Welcome

Welcome to the January 2010 edition of ‘In the Boxing Ring’. In this edition, I’ll focus on presenting a summary of the threat landscape in 2009, as well as what Network Box has delivered to its customers in the past year.

On page 2, we discuss the threat numbers for 2009. Network Box Security Response monitors and manages thousands of devices around the world, and this gives us an excellent view on the threat landscape. Here at Network Box, we strongly believe that only by being able to clearly see and measure a problem is the solution achievable (and gains measurable).

On page 3, we turn to look at the software enhancements and features delivered in 2009 and planned for 2010.

On page 3, we also leave space to discuss an important change to the Network Box recommended default policy regarding SCRIPT, IFRAME and OBJECT tags in eMails. Please take the time to read and understand this change, and discuss any special requirements you may have with your local support NOC.

Page 4 details the usual monthly features summary and January hint.

As usual, if you have any feedback, or comments, they are 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 Network Box Security Response twitter feed at:

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
January 2010
2009 Threat Round-Up

In 2009, Network Box Security Response PUSHed out 14,969 updates, totaling 2,905,697 signatures (down 10.0%, and up 6.9% respectively, compared with 2008).

That is approximately one new signature every 10.8 seconds.

Note: As the above figures only include signatures PUSHed to customer Network Boxes (and exclude cloud-based services), with the obsolescence of NBRS-1.1, and movement of several signature types (primarily including anti-spam and content-filtering) to ‘in-the-cloud’ approaches, the true growth of PUSH signatures is not clearly reflected.

Growth rates for anti-virus signatures continue to accelerate the greatest. Looking at just Anti-Virus updates (see chart, below), we see the dramatic growth that started in the second half of 2008 continues to accelerate, and we expect this to continue throughout 2010.

In 2009, the average Network Box blocked 5,854,972 attacks using firewall technology, and 1,572,211 attacks using IDP technology (up 19.8% and 47.9% respectively, compared with 2008).

The biggest change we have seen in 2009 is the movement from a threat landscape primarily composed of mass-mailed spam and malware to one of targeted/mass vulnerability exploit. Executable filters (such as that offered by Network Box) have grown so effective that the ‘black hats’ have changed tactic to exploiting vulnerabilities in applications, web browsers and servers (rather than just mailing out executable code).

The primary motivation for these ‘black hats’ has also moved from ‘fun’ and personal gratification, to commercial monetary gains. Nowadays, taking over a website or workstation (whether for further malware distribution or establishment of botnets) has real monetary value and more and more large criminal gangs are becoming instrumental in this lucrative business.

We expect this to continue throughout 2010 and beyond.

In 2009, the average Network Box blocked 821,983 websites due to company content filtering policy enforcement, with 27,132,231 website URLs visited over the year (up 131.7% and 37.9% respectively, compared with 2008).

These statistics clearly show the increased pressure IT systems are facing with respect to bandwidth and web usage, as well as the reaction of increased enforcement of content filtering policies. We’re seeing more than double the number of policy enforcement blocks than we did last year.

For 2010, Network Box Security Response will continue to work on staying on top of the anti-virus and anti-spam situation. However, increased emphasis will also be put on the vulnerability side of the problem.

With partnerships such as Microsoft’s MAPP, new products such as the NBIDPS system, and more offerings in vulnerability scanning, Network Box will continue to work on protecting our customers’ networks.

<table>
<thead>
<tr>
<th>Network Box Threat Statistics</th>
<th>2008</th>
<th>2009</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>16,636</td>
<td>14,969</td>
<td>-10.0%</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>2,718,770</td>
<td>2,905,697</td>
<td>+6.9%</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>4,885,567</td>
<td>5,854,972</td>
<td>+19.8%</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>1,063,056</td>
<td>1,572,211</td>
<td>+47.9%</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>976,374</td>
<td>621,302</td>
<td>-36.4%</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>35,044</td>
<td>20,251</td>
<td>-42.2%</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>354,757</td>
<td>821,983</td>
<td>+131.7%</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>19,668,707</td>
<td>27,132,231</td>
<td>+37.9%</td>
</tr>
</tbody>
</table>
2009 Enhancements

We started 2009 with a Q1 emphasis on our highly-effective eMail relationship system, with the introduction of spam score adjustments based on eMail relationships. We also continued our work on evangelising proper use of whitelisting, SPF and effective outbound policies.

In Q2, we took an active approach to the problem of Conficker, by offering remote vulnerability scans of our customers’ networks from the Network Box at the gateway. This sort of pro-active scanning technology was a first for Network Box, and forms the basis of further service offerings to be announced in 2010 Q1. By detecting known vulnerabilities, and assisting customers with their own patch deployment programs, Network Box can assist our customers to be more pro-active with the protection of their network (by addressing the core vulnerabilities rather than waiting for exploits to arrive).

The summer (late Q2, early Q3) saw the release of the Network Box customer portal, giving our customers a window into several Network Box internal systems. This system provides real-time status of Network Box devices under our management, and allows for formalised two-way communication with the Network Box Network Operation Centres (NOCs) responsible for monitoring and configuration of the equipment and network.

