Determining Intent — Opportunistic vs Targeted Attacks

Eoghan Casey

To assess the importance and potential impact of an incident accurately computer security professionals need to understand an offender's criminal skill, knowledge of targets, and intent. A thief who selects targets of opportunity based on insecure systems presents a significantly different threat than an individual who targets a specific organization to obtain specific information. This article compares two intellectual property theft cases to provide readers with practical investigative insights, noting costly mistakes and pointing out behaviour reflected in digital evidence. Although these cases are based on actual investigations, they have been modified to protect the innocent.

Introduction

Intellectual property theft ranges from an employee using proprietary information to establish a competing product, to an individual holding valuable information ransom, to an unethical organization breaking into a competing organization's systems. In such cases the target is generally information and, to varying degrees, the organization. The thief may intend to use the information to create a competitive advantage, in which case the information is the primary target. If the thief takes the information and then destroys the original copy to effect the organization adversely, the information and organization are targets to equal degrees. However, if the thief attempts to make a profit by holding the information ransom, the organization is the primary target.

Generally, a thief with inside knowledge of an organization can cause more damage than an outsider. However, such generalizations are of limited use in actual investigations because each situation is different. It is more informative to examine available evidence to determine the threat posed by a given thief. An organization's ability to assess the threat in a given case and apprehend the perpetrator depends largely on how the incident is handled. Proper evidence collection and interpreting behaviour represented in the digital evidence are cornerstones of effective incident handling.

To understand how digital evidence reflects behaviour, it is instructive to consider some examples. When thieves target an organization's computer systems, their actions leave behind digital evidence that can reveal their intent, skill level, and knowledge of the target. Network logs may show a broad network scan prior to an intrusion, suggesting that the individual was exploring the network for vulnerable and/or valuable systems. This exploration implies that the individual does not have much prior knowledge of the network and may not even know what he/she is looking for but is simply prospecting. Conversely, thieves who have prior knowledge of their target will launch a more focused and intricate attack. For instance, if a thief only targets the financial systems on a network, this directness suggests that the intruder is interested in the organization's financial information and knows where it is located.

So, if the targeting is very narrow – the thief focuses on a single machine – this indicates that he/she is already familiar with the network and there is something about that particular machine that interests him/her. Similarly, time pattern analysis of the target's file system can show how long it took the intruder to locate desired information on a system. A short duration is a telltale sign that the intruder already knew where the data was located whereas protracted searches of files on a system indicates less knowledge.

The sophistication of the intrusion and subsequent precautionary acts help determine the perpetrator's skill level. The thief's knowledge of the target and criminal skill can be very helpful in narrowing the suspect pool, particularly when only a few individuals possess the requisite knowledge and skills suggesting insider involvement, as in the "Breaking the Bank" case presented by Fred Cohen in the November 2002 issue of *Computer Fraud and Security*.

The following two case examples provide different lessons for dealing with and interpreting digital evidence in computer intrusion cases.

Case #1: Compromised W2K Domain Controller

In February 2002, a client called an information technology consultant to report that their sole Windows 2000 domain controller was running slowly and had rebooted unexpectedly on several occasions. The consultant scanned the server using Internet Scanner and looked at running processes using fport (www.foundstone.com) to get an initial sense of the system. Internet Scanner found only one security problem with the domain controller – it was running a variant of Back Orifice 2000 (BO2K) on TCP port 1177. The output of fport showed that port 1177 was associated with the executable c:\windows\system32\wlogin.exe.

When the client was informed of this problem, their primary concern was business continuity. Because of the critical role that this server played in the Windows domain, a rapid response and recovery was required. The client was unwilling to take the domain controller offline because this would disrupt business operations. In short, the client wanted the server to be fixed with minimal impact on the organization and was only casually interested in apprehending the culprit.

The consultant's first task was to determine how BO2K had been installed on the domain controller. The system was located in a locked room and only one employee could access it physically using a smartcard. This individual was the only suspect because the domain controller did not have any obvious vulnerabilities and nobody else could legitimately access the system over the network to install programs. Although the system administrator vehemently denied any involvement, the consultant knew that it would be relatively straightforward to find incriminating digital evidence on the server. Therefore, before attempting to remove BO2K, the consultant saved system logs and file system date-time stamps from the server for later analysis if the client decided to discipline the system administrator.

In the past, the consultant had successfully removed BO2K by removing the associated value in the HKLM\Software\Microsoft\Windows\CurrentVersion\Run Registry key, rebooting the system, and deleting the executable. However, there was no sign of BO2K in the Run Registry key so the consultant performed an extended search of the Registry and system files for references to the Trojan program. In this case, dumping the Registry and searching for references to wlogin.exe revealed that BO2K was being started as a service.

After removing the rogue service from the Registry, the consultant obtained permission to reboot the server to ensure that all remnants of the process were eliminated. Unfortunately, the domain controller did not reboot successfully because the Trojan horse program had replaced the legitimate WinLogin service. By removing the rogue service, the consultant had effectively done more damage than the intruder, interrupting business operations while attempting to restore the server. After some pandemonium, the system administrator came to the consultant's aide and resolved the problem by changing the HKLM\System\CurrentControlSent\Services\WinLogin\ImagePath Registry key to point to the legitimate WinLogin.exe executable.

