# The Rise of the Digital Thugs

By *srlinuxx*
Created *07/08/2005 - 6:31am*
Submitted by srlinuxx on Sunday 7th of August 2005 06:31:19 AM Filed under Security [1]

EARLY last year, the corporate stalker made his move. He sent more than a dozen menacing e-mail messages to Daniel I. Videtto, the president of MicroPatent, a patent and trademarking firm, threatening to derail its operations unless he was paid $17 million.

In a pair of missives fired off on Feb. 3, 2004, the stalker said that he had thousands of proprietary MicroPatent documents, confidential customer data, computer passwords and e-mail addresses. Using an alias of "Brian Ryan" and signing off as "Wounded Grizzly," he warned that if Mr. Videtto ignored his demands, the information would "end up in e-mail boxes worldwide."

He also threatened to stymie the online operations of MicroPatent's clients by sending "salvo after salvo" of Internet attacks against them, stuffing their computers so full of MicroPatent data that they would shut down. Another message about two weeks later warned that if he did not get the money in three days, "the war will expand."

Unbeknownst to the stalker, MicroPatent had been quietly trying to track him for years, though without success. He was able to mask his online identity so deftly that he routinely avoided capture, despite the involvement of federal investigators.

But in late 2003 the company upped the ante. It retained private investigators and deployed a former psychological profiler for the Central Intelligence Agency to put a face on the stalker. The manhunt, according to court documents and investigators, led last year to a suburban home in Hyattsville, Md., its basement stocked with parts for makeshift hand grenades and ingredients for ricin, one of the most potent and lethal biological toxins. Last March, on the same day that they raided his home, the authorities arrested the stalker as he sat in his car composing e-mail messages he planned to send wirelessly to Mr. Videtto. The stalker has since pleaded guilty to charges of extortion and possession of toxic materials.

What happened to MicroPatent is happening to other companies. Law enforcement authorities and computer security specialists warn that new breeds of white-collar criminals are on the prowl: corporate stalkers who are either computer-savvy extortionists, looking to shake down companies for large bribes, or malicious competitors who are trying to gain an upper hand in the marketplace.

"It's definitely a growing issue and problem, and it's something we think will definitely increase in both the numbers and severity," said Frank Harrill, an agent with the Federal Bureau of Investigation who specializes in computer crimes and who has investigated corporate stalkers and online extortionists. The reason, he said, is that "the Internet is ceasing to be a means for communication and commerce and is becoming the means for communication and commerce."

Though the number of corporate stalkers appears to be growing - along with the number of payoffs to online extortionists - quantifying the dimensions of the threat is difficult. Last fall, a researcher at Carnegie Mellon University in Pittsburgh published a study of online extortion involving small and medium-sized businesses, saying that the Internet's global reach had produced "a profound change in the nature of crime, as the existence of information systems and networks now makes criminal acts possible that were not before, both in increased scope and ease."

THE study also concluded that while the threat of cyberextortion was real and mounting, data and research about the subject were scant. That is because most businesses, particularly blue-chip companies, are concerned about negative publicity from computer security breaches and do not want to report digital bullying and intrusions to law enforcement officials.

"Cyberextortion was the main threat I identified that I thought corporations were overlooking," said Gregory M. Bednarski, the author of the Carnegie Mellon study, who now works at PricewaterhouseCoopers as a computer security consultant. "Unfortunately, I think that's still the issue - most companies are still not taking cyberextortion seriously enough. They just don't see themselves as vulnerable."

MicroPatent, based in East Haven, Conn., realized firsthand how vulnerable its data was. The company was also an exception in the world of cyberextortion victims: it chose not only to fight back and to contact the authorities, but it also assembled its own team of specialists familiar with the strategies and weaponry of cybercriminals.

