

No Stone Unturned, Part Three

H. Carvey 2002-04-30

No Stone Unturned, Part Three

by H. Carvey

last updated April 30, 2002

Introduction

This is the third installment of a five-part series describing the (mis)adventures of a sysadmin named Eliot and his haphazard journey in discovering "the Way" of incident response. As we left off last time, Eliot had just begun compiling a list of tools that would be helpful in incident investigation when he was interrupted by a call from Dave, a sys admin with a branch office on the West Coast. Dave had asked for Eliot's assistance with an apparent incident. Now, having begun an investigation, Eliot was baffled and had asked Dave for some clarifying information.

Part III

Eliot pondered Dave's response for a long time. Why would Dave have said that he'd found "a ton of failed log-ins" to his servers, yet only have this relatively few to show for it? His e-mail included only the three EventLog entries he'd retrieved. On top of that, Dave seemed to have decided not to simply extract the EventLog entries in text format, but rather open the entries in the Event Viewer and make screen captures. This made for three very large bitmaps as attachments to his e-mail.

Eliot decided to call Dave again, and ask him about the situation, rather than play "e-mail tag" throughout the day. Dave answered on the second ring.

"Yeah?"

"Dave, it's Eliot. I need to ask you a couple of questions about the failed log-ins you sent me."

"Sure. Shoot."

"Well...uh...first of all, I guess I'm a little confused. I thought you'd said there were several entries, but all you sent me were three entries from two servers."

Dave was quiet for a moment. "Yeah, that's all there was."

Eliot paused, considering how best to ask the next, obvious question. "Well, I guess I missed something along the way. Why would you tell me that there were a bunch of failed log-in attempts, when there were in fact only these three?"

Dave's response came quickly. "I saw the EventLog entries and thought the servers were under attack."

Eliot noted a palatable increase in the tension in Dave's voice. Something in the bitmaps he was looking at on his monitor captured his attention, and a thought leapt into his mind. "Dave, you called me yesterday at about 4 PM my time, making it around 1 PM your time, right?"

"Yeah, I guess."

"Well, according to the screen captures you sent me, these failed log-ins all occurred just before 9 AM, your time. Are the system times accurate?"

"Yeah, I guess so."

Eliot found himself in a fairly awkward position. Dave was obviously trying to do well, and had incorporated some of the things Eliot had suggested. Yet, there still seemed to be a long way to go with regards to really understanding, reporting, and handling incidents. Eliot decided that the best thing was to be direct.

"Dave, if you felt you were under attack, why was it four hours before you said anything to me?"

It was quiet on the other end of the phone. Eliot felt he'd made his point, and wanted to break the tension. Eliot didn't want to scare Dave off from ever looking at his EventLog entries, or reporting an incident, again.

"Forget it, Dave. The point is that you found the entries and you did something."

"Yeah, I know. I looked into it, but I haven't found anything yet."

This caught Eliot by surprise: "You looked into it? What did you do?"

"After I sent you the e-mail, I wanted to see what the user was up to. I thought maybe he was trying to hack my servers, or he had a virus of some kind, like Nimda, that was trying to map drives. So I mapped the user's drive and checked out some files. I haven't found anything yet."

Eliot thought for a moment: "What do you mean, Dave...What did you do?"

With that question, Dave seemed to open up a bit, as if he'd been asked to present his technical skills and show how adept he was. "After I mapped his drive, I wanted to check out some files. Since we use Eudora for e-mail, it was pretty easy to copy the files for his mailboxes and check them out. I read through it and didn't find anything, just some business and personal junk. I copied his entire attachments directory to my hard drive, and scanned it with anti-virus software. I didn't find anything, so I copied a couple of other directories, and still didn't find anything. There weren't any macro viruses in the Word and Excel documents I found, so it might not be a virus. I scanned his machine with a port scanner, and found a couple of odd ports open, so I checked them against a list of trojan ports I found on the Internet."

Eliot took a deep breath and held it. He didn't want Dave to know how disappointed he was. He couldn't believe what he was hearing. It was as if Dave had gone off and conducted this "investigation" of his without thinking about the possible consequences of his actions. Eliot couldn't help but think if this incident did involve malicious actions from this user, Dave's actions were tantamount to spoiling a crime scene. Eliot's next thought was to try to find out as much about what Dave had done, and try to salvage the situation.

"So, did you find any trojans or anything?"

"No, I haven't found anything yet. It's funny, too, because he's got a couple of open ports on his system that aren't the normal NetBIOS stuff, but none of the files I've copied and scanned show any signs of being backdoors or anything."

Eliot thought for a moment. "Dave, what makes you think this guy has a trojan or virus or anything on his system?"

