Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197  Email: assist@dsd.gov.au

# HANDBOOK 12

# MALICIOUS SOFTWARE

# Version 1.0

## Objectives

1201. This handbook discusses the threat from malicious software along with the principal countermeasures employed. It is strongly related to **Handbook 10 - Web Security** and **Handbook 11 - Email Security.**

1202. Malicious software is defined as any software that attempts to subvert the confidentiality, integrity or availability of a system. The introduction of malicious software on to systems from the Internet and internal sources has become one of the most significant threats to information security.

## Overview and Terminology

1203. The boundary between the different types of malicious software, such as logic bombs, trapdoors, trojans, viruses, worms, and mobile malware, is becoming increasingly blurred. However, the following definitions are given:

1204. A **logic bomb** (also known as a backdoor) is code inserted into legitimate software which is designed to produce a result unintended by a legitimate user of the software.

1205. A **trapdoor** is a method of gaining access to some part of a system other than by the normal procedure (eg gaining access without having to supply a password). Hackers who successfully penetrate a system may insert trapdoors to allow them entry at a later date, even if the vulnerability that they originally exploited is closed. There have also been instances of system developers leaving debug trapdoors in software, which are then discovered and exploited by hackers.

1206. The strict definition of a **trojan** is a program which is overtly attractive to legitimate system users (eg a computer game or utility), but which has a hidden malign purpose (eg stealing passwords). However, the generic term 'trojan' is frequently used in place of the terms 'logic bomb' and 'trapdoor'.

1207. A Trojan program can be placed on a system in a number of ways, including email, web services, diskettes, file transfers and news. A particularly malicious type of Trojan involves remote control programs. Some trojans pass control information and data through protocols such as HTTP, thus tunnelling through firewalls.

1208. A **virus** is code inserted into legitimate software, where the virus code is written to reproduce itself by copying itself into other legitimate software. Viruses may contain logic bombs, some benign but mostly malign.

1209. A **worm** is a complete program that reproduces itself. Propagation is usually across a network (eg via email). There is an increasing trend to use the generic term 'virus' to cover both viruses and worms. In this section, the generic term 'virus' is used to cover both 'viruses' and 'worms'.

1210. There is a clear upward trend in the number and sophistication of attacks using viruses. Email viruses are prevalent, with the virus normally activating when the attachment is opened. One prevalent type of virus which relies on the lack of authentication in email is where the email purports to come from an acquaintance, and the virus does a lookup on the infected system for further email addresses.

1211. In some cases malicious code has been executed by a user viewing the email, as opposed to traditional infections that have occurred by users selecting the attachment or opening a document. These types of infections occur due to some interoperability and automated settings within some email products.

1212. Antivirus products continue to play a game of catch-up, with viruses sometimes able to spread widely before antivirus companies deliver detection strings and antidotes.

1213. **Mobile malware.** Web documents often have server-supplied code associated with them which executes inside the web browser. This active content allows information servers to customise the presentation of their information, but also provides a mechanism to attack systems running a client browser. Mobile malware may arrive at a site through active content such as JavaScript, Java Applets and ActiveX controls. Refer to **Handbook 10 – Web Security** for further details.

1214. The Internet is constantly being flooded with information about computer viruses and trojans. However, interspersed among real warnings are computer virus/trojan **hoaxes**. While these hoaxes do not infect systems, they are time consuming and costly to handle. Chain letters are an irritation rather than a major problem. They can be a way of distributing viruses and trojans.

1215. The impact of an infection of malicious code is as varied as any function that can be performed using a programming technique, eg. System flooding, system shutdown, deletion of data, data capture, data transfer etc. Malicious code can impact on one or all aspects of the security requirements ie. Confidentiality, availability and integrity.

### Malicious Software Countermeasures

1216. Each organisation should develop a malicious software strategy which clearly outlines the objectives and procedures for malicious software control and recovery. The risk of infection cannot be completely mitigated, and each site will need to develop a cost-effective solution appropriate for their environment.

1217. The primary countermeasures used for malicious software include:

a. **Security Awareness.** Discretion should be used in the source of software and data. For example, software should only be obtained from trusted companies, and data should only be accepted from trusted sources. This can be difficult to determine in the context of the Internet, but users can be warned not to open suspicious email from unexpected sources, and not to visit 'hostile' websites. Similarly, users should not be free to introduce unchecked media on to systems. User awareness is one of the most powerful countermeasures in virus control. User awareness of recovery/containment procedures is also important.

b. **Anti-virus scanners.** These products scan files and email for signature patterns that match known malicious software. Since new viruses are continually emerging, these products can only be effective if they are regularly updated with the latest virus signatures. It can be valuable to combine more than one anti-virus scanner at various points in the network to gain more assurance that malicious software will be recognised.

Anti-virus scanners can be positioned on gateways to the network and/or on network hosts. A multi-level strategy is suggested to capture viruses through the various entry points into a system. Anti-virus scanners are only as effective as the frequency of update. It is recommended frequency and method of update be considered when selecting anti-virus products.