Q4 saw the release of NBIDPS and the announcement of our partnership with Microsoft and their MAPP program. MAPP provides us with vulnerability information in advance of Microsoft’s monthly security update release to offer protection to customers efficiently and effectively. By receiving vulnerability information earlier, our clients benefit from additional possible improvements that provide security protection, such as Active Intrusion Detection and Prevention, as part of the Network Box managed UTM+ services. Partnerships such as Microsoft MAPP, Mitre CVE, and others, allows Network Box earlier and better access to information, and allows us to release earlier and better protection updates.

Q4 also saw the announcements of the availability of enhancements to support encrypted SMTP emails.

Throughout the year, numerous enhancements to the my.network-box.com administrative and Mail Portal user web interfaces were released. These included such features as remote shutdown / reboot, detailed network address information, DHCP lease status and information, trace route and ping test functionality, improved quarantine release, as well as support for an on-the-box SSL Certificate Authority fully integrated to the Network Box SSL, SMTP, SMTP, and using Mail Portal / eMail for certificate and VPN client distribution. This culminated with the September release of re-vamped web interfaces to improve performance and ease-of-use of these powerful web interfaces.

Throughout 2010, we intend to continue our enhancement work.

Default Policy Change

Since 2001, Network Box has recommended customers employ a default policy of blocking eMails with certain attributes (along the lines of an executable attachment blocks). These include:

- NBH-BHIDIFM hidden iframes
- NBH-BHIDOBJ hidden objects
- NBH-BHIDSCR hidden scripts
- NBH-BIFRAME iframes
- NBH-BOBJECT objects
- NBH-BSCRIPT scripts

Note: It has always been, and will continue to be, the customer policy as to what is blocked/allowed. Network Box merely enforces the customer policy.

Recently, this has become more of an issue as rich HTML emails are adopted by corporates, and the practice of forwarding website pages (rather than links) becomes widespread. We see more and more quarantine releases for these eMails.

Accordingly, on February 2010 Patch Tuesday, Network Box will be changing its default recommended policy, as follows:

1. For CAN-2002-1121, we will continue to recommend that message/partial be blocked by default.

2. For The IFRAME, OBJECT and SCRIPT blocks, we will change our default recommend policy from ‘block all’ to ‘block hidden’.

Customers who have not expressed a preference will have their policies migrated to the new default recommended settings. You can see your current policy under the Mail / Policy section of my.network-box.com.

If you have any questions on this, please contact your local support NOC for assistance.
January 2010 Features

On Tuesday, 5th January 2010, 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:

- Refinements to the logging system, to better handle logging of disconnections of VPN clients under some circumstances.
- Enhancements to the logging system, to better handle logging of mail client disconnections during scanning (but before final mail delivery).
- Enhancements to the health monitoring system, to include monitoring of sub-services such as individual VPN links and multiple dynamic routing protocol services.
- Minor fixes to the my.network-box.com administrative web interface, relating to trace web usage with extremely large log queries, web proxy config groups with large numbers of group members, and improved validation of *@*.domain.com anti-spam sender whitelists.

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.

January 2010 Hint

Software vulnerabilities don’t just affect Microsoft, and other popular software and platform providers are releasing security patches.

In the past year, several major software houses have announced critical vulnerabilities in their products, including:

- Adobe has announced multiple vulnerabilities in their PDF reader and Acrobat software systems.
- Adobe has announced multiple vulnerabilities in its SWF Flash software.
- Wordpress blogs have been susceptible to multiple vulnerabilities leading to administrative password compromise.
- Several major web frameworks (including the popular Drupal web CMS) have had numerous vulnerabilities leading to remote code execution and SQL injection.
- Web browsers such as Apple Safari, Mozilla Firefox and Opera all have had critical vulnerabilities announced.

The January 2010 hint is that it is vitally important that you review your policies and procedures for all software systems in use by your organisation, and not just Microsoft. Microsoft may be the biggest target, but it is not the only one.

Mark Webb-Johnson,
CTO, Network Box Corporation

---

DECEMBER 2009 NUMBERS

<table>
<thead>
<tr>
<th>Key Metric</th>
<th>#</th>
<th>% difference (since last month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUSH Updates</td>
<td>1,394</td>
<td>+11.9</td>
</tr>
<tr>
<td>Signatures Released</td>
<td>146,314</td>
<td>-38.0</td>
</tr>
<tr>
<td>Firewall Blocks (/box)</td>
<td>635,866</td>
<td>-1.1</td>
</tr>
<tr>
<td>IDP Blocks (/box)</td>
<td>177,906</td>
<td>-15.6</td>
</tr>
<tr>
<td>Spams (/box)</td>
<td>47,738</td>
<td>-26.4</td>
</tr>
<tr>
<td>Malware (/box)</td>
<td>1,956</td>
<td>-32.7</td>
</tr>
<tr>
<td>URL Blocks (/box)</td>
<td>104,333</td>
<td>+3.6</td>
</tr>
<tr>
<td>URL Visits (/box)</td>
<td>2,901,600</td>
<td>-9.0</td>
</tr>
</tbody>
</table>

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jason Law
Nick Jones
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 © 2010 Network Box Corporation Ltd.