The client was outraged by the disruption cause by the failed reboot. The consultant was summarily dismissed but not before blaming the system administrator for installing BO2K on the server. The client decided to involve law enforcement to recover damages from whoever was responsible.

By discovering intent, the significance of the intrusion becomes clear, and relevant action can be taken.

A closer examination of the log files and other digital evidence the consultant collected from the system revealed that, although Microsoft Internet Information Server (IIS) was fully patched at the time of examination, the machine had been compromised via the IIS Unicode vulnerability before it was patched. Also, Norton AntiVirus had made numerous entries in the Application Event log reporting that BO2K had been found on the system but nobody had been reading these logs. So, although the system administrator could be faulted for patching the system too late and missing obvious signs of intrusion, it seemed less likely that he was guilty of installing BO2K particularly since he lacked a motive and appeared more interested in helping the organization maintain their operations than in disrupting them.

At this point, the investigators determined that they needed more evidence from the domain controller and the network to gain a more complete understanding of the intrusion. By this time, the client had formed many urgent questions including why this system was targeted, what was taken, and by whom.

A more complete examination of the domain controller revealed that the intruder had installed an IRC Eggdrop bot in C:\Winnt\Java. The Eggdrop bot's files contained information about servers, nicknames, channels, and channel passwords relating to the intruder. Additionally, log entries from the organization's intrusion detection system showed a broad network scan for vulnerable Web servers prior to the intrusion. Unfortunately, because the server had been in operation after the intrusion, investigators could not determine if the intruder had accessed sensitive files, captured passwords, or obtained other valuable information from the server. Fortunately, the intruder did not appear to be seeking proprietary information on the system. An analysis of the computer and network showed that the intruder primarily used the system for storage and to connect to IRC and was not interested in its contents. Additionally, the intruder did not exhibit a high amount of skill or knowledge of the network, suggesting an outsider looking for poorly secured systems.

The cost of damage caused by this intruder was difficult to determine because the consultant caused much of the harm. However, it was likely that this intruder had compromised other systems or would attempt to compromise other systems in the future. Therefore, a more detailed network assessment was warranted to locate other compromised systems and prevent similar attacks.

Mistakes in Case #1:

In addition to causing significant disruption, the information technology consultant made several mistakes in handling this incident. While examining and attempting to repair the system, the consultant altered many aspects of the compromised computer, including modifying important Registry values and file date-time stamps, effectively tainting the crime scene. Also, either by design or accident, the Trojan wlogin.exe was zeroed out after the system was rebooted. Thus, an important piece of evidence was lost – the executable may have contained characteristics or configuration options that reveal something about the intruder.

The consultant made another mistake in assuming that only one backdoor existed. The consultant stopped looking for other signs of intrusion once he found BO2K rather than checking all running processes to ensure that there are no other suspicious or unexplainable programs. The consultant also should have looked for new accounts in the administrator group and other changes to the system (e.g., Registry permissions) that could be used to regain access to the system.

Furthermore, the consultant only retained one copy of the evidence, compressing all evidentiary files into a single Zip file and transferring it to a remote system over the network. Unfortunately, the Zip file was corrupted in transit and could not be opened. The contents of the Zip file was partially recovered using a file repair program but some evidence was lost. Although there is nothing inherently wrong with compressing and saving evidence files in a compressed archive or transferring them to a remote system via a network connection, making just one copy of the evidence is high-risk behaviour. It is advisable to save a copy of all digital evidence in uncompressed form to a diskette and clearly label it with the contents, current date, and investigator's initials.

Case #2: Intranet Web Server

In December 2002, the CEO of a medium-sized organization contacted an investigator for urgent assistance because a competitor had obtained private information from his system and he wanted to know how. Only one computer contained this information and the investigator performed an analysis of running processes and other aspects of the system using a procedure that minimized changes to the system, but found nothing unusual. Extending his search to neighboring machines, the investigator found one computer on the same subnet that showed signs of compromise. The investigator quickly shut the system down, made an image of the hard drive, and performed a detailed analysis of the system. Although there was very little information on the system, Web server access logs indicated that the intruder gained access via the Internet Information Server (IIS) Unicode vulnerability.

The log entries indicated that the attack originated in Italy and the tools were downloaded from an IP address in Canada using **tftp**. Most notably, the intruder placed **netcat** on the system and configured it to give a command prompt to anyone connecting to port 443 using Telnet.

Date-time stamps of files on the system showed that most activity occurred early in the morning of 03/01/2002 with several files accessed. Interestingly, these date-time stamps did not indicate that the intruder searched around the file system, suggesting that she did not have interest in the contents of the server. However, one other file named **windump.exe** was added to the system on 02/28. Additionally, investigators found an unusual file on the compromised system named **dump** that was created around the time of the intruder's last connections containing network traffic from the organization's network. This file did contain sensitive information but not the specific data that the client was originally concerned with. It was likely that the intruder obtained the private information using the sniffer and deleted the file from the compromised system to cover her tracks.

