Welcome

Welcome to the October 2008 edition of 'In The Boxing Ring'. There is so much material to cover this month that we’re going to release this in two parts. This edition of In The Boxing Ring will provide details on the new Anti-Spam/Anti-Virus eMail systems about to enter beta-testing. At the end of this week (10th October 2008) we will release the second part, which will cover the new Network Box Office Customer Portal.

September was another busy month for Network Box Security Response; we were at Alert Condition 4 for most of the month, and only managed to relax that a week or so ago. The ongoing virus and spam onslaught from the Storm Botnet is still making headline news and driving anti-spam and anti-virus PUSH updates to an all-time high.

The Network Box Customer Portal project is now reaching its goals, and should start beta testing towards the end of October. This is a massive project, designed to take data from most of our internal systems (such as licensing, global network monitoring, inventory, deployment, ticketing, etc) and make them available to our customers in a single unified user interface (under the Box Office Customer Portal framework).

Last month I talked about ‘fighting a losing battle’ and promised more information in this October newsletter on the topic, and the Anti-Virus/Anti-Spam technologies that Network Box are developing in our on-going battle against email-based malware. You can find more information on pages 2 and 3 of this newsletter; where we present the techniques nearing release.

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
October 2008
Relationships

The Problem

In the September 2008 ‘In The Boxing Ring’ newsletter, I talked about how, 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 Network Box can do an amazing job at anti-virus (with PUSH updates to signatures, multiple engines, heuristics, policy blocks, etc) and we can achieve an almost perfect 100% success rate, our anti-spam success rate can never approach 100%. With current technology, if a customer gets 100 spams a day, 95->98 can realistically be detected and blocked, but that still means 2->5 spams a day getting through.

The resources, on the box, that we need to devote to anti-spam are also increasing day-by-day: millions of signatures, real-time DNS checks, multiple engines, thousands of regular expressions, OCR, etc. The end result is that benchmarking shows anti-spam takes between 7 and 10 times the resources of anti-virus.

So what is the solution?

When analysing spam, the single biggest thing that strikes us again and again is that there is one thing in common with almost every spam email:

I don't know the person that sent it to me.

The reason for this is clear (once you think about it): Spammers get email addresses by trolling websites, monitoring newsgroups, trojaned machines, buying lists from each other, etc. In all these cases, all they currently end up with is a basic list of email addresses. Each of these addresses is isolated, and the spammers do not currently have any notion of a "relationship" (i.e.; they have Joe's and Peter's email addresses, in amongst the 100 or so million others, but they don't know that joe sends email to peter).

The most viable long-term solution for effective anti-spam and anti-virus at the gateway is relationship enforcement.

What is Relationship Enforcement?

A relationship is an established connection between a sender and a recipient, based on pre-programmed or learned behavior. For example; relationships are often represented as a pair (sender and recipient email addresses). Other times, they may be a tuple (sender email address, recipient email address and sender location information).

Enforcement is actively blocking, delaying, or requiring a manual response. For example; with the SMTP protocol, we can drop / reject email, we can temporarily refuse to accept email, or we can quarantine and then challenge the sender to manually confirm their humanity.

Challenge-Response Systems

Challenge-response is a basic form of relationship enforcement. The problem with challenge-response systems is the poor response rate (even for human senders). Some reports put this at only 40% or less. People are scared to respond, and this means that once you turn on such a system you start losing mail (due to people wanting to contact you but being too scared/lazy to go through the hurdles of the response process).

However, the Network Box relationship enforcement system tackles these issues differently. By having a "learning" period, before "enforcement" is enabled, we have the ability to be more selective about who we have to challenge. Our relationship enforcement system has the ability to operate without challenge response, but can benefit from it for the last 1% of cases.

A Personal Test

I get a lot of spam. Some of my email accounts have been in use for more than 20 years, and are on countless mailing lists and web sites.

My email accounts are protected by Network Box, with spam and virus quarantine turned on, and I use Mail Portal to manage this all. On an average day, I get about three hundred spams and half a dozen viruses sent to me in eMail. The anti-virus is essentially 100% effective, and anti-spam runs at around 98% effectiveness. On an average day, that means I get about half a dozen spams though (and 294 blocked). Not had, but still aggravating to have to deal with on a daily basis.

Two months ago, I turned on Network Box Relationship management for all my email accounts. The box immediately started to learn who I was corresponding with, and after a couple of days of learning (I was impatient!) I enabled enforcement. The end result: in two months I haven’t received a single spam email through my Network Box.

I have had to deal with the occasional problem (normally old friends sending me email out of the blue) - but the tight integration to Mail Portal keeps this painless - one click and the email is released from quarantine to me; and the new relationship is learned so it won’t happen again.
Network Box Relationship Management

Network Box is now in the final stages of the testing and release of our relationship management system. We should be ready to start public beta tests towards the end of October, with a view to formal release (and offering this on a global basis) during November 2008.

