Evan Ratliff

The Zombie Hunters

On the trail of cyberextortionists

One afternoon this spring, a half dozen young computer engineers sat in the headquarters of Prolexic, an Internet-security company in Hollywood, Florida, puzzling over an attack on one of the company's clients, a penile-enhancement business called MensNiche.com. The engineers, gathered in the company's network operations center, or noc, on the fourth floor of a new office building, were monitoring Internet traffic on 50-inch wall-mounted screens. Anna Claiborne, one of the company's senior network engineers, wandered into the noc in jeans and a T-shirt. The MensNiche attacker had launched an assault on the company's Web site at 4 a.m., and Claiborne had spent the night in the office fending it off. "Hence," she said, "I look like hell today."

MensNiche's problems had begun a week earlier, with a flood of fake data requests—what is known as a distributed denial-of-service attack—from computers around the world. Although few, if any, of those computers' owners knew it, their machines had been hijacked by hackers; they had become what programmers call "zombies" and had been set loose on MensNiche. The result was akin to what

occurs when callers jam the phone lines during a television contest: With so many computers trying to connect, almost none could get through, and the company was losing business.

The first wave of the attack was easily filtered by Prolexic's automated system. The assailant then disguised his zombies as legitimate Web users, fooling the filters so well that Claiborne refused to tell me how it was done, for fear that others would adopt the same tactic. She spent the night examining the requests one by one as they scrolled by—interrogating each zombie, trying to find a key to the attacker's strategy.

"He's clever, and he's been trying everything," Claiborne said. "If we ever find out who it is, seriously, I'd be willing to buy a plane ticket, fly over, and punch him in the face."

Prolexic, which was founded in 2003 by a 27-year-old college dropout named Barrett Lyon, is a 24-hour, seven-days-a-week operation. An engineer is posted in the noc at all times to monitor Prolexic's four data hubs, which are in Phoenix, Vancouver, Miami, and London. The hubs contain powerful computers designed to absorb the brunt of data floods and are, essentially, massive holding pens for zombies. Any data traveling to Prolexic's clients pass through this hardware. The company, which had revenues of 4 million dollars in its first year, now has more than 80 customers.

Lyon's main business is protecting his clients from cyberextortionists, who demand payments from companies in return for leaving them alone. Although Lyon is based in Florida, the attackers he deals with might be in Kazakhstan or China, and they usually don't work alone.

"It's an insanely stressful job," Claiborne told me. "You are the middleman between people who are losing thou-

sands or millions of dollars and somebody who really wants to make that person lose thousands or millions of dollars." When the monitors' graphs begin to spike, indicating that an attack is under way, she said, "it's like looking at the ocean and seeing a wall of water 300 feet high coming toward you."

Only a few years ago, online malfeasance was largely the province of either technically adept hackers (or "crackers," as ill-intentioned hackers are known), who were in it for the thrill or for bragging rights, or novices (called "script kiddies"), who unleashed viruses as pranks. But as the Web's reach has expanded real-world criminals have discovered its potential. Mobsters and con men, from Africa to Eastern Europe, have gone online. Increasingly, cyberextortionists are tied to gangs that operate in several countries and hide within a labyrinth of anonymous accounts.

"When the attack starts, the ticker starts for that company," Lyon said. "It's a mental game that you've been playing, and if you make a mistake it causes the whole thing to go down. You are terrified."

Lyon, as usual, was wearing shorts and flip-flops. He has blond hair, a trim build, and narrow hazel eyes that were framed by dark circles of fatigue. A poster for the 1983 movie *WarGames*—a major influence—hung above his desk, on which were four computer monitors: one for writing program code, one for watching data traffic, one for surfing the Web, and one for chatting with customers. Lyon leaned over and showed me a program that he had created to identify the zombies attacking MensNiche. When he ran it, a list of countries scrolled up the screen: the United States, China, Cambodia, Haiti, even Iraq.

Examining the list of zombie addresses, Lyon picked one and ran a command called a "traceroute." The program followed the zombie's path from MensNiche back to a com-

puter called NOCC.ior.navy.mil—part of the United States Navy's Network Operations Center for the Indian Ocean Region. "Well, that's great," he said, laughing. Lyon's next traceroute found that another zombie was on the Department of Defense's Military Sealift Command network. The network forces of the U.S. military had been conscripted in an attack on a Web site for penis enlargement.

