Tech & Gadgets

By Danny Bradbury, September 15, 2009

The seedy underbelly of online crime

In the wild west of the 21st century, arm yourself with knowledge to avoid criminal minds.

Back in the good old days, you knew when a crime was being committed against you. It wouldn't be pleasant to discover that thieves had ransacked your office, or burgled your house, but at least you'd know that it had happened.

These days, online criminals can steal your banking details, your customer database, and even your online identity without leaving the comfort of their chair — and in many cases, without you knowing until it's too late. Unlike the average city, the Internet does not have its rough and gentrified areas — people can reach your computer from anywhere, which turns the whole place into a bad neighbourhood.

* Symantec's top web threats in the history of the Internet

Brian Bourne, founder of the Security education conference Toronto (SecTor)*, says that the Internet still represents the wild west of the early 21st century. Victims of online crime have little recourse, he warns, especially if the perpetrators are located overseas, as they often are.

The most pervasive means of online exploitation is still the botnet. Both consumer and small business computers can be compromised with malicious software via a variety of means. Once infected with the malicious software (commonly called 'malware'), a computer can be remotely manipulated by the cybercrooks and made to do their bidding.

In the early days of botnets, this remote manipulation was largely used for distributed denial of service (DDoS) attacks, in which large numbers of computers were all made to talk to a single computer on the Internet. The resulting storm of traffic would stop the victim's computer from functioning properly. DDoS attacks are still common today, and can be used for political purposes such as attacking government websites, or for financial gain (if mobsters threaten to take down your ecommerce site for a week before Christmas, how much would you pay to stop it from happening?)

Botnets today are used to send spam from unwitting users' computers, and in some cases to host illegal material such as child pornography on a victim's PC. Even more insidious is the harvesting of information from infected computers, such as online banking or ecommerce passwords, credit card details, and login credentials for online gaming accounts.

More on technology:

Jim Arbogast, Photodisc

Biggest games of the fall
Signs of internet addiction
Weird gadgets that never caught on
Why your laptop fails at coffee shops
Kurt Cobain character in 'Guitar Hero 5'
Blog: The death of DVD?

But how does that malicious software get onto your PC in the first place? Much of it is delivered to poorly protected computers by websites that have been infected with the malware. In times past, you'd have to be visiting the shadier regions of the Internet to become infected with this malware. Unless a site was offering pornography, or pirated software, you

could be considered relatively safe.

However, things are changing. Criminals have invested time and expertise in hacking poorly-written and badly-configured web applications, and are now infecting legitimate web sites with malware en masse. Sites that fell victim to malware infections recently have included BusinessWeek.com, Paul McCartney's website, and even sites operated by the UN. A common tactic involves inserting a command into the website that forces your browser to secretly access another malicious website operated by the criminals. The command checks to see which operating system and browser version you are running. The site will then deliver a specific attack designed to compromise your computer.

*** Video**: Could searching online for Jessica Biel news be dangerous?

Few people are safe, especially as criminals begin to automate the infection process. One recent botnet, Asprox, even instructed the PCs that it infected to automatically hack websites and infect them with malware links, using a pre-written set of instructions.

According to a recent report released by Symantec's Messagelabs subsidiary, the criminals are avoiding detection by hosting their malicious websites using "bulletproof" hosting services that don't respond to takedown requests. They are also using services designed to redirect victims' computers through multiple different online computers before they reach their final destination. This helps to throw law enforcers off the scent.

Nevertheless, cybercrime fighters have had some successes. Recently, Real Host, a Latvian ISP, had its service disconnected by its upstream connectivity provider. The disconnection of the ISP, which was allegedly hosting computers used to control thousands of botnet victims, saw a dramatic fall in the amount of spam associated with Cutwail, a popular botnet. Other ISPs that have been disconnected for alleged involvement in spam, botnet infections and other online crimes include Atrivo, McColo and Pricewert. Regulators and wholesale Internet connectivity providers are getting better at cutting off online criminals at the source.

** SecTor will run from October 6-7 at the Metro Toronto Convention Centre. It will feature presentations and education sessions on protecting your company networks against cybercriminals.*

Join the discussion!

Add a comment

Sort by: Oldest first

1-2 of 2