Case study: Network intrusion investigation — lessons in forensic preparation

Eoghan Casey

1150 Connecticut Avenue, Suite 200, Washington, DC 20036, USA

Received 15 November 2005; revised 15 November 2005

Keywords
Forensic readiness; Forensic preparation; Incident response; Incident handling; Network forensics; Computer intrusion; Rootkit; Forensic computing; Tracking intruders; Attribution

Abstract Investigations of network security breaches are both complex and costly. Even a moderate amount of forensic preparation in an organization can mitigate the impact of a major incident and can enable the organization to obtain restitution. A case study of an intrusion is outlined in which the victim organization worked with law enforcement agencies to apprehend the perpetrator. This case study contains examples of challenges that can arise during this type of investigation, and discusses practical steps that an organization can take to prepare for a major incident. The overlapping roles of System Administrators, Incident Handlers, and Forensic Examiners in a network intrusion are explored, with an emphasis on the need for collaboration and proper evidence handling. This case study also shows how effective case management and methodical reconstruction of events can help create a more complete picture of the crime and help establish links between computer intruders and their illegal activities.

© 2005 Elsevier Ltd. All rights reserved.

Introduction

This case study describes a network intrusion that occurred in 2000, significantly disrupting the victim organization. The most significant impacts of the intrusion included several 24 × 7 × 365 laboratories being shut down for several days, preventing them from conducting cancer and AIDS research and resulting in financial losses. The victim organization was in the early stages of forensic preparation — Incident Handlers had been trained to preserve digital evidence, and network monitoring capabilities had been implemented at the Internet border. The Incident Handlers were able to gather sufficient evidence while securing the network to help law enforcement agencies apprehend the intruder and build a solid case. The intruder was brought to justice in 2004.1

1 The disposition of this case is not public because he applied for and was granted Youthful Offender treatment. The names of individuals, computers, and the victim organization in this case have been changed to protect their identities.
Initial notification

On March 30 2000, a System Administrator was performing routine maintenance on one of his Solaris computers that was critical to running experiments in his research center, and noticed an unusual account named "omnipotent." Since he was the only person who was authorized to create accounts on the system, he immediately suspected that the machine had been hacked. His first response was to remove the account to prevent the intruder from regaining access and then he notified the organization’s Information Security Office (ISO).

The ISO sent one Incident Handler to investigate the compromised computer. As he had been trained, the Incident Handler performed a live analysis of the system using trusted, statically compiled binaries in his toolkit, including the `script` command to create an audit log of his actions. A preliminary inspection of the system revealed that the intruder had replaced the standard Telnet with a version that contained a backdoor and had installed a sniffer. In addition to containing the root password for several neighboring computers, the sniffer log had recorded the intruder accessing computers through his own backdoor. Specifically, the logs showed that the intruder was gaining access to compromised computers without having to provide a password by entering his backdoor code word "open_sesame" at the Telnet login prompt.

Preserving the evidence

The Incident Handler acquired evidence from the compromised research lab computers and saved the audit log of his actions. He then returned to his office to perform a scan of the entire network for the "open_sesame" Telnet backdoor that turned up dozens of compromised machines throughout the victim organization. As a result, the ISO deployed all available Incident Handlers throughout the organization to obtain evidence of the compromise from each system. Although guidelines had been developed for gathering digital evidence from live Solaris systems, one individual was not well-versed in the process and, consequently, failed to preserve the evidence properly. On some of the systems he investigated, he collected listings of files rather than the files themselves. In addition, he did not keep an audit log or notes of his actions and, consequently, he had trouble determining which items were obtained from which computers. As a result, of these failures the damage on seven computers which prevented important research from being performed could not be included in the criminal case.

In the process of locating the compromised machines and gathering evidence, Incident Handlers learned that on March 22 2000, another System Administrator in the victim organization had received an e-mail report regarding the potential compromise of a computer under his care. This System Administrator did not realize the broader implications of this incident and did not report it to the Information Security Office at the time. When Incident Handlers came to the System Administrator’s office to examine other machines that he did not realize were compromised, he realized that the machine he had dealt with on March 22 was not an isolated event.

A preliminary examination of the evidence from each system revealed that all of the unauthorized connections were coming from a dial-up in Texas. The ISO configured their intrusion detections system to monitor network traffic for connections from the subnet in Texas used by the intruder. Late in the evening on March 31, the intruder returned and connected to several machines that had not been detected by the earlier scan for the "open_sesame" Telnet backdoor. One of these newly-discovered systems belonged to an administrator who maintained critical systems in the organization. Knowing this, the Incident Handlers took decisive action to secure the system and preserve it as a key source of evidence. In addition, the Incident Handlers called the toll-free number of the national Internet Service Provider (ISP) being used by the intruder to inform their network security department of the situation and to ask the ISP to preserve all related logs and records.

