BUSINESS:
THE 8TH
LAYER

SNIPER FORENSICS

By Lynn Greiner

Security attacks and breaches leave clues for investigators who know why they matter.

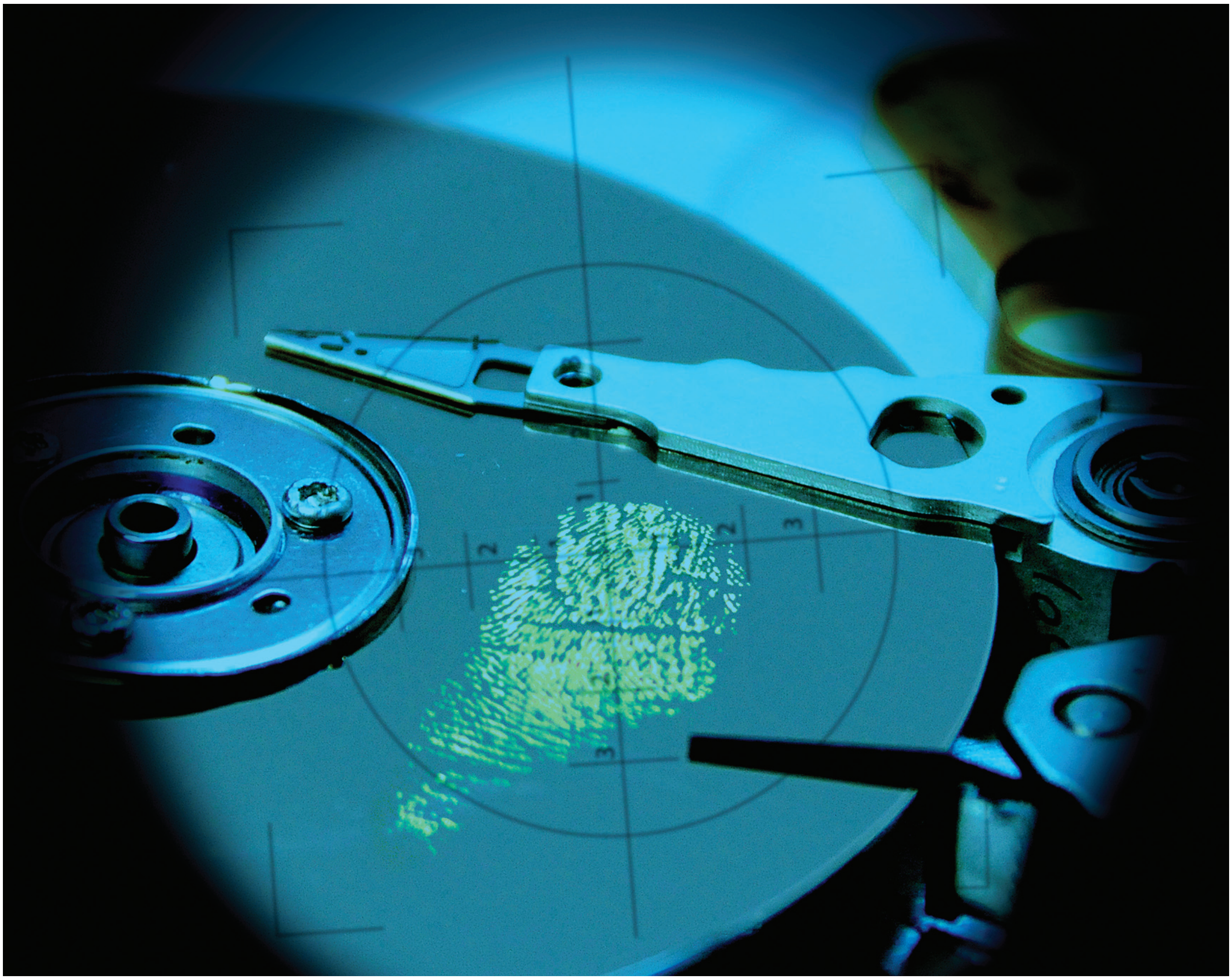
When an organization suffers a security breach, it may react in one of several ways, assuming it knows of the breach at all. In May 2007, the CPA *Journal* reported that TJX Companies, parent of department store T.J. Maxx, needed 18 months to discover that hackers had been rummaging through its systems, compromising credit and debit card records from 2003 onward.

To its credit, TJX publicly disclosed what had happened and took the heat (including numerous lawsuits), but some organizations prefer to conceal the problem from the public, knowing full well the impact public disclosure would have on their business. Hapless customers then learn the hard way that their personal and/or financial information has been stolen after the bad guys make use of it, though, fortunately, many jurisdictions have now legislated full disclosure of breaches.

Regardless of whether something has indeed been swept under the corporate rug, chances are there will be significant internal effort to find and plug the cause of the leak. It is likely that the victim organization doesn't want to risk another disaster to its public image (and probably to its share price). Such frantic efforts might lead to what Christopher E. Pogue, a senior security analyst of Trustwave SpiderLabs, calls "shotgun forensics." In a session at the annual SecTor security conference in Toronto last October, Pogue described the technique as a haphazard, unguided approach to forensic analysis that basically tells analysts to image everything and then look for the bad stuff, which, he says, is a waste of time and energy.

