New Zealand Security of Information Technology Publication 208

DEALING WITH MALICIOUS SOFTWARE

CHAPTER 1

INTRODUCTION

Introduction

101. "Malicious software" is a general term covering several types of computer code intended to compromise an Information Technology (IT) system. This can occur by affecting the system's availability, corrupting its integrity or breaking its confidentiality. The main categories of malware are *Viruses, Worms, Logic Bombs, Trojan Horses* and *Hoaxes.* Some malware may behave with actions from more than one of these categories, this is known as a *blended threat*

102. Some forms of malicious software, especially viruses, present a significant risk to the integrity, availability and confidentiality of New Zealand's IT systems. Relatively simple countermeasures can minimise this risk. A key countermeasure is high user awareness of the problem. This document provides practical advice on how to implement the policy outlined in the "Security in Government Sector" document and describes:

a. the various types of malicious software that could affect your system:

b. how they are disseminated;

c. what you can do to reduce the risk of infection;

d. how to deal with an infection if it occurs.

103. Variants of malicious software types appear almost on a daily basis. The visible impact on your system may be different from that described though the general advice contained in this document will be relevant. Information relating to specific instances of malicious software types and the individual threats they pose will be maintained in the web page of the Centre for Critical Infrastructure Protection(www.ccip.govt.nz) â€“ see Chapter 7 "Liaison, Reporting, and Assistance" later in this document.

CHAPTER 2

VIRUSES

Nature of the Threat

201. Most viruses are designed to attack personal computers running the most popular operating systems. Currently these are Microsoft Windows 9x, 2000/ME and NT. Viruses have been written for other operating systems such as Linux and the Apple Macintosh environment but these make up a small proportion of the overall virus population.

202. Virus writers have also realised the potential of macro and scripting languages. The macro language facility in Microsoft Office products, especially Microsoft Word, provides a new environment for virus writers. Others application documents such as Powerpoint and Excel can also be infected by this method. This technique also allows macro viruses to cross to different operating systems. For example, an infected Word document created on a Windows machine might run on an Apple Macintosh running Word.

203. The popularity of Microsoft Word has led to the majority of macro viruses to date being written for this, and other, Microsoft Office products. IT staff should not assume the macro virus problem only exists for Microsoft - any product that gains popularity and has a facility to execute system functions is liable to be exploited by virus writers.

Vulnerabilities

204. Any form of executable file or object is vulnerable to virus infection. Once activated the virus payload may attack any file stored within the system, or any system within a network. The virus may take control of the computer, and use it for other purposes, such as attacking other computers. Systems are particularly vulnerable in working areas where access and the circulation of floppy disks are uncontrolled. E-mail attachments are now the primary method for transporting infected objects.

205. Actual infection of a host computer occurs when the virus code is executed. Most viruses are designed so that the act of executing them is triggered without the knowledge or consent of the user, when a normal process is carried out.

Carriers

206. Any medium that can be used for storing or transmitting data is potentially a carrier. Carriers therefore *include:* floppy disks, removable hard disks, magnetic tape cartridges, optical disks, CD-ROMs, disk fax machines and e-mail attachments.

Infiltration Sources

207. Common sources of infection may include:

a. pirated software;

b. bulletin boards;

c. shareware;

d. public domain software;

e. exchange of files with home computers;

f. cover disks on magazines;

g. service engineers;

h. shrink-wrapped software;

i. pre-installed software on hard disks;

j. pre-formatted floppy disks;

k. reputable suppliers of software;

l. e-mail attachments;

m. public networks eg Internet (this includes all services, such as the World Wide Web, Peer to Peer networking, and Internet Relay Chat);

n. word processor document files with embedded macros;

o. other documents (e.g. spreadsheet, database and presentation) with embedded macros;

p. consultants, contractors, visitors, colleagues and others.

Risks and how to reduce them

208. The number of viruses now in existence, the number of infiltration routes, and the general susceptibility of computer-based office systems to virus attack, lead to a generally high risk of infection. This risk will be at its highest where there is a large user community and a culture that permits free interchange of unchecked media.

