

Episode Three: From Out of the Blue

Robert G. Ferrell 2000-12-06

Chasing the Wind Episode Three

From Out of the Blue

by *Robert G. Ferrell*

last updated Dec. 6, 2000

It was just after two o'clock in the morning, local time, when the logging daemon of the facilities department workstation recorded a remote login from a dialup account over two thousand miles away across a sleeping nation. The connection was made using a legitimate user ID and password, so there wasn't much to be done but to allow it and get on with business. The firewall didn't even blink; it was an unfiltered port.

Ian was taking no chances. He had made a checklist this time, just to make sure that in the excitement of the kill he didn't forget one of the critical concealment steps. He followed it to the letter. The last part of it looked something like this:

1. Disable auditing (auditpol /disable)
 2. Clear event logs (elsave -s \\facwks01 -l logname -C)
 3. Check logs with event viewer to make sure
-

Jake was wandering along a path in a campground he visited often as a young boy. The woods were familiar, as was the gurgling of the nearby brook, but something was a little...odd. The trees seemed to be moving around, some of them even pacing him as he walked. Also, there were things in the branches that he couldn't identify; they, too seemed to be moving with him. Jake was a little disturbed by this, but somehow it didn't seem to be particularly out of the ordinary. He rounded a corner and was surprised by a small gazebo in a clearing he didn't remember seeing before. As he approached, the gazebo suddenly disgorged a brass band, complete with brightly colored uniforms. They marched up to him in neat ranks and began to play. Rather than a big, bold marching tune, however, what blared forth from their shiny bells was an incongruous Bach minuet. Stranger still was the fact that the music sounded not at all as though it came from brass instruments. No, it had a simpler, more mechanical quality to it. Almost electronic...

Jake snapped awake in his darkened bedroom and was instantly disoriented. Things weren't where they were supposed to be. What was that over his face? And what was that weird piercing music he could hear drifting through the air? It took a few moments of thrashing for him to realize that he had pulled the comforter up over his head and piled pillows on both sides of himself to build a sort of bunker. Once free of this impediment, he could finally reach over to the night table and grope for the thing that had awakened him. It was his pager. He struggled to a sitting position and stared through blurred eyes at the backlit display. It read:

```
8 NOV 02:28:34 [TRIPWIRE] CHECKSUM  
MISMATCH DETECTED ON FACWKS01
```

Jake blinked uncomprehendingly for a couple of seconds. His brain flipped through a few million mental database records looking for something that would make sense of this message. Finally it clicked: one of the files he had marked for monitoring by Tripwire had changed. He remembered writing a Perl script that would send this message to his pager in the event of an unauthorized system file modification. There is absolutely nothing more inconvenient, Jake thought bitterly, than a warning system that works.

He swung his feet over the side of the bed and growled to one of his cats, "This had better not be a false alarm." The cat remained noncommittal, in the immemorial manner of things feline.

Ian started dumping directory listings and mapping the network. He was determined to find a spectacular and newsworthy hack buried somewhere in the electronic jungles of Acme Ailerons. He zipped up all the gathered intelligence data and pulled it over to his Linux box. Moving slowly and carefully, following his checklist, he erased his tracks one by one until, at last, he started the program that would delete the final log entries, restore the original binaries, and then destroy itself. He did leave one small back door though; he knew that eventually someone would forward the trojaned email to the IT department, whose natural response would be to change everyone's passwords, thus cutting off his future access. Ian had far too much left to do at AA to allow that to happen.

```
cp nc.exe hidparse.sys:nc.exe
```

He also left a red herring in the system registry, just to throw off any pursuit. If it wasn't discovered, great. He'd have a backup copy. Just as he was about finished, a little red skull

popped up on his display. That meant someone had done something on the network that might indicate he'd been spotted. He didn't care what it was. He just shut down the connection immediately and started sending out a flurry of spurious packets from spoofed IP addresses as a smokescreen.

