

OCT 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the October 2018 edition of In the Boxing Ring

This month, in our feature article, Network Box's Managing Director, Michael Gazeley, talks about security issues facing **The Internet of Things**. The IoT (Internet of Things) has made everything significantly more complicated than before. All of a sudden, your photocopier, televisions, printers, projectors, phone system, refrigerators, microwaves, and even lighting systems, are becoming computers too. Without adequate cyber protection, all these devices are vulnerable to hackers and cyber criminals. On pages 2 to 3 we discuss this in further detail, and highlight the dangers for IoT.

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

In other news, Network Box Hong Kong was at the launching ceremony of the Office of the Government Chief Information Officer's (OGCIO) Pilot Partnership Programme, **Cybersec Infohub**. In addition, Network Box was featured in several media outlets including the **South China Morning Post** and **Security Insider**. Finally, Network Box held a cyber security seminar titled "**10 Cyber Security Facts (that you need to know)**."



Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2018

Stay Connected

You can contact us here at Network Box 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:



<https://twitter.com/networkbox>



<https://www.facebook.com/networkbox>
<https://www.facebook.com/networkboxresponse>



<https://www.linkedin.com/company/network-box-corporation-limited/>



<https://plus.google.com/u/0/107446804085109324633>

In this month's issue:

Page 2 to 3

The Internet of Things

It is estimated that as of right now, there are already 3 internet connected devices, for each man, woman, and child on planet Earth. However, most of these 'smart' devices are not protected from cyber attacks and many have default user names and passwords which cannot even be changed. In our feature article, we discuss the security issues and challenges facing IoT.

Page 4

Network Box 5 Features

The features and fixes to be released in this month's patch Tuesday for Network Box 5.

Page 5

Network Box Highlights:

- **Network Box Hong Kong**
Cybersec Infohub Launching Ceremony
- **Network Box Cyber Security Seminar**
10 Cyber Security Facts (that you need to know)
- **Network Box Media Coverage:**
 - South China Morning Post
 - Security Insider



The Internet of Things

Your smart devices may be your biggest security threat

by Michael Gazeley
Managing Director, Network Box

How many doors, or windows, need to be left open, for a criminal to be able to get into your office?

Not a trick question; the answer is obviously just one.

Exactly the same is true in the cyber realm.

Every single connection from your office network to the Internet, is a potential channel for hackers, viruses, and worms, to enter your theoretically private workplace; and from the moment your office network is compromised, your commercial secrets, bank account details, upcoming product designs, indeed anything and everything you store in digital form, may also be compromised.

To make things significantly worse; the explosion in smart device usage, has seen a corresponding explosion in cyber risk.



It is estimated that as of right now, there are already 3 internet connected devices, for each man, woman, and child on planet Earth. Each of these is essentially a computer, but with the advent of the IoT (Internet of Things), or 'physical Internet,' typically not a computer which the average end user knows how to interact with in the same vein as a Windows PC, or an Apple laptop.

Most people know that computers, networks, and private data, are vulnerable to hackers. Cyber-security issues, have made for far too many frightening news headlines over the last few years, not to have made a significant impression on almost every person in the developed world.

Home Depot (50 Million Credit Cards), Sony PlayStation Network (77 Million Users), Anthem Health Care (78 Million Users), JPMorgan Chase (83 Million Accounts) and Target Stores (110 Million Accounts) are just a few examples of well-known hack attacks.

The last example, Target Stores, is of particular note.

The electronics retailer was one of the first major firms to lose its Chairman, President, and CEO, Gregg Steinhafel, over a cyber-security breach. Access to its POS (Point of Sale) systems, was gained through a third-party HVAC (Heating, Ventilation, and Air Conditioning) vender, allowing hackers to collect data from over 40 million credit cards. The firm's CIO Beth Jacob also resigned.



So, while the Internet is an amazing vector for business, research, and entertainment; unfortunately, it also acts as a conduit for hackers, malware, and undesirable content, all of which can reach you and your devices, twenty-four hours a day. The results can obviously be disastrous.

The IoT (Internet of Things) has made everything significantly more complicated than before. Up until quite recently, a computer looked like a computer. Sure, there were desktops, laptops, and servers, but in general, no one was in much doubt about what a 'computer' looked like.

All of a sudden, your photocopier is a computer, your televisions are computers, your printers are computers, your projectors are computers, your phone system is a computer, your refrigerator, microwave, and even your lighting system, are also becoming computers. Perhaps most disturbing of all, your physical security systems, including your burglar alarm, CCTV cameras, CCTV recorders, and even panic buttons, have all most probably become computers too.



Not all of these IoT devices are easy to secure. Many have default user names and passwords which cannot even be changed; typically, 'admin' and '1234.'

More than ever, it is critical to install and enable serious gateway cyber-security, which is updated in real-time, and which is monitored around the clock, to see if anything on your network is trying to 'phone home,' in the middle of the night.

We now live in a terrifying new world, where the physical security systems you installed to monitor criminals, could easily be used by those very criminals, to monitor you. And the alarm system which you are depending on to save your life, maybe rendered useless by little more than a mobile phone.

Network Box

5

.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd October 2018, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features October 2018

This month, for Network Box 5, these include:

- Suppression of VPN section in KPI report when VPN modules are installed, but not enabled
- Performance improvements in logging of network utilisation summaries
- Introduce support for granular filtering of event logs
- Provide an optional self-check of proxy services
- Improvements to SMTP proxy STARTTLS support
- Support optional bypass of mail scanning for specified content
- Improvements to websocket support and logging
- Enhanced support for Quality of Service (QoS) classification at the proxy level
- General enhancements for NOC engineering 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.

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 Hong Kong Cybersec Infohub



Network Box Hong Kong took part in the Office of the Government Chief Information Officer's (OGCIO) Pilot Partnership Programme, for Cyber Security Information Sharing. This program, **Cybersec Infohub**, aims to enhance the exchange of cyber security information with industry and enterprises, to jointly defend against cyber attacks.

The Cybersec Infohub launching ceremony, which took place at the Hong Kong Productivity Council, was opened by *Mr. Victor Lam, JP*, the Hong Kong Government's Chief Information Officer.



Network Box Cyber Security Seminar 10 Cyber Security Facts (that you need to know)

Network Box held a seminar titled, "**10 Cybersecurity Facts (that you need to know)**", covering the current cyberthreat landscape, and other issues such as Backdoors, Security for IoT, Phishing & Ransomware, Advanced Persistent Threats, and many more.



Network Box Media Coverage



South China Morning Post

South China Morning Post
Michael Gazeley, Network Box's Managing Director, was interviewed for an article in the SCMP, titled, "How you can protect your smart devices from cyberattack."

Link: <https://bit.ly/2zCDwy7>



Security Insider

Security Insider
Network Box Germany's Managing Director, Dariush Ansari, was interviewed for an article titled, "Cybersecurity for SMEs: MSSP as a solution to skill shortages."

Link: <https://bit.ly/2NPJnc3>

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
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