

“You need to pull apart all the little pieces, add up the puzzle. It’s like being a detective.”

—CINDY JENKINS,
security engineer, UW Medicine

From all indications, something bad had happened. After installing an intrusion prevention system, the security team at UW Medicine spotted several machines trying to communicate with an IRC botnet server in France. Cindy Jenkins, a security engineer and computer forensics expert at the medical and research organization, immediately went on a hunt for clues behind the suspicious activity.

Hours spent combing through images of the hard drives from the infected PCs turned up the attackers’ tools: an IRC bot, a rootkit and an FTP server. Passive network scanning detected more compromised systems. To save time, Jenkins made hash sets—digital fingerprints—of the malware so she could look just for the hash sets when inspecting additional images. She determined the machines were infected 18 to 24 months earlier—before the IPS and other security measures were installed.

It appeared that UW Medicine, part of the University of Washington, had been attacked by resource hogs—intruders who don’t target data but exploit the speed and ample storage of university networks in order to share movies and music. But then she discovered something that didn’t match the original hash sets. The attackers had done more than steal resources; they had accessed the password file for UW Medicine’s Windows domain.

DON’T TRAMPLE EVIDENCE IN A BREACH. MISSTEPS IN AN INVESTIGATION WILL COST YOU IN COURT.

BY MARCIA SAVAGE

CSI for the CISO

“I pretty much stopped breathing there, then lit up the phone tree,” Jenkins says, recalling her startling discovery in December 2005.

Although there was no evidence the intruders had used the passwords, time stamps indicated they had accessed them. The case was turned over to the FBI, along with Jenkins’ carefully documented work.

“Forensics is a lot like coding. You have to have very strong concentration and you have to be able to think analytically,” says Jenkins. “You need to pull apart all the little pieces, add up the puzzle. It’s like being a detective.”

While CSI-style forensics are splashed all over today’s TV screens, cybersleuths like Jenkins are quietly using technical savvy to track down digital criminals. Computer forensics is more important than ever in the enterprise as organizations battle increasingly sophisticated attackers in cyberspace and the ever-present insider threat. Yet companies can be caught off guard after an incident and make costly mistakes when it comes to a forensics investigation.

“Corporations are often their own worst enemy. They only think about being ready for forensics after the fact,” says Bob Hillery, co-founder and senior security analyst at Intelguardians, a provider of digital forensics and other security services.

From what he’s seen, many businesses don’t have their environment forensically ready. They’re not logging system

activity and they don’t have an incident response plan. When something does happen, a system administrator clatters away at the keyboard to figure out what’s wrong. “Because they don’t recognize what the problem is, they start stomping around. They’ve essentially been over the crime scene in muddy boots,” Hillery says.

So how does an organization avoid such missteps? With forensics needed for civil litigation and human resources investigations in addition to criminal cases, experts say organizations need to ensure they’re prepared and that evidence is preserved. Having a strategy for what you’ll do when something does happen is the first step.

AVOIDING PITFALLS

If there’s an intrusion—from outside or by a malicious insider—an organization should have a response plan and a team of IT, management, legal and HR representatives ready to take charge. Those on the front lines—typically the IT staff—need to know whom to call and the first course of action, says Chris Beeson, FBI supervisory special agent and director of the Silicon Valley Regional Computer Forensics Laboratory in Menlo Park, Calif.

For the most part, he recommends taking a suspect machine offline to block an intruder from further access. Any disks needed for evidence must be duplicated. If the system is connected to a massive amount of storage, how-

CHALLENGES

COMPLEXITY HINDERS INVESTIGATIONS

Mobile devices and monstrous hard drives are giving specialists fits.

Multiple types of computing devices, bigger hard drives and increased use of encryption are making the job of a digital forensic examiner tougher than ever.

“Go back seven years or so, all forensics in the business world was based on PCs. It was very simple,” says Luther Martin, security architect at vendor Voltage Security. “It’s a lot more complex today. Now you have PDAs, cell phones, BlackBerries, iPods—all which contain potentially interesting data.”

