In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the January 2014 edition of In the Boxing Ring

Happy New Year to you all! 2013 has been another landmark year for Network Box. Not only did we release the new Network Box 5 (NBRS-5.0) Software and Hardware platforms; but Network Box continues to win numerous awards, including a third Gold Award published out of Silicon Valley, taking our total awards tally to over 80. This and many other Network Box achievements are highlighted on page 5.

In addition, on page 3, we discuss the threat numbers for 2013. 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 2, Network Box Managing Director, Michael Gazeley, discusses the state of the current cyber security landscape, and the importance for companies to focus on protection against the 'next attack', rather than the last/current attacks.

Finally, on pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for NBRS-5.0 and NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years).

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
January 2014

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
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

IN THIS ISSUE

Focus on the NEXT ATTACK

(Not just the last one)

by Michael Gazeley
Managing Director, Network Box

At the start of each new year, the same question inevitably gets asked of me by both the media, and potential Network Box clients alike, "*what should we focus on this coming year, in terms of cyber security?*" Usually, the questioner then goes on to frame the question with a relatively recent marketing term or two, such as Advanced Persistent Threat, Zero Day Vulnerability, or Ransomware.

Well, ice hockey legend Wayne Gretzky famously said, "I skate to where the puck is going to be, not where it has been." This philosophy helped Gretzky become one of the most successful sportsmen of all time. And it's hard to find a better philosophy to apply to cyber security as well, for fairly obvious reasons.

Yet the vast majority of information technology managers around the world, and even well known cyber security professionals, seem to be almost pathologically fixated on the 'last attack,' rather than the 'next attack.' The last attack, either being what their own network suffered recently, or what is currently the hot cyber attack topic in the mainstream press.

For example, if a serious DDoS (Distributed Denial of Service) attack occurs against a local government department's website, making newspaper headlines, one can essentially guarantee that in the following weeks and months, IT Departments up and down the land, will be putting out Requests For Proposals for Anti-DDoS systems, arranging vendors to come in to give seminars on Anti-DDoS technologies, and generally shifting the entire focus of their cyber security onto this one single issue - until of course another kind of attack occurs - then suddenly the new attack will become the centre of attention.

Network Box's philosophy has never been to just focus on the last attack, nor do we just focus on one vector of attack. This is because your computers, networks, devices, data, and users; are probably not going to be attacked by what exactly attacked them last time; nor will they be attacked by just a single threat vector. Cyber attacks are constantly evolving, and successful cyber attacks seldom rely on just one technology or methodology, anymore.

Our Anti-DDoS technology for example, has won multiple awards right across the globe; but it is not the only aspect of cyber security which we focus on. Indeed, at Network Box, we pride ourselves on developing the very best cyber security technologies, to handle everything from zero day viruses, mobile malware, web application vulnerabilities, phishing spam, hackers, and a variety of other threats.

Just as a bodyguard in the physical world needs to be able to protect clients from all forms of harm; be it being shot, knifed, poisoned, strangled, drowned, burnt, blown up, or hit by a car; cyber security systems need to be able to deal with a very wide spectrum of threats too. And the ability to deal with all of these potential threats, also needs to be augmented with both real-time PUSH update technology, as well as twenty-four hour security operations centre monitoring, management, and support, to internationally recognized and certified standards.

So in the coming year, don't just focus on the last attack that impacted your network, nor just the current attacks which are in the headlines right now. And don't just focus on one or two threat vectors. The best way to defend your systems is to ensure every threat vector is taken into account. Because just about the only thing one can be certain of, in the realm of cyber security, as with most areas of life, is that there are very few certainties.

The only way to truly mitigate risk, and be ready for the next attack, is to be ready for everything. That's what Network Box's Managed Security Services are all about.

2013 Threat Round-Up

Summary and analysis of the *Network Box Threat Statistics* for 2013

Network Box Threat Statistics	2012 Numbers	2013 Numbers	% Change
PUSH Updates	6,328	**5,995**	-5.9
Signatures Released	4,484,811	**6,860,044**	+53.0
Firewall Blocks (/box)	10,497,946	**10,544,863**	+0.4
IDP Blocks (/box)	1,669,242	**1,227,740**	-26.4
Spams (/box)	163,126	**172,604**	+5.8
Malware (/box)	7,470	**19,793**	+165.0
URL Blocks (/box)	1,989,761	**1,858,598**	-6.6
URL Visits (/box)	50,247,987	**39,448,903**	-21.5

▸ Network Box Threat Statistics for the **2013 calendar year**, compared to the 2012 numbers

As always, every month we see more and more threats, with faster distribution times. Network Box will continue to invest in technologies to speed-up the protection release cycle, and will continue to leverage our excellent customer relationships so that we can all work together to co-ordinate an effective defense.