Jake sat in his underwear and a t-shirt at the computer terminal in his den. He connected to the remote access server at AA and turned on a sniffer located on a machine on the same subnet as facwks01. (The entire network was still shared 100 Mb Ethernet; one of his top priorities was to convert to switched, but that would require a hefty investment and a lot of justification.) He didn't touch the facilities machine at all, not even to ping it. There wasn't much to see at first but the kind of traffic you'd expect on a quiescent network at 3:00 A.M. - routine RIP packets, and the occasional ARP request. However, as he watched the packets scroll by, he noticed some TCP traffic to facwks01 with the FIN flag set. Bingo. Jake sat back and let the sniffer do its job, hoping he'd gotten there in time to snag something he could use.

About five hours later, Bob plopped down in the executive leather swivel chair in his office with an exceptionally large mug of coffee (like most CIOs, he had an entire shelf full of vendor-supplied coffee mugs) and punched the button to play back his voice mail. The first two messages were utterly mundane; one was a vendor who wanted make an appointment to demonstrate a new product (probably with a coffee mug as a reward), and the other was a message from himself not to forget his daughter's soccer game at 4:00 P.M. The third one, though, was a little less routine.

"Good morning, Mr. Briley; this is Jake. I got paged last night about a file integrity problem on one of the facilities workstations. I'm looking at the sniffer captures right now; looks like there might have been a remote compromise. I'll let you know as soon as I can. Cheers."

The time stamp was 3:23 A.M. Bob sat for a moment pondering this new menace, then decided there wasn't much point in worrying about it until Jake's full report came in; Jake was very thorough when it came to investigation and documentation. He sighed and pressed the "Continue" button on his voice mail panel. The next message caught him completely off guard. It was a man's voice, seemingly altered by some sort of electronic filter. It spoke only three words, slowly and distinctly: "Red Licorice Five." Bob grabbed the edge of his desk so abruptly

that he knocked his half-full coffee mug off onto the carpet, where it surrendered its contents without fuss and rolled quietly under a credenza. It was a long time before he even noticed.

Ian sorted through his ill-gotten gains cheerfully. He had email, proprietary documents, directory listings, and system configuration data to play with now. Somewhere in this mass of information there had to be a weakness he could exploit with sufficient drama and impact to force the BroadBandits to sit up and take notice. It was merely a matter of identifying and taking advantage of it. Time, he decided, was on his side, so much so that he felt a sudden strong urge to nap. The beast would still be here in an hour or two, waiting to be slain. He would slay it then.

Jake made it into the office at 6:30 A.M., although he hadn't intended to go in that early. He hadn't been very successful at getting back to sleep after the incident though, and felt that he might as well get a bit of a head start on what promised to be a long and eventful day. The first thing he did was to take the potentially compromised machine off the network, in case it was being used as a staging area for further illicit activity. Then he grabbed a notepad, portable backup drive and cables, and his largest mug of coffee and headed off to inspect the victim machine up close and personal.

The facilities workroom, where facwks01.acmeaileron.com was located, was not part of Jake's normal world, so he didn't have a key. While there were facilities folks on site 24 hours a day, finding any of them could be, well, a challenge. He walked up and down the hallways passing in front of and adjacent to the workroom, but saw not a living soul. Finally he stopped at a wall phone and called the front security desk.

"Security, Building One Entrance, A.P.S. McGregor speaking." The voice sounded, as well it might, a little sleepy.

"Good morning. This is Jake, the network administrator. I need to get into room 1F16. Can you send someone with keys down here for me?"

"Why do you need access to the facilities workroom?" McGregor asked.

"There's a computer in there that I need to, uh, work on." Jake was keeping the news of the compromise from as many folks as he could, per the new IT security policy.

"Work on," the voice echoed, a little suspiciously, "OK, Jake, hang on and I'll have a patrol officer there in a few minutes."

"Thanks," Jake replied, relieved that he hadn't needed to go into details.

The security patrol officer who showed up seven and a half minutes later was bigger than Jake, but seemed pleasant enough. After checking Jake's employee badge he opened the door and led Jake into the room crowded with work tables and tools. Jake went immediately to the area where the workstations were housed and found it behind a locked chain-link gate. "I wish our network were half as secure as the physical plant," he muttered under his breath. He turned to the guard.

