



TECHNOLOGY INSIGHTS

These are our own opinions.

We have no commercial
arrangements with vendors.

For more reviews, please
contact TECHNOLEDGE.

T +61 2 9909 0246
E info@technoledge.com.au
W www.technoledge.com.au

Security Jargon Glossary The Pocket Edition

Backdoor - a [program](#) that enters a PC and creates a backdoor through which it controls the affected system without the user realizing.

Dialer - a [program](#) that is used to redirect Internet connections and hook a PC user up to a premium rate number. Often, the user remains unaware of the switch until he gets an enormous phone bill.

Keylogger - a [program](#) that collects and saves a list of all keystrokes made by a user. The creators of the program have access to the list of keystrokes and analyse it for passwords, account numbers, emails and so on.

Malware – a general term used for [programs](#) that contain malicious [code](#).

P2P (Peer to peer) - a [program](#) or [network](#) connection used to provide services via the Internet (usually file sharing), which viruses and other kinds of threats can use to propagate. Some examples of P2P services are KaZaA, Emule and eDonkey.

Password stealer - a [program](#) designed to obtain user passwords. Password stealers tend to work in conjunction with other malware, such as keyloggers.

Phishing – emails from apparently reliable sources that try to make users reveal banking information by sending them to a spoof web page and asking them to confirm or update their details.

Potentially Unwanted Program (PUP) – any program that is installed without the user's express permission. One example is Microsoft's *Malicious Software Removal Tool*, which Redmond dispatches and installs millions of PCs once a month, usually among Windows updates. Most users don't even know they're downloading it.

Rootkits are designed to hide malware processes, files or Windows registry [entries](#), including their own. Rootkits are also used by [hackers](#) to cover their tracks in systems they've had their way with.

Spyware collects information about browsing activity, preferences and interests. The data collected is sold to third-parties who target the user with messages advertising their wares and services.

Trojans are programs that, once installed, carry out actions designed to compromise user confidentiality. Trojans can have similar effects as viruses but do not replicate.

Viruses are [programs](#) that can enter computers in a number of ways, causing effects that range from simply annoying to highly-destructive and irreparable.

Zombie - A computer controlled through the use of [bots](#). The owner of the botnet sends instructions to the zombies, which can include updating the bot, downloading a new threat, displaying advertising or launching [denial of service](#) attacks.

Zoo Virus – a virus that is not in circulation but only exist in laboratories, where they are used for researching the techniques and effects of viruses. Its opposite number is an in-the-wild virus.

For more details on current threats, check [THE SECURITY LANDSCAPE](#)

For techniques and tools that help keep malware away, see [DRIVER TRAINING](#)