OCT 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the October 2017 edition of In the Boxing Ring

This month, Network Box USA's CTO, Pierluigi Stella, talks about **WannaCry & NSA, and how they're connected.** Back in 2013, Edward Snowden revealed the unlawful collection of private information by the NSA (National Security Agency). They also did not disclose any vulnerabilities they found in security products to vendors, so they could exploit them for their own gain, and stored this information on their secured network. Fast-forward to today, and we are now seeing the effect of this. Hackers were able to steal their information about these security vulnerabilities, and used them for their own malicious purposes. The WannaCry outbreak is just one of the many results because of this. The issue could have been avoided if the NSA disclosed the information to security vendors, or did not keep such information, in the first place. This is discussed in further detail, on pages 2 to 3.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, we are proud to announce that Network Box won in the categories of *Unified Threat Management* and *Managed Security Services* in this year's **BizIT Excellence Awards**. In addition, Network Box USA was at **ASIS 2017**; Network Box Australasia attended the **Canterbury Tech Summit 2017**; and Network Box Managing Director, Michael Gazeley, was interviewed by the **South China Morning Post** about the recent *Blueborne* threat.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2017

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

WannaCry & NSA,

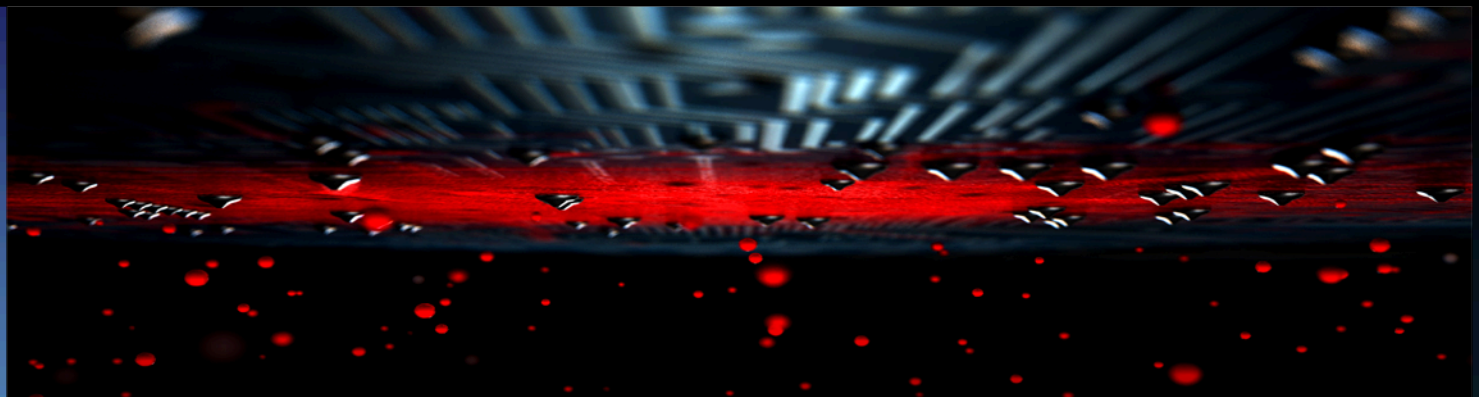
How they're connected

by Pierluigi Stella
CTO, Network Box USA

Remember when Snowden revealed what was going on with the NSA in 2013? How we were all being spied upon? How, with the excuse of preventing terrorism, this agency was collecting data on everyone, in flagrant violation of any reasonable privacy expectation (let alone law), we were all outraged! And demanded that someone be held accountable. And that the practice be stopped immediately. Do you remember that?

However, with time, some of us became convinced that in order to be safe, we may actually need to accept the new order of things. And that it's far better to let the NSA know when you called your grandmother than to risk a terrorist attack.

After all, what have we got to lose?



At the time, I too eased up on the outrage, however, as time passed and the situation changed, my stance on this issue also drastically changed. I came to the realization that I really don't want them collecting data about me.

So, how's this related to WannaCry?

One of the things we ended up accepting as a matter of fact is that the NSA (and other security agencies) withhold things. When they discover vulnerabilities in commercial products, instead of letting the vendor know about it so they can be patched, they keep it a secret, and see if it can be used as a backdoor to infiltrate computers they want to spy upon. The presumption being that their network is so secure, no one will ever know about these discoveries, so only they will be able to take advantage of them. Until, of course Microsoft and Co. finds that very same vulnerability on its own, and patches it anyway.

However, this arrogant presumption finally did backfire.

