COMBINED HARDWARE / SOFTWARE SOLUTIONS TO MALWARE AND SPAM CONTROL

Stephen Posniak
Office of Information Technology
US Equal Employment
Opportunity Commission

THE GROWTH OF ‘APPLIANCE’ – BASED SOLUTIONS

- spam and spyware (along with other types of malware) have increased as a threat to the network infrastructures of organizations.
- The need for a more rapid automated response without a drastic increase in staff resources

EMERGENCE OF NEW ‘APPLIANCE–WARE’

- *Barracuda*
- *IronPort C-Series*
- *NetAppliance’s NetCache*
- *Tumbleweed’s Mailgate Edge*

OBJECTIVE OF THIS PAPER:

Study the decision making and
subsequent experiences of the
group of 21 government agencies
(including my own) which selected *IronPort*

The US Federal Networking Environment: Some Background

EEOC SCREEN WARNING REQUIREMENT ON EXTERNALLY CONNECTED SYSTEMS:

EEOC's Computer Systems Important Notice

This is an Equal Employment Opportunity Commission Computer System. This system is intended to support official government business. Any information on this system is subject to recording, copying, reading, or interception by authorized personnel, including the Office of Inspector General. Use of this system constitutes consent to any such action and acknowledgment that there is no reasonable expectation of privacy with respect to any information or communications on this system.

Unauthorized users may be subject to civil and criminal penalties or administrative action for computer fraud or abuse.

Responsibilities Under the Confidentiality Provisions of Laws Enforced by EEOC

The confidentiality provisions of Title VII of the Civil Rights Act of 1964 and Title I of the Americans with Disabilities Act prohibit the Commission, its officers and employees from disclosing to the public, prior to the institution of a lawsuit, information involving: (a) any charges filed under those Acts, (b) anything said or done during informal efforts to resolve such charges, (c) any reports that employers are required to file with the Commission under those Acts, and (d) any information obtained by the Commission during the investigation of such charges. Violators can be fined not more than $1,000, **imprisoned for not more than one year**, or disciplined. (Emphasis added.)

Privacy Act Responsibilities

The Privacy Act of 1974 prohibits any disclosure by an agency officer or employee of information from any system of records about individual persons, unless the disclosure is consented to by the individual to whom the record pertains, is covered by an exception, or would be for a routine use, as defined by the Act. Violation is a criminal misdemeanor subject to a fine of not more than $5,000. The same penalty also applies to any agency officer or employee who maintains a system of records (manual or automated) about individual persons without complying with the Privacy Act notice requirements.

IRONPORT C-SERIES CONCEPT AND FEATURES

- Dedicated Dell Server, installed just inside the Firewall
- Operating System – Independent
- Real-time Detection, using
  - Reputation Filters
  - Advanced Content Filtering
  - Virus Outbreak Filters
  - (All of the above are built into the appliance.)

SOFTWARE COMPONENTS

- *Symantec Brightmail* anti-spam scanning
- *Sophos Anti-Virus* anti-malware scanning
- Engineered and sold as a one-product solution in which the hardware comes pre-configured ‘out of the box.’
- Patches pretested by *IronPort* and delivered via a TAR file directly to the appliance,which then only requires a simple reboot.

SURVEY STRUCTURE AND OBJECTIVES

- Sent to all points-of-contact at the Federal agencies known to have deployed and used the *IronPort* email security appliance.

- Explained background and objectives: [to summarize (on a not-for-attribution basis unless specifically authorized by a particular respondent), agency responses to specific questions]

SURVEY QUESTIONS AND RESPONSES

Q1. *What other spam / malware control appliance products besides IronPort did you review prior to making your decision?*

SURVEY QUESTIONS AND RESPONSES

Q2. *What information or findings led to your decision to acquire and deploy IronPort?*

SURVEY QUESTIONS AND RESPONSES

Q3. *What specific criteria were most applicable to your final decision to deploy IronPort?*

SURVEY QUESTIONS AND RESPONSES

Q4. *In your estimate, by what percentage has the total incidence of tagged or intercepted email spam changed since you fully deployed IronPort?*

SURVEY QUESTIONS AND RESPONSES

Q5. *What (if any) have been the most serious problems or issues which you have encountered since the full deployment of IronPort?*

MOST SERIOUS PROBLEMS OR ISSUES

Retrieval of messages in cases where spam is quarantined and the user then decides that an item was something legitimate which she/he needed?

MOST SERIOUS PROBLEMS OR ISSUES

Slow response of the software management interface browser?

MOST SERIOUS PROBLEMS OR ISSUES

Some innocuous messages get tagged as possibly containing malware?

MOST SERIOUS PROBLEMS OR ISSUES

Some obvious spam messages were passed without comment?

MOST SERIOUS PROBLEMS OR ISSUES

Other?

CONCLUSIONS

- Not yet a panacea for solving
  all malware problems.

- The spyware problem is not explicitly addressed by tools such as *IronPort*.

- Spyware could be addressed to the extent that e-mail is an involved vector.

QUESTIONS?