Michael Alculumbre's first communication from the extortionists arrived on a Thursday evening in August 2004. An e-mail message was sent to him just after 8 p.m. at Protx, an online-payment processing company based in London, where he is the chief executive officer. The subject line read, simply, "Contact us," and the return address—commerce_protection@yahoo.com—offered no clues to the message's origin. The note was cordial and succinct, written in stilted English. "Hello," it began. "We attack your servers for some time. If you want save your business, you should pay 10.000$ bank wire to our bank account. When we receive money, we stop attack immediately. If we will not receive money, we will attack your business 1 month." The note said that $10,000 dollars would buy Protx a year's worth of protection. "Think about how much money you lose, while your servers are down. Thanks John Martino." Alculumbre had never heard of John Martino. He decided to ignore the demand.

Two months later, Alculumbre's network technician called him at home. He said that customers were complaining that the system was off-line. By the time Alculumbre arrived at the office, the source of the disruption was clear. Thousands of computers were inundating Protx's Web site with fake data requests. Many of Protx's legitimate customers received the Internet equivalent of a busy signal—a message saying that the company's servers weren't responding.

Every minute that the Web site remained off-line, Protx's business suffered. As the company's engineers struggled to contain the attack, another $10,000 e-mail demand arrived, this time signed "Tony Martino." Again, Alculumbre ignored it. He had received a call from an agent of the British National Hi-Tech Crime Unit, which had been monitoring the attack. The agent let him know that paying Martino wasn't an option; the extortionist would only return. Beyond that advice, there wasn't much that the NHTCU could do to help. By the time Alculumbre's engineers were able to get the site running, it had been disabled for almost two days.

Alculumbre heard from Tony Martino again the following April, when he received a message offering a $1,000-a-month protection-money payment plan. Before he could respond, an army of up to 70,000 zombies ripped through Protx's defenses and knocked its Web site off-line. This time, it took Protx's engineers three days to fight off the attack.

The company now spends roughly $500,000 a year to protect itself—50 times what Martino had asked for. This includes a $100,000-a-year security contract with Prolexic. Martino, it turned out, had been targeting Lyon's clients for months before he hit Protx.

"This is very similar to the pubs and clubs in London 40 years ago that used to pay money to not have their premises smashed up," Mick Deats, the deputy head of the NHTCU, told me. "It's just a straight, old-fashioned protection racket, with a completely new method." The cyberextortionists also make use of an elaborate money-laundering system, Deats said. "They have companies registered all over the place, passing the money through them."

"I started prosecuting network-attack cases in 1992, and back then it was more the sort of lone hackers," said

Christopher Painter, the deputy chief of the Computer Crime and Intellectual Property Section at the Department of Justice. Today, he says, "you have organized criminal groups that are adopting technical sophistication."

The most potent weapon for Web gangsters is the botnet. A bot, broadly speaking, is a remote-controlled software program that is installed on a computer without the owner's knowledge. Hackers use viruses, worms, or automated programs to scan the Internet in search of potential zombies. One recent study found that a new PC, attached to the Internet without protective software, will on average be infected in about 20 minutes.

In the most common scenario, the bots surreptitiously connect hundreds, or thousands, of zombies to a channel in a chat room. The process is called "herding," and a herd of zombies is called a botnet. The herder then issues orders to the zombies, telling them to send unsolicited e-mail, steal personal information, or launch attacks. Herders also trade, rent, and sell their zombies. "The botnet is the little engine that makes the evil of the Internet work," Chris Morrow, a senior network-security engineer at MCI, said. "It makes spam work. It makes identity fraud work. It makes extortion, in this case, work."

Less than five years ago, experts considered a several-thousand-zombie botnet extraordinary. Lyon now regularly faces botnets of 50,000 zombies or more. According to one study, 15 percent of new zombies are from China. A British Internet-security firm, Clearswift, recently predicted that "botnets will, unless matters change dramatically, proliferate to the point where much of the Internet . . . comes to resemble a mosaic of botnets." Meanwhile, the resources of law enforcement are limited—the NHTCU, for example, has 60 agents handling everything from child pornography to identity theft.

Extortionists often prefer to target online industries, such as pornography and gambling, that occupy a gray area and may be reluctant to seek help from law enforcement. Such businesses account for most of Prolexic's clients. I asked Lyon how he felt about the companies he defended. "Everybody makes a living somehow," he said. "It's not my job to worry about how they do it."

