IN THE BOXING RING

Welcome

Welcome to the December 2008 edition of 'In The Boxing Ring'. With the shutdown of the McColo hosting service, in mid-November, the world saw a dramatic reduction in spam and malware volumes. Why is this, how will it affect you, what was the impact and what does the future hold in store? I’ll be discussing these questions, giving some background information on ‘botnets’ in general, and presenting my opinions on page 2 of this newsletter.

During November, we continued to monitor significant malicious activity on NETBIOS ports (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, and on page 2 of this newsletter I’ll give some more information on this threat and recommended preventative actions you can take to minimize the possibility of a problem to your systems.

The Network Box Global Monitoring System (GMS) is a key foundational component for our ability to monitor and respond to problems in service delivery. Over the past few months, a lot has been done towards extending this system ‘into the enterprise’, improving its performance, and mirroring the data for presentation to our customers. In this edition, I devote a full page towards describing this system, how it works, and what it is doing. As the data from the system will become available to customers in the upcoming general release of the Network Box Office Customer Portal, it is important that you can see the source of this health and monitoring data.

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
December 2008
McColo Shutdown  

During October 2008, several Internet Security Researchers identified the servers hosted by McColo Corp (in San Jose, California, USA) as a major source of command-and-control of International Spam Botnets. On November 12th 2008, the Internet Connectivity to McColo Corp was cut by both its connectivity providers (Global Crossing and Hurricane Electric) - effectively disconnecting all the McColo Corp hosted servers from the Internet.

Since then, we have monitored a dramatic decrease in both Spam and Malware on the global Internet. The ‘In The Boxing Ring’ figure for October 2008 was 88,849 spams per box. The corresponding figure for November 2008 is 59,238 (a 33% month-on-month reduction). Looking at the daily figures for 12th and 13th November 2008, we see an even more dramatic reduction of close to 66%.

The global average number of Spam and Malware emails has dropped to about 1/3rd of previous levels, and the global percentage of spam in email has dropped from 58% to 42%. We have not seen any reduction in the level of malicious network probes or Intrusions (indicating that the McColo affect is limited to eMail based threats).

Network Box Security Response has been closely monitoring the situation since the shutdown of McColo, but we haven’t seen any resurgence of spam.

A Botnet is a collection of compromised computers, under the control of one individual / organization; often used for malicious or criminal activity. Each computer in the Botnet periodically connects back to a command-and-control system (either directly, or via some messaging system such as IRC) and listens for commands. Some of the largest Botnets, today, have more than 100,000 compromised computers and are used for such malicious activities as spam / malware distribution, and organized distributed denial of service attacks.

Targeting the command-and-control systems of Botnets (rather than the individual compromised member computers) is a new tactic, and appears to be highly effective (at least in the short term). By cutting off their control, the Botnet computers can only sit idle (without instructions as to what to do).

While the command-and-control systems of the botnets have been impacted by the shutdown of McColo, the botnets themselves are still in place and waiting for commands. It is uncertain how easily the affected spammers will be able to regain control of their botnets and resume their activity. While this is undoubtedly the largest such impact we have seen from enforcement activities against spammers, it is not a fatal blow and will likely only delay the spammers.

We saw 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, and this activity has been ongoing through October and November.

A lot has changed, in the windows world, over the past few years. With the introduction of a default-on firewall and removal of raw socket support in later versions of Windows XP service packs, we have seen the impact of such network-level worms reduce. However, this does not mean we can afford to be complacent.

While Network Boxes, in their default configuration, will protect against this vulnerability, we (as with other gateway defensive systems) can only effectively protect traffic that actually passes through the box. In such cases, it only takes one laptop to be unprotected, infected, and plugged into the LAN to infect all the other workstations and servers on the network. USB thumb-drives and hard disks are also equally vulnerable.

We recommend that windows users install the MS08-067 update as soon as possible, to protect against this (and other similar) threats. We also suggest that you verify this on all your Windows computers, by visiting Windows Update, and ensuring that you are up-to-date.
Global Monitoring System

In the October supplement to the “In The Boxing Ring” newsletter, I mentioned the Network Box Global Monitoring System (GMS) as a key component of the upcoming Network Box Office Customer Portal. I’d now like to take some space, in this newsletter, to give you some more information on this system and how it helps us to help you.

