Welcome to the July 2013 edition of In the Boxing Ring

This month, the two main topics being discussed are: Trojans and the new OWASP Top 10.

With the Composite Blocking list (CBL) recently using HTTP sinkholes to detect trojan infected clients, making an HTTP request may get your IP address SMTP backlisted. This is drawing attention to the issue of trojans ‘calling home’. This is discussed further on page 2, and how to protect against the threat within your network.

On page 3, we compare the old OWASP Top 10, released in 2010, with the current one as released by the Open Web Application Security Project (OWASP). OWASP is an open community focused on improving the security of application software. For your further reading, we have included a link to their report.

Finally, we are proud to announce that Network Box’s Web Content Filtering Engine, S-Scan, won a 2013 Computerworld HK Award in the Content Filtering / Anti-Spyware category. This is the third year in succession that Network Box has won an internationally contested award from Computerworld.

IN THIS ISSUE

2 Real-Time Detection and Blocking of Outbound Trojan Activity
We discuss the current issue of trojans and compiled a list of security recommendations on how to protect yourself against the treat of undetected trojans with your network.

3 OWASP Top 10 - 2013
We highlight the top ten web security risks as released by the Open Web Application Security Project.

4-5 NBRS-5.0 Features and Roadmap
The features and fixes to be released in this month’s patch Tuesday for NBRS-5.0. NBRS-5.0 roadmap, which gives a clear overview of what we have recently released, as well as the final milestones.

6 NBRS-3.0 Features
The features and fixes to be released in this month’s patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years).

Mark Webb-Johnson
CTO, Network Box Corporation
July 2013
Network Box Security Response has recently made the following 6 recommendations that can better protect you against the threat of undetected trojans within your network:

1. Configure an effective outbound policy both in the firewall LAN->NET as well as Network Box proxies. In particular, permit only that which is explicitly required, and malicious categories such as "Virus/Malware Infected" should be blocked by default.

2. Enable the Network Box Intrusion Detection and Prevention System (NBIDPS) on your network.

3. HTTPS proxy 'CONNECT' connections to dotted decimal addresses (e.g. 123.456.789.0) should be denied by default, and only permitted where explicitly required.

4. Executable blocks (both by extension and file type) should be enabled for inbound eMail, wherever possible.

5. Different outbound proxies can be configured to use different IP addresses. Network Box generally recommends that outbound eMail be sourced from a different IP address than outbound HTTP/HTTPS traffic. Following this recommendation will mean that HTTP blocks such as CBL is now using would not affect the eMail service.

6. The service RBLMON (http://www.rblmon.com/) will monitor IP addresses you list against 60+ RBLs and alert you should one or more of your addresses be blacklisted. This service will monitor up to 3 addresses for free, and they have paid plans for larger customers. There are also several other similar competing services (rbltracker, rbl-check, rblwatch, etc). It makes good sense to subscribe to such services and keep an eye on the RBL state of your addresses. If you use a different outbound IP address for your HTTP/HTTPS vs SMTP traffic, then you should monitor both IP addresses (so that you will get notified of a HTTP/HTTPS problem even though it won't affect your SMTP traffic).

Network Box continues to closely monitor the situation, and will PUSH further protection signatures as necessary. Following the above guidelines should help mitigate any trojan infection (for example, a laptop brought into the office network) and provide for early detection and blocking of the undesirable outbound traffic.

The CBL lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, wingate, Bagle call-back proxies etc) and dedicated Spam BOTS (such as Cutwail, Rustock, Lethic etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of trojan-horse or 'stealth' spamware, dictionary mail harvesters etc.

http://cbl.abuseat.org/
OWASP Top 10 2013
The Ten Most Critical Web Security Risks

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. They have recently released their Top 10 Most Critical Web Application Security Risks for 2013. This document provides an excellent foundational understanding of the primary threats affecting web applications, and how you can best defend against them.

**LINK:** OWASP Top 10 2013 document (PDF)

The Network Box Anti-DDoS WAF+ system (based on NBRS-5.0 platform) is specifically designed to provide effective and comprehensive protection against these, and other, web application attacks.