In some instances, the Incident Handlers were collecting evidence remotely while the intruder was actively accessing the system. They did not have physical access to, or even accounts on, some of the compromised systems, but they were authorized by the organization to gather evidence from any of the compromised systems on the network. To ensure that valuable evidence was not lost, Incident Handlers connected to several systems via the "open_sesame" backdoor and collected evidence remotely. One advantage of this approach was that the intruder was less likely to notice the Incident Handlers’ activities on the systems because they were hidden by the intruder’s own rootkit.

All data that the Incident Handlers collected during this initial phase of the investigation,
including audit logs that they generated to document their collection process, were digitally signed and saved to CD-ROM.

**Reconstructing the crime**

Using the evidence they had collected, investigators were able to show that the same modus operandi (MO) was exhibited on all of the compromised systems. The intruder used exploits for three vulnerable services on Solaris: cmsd (Calendar Manager),\(^2\) ttdbserverd (Tool Talk),\(^3\) and sadmind (AdminSuite).\(^4\) Deleted system logs recovered from some compromised hosts showed the traces of these exploits, showing how and when the intruder broke into the system. One troubling fact was that the Internet border router was configured to block connections to these ports. Therefore, the intruder most likely launched the attacks from within the organization’s own network. Unfortunately, the organization only had monitoring systems on the Internet border, but none on its internal subnets. Therefore, it was not possible to detect the intruder’s network activities within the organization, creating a significant blind spot. Fortunately, one Incident Handler recalled something from an incident several months earlier. By searching the incident database for past intrusions that originated from the same subnet in Texas, the investigators found one seemingly minor incident report relating to a stolen UNIX logon account (“user13”) and password. A reexamination of the evidence for that incident revealed that the intruder had used the stolen logon account as a base of operations to attack the organization from within.

From this base of operations, the intruder had scanned the network for vulnerable computers and launched exploits against them. After gaining unauthorized access to a machine, the intruder retrieved a file named “s1.tar” from the stolen “user13” account he was using as a base of operations. The contents of the “s1.tar” file included a script named “go” shown below that automated the installation of the rootkit. In addition to replacing system components with trojanned versions to create the backdoor and conceal the intruders’ presence, this script patched vulnerabilities to prevent others from using them to gain access to the system.

```bash
#\{\} - hacker omnipotent
#\{\} - SunOS rootkit v1
echo "creating directories"
mkdir /var/yp/.../
mkdir /var/yp/.../old/
echo "switching directory..."
cd stuff
echo "moving files..."
mv * /var/yp/.../
echo "cleaning up..."
cd ..
rm -rf stuff
rm -rf s1.tar
rm go
echo "switching directory..."
cd /var/yp/.../
echo "changing file permissions..."
chmod +x *
echo "backdooring login, rsh, and fingerd..."
./fix /usr/sbin/in.rshd /in.rshd /var/yp/.../old/in.rshd
./fix /usr/sbin/in.fingerd ./in.fingerd /var/yp/.../old/in.fingerd
./fix /bin/login ./login /var/yp/.../old/login
rm fix
echo "starting sniffers..."
nohup ./sls -a > log 

nohup ./sol -a > log2 &
sleep 2
```

\(^2\) http://www.cert.org/advisories/CA-1999-08.html.
Once he was ensconced on a computer, the intruder returned regularly to gather sniffer logs and obtain other sensitive data from the network.

Investigators combined data from all of the compromised systems and network logs to create a timeline of events.