The relationship management system works as follows:

1. A central relationship database is maintained. This database stores relationships for all email accounts managed by the Network Box.

2. The relationship is defined as sender + recipient + type + score.
   - Sender is the sender email address + attributes. Attributes include IP address, network address, country, reverse-IP domain, and others.
   - Recipient is the recipient email address.
   - The 'type' describes the relationship detail and identifies how the relationship was established.
   - Score indicates the trust and strength of the relationship.

3. The sum of all the scores for all detail records make up the total relationship score for that sender and recipient.

4. The system always learns.
   - If I send an email outbound from A to B, it will create (or strengthen) the score of the reverse relationship (sender B, recipient A, detail type "outboundemail").
   - If someone goes through a challenge successfully, that relationship will be strengthened.
   - If someone sends me an email from the same IP or country, that relationship will be strengthened, etc.

5. The system, when moved into one of its "enforcement" modes, has the ability to enforce relationships. It makes this decision based on its configuration, the score, and detail records. The enforcement options include:
   - challenge-response
   - spam quarantine
   - policy quarantine
   - temporary deferment

6. The relationship database becomes a valuable database of historical summary information. For example, if an exe file comes in, we can look at our previous relationship with that sender (email address, domain, country or IP address) and decide the likelihood of a virus.

7. The relationship database can be queried and tuned (in real-time) by the NOC, Administrator (via my.network-box.com) and end-user (via Mail Portal). It is a dynamic database; with relationships continuously created, strengthened and weakened by messages passing through the mail system.

8. The case of sender and recipient email addresses being in the same domain (or set of local domains) is problematic and handled by special algorithms. In particular, support for sender address verification is advised in order to be able to determine forgeries with 100% effectiveness.

9. Similar to the way that credit card companies use "exception correlation", we correlate relationship information. If I use my VISA card to buy a ROLEX watch in Yugoslavia (where all previous transactions are in the UK), VISA may temporarily refuse authorisation (or challenge) the transaction. Similarly, if I always get email from a colleague in Hong Kong, and now suddenly email from him is coming from Yugoslavia, I can reasonably defer (or challenge) the transaction.

10. The system, when moved into one of its "enforcement" modes, has the ability to enforce relationships. It makes this decision based on its configuration, the score, and detail records. The enforcement options include:
    - challenge-response
    - spam quarantine
    - policy quarantine
    - temporary deferment

A word on Reputation

There is an alternative system to Relationships, called Reputation. This involves maintaining a database of reputations of various senders. Many anti-spam vendors have hyped this approach in recent months, although it is actually a very old technique. A Real-time Black List (RBL) of source IP addresses is one such basic Reputation system.

The Network Box Relationship system goes beyond basic Reputation, to include the recipient in the formula (and to include mechanisms to apply attributes to the sender’s email and IP addresses).

Conclusions

No anti-spam or anti-virus system can ever be 100% effective. However, we know that Relationships will take us a huge bound in that direction. It will also lay the foundation for inter-box relationship sharing.

Over the past four months of testing, the relationship enforcement system has been found to be close to 100% effective against current spam techniques, and resilient to changes in approach by the spammers.

Regarding effectiveness with anti-virus, we need more data to be sure of the effectiveness. Already mass-mailing worms forge sender and recipient as email addresses found on the same infected computer, so there is a possibility that the recipient will have an established relationship with the sender (weakly, missing IP address, if the sender is forged, but strongly if the sender is just the configured email address for that infected PC or email server). Our relationship enforcement system is helpful in some of these cases, but no substitute for strong executable attachment policy enforcement (with per-user white-lists of policy blocks).

For the Network Box, relationship enforcement adds minimal overhead (and actually reduces overhead in some cases). For the spammers, they will have to redesign their entire database system.
Oct 2008 Features

On Tuesday 7th October 2008, we will release minor enhancements and bug-fixes to the web-proxy and content filtering systems. These new packages will be deployed, globally, and made available to all our customers, early in October 2008. 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 October 2008, we will be starting two public betas:

- The new Network Box Office Customer Portal will be ready for limited public beta towards the end of October (with a full launch expected during November 2008). The new system runs in parallel with the current Box Office, so you will be able to switch between the two systems.

- The Network Box Relationship System will be ready for limited public beta towards the end of October. We will be starting these betas with deployment of Relationship Enforcement combined with Challenge-Response (for customers heavily affected by spam), and will then be expanding this to the other functionality.

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.

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
October 2008

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>1,536</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>288,112</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>582,400</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>109,151</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>100,254</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>3,655</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>44,647</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>2,576,902</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.