

In The Boxing Ring



IN THIS ISSUE

2. CONFICKER WORM

The conficker worm has infected an estimated 6% of computers, globally. In the final days of March, Network Box released a network scanner for this and we discuss its implications.

2. MY.NETWORK-BOX.COM CERTIFICATES

We've added a full certificate authority, as well as SSL VPN status and reporting, to the my.network-box.com administrative interface.

3. MAIL SCANNING

Several new modules have been added to to enhance scanning functionality and performance.

3. SENDER POLICY FRAMEWORK

SPF technology permits sender domain authentication for the SMTP protocol. Fully supported by Network Box, this useful technology is presented.

4. APRIL 2009 FEATURES

The ongoing deployment of our recently released features.

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

Welcome

Welcome to the April 2009 edition of 'In The Boxing Ring'. In this edition, the top story will be about the Conficker worm and the availability of a remote scan, from the Network Box gateway, for infected machines.

And in an industry first: we managed to ship this out-of-cycle on March 31st - just hours before the April 1st Conficker.C activation date. On that day, thousands of scans were run, by NOC staff operating 24x7, and the overall safety of our customers vastly improved.

This month, we have a very large number of software updates to be released, as well as a significant enhancement to the my.network-box.com administrative interface used to query, report on and control a Network Box appliance.

We are releasing both a full Certificate Authority (with hybrid NOC/ Customer control) and support for status and analytic reporting of SSL VPN connections. Turn to page 2 for details.

On page 3, I'll be presenting some enhancements made to the mail scanning framework and progress made against spam and malware from one particular botnet.

I will also be introducing you to Sender Policy Framework (SPF) technology - which is straightforward to configure, and I would recommend all our customers implement it.

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.

You can also keep in touch by following our new Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
April 2009

Network Box Wins PC3 Platinum Brand Award 2008

Network Box has been awarded the PC3 Platinum Brand Award 2008 for bringing consumers the best quality product of 2008.

Look for details in the May issue of In the Boxing Ring.



Conficker Network Scanner

The Conficker worm has been very prolific. Estimates of the number of computers infected range from almost 9 to 15 million computers; one survey reported infection rates at 6% of tested computers. While Network Box has both Anti-Virus and IDP signatures for all known variants of this worm, it can propagate using network vulnerabilities, network shares and USB devices – so it could infect your LAN/DMZ without the traffic ever passing through Network Box gateway protection.

Security analysis of the Conficker worm showed the payload activates globally on April 1st, 2009. In the last days of March 2009, three security researchers (Dan Kaminsky, Tillmann Werner and Felix Leder) identified a network signature for Conficker-infected hosts. In the words of Dan Kaminsky: "What we've found is pretty cool: Conficker actually changes what Windows looks like on the network, and this change can be detected remotely, anonymously, and very, very quickly. You can literally ask a server if it's infected with Conficker, and it will tell you."

Network Box Security Response immediately packaged up this scanning

technology in order to make it available to our customers before April 1st. We offered our customers a remote network scan from the Network Box at the network gateway. It would scan reachable workstations and servers on the LAN and DMZ networks. The scan attempts to connect to windows SMB ports (tcp/445) and issue SMB protocol requests to try to identify whether the host is infected or not. The scan can only test Windows hosts which are powered on, connected to the network, and reachable on tcp/445 from the Network Box.

Since March 31st, the scan has been run thousands of times with great success. We are pleased to say that it does not appear to cause any major problems on the network (other than elevated network traffic and connections). But, like all such active scans it could cause problems with the network services of workstations or servers on the network. The scan has identified several Conficker.C infections, all of which the publicly-available security tools have removed.

Please understand that such active network scanning is not a usual service from a perimeter protection device such as Network Box. However, due to the seriousness of the Conficker problem we are offering this service to you free-of-charge and on a 'best efforts' basis.

