

.computer security

In his 30 years at the forefront of security and on the Internet, James Atkinson has developed a sour taste for script kiddies and hackers, whom he refers to as "usually kids who can't get a date." His company outside Boston focuses on preventing high-level corporate espionage.

"If someone is using technology to effect espionage, I hunt them," says Atkinson. "It's mostly corporate and a lot of government work."

In 2000, Atkinson's name briefly cropped up in headlines after he tracked down the Verdun, Que.-based hacker known online as Mafiaboy. Mafiaboy had used programs found online for denial-of-service attacks that shut down hundreds of major websites, including eBay, Dell and Amazon.com.

It took Atkinson just 15 minutes to figure out Mafiaboy's real identity, which is protected in Canada under provisions of the Youth Criminal Justice Act. After pleading out in court, the kid was sentenced to eight months in a youth detention centre in 2001.

"When some hacker who has just hacked a big bank or some corporate system is afraid his door is gonna get kicked in, it's because of me," he says. "I hunted Mafiaboy for sport. A lot of people out there think they can take their technical skill and parlay it into hacking, when they would be a lot better off to actually pursue getting into security. It's a lot more fun."

Atkinson figures the divide between the educated and uneducated hasn't increased over the years. "The overall population in each group has changed. There are just more people physically doing it. It's like somebody saying that there's been an enormous increase in traffic-related deaths over the last 100 years.



Rob Horncastle
... virus hunter

"If you choose to get on the Internet, you choose to make yourself vulnerable. We refer to it as the flu - if you travel around at this time of year, you may randomly catch the flu. If you're going to be on the Net, you will catch things and you will have people try to pick your pocket."

The inclusive nature of instant communication means even people who take the time to be secure will get hit, he notes. E-mail worms forwarded by someone you trust via Outlook would be one example.

"I've seen many cases where a corporate executive was very proud of

himself because he put McAfee and Black Ice on his company's network and was absolutely sure that there was no way anything could happen.

"They get us on phone, we go in the same day or next and a third of their hard drive is porn. Someone has hacked in while one of them was staying at a hotel and loaded all but a sliver of their porn business onto their hard drives."

Mafiaboy was easy to find because he was "way too unskilled. He didn't attack a new vulnerability. He got access to a number of machines that were under very loose control and was an extraordinary braggart about it," says Atkinson.

"That indicated to me that he was someone in his teens, probably not even 18. He was being a little juvenile delinquent, like the guy who burns someone's car and takes a picture of himself with it in before-and-after mode."

Atkinson's overall assessment of security threats is blunt and mirrors that of many users. "It comes from people who have a computer using an operating system or software that is sold by Microsoft and that is defective.

"It's all about money and it doesn't seem to matter any more who's wrong or right. It's about who has the deepest pockets. If attorneys general were as vigorous about software liability as, say, automobile liability, Microsoft would have complete recalls twice a week, regularly."

Coming tomorrow: Going wireless may be convenient, but if not done properly, it could open your machine up to all sorts of malicious threats.