Welcome

Welcome to the September 2008 edition of 'In The Boxing Ring'. It has been a busy month here at Network Box Security Response and we’ve been at Alert Condition 4 for most of the month. The ongoing virus and spam onslaught from the Storm Botnet is making headline news and driving anti-spam and anti-virus PUSH updates to an all-time high. More on this topic on page 2.

Early on in the month, we had a successful launch of the new Box Office regional mirrors, and we’ll give you an update on that and answer your Frequently Asked Questions on page 2.

We’ll also be devoting some space in this newsletter to talk about the work we have been doing to start a beta-test on, and ultimately release, some revolutionary enhancements to our Anti-Spam and Anti-Virus offerings, as well as multi-language support in the my.network-box.com and weekly report systems.

We have now completed a successful beta-test of our Google Safe Browsing and Google Safe Searching functionality. These new features offer significant benefits and allow for better and more fine-grained control in your content filtering policies. These two new features will be available for general release on Tuesday 2nd September 2008, and there is a little extra something that made it in at the last minute; support for Yahoo safe searching as well.

No search filter can replace proper supervision when it comes to children on the internet, but every little bit helps.

As usual, if you have any feedback, or comments, it is always appreciated. You can contact us here at HQ via email (nbhq@network-box.com). Or, drop by our office next time you are in town.

Mark Webb-Johnson
CTO, Network Box Corporation
September 2008
A Stormy Month

The onslaught of spam

Globally, customers have reported a spam onslaught. Whether its FEDEX / UPS deliveries, CNN / MSNBC news, or Britney Spear’s dress code, the links provided point to malware-download sites and the emails are definitely unwanted.

Security Response

Compared to the previous month, in August, we sent out 30% more push updates (about 14 extra updates each day) and about 120,000 more signatures. Statistics show viruses hitting our boxes are up 51% over the month. We have also been continually refining the anti-spam heuristics to cope with new variants as and when they appear.

Alert Condition 4

We are often asked ‘what is the alert condition, why does it show on my box, and can you please fix it?’.

The Network Box Alert Condition indicates our alert readiness and the overall threat level on the Internet. It ranges from 1 (the Internet is calm) to 5 (severe degradation of global service) and for most of this year we have been at a stable level 2. We are now at level 4 and expect to remain at that level for the duration of this attack (which has been ongoing for several weeks now).

The Alert Condition has real meaning for Network Box Security Response. High levels mean vacations get cancelled and extra staffing for both us and our OEM partners. I would love to be able to ‘fix it’ (in particular because we treasure our sleep), but unfortunately that depends on the attack finishing so that we can lower the level.

We will keep you apprised of any changes to the situation, but for the moment the best advise I can give you and your users is not to believe everything you read in email.

Network Box Office

The Launch

On Monday 11th August 2008, we successfully switched our main Box Office portal to a new set of distributed mirrors. The main portal now redirects to https://global.boxoffice.network-box.com and from there, at login, you are redirected to your local mirror, which will be one of:

- https://ap.boxoffice.network-box.com
- https://eu.boxoffice.network-box.com
- https://us.boxoffice.network-box.com

We suggest that the ‘ap’ mirror be used by customers in Asia-Pacific, ‘eu’ by customers in Europe/Africa, and ‘us’ by customers in the Americas.

Should you wish to specify a mirror yourself, there are two ways you can customize this:

- You can use the “My Account” option within Box Office to choose your preferred mirror. At login (to the global main portal), you will be redirected to the mirror of your choice.
- Enter the url for the Box Office mirror you require directly into your browser. Only the ‘global...’ mirror will redirect, while the regional ones won’t (to allow you to specify ‘ap’, ‘eu’ or ‘us’ directly).

The new Box Office system uses the UTF-8 character set, and includes support for Simplified Chinese, Traditional Chinese and Korean languages (as well as the standard English). You can choose your language in two ways:

- From the top TAB bar, select the language you want - your choice will last for the current login session.
- From the “My Account” option within Box Office, you can choose your preferred language - your choice will take effect the next time you login.