An investigation usually starts with a single system and grows to wherever evidence may reside, which can include

digital cameras, USB drives and even printers, says Brian Gawne, managing director of forensics at risk management firm Veritas Global. But the bigger challenge in forensics today is the sheer size of hard drives, he says.

“You’re seeing hard drives from desktops and laptops that are 400 gigabytes and growing,” he says. “So the amount of data we have to parse through is ever mounting.”

The 14 Regional Computer Forensics Laboratories across the U.S., which are jointly operated by the FBI and local law enforcement agencies, processed a whopping 2.8 petabytes of data last year.

“With disks getting as big as they are, we’re trying to find ways to work smarter, not harder,” says Chris Beeson, FBI supervisory special agent and director of the Silicon Valley RCF. “The days of being able to go through

every sector on a drive just don’t exist.”

One way investigators can work smarter is by tapping databases with hash sets of known software files; the hash values allow them to reduce the number of files they need to inspect, Beeson says. One such database is the National Software Reference Library, a project supported by the U.S. Department of Justice and federal, state and local law enforcement.

But encryption can pose a big problem for investigators. Attackers are encrypting files and stripping out references, which makes analysis harder, says Evan Wheeler, senior consultant in charge of forensics at IT services firm Akibia.

“Encryption can slow us down and stop us in our tracks,” Beeson says. “It just depends on the amount of resources we can plug into that case.”

—MARCIA SAVAGE

ever, a company will need to weigh whether it's worth duplicating everything—and taking a system offline for hours—or only certain areas, Beeson says.

"There's no one-size-fits-all way of dealing with this from a corporate standpoint," he says. "You'll want well-trained, smart people making those decisions, along with legal counsel."

Many forensics experts say it's best if organizations train their staff to take a hands-off approach in order to preserve evidence.

"If they suspect that they're going to do forensics on anything, be it a server or a laptop, the first rule is don't touch it," Jenkins says. "Stop and call someone in who knows what they're doing, whether it's internal or external resources."

Forensic examiners look at when files were last changed or accessed to put together a timeline of events, says Evan Wheeler, senior consultant in charge of forensics at IT services firm Akibia. "If someone starts poking around, they will change all those values."

A common mistake companies make is turning off or rebooting a computer, which can destroy evidence stored in memory. "If you have an immediate crisis, don't shut things down. Unplug them from the network and leave them running," says Ames Cornish, managing partner at consultancy Montebello Partners.

Another frequent blunder is giving the laptop of a former employee immediately to a new hire, stymieing any investigation of possible wrongdoing on the part of the ex-employee. If the circumstances are odd when an employee leaves, such as an abrupt departure or a firing, it's best to hang on to a computer for a while before repurposing it, Cornish says.

An investigation is certainly more difficult if evidence is tampered with or lost, but not necessarily impossible. "Part of what a clever investigator can do is find copies of it in other places," Cornish says. "But often it gets overwritten and it's gone or your costs of recovering it start to go way up."

LOGGING

Today's digital forensics involves more than just laptops and desktops; investigators need to look at network and communication data, making logging essential. But Intel-guardians' Hillery says he often gets a blank stare when he asks for logs, the lack of which impedes an investigation.

Late last year he dealt with a case involving a small online company in which two former employees—the CFO and the senior developer—conspired to steal intellectual property in order to launch a competing firm. The client company also suffered a cyberattack—possibly launched by the former developer—that knocked down its Web site for a few hours and disabled a shopping cart function.

But proving an incident occurred was impossible with just a hand-drawn network diagram and some Web access logs but no firewall, router or IDS logs. Ultimately, the company dropped any hope of obtaining restitution in court and went back to business—along with the new competitor.

"The original company said, 'Oh the heck with it, we weren't prepared,'" Hillery says.

David Lang, director of information assurance and forensics at risk management firm Abraxas, also often encounters a lack of logging when investigating intrusions. System administrators tell him they turned off logging because it slows things down too much. "It's going to cost you some system performance to have logging turned on, but if it's a critical system, that's a risk management decision you need to look at," Lang says.

