CSO
SECURITY AND RISK

From: www.csoonline.com

Incident Detection, Response, and Forensics: The Basics

Richard Bejtlich on how to build an effective cyber incident detection and response mechanism in your organization.

Richard Bejtlich, CSO

April 02, 2008

2008 is a special year for the digital security community. Twenty years have passed since the Morris Worm brought computer security to the attention of the wider public, followed by the formation of the Computer Emergency Team/Coordination Center (CERT/CC) to help organizations **detect, prevent and respond to security incidents**. Ten years have passed since members of the L0pht security research group told Congress they could disable the Internet in 30 minutes. Five years have passed since the SQL Slammer worm, which was the high point of automated, mindless malware. The Internet, and digital security, have certainly changed during this period.

The only constant, however, is exploitation. For the last twenty years intruders have made unauthorized access to corporate, educational, government, and military systems a routine occurrence. During the last ten years structured threats have shifted their focus from targets of opportunity (any exposed and/or vulnerable asset) to targets of interest (specific high-value assets). The last five years have shown that no one is safe, with attackers exploiting client-side vulnerabilities to construct massive botnets while pillaging servers via business logic flaws.

Despite twenty years of practical experience trying to prevent compromise, intruders continue to exploit enterprises at will. While they may not be successful attacking any specific asset (unless inordinate resources are applied), in aggregate intruders will always find at least one viable avenue for exploitation. The maxim that "prevention eventually fails" holds for any enterprise of sufficient size, complexity, and asset value to attract an intruder's attention. The threshold has fallen to the point where a single home PC is now considered "worthy" of the same sorts of attacks levied against multibillion-dollar conglomerates.

In a world where the adversary eventually breaches some aspect of a target's protective measures, what's an enterprise security manager to do? The answer is simple:
1) detect compromise as efficiently as possible;
2) respond to incidents as quickly as possible; and
3) investigate using digital forensics as effectively as possible.

This article will provide several ways to think about this issue and implement computer incident detection, response, and forensics capabilities to support your enterprise.

Incident Detection

Incident detection has suffered from a variety of misconceptions and miscommunications during its history. One of these has been the narrow way in which most operators view the detection process. I recommend thinking of incident detection in terms of three "orders."

First order incident detection is the traditional way to apply methods to identify intrusions. First order detection concentrates on discovering attacks during the reconnaissance (if any) and exploitation phases of compromise. Reconnaissance is the process by which an intruder learns enough about the target to effect intrusion. Exploitation is the process of abusing, subverting, or breaching a target, thereby imposing the intruder's will upon the asset. Almost all security products that seek to detect and/or "prevent" attacks monitor activity during these stages of the compromise lifecycle.

Second order incident detection moves beyond reconnaissance and exploitation to the final three stages of compromise: reinforcement, consolidation, and pillage. Reinforcement is the process by which an intruder leverages the unauthorized access gained during exploitation in order to build a more stable platform for repeated re-entry. Downloading and installing a remote access Trojan program is a classic reinforcement activity. Consolidate is the act of controlling a compromised asset using the means installed during reinforcement. Pillage is the execution of the intruder's ultimate plan, which could be pivoting on the target to attack another system, exfiltrating sensitive information, or any other nefarious plan the intruder may wish to execute. Second order detection focuses on identifying any of these final three phases of compromise, which can be highly variable and operate at the discretion of the intruder.

Third order incident detection occurs outside the realm of the five phases of compromise by concentrating on post-pillage activities. Whereas first- and second-order detection is done at the enterprise, either by watching hosts, network traffic, logs, or possibly even sensitive data, third order detection takes place outside the enterprise. Third order detection seeks to discover indications that preventative and detection mechanisms have failed by finding the consequences of an intrusion. Looking for these sorts of signs could take the form of searching for, and finding, private company documents on peer-to-peer networks, or intruder-operated botnet servers, or a competitor's release of a product uncannily similar to your company's own. Each of these events indicate a breach or policy violation occurred, yet none may have been detected by conventional means. Third order detection is a powerful way to determine if the formal detection mechanisms operated by an organization's security team make any difference in the real world.

A complementary way to think about detection takes the form of six maturity levels. Using the ideas below, you can determine how advanced your detection initiative may be.

Level 0. No primary detection method exists. No formal data sources are used. No actions are taken, since this "blissful ignorance" hides the fact that the enterprise could be (and probably is) severely compromised.

Level 1. Customers, peer organizations, and users are the primary detection methods. No data sources beyond those provided by the aforementioned parties are available. The predominate reaction is to form an ad-hoc team to fight fires on a repeated basis.

Level 2. Customers, peer organizations, and users are still the primary detection methods. However, the organization has some data store from which to draw conclusions -- once the enterprise knows it must look for clues. Reaction involves more fire fighting, but the officers aren't quite as blind as they were at level 1 thanks to the availability of some logs.

