



Who's watchin' who?

It might surprise you, but your computer is not a benign tool, quietly serving mankind in the information age. In fact it's probably spying on you right now. **Griffin Longley** explores the murky criminal world of zombies and bot-netters and realises just how vulnerable we've become to spy-ware.

Illustration Don Lindsay

Andrew Walls used to work in the online security team at BankWest in Perth. Now he's research director with a partner, one of the biggest technology research groups in the world, and he agrees computers are not a universal helpmeet.

"You think about it like your toaster, sitting there, physically controlled because it is in your house or whatever, but the minute you plug it into the internet it is like you have thrown open the doors of the house and you have invited the world in," he explains.

"There are a lot of clever people out there who want to do bad things. They may be after money. They may just want to mess up your system. Who knows what their motivations are? But they probably know more about technology than you do."

Most of us understand the dangers associated with toasters. Few of us have any real sense of the threats the internet can pose to the unguarded.

Spyware, Trojans, zombies, bot-nets, phishing attacks and cyber-bullying are all part of internet security landscape. They are the pickpockets, fraudsters and toilet wall slanderers of the modern world but how many of us have any idea what they are, let alone how to avoid them? Almost no one, says Mr Walls.

In one attack last month, dubbed "the Italian job", more than 10,000 websites for Italian hotels, travel agents, charities and government departments were infected with spyware — malicious software that

“If your computer is a zombie, it is probably part of a large group of zombies called a government in real life and a “bot-net” in cyberspace. Bot-nets are used by organised crime groups to behave badly.”

allows the attacker to monitor what you do on your computer, potentially giving them access to your bank details, credit card information and passwords. It was the height of the Italian tourist season and anyone who logged on to the infected websites inadvertently downloaded the spyware.

It's a growing problem. In the course of business last year internet security company ScanSafe came across 254 per cent more sites infected with spyware than it had in the year before.

“There is a statistic that is maintained known as the ‘time to live’ and that is if you take an unsecured computer and just put it on the internet and see how many minutes it takes, on average, before the first attack hits it. And these days that is measured in sub-20 minutes,” Mr Walls says.

“If you put your computer out there unprotected it will get hit. Fortunately most of them will fail. Some will be trivial, some may be major attacks, but something will attempt to take over your computer and it will be an automated system that does it.”

And that leads us to zombies. A zombie attack involves your computer being infected with software that allows it to be controlled by someone else over the internet. If your computer is a zombie it is probably part of a large group of zombies called a government in real life and a “bot-net” in cyberspace. Bot-nets are used by organised crime groups to behave badly.

“In the darker areas of the internet there are people who have gathered bot-nets, collections of compromised computers, and hire them out to the highest bidder.

“So if you want to attack a bank or an insurance company or whatever, there are people who for a sufficient amount of money will let you use the

network of compromised computers they have put together. I have seen reports of bot-nets as high as 80,000 computers under a single person's control. Law enforcement agencies around the world are getting a lot more aggressive about trying to track down who is preserving bot-nets, who is setting them up, and trying to break them. But it is like cutting the grass: doing it once doesn't mean it stays down.”

Finding enough lawnmowers has proved a significant challenge. In 2003 the Australian High Tech Crime Centre was set up in Canberra to help meet the challenge to protect government information systems, Australian businesses and private internet users against the complicated, evolving and trans-jurisdictional threats. AHTCC's co-ordinator Peter Sykora says the profile of internet crooks is changing, and not for the better.

“When we were looking at those traditional hackers back in the 70s and 80s, they were people really just testing their own skills and testing the skills of their peers trying to out-do each other,” he says.

“But since the internet has grown and become more involved, we are also seeing some organised groups who conduct criminal activity over the internet. Because of the borderless nature of the internet, it is very difficult to pin it down to any particular country or the like. But we do see a significant problem coming out of Eastern Europe and the Balkans. People have been trying to link it to the Russian Mafia, for instance, but we have no solid evidence of that at all.”

When it comes to the business world, internet security means big dollars. With companies increasingly dependent on computer systems, attacks against them are potentially disastrous. With company records and

financial information and, in some cases, the financial records of clients all stored on company systems, information security is a high priority. And that has helped to make the internet security industry worth an estimated \$US8 billion (\$10 billion) annually.

With offices in West Perth, London and Seattle — and clients all over the world, including top 500 companies, the Australian Stock Exchange and police forces in the US and the UK — WA-based company WebSpy is a significant player in internet security. And the business is based on protecting companies' computer systems from threats from within.

"Employees these days have grown up with the internet and it's second nature for them to use it as a tool at work, and as they use it as a tool, they also communicate with friends, they download stuff from YouTube, they go to MySpace and eBay and the like," WebSpy chief of operations Lagis Zavros says.

"There is constantly activity going on in these areas and that poses threats because employees can inadvertently download something which could cause the networks to clog up and could carry a virus."