209. The main aspects of an effective anti-virus policy are as follows:

a. on-access (real-time) and on-demand scanning where appropriate, using reputable anti-virus products. This applies to file servers and e-mail servers as well as workstations;

b. immediate application of scanning software updates;

c. anti-virus awareness training;

d. effective physical security, with practical physical access controls;

e. good configuration control;

f. effective system administration;

g. having and enforcing a policy on which software may be used, and requiring appropriate authorisation and virus scanning before new software is used;

h. purchasing software only from reputable dealers or software houses. Note: these should still be checked by an anti-virus product before use;

i. transferring software only via dedicated links between trusted sites. Note: these should still be checked by an anti-virus product before use;

j. prohibiting the use of software downloaded from the Internet unless that software is from a trusted source, and has been virus scanned;

k. approved password controlled access;

l. adequate protection of passwords.

Countermeasures

210. Anti-virus scanning software, available commercially, is obviously an important tool, but for greatest effect it needs to form part of a suite of measures addressing:

a. preparedness, including user training and awareness;

b. prevention and detection;

c. containment;

d. recovery

211. Some of the steps recommended here are part of good general IT Security practice, but they are included here for completeness.

212. These steps should be completed before a virus strikes:

a. **Create and enforce an anti-virus software policy.** Install anti-virus software and apply regular updates. Provide training to management and users, ensuring they understand the consequences of a viral infection;

b. **Make regular and sound backups.** All backups must be sound, with the integrity of the system and data being assured at the time the backup is made, and at regular subsequent intervals. Media should be write-protected, archived and stored in a safe place;

c. **Create a write-protected system recovery set.** This will normally be a floppy disk set or bootable CD. It should be prepared in advance and archived. It should contain all the system files and relevant device drivers that are essential for recovery. It is important to ensure that the media to be used to create the set are free from infection and created on a clean system.

d. **Create a contingency plan.** This should be produced in accordance with the guidelines located in the NZSIT101 - IT SECURITY POLICY HANDBOOK document. It should contain:

(i). Immediate response procedures, including a method to determine the severity of the incident and listing urgent steps required;

(ii). Names, addresses and telephone numbers of the on-site trained security staff and deputies responsible for dealing with the attack;

(iii). Details of external consultant(s) or specialists who can provide guidance and help in dealing with the attack;

(iv). Specific procedures for isolating infected media, computers and networks;

(v). Public relations guidance where appropriate.

top

Prevention and Detection

213. As ever, prevention is better than cure. Good housekeeping and good procedural habits are vital and will lead to detection before a virus infects the system. Steps include:

a. **Create user awareness.** This is the most important factor in an effective virus prevention policy. Through effective guidance and education, users must be made aware that using unauthorised software, such as demonstration disks and games can lead to virus penetration of the best-guarded system. Awareness material can include leaflets, posters, videos, virus demonstrations and presentations. The potential cost of an incident is such that deliberate introduction of a virus should merit specific mention in any staff disciplinary code. Any such sanction should be widely publicised.

b. **Follow hygiene rules.** Hygiene rules should be clear and well publicised, as should the disciplinary consequences of disobeying such rules. Advice to staff should make the following points:

(i). Virus check/scan all incoming media before use;

(ii). Virus check/scan all outgoing media. This includes CDs generated on site;

(iii). Do not use media from computer magazines;

(iv). Be careful when bringing in any media from outside your place of work;

(v). Beware of diagnostic media and devices used by service engineers;

(vi). Use only software from reputable manufacturers; don't use pirated software;

(vii). Conduct regular checks of software on systems supporting critical processes. Formally investigate any unauthorised files or amendments that are found.

(viii). Be particularly careful to check any existing software, which may have been downloaded from bulletin boards, shareware and public domain software from unknown sources.

(ix). Treat all e-mail attachments with caution:

A. Attachments from trusted sources may be opened if an on-access anti-virus scanner is installed.;

B. Attachments from other sources should not be opened. If there is a need to open one it should be done on a dirty PC (see paragraph 213(D)(v)).

(x). Write-protect floppy disks where possible;

c. **Scanning**. Make sure that all computer data in transit is examined by at least one anti-virus product. This may be achieved by a combination of the methods described below:

(i). **On-access scanner**: This anti-virus product type is installed on the workstation and examines each file for viruses when the file is opened. This applies to data and executable files. On access scanners may impact of workstation performance but have the benefit of detecting an infected file that may have passed unnoticed through other scanner types. This is because other scanners may not see the true file content if it is in an encrypted, compressed (non-standard) or password-protected state. When a file is opened for reading, writing or execution it cannot hide behind any of the states mentioned above. It is at this point that the on-access scanner strikes. Due to the possible performance degradation from this method, it should only be required on high availability systems. A risk analysis should be performed on the system, and this method only used where required.