Level 3. The **Computer Incident Response Team (CIRT)** is discovering incidents in concert with the parties listed at levels 1 and 2. Additional data sources augment those aggregated at level 2. The CIRT develops some degree of formal capability to detect and respond to intrusions.

Level 4. The CIRT is the primary means for detecting incidents. All or nearly all of the data sources one could hope to use for detection, response, and forensics are available. The CIRT exercises regularly and maintains dedicated personnel, tools, and resources for its mission.

Level 5. The CIRT is so advanced in its mission that it helps prevent incidents by identifying trends in the adversary community. The CIRT recommends defensive measures before the enterprise widely encounters the latest attacks. The CIRT operates a dedicated security intelligence operation to stay in tandem or even ahead of many threat agents.

Incident detection natually leads to incident response, where actions are taken to contain, eradicate, and recover from intrusions.

Incident Response and Forensics

Twenty years ago incident responders were taught to locate a potentially compromised computer and literally, physically, "pull the plug." The idea was to eliminate the possibility that an intruder occupying a compromised system could notice a normal shutdown and implement techniques to evade detection. Incident responders also worried that intruders might have planted rogue code that started cleanup routines upon initiation of a shutdown command.

Following the abrupt removal of the power cord, incident responders would duplicate the hard drive (usually 40MB -- if it had a hard drive at all in 1988!) and scrutinize the duplicate for evidence of malfeasance. Despite the small hard drive size, this process took time, physical locality (to acquire the hard drive), and expertise.

In 2008, and really for the last decade, the situation has been vastly different. Pulling the plug has been a discredited strategy for years. The major problem with abruptly removing power is the removal (heroic freezing efforts to the contrary) of volatile evidence from system RAM. System RAM is the place where computers store much of the data that incident responders care about, like running processes, active network connections, and so on. Most of that sort of high-value information is not stored on the hard drive, so it perishes when power disappears.

For example, do you remember the Slammer worm mentioned previously? Slammer was completely memory-resident. Remove the power and Slammer disappears. Unless an intruder takes steps to entrench himself on a system (in the reinforcement stage), sometimes a simple reboot is enough to remove him (at least temporarily). If the original vulnerability persists, re-exploitation may quickly follow. For a certain category of stealth-minded intruders, reliance on re-exploitation is the preferred means to maintain a low-profile network presence.

The question of who pulls the plug, and when it could happen, is also paramount in 2008. Most important systems run in data centers built for uptime and redundancy. Pulling the plug isn't a normal operation, and even getting to the server in question can be an adventure. Furthermore, few asset owners would consent to having their money-making systems abruptly removed from operation. Some managers are willing to tolerate compromise because losing a production host is considered the greater risk (never mind that hacker -- we need to make money!).

Given these realities, incident response in 2008 is now a different animal. Often a system suspected of being compromised is on another continent, in the hands of a user who may not even speak the same language as the security team. Hard drives are routinely 80-160GB on laptops and more than 500GB on servers, with storage area networks and related systems easily exceeding any investigator's ability to duplicate. With such huge volumes of data to analyze, it makes more sense to concentrate on the 4GB of virtual memory present on 32-bit systems.

Incident responders are increasingly relying on live response, or the collection and analysis of system RAM for indicators of compromise. Live response activities have been used for the last eight to ten years by professional investigators in high-end cases, but modern realities are forcing most security pros to add the techniques to their repertoire. Current tools usually push an agent or executable to a remote system, capture or parse memory, and communicate the results to a central location. There an expert human or, in some cases, a series of programs reviews the evidence for signs of malware or unusual activity.

In addition to remote retrieval and analysis of memory, incident responders and forensic investigators are trying to avoid duplicating the entire hard drive of target computers. Increasingly it is just not technically possible or cost effective to do so. Judges, agents, and investigators who were taught that only a "bit for bit copy" was a "forensically sound copy" will have to wake up to the expansive nature of today's digital environment. Why copy a 2-terabyte RAID array on a server if cursory analysis reveals that a small set of files provides all of the necessary evidence to make a sound case? Expect greater use of "remote previews" during incident response and select retrieval of important files for forensic analysis.

In addition to focusing on just the material that matters, modern incident response and forensic processes are more rapid and effective than historical methods. When hard drives were 40MB in size, it was feasible for a moderately skilled investigator to fairly thoroughly examine all of the relevant data for signs of wrongdoing. With today's volume of malicious activity, hard drive size, and efforts to evade investigators (counter- and anti-forensics, for example), live response with selective retrieval and review are powerful techniques.

Richard Bejtlich is Director of Incident Response for General Electric and author of the TaoSecurity Blog (taosecurity.blogspot.com) and several books, including The Tao of Network Security Monitoring: Beyond Intrusion Detection. Richard began his digital security career as a military intelligence officer at the Air Force Computer Emergency Response Team (AFCERT), Air Force Information Warfare Center (AFIWC), and Air Intelligence Agency (AIA).

http://www.csoonline.com/article/205960/incident-detection-response-and-forensics-the-basics
http://www.csoonline.com/article/print/205960