PUSH Updates & Signatures Released

During 2013, Network Box Security Response PUSHed out 5,995 updates, totaling 6,860,044 signatures (down 5.9%, and up 53.0% respectively, compared with 2012).

Firewall & IDP Blocks

During 2013, the average Network Box blocked 10,544,863 attacks using firewall technology, and 1,227,740 attacks using IDP technology (up 0.4% and down 26.4% respectively, compared with 2012).

Spam & Malware

During 2013, the average Network Box blocked 172,604 spams and 19,793 malwares (up 5.8% and 165.0% respectively, compared with 2012).

URL Blocks & URL Visits

During 2013, the average Network Box blocked 1,858,598 websites due to company content filtering policy enforcement, with 39,448,903 website URLs visited over the year (down 6.6% and 21.5% respectively, compared with 2012).

Network Box 5
NBRS-5.0

On Tuesday, 7th January 2014, Network Box will release our patch Tuesday set of enhancements and fixes.

NBRS-5.0 Features
January 2014

Our work this month primarily involves extensions and enhancements to existing security modules, as we prepare for the upcoming release of NBRS-5 UTM+ service packages. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-5.0, these include:

- Revisions to application identification for UDP protocol support
- Improvements to link failure detection of NBSYNC cluster connections
- Several new GMS sensors, and improvements in information display from existing sensors
- SMTP third-party relay protection
- Enhancements to SSL proxy for HTTP
- Support for custom-hooks in network and firewall modules
- Support for custom-hooks in mail scanning modules
- Various fixes and enhancements to SSL, IPSEC and PPTP VPN modules
- Support for IPv6 secondary addresses using defined subnet masks
- Improvements to information display to NOC engineers during signature re-synchronization
- Introduction of a mail search facility
- Improvements to SMTP quarantine
- Improvements to package management for NOC engineers
- Enhancements to the NBRS-5 NOC modules for configuration synchronization

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.

NBRS-3.0 Features
January 2014

On Tuesday, 7th January 2014, 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, for NBRS-3.0, these include:

- Extensions to Box Office regarding contract maintenance and display
- Extensions to Box Office to improve support for regional NOCs
- Revisions and enhancements to Global Monitoring Systems
- Various (mostly internal) enhancements to several internal 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.

* Note that this will be the last month that we publish the statistics in the table below. As we start to deploy more NBRS-5.0 Network Boxes, the statistics would become skewed due to the different methods of calculating totals between NBRS-3.0 and NBRS-5.0. Accordingly, we will resume publishing these statistics later in 2014, once the percentage of NBRS-5.0 boxes deployed increases.

Network Box
Year in *Focus* 2013

2013 marked another incredible year for Network Box. Not only did Network Box win the 'Award of the Year' at the HKICT awards 2013; but Network Box also won a third Gold Award published out of Silicon Valley. Network Box's continued commitment to producing cutting-edge technology has allowed the company to receive, now, more than 80 international awards. Indeed, Network Box's comprehensive security solutions have been internationally recognized and Forrester cited Network Box as a strong performer in its Emerging MSSP Q1 2013 report.

In addition to the many awards and accolades that Network Box has received, in November 2013, Network Box launched the new Network Box 5 (NBRS-5.0) managed security platform. The state-of-the-art software platform is up to eight times faster than the previous version; and a new range of 64bit hardware was also launched to support the new software platform.

To commemorate another landmark year, Network Box has published: **Network Box - Year in *Focus* 2013**. The brochure highlights Network Box achievements over the last twelve months including awards, events, seminars and trade shows.

LINK:
http://www.network-box.com/sites/default/files/files/Year%20in%20Focus_2013.pdf

DECEMBER 2013 NUMBERS*

Key Metric	#	% difference (since last month)
PUSH Updates	337	-19.6
Signatures Released	422,748	-61.0
Firewall Blocks (/box)	826,997	-3.2
IDP Blocks (/box)	113,540	+4.3
Spams (/box)	10,368	-9.9
Malware (/box)	7,501	+28.2
URL Blocks (/box)	115,317	+2.7
URL Visits (/box)	3,048,552	-1.6

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box UK
Network Box USA
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