MAR 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the March 2016 edition of In the Boxing Ring

This month, in our featured article, Network Box USA's CTO, Pierluigi Stella highlights the issue of **Cyber Crimes & Cyber Terrorism**. Today, hackers are constantly finding (and exploiting) new vulnerabilities to compromises your network, yet many organizations are still using security techniques that were already obsolete in 2002! This is discussed further on pages 2 to 4, and how you can prevent yourself from being a victim of these threats.

On pages 5–6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. Based on Sunset Policy, we will continue to support, Network Box 3 until at least late 2018.

Finally, Network Box was awarded the Best Enterprise Risk Management Gold Award by the Academy of Professional Certification; Network Box has been nominated in two categories in the upcoming Cybersecurity Excellence Awards, in the USA; and Network Box Hong Kong welcomed members of the HKICPA for a Cybersecurity Seminar.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2016

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:

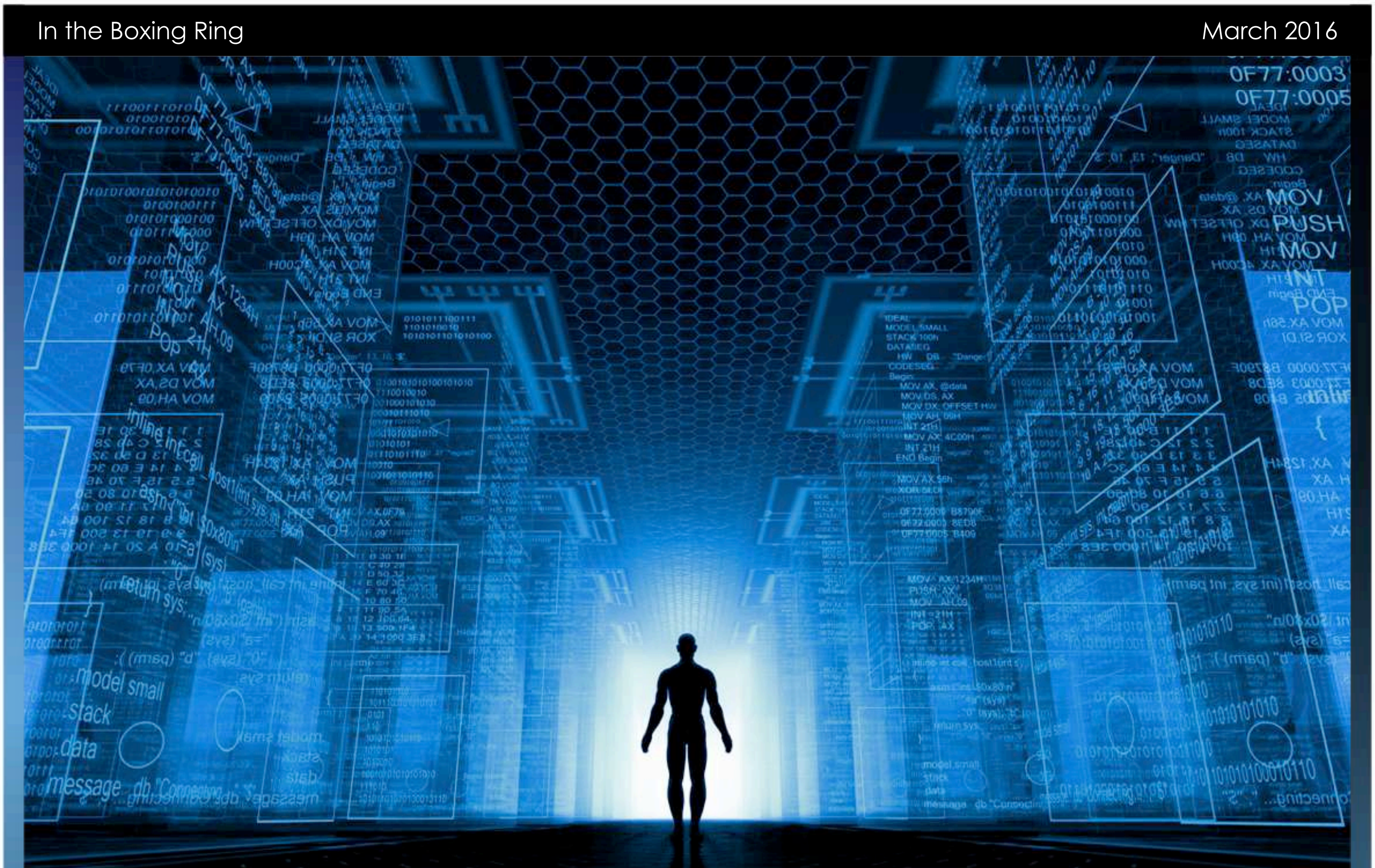
twitter http://twitter.com/networkbox

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

NETWORK BOX



Cyber Crimes & CYBER TERRORISM

by Pierluigi Stella

Chief Technology Officer
Network Box USA

The general issue of security needs to be put into proper perspective – anything made by humans can, and will be, broken by humans; and in reality, those who break always have an advantage – they're working with something that exists, and have the luxury of time to try and figure out how to break it. Whereas those who protect are in the opposite position – they're always on the defense, they're called to come up with new ways to create fences and perimeters that will withstand the constant assaults. Never has it happened in the history of humanity have defenses lasted through time.

