downstream, the victim may find itself a defendant in civil litigation brought by that downstream victim. If the victim has reported to law enforcement, it will be able to use the fact that it called in law enforcement as part of its defense of a claim, for example, that the victim did not take reasonable steps to prevent its network from being used as a platform to attack the plaintiff.

Making the Case and Selecting the Appropriate Audience

The summits illustrated that informal face-to-face meetings between law enforcement and representatives of potential intrusion victims is a valuable means to address concerns that the victims may have about reporting. Those industry representatives at the summits that had pre-existing relationships with law enforcement almost uniformly expressed an understanding of the need to report intrusions, and a willingness to do so. Those most reluctant to report, it appeared from the summits, were representatives who had no such relationship. Discussions in the heat of an investigation are far less likely to be productive than frank and informal dialogue prior to an incident. Prosecutors and agents should take the time to reach out to the large computer operators in their jurisdictions and build such relationships.

It is imperative that the message is heard by those who make the decisions. Some information security (IS) managers, for example, are very protective of "their" systems and will take umbrage at intrusions. They may not be content with simply re-securing the system in the hope that the hacker will not return, and will want the criminal arrested and prosecuted. They view law enforcement as a part of their security system; one of many resources that responsible network operators will use when the security of the network has been compromised. Other IS managers may be less receptive to reporting intrusions, even to their own superiors. The very fact of an intrusion, an IS manager may fear, suggests that he or she failed to properly secure the system. It has also become common for law enforcement to receive hacking reports from IS managers, but receive less than enthusiastic cooperation from the victim company once the fact of the hack is brought to the attention of the victim's higher-level management or general counsel. For the message to be effective, it must be heard by all the decision makers.

To get the word out, prosecutors and agents should take the time to reach out to the large computer operators in their jurisdictions. In addition to meeting with representatives of information technology companies such as Internet and telecommunications service providers, agents and prosecutors should look to other common targets of hacks including universities, e-

commerce and web-based retailers, and any organization that is reliant on large computer networks for operations. In addition, many jurisdictions are the home for information security associations, computer technology bar associations, and similar organizations. Those groups can provide law enforcement a solid forum in which to reach many network operators and counselors. The Computer Crime and Intellectual Property Section can help in this effort.

The perception that law enforcement and private computer network operators have separate and independent responsibilities in the battle against hackers is wrong. Although the network owners have the obligation to secure their systems, and law enforcement has an obligation to investigate and prosecute when appropriate,neither can function effectively without the other. Network operators need to view law enforcement as a necessary part of system protection, and law enforcement agencies need to be able to count on the cooperation of victims to fulfill their responsibilities.

ABOUT THE AUTHOR

Richard P. Salgado is a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice. In that role, he addresses a wide variety of complex legal and policy issues that arise in connection with new technologies. His responsibilities include training investigators and prosecutors on the legal and policy implications of emerging technologies and related criminal conduct. Mr. Salgado also prosecutes and provides advice on computer hacking and network attacks, and other advanced technology crimes including denial of service attacks, logic bombs, viruses and computer extortion, wiretaps and other technology-driven privacy crimes. Mr. Salgado also participates in policy development relating to emerging technologies, and in the Department's computer crime industry outreach efforts. Mr. Salgado has also served as lead negotiator on behalf of the Department in discussions with communications service providers to ensure that the ability of the Department to enforce the laws and protect national security is not hindered by foreign ownership of the providers or foreign located facilities.

###