Welcome to the January 2013 edition of In the Boxing Ring

This month, in our end-of-year edition, we discuss the threat numbers for 2012 and what is foreseen for 2013 and beyond. Network Box Security Response monitors and manages thousands of devices around the world, and this gives us an excellent view on the threat landscape. Here at Network Box, we strongly believe that only by being able to clearly see and measure a problem is the solution achievable (and gains measurable).

On page 4 and 5, we discuss in detail about NBRS-5.0 and outline what we have recently released, as well as the final milestones. The amount of work which has been going on around the clock, has been nothing short of astonishing in its scope. We have literally re-invented our approach to security - moving from a fixed threat blocking appliance to a flexible content classification and policy enforcement system. We are confident customers will be satisfied with the result.

Page 6 details the features and fixes to be released in this month’s patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.

Mark Webb-Johnson
CTO, Network Box Corporation
January 2013

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

Twitter  http://twitter.com/networkbox
Facebook  http://www.facebook.com/networkbox
Network Box Response  http://www.facebook.com/networkboxresponse
LinkedIn  http://www.linkedin.com/company/network-box-corporation-limited
Google+  https://plus.google.com/u/0/107446804085109324633/posts
PUSH Updates & Signatures Released

During 2012, Network Box Security Response PUSHed out 6,328 updates, totaling 4,484,811 signatures (down 11.2%, and up 15.6% respectively, compared with 2011).

That is approximately one new signature every 7.0 seconds. 2012 continued to see the number of signatures per-update fall, while the number of signatures released increase; reflecting the continued move to cloud-based signature systems (such as the Network Box Sentinel Z-Scan, and NBCP content categorization systems). We expect this trend to continue, as traditional signatures continue to be the most effective against the depth and breadth of malware, whilst cloud-based signatures are emerging as the most effective solution for zero-day outbreaks.

Spam & Malware

During 2012, the average Network Box blocked 163,126 spams and 7,470 malwares (down 21.6% and 6.7% respectively, compared with 2011).

As with 2011, the overall reduction in spam volume continues. However, the reduction in spam volume is somewhat masked by continued increase in use of pre-scan filtering (such as RBL blocks at the envelope stage and recipient address verification). Such envelope-stage blocks are effective against a huge amount of spam (currently estimated at around 41%, globally) and messages (both spam and malware) blocked at the envelope stage do not appear in our reported figures for ‘messages blocked as spam and malware’. With the release of NBRS-5.0, we hope to be able to better report on this. During 2012, the average Network Box blocked a spam or malware once every 185 seconds.
**Firewall & IDP Blocks**

During 2012, the average Network Box blocked 10,497,946 attacks using firewall technology, and 1,669,242 attacks using IDP technology (up 14.2% and 17.5% respectively, compared with 2011).

As global bandwidth increases, so do the network-level attacks. Attackers are now freely making use of vast botnets to launch DDoS attacks against enterprises - with our larger customers experiencing such an attack on average once every six weeks. This trend started in 2011, and continued throughout 2012. To improve our protection capabilities in this respect, Network Box launched the first NBRS-5.0 security modules to address network level attacks against web applications (the NBRS-5.0 WAF+ service offering).

The IPv4 address space is now so polluted that during 2012, the average Network Box customer blocked a firewall/idp network-level probe once every 2.6 seconds. In 2012, our partnership with Microsoft flourished and we launched our real-time Microsoft MAPP signature partnership page on the Security Response website.

**URL Blocks & URL Visits**

During 2012, the average Network Box blocked 1,989,761 websites due to company content filtering policy enforcement, with 50,247,987 website URLs visited over the year (up 19.6% and 9.6% respectively, compared with 2011).

As expected, the growth in bandwidth (and in particular web usage) continues. 2013 will see the launch of Network Box NBRS-5.0 Application Identification and Control packages, along with improved web content control in the NBRS-5.0 product. This will allow our customers to better extend their outbound policy control to not just web, but all application-level traffic.

**So, what is foreseen for 2013 and beyond?**

The demand for Bring-Your-Own-Device (BYOD), and cloud service offerings continues to grow, and upcoming Network Box service offerings will specifically address these requirements. We continue to forge partnerships with major cloud service providers, to be able to offer our security platform in the cloud - bringing the protection as close as possible to the assets being protected. However, a key point often ignored is that this does not remove the need for protection of the office network. Even if the DMZ servers are moved to the cloud, both inbound and outbound protection and policy control is still required in the office - and that is an issue that Network Box will continue to address. We are working hard on service offerings to address such hybrid deployments (where IT assets are split between the office and cloud / datacentres).

IN THE BOXING RING

Network Box Version Five
NBRS-5.0

NBRS-3.0 was a single product, with just four service offerings (FW+, CF+, AV+ or UTM+). NBRS-5.0, by comparison, is made up of a large number of security modules, with 57 of them making up an NBRS-3.0 UTM+ equivalent product, at last count. Some of these modules are relatively small, while some are massive, such as the base security module, or the web based administrative system, which come in at several hundred megabytes each.

