In the Boxing Ring
DEC 2022

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

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

This month, in part one of an ongoing series, we discuss **The Whitelisting Approach** to cybersecurity. Two very different and fundamentally mutually exclusive approaches to security exist: blacklisting and whitelisting. In our featured article, we summarize the differences between the two, and how whitelisting is a practical alternative to the traditional blacklist-based approach, as well as being a viable option for cybersecurity and company policy enforcement.

In other news, Network Box Germany was featured in funkschau to discuss a form of malware. Additionally, security issues were encountered some US Bank, certain Android App available in the Google Playstore, Rackspace, Medibank and Google Chrome. In this month's Network Box customer testimonial, Autotoll Limited's CIO shares his experiences. And finally, the latest episode of HPCC Hackpod Club is now available.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 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

In this month's issue:

The WHITELISTING Approach

[part 1 of 2]

There exist two very different and fundamentally mutually exclusive approaches to security:

1. **Blacklisting:** involves specifically blocking what you know to be unwanted and allowing everything else through.
2. **Whitelisting:** involves blocking everything by default and only allowing things you specifically want through.

At the Internet perimeter, we are well accustomed to using the whitelisting approach. Most, if not all, firewall inbound (NET->LAN) policies nowadays block all network ports and only open those ports specifically required for specific permitted services.

But outbound (LAN->NET) at the Internet perimeter, we see more of a mix of approaches. We recommend using the whitelisting approach - block all outbound, and permit only what is explicitly required. But, we still see many customer policies allowing everything outbound, except for a few ports specifically blacklisted.

For inbound email, Network Box has always offered comprehensive policy control and recommended a whitelisting approach - quarantine executables, scripts, etc. (by default), and allow only for specific trusted senders. Most of our customers follow this recommendation with the policies they ask us to implement.

Until recently, using the whitelisting approach on end-points (workstations and servers) has been problematic. By this, we mean blocking any application from executing, except those applications specifically whitelisted. The hundreds of thousands of applications available, each with dozens of interrelated components, combined with frequent updates, often resulted in excessive administrative workload and end-user impact in managing the whitelists. But now, with widespread deployment of code signing on both Microsoft and Apple platforms, combined with more powerful trust rule systems, this is becoming feasible. And it is a practical alternative to traditional blacklist-based approaches such as host-based anti-virus and intrusion prevention systems.

Modern host-based whitelisting systems are flexible (cloud-based, with powerful rules supporting application signatures, digital signing certificates, as well as metadata such as file paths, parent application, etc.) and easy to deploy with inherited trust mechanisms. They finally offer a viable alternative to traditional host-based anti-virus systems. They also go beyond merely stopping the latest ransomware attack, to cataloging and reporting on applications actually running on the hosts in your network - providing for effective per-host and per-user policy control. They are still more complex to maintain than traditional anti-virus systems, but combined with a managed service, are finally becoming something truly useful and perhaps the ultimate solution to secure end-point devices.

Network Box HIGHLIGHTS

Network Box Customer Testimonial: Autotoll Limited

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

"Often, our staff receive phishing emails, business email scams, and malware. Network Box provides timely professional blocking of these to reduce company loss and business impact."

Karel Au
Chief Information Officer
Autotoll Limited

Digitalization is the fundamental pillar of building a smart, competitive, and sustainable city. As the pioneer of smart solutions to support the HK Government's "Smart City Blueprint" Autotoll is committed to developing various intelligent solutions to create a smart city.
www.autotoll.com.hk

Autotoll

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

HPCC Hackpod Club
Episode #16:
Is Cyberpolicy simply priceless?
LINK: https://anchor.fm/hackpodclub

funkschau
Phishing via QR codes
LINK: https://bit.ly/3h2Pyti

CNN
US banks report more than $1 billion in potential ransomware payments
LINK: https://cnn.it/3EUQlEg

Bleeping Computer
Android malware apps with 2 million installs spotted on Google Play
LINK: https://bit.ly/3VMhrEA

The Register
Rackspace rocked by 'security incident' that has taken out hosted Exchange services
LINK: https://bbc.in/3CsdBty

The Hacker News
Hackers leak another set of Medibank customer data on the Dark Web
LINK: https://bit.ly/3FqJYdp

Bleeping Computer
Google Chrome emergency update fixes 9th zero-day of the year
LINK: https://bit.ly/3OYmdwD