(ii). **On-demand scanner:** A partial or complete scan of one or more disks or CDs is initiated by the user on an ad hoc or scheduled basis. It is normally installed on workstations and fileservers.

(iii). **E-mail scanner:** This scans all e-mail before it is passed through to the destination e-mail server. It is a good network design to use this (on a server) in combination with on-access scanners on workstations.

(iv). **Checksumming software**: This is often included as a component of anti-virus software but can also be purchased as a stand-alone product. It detects changes in a fileâ€™s contents allowing it to detect the presence of previously unknown viruses. Unfortunately it will also detect legitimate changes to files and may not be able to differentiate these from malicious causes.

(v). **Heuristics**: This component of most reputable anti-virus products looks for â€˜virus typeâ€™ code in executable files. It allows for some previously unknown viruses to be detected but occasionally declares a clean file to be infected (false positive).

d. **Implement Access Controls**

(i). **PCs:** where there is a risk of unauthorised users getting access to equipment and introducing unchecked software, access or guard control products (physical or software) may be appropriate, if these are not already in place for other IT security reasons.

(ii). **Networks:** most network operating systems employ security features which if applied correctly will provide adequate file protection. Any file or directory on the network that the user can modify is at risk from a virus. The system administrator should adhere to the following rules when setting permissions for files/directories on the network:

A. All executable files and shared templates on the network should be put into a read-only directory.

B. Each user should have their own private home directory on the network. Other users may be allowed to read from but not write to these home directories. If a userâ€™s workstation becomes infected the same userâ€™s home directory on the network may also become infected but the rest of the network will be safe.

C. There is often a requirement for shared directories on the network. These allow, for example, for documents to be created and modified by more than one user. If one userâ€™s workstation becomes infected the shared directory may become infected. If a second uninfected user workstation then accesses files on the shared directory this too may become infected. Each time a file is accessed from the shared directory it should be treated with caution and checked with anti-virus software prior to opening.

(iii). **Disabling "Drive A" Booting:** booting a PC with a floppy disk inadvertently left in Drive A is a common source of boot sector virus infection. Consider setting the "Try Hard Disk First" option (located in the BIOS at system startup) to ensure that the default action of looking for a boot disk in Drive A first is disabled. This ensures that an accidental boot from Drive A is prevented.

(iv). **Establishing a Quarantine PC:** a stand-alone machine, not connected to any network and under strict access and configuration control, should be

provided for running virus-scanning software to check all media entering and leaving the organisation. It is important that this computer should be restricted to this purpose. Success depends on making sure that all imported media (and where appropriate, all exported media) are scanned. Commercial disk authorisation products are available which prevent the use of floppy disks on an organisation's computers until they have been checked and electronically labelled.

(v). **Providing a Dirty PC:** in larger IT set-ups, it may be possible to reduce risk further by setting aside a stand-alone machine for trying out new software or doing anything that could be considered dangerous on a machine carrying operational data. Clearly, it is important that its use should be strictly limited to such functions. A quarantine PC should only be used for virus scanning media, whereas a "dirty" PC can be used to test new software or hardware configurations etc.

top

Containment

214. Once an infection has been detected, take the following steps:

a. **General:** identify and isolate infected computers, servers and media;

b. **Network Access:** depending upon the type and where on the network the virus has been detected, consider physically disconnecting the computers from the network;

c. **Media Interchange:** suspend any media interchange between the infected PC and others;

d. **Write Protect Tabs:** any disks etc used on a potentially infected machine are at risk from infection and should be write-protected if possible;

e. **Alert:** trace and warn all potential recipients of data from infected machines.

f. **Notify:** Report virus incidents to CCIPâ€“ see - Chapter 7 Reports - for details.

Recovery

215. Recovery from a virus attack involves two main stages:

a. Removal and elimination of the virus from infected media. This includes e-mail attachments on workstations and servers and the destruction of infected CDs.

b. Recovery from any side effects introduced by the virus. Use the disinfection utilities of an anti-virus software package. Ready-prepared backups and original master disks will be important elements of a successful recovery.

