NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring AUG 2023

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the August 2023 edition of In the **Boxing Ring**

This month, we are talking about **Artificial Intelligence and Machine Learning** (AI/ML). In recent years we have seen the gradual introduction of AI/ML technologies into our everyday lives. These new technologies are no longer 'programmed' procedurally. Instead, they are 'taught' or 'trained' in what is expected and respond with 'how' to do it, decided by the machine model itself. As with all such tools, the technology has both good and bad sides. On pages 2 to 3, we will talk about the positives of AI/ML by providing three examples of how it is being used for computer security.

In other news, Network Box Hong Kong was at the **Business GoVirtual Expo & Conference**, which took place at the HK Convention and Exhibition Centre. Additionally, Network Box Germany's Dariush Ansari was interviewed by **it-daily.net** to talk about the benefits of security awareness and how success can be measured. Furthermore, in this month's global security headlines, there were security issues with Microsoft, Apple, Cisco, and Fortinet. Finally, the latest episode of **HPCC Hackpod** is now available.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2023

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

Artificial Intelligence and Machine Learning

In recent years we have seen the gradual introduction of Artificial Intelligence and Machine Learning (AI/ML) technologies into our everyday lives. From talking to our Siri/Alexa/Google Home devices, to automated chat response systems, computer vision, and self-driving cars - these new systems are no longer 'programmed' procedurally. Instead, they are 'taught' or 'trained' in what is expected and respond with 'how' to do it, decided by the machine model itself.

We've grown accustomed to the predictability of computerized systems - given the same input, the same outputs will be derived time and time again. 2+2 will always equal 4. But these new AI/ML systems behave much more randomly - providing the ability to adapt to changing inputs - sometimes impressing with their comprehension of what we are asking, but also dramatically failing in bizarre ways.

As with all such tools, the technology has both good and bad sides. In this month's article, we'll talk about the positives of AI/ML by providing three examples of how it is being used today for Computer Security.

1. Access Denied Security Events Analysis

For decades, we've been using Heuristics to analyze access denied security events. An example would be setting a threshold for network port access denies per minute and alerting/blocking should that threshold be exceeded. The classic 'Portscan' deny.

The problem with this approach is twofold:

1. The threshold must be manually set and tuned depending on the individual network configuration
2. Slow scans (where the attacker deliberately scans very slowly) are not detected.

These types of heuristics are classic examples of procedural programming - **if this, then that.**

AI/ML models provide an alternative approach. Here, we train the model with examples of normal access denied traffic and targeted attack traffic. We teach the model by example and have it set the thresholds automatically based on that training. Like a child, the computer learns - we don't tell it how to detect a targeted attack, but merely train it to what such an attack might look like. After training, we can then feed a stream of real network events into the model, and it can tell us if it sees anything that looks like an attack worth responding to (so that we can alter/block/respond appropriately).

This approach can be used not just for port scan detection but also for more general high-level access denies such as application logins, detecting brute force, or user enumeration type attacks.

2. General Behaviour Analysis

While heuristics have worked well for access denied security events, they haven't been generally useful for network behavior analysis. The idea here is to set thresholds and criteria for what normal network traffic might look like, so we can alert on anything abnormal. There has been some success here with protocol enforcement (such as defining what particular packet types for a specific protocol might reasonably look like), but such a whitelisting approach is laborious and must be customized for each and every protocol and application.

AI/ML holds great promise for this. Rather than procedurally programming the behavior and thresholds for each and every protocol, we merely train the model with known good behavior and have it alert on anything different.

3. Meta Analysis

While general behavior analysis looks at protocols and applications, meta analysis looks at network traffic attributes (such as the source and destination IP addresses, authenticated users, countries, networks, times of day, etc.). Here, AI/ML can be trained with normal network traffic and alert on anything different. An example of this would be network logins on a Sunday from users who typically work Monday to Friday.

> **Despite the meteoric rise of ChatGPT, AI/ML is still in its infancy, particularly with respect to its use in computer security. Computers have historically been most useful in situations with clearly defined inputs, outputs, and procedural processes - and have struggled with more vague problems such as pattern matching. AI/ML is more 'fuzzy' and the requirements less well defined - the main issue being false positives. AI/ML often impresses with its accuracy but equally often fails dramatically for no discernable reason.**
>
> ***Network Box Security Response continues to work deploying AI/ML models at the moment, primarily to our NBSIEM+ Event Analysis and Incident Response systems. Over the coming months and years, we expect this tool to become more useful for this and start to be deployed to perimeter gateway protection and endpoints.***

Network Box HIGHLIGHTS

Network Box Hong Kong Business GoVirtual Expo & Conference

Network Box Hong Kong was at the **Business GoVirtual Expo & Conference**, which took place at the HK Convention and Exhibition Centre. During the three-day expo, visitors were introduced to Network Box's award-winning security technologies and managed services. Additionally, Network Box Managing Director, Michael Gazeley, gave a talk titled: ***The Vulnerability of Everything.***

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

Media Coverage and Security Headlines

it-daily.net

The success of security awareness training is measurable
LINK: https://bit.ly/43KB4jT

HPCC Hackpod Club

Episode #20:
Cybersecurity as a lateral entry
LINK: https://anchor.fm/hackpodclub

GB Hackers

Microsoft Message Queuing Service Flaw Allows DoS and RCE Attacks
LINK: https://bit.ly/3KkoXDb

Bleeping Computer

Lazarus hackers hijack Microsoft IIS servers to spread malware
LINK: https://bit.ly/3YcZMYW

Dark Reading

Actively Exploited Apple Zero-Day Affects iPhone Kernel
LINK: https://bit.ly/3OfusED

Security Week

Vulnerability in Cisco enterprise switches allows attackers to modify encrypted traffic
LINK: https://bit.ly/43NsT6o

Bleeping Computer

300,000+ Fortinet firewalls vulnerable to critical FortiOS RCE bug
LINK: https://bit.ly/3Kk60kj