SEP 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the September 2014 edition of In the Boxing Ring

This month, Network Box Managing Director, Michael Gazeley, discusses the issue of trust/reputation based cyber security systems. Instead of just relying on the scanning of data packets at the gateway, these systems allow additional judgments to be made, based on contextualized data about the files being scanned, or where the data packets being received actually came from; to add an extra layer of protection. This is discussed further on pages 2-3.

On pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, Network Box conducted a series of seminars with Jardine OneSolution on both the Network Box UTM+ and Anti-DDoS systems, to create awareness of Network Box service offerings. In addition, Network Box has created an Infographic of Healthcare Data Breaches in 2014. To view the full image, please click the link on page 5.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2014

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

TRUST In an unforgiving Cyber World

by Michael Gazeley

Reputation (or trust) based cyber security systems, are growing rapidly in popularity, for the simple reason that they work. They add an additional layer of much needed real-time protection, against the rapidly changing cyber threat landscape.

Instead of just relying on the scanning of data packets at the gateway, these reputation systems allow additional judgments to be made, some based on contextualized data about the files being scanned, and some based on where the data packets being received actually came from.

Such logic, of course, isn't new.

Financial institutions, have been relying on credit scores to make decisions about lending money to people and businesses, for a very long time. Corporations offering potential key hires important (or sensitive) jobs, often rely on background checks performed by trusted third-party organizations. And increasingly, airport security services around the world, are starting to look at travelers' histories, long before they even turn up at the ticket counter.

These are all reputation (or trust) based approaches, to real world security problems.

Organizations around the world, need to ensure that their vital business communications, can rely on data only going to and from trusted sources. Malware, SPAM, Phishing Emails, and other cyber threats, have grown exponentially over the last few years.

Advanced Threat Intelligence, is key, to dealing with Advanced Persistent Threats. Therefore, making the very fullest possible use of trust based systems and technologies, is vital.

The Network Box 5 Managed Security Services Platform, leverages an increasing number of reputation and trust based systems. Some developed in-house by our programming team, who have won more than 80 industry awards over the last decade, and others from world-class security partners and providers. The technologies involved, go well beyond that of a 'simple credit bureau approach' to trust, and integrates up to seventy-eight security engines, which are either updated using Network Box's patented high speed PUSH update technology, or Network Box's (even faster) multi-award winning Z-Scan cloud based cyber defense shield.

The augmented gateway security on offer with Network Box 5, takes the new systems' capabilities far beyond what is possible using Network Box 3 based technology.

Network Box 3 based systems, have done an absolutely amazing job over the last seven years, but the Network Box 5 platform is built for the future. The Intrusion Detection and Prevention systems built into Network Box 5, for example, are able to fully utilize the multi-core architecture of the CPUs in the latest hardware, to deal with emerging threats in the most efficient manner possible.

Once reputation security is implemented however, it is almost inevitable that some of the individuals, companies, and organizations which one deals with, will turn out to have a reputational issue, at least in cyber security terms.

It may be that a supplier's organization has been blacklisted as a spammer. It may be that a vendor's website has become compromised, and is now infecting visitors. It may even be that an important customer's network, has become part of a well-known botnet.

Security organizations are leveraging 'reputation,' to secure networks in a highly scientific way. Hackers, malware writers, and spammers, on the other hand, are leveraging 'reputation' in a highly emotional way, to try and compromise those very same networks.

The bottom line is that despite the fact you may know, and therefore personally trust, the victims who are the source of these cyber threats, that does not make the threats any less real.

Indeed, the potential threats are all the more dangerous, because they are either really from 'trusted' sources, or appear to be from 'trusted' sources.

So the next time a supplier's email gets blocked because their network is blacklisted, be careful not to whitelist them too broadly, or you could end up drowning in SPAM. If you visit a website you go to everyday, and it's suddenly blocked because it's listed as compromised, realize that it is almost certainly hacked and infected. And if you have an email blocked, because it has been sent from a network which is listed as part of a highly dangerous bot-net, don't be of the mindset that just because it's from your best customer, that you can simply ignore the warning.

In today's unforgiving cyber world, safe is definitely preferable to sorry.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd September 2014, 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 7 days.

Network Box 5 Features
September 2014

This month, for Network Box 5, these include:

- Enhancements to application identification to offer it as an optional filter on any network traffic
- Enhancements to application identification to support 'session promotion' to higher-level scanning modules
- Enhancement to provide LDAP support for SSL VPNs
- Enhancement to provide a configurable option to rewrite HELO/EHLO greeting of smtp client
- Enhancement to provide support for entitygroup for http protocols
- Performance and stability improvements in the handling of UDP traffic
- Enhancement to provide a result 'warn' (instead of 'audit') when HTTP response is 4xx or 5xx
- Improvements to memory utilization in proxy services
- Enhancement to provide a timeout in entry of comment when applying configuration changes
- Enhancement to support spam blacklist/whitelist rules with pop3client protocol
- Enhancement: Request for mailscan heuristics test BAD HDR
- Stability and performance enhancements to IDS/IPS scanning engines
- Improvements to logging of unexpected negative mail server responses (SMTP protocols)
- Improvements to IDS/IPS logging
- Improvements to quarantine mechanism for mail protocols
- Enhancements to the KPI screens, to include Frontline-IPS in IPS section
- Enhancement to provide multi-lingual support for web portals
- Introduction of Traditional Chinese (Hong Kong) language option in web portals
- Introduction of Traditional Chinese (Taiwan) language option in web portals
- Introduction of Simplified Chinese language option in web portals
- Enhancement to provide fonts for Chinese, Japanese and Korea in PDF reporting
- Improvements to fault trapping arrangements during dynamic content evaluation
- Enhancements to multi-link gateway system to provide support for primary/backup links (rather than load balanced)
- Enhancements to mail scanning engines related to anti-spam and anti-malware control
- Enhancement to introduce a configurable facility to disable 'release quarantine to others' on user portal
- Enhancement to introduce a Workload KPI
- Enhancement to introduce default values for system kernel configurable parameters
- Improvements to rule enforcement system during mail envelope scanning
- Enhancement to provide support for the BATV PRVS scheme during mail envelope verification
- Additional support and updates for Network Box Indonesia SOC

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 ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features September 2014

On Tuesday, 2nd September 2014, 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 7 days. This month, for Network Box 3, these include:

- Enhancements and improvements to Anti-Spam performance and accuracy
- Enhancements to Contract system to support HA contracts with optional services
- Various (mostly internal) enhancements to several internal support systems

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.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	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 2736-2078 Fax: +852 2736-2778 www.network-box.com

Network Box
Jardine OneSolution Security Technologies Seminar

Network Box is currently conducting a series of seminars with Jardine OneSolution on both our Unified Threat Management Plus, and Anti-Distributed Denial of Service Web Application Firewall Plus systems. These seminars include information on all of our very latest Network Box 5 technologies, such as Application Control, SSL Proxying, HTML-5 Dashboard, Custom Report Generation, and IPv4 / IPv6 Bridging.

Network Box USA
USA Today

Network Box USA's Chief Technology Officer, Pierluigi Stella, was Interviewed by USA TODAY about the recent event where a Russian crime ring amassed a cache of 1.2 billion username and password combinations.

LINK:
http://www.usatoday.com/story/tech/2014/08/06/russian-Crime-Ring-cybersecurity/13658595/

Infographic:
2014 Healthcare Data Breaches

LINK:
https://networkboxusa.files.wordpress.com/2014/08/2014healthcaredatabreaches1.png