Australian Government
Australian Institute of Criminology

<AHTCC>
AUSTRALIAN HIGH TECH CRIME CENTRE

no. 10 ▪ 2006 HIGH TECH CRIME BRIEF

Malware – viruses, worms, Trojan horses

Malware refers to malicious software. Software is potentially malicious if it can be used to harm either the computer on which it is hosted or another computer. Software may also be considered malicious if it is designed to install itself on a computer without the permission of the owner of that computer, particularly if it does so in a way that may compromise the security of the computer. *Malicious* may be loosely interpreted. A piece of software may be considered malicious even though it may have been launched with the intention of providing an arguable benefit. For example, the Nachi worm was intended to install updates from Microsoft's website. A wider term is *unwanted software* which includes spyware and adware.

Exploiting vulnerabilities

Most malicious software takes advantage of the vulnerability-exploit cycle in software development. Software is essentially code which tells a computer what to do. Developers have worked to ensure ease of use and high levels of interoperability between systems and applications. On a framework of globally connected computers, this ease of use and interoperability have come at the expense of security. Software applications can be created with inherent weaknesses that may only be apparent once the application is launched or which may be known as a theoretical possibility but the malicious use of which may not be contemplated. A security weakness in software is known as a vulnerability.

Hackers look for and test computer vulnerabilities. Part of that process may entail developing a 'proof of concept' which demonstrates that the vulnerability actually exists. The next stage in the cycle is the creation by a person with malicious intent, of an exploit which is used to gain unauthorised access to a computer or initiate specific malicious acts such as a denial of service of a computer system.

Developers may seek to repair the vulnerability in the software by creating a patch to re-write the vulnerable part of the software code to prevent it being misused. Protection will then depend on the user applying the patch before being infected by the malicious software. In the vulnerability-exploit cycle, Symantec

Table 1: Common malicious software distribution agents

Agent	Method of distribution	Insertion method	Self-executing or not	Examples
Hacking	Directed intrusion into a remote computer by a hacker	Direct transfer in course of hack	Manner of execution determined by hacker	
Virus	Self replicating	Attaches to host program	Activation can execute commands to harm computer	Jerusalem (1987) Michelangelo (1992) Love Bug (2000) Nimda (2001)
Worm	Self replicating	Stand alone and self executing	Can execute commands to harm computer	Morris (1988) Melissa (1999) Code Red (2001) Netsky (2004) Sasser (2004)
Trojan horse	Sometimes defined as unwanted or malicious software disguised as useful software	Hidden in a host program or inserted and hidden in the host computer	Can execute commands to harm computer Can take control of computer	AOL variants Netbus (1998) Back Orifice (1998, 2000) Clagger (2006)
Blended threat	Combining more than one of the above techniques in concert	Self inserting	Combined methods	Blaster (2003) Sobig (2003) SQL Slammer (2003)

Project no. 0074a

ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

DISCLAIMER
This research paper does not necessarily reflect the policy position of the Australian Government, the AIC or the AHTCC.

CONTACT
Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601

T: 02 6260 9200
F: 02 6260 9201
www.aic.gov.au

estimated that, in 2006, the average time between the exposure of a vulnerability and the creation of an exploit is 6.8 days (6 days in 2005) whereas the average time to the release of a patch is 42 days (54 days in 2005). An unprotected computer is likely to be attacked within an hour after connection to the Internet (Symantec 2006).

A more immediate line of defence is the use of regularly updated anti-viral software on a computer. Anti-virus products target known forms of malicious software and operate to block, delete or disable the unwanted code before it has a chance of being executed on the protected computer and exploiting vulnerability on that computer.

Distribution related malware

Hacking, viruses, worms and Trojan horses all involve unauthorised access to, or modification or use of, computers or data. The characteristics of each are summarised in Table 1. While actively propagating, viruses and worms may have the effect of degrading the capacity or operation of a network or computer by tying up bandwidth or the processing capacity of servers or individual computers. A virus depends on another piece of software to become active. A common form of viral transmission has been through the use of email. In contrast, a worm does not depend on another piece of software and is self replicating. Trojan horse software may or may not be self replicating but is disguised within some other software that a user might be enticed to activate on their computer.

The Symantec *Internet security threat report* (2005 & 2006) notes that the threat environment has shifted from large, multipurpose attacks on network perimeters, often motivated by curiosity and the desire to show off, to focused attacks on client-side targets motivated largely by profit. Because of this, there is a shift in how malicious software is analysed, from looking at the technical differences between viruses, worms and Trojans, to examining the type of harm that these distribution agents do to individual computers. Early viruses such as Michelangelo caused less damage than predicted. However, the Love Bug virus infected large numbers of computers worldwide and caused substantial losses. The Sasser and Netsky worms are examples of large scale applications that had a severe impact across the Internet. Viruses and worms infecting mobile phones and hand-held computers have begun to appear.

Families and variants

Within the vulnerability-exploit cycle, a hacker may develop a distinct form of malicious code that is not based on other malicious code already in existence. Each new form of code establishes a family of code and subsequent iterations based on that form are known as variants. Symantec (2005) reports that while the number of families of Win32 viruses and worms has remained fairly static, the number of variants had risen dramatically from 994 in June 2003 to 10,866 in June 2005. Symantec attributes the proliferation of variants to the implementation of bot features. A bot allows an infected computer to be taken over by a remote computer. The infected computer is referred to as a zombie.

Threat assessment

One way of comparing the relative risk associated with a vulnerability is to look at the level of access that it allows to a third party. The highest level of risk arises where privileged access is granted, allowing an intruder to execute code or alter arbitrary system files. A medium level of risk exists where an intruder has immediate access to a system with less than privileged access. An intruder may capture a password file and use it to seek privileged access. A low level of risk arises where the vulnerability enables the intruder to gather information that might be used to further compromise the computer.

Another measure of threat looks at a combination of three factors being the extent, severity and virulence of the software (see Table 2).

Table 2: Threat assessment: key measures

EXTENT – THE EXTENT TO WHICH THE SOFTWARE IS 'IN THE WILD'	**SEVERITY** – THE DAMAGE CAUSED IF ENCOUNTERED	**VIRULENCE** – THE RATE AT WHICH A MALICIOUS PROGRAM SPREADS
› Number of independent sites	› Triggered events	› Large scale email attack (worm)
› Number of computers affected	› Clogged email servers	› Executable code attack (virus)
› Geographic distribution	› Deleted/modified files	› Spreads only through download or copy (Trojan)
› Ability to combat threat	› Release of confidential information	› Network drive infection capability
› Virus complexity	› Performance degradation	› Difficulty to remove/repair
	› Compromised security settings	
	› Ease of fixing damage	

FURTHER READING

All URLs were correct at 6 April 2006

New scientist tech n.d. Special reports: computer viruses. http://www.newscientisttech.com/channel/tech/electronic-threats

Sophos n.d. Virus info: learn more about viruses, Trojans, hoaxes, spyware and adware. http://www.sophos.com/virusinfo

Symantec 2006. Internet security threat report vol. 9. http://www.symantec.com/enterprise/threatreport

Symantec 2005. Internet security threat report vol. 8. http://www.symantec.com/enterprise/threatreport