COMBINED HARDWARE/ SOFTWARE SOLUTIONS TO MALWARE AND SPAM CONTROL

Stephen Posniak
Office of Information Technology, US Equal Employment Opportunity Commission, Washington, D.C. 20507, USA

Tel +1 202 663 4449 • Email stephen.posniak@eeoc.gov

ABSTRACT

As spam and spyware (along with other types of malware) have increased as a threat to the network infrastructures of organizations, vendors have increasingly begun to offer 'appliance'-based solutions involving combined, dedicated hardware and software. These include products such as *IronPort*, *Tumbleweed*'s *Mailgate Edge*, *Barracuda* and *NetAppliance NetCache*, to list some of those most frequently referenced. This paper summarizes the experiences of 21 US Federal agencies in deployment of one such combined solution: *IronPort* [1]. While relating all pertinent input provided by the organizations, the paper also focuses on the impact of these organizational experiences on the mostly theoretical concerns and issues raised previously about the purported benefits of the hardware approach over software-oriented scanners [2–4].

ORGANIZATIONAL BACKGROUND INFORMATION

While the US Federal Government's executive branch is comprised, in addition to the major cabinet departments, of hundreds of large and small agencies – many independent of the major departments – there are a number of avenues for technical communication among Federal IT professionals and managers. These include (in addition to technical publications and the expected informal channels), organizations such as the NIST Computer Security Program Managers' Forum, the CIO Council, and the Small Agency Council. Federal agencies, while performing a wide variety of missions, all have as a common factor their reliance on email as one of their essential tools for getting their jobs done. Along with the requirement to control malware and spam and their impacts on email systems and networks, most agencies also have the need to accomplish this with minimal technical and staff resources.

There are undoubtedly other groups of organizations (both public and private sector) which choose other solutions for dealing with what is an undeniably a widespread problem and challenge. I decided that it would be useful and interesting to study the decision making and subsequent experiences of the group of 21 government agencies (including my own) which selected *IronPort*.

IRONPORT CONCEPT AND FEATURES

The *IronPort C* series consists of a dedicated *Dell* server which works at the network level, and is installed just inside the firewall. It is operating system-independent. Its architecture includes Advanced VCF with real-time detection, using both reputation filters and content scanning (advanced content filtering), which are built into the appliance. It also includes virus outbreak filters, which are designed to recognize and block any sudden influx of new, virus-laden email messages [5]. Its software components include *Symantec Brightmail* anti-spam scanning and *Sophos Anti-Virus* anti-virus scanning. However, it is engineered and sold as a one-product solution in which the hardware comes pre-configured 'out of the box' ready for deployment, thus requiring less time for setup and configuration. It is also engineered to make maintenance and disaster recovery more efficient. Patches are pretested by *IronPort* and delivered via a TAR file directly to the appliance, which then only requires a simple reboot. Only one configuration file needs to be added to replacement hardware during disaster recovery for it to be up and operational.

IronPort provides a comprehensive, in-depth centralized management console which coordinates the activities and reporting from all installed components (Mail Flow Central/ Mail Flow Monitor). From the console, administrative staff can easily and quickly access a real-time system status of any possible outbreaks, drill down to the email culprit, and quarantine the email for evaluation. Later, if the email is found to be malware-free or legitimate (not spam), the administrator can release it. From the management console, the administrator can also set specific content-scanning parameters based on specific user groups, and create detailed reports from the post office down to the specific mailbox [6, 7].

SURVEY STRUCTURE AND OBJECTIVES

A survey was emailed to all my points of contact at the Federal agencies known to have deployed and used the *IronPort* email security appliance. It was explained that, because there are still relatively few public and private sector organizations who have deployed this type of appliance solution, I had proposed the attached abstract of this paper, which the *VB* conference committee had accepted and requested that I prepare. The message went on to explain that, because most of the prior information which I had collected from the Federal community pertains to *IronPort*, that was the appliance/tool on which I had chosen to focus. The message also emphasized, as stated in this paper's abstract, that the paper would summarize (on a not-for-attribution basis unless specifically authorized by a particular respondent), agency responses to specific questions.

SURVEY QUESTIONS AND RESPONSES

The specific questions posed and a summary of the responses received follows, after which more detailed comments are quoted.

