FEB 2018

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the February 2018 edition of In the Boxing Ring

This month, we will be talking about the Network Box **Reputation Database** (or RepDB for short). RepDB is a big scale database where we store categorization and classification of threat, and productivity information. This is stored in the cloud and is regularly updated and managed by Network Box Security Response. Currently, we track more than 14 million reputation signatures, covering more than 100 million individual items. RepDB is currently growing at the rate of more than 200,000 signatures a month. On pages 2 to 3 we explain RepDB on more detail, and how we use it to protect our customers, and work with our security partners.

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

Finally, Network Box Hong Kong welcomed **Guardforce** for a seminar on the security threat landscape, and a sneak preview of new features for the Network Box 5.5 platform. In addition, Network Box Germany's Dariush Ansari was interviewed by **NetzPalaver** to share his thoughts on the technology trends that will affect businesses in 2018. Furthermore, Network Box's **Year in *Focus* 2017** is now available, and can be downloaded using the link on page 5.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2018

You can contact us here at 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:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

Reputation Database

The Reputation Database (or RepDB for short) is a big data scale database maintained by Network Box Security Response; it forms the core repository of information we store on categorization and classification of threat and productivity information. Given it's importance, we will now explain RepDB in more detail, and show how Network Box uses it to protect our customers, and work with partners.

RepDB is made up of a few related components:

Item Types

RepDB stores items of information of different types such as email addresses, IP addresses, telephone numbers, URLs, hashes and fingerprints. Overall, it stores data for more than a dozen different types.

Reputations

Each item entered into the database, with corresponding type, has an associated reputation. This stores information such as the category (politics, proxies & translators, real estate, virus/malware infected, spam, etc), the classification (spam, malware, executable, etc), as well as the percentage confidence in that classification. Most importantly, multiple sources can provide categorization, classifications and confidences for the same item of information (so we can grow/reduce overall confidence based on the number of sources reporting as well as the confidence in and of each source).

Reputation History

A full history is kept for each modification made to RepDB over time. This allows us to call up a complete list of changes to any reputation item.

Signatures & Threats

Triggered by changes to reputation items, signatures are automatically generated, assigned threat IDs, and distributed to Network Box threat protection devices in real-time using both PUSH and cloud signature delivery mechanisms.

Statistical Feedback

Network Boxes under management periodically report back threats seen, and this is integrated back to RepDB (using the signatures and threats relationship to reputation items) so real-time and historical statistics can be seen on whether a particular reputation item has been seen in the real world, if we are blocking it, and how prevalent it is.

