In the Boxing Ring
FEB 2023

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

This month, we are continuing our talk about **The Whitelisting Approach**. Last December, we introduced the concept of a whitelisting approach to security, the highly secure approach of defining only what is allowed and blocking everything else. At the core of a whitelisting product is the endpoint engine. This obtains signatures of objects being executed, compares them to the database of signatures listing what is permitted (aka 'the whitelist'), then enforces and produces audit logs. On pages 2 to 3, we discuss this in further detail and introduce our new specific whitelisting product and outline how it can improve security and policy control of workstations and servers.

In other news, Network Box USA's CTO, Pierluigi Stella, was a guest panelist in a Cyber Executive Roundtable at the Houston Cybersecurity Conference, which took place at The Westin Galleria Houston. Additionally, Network Box Hong Kong was at the Hong Kong Science Park to participate in an IT development conference titled, "Hong Kong Innovation And Technology Development Blueprint Pathway." And in this month's Global Security Headlines, security issues were encountered in Windows, Google Ads, Mailchimp, T-Mobile, PayPal, Microsoft Cloud, and Fortinet devices.

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

In this month's issue:

The WHITELISTING Approach [part 2]

Last December, in part one of this article, we introduced the concept of a whitelisting approach to security, the highly secure approach of specifically defining only what is allowed and blocking everything else. This month we conclude by introducing a specific whitelisting product and showing how it can improve security and policy control of workstations and servers.

Whitelisting Signatures

At the core of a whitelisting product is the endpoint engine. This obtains signatures of objects being executed, compares them to the database of signatures listing what is permitted (aka 'the whitelist'), then enforces and produces audit logs. But what is a signature?

Most commonly, one-way hash functions have been used. These are a form of one-way encryption, taking a large object, then applying a mathematical algorithm to reduce it to a much smaller 'hash' value. For example, the MD5 hashing algorithm takes any arbitrarily large object and produces a hash of just 128 bits. You cannot take a hash and reconstruct the original object (hence the term 'one way'), but you can simply compare the hashes of two objects and, if identical, deduce that the objects are the same. The hash collision rate (where two objects produce the same hash value) must be incredibly low for this to work. For security purposes, it should also be extremely hard to force a collision (by adjusting an object to make it produce a known hash).

The whitelisting approach is thus to take fingerprints of all permitted objects and store them in a list. Then, whenever an object is to be executed, we can compare its hash against our whitelist and permit/deny it as appropriate. Such an approach is very secure but has one critical vulnerability - if the attacker can adjust his malicious code to have the same hash value as a whitelisted (presumably common) application, then it will be permitted to be executed. While computationally hard to do, this is not impossible, and in recent years more and more hashing algorithms have fallen vulnerable to such approaches.

> The approach Network Box has chosen is to take multiple fingerprints, using a selection of five of the most secure hashing algorithms, to produce a 'handprint' for each executable object. The chances of one of these algorithms being compromised are small, but the complexity of all five being compromised is so infinitesimally tiny as to be practically impossible.

Note that signature technology can typically be applied to the objects or the certificates used to sign those objects (in the modern world of code signing certificates) - to minimize issues with installing application updates. But bear in mind the additional risks of trusting a particular developer entirely).

How to Deploy Whitelisting?

So how to deploy whitelisting on a workstation/server? There are three common approaches:

1) Learning Mode

With this approach, all the existing executables on the machine are pre-indexed and trusted, and the machine placed in learning mode will automatically trust new executables run during the learning period. The advantage here is simplicity - the whitelist is built automatically and is pretty complete. The disadvantage is obvious - not all pre-existing executables on the machine may be desirable (either from the point of view of policy control or simply because they may be malware).

2) Monitor Mode

Here we monitor all executables run on the machine over time, but instead of blocking, we merely alert and have an administrator review, categorize, and decide to permit/deny in the whitelisting policy. The advantage here is that the resulting whitelisting policy is very complete, but it does require administrative effort.

3) Pre-Trusted

The pre-trusted approach builds upon pre-existing lists of known common popular applications to be permitted by default, with everything else denied. The advantage is that it is quick and simple to implement, but the disadvantage is that anything custom or unusual would not typically be trusted by default.

Which is the best approach? In Network Box's view, the Learning Mode is simply not a good solution as it runs the risk of permitting malware into the organization during the learning period. Depending on the situation, we typically recommend a combination of Monitor Mode and Pre-Trusted. This balances the benefits of minimizing the deployment period while maximizing security.

Is Whitelisting for Everyone?

