Welcome

Welcome to the July 2012 edition of ‘In the Boxing Ring’.

This month, on pages 2 and 3, we present details on Engines, Signatures and Heuristics.

Engines and Signatures can be thought of as two of the most important weapons in the fight against malware, but they are not the complete solution. As with a conventional war, tanks and artillery are powerful weapons, but they are not much use against spies. For that, we need something more targeted, and that is where the Network Box Z-Scan and Heuristic engines step in.

As a managed service Network Box is obligated to install the box, get it working and keep it working to you, the customer’s, satisfaction. That is, quite simply, the Network Box difference.

Page 4 details the features and fixes to be released in this month’s patch Tuesday for NBRS-3.0. We continue to develop, and will continue to support, NBRS-3.0 for the foreseeable future (several years), and this page will be used to keep you informed as to what is happening with our core product.

You can contact us here at HQ by eMail (nqh@network-box.com), or drop by our office next time you are in town. You can also keep in touch by several social networks:

Twitter:  http://twitter.com/networkbox
Facebook:  http://www.facebook.com/networkbox
           http://www.facebook.com/networkboxresponse
LinkedIn:  http://www.linkedin.com/company/network-box-corporation-limited
Google+:  https://plus.google.com/u/0/107446804085109324633/posts

Mark Webb-Johnson
CTO, Network Box Corporation
July 2012
Engines vs Signatures vs Heuristics

Engines and Signatures

As I write this, it is already out of date, but here are the current (3rd July 2012, @9:30am) counts for the number of signatures and engines in the Network Box NBRS-3 product:

For up-to-date figures, see http://response.network-box.com/protection

Those are pretty impressive numbers. For anti-malware, we’ve got 16 engines and are approaching 10 million signatures. Think about it - those are identification signatures uniquely identifying close to 10 million individual malware threats. Ten years ago, that number was 30,000.

Overall, we’ve got 78 protection engines containing more than 74 million signatures, all being applied to the problem of scanning your network traffic and stopping the bad stuff.

In the world of threat protection, as a baseline, the number of engines really does equate to breadth of protection offered, and the number of signatures to the depth of protection.

Given the amount of snake-oil being peddled out there in the wild west of the Internet, when conducting a baseline comparison of threat protection systems, we encourage you to ignore the hype and compare the base numbers - they’ll give you a pretty good indication of what is being protected against by who.
Heuristics

Engines and Signatures can be thought of as two of the most important weapons in the fight against malware, but they are not the complete solution. As with a conventional war, tanks and artillery are powerful weapons, but they are not much use against spies. For that, we need something more targeted, and that is where the Network Box Z-Scan and Heuristic engines step in.

Z-Scan is Network Box’s multi-award winning zero day anti-virus solution. Typical anti-virus industry practice is to release malware signatures to clients three to 12 hours after a virus first appears. With Z-Scan, however, the signature cycle is so greatly reduced because virus samples are obtained in real time from more than 200,000 traps in the cloud, poised 24/7 for virus attacks to occur. While Z-Scan is signature based, the creation of those signatures is fully automatic and based on powerful cloud-hosted heuristics. Z-Scan is so powerful that the number of signatures maintained is tiny compared to traditional approaches. Its focus is purely on very recently emerging in-the-wild malware. Typically hovering around the 100,000 signature level, we regularly purge Z-Scan signatures more than a day or so old - to keep Z-Scan lean, mean and as high performance as possible - as traditional signatures are released, the Z-Scan signature can safely be removed.

Beyond Z-Scan, we enter the world of heuristics. Here, computer algorithms are applied to look at both the makeup and actual running code of executable programs - to determine if the program is malicious in nature without the requirement for a specific identification signature. This technology is particularly important for, and effective against, emerging web-based threats, and again Network Box employs industry leading heuristic engines.

Conclusion

Since its formation, more than 10 years ago, Network Box has been concerned with the protection and online safety of our customers, not merely selling boxes. While our competitors will sell you a box, and quite literally walk away - as a managed service Network Box is obligated to install the box, get it working and keep it working to you, the customer’s, satisfaction. That is, quite simply, the Network Box difference.

We’ve been doing this, day-and-night 24x7x365, for more than 10 years now, and to this day we remain 100% focused on the threat protection problem. Thank you for choosing us, and helping us to do what we do best - so that you can continue to do whatever is it that you do best.
**July 2012 Features**

On Tuesday, 3rd July 2012, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Enhancements to various internal NOC systems
- Changes to the display of 'license expiry' data and information in my.network-box.com, to reflect the Box Office contract in place.
- Enhancements to mail scanning anti-spam, for recent cases of .in and .ru domains being abused.
- Further support for NBRs-5.0 in Box Office systems
- Various (mostly internal) enhancements to Box Office and support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

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

**NETWORK BOX | ISO Certification Upgrade**


For our Security Operations Centre to upgrade to the latest ISO standards, took an enormous amount of work, involving a great number of our people, all of whom had to put in a huge amount of effort for a very significant period of time.

Without doubt, this is a milestone achievement. Network Box now not only has the latest triple ISO certification for its Security Operations Centre, but offers the only IPv6 Core Phase-2 certified managed security platform, as well as the only managed security service which can be monitored and managed from a secure Apple iPhone / iPod Touch / iPad HD app.

Network Box is truly leading the world of Managed Security Services.

For more information on Network Box, please see [www.network-box.com](http://www.network-box.com).