I asked whether that applied to extortionists as well. After a pause, he said, "I guess I'm partial to dot-commers."

Several weeks later, he called me to say that he'd reconsidered his answer. "The Internet is all about connecting things, communicating and sharing information, bits, pieces of data," he said. "A denial-of-service attack is the exact opposite of that. It is taking one person's will and imposing it on a bunch of others." In any case, Lyon added, his clients now included mainstream businesses—a Japanese game company, foreign-exchange traders, and a multibillion-dollar corporation that wanted to have additional security in the days before its IPO

Lyon first gained a measure of online fame in 2003, with a project called Opte, in which he created a visual map of the entire Internet—its backbone, transfer points, major servers. After reading that a similar project had taken several months to complete, he bet a friend that he could do it in a day, and he won. (A gorgeously rendered print of the map—which Lyon licenses free of charge—appeared in a traveling exhibition on the future of design.)

Lyon's obsessive interest in computer networks began early. In the third grade at a Sacramento, California, private school for learning-disabled children—Prolexic's name derives from Lyon's pride in overcoming severe dyslexia—he and a friend hacked a simple computer game. In junior high school, Lyon discovered the Internet, and with a friend, Peter Avalos, he soon founded a company called

TheShell.com, which provided accounts to chat-room users. But his grades suffered, and, after high school, he failed a year's worth of classes at California State University at Chico.

When a friend he met online, Robert Brown, offered Lyon a job at his computer-security company, Network Presence, he quit school and took it. Brown sent him off to secure the network of a large insurance company in the Midwest. Lyon was 19, and, he said, "I looked 13. So I wore a suit every day, and I worked my ass off for those guys." He burned out after two years—"I didn't know you had to meter yourself"—and returned to school, this time at California State University at Sacramento. There, Lyon signed up for philosophy classes, dumped his computers in a closet, and joined the rowing team. But he couldn't get away from computers entirely; he still took assignments from his old employer, and he and Avalos (who graduated from the United States Naval Academy and has recently returned from flying P-3s in Iraq) continued to operate TheShell.com. The company's clients tended to be advanced Internet users, and this had the effect of bringing the site to the attention of hackers. At one point, Lyon was fighting off several zombie attacks a day.

In August 2002, Dana Corbo, the CEO of Don Best Sports, called Network Presence for help. Don Best, which is based in Las Vegas, is a kind of Bloomberg for the gambling world, providing betting lines for both real-world and online casinos. The company had ignored an e-mailed extortion demand for $200,000, and it was under attack. Network Presence sent Lyon.

The next day, Lyon and another engineer flew to Las Vegas and helped Don Best's engineers set up powerful new servers. Lyon's strategy worked: the attackers gave up. Corbo treated them to a night out in Vegas, with dinner in

front of the Bellagio fountains. (He also paid Network Presence a fee.)

Lyon still wanted to find out who was behind the attacks. He and Brown scanned the traffic data; found a zombie; and, thanks to an opening in Microsoft Windows, were able to see what other computers it had been connected to. This led them to a chat server in Kazakhstan; when they connected to it, they saw more attacks in progress. They notified the FBI and the Secret Service, but, Brown said, "they sort of threw up their arms, because it was in Kazakhstan." To Lyon, however, the lesson was clear: With clever techniques and a little luck, any attacker could be found.

In the late spring of 2003, Mickey Richardson, the general manager of Betcris, a Costa Rican–based gambling firm, received an extortion e-mail. (Online bookmaking, which is illegal in the United States, has flourished in Costa Rica and the Caribbean since the mid-1990s.) The letter requested $500 in eGold—an online currency—and was followed by an attack that crippled Betcris's Web site, its main source of revenue. Richardson couldn't afford to have the site disabled. He paid the $500.

The extortionists began hitting other offshore bookmakers. One firm after another paid up, anywhere from $3,000 to $35,000, which they wired to addresses in Russia and Latvia. Richardson expected that he, too, would be hit again. He heard about Don Best's successful defense and called Lyon. But Lyon was back in school and reluctant to take the job. Instead, he told Richardson to buy a server that was specially designed to filter out attacks. "The box," as Richardson called it, cost about $20,000. Over the phone, Lyon helped Richardson's information-technology manager, Glenn Lebumfacil, configure it.