Dave paused for a moment. "Well, there's the open ports thing, and the failed log-in attempts on my servers. The only other thing it could be is that he's trying to hack into my servers."

"Okay, Dave. Let me get back to you on this. I'll check it out. Just don't do anything else without checking with me first, okay?"

"Sure, Eliot. No problem."

Eliot thought for a moment after ending the call with Dave. Then he decided to give the system administrator for that office a call. He looked up Ed's number in the company directory, and dialed. When Ed picked up, Eliot made some small talk, and then got to the point of the call.

"Ed, have you had any problems with one of your users?"

"Problems? Like what?"

Eliot told Ed about the incident he'd discussed with Dave.

"No, we haven't had any viruses or anything like that. We did have some fun with some spyware that one of the marketing guys downloaded and installed, but I keep updated copies of tools that find that stuff on hand."

"Ed, could I get you to do me a favor? Could you go check out the user's system, and run a scan with the latest anti-virus definitions?"

"Sure thing, Eliot. Let me check it out and I'll give you a call back. I want to take a look at these open ports myself."

"Thanks, Ed. Let me know if you find anything."

By now, Eliot craved the thing he needed most. Coffee. Hot coffee. He pushed his chair back away from his desk and stretched. After sitting for so long, moving was difficult, almost painful. Maybe it was the tension. He couldn't believe what Dave had told him, but he didn't want to think about it for a while. His body was craving caffeine. As he stepped out of his office, he was struck by an intense flash of pain. He realized that it was just normal lighting, and that he'd been in his cave for a little to long. He moved down the hall with his fingertips lightly brushing the wall to his left, and used his coffee cup like a blind man's cane. Eventually the pain and white spots faded to reveal that he was about two feet from the coffee urn...and Cynthia.

"Hey, Cynthia, how're you doing?"

"Eliot! Are you okay?"

"Oh, sure. I've just been sitting in my dark hole of an office for far too long."

"Poor boy! You need to get out more."

"Yeah, I know. Hey, let me ask you something. Do we have any kind of policy that says it's okay for duly authorized representatives of the company to monitor a user's computer?"

Cynthia thought for a moment. "No, we don't have a consent to monitoring policy for the employees."

"What about a computer use or acceptable use policy, or a privacy statement?"

"No, we don't have any of those. Well, not officially. The HR Director took our input and sent them up to corporate a couple of months ago, but I think they're still sitting on Corporate Counsel's desk."

"So, basically, what would happen if we checked out an employee's computer and he ended up getting fired based on what we found?"

"Well, I'm not a lawyer, but there have been case studies in the HR journals where the terminations in cases like that have been ruled wrongful, and the former employee awarded quite a bit of money. But I guess it really depends on the case, and what a lawyer says."

Eliot hesitated. "I thought so. I remember reading something like that on the Web, but I didn't remember the specifics." Eliot's mind was reeling with the implications of Dave's actions. In fact, it was now even possible that Dave would be in some sort of trouble if Eliot were to tell anyone what happened.

"Why do you ask?"

"Oh, nothing in particular. I was just talking to another system administrator about some activity on the network, and it turns out someone might have looked at files on another user's

hard drive.”

Cynthia seemed to wake up and become more alert. She looked at Eliot long and hard for several moments, and then said, “Well, if you find out anything specific, let me know. We can’t just have users looking at other user’s hard drives. Also, anything affecting employees directly, especially anything that may lead to termination, needs to be brought through HR. Whatever it is, it may also need to go through Legal Counsel, if it might cause the company to incur liability.”

“Uh, sure. Okay.” Eliot was even more nervous about what he’d discussed with Dave, and decided to shift tracks. “On a completely different note, do you know Dave Campbell?”

“Oh, yes, he’s another one of our administrators. I remember him because he was hired from the police force. It seems he was pretty good with computers and got some of the Microsoft certifications before he stopped being an officer. I think he’s got a degree in criminal justice, with a minor in computer science.”

“You mean he was a cop?” Now Eliot was really confused. How could someone who’d been a police officer, and was trained in the handling of evidence, take the actions Dave had?

“Yes, he was. As a matter of fact, he was a police officer for about six years.”

Things just kept getting more and more interesting for Eliot. So Dave had been a cop, eh? If that was the case, and he had all of this experience and education, Eliot thought to himself, wouldn’t it stand to reason that Dave would also understand things like searches and rules of evidence?

Eliot was back in his office and going through e-mails when his phone rang. It was Ed calling back.

“Did you find anything?” Eliot asked.

“Not on the user’s computer. I updated his anti-virus definitions and ran a scan. The drive came up clean. I even checked out the ports on the system, and didn’t find anything.”