Even so, MicroPatent's stalker, using hijacked Internet accounts and pirated wireless networks, was remarkably elusive. "What this means is that the criminals are getting smarter," said Scott K. Larson, a former F.B.I. agent and a managing director of Stroz Friedberg, a private investigation firm that helped hunt down MicroPatent's stalker. "There's an arms race going on in cyberspace and in cybercrimes."

MicroPatent, a business that court papers describe as one of the world's largest commercial depositories of online patent data, first came under attack four years ago. Someone penetrated the company's databases and began transmitting phony e-mail messages to its customers. The messages were what are known as "spoofs," online communications - embroidered with pilfered company logos or names and e-mail addresses of MicroPatent employees - that are meant to trick recipients into believing that the messages were authorized.

The spoofs, according to court papers and investigators, contained derogatory comments about MicroPatent in the subject lines or text. Some included sexually explicit attachments, such as sex-toy patents that a computer hacker had culled from the company's online files.

MicroPatent and its parent company, the Thomson Corporation, did not respond to several phone calls seeking comment. But others with direct knowledge of the hunt for the company's stalker said MicroPatent, which had grown rapidly through acquisitions, had a computer network containing stretches of online turf that were once used by acquirees but were abandoned after the takeovers.

Those digital back alleys offered access to the entire MicroPatent network to people with old passwords. Once inside, they could inhabit the network undetected - in much the same way that anyone with a key to one abandoned house on a block of abandoned houses can live in a populous city without anyone knowing he is there. And MicroPatent's stalker was lurking on one of its network's nether zones.

By 2003, MicroPatent had become so frustrated with its unknown stalker that it reached out to the F.B.I. for help. But with its resources spread thin, the F.B.I. could not pin down the stalker's identity, his motivations or how he managed to trespass on MicroPatent's electronic turf. A year later, MicroPatent hired Stroz Friedburg and secured the services of Eric D. Shaw, a clinical psychologist who had once profiled terrorists and foreign potentates for the C.I.A.

The first order of business, investigators said, was to narrow the field of MicroPatent's potential stalkers and to try to isolate the perpetrator. "You need to take the temperature of the person on the other side and determine how seriously you need to take them," said Beryl Howell, who supervised the MicroPatent investigation for Stroz Friedburg. "Is it a

youngster or is it someone who's angry? Is it someone who's fooling around or someone who's much more serious?"

Investigators said their examination of the stalker's communications indicated that he was much more than a hacker on a joy ride. That would be consistent with what law enforcement authorities and computer security specialists describe as the recent evolution of computer crime: from an unstructured digital underground of adolescent hackers and script-kiddies to what Mr. Bednarski describes in his study as "information merchants" representing "a structured threat that comes from profit-oriented and highly secretive professionals."

STEALING and selling data has become so lucrative, analysts say, that corporate espionage, identity theft and software piracy have mushroomed as profit centers for criminal groups. Analysts say cyberextortion is the newest addition to the digital Mafia's bag of tricks.

Generally speaking, it's pretty clear it's on the upswing, but it's hard to gauge how big of an upswing because in a lot of cases it seems companies are paying the money," said Robert Richardson, editorial director of the Computer Security Institute, an organization in San Francisco that trains computer security professionals. "There's definitely a group of virus writers and hackers in Russia and in the Eastern European bloc that the Russian mob has tapped into."

Mr. Richardson is a co-author of an annual computer-security study that his organization publishes with the F.B.I. The latest version said that while corporate and institutional computer break-ins increased slightly last year from 2003, average financial losses stemming from those intrusions decreased substantially in all but two categories: unauthorized access to data and theft of proprietary information.

Among 639 of the survey's respondents, the average loss from unauthorized data access grew to $303,234 in 2004 from $51,545 in 2003; average losses from information theft rose to $355,552 from $168,529. The respondents suffered total losses in the two categories of about $62 million last year. While many cyberextortionists and cyberstalkers may be members of overseas crime groups, several recent prosecutions suggest that they can also be operating solo and hail from much less exotic climes - like the office building just down the street.