Anti-virus Disinfection Utilities

216. Many anti-virus software packages incorporate "disinfection" utilities designed to eliminate the virus from infected disks. Generally, these are particularly effective against boot sector viruses. However, it is important to realise that although a virus may have been removed successfully, its effects may still be present elsewhere in the system. After a virus infection, a decision must be made whether to attempt to disinfect the system, or rebuild it from scratch. If the decision is made to disinfect, data files will need to be inspected, repaired or restored from backups as required. Where many files have been infected and the virus has been correctly identified, the use of disinfection utilities may considerably speed up and minimise the cost of recovery. In the case of widespread infection, it may be worth seeking additional guidance from the maker of the anti-virus package you are using in reducing the cost of recovery.

Reinfection

217. This may occur after the "clean-up" has been completed. All it takes is one missed floppy disk or e-mail. Thoroughness and attention to detail will reduce the risk of reinfection. Disk authorisation software, which writes soft marks on all floppy disks to be used, may be employed to minimise the chance of this occurring. Complementary software, installed on a user's machine, will only allow access to disks with the electronic marks. These marks are then used to indicate which disks have been scanned.

Recovery from Side Effects

218. The range and scale of damage will depend on the virus. Many viruses spread without delivering a payload, but some make subtle changes to data files and others may overwrite large areas of the hard disk. Partial or complete restoring of the hard disk from the most recent backup may be the only solution.

Other Points

219. Remember: **Don't panic!** Very often more damage is done by users attempting to recover from a virus attack, than by the virus itself. This is why a plan and a methodology to recover from a virus attack is essential. Users who are unable to recover using anti-virus disinfection software or any written guidance should seek assistance from their IT Security Officer. Discover and close the loopholes which allowed the virus to enter or leave the work area.

220. Warn any outside recipients of possibly infected disks.

221. Consider any public relations angles if the incident is likely to attract external notice.

CHAPTER 3

TROJAN HORSES

Nature of the Threat

301. The target victim for trojan writers is typically the same as virus writers, namely the most popular personal computer operating systems and environments.

302. A Trojan Horse differs from a virus in the following way:

A virus will normally attach itself to another program or computer file. In doing so, it allows the program to maintain its original functionality. When this "host" program is run, the virus may infect other objects and may execute a destructive (or harmless) payload.

A Trojan Horse may be distributed along with other software, but does not infect other objects, and can exist on its own.

Vulnerabilities

303. The measures described for viruses apply equally to trojans. Signatures of known trojans are included in most reputable anti-virus products. The additional risk is that anti-virus products, even with heuristics enabled, will be unlikely to detect new trojans. This is because it is extremely difficult to define malicious but non-viral activity in general terms. For example: deleting a directory or e-mailing a file to another user are actions a trojan may take but are equally valid for the user to initiate. Some trojans may record and disseminate keystrokes, or allow distant users to control the target system, possibly circumventing a firewall.

304. The additional risk can only be countered by:

a. strictly observing the rule to only run approved software;

b. checksumming software.

CHAPTER 4

HOAXES

Nature of the Threat

401. Hoaxes are harmless messages normally transmitted by e-mail. They warn of a computer or network threat that does not really exist. Part of the message often contains a suggestion to forward the message to other people.

Risks

402. A system connected to the Internet is likely to receive the occasional hoax e-mail. This is not a problem if the users have been educated to deal with hoaxes properly. Uninformed users may pass on the hoax causing unnecessary panic and wasting the time of IT support, security and other staff, as well as increasing network traffic and affecting performance.

Countermeasures

403. IT staff should be aware of the latest hoaxes or have reliable contacts to confirm or deny that a hoax is indeed a hoax.

404. Users should be told about the concept of hoaxes and informed that deleting rather than forwarding is the correct action to take.

CHAPTER 5

WORMS

Nature of the Threat

501. Worms are similar to viruses but reproduce in their entirety, creating exact copies of themselves without needing a "carrier" program. Worms were first noted as a threat when the *Christmas Tree Executable* attacked IBM mainframes in December 1987, bringing down the world-wide IBM network.

Vulnerabilities

502. Worms exploit vulnerabilities in the operating system or inadequate system management controls to replicate. The worm uses up space on a computer system, causing it to slow down or even crash, and thus the impact of an infection will be quickly felt. The risk is increased through the use of public networks, such as the Internet, without proper safeguards - such as firewalls. The *Internet worm* was released on 2 November 1988 and attacked Sun and DEC systems attached to the Internet. Its success depended on the wide absence of adequate security controls. It utilised the TCP/IP protocols, common application layer protocols, operating system bugs and a variety of system administration flaws to propagate. This resulted in extremely poor system response and denial of service.