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

- *Barracuda*
- *BorderWare MX-Extreme*
- *Gwava*
- *Tumbleweed Mailgate Edge*
- 'We did look at software products, such as *SpamAssassin*, but we were concerned about false positives.'

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

- Review of vendor documentation.
- Review of articles in technical journals.
- Discussions with existing *IronPort* users.
- Cost/benefit considerations.
- 'Ability to incorporate *Sophos Anti-Virus* and *Brightmail*.'

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

- The need for an additional tool to control spam.
- The need for an additional tool to control malware.
- 'We wanted a system with zero false positives, and as close as possible to zero resource requirements in terms of system administrators and help desk involvement.'
- 'For spam, we had a home-grown anti-spam solution, plus we used black-hole lists, but the former used a lot of system administration time, and the latter were not particularly effective. For anti-virus, we had AV software on *Exchange*, but about 5% of our users did not use *Exchange*, and didn't always have or update their desktop AV software. So *IronPort* covered that small hole. Still, anti-spam was the primary reason for the decision to deploy *IronPort*, not anti-virus, although we do like that feature.'
- 'The need to upgrade from *Gwava*, an email protection product that works with *GroupWise* email but that shares server resources with the *GroupWise Internet Gateway* (GWIA).'
- 'The need to incorporate a subscription-based service to help control spam (*Brightmail*). We were relying solely on *Spamhaus* at the email gateway to identify spam.'
- 'The desire to use an anti-virus vendor other than our existing enterprise vendor.'

Q4. *In your estimate, by what percentage has the total incidence of tagged or intercepted email spam changed since you fully deployed IronPort? (Alternatively, if you have such data, on the average, what percentage of your email traffic was tagged or intercepted as spam prior to deployment of IronPort, and what percentage (on average) has been tagged or intercepted as spam since IronPort deployment?)*

Most of the respondents had not kept specific statistics about this. Those who did stated that between 25% and 33% of their total email received is now being tagged and/or blocked by *IronPort*. They stated that prior to its deployment, using white lists or other software-based tools, between 6% and 10% of the total email received had been tagged and/or blocked. Most added that *IronPort* had not tagged or blocked any false positives. One additional comment: 'Due to our email architecture, and the difficulty of identifying false negatives, we don't have hard numbers. But, from my own experience, and anecdotally, I would say spam incidence has declined by at least 90%. Complaints from users have declined more than that.' Another respondent, whose agency is under a court order not to filter any email stated that their worst problem was that 'some users complain that they are not receiving email tagged as spam by *IronPort*.' (This respondent did not provide any specific numerical data.)

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

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

Only one agency reported this to be a problem.

- Slow response of the software management interface browser.

Three agencies reported this to be a problem. The two detailed response were: (1) 'Worst problem: the GUI interface for the Quarantine is cumbersome.' and (2) 'Worst thing: the Web Console GUI is not as good as it could be.'

- Some innocuous messages get tagged as possibly containing malware.

Two agencies reported this to be a problem. (The first report is included and quoted above as part of the last response to Q4.) The second (and more detailed) response was: 'The most serious problem we had was that the *IronPort* dropped some legitimate email. What happened was that *Sophos* mistakenly identified some email as "Unscannable". Unfortunately, *IronPort* was initially configured to drop "unscannable" email. These two problems together resulted in 20 or 30 legitimate emails being lost over a few days.'

- Some obvious spam messages were passed without comment.

One agency made the following report with reference to this issue: 'This has been somewhat of a problem from the point of view of our users. In particular, the *IronPort*'s *Brightmail* seem to be particularly ineffective against "Nigerian scam" email. I suppose that's not surprising since these criminals have a great financial incentive to make sure their emails get through, but it is annoying to our users, who complain that "anybody can see that it's spam" ... I also was not impressed with the performance of *IronPort* against last week's [mid-May, 2005] Sober.P email containing political statements in German. Even though the subject lines of these messages were identified and distributed in the media, there were a few that *Brightmail* never identified as spam, and they were a bit slow in catching on. As of 5/17, I think we got 200,000 of these messages, and *Brightmail* let 36,000 (19%) through.'

- Other.

