From the dark corners of the Internet we bring you

Forensic Case Files

True Stories of Cybercrime

Vol. 1, Case 1

**Some names, places, and details have been changed to protect confidentiality*

Flying Blind

How one laptop killed an entire business and bankrupted a millionaire

As Fred* told me his story, I felt like a fireman who is called out too late. The house is already burnt to the ground. There stands the owner, asking the firemen what he should have done differently. All we could do is a "post-mortum" – investigate what had happened and try to give him some kind of closure.

For many years, Fred was a high-flyer in every sense of the word. He had his pilot's license, and was a broker of luxury private aircraft. The kind of fancy jets favored by the super-rich and featured in TV shows that make us shake our heads in disbelief. Fred's expertise in these aircraft made him the "go-to" guy for some of the world's wealthiest clients. He had it all -- an excellent income, nice family, houses, boats, sometimes a plane or two, and the undying respect of luxury jet buyers and sellers around the globe. So why, when he finally hired a professional investigator, was he bankrupt and living in a friend's attic?

Fred had unintentionally opened up an electronic *wormhole* into his business. Through that hole, criminals had invaded Fred's world and stole him blind. He had no idea, and had almost driven himself mad trying to figure out what was happening to him. In a short time, we discovered the leak. But by then, it was too late to save his fortune, his marriage, or his reputation.

continued

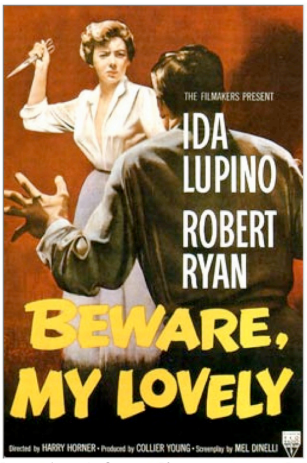
Barbarians at the Gates

Analysis revealed that hackers had gained access to Fred's laptop over the Internet, through a **trojan horse** program that created a back-door, so to speak. They then lay low, doing no damage to his computer, carefully covering their tracks so no anti-virus program would sniff out their covert opening into Fred's PC. Every day, they read his email, sifted through his files, and learned about his business deals. They then sold that information to his competitors. And yes, there are *always* unscrupulous people who will pay for such information; else hackers like these would have no income.

Brokers don't actually own the planes they are helping to sell, and several different brokers may offer the same plane at any given time, provided the owner didn't sign an exclusive agreement -- few in that industry do. Every time Fred would try to buy or sell an airplane, his competition knew about it and would undercut the deal. The hackers also learned inside details about Fred's methods. Not dishonest things, but details of his books and contacts that amounted to "trade secrets" of his business. These they also passed on to others, who then twisted these details to concoct and spread vicious rumors about Fred. Soon, his usual clients began to noticeably back away, or stopped taking his calls, *but all without telling him why*.

Fred's business began to dry up. The luxury jet marketplace is a small club, and it didn't take long for the word to get out. Nevermind that the rumors weren't true. His competitors were all too glad to pass on damaging information and thereby increase their own chances for success. In hardly any time at all, Fred had no income. He had unfortunately not prepared for any such thing, and therefore had little savings. He and his wife were divorcing during this time, and his concentration was divided between his business decline and his marital problems. Later, Fred freely admitted that he didn't see the full scope of his disaster until it was too late. As his income dwindled, Fred was forced to declare bankruptcy. All his remaining assets were sold to satisfy either creditors or his lawyers, and the repo men towed away whatever was left.

Hell Hath No Fury.....



A forensic examination of Fred's laptop revealed all. It turned out that Fred's wife, who had been caught in adultery and therefore stood to gain *nothing* from the divorce, was behind the hacking effort. She had decided that "If I can't have it, you can't either." Her new boyfriend was in with a crowd of unsavory cybercriminals, and they used her knowledge of Fred's computer, as well as of his business, to hack in, find exactly the right info, and turn it against Fred in the worst imaginable way.

All the proof was there -- the trojan, the back-door access, the log files; everything. But by the time Fred hired us and we did our work, it was far too late. His finances were so bad that he decided he couldn't even afford to pursue prosecution, even though he had the evidence to precisely pinpoint the perpetrators and almost guarantee they would be nailed. All we could do is stare at the ashes of his life and wish he had called *much, much earlier.*

What Could a User Do?

[x] Get a Mac. Love them or hate them, a Mac would have made all the difference in this case. It's far harder to gain illegal access to a Mac than a PC like Fred's. If he had had a Mac, it's likely *none of this would have happened.*

[x] If an employee, partner, or spouse leaves, **change all your passwords**. Fred left everything as it was, imagining his spouse couldn't remember the passwords any better than he could. *He was several million dollars worth of wrong.*

[x] Trust your instincts. If something's "just not right" about your business computers, or if your competitors seem to be just a bit too knowledgeable, too quick off the mark against you, your systems may be compromised. The cost of engaging a professional digital investigator should be weighed against the cost of losing your business, your intellectual property, and your hard-earned money to evil hackers. Sadly, the police can't help until a definite crime has been committed. Then it's too late. And what if the hackers are overseas?

Remember: Hackers rely on your ignorance first, and then on your personal embarrassment. *To succeed, they need your help!*

What Are Your Options?

It depends entirely on what you would like to see accomplished. Do you want to kick butt and take names, or just lock things up tighter and set some alarms?

Step 1: Find out what's actually happened. This must done by professionals, not some off-the-shelf software package. Black hat hackers go through that stuff like a hot knife through butter. Digital investigators know where and how to look.

Step 2: Decide if you want to catch the Bad Guys, lock them out, or – even more nefarious – *use their own spy system to feed them disinformation*. That last one can be very useful, and may also lead to a more iron-clad conviction later. Each has its own pluses, minuses, and inherent costs. A pro will also keep you from crossing legal boundaries as you progress.

Author: Drew Janssen is a digital forensic investigator and owner of Drive Rescue, Inc., a data recovery and forensics lab located in Baltimore, MD. Your questions & comments are welcome. Email: drew@driverescue.net