DEC 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the December 2014 edition of In the Boxing Ring

This month, we are releasing two major new features for Network Box 5: 1) Event Correlation and intrusion alerting system and 2) network-level infected LAN system. On page 3 we introduce the Event Correlation system. The system correlates intrusion activity across all the network-frontline, network-ips, network-ids and network-firewall systems.

On page 2 we talk in greater details about the enhancements to the core Network Box 5 modules - *network-frontline* and *network-infectedlan*.

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 Managing Director, Michael Gazeley, gave a talk about the cyber threat landscape at the Jardines Risk Management Conference 2014. Jan van Leersum, Network Box Singapore's Managing Director, was interviewed about the Heartbleed vulnerability, and Network Box USA was at the Expo-Telecom 2014, held in Costa Rica.

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

Frontline Protection and Infected LANs

The direction of a particular network connection is everything in network security. Protecting client workstations on the LAN from infected web servers on the Internet is a completely different task from protecting customer web servers in the DMZ from attackers on the Internet.

The issue is that while the core protocol may be the same (HTTP in this case), the threat landscape is often completely different.

Network Box 5 embodies that principle by providing different security modules, depending on the direction of traffic. For example, smtp-server vs smtp-client, or web-server vs web-client.

This month we're releasing enhancements to two core Network Box 5 modules – network-frontline and network-infectedlan.

network-frontline security module

Addresses the issue of front-line protection against scanning and intrusion activity. While higher-level modules (such as network-firewall, and network-ips) provide advanced protection using a huge number of signatures, network-frontline uses heuristics and a relatively small number of specifically targeted signatures to provide front-line protection with very little performance impact. Network-frontline is designed to be able to run on every Network Box 5 system.

This month we're releasing a new framework for our network-frontline security module in Network Box 5. This framework allows for highly configurable:

- Identification of scanning behavior from the Internet, by heuristic detection of protocol and port scanning rates.
- Highly-granular detection of non-protocol-conforming scans from known scanning engines.
- Standardized support for tripwire ports – particularly useful for detection of slow scans.
- Optional support for dynamically blacklisting detected scanners.

Note: To support those of our customers using Network Box 3, we have back-ported what we can, and this month we're also releasing some parts of the network-frontline framework for the Network Box 3 platform.

network-infectedlan security module

Addresses the issue of identifying infected workstations and servers in the LAN / DMZ areas of your network. While higher-level modules (such as anti-malware and content filtering) can detect access to malicious content, the network-infectedlan module attempts to identify outbound botnet access from your network. Again, it is very lightweight (performance wise) and designed to be able to run on every Network Box 5 system.

This month we're releasing a new framework for our network-infectedlan security module in Network Box 5. This framework allows for highly configurable:

- Detection of outbound access to known public botnet command and control servers.
- Detection of outbound access to known malware update sites.
- Highly-granular detection for highly-prolific malware (such as Palevo, Conficker, Zeus, etc, for example).
- Optional support for dynamically blacklisting detected infected workstations / servers.

This new network-infectedlan framework is only available on the Network Box 5 platform.

Together, both these modules provide highly effective, but extremely lightweight (from a performance point of view) protection for both inbound intrusions as well as infected workstations/servers connecting outbound.

NETWORK BOX

Event Correlation

One of the most common requests we receive at our Security Operation Centres is when customers ask us to notify them if there is an intrusion attempt against their network. The issue we have with this is twofold:

1) Our primary mission is to protect our customers. That means that our primary focus is Intrusion ***Prevention***, not just ***Detection***. We stop the attack, not just let it through and then tell you about it later.
2) Every minute of every day, the public Internet is scanned – from thousands of sources in hundreds of countries. They respect no network or international boundaries, and the scanners try to get into your network. Some of these scans are truly malicious, some are configuration mistakes, and some are purely for research purposes. Most are automated, but all are an intrusion attempts into your network. We call this ***Internet Background Radiation***.

Alerting on each and every one of these intrusion attempts would mean alerting dozens of times every hour on even the smallest of networks.

This month, for Network Box 5 customers, we're releasing our Event Correlation system. This new system correlates intrusion activity across all the network-frontline, network-ips, network-ids and network-firewall systems. For each source IP, it maintains statistics on the number of targets hit, the number of blocks seen, the number of scans seen, and the number of different types of attack seen. The system is highly configurable, and thresholds for each of these four attributes of an intrusion can be set, in order to escalate the intrusion incident for further processing.

