

Episode Eleven: Fire and Brimstone

Robert G. Ferrell 2001-10-16

"What do you mean, you want to get in touch with the feds? Have you been eating moron sandwiches again?"

Ian sighed and paused to calm himself before replying.

"Look, dude, I just found some stuff that I think might be serious. It might be some kind of spy stuff. It's encrypted and being burst in small packet fragments at irregular intervals from a computer that isn't supposed to be there."

"So what? What business is it of yours? You can't get involved, man. They'll drop your butt in the Mitnick suite so fast you'll be able to watch time dilate."

Ian wasn't having any more of this.

"I don't need a lecture, I need a plan. I figure you're my best shot at finding someone who'll listen. Are you gonna help me, or do I let my fingers do the walking?"

The voice at the other end of Ian's phone was silent for a minute. "Okay, okay. At least I can keep you from being too damn easy to track."

Ian wasn't very happy about that negative assessment of his own stealth skills, but now was not the time to get dragged into another largely pointless dialectic.

"I'll ship you a PGP-signed doc with some chained remailer URLs and an email address where you can send the tip. Wipe, and I mean really wipe, the message when you're done with it. Don't screw this up or we may both regret it."

"Thanks a lot, dude," Ian rolled his eyes but tried not to sound annoyed. "You sure you've got my public key?"

"I'm sure. I'm looking at it right now."

"Awesome. Later."

"Later." Click.

Ian plopped the phone down and stared at the wall for a moment, absorbed in thought. He was beginning to realize that most of his so-called friends in the underground were self-serving little egomaniacs with no social consciousness. "What a prick," he mumbled.

Jake sat in the hotel restaurant eating the rather expensive meal he'd bought himself as a congratulatory gesture after winning the DOS challenge in his hacking class earlier that day. He'd taken advantage of a known bug in the network interface card of one of his classmates' workstations to render the LAN more or less unstable. Packets were dropped, nodes were kicked off the network at random, and in general data communications were hosed. While his solution wasn't one the instructor had anticipated, it fell within the rules as established for denial of service, and Jake was declared the winner. He got a tee shirt and another coffee mug. He also got bragging rights, which he valued far more highly. He couldn't wait to tell Deanna.

Douglas' late-night discovery caused quite a stir the next morning. In typical sparse Douglas fashion, he had reported it to the project leader in an email as follows:

```
Found bad parameter. Bellatrix now operational.
```

```
D.
```

It would take some time to reassemble all the luminaries who were supposed to witness the first full scale test. Meanwhile, Douglas was free to noodle around with the settings and make some preliminary runs. It would be a bad thing if anything went wrong with the second test, so he had to make absolutely certain everything was shipshape. This meant exhaustively reevaluating the effect of each parameter on the outcome of the run.

As he was conducting these rather tedious exercises, Douglas found himself pondering the larger consequences of their engineering achievement. They hadn't just built a super fast computer: they had created a time machine. They had also developed a reliable means of producing and manipulating entangled photons, each pair of which (theoretically) remained perfectly coordinated even when separated by vast distances or millions of years. Although

Acme Ailerons wasn't the first to achieve this latter functionality, they had by far the most efficient entanglement generator, and the shortest cycle time. The implications of this were only beginning to dawn on Douglas. They hadn't escaped the people who were funding Project Bellatrix, either.

Colonel William Briggs was in a bad mood. Not only had his request for increased security on Bellatrix been flatly denied, but the S.U.V. he had bought a year earlier because everyone else in his social set had one was proving to be an unreliable, gas-guzzling monster. He remembered with exaggerated fondness the little two-seater sports car he'd driven while he was stationed in Germany just after the reunification. The Autobahn, the crisp Black Forest air, the heady highway smells...

He'd just poured his second cup of coffee and was reading the security dispatches from the previous evening when his adjutant called. The Captain's voice was hollow and shaking. "You'd better turn on CNN, sir." Will wrinkled up his nose. "TV, this time of morning? Don't tell me the Rangers actually won a game." Something about his aide's reply made Will's stomach turn to jelly. "No, sir...You need to see for yourself." Will walked over to his office television and reached for the switch. He found that he had to will himself to press it. The first image he saw was a very tall, strangely familiar building with heavy black smoke pouring out of it. Even before fully understanding the situation, he sensed instinctively that something fundamental about his universe had forever changed.

The threat analysts at the super-secret Defense Intelligence Analysis Center are responsible for scrutinizing thousands of mostly nebulous bits of information every day. While there are various levels of machine screening of incoming data using some extremely sophisticated algorithms, in the end the final determinations of threat validity and severity are made by human analysts. After a couple of years in that job, the best analysts develop a sort of 'sixth sense' (which is in reality probably just a highly developed pattern-recognition acumen) for picking out significant threats from seemingly innocuous looking words and phrases. Analysts could assign a threat index to each event they examined, from alpha (no plausible threat) to delta (clear and immediate threat to national security). However, since any events labeled 'charlie' or 'delta' were forwarded to field agents for immediate action, analysts were under considerable pressure not to classify events in the top two categories unless they were absolutely convinced that a

definite threat existed.