CHAIN OF CUSTODY

A big part of forensics is carefully documenting how evidence is handled so it can be presented in court. Without a chain of custody, lawyers can allege evidence was tampered with and prevent a successful prosecution.

"Every decision and every single step you take in forensics, you document it," UW Medicine's Jenkins says. "What you did, why you did it, what time you did it, and what effect it may have."

If an organization is going to do the forensics in-house, it needs to have a procedure employees can follow that details how evidence will be copied and transferred.

"That's the mantra of forensics. You're preserving data, documenting, and proving it didn't change during your investigation," Jenkins says.

Kevin Mandia, president and CEO of Mandiant, which provides forensics and other infosecurity services, says chain of custody is maintained by the following steps:

- Keeping evidence within an investigator's possession or sight at all times
- Documenting the collection of evidence
- Documenting the movement of evidence from one investigator's custody to another's
- Securing the evidence appropriately so it cannot be tampered with.

Besides the chain of custody, it's important to create hash values for a piece of evidence, says Bill Spornow, a consultant and former director of infosecurity, investigations and incident response at Experian. Creating hash values "substantiates the fact this is what it was on Monday, and when we show it to the court six months later, it's still the same thing," he says.

Forensics investigators typically make copies of a compromised system or other evidence and perform analysis on one of the copies. Jenkins usually makes three copies and puts the original system in an evidence bag for safe storage.

Courts will also accept evidence that is produced in the normal course of business, Spornow says. For example, if a firewall administrator routinely examines logs on a daily basis and sees evidence of a hack, those logs will be considered a normal business record.

"THERE'S NO

**ONE-SIZE-FITS-ALL
WAY OF DEALING WITH THIS FROM
A CORPORATE STANDPOINT.**

**YOU'LL WANT WELL-TRAINED,
SMART PEOPLE MAKING THOSE DECISIONS,
ALONG WITH LEGAL COUNSEL."**

—CHRIS BEESON, supervisory special agent, FBI



GETTING HELP

While some organizations have in-house resources to conduct forensics examinations, many need to call in a consultant. Resources for finding an expert include professional associations, forensic tool vendors, and certification providers such as the SANS Institute, which lists online those who have earned its GIAC forensics certification.

But there are no hard-and-fast rules for evaluating forensic experts. Certifications can be one means of assessing skill—there are vendor and vendor-neutral certifications available in the field—but hardly the only measure. In fact, Mandia says in his work, reputation and experience weigh more heavily than certifications.

“It’s more important that you’ve been involved in a lot of cases,” he says.

Forensics investigators use a number of different tools—commercial, open-source and custom—depending on the job at hand, so it’s tough to judge them based on the tools they use. “I don’t think there’s any one tool set that guarantees proficiency,” says Montebello’s Cornish.

“You need someone you can trust,” he adds. “Someone who has knowledge of IT systems, who’s not going to walk around like a bull in a china shop, and understands you have a business to run.”

When Spernow interviews candidates for organizations’ in-house forensics teams, he looks for people with an in-depth understanding of network architectures and how syslog environments function. “So they have a rounded picture of what a corporate infrastructure looks like.”

For her part, Jenkins is well versed in multiple platforms—Unix, Windows and Macintosh—and uses multiple tools including Guidance Software’s EnCase and Helix, an open source Linux-based bootable live CD. She has the EnCase forensics certification and a SANS incident handling certification. Master’s degrees in ancient history and library science also prepared her well for her job, she says.

Building an in-house forensics team makes sense for some organizations, particularly large ones. Boeing has handled computer forensics in-house for years because it was cost effective, says spokesman Tim Neale.

In a 2004 presentation, Spernow estimated that a forensics lab with one analysis system cost \$156,110, including personnel. A lab with 10 analysis systems cost \$388,640. Outsourcing costs can range from \$33,200 to \$55,100 for one event and from \$332,000 to \$555,100 for 10 events. Those estimates remain on target, he says.

“Depending on how big you are, the economies of scale come into play pretty quick,” he says.

