

In The Boxing Ring



IN THIS ISSUE

2.

2008 ROUND-UP

During 2008, Network Box delivered a large number of enhancements, functionality and major developments to our customers - we present a round-up of this here.

3.

2009 PREVIEW

Network Box has several developments planned for 2009. On page 3 we give a high-level preview of what is coming.

3.

CVE-2008-4844

A major vulnerability in Microsoft Internet Explorer was subject to a zero-day exploit during December 2008 - we discuss its implications and what can be done to protect our customers against this sort of attack.

4.

JAN 2009 FEATURES

The ongoing deployment of our recently released features.

4.

PATCH TUESDAY

Network Box has moved to a patch Tuesday form of software enhancement release mechanism.

Network Box Technical News from Mark Webb-Johnson, CTO Network Box

Welcome

Welcome to the January 2009 edition of 'In The Boxing Ring'. I plan to use this edition to present a summary of what we did in 2008 and what we have planned for 2009. I will also be devoting some space, on page 3, to discuss the recent CVE-2008-4844 (MS08-078) vulnerability that affected several versions of Microsoft Internet Explorer during December.

Turn to page 2 of this newsletter for a round-up summary of enhancements, functionality and major developments delivered during 2008. Over the year, we delivered on more than 300 enhancement requests and software/hardware fixes; and along the way achieved our targets on several key technological milestones. The enhanced functionality delivered will serve as a base for our Network Box service delivery platform for 2009 and beyond. For NBR3-3.0 customers, all this enhanced functionality was delivered free-of-charge as part of our service to you.

On page 3, I'd like to give you a preview of where we are heading with our technology and what enhanced functionality you can expect to receive. As space is limited, this can only be a summary and highlight of our product direction, with more detail to follow over the coming months. For NBR3-3.0 customers, this functionality will be delivered to you free-of-charge.

2008 has been a challenging year. We have seen an ongoing increase in spam, malware and other threats. New threat vectors have kept us busy, and we expect 2009 to deliver more of the same.

As usual, if you have any feedback, or comments, it is always appreciated. You can contact us here at HQ via email (nbhq@network-box.com). Or, drop by our office next time you are in town.

Mark Webb-Johnson
CTO, Network Box Corporation
January 2009





2008 Round-Up

NETWORK BOX

We started the year with a migration of our Network Box Network Operation Centres to the NBR3.0 platform. This allowed for faster PUSH updates and provided better tools for our NOC engineers to support our customers. During Q1, we also completed testing and deployment of a set of changes to our mail scanning system to support a new (faster) anti-spam signature system, automatic Bayesian training and started to issue anti-spam signatures for telephone numbers and email addresses used by spammers.

During Q2, we announced our E-x series of models (E-1000x, E-2000x and E-4000x). These replaced the Opteron-based E-series models with Intel Xeon multi-core technology (offering 2, 4 and 8 cores respectively). The new models also offered increased RAM and DISK capacity, as well as migration to PCI express architecture and expansion capacity to 12 Gigabit ethernet ports.

Q2 also saw enhancements made to the my.network-box.com administrative interface to support a 'Trace' function in the Web Proxy, Firewall, IDP and Mail modules (including real-time 'live watch' traces). We also released enhancements to our mail scanning system for support of Office 2007 documents and Microsoft Smart Tags (related to policy blocks on nested '.bin' attachments and object tags in html emails).

Late June saw the rise of a particularly malicious and widespread form of SQL Injection attack targeting web servers with backend SQL databases. Network Box Security Response released a new IDP module (called HTTP-SQLINJWORM). While no gateway device can 100% protect against such application-level attacks, we were pleased to see our new module effectively stop this worm in its tracks for our customers (and our global footprint allowed us to release this several days before it became a global problem).

July saw Network Box move to a patch Tuesday form of release cycle (with the first such patch Tuesday being 1st July 2008) and the launch of the "In The Boxing Ring" newsletter. That newsletter also announced the launch of several new functional enhancements to the NBR3.0 platform, including the NBCS content filtering engine, enhanced categorization of anonymous proxies, the uncategorized URL feedback loop and support for the newly launched E-1000x, E-2000x and E-4000x models.

August saw the release of the NBLDAP system for integrating active directory groups into Network Box content filtering policies. To speed-up access to the Box Office support system, regional mirrors (in America, Europe and Asia) were launched to provide local access points. The new mirrors support English, Traditional Chinese, Simplified Chinese and Korean languages (with more to follow).

In September, we released support for Google Safe Browsing and Google/Yahoo Safe Searching. We also released multi-language support for Traditional Chinese, Simplified Chinese and Korean (in addition to the standard English, and with more languages to follow) in the Mail Portal, my.network-box.com and weekly reports.

October was a busy month, with the announcement of both the Box Office Customer Portal and eMail Relationship systems.

