JUN 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the June 2014 edition of In the Boxing Ring

In this month's featured article, Network Box Managing Director, Michael Gazeley, talks about ***The Vulnerability of Everything***. This is a play off the CISCO slogan, 'The Internet of Everything,' which is being quoted across the globe now. Currently, there are a million new devices connecting to the Internet every three hours, and as more and more devices are coming on-line these devices are becoming vulnerable to cyber criminals and malicious hackers.

On pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally we are pleased to announce the launch of our new Security Operations Centre in Singapore; lead by our team at Network Box Singapore. If you want to contact Network Box Singapore, please feel free to contact us, we will be more than happy to put you in touch with them directly.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 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 month's issue:

NETWORK BOX

Businesses are now facing cyber threats, via vectors, which just a few short years ago, would have seemed like something out of a Hollywood science fiction movie, or a particularly inventive television episode of, 'Mission Impossible.'

The Vulnerability of Everything

by Michael Gazeley

When you plug into the world, it's easy to forget the world is also plugged into YOU

Risk Management, in a business context, is defined as the forecasting and evaluation of financial risks, together with the identification of procedures to avoid, or minimize their impact. But how can 'management' be made to understand, manage, and mitigate today's cyber risks? Unfortunately, outside of the IT Department, most managers simply don't understand, (or don't want to understand), the very real-risks posed by cyber-threats. And IT Managers often don't have the influence required to force through much needed changes, in both corporate thinking, and corporate spending, on cyber security.

Recently, 40% of the population in South Korea had their personal details stolen

How bad do things have to get, before people sit up and take notice? In the world today, we are faced with smart phones and tablet computers, which can bypass an organization's firewall, if the office network is not setup securely. Not only that, but in that office, more and more smart 'connected' devices are being installed, often without any planning, resulting in office printers, fax machines, telephones, video surveillance, web cams, and copiers, which can be leveraged to both spy inside the office network, as well as attack third-parties outside the office network.

One million new devices are being connected to the Internet every 3 hours

Examples of such attacks, range from the almost comical discovery that a Samsung refrigerator, which was compromised, and had become part of a spam bot-net. (It had sent out more than three-quarters-of-a-million spam emails, before the breach was discovered.) To more sinister examples of IP Teleconference Phones being hacked, to spy on organizations' board meetings. And far worse than that, hacked webcams (and even baby monitors!), used to spy on people (and their children) in their homes.

By 2020, there will be more than 50 billion devices connected to the Internet.

One of the largest recent successful cyber-attacks, on the retail sector, is believed to have been made possible by a security breach of the victim's Heating and Ventilation systems. Researchers have since discovered over 55,000 such HVAC systems connected to the Internet, and have noted that in most cases, these systems contain basic security flaws. Not to mention the fact that, "the security at such companies tended to be poor, and that vendors often used the same password across multiple customers."

Once hackers find your devices, many can be compromised just by logging in using:

ADMIN / 123456

The SHODAN search engine for internet devices, has been called, **"the scariest search engine on the Internet,"** by CNN. The engine itself advertises that it can help you find exposed online devices, including, "Webcams, Routers, Power Plants, iPhones, Wind Turbines, Refrigerators, and VoIP Phones." Forbes calls SHODAN, **"terrifying."** The system collects information on more than 500 million Internet-connected devices and services each month.

Medical equipment such as surgical and anesthesia devices, pacemakers, insulin pumps, and lab analysis tools, can all be hacked

The stark reality, is that major corporations and government departments, are moving at the speed of corporate red tape. While hackers and criminal organizations, are moving at the speed of the Internet.

It doesn't take much to realize who has the upper hand right now. And one shouldn't forget the other unfortunate reality, which is the fact that the potential victim needs to successfully defend themselves from a never ending onslaught of attacks; while the hacker only needs to successfully get in once.

NETWORK BOX

Yet despite all these facts, and despite the ever growing number of media headlines, highlighting successful attacks on companies and governments right across the globe, most senior managers are still all but ignoring cyber threats.

Sometimes it seems that the bigger the successful attacks are, often counting breaches of personal data accounts in the multi-millions, the more numb the entire world seems, to the shocking realities involved. And while you can usually change your password fairly easily, you can't as easily change your social security number, or passport number, or your home address, or your mobile phone number. As the number of successful breaches grow, we are all becoming more vulnerable, as the criminals get a clearer and clearer picture, of our **personally identifiable information**.

Unfortunately, time and again, organizations are only looking seriously at their cyber security, after they become a victim of a cyber-attack. Sometimes, not even then.