CASE STUDY

TRACKING AN INSIDER

A former employee left many traces as he hacked his company.

The investigation began like any other, with a phone call. A high-tech company believed an intruder had broken into its network.

“The first step I took was to find out as much as I could. ... That involved asking them for their logs and anything they could provide me that could lead us to what actually happened,” says Shelagh Sayers, FBI supervisory special agent.

Like other agents investigating computer intrusion cases, she sat down with company officials, asked a lot of questions and inspected computer logs for anomalies.

In the end, the case didn’t require complicated forensics, Sayers says. Roman Meydbray, a former network

administrator of Creative Explosions, a Scotts Valley, Calif.-based software company, had broken into the firm’s computer system.

According to federal court records, Meydbray gained unauthorized access into the network from his San Jose home within two weeks of being fired in 2003. He deleted an email server domain, accessed the company president’s email account, and made configuration changes to the mail servers that caused emails to be rejected.

Court documents cite evidence that proved the case: ISP records linked the intrusion to Meydbray’s IP address; his computer, which was seized from his home when officials executed a federal search warrant, indicated his access of the president’s email and deletion of the email server domain; and company logs confirmed his IP address was used to access the president’s unopened email. He pleaded guilty to one count of unlawful access to stored communications and one count of unauthorized

access to a computer and recklessly causing damage.

Sayers says companies need to have a plan in place before an incident occurs, including having logging enabled and policies on revoking employees’ access upon termination.

Also, a business shouldn’t assume the investigator it calls to an incident is going to be an expert on its network, she says. “You’re depending on someone knowledgeable to tell you how their network architecture is set up or what particular items in a log might mean.”

In the Creative Explosions case, like most other computer intrusion cases, FBI agents didn’t shut down the business during their investigation, Sayers says.

“We work extremely hard with the victim company to not further victimize them. We’ll take every step to ensure their business is not interrupted,” she says. ▶

—MARCIA SAVAGE

The updated Federal Rules of Civil Procedure are making an internal forensics lab a valuable asset for controlling future litigation costs, Spernow says. The new e-discovery rules require that parties in a lawsuit be able to articulate where in their infrastructure they have data relating to the case, provide estimates for the cost of extracting that data and criteria for filtering out privileged information.

“The identity of the data is something that anybody in IT can do, to show where it lives,” Spernow says. “But extracting and filtering it based on privilege becomes a forensics issue.”

THE LAW ENFORCEMENT DILEMMA

Deciding when to call law enforcement after a breach can be difficult. It usually involves weighing a lot of factors—whether there’s criminal activity suspected, the extent of damages and risk of public disclosure.

While law enforcement can have great resources to track down culprits, an organization essentially gives up control of an investigation when it calls for official help, Spernow says. Plus, there’s the risk that corporate “jewels” could end up revealed in a court case.

The FBI’s Beeson says an organization should have a good idea of what happened and its losses—estimates of downtime, personnel and lost business—before calling law enforcement.

“We don’t have the resources to open a case on every sin-

gle computer intrusion reported to us,” he says. “Sometimes we have to tell the victim, ‘Your losses just aren’t substantial enough for the FBI to be involved.’”

Federal law requires a loss of \$5,000 in computer intrusion cases, but federal prosecutors often raise the threshold much higher, he adds.

LESSONS LEARNED

Besides having an incident response plan and preserving evidence properly, Jenkins says it’s important for an organization to learn from a breach.

Since the breach three years ago, which remains under FBI investigation, UW Medicine boosted its security dramatically. In addition to stepping up network monitoring with a Tipping Point network-based IPS, it also implemented host-based IPS/firewall systems and banned IRC and other peer-to-peer traffic.

“The biggest thing is to be prepared, know your decision trees and when it comes to forensics, hands off until an expert is there,” Jenkins says. ▶

Marcia Savage is features editor of Information Security. Send comments on this article to feedback@infosecuritymag.com.

GET MORE ONLINE | Step inside a forensics lab at www.searchsecurity.com/forensics.