NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring JULY 2022

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the July 2022 edition of In the **Boxing Ring**

This month, Network Box USA's CTO, Pierluigi Stella, is discussing **AI and Cybersecurity**. Something we keep hearing of late is what cybersecurity is set to look like and how AI/Machine Learning will play a bigger role against ransomware and breaches. Imagine a system that "learns" and adapts its behavior based on what transpired in the past? While this may sound great in theory, we are still in the early stages of its development and is limited in its capabilities. Pierluigi highlights its limitations in our featured article and outlines approaches we can use today.

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

In other news, Network Box is pleased to announce our latest revision to the **M-295i** hardware unit for medium-sized companies. And in this month's Network Box customer testimonial, *Priscilla Chu*, VP of Operations of **YesAsia Holdings Limited**, shares her experience of partnering with Network Box.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
July 2022

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

AI AND CYBERSECURITY

by Pierluigi Stella
Chief Technology Officer
Network Box USA

Something I keep hearing of late is what cybersecurity is set to look like and how AI will play a bigger role against ransomware and breaches.

Firstly, it isn't AI if it doesn't have the element of prediction. And here, we're not predicting anything. To be honest, we're only inferring (at best). Inferring possible behaviors. As such, let's call AI for what it is, and that's Machine Learning (ML). And yet, the industry keeps trying to use AI because it sounds much more impressive. **IT'S INTELLIGENT.**

Well, Machine Learning is just as impressive, is it not? A machine that "learns" and adapts its behavior based on what transpired in the past? Tell me that's not mind-blowing?

Aside from this critical clarification, we must also consider that hackers aren't just sitting around idly. They, too, have access to "AI" tools. So, while we may think the new and ultimate tool is coming, our adversaries are likely already using those same precise tools. Innovation happens on both sides. Our enemies have access to the same resources. Most software tools are open source and available to everyone, for better or for worse. And those who have nefarious intentions are very skilled, very smart individuals too.

This initial consideration aside, we appear to be placing far too much reliance on something that, in all likelihood, will not deliver as we hope.

I have tested AI-based Anti-Virus for an entire year

I used it to test every email our filters were scanning in parallel with our filters. And in that one year, the AI-based Anti-Virus (AV) captured a grand total of four emails. I repeat, 4!!! Considering that we scan millions of emails daily, that number is beyond minuscule. Our "traditional" scanners, comprised of over 70 engines (each tailored to specific issues), captured hundreds of thousands of emails. Why? Because threats don't come inside emails as attachments. No hacker would send you a virus attached to an email because that's far too easy to catch. Block executable code altogether, and you're blocking every threat even if you don't know what threat that is, which ultimately doesn't even matter. A threat is a threat that needs to be stopped, regardless of its name.

For the most part, hackers send you links. They send you phishing emails. Spoofed emails. They send you something that aims to trick your users into clicking and downloading the threat code.

So, is that email a threat per se even though it does not contain executable code? **YES, IT IS.**

Because sadly, users will be users, and some will just keep clicking on things they're not supposed to because they can't help themselves. Instead of a "think before you click" mentality, they click first and think later. And that's when the real threat starts. When the clicked link goes out to grab that code, it will now infect your entire network.

How do you protect from all this? No need for fancy AI.

Scan HTTPS and ensure things are properly blocked in the web filtering. That's where you need to apply the real and best protection nowadays because once the user clicks (and you know someone will), you may still have a chance at blocking the threat. BUT only if you're properly filtering and scanning HTTPS.

Before closing, a final word about endpoint AV.

Traditional AV is practically useless

With more than 1,250 new threats per minute, a signature-based AV will never be able to keep up, and here's where pundits advocate using AI/ML. I don't necessarily disagree with this approach, but I believe it's insufficient. I mean, we're still in the realm of trust but verify. And we know that on its own is also no longer sufficient. Zero-Trust tells us that we need to "assume breach." That it's bad news from the get-go.

On that note, a better approach is to readapt the concept of whitelisting. The idea is that nothing is allowed to run on your computer unless it has been "trusted." And use certificates to identify legitimate software, checking everything that tries to run on your computer. Practically questioning everything and only allowing what's been whitelisted to run. **AND NOTHING ELSE.** You can try to install ransomware as much as you want. It just won't be allowed to run. So, even IF you get breached and download ransomware, it won't cause any problems because it will not be able/allowed to run.

I find this a much better approach than an ML tool since the latter may or may not recognize a threat. We're putting too much faith into a new technology still in its infancy and definitely not ready for the great things we tag it as capable of doing.

AI/ML will likely be great. Some day.

But, by that point, hackers will also have a similar tool, so the battle continues. **Wouldn't you agree?**

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th July 2022, 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

July 2022

This quarter, for Network Box 5, these include:

- Support for new 2022 UTM 5Q box model
- Support for new 2022 VPN 5Q box model
- Support for new 2022 S-80i box model
- Support for new M-295i box model
- Improvements to SYSINFO GMS sensor, to better report disk mounting issues
- Introduce support for GMS Incidents in job control service
- Support incidents in FRONTLINE GMS sensor
- Support incidents in INFECTEDLAN GMS sensor
- Change admin portal network utilisation chart to show INTERNET interfaces by default
- Address CVE-2020-1763 in IPSeC (Malicious IKEv1 packet may cause service restart)
- Introduce base support for configuration maintenance via NBSIEM+
- Change to High Availability group IDs, to limit to 8 characters
- Update public IP address ranges for regional SOCs and Security Response systems
- Address a bug where, under certain rare circumstances, a configuration change would not immediately be visible to services
- Deprecate HTTP for Admin and User portals, by default

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 M-295i
Hardware Upgrade

Network Box is pleased to announce our latest revision to the M-295i hardware unit. The unit is designed to offer near Enterprise RAM and HDD capacity and CPU performance for medium-sized companies.

Features	Details
Processor	64bit, 3.6GHz, 4 physical cores
RAM	1 x 8GB, 2666MHz DDR4
Storage	1 x 1TB 3.5 HDD
Networking	6 x 1GB RJ45
Power Supply	250w
Chassis	1u rackmount – ¾ depth
I/O Interface	1x reset button 1x RJ45 console 2x USB 3.0
Physical Dimensions	438 mm(w) x 422 mm(d) x 44 mm(h)
Weight	9.0kg

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

Network Box Customer Testimonial:
YesAsia.com

LINK: https://mcdn.network-box.com/CS/YesAsia_Testimonial.pdf

"It has been many years since we started cooperation, and we are very pleased with Network Box's cyber security solutions, especially the 24/7 support,"

Priscilla Chu
VP of Operations
YesAsia Holdings Limited

Global Security Healines

TechCrunch

Cloudflare outage hit crypto exchanges FTX, Bitfinex and more

LINK: https://tcrn.ch/3OGBGR3

The Hacker News

Google Blocks Dozens of Malicious Domains Operated by Hack-for-Hire Groups

LINK: https://bit.ly/3OZIXLh

ZDNet

A tiny botnet launched the largest DDoS attack on record

LINK: https://zd.net/3nBBnuP