Even the Great Wall of China, albeit still standing, in reality failed its purpose; it's there simply because at some point it became useless, obsolete, so no one even bothered to attack it. Enough of philosophy though.

Can we stop or prevent the attacks?

No.

Can we at least try to make their life difficult?

We certainly can.

Unfortunately, the actual situation of cyber defenses is far from where it should be. Recent attacks on federal government data have clearly demonstrated that even those agencies are still ill prepared to fend off attacks. It isn't that they're not doing enough; essentially, in many cases, they're doing it all wrong. Many private companies, even today, are running firewalls that were obsolete 10 years ago, they're not running IPS, they're not running AV at the gateway, or web content filtering; they're not scanning encrypted traffic. In a time when even a google search is encrypted, pretending that viruses can't come through encrypted streams is ludicrous.

I ask you, how many companies today are actually scanning for viruses at the gateway through encrypted streams?

I often have a hard time convincing my own clients that this is vital; they don't want to take the time to do the setup necessary to implement such protections. They do not want to take the time to troubleshoot the few possible issues such implementation may bring about. Security takes time and patience, and not everybody is willing to put in the effort required.

Furthermore, many companies still try to do security on their own as if you could invent security expertise overnight; they don't take security seriously, that is, until it hits them where it hurts – they lose something and, ultimately, they lose money and possibly the entire business.

As a managed security provider, we run into such situations every day. We acquire a new client, we analyze the configuration of their old firewall, and we realize there wasn't even one. In this day and age, they're still considering the LAN a trusted area, allowing all traffic outbound, opening ports right and left where it simply isn't necessary. They're still adopting security tactics that were already obsolete in 2002. Attempting to do security without spending money, treating it as, well, as a nuisance. For as long as this continues, hackers will always have the upper hand.

You ask if we can prevent or stop the attacks.

I would ask in return, can we ever hope to get ahead of the curve?

Right this moment, we are left far behind, eating the dust. Hackers have basically demonstrated that if they want in, they'll get in; period. To provide an idea of the extent of the issue, consider that we're seeing more than 300,000 new threats per day. Think about that for a second; how many security people can you possibly ever hire to mount protection against 300,000 new threats every single day? AV companies themselves have lost the battle and conceded defeat long ago. They've been trying to create new technologies that could recognize threats without having to create signatures. In fact, many experts believe signatures are obsolete, and I tend to partially agree with that statement.

I say partially because signatures are still useful in recognizing existing, well known threats. Imagine if we threw away all antibiotics because they can't stop that new bacteria we've detected but then you get strep throat and you can't be cured? Existing signatures are still very pertinent, to ensure that known and well recognized threats don't destroy your network. For as much as there are 300,000 new threats every day out there, there are also more than 15 million well known threats that CAN be stopped by an AV. We don't pay much attention to them because the AVs are stopping them; but I assure you if we removed the AVs, those threats would join the legions of new threats and become a horrendous nightmare for us all.

The state of security today, I feel, is somewhat mishandled. Indeed, security is neither for the faint of heart nor for the untrained person.

Can we ever hope to get ahead of the curve?

The way security should ideally be approached is by integrating it within the business processes as, for instance, process plants do with their physical security. You don't walk into a refinery and define a new business process without keeping very closely in mind that the whole plant might blow up if you aren't careful. Similarly, no one should design business processes that could jeopardize the integrity of a company's data. A security expert should be called to attend

all such planning sessions, to ensure security is built into the business processes, and not designed only as an afterthought. We all need to realize that we're under perpetual attack and we need to know how to prevent such situations.

How many companies spend even a dollar per employee to train them on security issues? To just show them how a link in an email could compromise an entire organization? To teach them not to click unless they know what they're clicking?

This doesn't seem at all technical, and yet, it is, in my opinion, the single most important area wherein security is lacking, aside from the perimeter defense. Recently, we've taken to calling this 'the human element' and finally, our industry has recognized this as the most vulnerable part of any company. And please don't go looking at unskilled employees as the culprits. We're all targets and I personally have witnessed numerous situations whereby a C level employee was the one clicking on a link that was clearly **not** to be touched.