The Box Office Customer Portal is an ongoing project, which is about to go public globally (during 2009Q1). The project integrates Network Box systems for Monitoring, Inventory, Licensing, Deployment, Ticketing and Workload Statistics into a single web-based framework hosted in the cloud.

The eMail Relationship system is a game-changing approach to how to handle spam and viruses in emails. For the Network Box, relationship enforcement adds minimal overhead (and actually reduces overhead in some cases).

For the spammers, they will have to re-design their entire database system. The first of our relationship-based systems was released to customers in November, and we continue to rollout this functionality, phase by phase (with more to follow early in 2009).

Also in November, we released a new anti-spam engine utilizing fuzzy fingerprints (able to detect, and block, subtle variations in text/attachments to a spam email).

December saw the release of the Network Box Global Monitoring System to all customer boxes. With the migration to GMS, we are able to offer our customers access to a truly useful resource for ensuring network, equipment and service availability. We monitor more than 100 metrics for each Network Box, and this system gives customers a window into that status information, in real-time - and with a global overview for multi-box / multi-country customers.

In addition to the above functional enhancements, 2008 was as busy a year as ever for our Network Boxes out in the field. We enforced per-box averages of 6.3 million firewall and 1.3 million IDP blocks, 1.2 million spams, over 44,000 email borne malware/viruses, while scanning over 24 million web page objects for malware/viruses and blocking access to close to half a million undesirable websites. In addition to this, Network Box headquarters distributed almost 2.7 million protection signatures in more than 16,800 PUSH updates.

Instead of merely providing a unit containing a fixed set of features and updating only the signatures to recognize threats, Network Box provides the product model and infrastructure to evolve the features of devices in the field; to not only keep the recognition of threats up to date, but to also evolve the tactics employed to isolate those threats. As hackers, virus writers and spammers change tactics over time, only an equally dynamic, service-based solution such as Network Box can keep up with this adaptive security landscape.



2009 Preview

NETWORK BOX

The roadmap for Network Box in 2009 emphasizes five primary areas for enhancement. Let's present each of these in turn.

1. **Visibility of management and monitoring system metrics and unification with per-box metrics.** This project will unify the Box Office Customer Portal and the presentation of management information from the monitoring, inventory, licensing, deployment, ticketing and workload statistics systems. It will also unify the per-box reporting with that available through Box Office, so figures can be compared with others of similar geography, organization type, size or industry.
2. **Provision of a single holistic GUI view of the network traffic by user and service (unifying mac, IP assignment, email address, and username).** This is a key component of our product direction. The Network Box product will interface to existing DHCP and LDAP directories, as well as on-the-box systems, to provide a single holistic view of user and machine activity. The different addressing concepts (such as MAC, IP, eMail, Username) will be unified into one reported 'entity'. The current per-module approach will blend into a multi-dimensional reporting framework with services on one axes, and entities (or entity groups) on the other.
3. **Improvement of on-the-box reporting and analysis, using a unified reporting and data export framework.** The existing my.network-box.com, Mail Portal and Periodic Reporting frameworks will be unified into a single framework using web-based AJAX, PDF, eMail and data export capabilities. All reporting will be through this new

framework. This will allow for data export, printing, and reporting (via HTML or PDF) and for retrieval of previously-generated reports. The framework will allow for the definition of periodic reporting to be delivered via email, web or file transfer mechanisms.

4. **Unification, and improved granularity, of the box configuration and management of clusters of Network Boxes.** Configurations will be able to be defined globally, per-cluster, per-box, per-domain or per-user. Configuration changes will be able to be made centrally, and replicated across a wide-area network of connected Network Boxes. Cluster support will be core to this, and will allow workloads to be automatically balanced across a local or wide area network of Network Boxes.
5. **Extensions to protocol support.** The majority of work here involves both client and server side support for SSL across the major protocols (ie; POP3S, SMTPS, IMAP4S and HTTPS). But, we are also working on introducing scanning for some new protocols (in particular in the areas of P2P and Instant Messaging).

The above will provide for a single holistic view of an entire global network of Network Boxes, but with configuration granularity down to the per-user level. It will not matter if you have 1 or 100 Network Box sites - the configuration system will be the same and completely scalable.

The #1 request we have had from users has been for improved reporting. A completely new reporting and data storage framework is designed to satisfy most compliance and management reporting requirements (with data export capability, using standard formats).

We expect to be able to deliver the above as a free-of-charge software enhancement, before the end of 2009.