<table>
<thead>
<tr>
<th>Date in 2000</th>
<th>Event summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 1 – Mar 23</td>
<td>Password theft and unauthorized access to UNIX logon account &quot;user13&quot; belonging to employee of victim organization. The stolen account was used without the owner's knowledge to store hacker utilities, including tools identical to those found on compromised machines. The intruder used this stolen account as a base of operations to break into other computers on the victim organization's network.</td>
</tr>
<tr>
<td>Mar 14</td>
<td>First recorded unauthorized access to a Solaris system by the intruder from the dial-up subnet in Texas (toolkit installed 4 min later).</td>
</tr>
<tr>
<td>Mar 15</td>
<td>First recorded unauthorized access to five computers in research laboratory from the dial-up subnet in Texas and other dial-up accounts. A forensic duplicate of one of these systems was created using EnCase.</td>
</tr>
<tr>
<td>Mar 17</td>
<td>First recorded unauthorized access to 19 computers in various research centers from the dial-up subnet in Texas.</td>
</tr>
<tr>
<td>Mar 18–21</td>
<td>First recorded unauthorized access to three more computers from the dial-up subnet in Texas.</td>
</tr>
<tr>
<td>Mar 22</td>
<td>A System Administrator in a division of the victim organization received an e-mail report from an outside organization regarding the potential compromise of a computer under his care but did not report the incident to the ISO of the victim organization.</td>
</tr>
<tr>
<td>Mar 28–29</td>
<td>First recorded unauthorized access to 13 machines in a research center from the dial-up subnet in Texas.</td>
</tr>
<tr>
<td>Mar 30</td>
<td>ISO received report from System Administrator of research center that one of the computers under his care had been hacked.</td>
</tr>
<tr>
<td>Mar 31</td>
<td>Incident Handlers scanned network for other machines with open_sesame backdoor.</td>
</tr>
<tr>
<td>Mar 31</td>
<td>While recording intruder connecting to compromised systems, Incident Handlers contacted Internet Service Provider in Texas being used by the intruder.</td>
</tr>
</tbody>
</table>
Tracking the intruder

It did not take long for the victim organization to realize how much damage the intruder had caused, and the research labs that were disrupted decided to take legal action. The organization contacted the FBI and provided the Bureau with sufficient evidence to initiate a criminal investigation.

FBI agents first contacted the Internet Service Provider used by the intruder to determine who owned the dial-up account the intruder used to connect to the Internet. This process turned out to be more challenging than investigators anticipated. Although most of the intruder’s connections were associated with a single dial-up account, one of the unauthorized connections appeared to implicate a staff member of the Internet Service Provider. It took several days for the FBI and victim organization to realize that they had made a typographical error in the paperwork, much to the relief of the ISP.

To complicate matters, the account belonged to a 50-year-old woman in California. Investigators doubted her involvement based on the fact that all of the intruder’s connections originated in Texas. Agents discovered that the dial-up account information had been stolen and was being used by the intruder without the owner’s authorization. Fortunately, the Internet Service Provider kept Automatic Number Identification (ANI) information from their modems. Using this information, investigators tied all of the intruder’s connections to a single residential phone number in Texas.

The FBI obtained a search warrant to search the suspect’s residence and seize evidence relating to the intrusions. Investigators determined that the most likely suspect was the 17-year-old son of the family that lived in the residence. While the FBI was executing the search warrant, the suspect acknowledged that his online nickname was "omnipotent."

Forensic examination

After the FBI seized the suspect’s computers, Forensic Examiners made duplicates of the hard drives and conducted a forensic examination of them. The Forensic Examiners found nmap port scan logs organized in folders labeled by victim organizations. The scan logs showed that nmap was used to scan the victim networks for ports 22, 23, 111, and 513.

Using the MD5 hash values of files that the intruder placed on the compromised computers, the Forensic Examiners quickly located the same files on the intruder’s computer, including the "s1.tar" file containing the rootkit used by the intruder. The "s1.tar" file found on the intruder’s computer also contained metadata from the stolen "user13" account, which was embedded in the tar file when it was initially created.

Other indications that the intruder’s computer had been used to gain unauthorized access to the compromised computers included sniffer logs and partial directory listings from the compromised systems in unallocated space of the intruder’s computer. Configuration files for the Secure CRT and LeapFTP applications referred to the compromised host names, and contained stolen account names and passwords. The intruder had also created text files with lists of stolen user accounts and passwords, and commands for downloading and installing the rootkit from his base of operations such as "rcp user13@logonserver.victim.com:/s1.tar/; tar-vxf s1.tar; ./go.sh."

Searching unallocated space and the swap file of the suspect’s computer revealed Internet Relay Chat session logs between the intruder and his cohorts. These logs served several purposes. They contained transcripts of the intruder boasting about which computers he had gained unauthorized access to, how he had gained access, the backdoors he used, and the kinds of data he had stolen. The logs also contained dates and times that coincided with periods when the victim computers were compromised and accessed by the intruder, demonstrating that the intruder was actively using the Internet at the time. Furthermore, the chat logs confirmed the association between the intruder’s real name and his nickname "omnipotent." Finally, the logs also contained IP addresses of his cohorts who were virtual witnesses and potentially the accomplices to the crimes, including the original developer of the rootkit.