The whitelisting approach is not a universal solution suitable for everyone. Like most things involving IT security, there is a trade-off of security vs. convenience, and the whitelisting / blacklisting approach seems to exemplify that.

IT Administrators are very familiar with traditional blacklisting anti-malware systems. They deploy them onto the network, and within minutes, pre-existing malware is identified and ongoing protection provided. However, such systems are proving to be increasingly hard to maintain their effectiveness. The explosion in the sheer volume of malware, and the increase in ransomware attacks for commercial gain, have seen more and more malware get through to infect systems. It doesn't matter how good an anti-malware blacklisting system is and how much malware it blocks; it only has to let one single thing through to result in a nightmare.

Whitelisting provides an alternative to this, which is probably as close to 100% secure as can be realistically achieved. Whatever the malware authors come up with is blocked by default, but that comes with the downside that whatever new applications or updates you require on your network will also be blocked by default. Whitelisting introduces an authorization step into the flow of application installation/update, which can be good or bad, depending on your viewpoint.

That said, one very positive side-effect of deploying whitelisting is the increased visibility of what applications are being run on your workstations/servers and by whom; that comes from the audit logging and policy control. Whitelisting can be used to block not just unwanted malware but also non-core applications from your network.

The Network Box Whitelisting Solution

Network Box has partnered with Whitecloud Security to bring managed zero-trust endpoint security to our customers. With the mature and well-established Whitecloud Security endpoint, using unique five signature handprint technology, and combined with trust architecture and Network Box Managed Security Services taking on the administrative overhead, the solution will start to be offered towards the end of 2023Q1.

The approach involves a small zero-trust endpoint agent installed on Windows servers/workstations, connecting to a cloud-based service for management and control. The usual deployment approach is:

1) Identified suitable endpoints to be protected. This can be all endpoints or only those at high risk (such as accounts/finance workstations, laptops leaving the office, servers, etc). These endpoints are grouped so that policies can be applied to the group (whitelisting an application on one workstation automatically whitelists it on all others in the group) or for specific workstations.
2) Deploy zero-trust endpoint protection in Monitor mode. During the monitoring period, Network Box SOC engineers will adjust trust policies as necessary and alert as to any malicious activity detected.
3) After a suitable monitoring period (usually one to two weeks), enable enforcing of the policy.
4) Network Box SOC engineers provide ongoing monitoring and support to enforce the whitelisting policy.
5) Customer Administrative staff have complete visibility and control over the above process, working alongside Network Box SOC engineers.

This technology also brings with it an interesting solution to pre-existing infected machines (ransomware, etc). In such cases, the endpoint agent can be installed on the infected machine in Pre-Trusted mode (only trusting base Microsoft and other common applications), and the machine then brought safely back online for investigation and recovery (safe in the knowledge that nothing untrusted will be permitted to run).

With a simple per-device per-month cloud-based pricing model, bringing zero trust endpoint protection to the Network Box customer base provides us exciting opportunities to help customers with their high-risk endpoints, serviced from our existing Managed Security Services frameworks.

Network Box HIGHLIGHTS

Network Box USA
Houston Cybersecurity Conference

Network Box USA's CTO, Pierluigi Stella, was a guest panelist in a Cyber Executive Roundtable at the Houston Cybersecurity Conference, which took place at The Westin Galleria Houston. During the event, attendees gained insights on vital security topics ranging from cloud security to protecting their organizations from advanced threat actors.

Network Box HK
IT Development Conference

Network Box Hong Kong was at the Hong Kong Science Park to participate in an IT development conference titled, *"Hong Kong Innovation And Technology Development Blueprint Pathway."*

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

Global Security Headlines

Bleeping Computer
Hackers abuse Windows error reporting tool to deploy malware
LINK: https://bit.ly/3JIFvW5

Info Security
Hackers Leverage Compromised Fortinet Devices to Distribute Ransomware
LINK: https://bit.ly/3YsAa9q

Bleeping Computer
Hackers push malware via Google search ads for VLC, 7-Zip, CCleaner
LINK: https://bit.ly/3DDA8Un

TechCrunch
Mailchimp says it was hacked — again
LINK: https://tcrn.ch/3wWdQt1

CNN
37 million T-Mobile customers were hacked
LINK: https://cnn.it/3x4fuc5

Bleeping Computer
PayPal accounts breached in large-scale credential stuffing attack
LINK: https://bit.ly/3HZE6sT

Reuters
Microsoft cloud outage hits users around the world
LINK: https://reut.rs/3I1yOgM