"I guess I'll need this one unlocked, too." Jake braced for what he knew was coming.

"Control didn't say anything opening 1F16A. Only 1F16," replied the guard, a little stiffly.

Jake tilted his head a bit to the left and went into his 'patiently explaining things to morons' mode. "That's because I don't know the layout around here well enough to know that the computer I was after would be behind yet another lock. My equipment tracking database just says "Facilities Workroom, Rm. 1F16."

"I'll have to okay it with control," said the guard, doubtfully.

"Fine," replied Jake, "Can you do it soon?"

Jake eventually got into the locked area, and after a little poking around identified facwks01. He logged on with the admin password and dumped the entire disk image to his portable drive for archival purposes. He took the media out of the drive, sealed it in a plastic evidence bag and labelled it with the contents, time and his initials. Then he started the long post-mortem process by logging into another machine where he kept the Tripwire binary and the original checksums for the protected files on read-only media. He first looked at the files that Tripwire had reported changed. One of them was the Registry. Comparing the old Registry and the new version, he found only one small difference: the key `\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\netcat,`

contained the data

```
"C:\TEMP\NC\nc -L -d -e cmd.exe -p 9999."
```

"Got you, you little turd," Jake crowed in triumph. He deleted the key and the referenced directory with, as they say in the military, 'extreme prejudice.' He didn't know about the copy of netcat hidden in the NTFS file stream, of course...

"Come in, Bob," said Mr. Easton, the founder and CEO of Acme Ailerons, "have a seat." Bob sat nervously in one of the enormous stuffed leather chairs arrayed around the executive suite like exquisite sculptures in a formal garden. "What's on your mind?"

Bob cleared his throat. "Sir, I have something that might be relevant to our new DoD contract." Mr. Easton raised his eyebrows and nodded for him to continue. Bob squirmed a little and drove on. "This morning I received a rather disturbing phone message..." he tailed off, unsure how to proceed. The CEO looked at him expectantly and Bob noticed that he was tapping the index finger of his right hand. Bad time to stall out, he thought.

"Uh, sir, I don't know if you recall this from when I was hired, but my background before coming here was largely in the military intelligence field."

"Of course I know that, Bob," Easton replied, gently, "We all had to submit to that bloody security investigation before they would award the contract. I've got a dossier on every cleared employee right here in my computer. Tells me how many times you go to the bathroom every day and even," he chuckled, "which stall you prefer."

Bob smiled a little, relieved by Easton's sense of humor. "Well, sir, one of the projects I was assigned to involved, among other things, evaluating the security of various equipment located aboard the President's mobile command planes." He paused, trying to sort out what he was going to say next. "We had code words for everything in the service - that's an occupational fact of life in the intelligence community - and we could convey a lot of information with very few words that way." He paused once more, this time to take a deep breath. "I hadn't heard anyone speak in that code for almost five years until this morning. A man's voice, heavily filtered, left a message for me using the code phrase 'Red Licorice Five.'" He stopped, as though finished, and looked out the window.

Easton waited for a few moments, then asked, softly, "What does 'Red Licorice Five' mean, Bob?" Bob said nothing for a moment, but then he swivelled his eyes to meet Easton's and said, in a flat, cold voice, "Catastrophic threat to national security in this facility."

To Be Continued...

To read **Episode Four: Through a Glass, Darkly**, click [here](#).

Robert G. Ferrell, CISSP, is the Information Systems Security Officer for the National Business Center of the U.S. Dept. of the Interior. He is also active as a Perl Monger, an Internet Technologist, and a member of the Netwits. He has been involved with (primarily Unix) systems programming, administration, and security on and off since 1977.

Relevant Links

[Chasing the Wind Episode One: No Place to Hide](#)

By Robert G. Ferrell

[Chasing the Wind Part Two: Raising the Stakes](#)

By Robert G. Ferrell

[Subscribe to the Incidents Mailing List](#)

SecurityFocus.com

[Subscribe to the Focus-IH Mailing List](#)

SecurityFocus.com

[Privacy Statement](#)

Copyright 2006, SecurityFocus