Some anti-virus products also contain signatures for prevalent trojan programs.

c. **Integrity checkers.** These products create a database of file checksums for a set of system files. The integrity checker can tell if any of the files have been modified by comparison of the current checksum against the baseline checksum determined at installation time. These products are useful to detect the insertion of logic bombs and trapdoors, as well as for detecting virus infection.

d. **Audit information**. Audit logs, including firewall logs, may detect abnormal activity. Examples are trojans attempting to send data from a site, or malicious programs attempting to write or read to unauthorised areas.

e. **System hardening**. Careful implementation of system access controls, and the policy of running applications with least privilege, can minimise the damage caused by malicious software. This needs to be coupled with tight configuration management procedures.

f. **Active content blocking.** Active content can be blocked through the use of gateway content filters or through security settings on client browsers. However, this approach may meet user resistance due to the loss in functionality.

An alternative to total blocking is to use digital signatures to restrict active content to trusted sources. However, the assurance on digital signatures for active content is low, unless a model of trust like Gatekeeper is built in.

g. **Isolation.** High value internal systems can be isolated from 'at risk' networks that have a gateway to the Internet. However, this option may only be practicable for highly classified National Security networks. Even with this approach, malicious software may still reach the 'isolated' network through installation of programs from removable media or via 'limited function gateways'.

h. **Firewalls.** Firewalls can restrict the ability of some remote control programs to execute if they rely on a port that is generally blocked. However not a large degree of reliance can be placed on firewalls for malicious software control unless a gateway incorporates an active content filter.

### Recovery and Containment

1218. A recovery and containment procedure should be developed as part of an organisations malicious software strategy. The principle requirements of a recovery procedure are:

a. The ability to isolate infected systems

b. The ability to purge malicious software from a system.

c. The ability to restore the integrity of a system after an attack has occurred. If data has been corrupted, this will usually involve recovery from backup media.

d. The recovery procedure must be clearly documented and regularly tested.

1219. The recovery procedure also should outline the process for making users aware of their requirements to report and act in the event a virus contamination.

1220. External authorities to be involved in virus response should also be detailed in this strategy. It is important to report incidents of malicious software to ISIDRAS, so that DSD can accumulate knowledge of attack trends. Reports should include estimates of the damage caused, including loss of data and the resources required for recovery.

### Selecting Security Products

1221. The key requirements for anti-virus scanners are :

a. Regular updates of virus signatures.

b. Prompt updates for any new and rapidly spreading virus.

c. A purge facility for malicious software.

d. The ability to handle a wide range of file compression modes.

e. Reliable and ongoing support for the product.

1222. The key requirements for an integrity checker are:

a. A sound algorithm for the 'checksum' process.

b. The ability to protect the checksum database. This could be achieved by holding the database offline.

1223. The key requirements for an 'active content filter' are:

a. The ability to recognise the increasingly wide variety of active content.

b. An audit log describing the active content found and the action taken.

### Further Information

1224. A wide range of information on malicious software, including virus information, can be found on the **AUSCERT, CERT/CC** and **SANS** websites.

### Grades of Malicious Software Control

1225. The following grades have been included to assist in determining the level of effort that should be allocated mitigating the risk of malicious software. They are not definitive, and when developing a malicious software strategy should be used as a guide.

a. **Grade 1**

i. Develop a virus strategy for the organisation considering all possible points of entry for malicious software

ii. Deploy anti-virus programs on workstations, gateways and server.

iii. Contract with vendor for signature updates.

iv. User awareness program

b. **Grade 2**

i. Develop a virus strategy for the organisation considering all possible points of entry for malicious software

ii. Deploy more than one type of anti-virus programs on workstations, gateways and server.

iii. Contract with vendors for signature updates.

iv. Attachments scanned on all emails, web pages on file transfers

v. System integrity checking on all gateway and critical systems

vi. Boot from floppy disabled on all workstations

c. **Grade 3**

i. Develop a virus strategy for the organisation considering all possible points of entry for malicious software

ii. Deploy more than one type of anti-virus programs on workstations, gateways and server.

iii. Contract with vendors for signature updates.

iv. Attachments scanned in emails, web pages

v. Active content only allowed from trusted sites

vi. System integrity checking on all gateway and critical systems

vii. Restricted file transfer and diskette use

viii. Boot from floppy disabled on all workstations

d. **Grade 4**

i. Develop a virus strategy for the organisation considering all possible points of entry for malicious software

ii. Deploy more than one type of anti-virus programs on workstations, gateways and server.

iii. Contract with vendors for signature updates.

iv. Attachments removed from emails and web pages

v. System integrity checking on all gateway and critical systems

vi. Floppy disk drives disabled on user workstations. Boot from floppy diskette drive disabled on workstations.

vii. Active content blocked