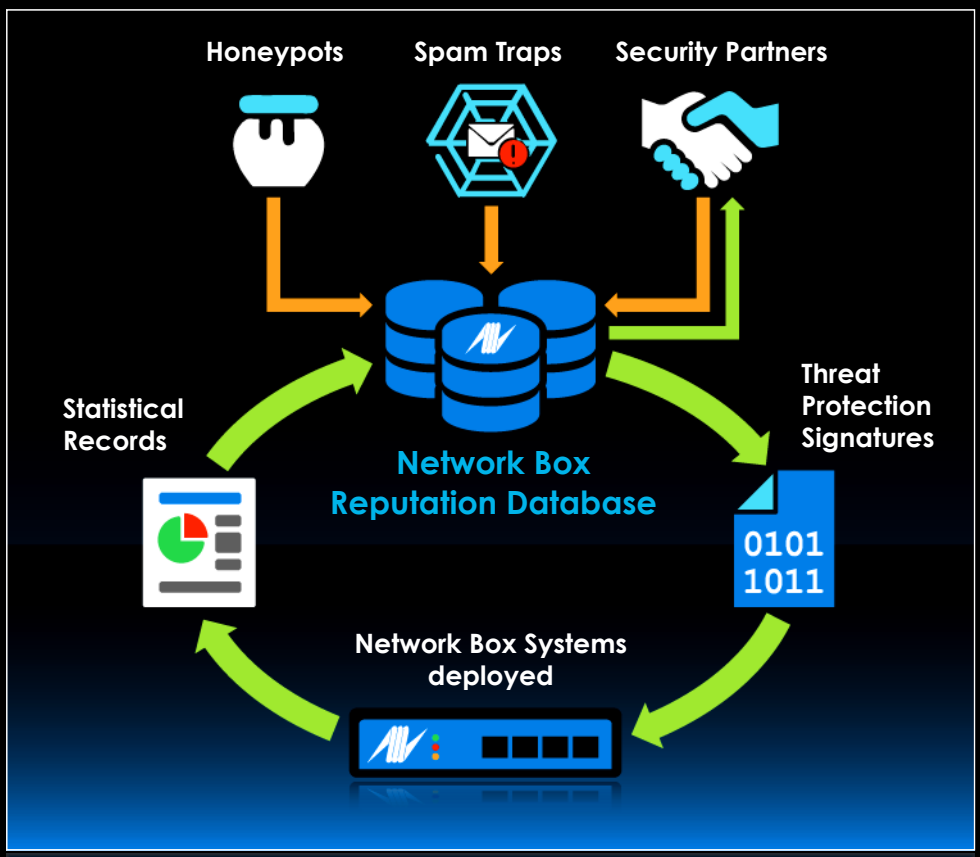
NETWORK BOX

All this is stored in the cloud, in a high availability real-time distributed database system. We currently track more than **14 million reputation signatures**, covering more than **100 million individual items**, with historical data going back more than 15 years. RepDB is currently growing at the rate of more than **200,000 signatures a month**.

Partnerships and threat information sharing arrangements are key to this system. As well as information coming in from partners and devices under management, we also maintain a large collection of honeypots and spam traps. Overall, we have several hundred sources of threat data and intelligence, all feeding into RepDB in real-time.

Let's look at an example, to show how this works:

1. RepDB receives threat intelligence (from a partner or honey pot) and creates reputation items to record the classifications and confidences.
2. RepDB immediately raises signatures and threat indicators.
3. Network Box Z-SCAN immediately issues protection.
4. Traditional signatures are raised and pushed out to (a) mail scanners, (b) file scanners, and (c) on-demand scanners.
5. Threat indicators and samples are provided to our information sharing partners.
6. Over time, as Network Box devices start to record blocks on this emerging threat, the statistics flow back to RepDB. This is used to strengthen/weaken reputation scores, based on real-world experience.



While traditional anti-malware vendors continue to work on the scale of hours to release protection, Network Box's RepDB has been fine-tuned over the past 15 years to the stage now where we can issue threat protection signatures in milliseconds. Both cloud-based and PUSH technology are used to get these protection signatures released, and statistical feedback loops keep us informed as to the effectiveness of that protection.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th February 2018, 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
February 2018

This month, for Network Box 5, these include:

- Improvements to policy file name extractions for 7z archives
- Add support for non-UTF-8 filename encodings in 7z archives
- Fix to not display names of removed network interfaces in 'show network interface list'
- Enhancements to configurability and monitoring of permanent IPSec VPN connections
- Performance improvements in DH and ECDH for SSL connections
- Improvements to handling of protocol-level DNAT (for variable, non-deterministic, network outputs)
- General performance improvements in proxied connections
- Support header change directives in IMAP protocol
- Support header change directives in POP3 protocol
- Improvement to statistic reporting in HTTP protocol transactions (detailed output)
- Enhanced search capabilities in Web Client Activity report
- Add support for hybrid dual-factor TOTP authentication against RADIUS servers
- Add support for hybrid dual-factor TOTP authentication against LDAP servers
- General improvements in eMail address parsing and sender/recipient address extraction

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

Network Box Hong Kong
Guardforce Seminar

Guardforce, the global experts in physical security, visited Network Box HQ, for a briefing on the current cyber-security landscape, as well as a sneak preview of the upcoming features in Network Box 5.5 – the latest Network Box managed cyber-security platform.

Network Box
Year in *Focus* 2017

2017 was another eventful year for Network Box. Last year, we saw a massive rise in ransomware and vulnerabilities, with *WannaCry* and *PetrWrap*, affecting systems all across the world, and making headline news. To provide our expert opinion on cyber threats, Network Box was interviewed by various media outlets including: **CNN**, **Reuters**, **BBC** and **Forbes**.

Also, in addition to being named in **CIO Review's Most Promising DDoS Solution Providers**, Network Box won numerous awards, taking the total number of industry, media and governmental awards Network Box has received, to over **140**.

Furthermore, Network Box participated in various international IT and Security events across the world. And finally, 2017 saw the launch of the **UTM-5Q**, and **VPN-5Q** hardware appliances.

LINK:
http://www.network-box.com/sites/www.network-box.com/files/files/Year_in_Focus_2017.pdf

Network Box Germany
NetzPalaver Interview

Network Box Germany Managing Director, Dariush Ansari, was interviewed by Netzpalaver to talk about the evolutions, revolutions and transformations that, from his point of view, will affect businesses in 2018.

LINK:
http://netzpalaver.de/2018/01/21/palaver-mit-network-box-zu-den-trends-in-2018/

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