In the Boxing Ring
APR 2019

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the April 2019 edition of In the **Boxing Ring**

This month, we will be talking about Network Box's **Cybersecurity Ethos**. The Network Box approach to cybersecurity has always been different. Since the company's launch 20 years ago, we have always deployed full sets of signatures covering both modern and ancient malware and threats, and used multiple overlapping protection engines, to increase both the depth and breadth of protection capability. Currently we are using 79 classification and policy enforcement engines, utilizing more than 63 million signatures. On pages 2 to 3 we talk about why this is necessary in today's heightened security landscape, and discuss the Network Box approach.

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 Taiwan participated at **Cybersec 2019**. During the event, Network Box Singapore's Jan Van Leersum, gave a keynote presentation on the *Dark Web*. In addition, Network Box Hong Kong was invited by **The Law Society of Hong Kong** to give a talk at their *Cybersecurity for SME* Event. Finally, Network Box Germany held a partner event to brief them on the latest Network Box offerings and technologies.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2019

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://www.youtube.com/user/NetworkBox

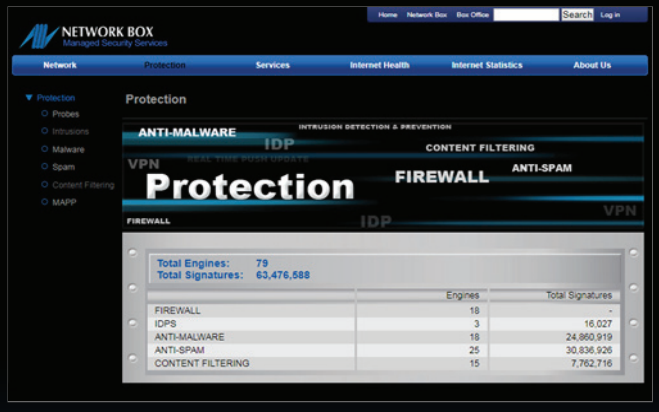
In this month's issue:

Network Box Cyber Security Ethos

The Network Box approach has always been different. Since our launch 20 years ago, we have always deployed industry leading scanning engines, with the full capabilities of their desktop / server brethren. We have always deployed full sets of signatures covering both modern and ancient malware and threats. And we have always used multiple overlapping protection engines, to increase both the depth and breadth of protection capability.

79 Engines
63 million Signatures

Network Box UTM+ devices today contain 79 classification and policy enforcement engines, utilizing more than 63 million signatures. These numbers grow every day and are expected to pass 64 million signatures within the next few months. Given that those numbers are many multiples higher than most of our competitors', we can see that this approach is different, but why is it necessary?



■ *http://response.network-box.com/protection*

The origin of the cursory scan

Back in the early days of UTM+, it was commonplace for devices to use just a few thousand signatures to scan traffic for recent threats. The CPUs were just not powerful enough to do full anti-malware scanning even for one PC, let alone at the gateway protecting hundreds/thousands of devices. Some vendors tried to do the scanning in custom silicon hardware, which offered improved performance, but at the expense of the number of signatures that could be supported (aka loaded into RAM).

OEM partners introduced scanning engines with fancy marketing names, but all were limited cut-down versions of their full desktop/server scanning products, intended to be used in low-end gateway devices performing just a 'cursory scan' of the data streams.

Even nowadays, this limited technology persists. Take the lids off most gateway perimeter protection devices and you will see low-end/embedded CPUs with just 1GB or 2GB of RAM and small solid-state disks.

The Network Box Approach

Our approach is to firstly thoroughly unpack the network stream, and objects to be scanned, to their basest form (we currently support more than 700 encoding and unpacking formats). Once we've got the unpacked objects, we'll scan them with multiple engines, utilizing tens of millions of signatures, to obtain the most accurate classification result. Policy is then applied to that result (whether to permit/deny the traffic).

Over the past two decades, this approach has been proven time and again to be the correct one. We have the highest customer retention rates in the industry simply because of the quality of our protection.

How do we do this, when the competition can't? The answer is to think inside the box. All Network Box appliances (real/virtual, small/large) run exactly the same full suite of protection firmware. Even the lowest end small branch office VPN appliance has a multi-core 64bit Intel processor with 4GB of RAM, and most of our appliances have 8GB or more. Hardware is just a small portion of the total long-term ownership cost, and it is our approach to use the best. The cost of cleaning up a ransomware outbreak, by comparison, is often much greater.

The 80/20 rule

Back when we started Network Box, the CSI/FBI conducted annual Internet Cyber Crime surveys, and produced annual reports (they still continue this practice today). Every year, those reports highlight two simple facts:

1. **80% of cyber security problems are because protection was not in place.**
2. **The remaining 20% of problems are because the protection was not maintained or installed properly.**

Network Box addresses this first 80% by including the most effective threat protection technology covering everything from basic firewall, though Intrusion Protection, up to Anti-Malware, Anti-Spam, and beyond; in every single Network Box appliance. Sometimes we work alongside other equipment, and other times we supplement with additional protection, but we always recommend deployment of protection in both depth and breadth.

We address the last 20% with our Managed Security Services. By employing our own dedicated security professionals providing local support in Security Operation Centres around the world, we ensure that each and every Network Box appliance is configured and maintained to the highest standards.

That is the Network Box approach.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd April 2019, 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
April 2019

This month, for Network Box 5, these include:

- Additional support for prioritisation of scanning services
- Improvements in handling of scanning jobs cancelled while in flight
- Enhanced support for SYSLOG inputs to NBSIEM+
- Support for RPC_IN_DATA and RPC_OUT_DATA methods in Web Application Firewall proxying
- Performance improvements to Admin Portal display of entity lists
- Improved validation of SSL VPN configurations
- Enhanced support for NOC 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 HIGHLIGHTS

Network Box Taiwan
CYBERSEC2019

Network Box Taiwan exhibited at **Cybersec 2019**, held at the Taipei World Trade Center. During the event, Network Box Singapore's Managing Director, Jan van Leersum, gave a keynote presentation on the dangers of the **Dark Web** and introduced Network Box's new Dark Web Monitoring Service.

Network Box Hong Kong
The Law Society of Hong Kong

Network Box Hong Kong was invited by **The Law Society of Hong Kong** to talk at their, 'Cybersecurity for SME Firms' event. The law firms present were briefed on Managed Cybersecurity in general, but focused on the threats posed by the Dark Web, and how firms can protect themselves, by leveraging Network Box's new **Dark Web Monitoring Service**.

Network Box Germany
Partner Event

Network Box Germany held their first partner event, held at Kochfabrik Köln, to brief them about the latest Network Box offerings and technologies.

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