Upcoming Work

Fighting a losing battle

For the past year or so, it has become increasingly obvious to us that we (and our industry) cannot continue as we are. Since Network Box started work on this, we have gone from perhaps 30,000 known viruses to more than 1,000,000. Anti-Spam signatures are approaching the 2,500,000 mark. In the past month alone, we’ve added support for more than 50,000 new virus variants.

While we strive for a 100% success rate, blocking more than 7,600 viruses and 107,000 spams, per Network Box, during the month of August; the virus/spam writers just need to get 1 through to claim their success.

I really do not understand how some vendors still manage to sell products with limited databases of signatures/heuristics - tracking only the wild-list is not feasible when the wild-list is bigger than your available memory for signatures.

Perhaps the only way to win is not to play at all?

A famous saying, and one that sums it up for me. While some developers look at high-maintenance solutions such as blanket whitelisting (block everything except that which is explicitly permitted), we’ve been doing some truly revolutionary thinking and coming up with technologies and systems that will make a drastic difference. Functionality and system configurations that will not only win this battle, but that will eventually help to win the war (and consume less system resources while doing it).

We hope to be able to announce the availability of closed beta tests for this technology during this month (September 2008), with a view to releasing these as an option during the October / November timeframe. I have reserved an entire page in the October newsletter, to talk about this, and will be able to explain things in more detail then.
Google Safe

Continuing our work on the Network Box Content Filtering Web Proxy, we have been developing support for two new Google features, and are now ready to globally launch these features on 2nd September 2008.

Google Safe Browsing

The Google Safe Browsing API enables client applications to check URLs against Google's constantly updated blacklists of suspected phishing and malware pages. The client application can use the API to download an encrypted table for local, client-side lookups of URLs that it would like to check.

Network Box has integrated this API directly into our policy engine as an optional engine that can be enabled / disabled on a per-box basis. We have also taken the opportunity to introduce a standardised URL normaliser into the policy engine, to convert obfuscated URLs into a standardised form prior to categorisation and policy enforcement.

The new engine maps Google's blacklist hash to a new category ‘GSB Phishing’ and Google's malware hash to another new category ‘GSB Malware’. This allows Google’s results to be separated from other engines and a fine granularity of control over the policy for these categories.

Both new categories have been added to the ‘nb-malware’ and ‘surfcontrol-core’ filter sets - so that customers using those standard filter sets can instantly get support for this new functionality, without requiring a policy change.

The standard policy block web page (which shows users a message that they have attempted to access a blocked web site) has been extended to add a warning if either the ‘GSB Malware’ or ‘GSB Phishing’ categories is found. The warning states that ‘this advisory has been provided by Google’ and provides a link to Google’s standard answer page on this functionality.

Updates from Google

Updates for the GSB databases are retrieved directly from Google (who hosts a worldwide mirrored, highly reliable set of update delivery servers). The default configuration will keep the databases up-to-date once every fifteen minutes using a highly bandwidth-optimised incremental update. The mechanism can be tuned, if required, on a per-box basis.

The Network Box update engine adheres to Google’s specification for downloading of updates and follows Google’s extensive recommendations for failure back-off and timings. Health checks are being deployed, to monitor this update system and alert the NOC if the updates cannot be retrieved, or are delayed.

Integration to eMail

The two new ‘GSB’ categories are also available to the URL scanner in Network Box eMail. This means that URLs found in emails can automatically be checked against Google’s published databases (using the Google Safe Browsing API) and enforced as phishing or virus blocks.

Google Safe Searching

Google, as well as other search engines, supports ‘Safe Searching’ options. These are intended to filter search results to only return safe links for those who want to search the Internet while reducing the risk of inappropriate material being viewed.

No search filter can replace proper supervision when it comes to children on the internet, but every little bit helps.