In March, a federal judge in San Francisco sentenced a Southern California businessman, Mark Erfurt, to five months in prison, followed by three and a half years of home detention and supervised release, for hacking into the databases of a competitor, the Manufacturing Electronic Sales Corporation, and disrupting its business. In June, the F.B.I. in Los Angeles arrested Richard Brewer, a former Web administrator for a trade show company, accusing him of disabling his employer's Web site and threatening further damage unless he was paid off. And last month in New York, the Westchester County district attorney's office charged a Tarrytown businessman, Gerald Martin, with hacking into a competitor's computer network in order to ruin its business by tampering with its phone system.

Small-fry stuff, some of this, except that even local law enforcement officials say the episodes are multiplying. "We have 590,000 people in our county, but we're seeing lots of examples of lax or lackadaisical computer security," said Sgt. Mike Nevil, head of the computer crimes unit of the Ocean County, N.J., prosecutor's office. "We've seen lots of examples of people going onto a competitor's computer network and clearing out whatever information they can get."

For its part, MicroPatent initially believed that its problems were the work of a competitor. It sued one company that it suspected but later dropped that lawsuit. After Ms. Howell's team joined the fray in late 2003, MicroPatent and its consultants began to isolate the stalker, using a small list of candidates distilled from earlier investigative work.

Dr. Shaw's analysis of e-mail messages led them to believe that they were tracking a technologically sophisticated man, older than 30, with a history of work problems and personal conflicts, who was compulsively obsessed with details and who might own weapons. The stalker was extremely angry and "holding a grudge," Dr. Shaw recalled. "People like that can be very dangerous. He referred to himself as a soldier behind enemy lines."

Within a few weeks, Dr. Shaw's analysis led the investigative team to focus on Myron Tereshchuk, a 43-year-old Maryland entrepreneur who ran his own patent business and had once been rebuffed by MicroPatent when he applied to the company for a job. And Mr. Tereshchuk was indeed their man. Members of Ms. Howell's investigative team all

said that Dr. Shaw's profiling was a breakthrough in the pursuit, but that without the subsequent involvement of local and federal law enforcement officials, Mr. Tereshchuk would not have been captured.

"It's about grinding out a lot of data; it's not about intuition - though years of working clinically with patients is certainly important," Dr. Shaw said. "The Myron case involved a fair amount of case management because we needed to keep him talking, we needed to keep him engaged, so we could set him up for an arrest."

Indeed, the detective work that led to his arrest offers a revealing glimpse into how the new cat-and-mouse game is played in cyberspace - especially when the cloak of secrecy offered by newfangled wireless devices makes digital criminals so hard to track.

In early 2004, private investigators began corresponding with the stalker, sending spoofed e-mail back to him in the "voice" of a MicroPatent lawyer. At the same time, federal authorities began physically tracking Mr. Tereshchuk's comings and goings in the real world. By February, the stalker had also become an active e-mail correspondent with Mr. Videtto, the MicroPatent president.

It was then that the stalker made a series of mistakes. Among them, he began to brag. In an e-mail message titled "Fire them all," he informed Mr. Videtto that he had found valuable MicroPatent documents by going "Dumpster diving to the Dumpster and recycle bins located in a parking lot on Shawnee Road" in Alexandria, Va., where the company maintained a branch office. That allowed investigators to zero in on his location, further buttressing the notion that Mr. Tereshchuk, who lived nearby, was the author of the scheme.

In the same message, the stalker wrote angrily that staff members at the United States Patent and Trademark Office in northern Virginia had snubbed him and given preferential treatment to MicroPatent employees. Several years earlier, a patent office worker accused Mr. Tereshchuk of threatening to bomb the agency.