Historically, Network Box has relied on a network of regional network monitoring systems to monitor the health of boxes under our managed service. The system has been extremely successful, is doing what it is intended to do, very well, and has scaled to thousands of monitored devices. It has, however, some limitations:

- Each regional monitoring centre is independent (which offers great reliability, but limits our ability to monitor devices simultaneously from multiple centres).
- There is no clear definition of ‘reach-ability’, and there are issues with determining reach-ability in the cases where ISPs limit ICMP testing of their (or the customer’s) equipment.
- The system only monitors Network Boxes, and is not intended to monitor customer equipment.
- The monitor database is private, and cannot be published for customers to see their own status.

The Network Box Global Monitoring System (GMS) is intended to address these, and other, limitations. We are currently running both historical and GMS monitoring systems in parallel, and aim to phase-out the historical system (with complete migration to GMS) in the first quarter of 2009.

Within GMS, each box is a full capability monitoring system. Think of the box as a mini network management system. It has the ability to monitor its own services and performance metrics, as well as those of other configured devices (including customer equipment). The box maintains a database of health status, and reports changes back to Network Box using the same port tcp/4201 that it uses to report back health and statistics.

GMS employs a network of active monitoring stations, all centrally reporting back reach-ability status (including packet loss percentages and round-trip-times). In addition, each box monitors several Internet test points. By combining the reach-ability results from the box with the results from the active monitoring stations, we can determine (with high reliability) a global reach-ability status. This tells us whether the box is reachable (OK), has a link problem (NO-LINK: both the box and its gateway are unreachable) or is unreachable (CRITICAL: the gateway is reachable, but the box is not). The GMS supports multiple gateways, and is able to monitor health and reach-ability for multiple gateways per device.

In addition to the service health status, and global reach-ability, GMS also supports the monitoring of VPN links. It handles testing of IPSec, SSL client and SSL server VPNs, and supports basic UP / DOWN status results. These are then reported back to the central GMS using the the same tcp/4201 system used to send back health and statistics.

The health database from the GMS is made available to customers via the Network Box Office Customer Portal. Currently, we are offering visibility of box reach-ability (including global round-trip timings and packet loss to Asia, Europe and America), VPN status (for all fixed VPN links on IPSEC or SSL), and overall health service status. The system is integrated to the Box Office Ticketing system, for alerting customers to issues requiring their attention.

The GMS supports a flexible alerting mechanism. Initially, we are offering customer email alerts to reachability/service/vpn issues via the Box Office eMail notifications. However, this will be extended early on in 2009, to support per-user alert configuration and more options (such as short SMS alerts, and others). We have some very exciting developments in this area, that I should be able to announce to you next month.

While GMS supports monitoring of customer equipment (such as web servers, mail servers, LDAP systems, etc), we need to fully finalize the migration to GMS before offering that functionality to customers.

The GMS database is mirrored, in real-time, to Box Office regional mirrors. This provides fast access to local status, but also supports a global overview (for customers with boxes in more than one country / under management from more than one Network Operation Centre).

With the migration to GMS, Network Box is able to offer our customers access to a truly useful resource for ensuring network, equipment and service availability. We monitor more than 100 metrics for each Network Box device, and this system gives customers (and NOC engineers) a window into that status information, in real-time - and with a global overview for multi-box / multi-country customers.
Dec 2008 Features

On Tuesday 2nd December 2008, we will be releasing the Network Box Global Monitoring System (GMS) system to all our managed boxes, world wide. This system will run alongside our current monitoring systems, with a view to complete migration during Q1 2009. See page 3 of this newsletter for more information on this important new functionality.

We will also be releasing some enhancements to our mail disclaimer feature, to permit better compatibility and support for Lotus Notes mail clients.

Finally, there are two new small enhancements to the mail delivery and core api systems - to support revisions to challenge/response and email tracking. These revisions will require that the mail server on the Network Box be restarted.

Our new website www.network-box.com will launch on 2nd December 2008 - it should be live by the time you read this.

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.

This month is primarily a clean-up month, as we prepare for global release of the Network Box Office Customer Portal and relationship systems. It is likely that these systems will be ready for global release during January 2009.

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
December 2008