U.S. Customs and Border Protection

Attachment V

Virus and Malicious Code Procedures

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27. 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27. 2009	Initial CBP 1400-05D release is based solely on existing 1400-05C, Version 2.1 appendices which were found to be unrelated to existing DHS 4300A, Version 6.1.1 attachments. The policy content of this attachment is exactly the same as the 1400-05C, Version 2.1 appendix. It is now presented in the attachment format.
2.0	December 21, 2010	No Changes

CONTENTS

1.0 MALICIOUS CODE

Any computer system that receives data from any external source (e.g., network connections, removable media) is susceptible to infection by malicious code. Malicious code is also referred to as "malicious software," or "malware." Malicious code may consist of (but is not limited to) a virus, network worm, Trojan horse program, or a network backdoor application. The purpose of the malicious code depends upon the type of code being employed, but is generally intended to disrupt computer operations. Malicious code may be used to collect or modify data (The destruction of data is the extreme form of modification.), provide unauthorized access to computer systems, etc.

Malicious code may consist of application code specifically created for malicious purposes or a legitimate application used in a manner other than what was originally intended.

Therefore, malicious code poses a significant risk to the confidentiality, integrity, and availability of CBP-owned information. As such, specific procedures must be followed in order to protect against and respond to security incidents involving malicious code. This appendix lists those procedures.

2.0 RECOGNIZING MALICIOUS CODE SYMPTOMS

If a computer system appears to be acting in an unusual manner, then the possibility exists that a malicious code has been introduced into the system or network. Listed below are a few of the indicators that could indicate a computer system has been infected by malicious code:

1. Any unexplained messages or graphics on the screen.
2. An increase in the time required loading or executing programs.
3. An increase in the time required to access or process data from a disk.
4. Unusual error messages.
5. Programs or files mysteriously disappearing.
6. Less memory available than usual.
7. Executable files changing size for no apparent reason.
8. Accesses made to non-referenced devices.
9. Data consistently out of balance.
10. File date and time stamps changing for no apparent reason.
11. Unexplained user accounts in use.
12. The presence of unexplained hidden files.
13. Unusual processes on the system or unusual network activity.

3.0 ANTI-VIRUS SOFTWARE

The ISSO or SA shall ensure that all information storage media such as diskettes, optical disks, and computer hard drives introduced into or removed from CBP facilities are scanned with a CBP-approved, updated anti-virus program. If the media cannot be scanned, it is considered high-risk and must be approved by the CISO before being used.

The CBP-approved anti-virus signature files shall be updated in a timely and expeditious manner. This policy pertains to all systems on which the CBP-approved anti-virus solution is installed (e.g., servers, workstations, desktops).

3.1 Email Scanning

All email attachments, both incoming and outgoing, shall be scanned with an updated, CBP-approved anti-virus product at both the server (e.g., email server, Mail Transfer Agent [MTA]) and client (e.g., workstations, desktops, laptops) level. The anti-virus solution installed on the email server or MTA shall, at a minimum, meet the following criteria:

1. Anti-virus signature files shall be updated on a regular basis.
2. Anti-virus solutions shall be configured to scan all incoming and outgoing attachments.
3. Anti-virus solutions shall be configured to run periodic (weekly) full system scans. These scans may be scheduled for a time that will cause minimum disruption to workflow.

3.2 Scanning Windows and DOS-Based Systems and Media

The current CBP-approved version of scanning, detection, and removal software will be used to scan all Windows and DOS-based systems (desktop, network, and media) including media created under any DOS partition of a UNIX-based system.

3.3 Scanning of Windows-based Workstations

All Microsoft Windows-based workstations, either connected to the CBP network or operated in a standalone configuration shall employ anti-virus protection. The anti-virus solution shall, at a minimum, meet the following criteria:

1. The anti-virus solution shall run as a centrally managed background service and permit users on-demand scanning of files and media.
2. Definitions shall be updated on a regular basis (definition updates shall be tested prior to deployment to individual workstations).
3. Anti-virus solutions shall be configured to employ real-time file protection.
4. Anti-virus solutions shall be configured to run periodic (at a minimum, weekly) full system scans. These scans may be scheduled for a time that will cause minimum disruption to workflow.

5. Anti-virus solutions shall be configured such as to prevent a user from disabling any function.

4.0 MALICIOUS CODE COUNTERMEASURES

The best protection against the loss of a system or data due to malicious code infection is to establish good security practices. Malicious code scans should normally be performed on data coming into CBP from external sources. However, ISSOs can approve alternatives to such scanning when compensating controls minimize the risk of negative impacts.

4.1 Backing Up Software

Whenever software must be backed up, the preferred method is to use a network drive or an authorized network service. The original media used to distribute software should be labeled and maintained in a secure location.

In the case where the original distribution media consists of 3½ inch floppy diskettes, System Administrators (SAs) must backup the software prior to using it, retaining the original distribution diskettes in a safe and secure location. Write-protect both the originals and the backup copies. Use the backup copies to load the software onto CBP computer systems. If a virus destroys the backup copy, the original can be used to make new backup copies. Use only newly formatted diskettes for making backup copies. Used diskettes may be used if they are first scanned for viruses and then reformatted. Note: This is not considered a violation of the copyright laws. Authorized OIT personnel normally conduct software backup.

4.2 Exchange of Data via Removable Media

The delivery of malicious code from CBP to another organization could affect CBP credibility. Likewise, CBP does not want to be infected by data received from others. Care must be exercised in the exchange of data via removable media. Removable media can include (but is not limited to) diskettes (i.e., also referred to as “floppies”), Jazz or Zip drives, CDs, DVDs, USB-connected thumb drives. The following policies apply:

1. Where applicable, use only new media when creating data for exchange.

2. Virus scan all media before release from CBP premises.

3. Virus scan all media received from outside organizations. Where applicable, use a standalone, isolated, non-networked system before allowing the media to be placed into the drive of any CBP system. If such a system is not available, a SA should be contacted to conduct the scan.

5.0 SYSTEM CONFIGURATION

All CBP computer systems shall use the OIT LAN standard configurations in accordance with the *Principle of Least Privilege*. In essence, this means that only the necessary services and functionality will be provided by the CBP-owned computer systems. This includes (but is not limited to) providing the user with only the necessary level of access to write to the system. In the event that a malicious code infection occurs within the user’s security context, limiting write access to the system can hamper or even prevent the malicious code infection.

6.0 REPORTING INCIDENTS OF MALICIOUS CODE

If malicious code is suspected or detected on any CBP-owned information system, immediately notify your system or LAN administrator, your manager and the CSIRC for assistance and to report the suspected malicious code. Contact information for incident reporting is provided in Section 4.9.6.1.

7.0 IMMEDIATE ACTIONS

As with other types of security incidents, the nature and scope of malicious code infections must be determined when they are discovered. The system or LAN administrator and the CSIRC to which the incident is reported should include the results of an anti-virus scan as part of the Incident Report. If a scan of the system with the anti-virus solution identifies the malicious code, this will allow the LAN administrator, ISSO, and CSIRC to determine the potential infection vector (i.e., how the malicious code got on the system in the first place), as well as the potential scope of the incident (e.g., is it possible that any other systems have been infected?).

If the anti-virus scan does not identify the malicious code and the reported behavior persists or if any additional unusual behavior occurs on the system, contact the CSIRC immediately. It is possible that supposedly "unusual" system behavior thought to be the result of a malicious code infection may really be normal system behavior. However, unusual system behavior that persists or escalates may indicate previously unknown or undocumented malicious code and should be thoroughly investigated.