Worm:Win32 Conficker

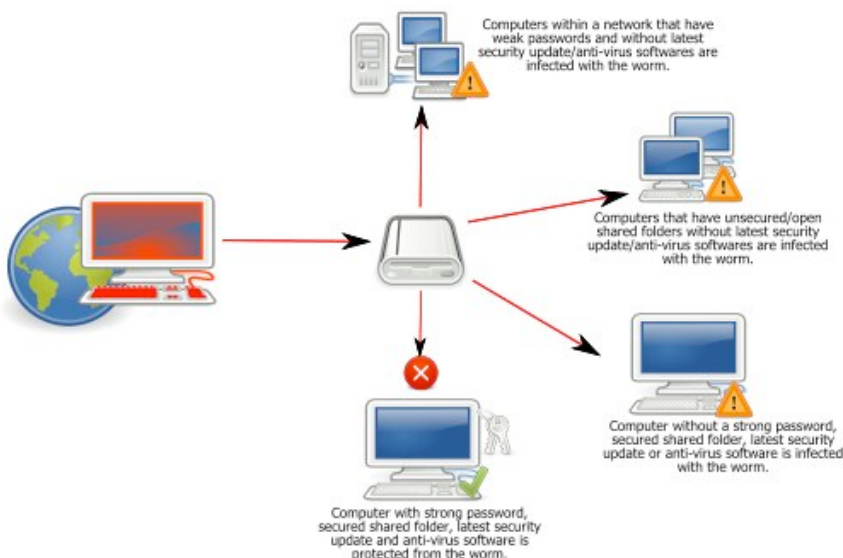


Diagram reproduced (with permission), Gppande, Wikimedia Commons



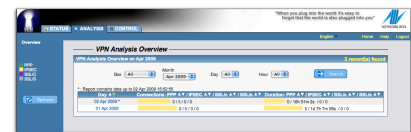
Certificate Authority and SSL VPNs



We've added a full Certificate Authority to the my.network-box.com administrative interface. You will be able to use this to issue certificates for use by the SSL VPNs.

The authority will allow you to issue and revoke certificates, as well as download them for your users. We've also incorporated Mail Portal as a mechanism to distribute certificates to your users.

You'll find the new functionality under ADMIN / CONFIG.



We've also added status and analysis reporting for SSL (client and server) VPNs into the VPN / STATUS and VPN / ANALYSIS modules. This support is included alongside the existing IPSEC and PPTP support.

The status screen allows you to see the status of all your VPNs, in real-time. For VPN servers, the status of each client VPN is listed.

On the analysis screen, you can see historical VPN connections, and analyse activity.

The control screen will also allow you to see the status of the SSL VPN services, and to stop and start as required.

Full NBGMS support is included, so you can see VPN status from the Box Office Customer Portal and the newly released iPhone / iPod Touch App.



Mail Scanning

Network Box Security Response has been tracking the emergence of a new variant of the DHL/FEDEX/etc. tracking style of malware distribution. We have globally released two new mail scanning modules (NBH-BGTRACK and NBH-BBADHDR) to detect and block emerging variants of these and other threats.

The NBH-BGTRACK heuristic module looks for suspicious characteristics of the emails themselves. It can block new emerging variants even without specific signatures.

The NBH-BBADHDR heuristic module looks for attributes of the botnet produced emails themselves (in particular relating to header formation and mechanics of the SMTP transaction itself) and is very effective at detecting new variants of messages from that botnet. In the first few hours of release, this module blocked more than 25,000 malicious messages from 16,000 sources. Because we are targeting aspects of the botnet, rather than the message itself, this heuristic is also extremely effective at detecting (and blocking) other messages produced by the same botnet (including 'pill' spam, Russian, Chinese and other malware spam).

Also, this month started the migration of a large number of anti-spam signatures to a new high-performance rules engine. The new engine is highly tuned and very selective in what signatures are run against what parts of the email (based on textual, message structure, content, heuristic and other in-depth analyses). The result is scan times are reduced and more email can be scanned with less CPU cycles – all with little impact on effectiveness.

Should you have any questions on these, or other, protection modules or mail scanning systems, please contact your local NOC for assistance.



Sender Policy Framework

Wikipedia defines this as *“Sender Policy Framework (SPF) allows software to identify messages that are or are not authorized to use the domain name in the SMTP HELO and MAIL FROM (Return-Path) commands, based on information published in a sender policy of the domain owner. Forged return paths are common in e-mail spam and result in backscatter. SPF is defined in RFC 4408”*.

The SMTP protocol allows any computer to send an e-mail claiming to be from anyone. Thus, it is easy for spammers to send email from forged addresses. This makes it difficult to trace back to where the spam truly comes from, and easy for spammers to hide their true identity in order to avoid responsibility.

Sender Policy Framework addresses this by allowing the owner of a domain to effectively list the addresses that emails from that domain are permitted to come from. It is implemented by publishing a TXT record, in a special format, in the domain being protected.

For example, here is the SPF record for network-box.com:

```
V=SPF1
IP4:218.189.244.64/27
IP4:203.174.43.16/29
IP4:202.177.22.160/27
IP4:203.198.45.104/29
?ALL
```

The record states that we are using SPF v1 and lists the four address ranges that mail comes from. It then states “?ALL” (which means that that list is not exhaustive and network-box.com email may also come from other addresses).

