Carnegie Mellon

Procedure for Responding to a Compromised Computer

Document Information	
Identifier	
Status	Published
Published	04/11/2006
Last Updated	05/18/2011
Version	2.1

Carnegie Mellon

Revision History

Version	Published	Author	Description
1.0	04/11/2006	Stephanie Caviccchi John Lerchey	Original publication
1.1	05/11/2006	Stephanie Caviccchi John Lerchey	Minor edits for clarify.
1.2	09/04/2007	Doug Markiewicz	Relabeled document as a procedure instead of a guideline.
2.0	04/18/2008	Doug Markiewicz	Reformatted to fit new procedure template and largely rewritten to provide greater clarity. Contact information has also been updated. No significant changes to the actual process have been made.
2.1	05/18/2011	Doug Markiewicz	Updated Definitions, Additional Information and contact information in step 2 of the procedure.

Carnegie Mellon

Purpose

The purpose of this Procedure is to provide step-by-step instructions for responding to an actual or suspected compromise of Carnegie Mellon's computing resources.

Applies To

This Procedure applies to anyone using Carnegie Mellon's computing resources that suspects that the security or privacy of these resources has been compromised. This Procedure also applies to situations where there has been no compromise but someone suspects their computing resources are actively being attacked. This Procedure does not apply to computing resources owned by students.

Definitions

A Compromised Computer is defined as any computing resource whose confidentiality, integrity or availability has been adversely impacted, either intentionally or unintentionally, by an untrusted source. A compromise can occur either through manual interaction by the untrusted source or through automation. Gaining unauthorized access to a computer by impersonating a legitimate user or by conducting a brute-force attack would constitute a compromise. Exploiting a loophole in a computer's configuration would also constitute a compromise. Depending on the circumstances, a computer infected with a virus, worm, trojan or other malicious software may be considered a compromise. If the malicious software is detected and removed by antivirus software in a timely manner, it is probably not necessary to follow this process. Some level of judgment will need to be used in these situations. Symptoms of a *Compromised Computer* include, but are not limited to, the following:

- The computer is experiencing unexpected and unexplainable disk activity
- The computer is experiencing unexpected and unexplainable performance degradation
- The computer's logs (e.g. system logs, application logs, etc.) contain suspicious entries that indicate repeated login failures or connections to unfamiliar services
- A complaint is received from a third-party regarding suspicious activity originating from the computer

Non-public Information is defined as any information that is classified as Private or Restricted information according to the Guidelines for Data Classification.

Personally Identifiable Information is a subset of Non-public Information defined by various state and federal regulations. Examples of *Personally Identifiable Information* include, but at not limited to, social security numbers, driver's license numbers, health information and certain types of financial account information.

Regulatory Requirements

Carnegie Mellon is required by various state and federal regulations to investigate any incident that may involve the breach of personally identifiable information. Carnegie Mellon is also required to notify an individual if the privacy of their personally identifiable information has been breached. Failure to preserve evidence or conduct an investigation related to a compromised computer could result in unnecessary financial costs for the instiution. It is also important that the details of a compromise and the ensuing investigation remain confidential. All communications related to a compromise should be coordinated with the Information Security Office and the Office of General Counsel. Any contact with law enforcement should be immediately referred to or authorized by the Office of General Counsel.

Carnegie Mellon

Procedures

The following steps should be taken to response to an actual or suspected compromised computer:

1. **Disconnect the computer from the network**

   Disconnecting the computer from the network prevents a potentially untrusted source from taking further actions on the compromised computer. This also prevents any further leakage of non-public information if that is a potential concern. Shutting down the computer would also have this effect but could destroy evidence that is essential to investigating the compromise. Similarly, rebuilding the computer would destroy all evidence pertinent to an investigation.

2. **Contact the Information Security Office**

   Prior to taking any additional action on the compromised computer, the Information Security Office should be contacted. Continuing to use the compromised computer or attempting to investigate the compromise on your own could result in destruction of evidence pertinent to an investigation. During standard working hours, the Information Security Office can be contacted by phone at **412-268-2044** or by email at iso-ir@andrew.cmu.edu. In the event that the Information Security Office is unavailable to take your call, emergency contact information is provided in the voice message.

3. **Notify users of the computer, if any, of a temporary service interruption**

   If the compromised computer provides some type of service, it is likely that users of this service will be impacted by the interruption brought on by disconnecting the computer from the network. These users should be notified in some manner of the interruption. Options for notification may include an email to the user base or posting a notice to a frequently visited web site. As stated previously, the details of a compromise and the ensuing investigation should be kept confidential. Therefore, the notification of service interruption should not indicate that there has been a compromise.

4. **Preserve any log information not resident on the compromised computer**

   All log files, pertaining to a compromised computer, that are stored on a secondary computer or on some type of external media should be preserved immediately. Preservation may include making a copy of the log files and burning them to a CD. If there is no immediate risk of the logs being deleted or overwritten, this step can occur following Step 5. Log files stored locally on the compromised computer will be collected as part of a forensic investigation coordinated by the Information Security Office. This will help ensure that no evidence is destroyed or altered during the collection process.

5. **Wait for further instructions from the Information Security Office**

   The Information Security Office will conduct some preliminary investigation prior to determining the best course of action for the Compromised Computer. While waiting further instructions, do not share any details related to the compromise unless absolutely necessary. Additionally, do not attempt to contact law enforcement officials. Such communication must be coordinated with the Information Security Office and the Office of General Counsel due to the potential legal implications of a compromised computer.

Carnegie Mellon

Additional Information

If you have any questions or comments related to this Procedure, please send email to Carnegie Mellon's Information Security Office at iso@andrew.cmu.edu.

Additional information can also be found using the following resources:

- Information Security Policy
  http://www.cmu.edu/iso/governance/policies/information-security.html

- Information Security Roles and Responsibilities
  http://www.cmu.edu/iso/governance/roles/

- Guidelines for Data Classification
  http://www.cmu.edu/iso/governance/guidelines/data-classification.html

- Guidelines for Data Protection
  http://www.cmu.edu/iso/governance/guidelines/data-protection/