“What did you do to check out the ports?”

“Well, I started with the usual netstat output, then grabbed the process list with pslist.exe from [SysInternals.com](http://www.sysinternals.com). Then I used [FoundStone's](http://www.foundstone.com) fport.exe to get the process-to-port mapping, and finished up with SysInternal's listdlls.exe. The cool thing about listdlls is that it gives you the full path and command line used to launch the process, so you can pretty much tell whether the process is legit or not. I even ran `pu`list from the Resource Kit to see who owned the processes. After all that, I had a pretty good snapshot of what was happening on the box, and to be honest, there just wasn't anything out of the ordinary.”

“What about the open ports?”

“Just client ports used by the browser and RPC on the system, that's all.”

“So you didn't find anything then.”

“Well, now, I didn't say that. While we were running the anti-virus scan on the system, I chatted with the user about what he'd been doing, and I think I solved your little mystery.”

“Really?”

“Yeah. We'd had a problem with one of our printers, and the user was browsing the domain looking for a printer. Unfortunately, he really didn't have much of an idea of what he was looking for. But that accounts for the failed log-in attempts, right down to the timeframe.”

“Ah, okay. That makes sense. Thanks for your help.”

“No problem. You need anything else, let me know.”

So that was it. Ed had found the problem, and hadn't had to rifle through the files on anyone's hard drive. Eliot figured he better give Dave a call back before anything else happened. When he got him on the phone, Dave seemed a little distracted. Eliot figured he'd cut to the chase and just let him know that the mystery had been solved, but Dave didn't react with anything he could call interest. So Eliot thought he'd try to draw Dave out with small talk.

“So you used to be on the police force, eh?”

"Yeah, I used to be a cop."

"So what did you do?"

"The usual cop stuff. Tickets, domestic stuff. Nothing with computers, though."

"So what got you into administering systems?"

"I was always interested in computers, and I got my minor in computer science. This seemed like something interesting to do."

"So I guess you know about how to conduct investigations and gather evidence then."

"Yeah. Why?"

"Well, I was just thinking that when you found those failed log-in attempts, you sort of reacted in an un-cop-like fashion."

"Oh?" Eliot immediately regretted what he'd said. He could almost hear Dave clamming up again.

"What I meant was that if something really had been going on, you'd be the first one who'd want to preserve evidence. You know, preserve [MAC times](#) from files, that sort of thing."

There was a pause on the other end of the line. "Uh, yeah, I guess I should have thought of that. But I just wanted to find out what was going on, in case someone was hacking into my server."

"But no one was really hacking anything."

"Yeah, but I didn't know that at the time."

"Okay, hold on a second." Eliot had a point to make, but he also wanted to diffuse the situation. After all, there was no reason to alienate Dave, or worse yet, make an enemy of him, but he wanted to make his point.

"Dave, you had three failed log-ins across two servers, and you waited four hours before saying

anything. It couldn't have been that important."

"Look, I thought someone was trying to hack my servers. I started to look into it, but something else came up."

"So what made you decide to map the user's drive and look through his files?"

"I thought he might have a virus or something."

"Okay, I got that. But now, instead of having a situation where a user was hacking or had a virus, we've got a situation where a system administrator abused his power, and violated a user's privacy."

With that, Eliot couldn't even hear Dave breathe. Eliot got the feeling that maybe his point had been made.

"So, what're you going to do?" Dave finally asked.

"Look, from now on, if you find something unusual, call me before you do anything else, okay?"

"Yeah, sure. No problem."

With that, Eliot figured he done his good deed for the day. He'd also done a lot of thinking about how not to run an incident response investigation. He realized that steps had to be taken to preserve potential evidence when approaching an incident, and that some of the things that could be done, such as port scanning a system from the network, were exercises in futility. Eliot also realized that whatever tools he used, he had to keep two things in mind. One was to be aware of how the tools he used worked, and the other was to have a plan when approaching an incident. It was better to think things through ahead of time than to make serious mistakes in the heat of the moment. With that, Eliot decided to continue his search for tools and utilities, and to develop and document a methodology.

Next Time

In the next installment of "No Stone Unturned", Eliot conducts an investigation of his own. Stay

tuned.

To read Part Four of this series, please click [here](#).

Relevant Links

[No Stone Unturned: Part One](#)

H. Carvey, SecurityFocus

[No Stone Unturned, Part Two](#)

H. Carvey, SecurityFocus

[No Stone Unturned, Part Four](#)

H. Carvey, SecurityFocus

[Privacy Statement](#)

Copyright 2006, SecurityFocus