As of today, we have released a total of 25 NBRS-5.0 security modules. These make up the WAF+ product, and its support systems. Amongst others, they include the most important 'base' security module, as well as firewall, DDoS protection, proxies, reporting, and a web based administrative user interface. That is a little under half the number of security modules required for UTM+, but over 90% of the estimated completed code.

We've also already released our entire infrastructure to support NBRS-5.0, including 'Box Office' enhancements, a content delivery network for code package repositories, a global signature release system, as well as, global NOC, licensing and provisioning systems.

The amount of work which has been going on around the clock, out of sight of both our distribution partners and our clients, has been nothing short of astonishing in its scope. We're literally re-inventing our approach to security - moving from a fixed threat blocking appliance to a flexible content classification and policy enforcement system - and we ensure everything needs to meet our very exacting production standards before anything is allowed out of our research and development laboratories. That means extensive programming, documentation, testing and fine-tuning; which all takes a great deal of both time and effort. It is hard and exacting work, but like everything worthwhile, the rewards would not have been as great, if we had taken any shortcuts along the way.

Now that our NBRS-5.0 (Network Box Reserve Set Five) based Anti-DDoS WAF+ (Anti-Distributed Denial of Service Web Application Firewall Plus) has been officially launched, the most frequently asked question we get is, "when is the NBRS-5.0 based UTM+ (Unified Threat Management Plus) coming?"

The short answer, is that a significant portion of it is already here.

We're literally re-inventing our approach to security - moving from a fixed threat blocking appliance to a flexible content classification and policy enforcement system - and we ensure everything needs to meet our very exacting production standards before anything is allowed out of our research and development laboratories. That means extensive programming, documentation, testing and fine-tuning; which all takes a great deal of both time and effort. It is hard and exacting work, but like everything worthwhile, the rewards would not have been as great, if we had taken any shortcuts along the way.
Below is a roadmap, which gives a clear overview of what we have recently released, as well as the final milestones, culminating in a product and service, which far surpasses the current UTM+ capabilities of NBRS-3.0.

1. Back in the summer of 2012, we completed and released the base platform and support infrastructure for NBRS-5.0. This made up the bulk of the product's code base, and forms the foundation for all our NBRS-5 product offerings.

2. We followed that up, in the winter of 2012, with the NBRS-5.0 WAF+ service package. This package provide new functionality (not previously available with NBRS-3.0) to protect DMZ/cloud based web servers from Internet-based attackers. It provides network firewall, web application firewall, DDoS protection, and protocol translation (IPv4-IPv6 / IPv6-IPv4 bridging) functionality, into a single service offering.

3. To produce a web application firewall, we had to design and build a proxy capable of understanding the web's HTTP protocol. We're now turning that around, and combining it with our advanced scanning technology, to make up our next NBRS-5.0 offering - SURF SCAN. This will provide for protection of web based clients on the LAN, browsing web servers in the Internet. It will support anti-virus scanning, as well as web site and content classification - for comprehensive policy control. It will also support extensive reporting capabilities.

4. Following on from that, we will be releasing APP SCAN - the application identification system that we have been working on for some time. This, operating standalone, or combined with SURF SCAN, is capable of identifying applications at the network level, and extracting meta data and content from the data streams. Both anti-virus scanning and policy control technology can then be applied.

5. At that point, we will have comprehensive web server, and LAN client support, so we will be releasing our mail server protection MAIL SCAN. This will provide support for scanning mail traffic using the SMTP, POP3 and IMAP4 protocols.

6. Finally, we will round-out the UTM+ equivalence, with the release of a set of security modules implementing such functionality as QoS (Quality of Service), VPNs, Clustering, High Availability, etc. Some of these will actually released alongside the earlier service offerings, as and when they are ready.

Migration

Over the coming few months, we will release information on migration options for NBRS-5.0. As with the previous NBRS-3.0 upgrade, we will offer this to existing customers who are running current Network Box hardware (or approved virtual systems), with the goal of migrating all customers over to the Network Box Version Five platform as soon as possible. Without a doubt, 2013 is going to be the most exciting year yet, for technological advancements from Network Box.
January 2013 Features
On Tuesday, 1st January 2013, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Enhancements to various internal NOC systems
- Minor fixes to my.network-box.com administrative web interface
- Minor enhancement to mail scanning system for envelope recipient blacklisting
- Further support for NBRs-5.0 in Box Office systems
- Various (mostly internal) enhancements to Box Office and support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

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

NETWORK BOX | December 2012 Awards

IT Pro Corporate Choice Awards 2012
Network Box is extremely pleased to be able to announce, that both S-Scan, Network Box’s high performance Web Content Filtering engine, and WAF-Scan, Network Box’s Anti-DDoS Web Application Firewall system, won IT Pro Corporate Choice Awards 2012, in their respective categories.

MIS Asia, The Strategic 100
Network Box was recently honored as one of the MIS Asia | The Strategic 100. This is the fifth time that Network Box has been named in this prestigious group and is privileged to be included with other respected honorees such as Google Inc., Apple Inc., Adobe Systems Inc. and Samsung Electronics Co. Ltd.