



Mafiaboy's Story Points to Net Weaknesses

Hacker pleads guilty, but security experts say networks are still far too vulnerable.

James Evans, IDG News Service

Wednesday, January 24, 2001

Canadian law enforcement officials contend that the hacker who last week admitted responsibility for one of the most notorious attacks ever on commercial computer networks is no more than a youth with a tool and the instructions to use it.

Details of the story of the 16-year-old Montreal youth known as "Mafiaboy" that have come out in the wake of [his guilty plea](#), however, are renewing controversy over how easy it is to create havoc on the Internet.

Mafiaboy was not scripting code or devising his own hacker exploits, law enforcement officials contend. Nearly a year after [Mafiaboy's attack](#), observers in the computer security community agree that it still is too easy to conduct a denial-of-service attack and locate some sort of vulnerability in a network.

In general, the tools are installed on someone else's computer and the command controls are held on the hacker's base computer. The attack software allows a [flood of messages](#) to be sent to the desired victim. Routers connecting the victim sites to the rest of the Internet become inundated with so much traffic that they eventually cannot cope.

'Unimaginable Damage' Warned

Mafiaboy's lawyer suggests, however, that if it were easy to do, the Internet would have seen other crippling attacks on commercial networks since his client's admitted exploits in February 2000. He also says his client is much brighter than authorities suggest.

"If he used all his powers, he could have done unimaginable damage," says Yan Romanowski, the boy's attorney in Montreal.

Mafiaboy never spoke with authorities directly about his online exploits attacking 11 corporate giants' networks. Information gathered in the case and the plea entered through his lawyer, however, offer concrete evidence that his keystrokes caused major problems for the likes of [Amazon.com](#), [eBay](#), and [Yahoo](#) for various periods of time between February 6 and 14, 2000.

The scope of Mafiaboy's doings prompted U.S. and Canadian authorities to seek out the origin of the hacker attacks, which led to an early morning raid on his family's home in Montreal. The boy, who now just wants to go on with his life, was captured thanks to straightforward police work and his bragging about his hacker capabilities.

On the Trail of a Hacker

On February 14, 2000, U.S. FBI investigators notified Cpl. Marc Gosselin with the Royal Canadian Mounted Police in Montreal that the trail to a hacker possibly responsible for several denial-of-service attacks led over the Canadian border. FBI investigators had learned that a hacker was bragging about the attacks in online chat rooms and on a Web page.

The FBI had seen that a hacker named Mafiaboy was boasting about attacks on the [Dell Computer](#) site, and appeared to be the only hacker familiar with the attack. In addition, FBI investigators were able to associate IP addresses with the attacks--and one of the addresses was for the hacker Mafiaboy's Web page, says Gosselin, the RCMP's lead investigator on the case.

The IP addresses came from the ISPs TotalNet and DSupernet in Montreal. Gosselin and his colleagues obtained a warrant to review the hacker's accounts.

"That was a good lead," Gosselin says. "I was able to make a link with the phone numbers" belonging to Mafiaboy's family's home.

Bragging to His Friends

Police then obtained a warrant to utilize technology that would show all the incoming and outgoing traffic from the residential phone line. Soon it was established that the TotalNet account used in the attacks was registered to the hacker's father.

Eleven days into their investigation, Canadian authorities were given a warrant for a wiretap. Investigators soon learned definitively who Mafiaboy was, Gosselin says.

"He was talking to friends, bragging about his skills," Gosselin says. "He said he was so good that the police would never catch him," he recalls.

'Not the Nerd Type'

Attorney Romanowski had never worked on a case about hacking. In fact, he suggests no one in the Canadian province of Quebec had worked on a computer hacking case of the magnitude that he was given on April 15, after the RCMP raided the home of the hacker at 2:30 in the morning. Romanowski was chosen because the boy's father had hired him before for legal counsel, he says.

During approximately two months of off-and-on legal work, Romanowski learned about his young client and about technology.

"He is not the nerd type," Romanowski says. "He is not the guy who will only talk about computers. He used to attend school, play basketball."

The boy's computer interests started young, with Nintendo of America and later games on the computer, he says. His parents separated more than ten years ago and for much of that time he lived with his mother, Romanowski says. For the past two years, however, he has been living with his 46-year-old father.

Romanowski says his client's interest in hacking was not fueled by an interest in causing damage. The challenge Mafiaboy got out of the hacking, however, created headaches for network administrators.