The analyst who received the anonymous email skimmed it for anything really significant. It seemed to be classic paranoid geek babble about security flaws and foreign spies. While it mentioned a known Defense Department contractor facility, there were no references to any classified project names or details, just something about "data bursts" and encryption. She read it again, then clicked on the 'alpha' category, with a subcategory of 2 (threat unsubstantiated by evidence), and was about to hit the 'enter' key when her screen locked up. At the same time, the red ThreatCon Delta beacon began flashing high on the wall. She closed and locked the metal housing that secured her keyboard, as per regulations, and headed off to the briefing room. Another drill, she thought.

When she returned to her duties about an hour later, she was visibly shaken. She sank mechanically into the fabric-covered chair at her console and fumbled with the little silver key and seven digit code that restored access to her keyboard. It took her a few seconds to remember where she had left off. Her screen was now unlocked, and she reached for the 'enter' key again. As she did, however, she glanced once more at the message she had just classified as 'no threat' and her eyes came to rest on one detail she had somehow missed before.

The message sender had thoughtfully looked up the registrant for the IP address to which the encrypted data were supposedly being sent. It was Global Technical Products, AG, with an address in the Netherlands. Something about that corporate designation struck her as suspicious, although she couldn't immediately put her finger on the anomaly. She punched up an intelligence database on an adjacent system and did a search. Global Technical Products, AG, was considered a 'questionable' corporation, with some as yet unconfirmed ties to organizations the United States classified as "supporting terrorist activities." Yeah, well, this described half the companies in Eurasia. All you had to do was sell one wing nut to the mechanic who once fixed a car belonging to one of Yasser Arafat's lieutenants to get on that list; this wasn't enough to rate even a 'baker' classification in and of itself.

As she tapped her fingers thoughtfully on the keyboard wrist pad, the "AG" part suddenly struck her as the incongruity. AG was an acronym for *Aktiengesellschaft*, a German designation roughly equivalent to the American *Incorporated*. GTP was headquartered in Holland, however, where the same designation was *Naamloze Vennootschappen*, or "N.V." A minor point, to be sure, and possibly just some sort of clerical error, but it rang her alarm bell nonetheless. She reached for the mouse and moved her check mark from the 'alpha' box to one marked 'charlie.'

She had no concrete justification for this upgrade to "probable real threat" except a deep gut feeling that was likely at least partially the result of recent events. She was being paranoid, but 'informed paranoia' was, after all, her stock in trade.

She took a deep breath and sent the analysis on its way. She knew immediately that this was the right thing to do, paranoid or not. Sometimes instinct overrode all other considerations.

Baseball cap watched the horrific scenario unfolding on the American east coast with concern. He wasn't really bothered by the almost unimaginable destruction and loss of life--that was philosophically compatible with his own goal--but by the disruption this event was probably going to cause to his own operation. His organization had spent thousands of man hours training, infiltrating, and now harvesting. He was a highly proficient surgeon, skillfully extracting information of immense value from the bloated and decadent West with a deft scalpel. Now, just as things are going perfectly, some maniac comes along and attacks the surgical ward with a wrecking ball. Another two weeks and it wouldn't have mattered so much. The salient data from the project would be gleaned and the operation could be quietly shut down without detrimental effect to the cause.

Oh well, the damage was done. All he could do was ride out the storm and hope for the best. He ran his finger around the safety latch over the radio controller that would detonate the small explosive charges on the transmitters deep in the flooring beneath the Acme Ailerons secure facility computer room. Sooner or later he would press that button, but when that happened he needed to be in the car on the way to the airport. Of course, that would require the airport to be open. The uncertainty surrounding the time frame for the availability of his carefully planned escape route made him uneasy and angry. No one in his organization had warned him of this turn of events. Someone, somewhere, had failed him, and he would find out who if it was the last thing he did in this life.

Bob, Vijay, and a couple of senior vice presidents were holed up in a conference room in the secure facility. They were having a 'pre-meeting meeting' to agree on Acme's stance before the DoD officials arrived. Everyone at the table was still in a state of shock over the events of earlier that morning, but the ramifications of America's worst terrorist attack were already beginning to manifest themselves. Every military base in the area was locked down at

ThreatCon Delta. All non-military air travel was suspended indefinitely. The company's--the nation's--neatly arranged priorities had been scattered like leaves in a sudden violent September squall.

When the two Defense Department liaisons finally arrived, they wore ashen faces, grim with resolve. One of them handed a bright red envelope to Bob. He opened it slowly, reluctantly, as though it might contain anthrax spores. Inside was a solitary sheet of paper, with the letterhead of Col. William Briggs, USAF. On it was written a single arresting sentence:

Red Licorice Five confirmed.

To read **Episode Twelve: The Serpent's Tooth**, click [here](#).

[Robert G. Ferrell](#), CISSP, is a Systems Security Specialist in San Antonio, Texas. He is also active as a [Perl Monger](#), an Internet Technologist, and a [literary humorist](#). He has been involved with (primarily Unix) systems programming, administration, and security on and off since 1977.

Relevant Links

[Chasing the Wind Episode One](#)

[Chasing the Wind Episode Two](#)

[Chasing the Wind Episode Three](#)

[Chasing the Wind Episode Four](#)

[Chasing the Wind Episode Five](#)

[Chasing the Wind Episode Six](#)

[Chasing the Wind Episode Seven](#)

[Chasing the Wind Episode Eight](#)

[Chasing the Wind Episode Nine](#)

[Chasing the Wind Episode Ten](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus