Crackers, phishing, worms, Trojans & zombies are out to **get you!**

By Rob Davis

Here is something you don't want to know but need to know. No computer network is 100% secure and eventually you will become (if you have not already) a victim of computer attack. What this means is that if you have a computer and use the internet then you will eventually lose data, have your identity hijacked and probably be a victim of credit card fraud.

Fifteen years ago most computer attacks came from pimply faced kids with access to a modem, a PC and too much time on their hands. What started as simple pranks and a way to kill time has since morphed into a global enterprise run by crime syndicates whose activities threaten the future of the internet. These operations use skilled crackers and sophisticated technology to steal credit card, bank account and identity details from ordinary computer users around the world.

CRACKER TRICKS

A 'cracker' is a malicious hacker, sometimes called (in the adolescent language of smart people who drink too much caffeine and lack a real life) 'black-hats'. They are people who, for fun or profit, devote themselves to breaking into computer systems and stealing information.

Their techniques can be reduced to three simple strategies:

1. Accessing unprotected computers.
2. Breaking into protected networks and computer systems, either by brute force, exploitation of security weaknesses in operating systems, or by employing a bewildering variety of technologies and techniques to induce users to allow them in.
3. Inducing internet users to give them their credit card details by intercepting emails or using bogus websites cloned to resemble secure sites of banks, software suppliers, and others that provide e-commerce facilities over the internet.

It is surprising how many computer-users have performed operating system installations where all security has been turned off by default. These users leave themselves as wide open to theft as a houseowner who goes out and leaves the front door open. No talent or skill is needed to enter an unlocked system. All that is necessary is for someone with the right software to detect the computer on the network and enter it. This software is readily available. Indeed, statistics from the US suggest that computers connected to the internet are quickly detected by automated software belonging to crackers.

Ensuring your system is password-protected is little help if you do not choose an appropriate password or do not make concerted efforts to repel attempts to enter it by stealth. For example, most users do not monitor their systems for probing by automated systems using simple dictionary attacks. This makes many computers protected by common passwords (such as names or birth dates) vulnerable to frontal attack in a relatively short period of time.

These attacks are made easier if the attacker already knows the identity of the person against whom the attack is made. For example, crackers commonly use social engineering (identity spoofing) to induce staff (whose identities and positions are commonly published in corporate websites) to part with user names and passwords. All that is necessary, often, is a couple of calls to different staff at different times to find out discrete pieces of information, such as the name of a computer supplier. The cracker then uses that information to contact the supplier, pretending to be from the 'client' to find out information about the computer system of the client. This information may be all they need to exploit weaknesses in the client's security. But if it is not, then the cracker can use the information obtained from the supplier to induce the client's staff to reveal system passwords. A common trick is for a cracker to pretend to be from a software supplier needing access to upload system upgrades, etc.

The most common form of attack, for ordinary home compute-users at least, is from spyware, worms and Trojans that the computer-owner unwittingly installs themselves. These are small executable software applications that usually enter a user's computer either as attachments to emails, or as

>>

code added to otherwise innocuous documents (such as text files, spreadsheets, etc). These applications can perform a range of functions, from taking control of the user's computer, logging and reporting on keystrokes, or providing a back door to permit a cracker to enter the computer at will.

A more insidious, and rapidly expanding, form of fraud known as 'phishing' requires very little computer knowledge. This technique clones websites belonging to major banks and 'trusted' e-commerce providers (such as credit card companies); hosts these bogus clones on systems of unsuspecting internet users; and directs traffic to these bogus sites to fish for usernames and passwords. Traffic is commonly driven to the bogus sites by spam emails, pretending to be from the trusted company, asking the unsuspecting user to click a link to change password details. Naturally, to change the password the user has to type in their valid user name and password, which are then sent to the cracker for illicit use. The unsuspecting user remains unaware that they have been conned out of their password until they get their next credit card bill or bank statement.

Phishing scams vary widely in their sophistication. At the low end they are crude and rarely withstand the sceptical scrutiny of most computer-users. Of course, the instigators of the scam don't care if the majority of users smell a rat. They broadcast the same spam to millions of users in a particular country domain, and if only a fraction of the recipients are conned that is all that is necessary for them to make tens of thousands, possibly millions, from each attempt. Other scams employ very skilled coding to mask features that might otherwise lead someone to suspect the site is a fraud. For example, a cloned web page may contain Java script that obscures the address bar of the user's browser with, what on ordinary inspection, appears to be the address of the legitimate secure site.

PROTECT YOURSELF

There are a number of things that you can do to reduce the risk that you will fall victim to computer fraud:

1. Ensure your operating system's security features are turned on and properly configured (for example, use firewall protection).
2. Use passwords that are difficult or impossible to guess (for example, mix text and numbers into strings at least eight items long) and change them regularly.
3. Back up all critical data daily on removable media using a rotating schedule and verify all back-ups for integrity.
4. Use virus protection to screen all material entering the computer (but remember to keep your virus definitions updated to protect against new variants).
5. Never open email attachments or install software unless it is from an absolutely trusted source (be careful of all email attachments as they may not be from the person whose name appears as sender).
6. Regularly download and install security patches from the supplier of your operating system.
7. Use a more secure operating system (for example, the Mac OS, because of its market niche, has remained free of attacks from worms or Trojans, whereas some others have a lamentable history of poor attention to security).
8. Do not remain online when you are not using your computer (nobody can crack into a computer when it is physically disconnected from the internet).
9. Avoid using e-commerce facilities on the internet unless you are absolutely sure that you have a secure (encrypted) connection to the party you think you are dealing with and that party is a trusted reputable entity.
10. Ensure your staff (if you operate a network with dial-in access or connected to the internet) never divulge password details to anyone. ■

Notes: **1** John K Waters, *Can Hackers Be Stopped*, (6/3/02), *www.adtmag.com/article.asp?id=6401*.
2 VeriSign Alert, *Internet Commerce Grows 13.2%; Phishing Attacks Become More Acute and Globally Diverse* (26/7/04), *http://security.ittoolbox.com/common/print.asp?i=118514*.
3 Several of these are adapted from article by John K Waters, 'Seven Security Basics', (6/3/02), *www.adtmag.com/article.asp?id=60402*. Also see article entitled: *Computer & Network Security & Computer Viruses*, *www.davislogic.com/computer_security.htm#Guidelines*.

Rob Davis *practises as a trial and inquest advocate, mediator and law practice consultant. He can be contacted at www.davislegal.com.au.*