Mafiaboy's Story: Anatomy of the Attacks

The distributed denial-of-service attacks attributed to Mafiaboy spanned eight days and a continent. It was a first-hand chance for some of the leading sites to check the security of their servers. Some contend the lessons totaled [more than \\$1 billion](#) in damages.

On February 8, 2000, network administrators for Time Warner's [CNN.com](#) started to notice that their site was slowing down around 7 p.m., says company spokesman Paul Schur. The night was otherwise not a heavy traffic night, as there was no major breaking news to report, he says.

The denial-of-service attack never shut down the news provider's site, but it did slow it down.

"Our site was never taken down," Schur says. "We continued to serve content throughout the attacks. Our content was never compromised. Since we are used to breaking news, we are used to having large spikes in use. Although it was slow, content was served throughout."

The attack began at 7 p.m., and by 8:30 p.m. CNN's service providers had successfully protected CNN's site from the attack. CNN has a significant amount of bandwidth to deal with traffic for breaking news, and Schur says the slowdown demonstrates how serious the attack was.

[Buy.com](#) also was hit with a denial-of-service attack on the morning of February 8, which caused its Web site to become virtually inaccessible. At the time, the company's chief executive released a statement indicating the magnitude of the attack.

"We had 800 megabits per second hit our site, which equals eight times our capacity," said Greg Hawkins, Buy.com's chief executive officer.

A day later, online brokerage firm [E-Trade](#) reported customers had difficulty gaining access to its site, which functioned throughout the attack.

In total, 11 sites were attacked, and investigators suggest that it cost some \$1.7 billion in damages, from network downtime to lost sales and lost stock trades. Romanowski disputes the figure.

Distributed Denial of Service

RCMP investigators learned Mafiaboy gained illegal access to 75 computers in 52 different networks, Gosselin says. Of the 52 networks, 48 were at universities. He used networks in Canada, Korea, Denmark, and the United States.

Once he hacked into the networks, Mafiaboy planted a denial-of-service tool on them--a tool he got from a hacker named Sinkhole, Gosselin says. Sinkhole told Mafiaboy not to use the tool for malicious purposes once Mafiaboy registered it under his own name, Gosselin says. But the same tool, in fact, was used in the February attacks on CNN.com and other sites. The software used was what is known as an IMP tool, according to Gosselin and Jean Pierre Roy, staff sergeant in charge of the RCMP's Computer Investigation and Support Unit in Montreal.

A copy of the tool was located on networks at the University of California, Santa Barbara and the University of Alberta, Gosselin says. The copy found on the University of California, Santa Barbara's network was registered to Mafiaboy and to Short, another of the boy's handles, he says.

Mafiaboy used a distributed denial-of-service attack on the network victims, law enforcement officials say. In such an attack, phony requests are made to networks from various other networks or computers on the Internet. In a traditional denial-of-service, the requests would come from only one computer.

Romanowski would not discuss his client's hacking methods. He confirms his client disposed of his hard drive, which is believed to have contained evidence. He says the RCMP did not have its facts straight on how Mafiaboy waged the attacks.

"Had we gone to trial, we are convinced we could have brought (about) a reasonable doubt in four to eight months," he says.

Not Hard to Find

Getting such tools is not that difficult, says Richard Smith, an Internet security consultant. "They are just in Web sites in search engines," he says. They often are in news releases from security groups, adds.

Mafiaboy used a tool that could send an estimated 10,700 phony information requests in ten seconds, Gosselin says.

This type of attack is not difficult to administer, in general, says Mark Rasch, vice president for cyberlaw at [Predictive Systems](#), and former head of the Computer Crime Unit at the U.S. Department of Justice.

"It is not to say everyone can do it, but if a hacker is willing to put the time in to it, it can be done, he says.

A Career in Computers?

Mafiaboy admitted his part in the attacks before the Youth Court of Quebec in Montreal on January 18. He pleaded guilty to five counts of mischief, 51 counts of illegal access to a computer, and one count of breach of bail conditions. He will be sentenced on April 17 and 18.

Judge Gills Ouellet will have broad discretion in sentencing, ranging from a fine to detention.

The boy has dropped out of school and works as a steakhouse busboy. He is no longer using a computer but is reading about them, Romanowski says. At the time of his arrest he had three computers in his room. He now wants to go back to school and eventually study computers.

"He is anxious to get back using computers," Romanowski says.