Now, when a mail server receives an email message from a user@network-box.com, it can look up the SPF record and compare the IP address the email actually came from with what is permitted. This can be used to determine (a) positively that the email came from one of the trusted addresses, (b) negatively that it was forged, or (c) neutral (no opinion).

Publishing a “?ALL” style SPF record is not hard, but means that when someone receives email from one of your listed addresses, they *know for sure* that it came from you. If they get email from another address, the result is “neutral” (no better or worse than having SPF at all). To publish a “?ALL” record, you just need to list where the majority of your outbound mail most likely comes from.

Publishing a “-ALL” record may be more restrictive - but offers the dramatic advantage that you are listing 100% of the addresses your mail comes from. Recipients using SPF can positively determine whether the email came from you or not. They can detect forgery and this will lead to reduced backscatter and overall better domain protection.

To publish a “-ALL” record, you need to make sure that all your outbound mail goes through the listed servers. Network Box can assist with this, by using SMTP AUTH or VPNs for road warriors, and SMTP mail routing rules in the case of multiple sites.

Here are some useful links for publishing such records:

The Kitterman site has a good SPF record tester (which you should use before publishing the record live):

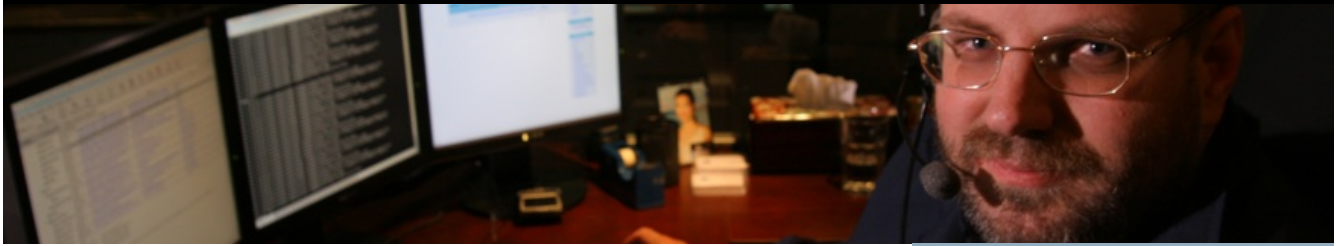
<http://www.kitterman.com/spf/validate.html>

The OpenSPF site is the home page for SPF and has tools to help you build SPF records:

<http://www.openspf.org/>

Overall Internet statistics estimate SPF usage at 9.9% of domains. Approximately 10.3% of Network Box customers publish useful SPF records on their domains, so we are ahead of the pack but could do better.

We looked at SPF enforcement, and its affect against spam, and found the rate to be at least 1.4% of March spam could be dropped at pre-envelope scanning stage by SPF.



April 2009 Features



On Tuesday 7th April 2009, we will be releasing a large number of bug fixes and enhancements for NBR3-3.0.

These changes include:

- Full Certificate Authority in the my.network-box.com administrative interface.
- Support for SSL VPN status and analysis reporting in the my.network-box.com administrative interface.
- New housekeeping, logging and mail scanning code, offering both functional and performance enhancements.
- A dramatic speed increase in the web proxy policy engine, to allow faster logging – even under extremely high workload.
- Several improvements to the my.network-box.com User Interface, to improve the look-and-feel and the performance/compatibility. We have also added support for the newly released Internet Explorer v8 browser.

The above changes will not require any impacting service or device restarts, and should not cause any significant interruption to device operation. The regional NOCs will be conducting the rollouts of new functionality in a phased manner.

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

April Hint



Network Box now has an iPhone / iPod Touch App. Due to be released April 7th, 2009, you'll find it on all the worldwide Apple App Stores. You can download and install it onto any v2.2 Apple iPhone or iPod Touch device.

The App offers mobile access into the Network Box Office Customer Portal and has the ability to manage box inventory (including health, contracts, VPNs, and reachability, etc.) and ticketing (view, create and respond to tickets).

Free of charge to Network Box customers, the App also provides a screen showing the top issues from the Network Box Security Response website.

Enter your Network Box Office username and password, choose the mirror <https://beta.boxoffice.network-box.com/> and you'll have access to your Box Office boxes and tickets.

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
April 2009

MAR 2009 NUMBERS

Key Metric	#
PUSH Updates	1,386
Signatures Released	242,326
Firewall Blocks (/box)	568,147
IDP Blocks (/box)	123,231
Spams (/box)	54,882
Malware (/box)	821
URL Blocks (/box)	53,925
URL Visits (/box)	2,535,093

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Pauline Chiu
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 © 2009
Network Box Corporation Ltd.