

Cheats, Vandals, Spys and Villians

By Al Emid

August 2003 was a bad month - the worst month, in fact, for Internet viruses and worms, according to the experts. Last summer saw the debut of the Blaster worm, followed by variants such as W32.Blaster.C worm. Following a typical sequence of events, someone writes and releases a new worm, and then the copycats jump in, tweaking the beast and producing their own versions, called variants.

Blaster itself followed seven months of 'net crises over the SoBig virus, its variants, other viruses and then their variants. And viruses are only one danger out there in the wild world of the Internet. There are political activists, porn purveyors, password crackers and good old-fashioned financial scammers. In fact, e-mails like the one that follows are all too common these days.

Note: Spelling has been left uncorrected but contact information has been deleted.

VERY CONFIDENTIAL

Dear Sir or Madam,

I am John Robert, personal Aide to the former President of Liberia — President Charles Taylor who is presently on Presidential Asylum in Nigeria — Cross River State, Calabar.

I know you will be surprise to receive this letter from someone you do not know or have seen before; I got your contact from the Presidential Library. I would want you to treat this letter with ought most confidentiality I need a reliable, trustworthy individual-company to move the sum of US\$40M (Forty Million United States Dollars), which is in a safe custody (company).

In the course of the pressure, which called for President Taylor's handing over power, he secured the above sum and because he had always confided in me, I am part of this deal.

The United Nation had issued a warrant for his arrest and trial on war crime tribunal holding in Sere Leon. Due to this problem, he is not allowed to communicate with the outside world.

I am therefore soliciting your assistance to move the money to your country, as the sharing percentage will be discussed later. If you are interested in striking this with me, then contact me on email and Tel for details.

I look forward to hearing from you urgently.

*Yours faithfully,
John Robert*

NOTE: Due to the confidentiality of this deal, I would want us to go with a code, which is JR40. Each time you call me on phone, simply ask, "What is the code" and if the code is mentioned, do not disclose anything. This is very important.

This type of scam is typical of the problem facing both Canadian 'net users and law enforcement officials, said Constable Patrick Boismenu, an investigator with the RCMP's Integrated Technological Crime Unit in Montreal. "Nigerian fraud (artists) have been attacking Canada for a long time. There is little we can do about it. Why? Because they're in Nigeria and we're here.

They can touch our country, bypassing borders using the phone or letters or e-mail to (trick) people into giving money or bank account numbers. They can (bypass) any security feature that we implement on the borders," he said.

Similarly, many viruses, worms and Trojans originate from America, Russia, China and other Far Eastern countries. "You can't touch anybody outside the country for that type of offence," he said. "Viruses come from around the world."

WORLD WIDE HIT

But as long as you don't call up John Robert and give him your bank account number, there's no problem, right? Wrong.

According to the Australasian Centre for Policing Research in a paper entitled On-Line Security And Electronic Crime. The paper, which focuses on viruses and worms, said "Electronic crime presents one of the major challenges of the future. E-security is a major consideration for business as it strives to maintain competitiveness in a global marketplace and capitalize on the enormous potential benefits of electronic commerce." Moreover, developing countries such as China have weak legislation and sometimes not enough police expertise to enforce the legislation that does exist.

The very nature of technology guarantees a continuing battle, said Gary Bouchard, head of the technology law group at Fogler, Rubinoff, Barristers and Solicitors in Toronto. "You've got people from all over the world developing cutting-edge technology. It's the old oneupmanship problem — good guys keeping up with bad guys and bad guys keeping ahead of good guys — making for constant struggle."

Outside of cyberspace, real-time issues include dollars-and-cents problems. Legal sources suggest that the RCMP understandably directs a large proportion of its limited computer crime-fighting resources toward Internet child pornography, a crime with its own set of complications. For the international spy set, mi2g Ltd., a British security company, predicts an increase in politically motivated digital attacks, although this has not yet been a factor in Canada. "We don't see much of this as politically motivated," said Mark Fernandes, manager of the security services group at Deloitte & Touche in Toronto.

In September, Fernandes predicted more attacks would come in the near future. Shortly after, Microsoft issued an alert about a new-found vulnerability in its Windows system, followed by dire warnings of possible damage from security companies. Microsoft tacitly admitted the continuing struggle in a statement. "Microsoft understands that consumers are increasingly faced with a variety of cyber threats and (is) doing an unprecedented level of outreach to PC users with our "Protect your PC" campaign to help raise awareness of the need for computer users to take steps, and ensure that those steps are as easy to understand and easy to implement as possible," an assertion that does not suggest imminent victory over evil-doing cyber jerks.

SOME GOOD NEWS

On the good news side, Canadian law usually leaves the average computer user clear of liability. "There is no absolutely strict or automatic kind of statutory liability for any of the things that might flow from (unintended) involvement in a virus scenario," Bouchard said. Which means if a virus makes your computer do something bad to another computer, you are probably not going to get dragged into court over it.

Outside Quebec, Canadian common law applies in civil situations such as the now-familiar mass e-mailing of a virus to everyone in an Address Book.

"If there's no contractual relationship between us that would impose a standard on you then you're not going to be liable," Bouchard said. Where sender and receiver have a professional relationship, such as when the Address Book's owner works as a contract computer professional, the situation remains unclear because there are few legal precedents.

On the criminal law side, when authorities do nab ne'er-do-wells, they can charge them under mischief provisions of Section 430 of the Criminal Code, which refers to destroying data or rendering it meaningless. The Code provides penalties ranging from up to two years less a day plus fines for summary conviction and two years or more and a larger fine upon conviction of an indictable offence.

BOYS WITH TOYS

In Canada, the typical 'net villain is a male between 13 and 24 years old, Boismenu said. "For other countries, I'm not sure but I would assume the age group would be very similar." His investigatory caseload has included suspects accused of creating Trojans, often by using freely circulated virus kits, applications which automate the creation of basic malicious code.

The goal for these scoundrels probably rests with Andy Warhol's oft-cited 1976 remark that "in the future everyone will be famous for 15 minutes." They're looking for that 15 minutes. "It's mainly for some type of fame. They want to feel good about themselves. They are kings behind the keyboard," Boismenu said. "And it's these kings who write every virus, worm or Trojan," said Neel Mehta, research engineer at the X-Force, a research and development team at Internet Security Systems in Atlanta. "Quite often they have specific intent and that intent is to cause damage. Code is deliberately written by people and not something that just occurs out of nowhere," he said.

Mehta warns that the near term promises continuing assaults, especially if the manufacturers of operating systems find additional vulnerabilities of the type that allowed Blaster to wreak so much damage. "You can expect more serious vulnerabilities will be encountered in software and there will be the potential for a worm like Blaster to surface again," he said, adding viruses of the type that generate mass e-mailings can get into a computer system regardless of vulnerabilities.

"Those aren't really dependent on vulnerability, just someone's whim. They may choose to release one today or next year."