Upon closer inspection, comparing the Web access logs with file date-time stamps, the investigator realized that some IIS log entries from later on 02/28 and 03/01 were missing, indicating that the intruder had deleted them. The investigator began to suspect that all was not as it seemed. This concealment behaviour along with the relative sophistication of the attack convinced the investigator that he was dealing with a highly skilled adversary. So, the investigator sought more reliable sources of evidence on the network to get a complete picture of what had occurred.

Analyzing the organization's firewall configuration showed that the compromised Web server could not be accessed from the Internet. This implied that the Italian IP address in the compromised Web server logs was fabricated to conceal the actual source of the attack. An analysis of relevant Snort and NetFlow logs showed that the attack was actually launched from another system inside the organization's network and indicated that the initial compromise occurred on 02/28 between 18:57 and 19:03. This machine did not have log files or other information that could be used to determine how the system was compromised or where the attacker came from. However, network logs showed one remote logon to the machine at the time from a large Internet Service Provider (ISP). Additionally, NetFlow and Snort logs showed that this was a focused attack on the target systems – the intruder did not probe any other systems. The fact that no other machines were attacked in this incident indicated that the intruder had some prior knowledge of the network and her target. This was a highly targeted attack and the type of information sought using the sniffer suggested that intellectual property theft was the likely intent.

Based on the level of skill of the thief and the likelihood that sensitive information was stolen, the investigator informed his client of the seriousness of the incident and advised them to involve law enforcement. Law enforcement was contacted and they obtained information about the intruder from the originating ISP. Although the dial-up account that the intruder used turned out to be stolen, the ISP maintained Automatic Number Identification (ANI) information that revealed the intruder's phone number. A search warrant was served on the intruder's home and an examination of her computer revealed not only the stolen information from the client's system but also relevant communications with the competitor.

How it should be done

This case highlights the importance of a methodical approach to incident handling and digital evidence processing. The investigator was thorough and efficient, causing less disruption than the previous case although the incident was more serious and more sources of evidence were involved. Additionally, the investigator quickly assessed that he was dealing with a highly skilled offender and reacted accordingly by obtaining evidence from the target network that the intruder could not alter.

Notably, the investigator did not attempt to fix the compromised system. As noted in the previous case example, attempting to fix a system while conducting an investigation can undermine evidence preservation efforts. Additionally, the intruder could subtly alter a system to facilitate future compromise, making it more difficult to eradicate the intruder completely. Instead, the investigator focused on preserving evidence and determining what had occurred. Afterwards, the investigator recommended that the compromised system be reformatted and rebuilt before reconnecting it to the network. The process of rebuilding a compromised system involves backing up data files before reformatting the drives, reinstalling and securing the system, and carefully examining files before placing them on the rebuilt system to ensure that they do not contain a backdoor. The investigator also recommended using network encryption (IPSec) between critical systems to prevent the type of eavesdropping that occurred in this incident.

When dealing with more sophisticated offenders, investigators must be prepared for misdirection and concealment.

Conclusions

These two case examples compared a target of opportunity versus a deliberate attack. In the first case, a low-skilled intruder with little prior knowledge of the target system found a vulnerable host by scanning the network indiscriminately. This intruder appeared to be satisfied with just gaining access to the compromised host and made no effort to obtain valuable information, as the client had feared. If handled properly, the damage caused by this low-threat incident would have been minimal and the organization could have continued normal operations without the added cost and disruption of a full investigation. This case example demonstrated that determining the intent is of little use when an incident is handled improperly.

In the second case, a highly skilled attacker demonstrated knowledge of the target system, bypassing the firewall and gaining access to a sequence of computers with the specific intent of obtaining valuable information. When dealing with more sophisticated offenders, investigators must be prepared for misdirection and concealment. In this case, the intruder altered server logs to misdirect the investigator. If the kernel is modified, signs of intrusion are more difficult to detect so investigators should not assume that a system is not compromised just because there are no obvious signs. These types of concealment behavior can be detected by correlating evidence from the compromised host with network logs. The investigator in this case handled evidence properly, correctly assessed the skill level of the offender, and ultimately helped the organization resolve the incident with minimal impact on their operations. Evidence from multiple independent sources on the network were used to overcome missing and misleading evidence on the compromised hosts, enabling the investigator to reconstruct a more complete picture of the crime.

In both cases, digital evidence revealed the intruder's behaviour to the extent that an investigator could deduce the intruder's intent, level of skill, and knowledge of the target system.

About the Author

Eoghan Casey is Technical Director and Partner in Knowledge Solutions, LLC. He investigates network intrusions, intellectual property theft, and other computer-related crimes, and has extensive experience analyzing digital evidence. He has assisted law enforcement in a wide range of criminal investigations including homicide, child exploitation, cyberstalking, and larceny. Mr. Casey also has extensive information security experience. As an Information Security Officer at Yale University and in subsequent consulting work, Mr. Casey has performed vulnerability assessments, deployed and maintained intrusion detection systems, firewalls and public key infrastructures, and developed policies, procedures, and educational programs. Mr. Casey is the author of Digital Evidence and Computer Crime and the editor of the Handbook of Computer Crime Investigation.