Pogue—whose credentials include a veritable alphabet soup of security certifications: a master's degree in information security, a stint at the CERT Coordination Center at Carnegie Mellon University's Software Engineering Institute[1], authorship of many security articles and the *Unix and Linux Forensic Analysis DVD Toolkit,* and a tour of duty in the U.S. Army Signal Corps—says shotgun forensics is an old-school approach to security

[1] The CERT program is part of the Software Engineering Institute, a U.S. federally funded research and development center. Following the Morris worm incident (http://en.wikipedia.org/wiki/Morris_worm), which froze 10 percent of the world's Internet systems in November 1988, the U.S. Defense Advanced Research Projects Agency charged SEI with setting up the CERT Coordination Center to coordinate communication among experts during security emergencies and help prevent future incidents.



issues and instead recommends the much more focused "sniper forensics."

According to Pogue, Sniper forensics is a clear, targeted, deliberate approach to forensic analysis of compromised systems or of systems suspected of being compromised. It includes time-tested principles to extract pertinent data from them, allowing it to tell the story. To apply sniper forensics, he says to first create an investigation plan, aiming to answer several basic questions:

- How did the bad guys get onto the system?
- What did they do while there and what did they steal? and
- How did they escape and how did they get the stolen data off the system?

Pogue says investigators must know what they're looking for, when they've found it, and when to stop looking. How? Through proven principles of logic. For example, Locard's exchange principle teaches how everything that comes in contact with something else leaves traces of itself behind and takes traces of what it has contacted. Anyone who's seen TV shows like "CSI" knows how useful trace evidence, like hair and fiber, is for helping identify criminals; hackers might leave behind virtual traces that serve the same purpose.

Occam's Razor teaches that the simplest answer is usually the right one, reminding us not to speculate, but let the data speak for itself.

Industry wisdom Pogue dubs the "Alexiou Principle" (named after its creator Mike Alexiou of IT infrastructure services provider Terremark Worldwide, Inc.) reminds us to ask ourselves: What question are we trying to answer? What data do we need to answer it? How do we extract that data? What does the data tell us?

Each element influences the plan, which lays out the goals of the investigation (you can't find what you're looking for if you don't know the goals), explains what success looks like and ensures that you (as security investigator) and your client (the compromised organization) are in agreement on them. The plan, says Pogue, is the most important part of the investigation. "You can't just say, 'find the bad guy stuff' and walk away… If you blow it, the entire case could be in jeopardy."

The first thing to do, he says, is determine what is "normal." Everything else then becomes abnormal and subject to scrutiny, providing new questions to be answered ("good old-fashioned leads," he calls them).

DON'T TWIST THE DATA TO SUPPORT A THEORY; RATHER, THEORIZE BASED ON THE DATA.

As you go along, everything must be documented. As my high school math teachers used to say, "Show your work" and note the results. All of your work, even if it provides negative results, must be documented, so, if necessary, the entire chronicle can be used as evidence in court.

If you're really lucky, you sometimes get to review a system while it's still under attack. Though you should grab a forensic image of the machine, Pogue says that data gathering on what is in effect a live crime scene can be critical in identifying exactly what the attack is trying to do and in tracking down the bad guys. "The attacker may still be present," he says, "and the malware is in its original state." Use trusted tools (Pogue says there's no such thing as a "court-approved" tool) and know what traces each tool may leave so you're not led astray by its footprint.

The customer, or system owner, is another source of information. Who knows better what a system is supposed to be doing than the people who set it up? The owner is also best able to define normal, including the connections that must be made and the ports and processes that must be running. If, for example, an investigator sees an open connection to North Korea, the system owner should be able to confirm whether or not it's legitimate.

Pogue says investigators can find evidence of mischief in all sorts of unexpected places. Even a seemingly legitimate process can be suspect if it's being run from the wrong location. On a compromised ATM, for example, he discovered network processes initiated by malware stashed in the recycle bin; legitimate software does not run from the recycle bin.

Log files, if present, also provide clues, even if the intruder only deleted or altered them. Logs can show what user ID logged in, at what time, from where, and what it did. Pogue says the system registry in particular is a goldmine; it can be examined on a live system and parsed with forensic tools like RegRipper.

Shadow-copy volumes (or restore points) are another source of clues. They record major changes to the system and can help investigators determine when a system was compromised and sometimes how. They even include registry changes. Parse them with a tool like RipXP, a subset of the RegRipper suite for examining registry data in Windows XP restore points.

Where else should investigators look for evidence? Dumping system memory for a real-time peek at everything from running processes to user credentials, encryption keys, and in-use files can provide more information about what mischief has occurred; a tool like MANDIANT Memoryze would be beneficial.

Finally, says Pogue, you, as investigator, should bring all these clues and data together, then restate the goal of the investigation. Your conclusions should support it. Be specific about your data and how you acquired it, so anyone can reproduce your results if necessary. Say exactly what you did and why, what results emerged, and how they supported the goal of the investigation. Don't twist the data to support a theory; rather, theorize based on the data.

"Sound conclusions are indisputable," Pogue says, and can help identify some of those suspicious lumps lurking under the corporate rug.

Lynn Greiner (lynng@ca.inter.net) analyzes the business of technology from Toronto.

DOI: 10.1145/1655737.1655740