This is simply not acceptable anymore. You cannot get your company's private data back, once it's gone. You cannot easily regain your clients' trust, once their personal details have been stolen. Money stolen via on-line attacks, is just as real, as money stolen out of an armored car.

Cyber-attacks can, and do, cause very tangible damage, in the real-world.

There's no time to waste, get properly protected today.

"You cannot escape the responsibility of tomorrow by evading it today."

– Abraham Lincoln

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd June 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features
June 2014

This month, for Network Box 5, these include:

- Throughput and stability Improvements to generic proxy regarding data pipes
- Improvements to core HTTP protocol support (Web Client, Web Server and WAF+ modules)
- Enhancements to policy rule processing for application identification security modules
- Fix to subroutine policy rules in proxy modules
- Improvements to block pages for HTTP protocols
- Support for alert-by-email option in proxy mail policy rules
- Layout improvements to LDAP search for display of search results with multiple values
- Improvements to LDAP server connection specification to permit direct specification of basedn and bind parameters
- Enhancement to LDAP synchronisation to permit enable/disable of sync on a per-connection basis
- Enhancement to LDAP synchronisation to provide an option to filter users only in one or more groups
- Add support for 'group_member' entity attribute, as 'groupmember' acl term in proxy web client
- Stability improvements in database logging subsystem (to better cope with connection faults)
- Revisions to Z-SCAN system for mapping Z-SCAN confidences to spam confidence levels (for confidences < 50%)
- Add support for port ranges to network firewall security module
- Performance improvements in generic UDP proxy
- Improvements to logging of SMTP client and server envelope-stage blocking
- Change to proxy so that domain ACL checks are now case-insensitive
- Add support for PEERDNS=no option in DHCP client (to disable setting of DNS servers from peer)
- Enhancement to SSL VPN to permit definition of multiple routes per connection
- Improvements to reporting on SSL, IPSEC and PPTP VPNs
- Enhancement to reporting to provide for graphical drag-and-drop layout changes, as well as 1/2 width report option
- Addition of a confirmation dialog for dashboard layout reset in administrative web portal
- Change to administrative web portal 'Guide' menu option to support download of multiple types of guides
- Release of Admin Portal Dashboard Overview guide
- Release of Admin Portal Quick Start guide
- Release of Admin Portal User guide
- New 'primaryemail' entity attribute type (to define a primary eMail address for an entity with multiple email addresses)
- Add support for a policy rule to permit fine-grained entity selection in user portal email reports
- Change to user portal to include all blocked emails (not just those quarantined) in email report
- Support for SSH to multiple selected boxes in NOC modules
- Revise logic used to determine if box is in SOC mode
- Performance and stability improvements to SOC<->BOX configuration synchronisation mechanism
- Performance and stability improvements to box provisioning services
- Performance and stability improvements to signature push services
- Add support for Singapore Network Operation Centre

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 SOC will contact you to arrange this if necessary.

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

NETWORK BOX

Network Box 3 Features June 2014

On Tuesday, 3rd June 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Anti-spam engine improvements regarding large attached word/excel documents
- Renewal of my.network-box.com NOC support certificate
- Various (mostly internal) enhancements to several internal support systems

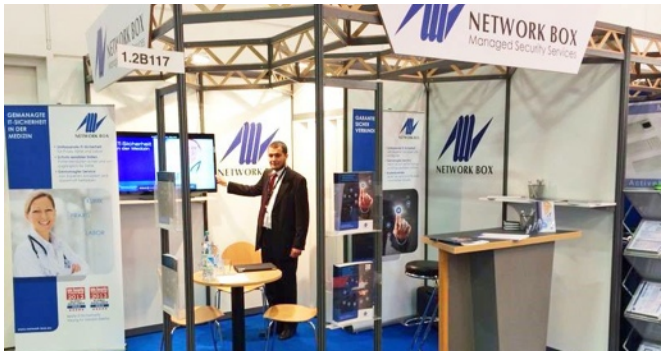
In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	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

Network Box Singapore
New Security Operations Centre

Network Box is extremely pleased to announce that Network Box Singapore Security Operations Centre was officially launched on the 22nd of May. Lead by **Jan van Leersum** and his dedicated team, Network Box Singapore will be providing world class Managed Security Service to new and existing Network Box customers in the region.

Network Box Germany
conhIT 2014



Network Box Germany, exhibited at conhIT 2014. This key event in the global Healthcare IT calendar, took place on the at the Messe Berlin, in Germany. The expo connects Healthcare IT vendors, users, and representatives, from the right across the political and scientific communities.