For years, we in the security industry have been telling everyone that this practice is dangerous, ethics and legality aside. We've been telling everyone that there's no such thing as a secure network. And that despite their arrogant presumption, sooner or later the NSA network could be hacked and this information leaked.

And, there you have it. Hackers were able to steal this information about a vulnerability that allows them to take over a workstation and encrypt all files. But what's worse, it allows this threat to spread horizontally. Up until now, ransomware spread vertically, as in from the server containing the malware to the workstation downloading it.

WannaCry spreads horizontally, within workstations, within a network. And that's where the big issue has been. That's what has allowed this major attack to take place.

Because once one workstation was infected, many others followed easily, and entire networks fell prey to the attack. Microsoft released a patch in March to protect against this horizontal attack. And that's likely the reason why we've seen much less of a problem with WannaCry in the US than as experienced by the rest of the world.

With Network Box, our processes and procedures are fairly stringent, and work. We patch and protect, and things don't get out of control. But frankly, that's besides the point. The real issue here is, if the NSA didn't keep such information in the first instance, it wouldn't have been available to steal to begin with, and none of this would've happened.

How's that for protection?

NETWORK BOX

Network Box 5

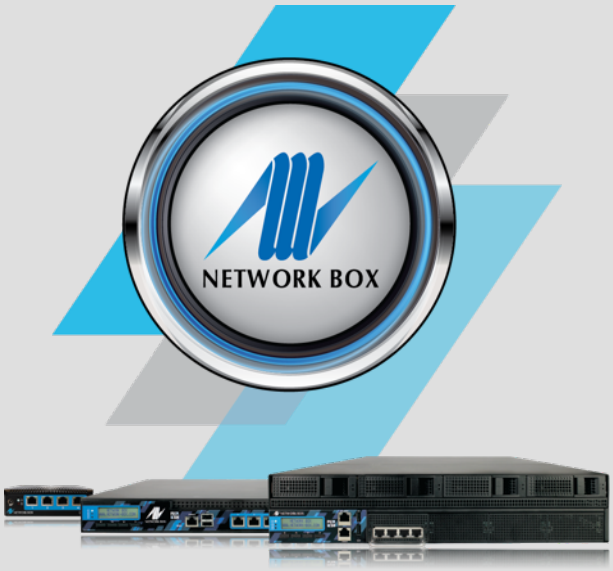
NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd October 2017, 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 14 days.

Network Box 5 Features
October 2017

This month, for Network Box 5, these include:

- Minor improvements to network firewall logging
- DNS server and resolver support for the DNSSEC key signing key rollover 2017
- General security and performance upgrades to DNS server and recursive resolved
- Additional support for optional renegotiate timeout setting in SSL VPN server
- Periodic updates and improvements to IP geolocation
- General security and performance upgrades to IPSEC VPN server
- Introduction of a standardized hook mechanism to IPSEC VPN server
- Improved performance in configuration database consistency check
- Improvements to web client rule parsing using subroutines
- Add support for a case insensitivity option for LDAP entity synchronization
- Introduction of an option to disable tracking on high availability primary 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

Network Box
BizIT Excellence Awards 2017

Network Box won the **BizIT Excellence Awards 2017** in both the *Unified Threat Management*, and *Managed Security Services* categories. The double win, showcases both the hard work by the Research and Development team, who ensure Network Box's cyber security technologies remain well ahead of the competition, as well as the non-stop dedication by the Security Operations Center engineers, who work around the clock, to protect customers from the never ending threats, attacking their computers and networks.

Network Box USA
ASIS 2017

Network Box USA exhibited at the **ASIS International 63rd Annual Seminar and Exhibit**, held in Dallas, Texas. For more than six decades, the ASIS Annual Seminar and Exhibits has been the premier event for security professionals worldwide, providing industry-leading education, and the latest products and services.

Network Box Hong Kong
SCMP Interview

Network Box Managing Director, Michael Gazeley, was interview by the South China Morning post regarding the **Blueborne** threat, which exploits a flaw found in most bluetooth devices, to spread malicious code.

LINK: http://www.scmp.com/tech/social-gadgets/article/2111185/mobile-devices-hong-kong-risk-cyberattacks-after-flaws-found

South China Morning Post

Network Box Australasia
Canterbury Tech Summit 2017

Network Box Australasia was at the **Canterbury Tech Summit 2017**, held in Christchurch. The summit explores trends, opportunities, and major shifts on the horizon. This year's theme 'Grow' encapsulated 4 topics: *Artificial Intelligence, Cybersecurity & Bitcoin, Hi-tech Export*, and *Strategy and Leadership*.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **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 2736-2083 Fax: +852 2736-2778 www.network-box.com