Escalation options include:

- Dynamically blacklisting the source of the attack, usually for a small number of minutes (sufficient to interfere with the attack).
- Alerting (via eMail) administrators as to the source and details of the attack. An alert is raised both when the attack is first seen, as well as when it is determined to have finished.

With this event correlation system, the number of alerts raised can be dramatically reduced (removing most of the noise of *Internet Background Radiation*). However, while the size of intrusion necessary to raise an alert can be configured, this system is still likely to raise several alerts each day (for small networks) and hundreds of alerts each day (for large networks). The sad reality is that there is so much malicious scanning and automated intrusion activity on the Internet every day. For this reason, we don't recommend that this alerting mechanism be generally enabled – but it is available for customers who need it.

Remember that our primary mission is prevention of the attack, and the dynamic blacklist facility, based on event correlation, provides an excellent tool to interfere with external network scanning and intrusion activity.

To support those of our customers using Network Box 3, this month we're also releasing our event correlation and alerting system for the Network Box 3 platform, as well as Network Box 5.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

This month, we are pleased to announce the release of two major new features:

1. **Event correlation and intrusion alerting, combined with extensions to front-line intrusion prevention**
2. **and the release of the network-level infected LAN system**

The event correlation system is discussed in more detail in the article included in this month's In The Boxing Ring newsletter.

The network-level infected LAN system is designed to detect connections to known command-and-control hosts from workstations on the LAN/DMZ segments of your network. As well as alerting, it can also optionally dynamically quarantine the infected workstation for a defined period of time.

Network Box 5 Features December 2014

On Tuesday, 2nd December 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 5, these include:

- Event correlation and intrusion alerting
- A new TRACEROUTE test on the administrative web portal
- A new PING test on the administrative web portal
- Improvements to anti-malware scanning engines
- New support for front-line whitelist and dynamic blacklist
- New support for infectedlan whitelist and dynamic blacklist
- Support for configuration of customized IDS/IPS rules
- Support for configuration of customized anti-spam rules
- Support for configuration of customized anti-malware rules
- Support for configuration of customized anti-DLP rules
- Improvements to anti-spam for new top-level-domains
- Improved support for export of large reports in CSV format
- HTTP host and path target host routing for web server and WAF protection
- Support for a new non-enforcing 'alert only' mode for Intrusion Prevention System
- Improvements to NBSYNC to allow deployment of more than 1,000 simultaneous cluster connections
- Enhancement to notes on mail policy block to show file extension and content type blocked
- Support for personal whitelists in user web portal and reporting
- Support for personal whitelists in administrative web portal
- Support for a configurable DHCP lease time limit
- Report schedule support for KPI reporting
- A number of new configurable options for web application firewalling (WAF)

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 3 Features December 2014

On Tuesday, 2nd December 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:

- Improvements to spam detection, related to exploits against new top level domains
- Frontline SCAN/INTRUSION detection, event correlation and alerting option
- 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	Network Box Corporation nbhq@network-box.com or via mail at:
Michael Gazeley **Nick Jones** **Kevin Hla** Production Support	**Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong
Network Box HQ **Network Box UK** **Network Box USA** Contributors	Tel: +852 2736-2078 Fax: +852 2736-2778 www.network-box.com

Network Box
Jardines Risk Management Conference 2014

Network Box Managing Director, Michael Gazeley, gave a talk titled,'Cyber Security Landscape: Extreme Evolution,' at the Jardines Risk Management Conference 2014.

Network Box Singapore
Media Coverage

Network Box Singapore Managing Director, Jan van Leersum, was interviewed by MIS Asia and Computerworld about the Heartbleed vulnerability, and how Network Box were able to protect their customers from the attack, without even needing an update.

MIS ASIA COMPUTERWORLD MALAYSIA

LINK: http://www.mis-asia.com/resource/security/fighting-heartbleed-the-network-box-way/?page=1

LINK: http://www.computerworld.com.my/resource/security/fighting-heartbleed-the-network-box-way/?page=1

Network Box USA
Expo Telecom 2014

Network Box USA, in partnership with ITS InfoCom, exhibited at 'Expo-Telecom 2014' held in Costa Rica.