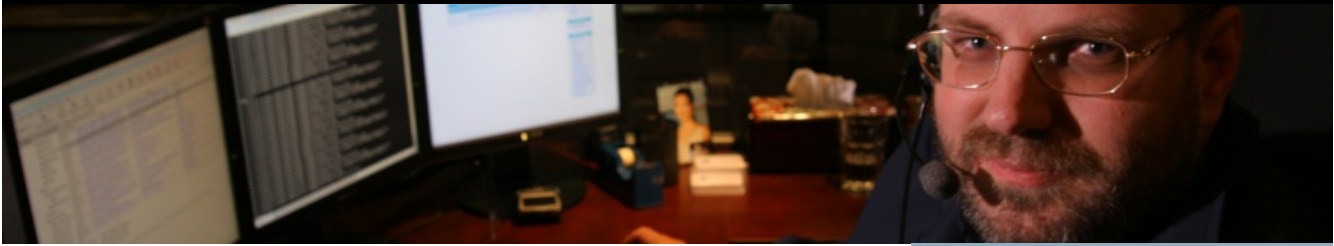


CVE 2008-4844

During December 2008, Microsoft advised of a 'zero-day' vulnerability in its Internet Explorer versions 7 and earlier, that allows the execution of malicious programs on a victim computer. Network Box gateway devices were able to protect users by nullifying and isolating malicious payloads at the network gateway (ie; before they reach client computers) using HTTP antivirus scanning. Because the vector of attack is within Internet Explorer itself, attackers can vary the payload of the attack, making it impossible to give a generic identification to the payloads that are delivered through this vulnerability. This means that specific signatures need to be developed on a case by case basis.

Network Box advises its customers to take the following steps to increase the level of protection against the vulnerability CVE-2008-4844:

1. Ensure that Content Filtering is enabled on the Network Box. Malicious payload hosting sites are categorized as undesirable by Network Box, so content filtering can restrict outgoing web browsing requests to such sites even before those requests leave the network.
2. Ensure that HTTP AV scanning is enabled on the Network Box. This enables incoming threat payloads to be identified before they reach the client computers.
3. Ensure that your internal network computers are configured to pass HTTP requests through the Network Box, either directly through local browser Proxy settings, or indirectly through redirection at the Network Box gateway.
4. Download and install the Microsoft security updates for Internet Explorer. Or alternatively, customers should enact their own corporate policies for managing critical updates.



January 2009 Features



Due to both the christmas and New Year holidays, we expect the upcoming patch Tuesday, on 6th January 2009, to be a fairly light one. We will be releasing some minor enhancements including:

The mail disclaimer package has undergone some work for support of Lotus Notes and for large (>999 character) disclaimers in quoted-printable encoding.

There are enhancements to the client-server policy categorization system (for small, light-workload, boxes) to better (and faster) detect and work around network connectivity faults. This will require a restart of the policy service on some boxes, but will have minimal impact to browsing and mail scanning.

We have done some work to improve the auditing of NOC engineer maintenance work on the box itself. This, coupled with the auditing done on the NOC, better allows us to satisfy compliance requirements and have accountability for maintenance work.

And, finally, we have improved the kernel module for H.323 connection tracking and NAT (used for H.323 VOIP installations).

This work will not require noticeable down-time for your users and will not require a reboot of your Network Boxes - so should have minimal impact.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

Patch Tuesday

Network Box has moved to a patch Tuesday form of software enhancement release mechanism. This is to allow the NOCs and our customers to release, and install, new software and enhancements in a globally co-ordinated manner. All NOCs will operate to the same patch Tuesday schedule. This does not affect the normal real-time PUSH updates, and is for new features and enhancements only.

For Network Box, patch Tuesday is the first Tuesday of every month, and the first was Tuesday 1st July 2008.

While critical software patches, signatures and other such day-to-day (or minute-by-minute) releases will still occur out of cycle, throughout the month, we will usually release new software features and enhancements on patch Tuesday; and conduct a phased deployment to all customer boxes early in each month.

For our customers, this “In The Boxing Ring” newsletter is used to keep you informed as to what we have been doing for you, and what you can expect in the upcoming patch Tuesday monthly feature / enhancements release.

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager; please don't hesitate to contact us for assistance.

Mark Webb-Johnson
 CTO, Network Box Corporation
 January 2009

DEC 2008 NUMBERS

Key Metric	#
PUSH Updates	1,232
Signatures Released	214,664
Firewall Blocks (/box)	556,622
IDP Blocks (/box)	131,137
Spams (/box)	54,643
Malware (/box)	1,991
URL Blocks (/box)	54,773
URL Visits (/box)	2,364,433

NEWSLETTER STAFF

Mark Webb-Johnson
 Editor

Michael Gazeley
Jasmine Arif
Jason Law
 Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
 Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
 or via mail at:

Network Box Corporation
 16th Floor, Metro Loft,
 38 Kwai Hei Street,
 Kwai Chung, Hong Kong
 Tel: +852 2736-2078
 Fax: +852 2736-2778
www.network-box.com

Copyright © 2009
 Network Box Corporation Ltd.