The difference is that when someone at the lower levels loses their computer, it's quite possible that not much damage will occur. But when a C level does the same, the risk is exponentially higher.

One very common type of attack is aimed at stealing corporate bank credentials; only the CEO and CFO may have those. Once hackers gain that information, they can transfer money to their own accounts anywhere in the world, and the bank is no longer responsible for the loss because the transfer was made with legitimate (albeit stolen) credentials. So, C level people, you above all should take the security class before anyone else in your company! Then embrace security and show to all your employees that it's important, show it by example, show it by creating policies that always include security; just create an environment around you that breathes security (without breathing fear).

Going back to the technical aspects, many tools are available today, to protect your network. A firewall is necessary but please, do not stop there as that was enough way back in 2002. You will need IPS, AV at the gateway, web filtering; you MUST be scanning encrypted streams, and when I say scan, I mean decrypt, open, scan, re-encrypt – yes a MitM attack of sort – you need to ensure that the company doing this gives you a certificate, which will be used to intercept all the encrypted calls outbound, ensuring that they can be properly decrypted and scanned.

Never connect to your network remotely without a VPN. Never allow anyone who's not a security expert access to your firewall. The common practice of allowing network people to manage the firewall while security people manage the IPS is absolutely to be abhorred; network engineers' objectives are often in contrast with security – they need to get things working and are prone to taking short cuts in order to get there.

A security experts understands the hidden consequences of an incorrect or 'loose' configuration, and will take a few more seconds to think it through, and provide a solution that is secure while still allowing business to continue without interruptions.

Spend money, where it matters, and do not underestimate the danger, because it is real and it is frightening, my friend. But take heart that it is also possible to contain it. Afterall, you want to be the one in the parking lot who has an alarm. That way, the thief will move on to the next car – that too is a viable way of doing security.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st March 2016, Network Box will release our patch Tuesday set of enhancements and fixes. This month, the regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
March 2016

This month, for Network Box 5, these include:

- Support for host groups with more than 1,024 individual host entries (now only subject to memory limitations).
- Support for network routing rule sets with more than 1,500 individual rules (now increased to 65,536 individual rules).
- Improvements to transparent POP3 proxy, related to pipelined email.
- Improvements to transparent web server proxy, related to handling of non-standards-conformant spurious response data.
- Provide an option to not log invalid packets in network-firewall security module.
- Introduction of a new Global Monitoring System firewall sensor.
- Show attacker IP address in Frontline GMS sensor (when 5 or less attackers).
- Introduction of a Nth policy rule term in network and proxy layers, to facilitate fairer load balancing.
- Provide a facility to show chosen SSL cipher and version for cluster connections.
- Improvements to cluster sync re-connections, related to highly unreliable links.
- Introduction of automatic network firewall rules for DHCP client links.
- Improvements to URL canonicalisation (and normalisation) library.
- Mail scanning support for detection of VBA scripts in office documents without MACROS directory structure.
- Improvements to validation of user input errors in admin web portal.
- Support customisation of search range day limit in admin and user web portals.
- Improvements to memory consumption when downloading large PDF reports from admin web portal.
- Enhancement to display personal whitelists and blacklists on user web portal.
- Base support for configuration templates.
- Introduction of fine grained control over release and whitelist options for policy, spam and malware in user portal report.
- Improvements to SOC facilities for selection and working on multiple managed devices.

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 ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features March 2016

On Tuesday, 1st March 2016, 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:

- Enhancements to Box Office and Response web sites
- 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.

Academy of Professional Certification

The Best Enterprise Risk Management (ERM) Gold Award

Network Box is extremely pleased to announce that the company won the Best Enterprise Risk Management (ERM) Gold Award 2015. This prestigious award is given by the Academy of Professional Certification (APC), to honor companies, NGOs and organizations, in any industry, that demonstrate excellence and achievement in Enterprise Risk Management, leading to ISO and best practice world class standards.

Network Box USA

Cybersecurity Excellence Awards

Network Box has been nominated for the upcoming Cybersecurity Excellence Awards 2016, in two categories:

- Unified Threat Management
- Managed Security Service

Network Box Hong Kong

HKICPA Visit

Network Box Hong Kong welcomed the Information Technology Interest Group (ITIG), of the Hong Kong Institute of Certified Public Accountants (HKICPAs). During the visit, Michael Gazeley, Network Box's Managing Director, gave a detailed talk titled, 'Cyber Attacks and Your Business,' covering the latest cyber issues and risks, as well as the security technologies that should be used to mitigate those threats.

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 2736-2083
Fax: +852 2736-2778

www.network-box.com