IN THIS ISSUE

2. FUZZY FINGERPRINTS
Fingerprinting is an effective technique for accurately identifying an individual. Fuzzy Fingerprints can automatically take into account subtle changes to the content of email messages and are effective in combating spam.

3. CHALLENGE/RESPONSE
Challenge/Response systems are an effective anti-spam technique for mailboxes experiencing an extremely high volume of spam - Network Box is introducing optional support for this technology as part of our Relationship system.

4. NOV 2008 FEATURES
The ongoing deployment of our recently released features, as well as up-coming public betas

4. PATCH TUESDAY
Network Box has moved to a patch Tuesday form of software enhancement release mechanism

Network Box Technical News from
Mark Webb-Johnson, CTO Network Box

Welcome

Welcome to the November 2008 edition of ‘In The Boxing Ring’. It has been a less stressful than usual month here at Network Box Security Response, as the onslaught of the Storm worm died down. All the threat metrics are down around 10-15% from the previous month’s highs - with the exception of URL Content Filtering Blocks (which are up a few percent).

We did see a small increase in NETBIOS probes (on ports tcp/139 and tcp/445), on the 28th and 29th October - most likely due to the MS08-067 vulnerability announced by Microsoft on 23rd October. Network Boxes, in their default configuration, will protect against this vulnerability; if you have any questions on this, please contact your local NOC for assistance.

We’re still working hard on preparations for our new Relationship and Box Office Customer Portal systems - beta tests for both of which are about to start.

We’ve also put the finishing touches on, and finished beta testing and preparations for deployment of, a new anti-spam technique known as fuzzy-fingerprinting. This will be released, to all customers, this coming patch Tuesday. I’ll be giving you a detailed explanation of this new functionality on page 2.

A lot of questions have come in concerning Challenge-Response, how the technology works and how it fits in with the Network Box Relationships system. I give a detailed description of this technology on page 3; as well as information on how Network Box can now apply it as a last line defense layer against spam.

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
November 2008
Fuzzy Fingerprints

In the real-world, a fingerprint uniquely identifies an individual. A fingerprint captured at a crime scene can be compared against a database of the fingerprints of known individuals; with a match uniquely identifying a single individual.

This has been applied to the world of computers as digital signatures. A digital signature is the result of a mathematical algorithm applied to some binary data. It can reduce large, complex data to a statistically unique number. Often, sizes of 128 or 256 bits are used and industry standard algorithms such as MD5 and SHA are available.

A digital signature is an excellent high-speed mechanism for uniquely identifying a piece of binary data. We can take a digital signature of a virus and store it in a database of known malware. Then, whenever we get a new suspicious attachment, we can compute the digital signature and compare it against the database. The advantages of such a system are speed (both the digital signature algorithm and database lookup are extremely fast, scalable and efficient) and simplicity.

However, there are times where we don’t want to identify an individual. We want to identify a trend, or aspect of some piece of binary data. We don’t want the fingerprint match to be exact - we want it to be ‘fuzzy’ (ie; to match objects close to, but not identical to, the original object we took the fingerprint of).

Spam Obfuscation

An example of this is with spam. Spammers have the ability to subtly alter every single email message they send out. They don’t send the exact same message to 100 million people, but instead send minor variations each time. This allows them to defeat digital signatures (which can only identify a unique message). Common techniques include adding gibberish text before, after or in-between (in html markup comments) the text of whatever they are promoting.

In such circumstances, taking a conventional digital signature of the email message, or even each part of it, is of no use. Each message sent by the spammer will have a unique digital fingerprint and there is no way to see them as one.

Strangely enough, a human could look at two such messages and consider them the same (and often would not even notice the differences - hence those games of ‘count the differences’ where you are presented with two pictures and have to find the differences). But computers are best at dealing with 1 and 0 - and are best suited to looking at differences (rather than similarities).

Anti-Spam Fuzzy Fingerprints

The solution to this problem is 'fuzzy fingerprints'. These work by dividing the message into blocks of text, removing obfuscation blocks (such as comments, markup, etc), mapping obfuscation characters (such as the letter ‘l’ and the number ‘1’), and finally taking a digital signature of the result. This resulting digital signature is ‘fuzzy’ in that it will match two or more different, but similar, text blocks.

Applying the above technique to a single email message will thus result in multiple fuzzy fingerprints - each of which can be compared against a database of known spam fingerprints.

Network Box Outbreak

Network Box have extended our Outbreak system (including all spam traps and customer-submitted spam samples) to support Fuzzy Fingerprints. The outbreak system now automatically generates fuzzy fingerprints from each email message it sees and correlates these fingerprints across all the spam and virus submissions it has seen. It then presents this to the security engineers, who can raise new signatures for new and emerging classes of spam/malware and PUSH out to our customer Network Boxes.