The Network Box implementation acts as a filter on Google search engine searches, and can optionally transparently and automatically enable ‘safe searching’ on such searches. The policy is enforced at the Network Box gateway to set the required level. Currently, we support three levels:

- Off - no modification of user’s browser preference for safe searching
- Moderate - enforcement of moderate safe searches (filtering explicit images and videos only)
- Strict - enforcement of strict safe searches (filtering both explicit text and explicit images/videos)

As well as the Google search engine, this functionality is also active for Yahoo searches.

How to enable these features?

The features will be launched on 2nd September 2008, and will be deployed to all NBRS-3.0 Network Boxes early in the month. Default policies will be applied to boxes at that time. If you would like further information on this, or need to fine-tune your policies, please contact your local NOC for assistance.

Language Support

Multi-lingual Support is being added to the Mail Portal, my.network-box.com and weekly report systems; initially with Traditional Chinese, Simplified Chinese and Korean options. Other languages are in progress and will be released over the coming months.

The support must be enabled in your box configuration, by the NOC; so contact your local NOC for help with this. Once enabled, you can choose the language you wish to work in from the menu bar at the top of the Mail Portal and my.network-box.com interfaces.

For the weekly reports, the language must be set by the NOC, so please contact your local NOC to change this if you require.

This functionality will be released on 2nd September 2008, and will be deployed to all NBRS-3.0 Network Boxes early in the month.
Sept 2008 Features

On Tuesday 2nd September 2008, we will release the following features and enhancements, for all NBRS-3.0 Network Boxes. These will be deployed, globally, and made available to all our customers, early in September 2008.

- Google Safe Browsing - using the Google API, the Network Box web proxy will support two new categories; “GSB Malware” and “GSB Phishing”. These categories are automatically, and dynamically, updated from Google’s published lists of malware and phishing URLs. The new categories are already included in the nb-malware malicious URL filter set.

- Google (and Yahoo) Safe Searching - enforcement, at the Network Box web proxy, of Moderate or Strict safe searching for both Google and Yahoo users. Protection is provided for both textual and image/video searches and enforcement of the policy at the Network Box gateway means that the users cannot easily work-around the restrictions.

- Multi-lingual support in Mail Portal, my.network-box.com, and weekly reports. Similar to the support in Box Office, released last month, we plan to release support for Traditional Chinese, Simplified Chinese and Korean languages. Other languages are in progress and will be released over the coming months.

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

Patch Tuesday

Network Box has moved to a patch Tuesday form of software enhancement release mechanism. This is to allow the NOCs and our customers to release, and install, new software and enhancements in a globally co-ordinated manner. All NOCs will operate to the same patch Tuesday schedule. This does not affect the normal real-time PUSH updates, and is for new features and enhancements only.

For Network Box, patch Tuesday is the first Tuesday of every month, and the first was Tuesday 1st July 2008.

While critical software patches, signatures and other such day-to-day (or minute-by-minute) releases will still occur out of cycle, throughout the month, we will usually release new software features and enhancements on patch Tuesday; and conduct a phased deployment to all customer boxes early in each month.

For our customers, this “In The Boxing Ring” newsletter is used to keep you informed as to what we have been doing for you, and what you can expect in the upcoming patch Tuesday monthly feature / enhancements release.

Conclusions

Thank you for your support of Network Box, and the continued entrustment of your network security to our managed service. I hope you find this communication useful – if you have any suggestions, they are most appreciated, and should be directed towards your local NOC or account manager; please don’t hesitate to contact us for assistance.

Mark Webb-Johnson
CTO, Network Box Corporation
September 2008

AUGUST 2008 NUMBERS

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>1,850</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>465,816</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>571,739</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>119,521</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>107,032</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>7,604</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>40,944</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>2,351,496</td>
</tr>
</tbody>
</table>

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jasmine Arif
Jason Law
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
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 2736-2078
Fax: +852 2736-2778
www.network-box.com

Copyright © 2008
Network Box Corporation Ltd.