Welcome

Welcome to the first edition of ‘In The Boxing Ring’. Timed to coincide with Network Box Patch Tuesday, and released on the first Tuesday of every month, this newsletter is my personal communication to you.

Here, I present a summary of recent noteworthy security events that Network Box Security Response has handled in the past month. I will also outline what features and functionality is being released; in order to address these, as well as future anticipated, threats, and to give you better control of your organization's network traffic.

Basically: to keep you informed as to what we have done for you, and to let you know what new things we are doing while managing your perimeter security.

As this is the first edition of these newsletters, we have quite a lot to catch up on, and a large amount of material to present. I apologize, in advance, for the length of this edition - I'll try to keep it briefer in future.

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
July 2008

Network Box Headquarters, Hong Kong
SPAM Back-scatter

The Back-scatter Problem

The core of the back-scatter problem is that it is trivial to forge the sender address of an email; as the standard email protocols provide no mechanisms to authenticate the sender's email address.

Spammers don't want to deal with backscatter, and they don't want complaints coming back; so they forge the sender address in spams they send out. However, while there are no truly standard and universal mechanisms to authenticate a sender's claimed email address, there are mechanisms to determine if an email address is valid or not. So, the simplest solution for the spammer is to forge the sender address to be not his own, but still a valid email address (or at least domain). The spammer simply chooses a random valid email address and uses that. If that random valid email address happens to be one of yours, however, the result is a huge amount of back-scatter (non-deliverables, vacation messages, etc) directed back to you. This can overload email systems and consume bandwidth and resources.

Legitimate NDRs

The actual messages that make up back-scatter are perfectly valid and conform to the Internet RFCs (standards). Most of these take the form of NDRs (Non-Delivery-Receipts). The Internet SMTP standards state that if a mail relay has already accepted, but cannot deliver, an email message, it should raise a NDR back to the sender (to inform the sender of the problem) and then discard the message. These NDRs are always in response to a message sent to the original, non-deliverable, recipient. They are never sent unsolicited. While there is no standard for the structure of the message, a common (and best) practice is to include a short non-delivery report, and then attach (or include) a fragment of the original non-deliverable message. To stop NDRs being raised for NDRs, the envelope sender for NDRs should always be the 'null' sender ("<>").

Network Box Protection

The key to controlling back-scatter is differentiating between legitimate NDRs and undesirable back-scatter. The solution is discovering if the original message, now reported as undeliverable, was actually sent out by the sender. Network Box offers protection, using the as_bounces scanning module, at two levels:

- For very coarse protection (usually during periods of extreme backscatter attack), Network Box offers a block-all NDRs filter (operating at an early stage of the full message scan). If enabled, all NDRs will be blacklisted as spam. This is extremely coarse and will block both valid and back-scatter NDRs.
- Network Box also offers a sophisticated mechanism for digitally signing all outbound messages (including signing on behalf of a group of Network Boxes). A mechanism is provided whereby the Network Box can scan NDRs for digital signatures and specific relay host entries, looking for evidence that the original message was outbound. Should this be found, we can permit the NDR through. Should it not be found, we can mark the message as spam. To use this feature, it needs to be enabled/configured and all outbound mail needs to go either through the Network Box or defined relays.

Conclusion

The problem with back-scatter protection is differentiating between legitimate NDRs and undesirable backscatter – and blocking the latter. The key to the solution is discovering if the original message, now reported as undeliverable, was actually sent out by the sender. The as_bounces scanning module provides this functionality, and is now available as standard in the Network Box NBRS-3.0 firmware.

SQL Injection Attacks

Mid-June, we saw a targeted SQL injection attack affecting a single box in Australia. The attack first identified a specific version and account of Microsoft IIS and SQL Server, and then delivered a complex encoded SQL Injection payload.

These forms of attack are extremely hard to stop at the gateway; as the attacks are application dependent and therefore generic IDP/IDS rules can provide only limited defense. While Network Box has a number of IDP rules in place, application level security (by way of strict input validation) is ultimately the only way to thwart these type of attacks.

In response to this heightened activity, Network Box Security Response developed two new IDP modules (named HTTP-S-SQLINJECT and HTTP-S-SQLINJWORM) to further improve our detection and protection abilities for generic and specific known SQL Injection threats. This new protection has already been released to all our customers running the current NBRS-3.0 firmware.

Then, June 20th, around midday GMT, we saw a dramatic increase in malicious activity. We recorded blocks (as HTTP-S-SQLINJWORM) across all continents and from over 40 source countries. A major botnet (with at least 4,000 compromised hosts) is responsible. In response to this activity, we increased our global threat level indicator to alert condition 3. We continue to closely monitor the situation, and will further refine and improve our protection signatures and heuristics, as necessary.