A few months later, Richardson got another e-mail

from the extortionists. It arrived just before Thanksgiving, one of the busiest betting periods of the year, and it asked for $40,000. The e-mail said:

> If you choose not to pay for our help, then you will probably not be in business much longer, as you will be under attack each weekend for the next 20 weeks, or until you close your doors.

Richardson believed that he had "everything in place to protect the store," and he refused to pay.

When the attack came, it took less than 20 minutes to overwhelm the box. The data flood brought down both Betcris and its Internet service provider. After a few days of trying in vain to make the box work, Lebumfacil called Lyon in a panic. "Hey, man, remember that thing you set up for us?" he said. "It just got blown away."

Lyon saw a business opportunity. He quit school again and started a company, with Betcris as his first customer. He knew that he couldn't just add capacity to Betcris's system to capture the zombies, as he had with Don Best, because Costa Rica wasn't wired for that sort of system—there wasn't enough capacity in the entire country. So he decided to build his own network in the United States and use it to draw the attackers away from Betcris. The extortionists would think they were attacking a relatively defenseless system in Central America but would find themselves up against Lyon's machines instead.

Richardson, meanwhile, was stalling for time with the extortionists, claiming a medical emergency. "I guess you did not take my warning seriously," came the reply. "The excuse that you were in the hospital does not matter to me." The correspondence became increasingly belligerent. "Sorry moron but I am just having so much fun fucking with you,"

one e-mail said, raising the price to $60,000. Richardson responded by offering the extortionists jobs in Betcris's IT department. "I appreciate the offer to do work for you, but we are completely booked until the football season is over," one of them replied.

As Lyon brought his system online, the confrontation turned into a chess match. "Every time Barrett would change something, these guys would change something else," Brian Green, the CEO of Digital Solutions, Betcris's Internet service provider, said. "They threw wrenches, they threw everything they could at Betcris."

Finally, after three weeks, the attacker gave up. "I bet you feel real stupid that you did not keep your word," he wrote. "I figure by now you have lost 5 times what we asked and by the end of the year your decision will cost you more than 20 times what we asked." Richardson says that those numbers may not have been far off.

By then, everyone in the insular gaming world seemed to have heard that Lyon could stop zombie attacks, and he was getting calls from Jamaica, Costa Rica, and Panama. "It was kind of like stumbling into this strange little community in the middle of nowhere, where everybody worships a weird stone," Lyon said. "They all had superstitions about when they were going to be attacked."

Lyon decided, once again, to trace the source of the attack. He and Dayton Turner, a goateed 24-year-old engineer he had hired, allowed one of their own machines to become a zombie and watched as it was drawn into the botnet; by early January they had found the chat channel that controlled the zombies.

Logging on as "hardcore," Turner pretended to be a bot herder who had been out of the game for a while. "i want to get back into it," he wrote. "i ha[v]e a small group of zombies so far which is why i came back looking." Turner had

spent years in chat rooms and communicated easily in the emoticon-heavy shorthand common to hackers. He gradually ingratiated himself with a Russian who called himself eXe and often logged in from a server that he'd named "exe.is.wanted.by.the.FBI.gov." Other members were not so welcoming; when Turner wrote, "i wanna help," one of them, uhdfed, replied, "we don't need ur HELP," and set his zombies on him. But Lyon and Turner kept returning, establishing their technical credibility and becoming a part of the scene.

They continued the ruse for weeks, occasionally with an FBI agent on the phone helping to direct the conversation. As bait, Turner described a program he had written that would help eXe to collect zombies, which he promised to give him as soon as he could rewrite it in a different programming language. "It was a matter of simply befriending the guy and making him think that he could trust us," Lyon said. Piece by piece, eXe revealed himself:

> hardcore: its pretty cold here right now, what's russia like? hehe
> eXe: i'm good
> eXe: something hot
> eXe: =)
> eXe: Russia is like the Russian Vodka=)
> hardcore: hehehe
> eXe: u give me code?

At one point, during an exchange about the number of computers each had infected, eXe asked Turner how old he was. Turner replied that he was 23 and added, "How about you? :)." eXe told him that he was a 21-year-old Russian student named Ivan. Turner said that his name was Matt and he lived in Canada. Then, trying to provoke a confession, he

told Ivan that he made money from extortion: "They always pay because they want their business back and they don't want to admit they have a weakness . . . stupid Americans."