On the Box

On the Network Box itself, enhancements have been made to the mail scanning code to calculate fuzzy fingerprints for emails being scanned, and to lookup those fingerprints in the database of known spam.

Currently, we classify these fingerprints as either HINT (suspected spam) or BLOCK (known spam) and they are scored appropriately.

Performance

The calculation of fuzzy fingerprints, and lookup of those fingerprints in the database, has a performance impact for both cpu and disk.

However, in our testing, the performance impact of this is minimal and is more than offset by not having to run later (more cpu and disk) stages of scanning, in the case of a fuzzy fingerprint match. In our benchmark testing, this new tool has almost zero impact on anti-spam workload (but has a great benefit to performance and the ability to successfully detect spam).

Rollout

The Network Box Fuzzy Fingerprint Anti-Spam systems have been under testing for some three months now, and are performing well enough for global release. The new system has been shown to have a good incremental impact on certain types of spam (such as recruitment, phishing, pump-n-dump, hoaxes and viruses).

The new system will be rolled out to all customers, globally, on Tuesday 4th November 2008 as part of the patch Tuesday PUSHCODE update. This will not require any down-time for your users and will not require a reboot of your Network Boxes - so should have minimal impact.
There are many more such problems, but I am sure you get the idea.

**Network Box Relationships**

The Network Box Relationship system provides a database tracking who is sending what to who. It tracks the history (such as spam and virus rates) and establishes a trust relationship between the tuple of sender, sender attribute (such as IP address) and recipient.

The relationship database is an ideal foundation for a smart challenge/response system based on a full knowledge database.

**Network Box Challenge/Response**

The Network Box implementation of Challenge / Response is built on the Relationship system foundation. It can be selectively enabled either per-recipient or per-domain and is most suited to those mailboxes experiencing a very high volume of spam. The key points of the system are:

- An initial learning period is employed. During this time, relationships (such as who you are emailing) are learned before enforcement is enabled. This means that the majority of people you communicate with are already in the system, and don't need to be challenged when the system is enabled.

- The system fully conforms to RFC3834, to avoid email loops and problems with mailing lists and bulk emails.

- The system fully conforms to the industry standard 'best practices' for challenge / response systems - minimizing the impact to innocent third-parties.

- The system runs after conventional anti-spam and anti-virus. This means that it is an addition to the existing protection and there is no need to challenge the 95%-98% of spam, and almost 100% of viruses that are blocked by our conventional systems.

The system is purely targeting the small portion of non-ham that would otherwise get through. However, anti-spam aggressiveness can be tuned down once this system is enabled.

- The system is per-recipient, but supports 'introductions' - an outbound email to internal as well as external recipients is treated as an introduction by the database (establishing a relationship between the external and other internal recipients). The system is also optionally configurable to allow relationships to be shared on a per-domain or per-box basis.

- The system is fully integrated to Mail Portal. The web based UI allows recent challenges to be seen and manually released. The periodic email report shows challenges made (and responses received) and allows for click-and-release handling as necessary.

**Deployment**

We deploy challenge / response by first enabling outbound learning for a period of one-to-two weeks. This lets the system learn who is talking to who and build up its database of relations.

Once the database has been learning for some time, challenge / response can be enabled. The system will then start challenging previously unknown users. Network Box uses email-based challenges with clear descriptive text and full headers. The challenges are also issued in real-time (so when a previously unknown user emails you, they get an immediate challenge - increasing the likelihood of a successful response).

**Issues**

The primary issue still seen with the system is the large number of automatic responders not conforming to the RFC3834 standard. In such cases, a manual release may still be required - but the integration to Mail Portal makes this relatively painless. We continue to work on this aspect of the system (to add built-in exceptions for known non-conforming systems).
Nov 2008 Features

On Tuesday 4th November 2008, we will be globally releasing PUSHCODE for our mail scanning anti-spam systems. This new code adds support for fuzzy fingerprint detection and enforcement. See page 2 of this newsletter for more information on this important new functionality.

This work will not require noticeable down-time for your users and will not require a reboot of your Network Boxes - so should have minimal impact.

In addition, during November 2008, we will be expanding the deployments for our two current public betas:

- The Network Box Office Customer Portal (which runs in parallel with the current Box Office, so you will be able to switch between the two systems).

- The Network Box Relationship System is starting beta with deployment of Relationship Enforcement combined with Challenge-Response (for customers heavily affected by spam).

If you wish to participate in any of the above two betas, then please let your local NOC know. They will then contact you, nearer the time, with further details. We are still strictly limiting participation in these betas, to be able to closely work with the customers involved in this important work.

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

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
November 2008

OCT 2008 NUMBERS

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>1,472</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>216,447</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>555,029</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>96,698</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>88,849</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>3,394</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>46,682</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>2,342,150</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.