For further information, please refer to the December 2012 In The Boxing Ring article or contact your local Network Box support office.
Network Box Version Five
NBRS-5.0

On Tuesday, 2nd July 2013, Network Box will release our patch Tuesday set of enhancements and fixes. These enhancements have been primarily made to support the new web client security modules.

NBRS-5.0 Features
July 2013

The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-5.0, these include:

- Release of 7 new security modules to final beta testing:
  - scan-base (base module for all scanning functionality)
  - scan-file (file scanning for HTTP)
  - scan-url (URL scanning for HTTP)
  - scan-provider-antimalware-nb (Network Box Z-Scan, and other, scan engines for anti-malware)
  - scan-provider-antimalware-kaspersky (Kaspersky anti-malware scanning engine)
  - scan-provider-url-nb (Network Box URL categorisation engines)
  - scan-provider-url-sscan (Network Box S-SCAN URL categorisation engine)
- Add support for VLANs to base product.
- Extensions for support of web client scanning service packages (including URL content filtering and HTTP anti-malware scanning).
- Support for web session tracking for web clients.
- Change to log threat type ‘firewall’ for traffic blocked by the network firewall.
- Change to log the threat type as the module name for generic threats blocked by all security modules.
- Support for geographic identification of the country of traffic source and destination, as well as policy control, in network firewall.
- Including of a NTP service daemon in base product.
- Enhanced support for tracing of log messages in the nbsyslog subsystem.
- Improvements to front-panel display and functionality for physical hardware.
- New unified tooltip appears in my.network-box.com administrative web interface.
- Other minor revisions and improvements to my.network-box.com administrative web interface.
- Speed and control improvements during box start-up (following cold boot or restart).
- Various (mostly internal) enhancements to Box Office and 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 NOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.
Network Box Version Five
NBRS-5.0

NBRS-5.0 Roadmap

We are now well into the ramp-up phase of our road-map for NBRS-5.0. The majority of development work has been completed, and we are now conducting final development, packaging and beta tests for the remaining security modules.

With this month's patch Tuesday we will release our SURF SCAN product, and this will include anti-malware and content-filtering support for web clients - rounding-out our web content protection offering (both client and server). In the August 2013 patch Tuesday, we will release our mail scanning product, and that will be followed by the remaining miscellaneous modules to bring NBRS-5.0 up to, and beyond, full UTM+ equivalence to NBRS-3.0. Once we have reached those milestones, we can start the process of offering NBRS-5.0 upgrades to our existing NBRS-3.0 clients.

The NBRS major releases for Network Box (NBRS-1.0, NBRS-3.0, NBRS-5.0, etc) include long-term support, of 5+ years, so this is just the start of a long journey with NBRS-5.0. We have some truly exciting new product offerings, taking advantage of the new foundational support architecture of NBRS-5.0 that will help us to help you to keep your online networks secure.
NBRS-3.0 Features
July 2013

On Tuesday, 2nd July 2013, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for NBRS-3.0, these include:

- Revisions to SMTP mail, to address false positives from CVE-2011-1431 scanners.
- Improvements to handling of repetitive invalid responses in the HTTP proxy system.
- Support for forced-addition of disclaimers to badly formatted SMTP emails.
- Various (mostly internal) enhancements to Box Office and 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 NOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local NOC. They will be arranging deployment and liaison.

Network Box wins Computerworld HK Award 2013 for Content Filtering / Anti-Spyware

21st June 2013

Network Box is extremely proud to announce that our S-Scan Web Content Filtering Engine, won the Computerworld Hong Kong 2013 Award for Content Filtering / Anti-Spyware. This is the third year in a row that Network Box has won an internationally contested award from Computerworld.

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
<th>% difference (since last month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>642</td>
<td>+1.3</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>568,821</td>
<td>+4.1</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>926,948</td>
<td>+2.4</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>107,288</td>
<td>+9.1</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>18,008</td>
<td>+8.2</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>603</td>
<td>+19.2</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>186,439</td>
<td>+8.2</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>3,298,188</td>
<td>+1.1</td>
</tr>
</tbody>
</table>

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

Copyright © 2013 Network Box Corporation Ltd.