Turner then asked Ivan about a specific attack: "I figured it would be you since you have so many bots :P."

"Good idea . . . hehe," Ivan replied.

Before they signed off, Ivan wrote, "Bye friend."

In February 2004, Lyon and Turner submitted a 36-page report to the FBI and the NHTCU, outlining their profile of Ivan and their correspondence with his crew. At this point, they were operating as DigiDefense International, which Lyon had founded, hiring Turner and Lebumfacil as his first employees. At the company's temporary headquarters, in an office building in Costa Rica, paranoia about reprisals from Russian mobsters reigned, even though there were armed guards in the lobby. Meanwhile, Lyon and Turner kept chatting with Ivan.

A few weeks later, on a Saturday in March, Ivan slipped up: he logged in to the chat room without disguising his home Internet address. The same day, Turner happened to be online and decided to look up eXe's registration information. To his astonishment, he found what appeared to be a real name, address, and phone number: Ivan Maksakov, of Saratov, Russia. Lyon dashed off an e-mail to the authorities with the subject line "eXe made a HUGE mistake!"

A few months later, the Russian police, accompanied by agents from the NHTCU, swept into Maksakov's home, where they found him sitting at his computer. In television footage of the arrest, Maksakov looks like a clean-cut kid, with brown hair and a teenager's face. He sits glumly on his bed in shorts and a T-shirt as the police rummage through his room and carry out his equipment. The video shows the officers walking him to the local station and slamming the door shut on his cell.

In simultaneous raids in St. Petersburg and Stavropol, the police picked up four other Russians whom the NHTCU had traced by setting up a sting at a bank in Riga, Latvia, where a British company that was cooperating with the authorities had been directed to send its payment. "We were waiting for people to come pick the money up," Mick Deats, of the NHTCU, told me. "But that didn't happen immediately. What did happen was that the bad guys we were watching picked up lots of different payments—not ours. We were seeing them pick up Australian dollars, U.S. dollars, and denominations from all over the world. And we're thinking, Whose money is that?"

The NHTCU has never explicitly credited Prolexic's engineers with Maksakov's arrest. "The identification of the offenders in this came about through a number of lines of inquiry," Deats said. "Prolexic's was one of them but not the only one." In retrospect, Lyon said, "The NHTCU and the FBI were kind of using us. The agents aren't allowed to do an Nmap, a port scan"—techniques that he and Dayton Turner had used to find Ivan's zombies. "It's not illegal; it's just a little intrusive. And then we had to yank the zombie software off a computer, and the FBI turned a blind eye to that. They kind of said, 'We can't tell you to do that—we can't even suggest it. But if that data were to come to us we wouldn't complain.' We could do things outside of their jurisdiction." He added that although his company still maintained relationships with law-enforcement agencies, they had grown more cautious about accepting help.

When the authorities picked up Ivan Maksakov, he was one semester away from graduation at a technical college in Saratov. He spent five months in prison before being released on bail and now awaits trial. According to the authorities, he was a lower-level operative in the gang, which paid him about $2,000 a month for his services. A

source close to the investigation told me that Maksakov, who faces 15 years in jail, is cooperating with the Russian police.

One afternoon in Prolexic's offices, I asked Turner if he had felt a sense of justice when Ivan was arrested. "I suppose," he said halfheartedly. "It was a difficult situation for me when I saw his picture, because I kind of felt for the kid. He wasn't necessarily a bad kid." Perhaps, Turner told me, Ivan had "just said, 'Let's see if it works. Hey, it works, and people pay me for it.'"

Lyon, too, was one semester from graduation when he dropped out of college to start his company. He was, in his own way, unable to resist the challenge, and he, too, had discovered that people would pay him for what he did. I asked him if he'd ever done anything illegal on the Net. He thought for a minute and then told me that once, as a teenager, he had poked around and discovered a vulnerability at Network Solutions, the company that at the time registered all the Web's addresses. "I went in and manipulated some domain names," he said. "A month later, I got a call from somebody with a badge," who had traced the intrusion back to Lyon's computer.

In the end, Lyon said, the authorities let it go. Those were simpler times. "I was scared shitless, but I learned my lesson," he said. "If something like that happened now, I can't imagine what would happen to me."