WebSpy's software is essentially a reporting tool that mines information out of the logs which store data on every use of the internet. Websites visited, search terms used in Google, the subject lines and content of email sent and received are all logged and can be searched.

"They can get trend reports at a high level and then they have the ability to drill down at an individual level. So they can say, for example, within our organisation for the past month what were the top 10 sites that were accessed.

"And all of a sudden at the top of the list, quite often we see this, is YouTube. From YouTube they can say, OK, who accessed YouTube the most? They click on YouTube and it gives them the top 10 users that accessed that site and then from there they can see how much each person downloaded, what they downloaded. Was it work related?"

Another arm of information security is computer forensics — the job of retrieving often long-lost information out of computers where a serious breach of security is thought to have occurred. In the Perth internet security neighbourhood, Matt Fehon and Darren Michael, from KPMG Forensic, stand pretty tall when it comes to this stuff.

In his previous incarnation Mr Fehon served in the NSW police for 18 years, including a stint in the homicide squad. Since moving into computer forensics he's been involved some well-known investigations, including the HIH collapse.

Mr Michael's history is no less colourful. He's spent 27 years in IT security, six of them with the Federal Police, and back in 2003 was invited on to the United Nations' weapons inspection team in Iraq, examining computer records for evidence of weapons of mass destruction.

A lot of the work the pair, and their colleagues, do involves examining email flows, transaction records and general computer use. In one recent case they were able to trace emails sent among company executives who had been sharing sensitive information. The emails had not been sent on company email but they had accessed webmail via the company internet. Mr Fehon and Mr Michael were able to find remnants of the information shared hidden in documents that were being circulated.

"Another major one was defamatory material that had been posted on a blog site," Mr Michael says.

"The investigation went on for quite a long time and was quite complex but it actually backtracked through the (internet service providers) and we tracked it back to a hotel in the US and from that we were able to look at some of the travel records and figure out which person was actually at the hotel at the time."

Internet defamation and cyber-bullying is a significant problem on the net. With online bad guys having means at their disposal to hide their identity, the internet can become an abuse free-for-all that can have serious repercussions for its victims beyond cyberspace. Enter 28-year-old Harvard law school graduate Michael Fertik and his Silicon Valley company, ReputationDefender.

The company was conceived to help mitigate online attacks like the one launched against Sue Scheff, a consultant to troubled parents of troubled teenagers, after one of her clients turned on her, by either having offensive material removed or burying it under a mountain of positive websites.

At the height of the attack on Ms Scheff a Google search on her would bring up page after page of vitriolic abuse — claims that she was a fraud, a prostitute and a con. The impact was enormous. With more and more people using the internet to research everything from local pizza joints to professional services, the attack was emotionally and financially damaging.

But not even successfully suing the perpetrator for \$US11.3 million (\$13.2 million) could stop the attacks.

The ReputationDefender remedy pushed the abusive comments well down the Google search listings. But after a story on the case appeared in The Washington Post, the attackers renewed their efforts, and the battle for pride of place on Google goes on.

But their services are not limited to defamation and they have customers, including 20 in Australia and one in Landsdale, that range from household names to average Joes.

"Several of our clients are business celebrities and they want a super-discreet handling of their online profile," Mr Fertik says from Silicon Valley.

"And they either want it because there is bad press about them or unwelcome commentary about them that they don't want showing up first, when somebody does



a search on them. Or because they have done something a little wrong and they don't want people to find out about that first. They don't want to hide it but they don't want it to be the first and only thing that people find out about them. Or, in some instances, they just want to promote a certain image about themselves."

The company has a simple policy when it comes to the ethics of manipulating internet search results. They say they won't lie for customers and will not seek to have news articles or government documents removed from the internet. Which is almost reassuring.

"Even here in the US people are not sufficiently cynical about the internet or aware of its dangers," Mr Fertik says.

"When there is unlawful information about you online and somebody reads it, they don't have to believe it beyond a reasonable doubt. That is the legal standard. They just have to believe it enough not to take a risk

Another arm of information security is computer forensics – the job of retrieving often long-lost information out of computers

with you. That threshold is extremely low. If you are applying for a job and somebody online says you are reckless, that is going to cause some doubts. Why would they hire you? If a girl is going on a date with you and she reads that you have herpes online, even if it is total bullshit, is she going to think twice? Maybe."

So what do we do? There is no avoiding the internet in the modern world, so how do we avoid its dangers? Mr Walls says it's simple.

"It is important to realise that you are not going to out-think the bad guys out there," he says.

"They have more time on their hands than you do, so make use of the brains of a company that produce anti-virus, or basic firewall products, but look to advice from experts. Don't simply say, 'I'm OK. I'm small enough. Nobody will bother with me.' And if you do not need to be connected to the internet, don't be because the longer you are connected to the internet, the more attacks you are going to be exposed to." ■

Lagis Zavros, left, from Webspy and Matt Fehon from KPMG.

