AUG 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the August 2016 edition of In the Boxing Ring

This month, in part one of a special three-part series written by Network Box USA's CTO Pierluigi Stella, we cover the issue of **why you need WAF**. Attacks on web servers are the most prevalent issue in cyber security and in 2016, we have seen significant rise in this. Without proper protection, your network is vulnerable to these kinds of attacks. On pages 2 to 3, we discuss this issue in greater detail.

Also this month, we are releasing support for a new URL category: **INFL botnet cac *(Infected LAN botnet command and control)***. This category includes URLs which have been classified as malicious and part of known botnet command control networks and protocol. This, and the **Proxy Infected LAN** module are discussed in detail on page 4.

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

Finally, Network Box Hong Kong conducted a cyber security seminar for members of the **Hong Kong Security Association (HKSA)**, to highlight the current cyber risk landscape, Network Box Australasia was at the **2016 ITx Expo** held in Wellington, New Zealand, and Network Box Germany participated in the **econnect on Tour 2016**, organized with *eco - Association of Internet Industry*.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 2016

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

Why you need WAF

(part 1 of 3)

by Pierluigi Stella

Chief Technology Officer
Network Box USA

At the time of writing, attacks against web servers are (by far) the most prevalent issue in cyber security. A Data Breach Investigations report for 2014 showed that **35%** of breaches were caused by web application attacks. And by mid 2016, this number is only rising.

Hackers are getting control of web servers for different reasons, the main ones being the ability to control a server and spread malware. Often, these two objectives go hand in hand.

Why do hackers want to control a web server? Because a server is often hundreds of times more powerful than a workstation, and that allows them to have a platform to launch attacks from a single point, rather than having to deal with multiple workstations. Servers are often also connected to larger bandwidths, enabling these attacks to be increasingly efficient. They are also online 24/7, users don't turn them off at night as they tend to do with a personal computer. And they are connected to public IP addresses on a public network, not in someone's home or office. A server can, and most times is, used as a command and control center to manage a network of zombies – a botnet. Finally, a server can be used to 'serve' malware. In this case, the web server may not even look compromised, and yet malware lurks in the background, ready to attack unaware browsers.

This should make one thing abundantly clear – protecting web servers is critical; not only does a company stand to lose data, the server can also be used as a bridge into the company's network. Or to launch attacks against other companies; and although we have yet to see lawsuits in such cases, it is only a matter of time before someone gets sued over allowing their server to become a tool for conducting attacks against someone else.

But how exactly does one protect a web server? Especially one that is running an application, which is, in turn, connected to a database?

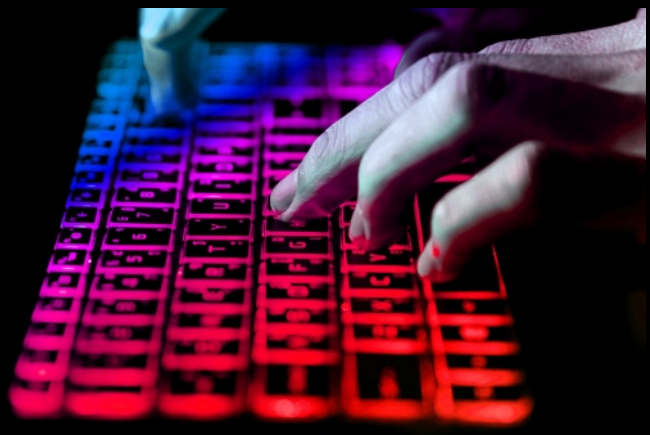
Up until a few years ago, the practice was to put the web server itself into a DMZ, the database server on the LAN, and 'hope' that the firewall and IPS could stop malicious traffic between the two. The idea being that if the web server were to become compromised, it is easy to rebuild and data is not lost. Unfortunately, this method of protection is insufficient; it never really was to begin with, but today, it is clear how and why.

First of all, too many people misinterpret the meaning of DMZ and allow all traffic, rendering the very idea of DMZ pointless. Second, the ports needed for the web server to run queries against the database are the very ports hackers are trying to attack. This does not in any way prevent a SQL injection or a database DDoS attack, as both methods use database ports that are open from DMZ to LAN to allow the web server to run queries.