A computer forensics expert embedded a Web bug, a kind of digital tracking device, in one of the e-mail messages that Mr. Videtto sent to the stalker. But the stalker screened his e-mail with decoding devices that included a hex editor, software that allows users to preview the contents of incoming files, and he uncovered the bug. "Was it a script to capture my IP address?" the stalker wrote tauntingly to Mr. Videtto after finding the Web bug, referring to his Internet Protocol address. "I'll look at it later with a hex editor."

Investigators said the failed bug worried them because they thought it might scare off the stalker, but by this point Mr. Tereshchuk had already demanded his $17 million extortion payment. He also clumsily revealed his identity by demanding that the money be sent to the person accused of threatening to bomb the patent office. And he kept sending e-mail messages telling Mr. Videtto that he had MicroPatent's customer lists, patent applications, customer credit card numbers and the Social Security numbers of some employees, as well as the employees' birth dates, home addresses and the names of their spouses and children.

The stalker also threatened to flood the computer networks of MicroPatent clients with information pilfered from the company, overwhelming the customers' ability to process the data and thereby shuttering their online operations - a surreptitious digital attack known as distributed denial of service, or D.D.O.S. Such assaults, analysts and law enforcement officials say, have become a trademark of cyberextortionists. Federal prosecutors in Los Angeles are currently investigating a group of possible cyberextortionists linked to a television retailer indicted there last August. The retailer was accused of disrupting competitors' online operations, and prosecutors have called suspects in that case the "D.D.O.S. Mafia."

"D.D.O.S. attacks are still one of the primary ways of extorting a company, and we're seeing a lot of that," said Larry D. Johnson, special agent in charge of the United States Secret Service's criminal division. "I think the bad guys know that if the extortion amounts are relatively low a company will simply pay to make them go away."

Mr. Tereshchuk's apparent ability to start a D.D.O.S. attack attested to what investigators describe as his unusual technological dexterity, despite evidence of his psychological instability. It also explained how he was able to evade

detection for years, and his methods for pulling off that feat surfaced after the F.B.I. began following him.

Using wireless computing gear stashed in an old, blue Pontiac, and fishing for access from an antenna mounted on his car's dashboard, Mr. Tereshchuk cruised Virginia and Maryland neighborhoods. As he did so, federal court documents say, he lifted Yahoo and America Online accounts and passwords from unwitting homeowners and businesspeople with wireless Internet connections. The documents also say he then hijacked the accounts and routed e-mail messages to MicroPatent from them; he used wireless home networks he had commandeered to hack into MicroPatent's computer network and occasionally made use of online accounts at the University of Maryland's student computer lab, which he had also anonymously penetrated.

BY late February of last year, however, the F.B.I. had laid digital traps for Mr. Tereshchuk inside the student lab, which was near his home. As investigators began to close in on him, his e-mail messages to Mr. Videtto became more frantic. A note sent on Feb. 28 told Mr. Videtto that if he forked over the $17 million then "everything gets deactivated, sanitized, and life will go on for everybody."

In his last e-mail message, sent several days later, he dropped his guard completely: "I am overwhelmed with the amount of information that can be used for embarrassment," he wrote. "When Myron gets compensated, things start to get deactivated."

On March 10, 2004, federal agents swarmed Mr. Tereshchuk's home, where they found the hand-grenade components and ricin ingredients. The agents arrested him in his car the same day, in the midst of writing his new crop of e-mail messages to Mr. Videtto.

Late last year, Mr. Tereshchuk was sentenced to five years in prison after pleading guilty to a criminal extortion charge filed by the United States attorney's office in Alexandria. Earlier this year he pleaded guilty to criminal possession of explosives and biological weapons, charges that the United States attorney's office in Baltimore had filed against him. Possessing illegal toxins carries a maximum term of life in prison. Mr. Tereshchuk is expected to be sentenced this fall.

By TIMOTHY L. O'BRIEN
The New York Times [2]

Security

---



**Links:**
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://www.nytimes.com/2005/08/07/business/yourmoney/07stalk.html