During their analysis, the Forensic Examiners found lists of credit cards and stolen Internet dial-up accounts and passwords, including the dial-up account belonging to the 50-year-old in California that the intruder used while breaking into the victim organization’s computers. The intruder had apparently obtained these accounts from various computers using a Trojan Horse program called Back Orifice.

Lessons learned

The primary lesson to gain from this case study is that even a moderate amount of preparation can enable an organization to bring legal action against
the person who harmed them. Digital investigations such as this one are complex and time consuming, and forensic readiness reduces the per incident costs. Developing forensic readiness in conjunction with an information security program improves an organization’s overall security posture and helps integrate proper evidence handling into an organization's incident handling capabilities.

One of the most critical aspects of forensic readiness is teaching System Administrators and Incident Handlers how to respond to an incident. Unless System Administrators are educated about the ramifications of an intrusion, and understand the need to report even seemingly minor incidents, an organization may not be informed about a developing problem when it is first detected. Therefore, it is critical to educate System Administrators not to assume that a computer intrusion is an isolated event and that they need to inform others because it is likely that the intruder has caused additional damage on the network. In addition, System Administrators may unintentionally disturb the crime scene in an innocent attempt to correct the problem. Although it is often possible for investigators to work around this type of evidence dynamics, organizations that train their Systems Administrators to take the appropriate actions to preserve the crime scene will be in a better position to resolve the incident. Similarly, unless Incident Handlers are properly trained, they will not preserve evidence properly.

Although this case distinguishes between Incident Handlers and Forensic Examiners, there is significant overlap between the two roles. Incident Handlers need to perform some level of forensic analysis and reconstruction during the initial phase of the investigation to establish how and when the intruders gained access, and determined the scope and timeline of the intrusion. In addition, Incident Handlers need to analyze evidence to understand the intruder's backdoors, rootkits, and MO. An intruder’s MO is not only useful for determining that multiple machines were compromised by the same individual, but can also help link the perpetrator to the crime. In this case, Incident Handlers knew what types of information to gather from the compromised hosts that would enable Forensic Examiners to link the intruder to the crime scenes. Ultimately, given the significant overlap between the two roles, individuals who deal with network intrusions should be trained as both Incident Handlers and Forensic Examiners.

Another important step that organizations can take to prepare for network investigations is to identify their most valuable digital assets and develop a strategy to prepare the underlying systems from a forensic viewpoint. Knowing which systems on a network contain sensitive information enables Incident Handlers to prioritize and rapidly protect the most important systems first. In this case study, Incident Handlers recognized that one compromised system posed a higher risk than others and took immediate action to secure and preserve evidence on that system. This type of knowledge management is particularly useful when confronted with more sophisticated intruders, when it is difficult to determine which systems have been compromised. In such a situation, having a list of the most important assets in an organization enables investigators to focus their initial efforts on the most important systems and quickly determine whether intruders gained access to them.

Having a logging infrastructure that is designed with digital investigations and forensic principles in mind greatly facilitates network investigations. The lack of internal monitoring of network activities makes it difficult to detect intruders after they gain access to a machine on the network. Fortunately, in this case, evidence from a prior investigation revealed the intruder’s base of operations within the network. This demonstrates the value of case management and incident tracking. Well-organized records for every incident can help identify relationships between seemingly unrelated incidents. Case management is also important because an investigation like this one can take years to reach a court, making thorough record keeping and documentation of the investigation and forensic examination critical to enable investigators to recall details several years later.

The biggest mistake that investigators can make is to implicate the wrong person for a crime. Investigators must be careful when communicating information to law enforcement, ISPs, and other third parties because transcription errors in search warrants and other documents can cause confusion and waste time, and lead to unforeseen consequences. In addition, investigators cannot assume that the owner of an Internet account is responsible for criminal activities associated with that account, since the owner’s account information may have been stolen.

The most incriminating source of evidence in a network intrusion is generally the intruder’s own computer(s). Searching the intruder’s computer(s) for information transferred from the compromised systems, including sniffer logs and other trophies, can reveal overwhelming evidence connecting the intruder to the crime (Locard’s Exchange Principle). The more information that Incident Handlers preserve on compromised systems, the better...
equipped Forensic Examiners will be to establish links to the intruder’s computer. In addition, logs of online chat sessions may be recovered from the intruder’s computer, providing investigators with a variety of useful information and leads.

In the end, even if the cost of conducting a network intrusion investigation exceeds the financial returns, a successful outcome generally has many intangible benefits. An organization that takes such matters seriously rather than sweeping them under the rug will benefit from a due diligence standpoint. Furthermore, by developing a reputation for tracking down intruders rather than accepting defeat, an organization may become a less attractive target for intruders in the future.