The next idea was to set up IPS in line with firewall, to intercept malicious traffic. Though not a bad idea, it is, unfortunately, very limiting. An IPS is a layer 3 protection. Think of it as an AV at the packet layer. It reads the content of a single packet in a stream, inspects it against known vulnerabilities and exploits, using a mix of signatures and heuristics (behavior analysis). And that is all it does. You might be wondering what the issue is. IPS is used for many different reasons. The problem is that IPS is a layer 3 protection, whereas HTTP is a layer 7 – it is an application layer protocol. And web servers run applications. This means that attacks can be carried on using transactions that span across several packets or streams; and each packet or stream can appear to be perfectly clean. An IPS can protect against some low level SQL injections and XSS attacks; it can protect against things like the Slammer worm, on which more information can be found here:

https://en.wikipedia.org/wiki/SQL_Slammer

SQL Slammer is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic, starting at 05:30 UTC on January 25, 2003. It spread rapidly, infecting most of its 75,000 victims within ten minutes. The reason why that is possible is because the Slammer was less than 400 bytes in size, so the entire malware fit into one ~~a~~ single packet.



But a web server attack of recent times is almost never just a single packet of malware. More often than not, such attacks try to work around the HTTP protocol, injecting commands that are not part of a normal sequence, to gain access to resources on the server or cause the application to react in a way it wasn't designed for. In other words, an IPS cannot understand web application protocol logic, and cannot fully distinguish if a request is normal or malformed at the application layer.

In part two of this article, we will explain (at length) why an IPS is ineffective when it comes to providing a safeguard against application vulnerabilities.

INFL botnet cac URL Category and Proxy Infected LAN

This month, we are releasing support for a new URL category "INFL botnet cac", in Network Box 5. URLs categorized as this are malicious in nature and used by botnet clients to access botnet command and control servers. As such, we recommend such accesses be denied, and include this category in both our standard nb-core and nb-malware ACLs.

Category: INFL botnet cac
Title: Infected LAN botnet command and control

This category includes URLs which have been classified as malicious and part of known botnet command and control networks and protocols. Typically, botnet clients use these URLs to communicate with their command and control servers. The category is very precise and there is a low risk of false positive.

The **Proxy Infected LAN** security module subscribes to a PUSH update signature set of several thousand malicious URLs used by known botnet command and control centres. This URL categorization support extends the botnet IP address support provided by the base "Network Infected LAN" security module. We currently provide URL categorization coverage for:

- cryptowall
- feodo
- locky
- palevo
- teslacrypt
- torlock
- zeus
- and other common botnets.

Customers using the Proxy Infected LAN and web client content filtering security modules can now take advantage of this new category by either blocking the nb-core and/or nb-malware category ACLs, or specifically blocking category "INFL botnet cac", in their web client policies.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 2nd August 2016, 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
August 2016

This month, for Network Box 5, these include:

- Support for transfer of IP address attribute in the entity learning system, in the case where a new user logs in from the same address as an existing user
- Support for commands to show live policy routing rules and routing tables
- GMS sensor support for hardware raid
- Improved hardware raid support in administrative console
- Support for switchable GMT/local time stamps in syslog output
- Introduce notification message for administrative console, for NOC-BOX configuration synchronisation
- Smart numeric ordering of IP and port ACLs in console and web administrative interfaces
- Change to user portal report to not include audit records, even if mail is quarantined
- Introduction of proxy infectedlan security module\
- New 'INFL botnet cac' URL category, for Botnet Command & Control servers, and dynamic URL signatures

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
HKSA Seminar – Cyber Risk Landscape 2016

Network Box Hong Kong welcomed members of the Hong Kong Security Association (HKSA), to attend a cyber security seminar titled, 'Cyber Risk Landscape 2016.'

The seminar highlighted the top 10 cyber risks facing most businesses and organizations, and introduced Network Box's next generation security technologies. In addition, those that attended were also given a tour Network Box's triple ISO certified SOC.

Network Box Australasia
ITx Expo 2016

Network Box Australasia was at ITx 2016, highlighting Network Box's latest Network Box 5.3 Managed Security Service Platform, designed to offer multi-award winning, world class managed security services, to organizations of all sizes.

Held at the TSB Bank Arena, Wellington, New Zealand, ITx focuses on innovation, technology and education and brings IT professionals, decision-makers, leaders and academics together under one roof.

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 2736-2083 Fax: +852 2736-2778 www.network-box.com

Network Box Germany
econnect on Tour 2016

Network Box Germany, in association with ***eco*** – *Association of Internet Industry*, participated in the, "econnect on Tour 2016." During the event, Network Germany's General Manager, Dariush Ansari, introduced Network Box's technologies to the delegates.