The following detailed statement is from a single agency: 'We've also had problems with disk drives failing. Fortunately, we have two *IronPorts*, so we didn't experience any outages, but we've had one machine down for many hours as *IronPort* support tested the RAID array. The most trouble we had (although it didn't cause any disruption or lost email) was getting the Quarantine server to run reliably. *IronPort* support finally isolated the problem to the way we were doing backups, and it's been reliable since ... A minor problem we had was that while both the *IronPorts* and our mail relays were properly configured not to relay email, it was possible for a spammer to do something called "multi-hop relay", which resulted in some of our users' email being rejected by other sites ... Overall, though, I don't want to give the impression we've had a lot of problems. The *IronPorts* are still a great success story, and for the most part, they just run and do their job. The system software is very sophisticated, and upgrades have been very easy and uneventful.'

CONCLUSION

The concept of a single hardware platform on which several different kinds of proactive software can be deployed in a way that simplifies both the updating process and the capability of managing and controlling email issues is obviously attractive. A review of the VB2004 Conference Proceedings makes it clear that this was already becoming evident. As Chris Lewis and John Morris [8] stated, ‘In order to maximize performance of the email servers, an early design decision was to place the [software] on dedicated hardware sitting in front of the pre-existing email infrastructure.’

I have examined the reported experiences of one relatively small group of ‘corporate’ (aka ‘government’) users in deploying and working with just one such tool. Clearly, this and similar tools have not yet become a panacea for solving all malware problems (e.g., most of the respondents still deploy a separate anti-virus tool on the users’ desktops.)

The spyware problem to which I alluded at the start of the paper is not explicitly addressed by tools such as *IronPort*, which is designed to control Port 80 SMTP email traffic – not HTTP browser activity. However, one could readily envision tracking and filtering spam email with texts known to contain URL references which definitely steer unsuspecting users to spyware-infected websites. One could also envision an appliance solution which combines on a single platform not only *Symantec Brightmail* and *Sophos Anti-Virus*, but also an explicitly anti-spyware-oriented product such as *Webroot Spy Sweeper Enterprise* [9].

The argument will, of course, be made that whatever problem or group of problems a product is designed to address, there will always be new, additional threats which the product is not designed to counter. Within reasonable limits, it is not out of line to expect appliance product designers to make some pragmatic enhancements to incorporate responses to related problems and issues.

As John Curnyn stated in his VB2004 paper [10], ‘A growing trend in the AV and AS worlds is the use of specialist hardware that can accelerate certain functions that up until now have been performed in software ... There is no single solution or architecture that must be chosen, as each service may have different functionality, price and performance goals. However, it is clear that the key attribute in any architecture is the selection of hardware and software design elements, and the way in which they are married together to offer the goals of performance, flexibility and extensibility.’

It is only through the use of such a pragmatic combination of approaches and tools, not only concerning email but also concerning the exploitation of web browsers and network shares, that organizations can hope to control the varying types of malware and spam which periodically evolve and repeatedly confront them in our day and age.

ENDNOTES AND REFERENCES

[1] The information reported in this paper was obtained on a not-for-attribution basis with the understanding that the names of specific organizations and individuals would not be published.

[2] Wagner, Matthew; ‘Hardware anti-virus solutions?’, *Virus Bulletin*, January 2004, p.12.

[3] Fitzpatrick, Tony; ‘New system halts malware’, *E4 Engineering.com*, November, 2003.

[4] Goodwing, Ruppert; ‘Alternative medicine: future virus fighting’, *Ednet.com*, November, 2003.

[5] Chernicoff, David; ‘IronPort C-30’, *Windows ITPro*, 27 January 2005.

[6] IronPort C series overview, http://www.ironport.com/products/ironport_c-series.html.

[7] ‘Group test: anti-spam and content filtering’, *SC Magazine*, April, 2005, p.52 http://www.scmagazine.com/.

[8] Lewis, Chris and Morris, John; ‘Corporate spam fighting: 5 years of success and lessons learned’, *Proc. Int. Virus Bull. Conf.*, 2004.

[9] See review by Jon Tullet in *SC Magazine*, http://www.scmagazine.com/products/index.cfm?fuseaction=productDetails&productID=18554&type=review.

[10] Curnyn, John; ‘How to achieve 10 GBit/s performance for integrated anti-virus and anti-spam network-based security systems’*, Proc. Int. Virus Bull. Conf.*, 2004.