

Document type: Reference

Maintaining information sources for a WARP Filtered Warnings Service

(V1.0) June 2004

Keywords

[Information sources, Filtered
Warnings]

Version control

This document may be made available in more than one electronic version or in print. In a case of existing or perceived difference in contents between such versions, the reference version is the version available for download from the WARP Toolbox site <http://www.warp.gov.uk>

If you find errors in the current document, please send your comment to editor@warp.gov.uk

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

Copyright notification

The copyright and the foregoing restrictions, extend to reproduction in all media. The rights to modify and reproduce are described in the WARP Toolbox terms and conditions described on the WARP Toolbox site.

© Crown Copyright 2004

Contents

- 1 Scope 2
- 2 References **Error! Bookmark not defined.**
- 3 Definitions and abbreviations 2
 - 3.1 Definitions 2
 - 3.2 Abbreviations..... 2
- 4 Trusting Sources 2
 - 4.1 Levels of Trust..... 2
 - 4.2 Acting on Trust 3
- 5 Housekeeping 3
- History 4

1 Scope

Information sources used to feed a WARP Filtered Warnings Service will be numerous and diverse. It is therefore important to keep the quality of information high, by assessing each source to determine the level of trust that should be applied to it, and by performing periodic housekeeping, to weed out irrelevant feeds. This document discusses these important aspects of operating a WARP Filtered Warnings Service.

2 Definitions and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply:

CERT: Computer security incident response team, based on the model developed by the Carnegie Mellon University.

2.2 Abbreviations

For the purposes of this document, the following abbreviations apply:

UNIRAS: Unified Incident Reporting and Alert Scheme

WARP: Warning, Advice and Reporting Point

3 Trusting sources

When deciding to use an information source to feed the WARP community, it is important to take some time to assess how trustworthy that source is. One of the main benefits of the WARP Filtered Warnings service is that any information passed on to the community will be of high quality, as well as being filtered to be relevant to the receiver.

3.1 Levels of trust

The WARP administrator should look at each information source that will be used, and place it into one of the following trust categories:

Trust Level	Examples of Source
High	UNIRAS or other CERT organisation Vendor advisories regarding their own products Alerts from Anti-Virus vendors that are corroborated by other Anti-Virus vendors
Medium	Media reports (traditional and on-line) from known media organisations (not web-sites that will publish anything).
Low	Public mailing lists Newsgroups

Care must be taken to understand what level of trust should be applied to a new source. For example, a moderated mailing list may seem reliable, but the moderator's job is usually to keep discussions on topic and keep out spam – they are not in anyway bound to ensure the content is accurate.

3.2 Acting on trust

Establishing the trust level of a source up front makes decisions about whether or not to pass an alert on to the community easier to make. A policy can be created based on the trust level of sources like the one shown below.

Trust Level	Action
High	Advisories from these sources can be passed on to the WARP members without further checks.
Medium	Look for corroboration from highly trusted sources. Once corroborated, information from these sources may help in the creation of well-informed alerts.
Low	Advisories should not be sent to WARP members based on information from these sources alone. Look for corroboration from trusted sources. The WARP administrators may use sources of low trustworthiness to give a “feeling” for what to expect next.

4 Housekeeping

Once a list of sources has been constructed, and is being monitored, it is important to schedule a regular task to assess the quality of information being supplied by each source.

Some sources will remain constant in quality, but others may not. Additionally, from time to time sources will cease to operate, or be taken over by other organisations and change format. Try to assess all sources against the following criteria on a monthly basis:

1. Activity – Is the source actively supplying information?
2. Trust – Should the level of trust currently assigned to the source be changed?
3. Relevance – Is the information supplied of interest to your WARP community? If the Filtered Warnings Application is being used, you can easily establish whether or not tick-list categories have subscriptions from WARP members.

It is also important to seek out new information sources, particularly in areas of unique interest to your WARP community.

History

Version	Date	Description
V1.0	June 2004	First issue.