Carriers

503. Typically, worms are carried across and move around the interconnection infrastructure of computer networks.

Infiltration Sources

504. These are mainly public computer networks and communications bearers. Additionally, worms have become a favourite tool of hackers who exploit their properties to conduct automated hacking attacks.

Risks

505. Providing there are no direct (uncontrolled) connections to any public network, the risk of worm attacks on official systems is low. If the worm is introduced in the form of a trojan or e-mail attachment it will then spread from the inside as was demonstrated by the "Nimda" worm.

Countermeasures

506. Worms propagate through vulnerable computer services. Therefore, through correct system configuration, a reasonable level of protection can be achieved. This configuration should include disabling all unnecessary services, applying file and directory access rights on the "least-needed" principle, and enabling strong access control. System managers should be properly trained in the security aspects of system configuration and measures implemented to ensure that operating system updates designed to plug security loopholes are applied promptly. They should also have access to any relevant alerts or briefings put out by security groups. Many virus scanners include definitions for worms, so a virus scanner should also be used, as suggested in Chapter 2.

CHAPTER 6

LOGIC BOMBS

Nature of the Threat

601. A logic bomb is a section of malicious code contained in a useful program, that executes when a certain condition is fulfilled. Although many viruses contain malicious payloads that are conditionally triggered, these are not usually considered to be logic bombs as they are not intentionally introduced into the system. The condition can be based on time or the presence or absence of data such as a name. Few cases have been reported in the public sector.

Vulnerabilities

602. Situations favouring the introduction of logic bombs could include:

a. poor staff relations;

b. lack of proper configuration control;

c. system support procedures that are all in the hands of one person;

d. ill-defined or poorly controlled system responsibilities, such as might happen where services are remote or sub-contracted.

603. Infection by logic bomb is frequently the work of a disaffected computer staff member and tends to be technically complex. A classic case involved a programmer who maintained his company's payroll package. Concerned about his continuing employment, he introduced a logic bomb that checked to see if his payroll number was in the payroll file. If it was, no action was taken, but if it was not, the file and other important computer records would be erased. When he was eventually fired, the logic bomb was triggered and the company's system was brought to a halt.

Carriers

604. The carrier is the code within which the logic bomb is embedded.

Infiltration Sources

605. A logic bomb is usually an inside job by someone with direct system access.

Risks

606. Providing trusted system support staff are employed, the risk to systems is generally low. The risk can be further reduced through

a. Strong change control of programs in development;

b. Using recognised development methodology.

Countermeasures

607. These include good software configuration control procedures; using approved commercial software from trusted sources; good IT awareness, and attention to any relevant alerts or briefings. Logic Bombs are very difficult to detect without prior indication. If there are grounds for suspecting an attack of this sort, suggested methods of detection include:

a. Program code comparison;

b. Testing of suspected program.

CHAPTER 7

LIAISON, REPORTING AND ASSISTANCE

Liaison

701. For computer security matters, the normal IT security contact in departments is the Departmental Security Officer (DSO). Some departments may wish to delegate the computer security liaison function to a specific Information Technology Security Officer (ITSOs).

702. From time to time GCSB may coordinate computer security working group meetings of DSOs/ITSOs to discuss computer security issues and provide a forum for interdepartmental discussions.

Reporting

703. Any acts of espionage, sabotage, terrorism, or subversion involving COMPUSEC violations are to be reported to the GCSB. Departments should also report any other computer security attack so that vulnerabilities can be identified and other departments notified accordingly.

704. To help safeguard New Zealand Governmental systems, all incidents of attack by malicious software should be reported to:.

Centre for Critical Infrastructure Protection
PO Box 12-209
Wellington
New Zealand
Ph: (04) 498-7654
Fax: (04) 498-7655
E-mail: reports@ccip.govt.nz.

Assistance

705. The identification and resolution of COMPUSEC incidents is the responsibility of the department concerned. Where it is beyond the capability of individual departments to resolve the incident, the GCSB will provide advice and assistance within the limits of available resources.

706. The GCSB on request is able to provide advice and assistance to Government departments in development of computer security policy, application of computer security, evaluation of products and systems, and approved protection measures; however, the GCSB does not generally provide specialist advice on issues such as backup, disaster recovery, electronic vandalism and fraud unless classified information is involved.

707. For CCIP reports and alerts along with general security suggestions see the CCIP website.

708. Requests for advice or assistance in any area of computer security should be made in the first instance to the Director, GCSB.