We do recommend that customers operating public web servers (in particular those accessible to the Internet) review the scripts and applications on their web servers to ensure that they are up-to-date and patched so as not to be vulnerable to this class of attack.
Anonymous Proxies

We have had reports from customers concerning ‘aggressive’ users attempting to use anonymous web proxies to bypass web proxy policies they consider restrictive (or a challenge).

SurfControl categorize such anonymous web proxies as ‘Proxies & Translators’. But, the problem is that these proxy sites are extremely dynamic; several new ones appear every hour. While SurfControl does an excellent job at categorizing (as ‘Proxies & Translators’) the sites listing these anonymous proxies, they quite simply cannot keep up with the new anonymous proxies themselves.

We have been conducting a beta test of a new database engine called NBCS. This will be released to all Network Box NBRS-3.0 firmware customers during July 2008, and is intended to supplement the URL categorization work done by SurfControl. This runs both before (allowing us to override) and after (allowing us to supplement) the SurfControl engine.

The first database category released under the new engine is a ‘Proxies & Translators’ category intended to supplement SurfControl’s efforts in this area – but with PUSH technology and 24x7 categorization of new anonymous proxies. During the beta test, we pushed signatures for more than 11,000 anonymous proxies; and we are currently pushing further signatures for an average of 47 new anonymous proxies each day. One interesting statistic that has appeared from this effort is that currently, 15% of newly announced anonymous proxies are not classified as an anonymous proxy (but are actually spyware, spam URLs, advertisements, and adult sites). The threat of these sites extends beyond policy avoidance.

As this new functionality will be available during July 2008, we suggest you contact your NOC with a view to discussing your handling of the ‘Proxies & Translators’ category, and your outbound (LAN->NET) policy in general.

Uncategorized URLs

One request we often receive from our customers is an explanation as to why URLs are ‘uncategorized’ and the reason why such a large proportion of web traffic is uncategorized by SurfControl.

The Network Box web proxy, using SurfControl URL, as well as our own, categorization technology, supports 57 categories. The database covers over 17 million web sites, 3 billion web pages, 70 languages and 192 countries. Over 100,000 new sites are added/re-categorized each week.

However, impressive as they are, those numbers are dwarfed by the sheer size of the Internet. A recent Netcraft survey sized the Internet at more than 155 million web sites – with more than 1.2 million being added each week. It is, quite simply, impossible to categorize the entire Internet.

Some suppliers are now offering dynamic content-based categorization technology – based on the concept of a computer algorithm ‘looking’ at a web page and deciding its category (rather than the Network Box / SurfControl approach of a human doing the same). Network Box has been evaluating, and closely watching developments in, this technology for some time now.

A recent evaluation of dynamic categorization algorithm incorrectly identifying 1 in 200 legitimate business sites as adult; a completely unacceptable false-positive rate, unsuitable for business purposes. We continue to review our strategy as the technology improves; and if it continues to improve at the rate we have been observing, it is likely that it will pass the threshold to be useful enough to offer to our customers sometime late 2008 / early 2009. But today, we do not consider this technology of significant benefit to the actual requirement of enforcing company policy in web browsing with minimal impact on traffic.

Along with our work on supplemental anonymous proxy categorization, we are launching (with the new NBCS engine, to all NBRS-3.0 firmware customers, in July 2008) a feedback loop to improve the situation with common and popular uncategorized URLs. The system operates as follows:

1. User visits an uncategorized website.
2. We collate, hourly, the top uncategorized websites observed.
3. We then sort the collated top uncategorized websites and rank them by relevance (including factors such as the number of visits to the site, number of visitors, and number of different devices that this URL was seen on).
4. We use a computer-assisted but human-driven, system to manually visit and expertly categorize these top uncategorized websites.
5. The resulting categorizations are packaged up and released to all Network Boxes, using NBCS.
6. We re-collate all the new top uncategorized websites, and the process repeats back at step 1.

This system provides for a very dramatic reduction in the number of uncategorized websites, over time.

An updated white paper (entitled ‘The Meaning of Uncategorized in Web Proxy’) is available to document these new technologies and how they fit into our content filtering offering.
July 2008 Features

On Tuesday 1\textsuperscript{st} July 2008, we will release the following features and enhancements, for all NBRS-3.0 Network Boxes.

- Periodic housekeeping enhancements, to support POP3 acceleration.
- Enhancements to our web proxy categorization engine; including the new NBCS engine.
- The anonymous proxy categorization NBCS database option for web proxy categorization.
- The uncategorized URL feedback loop NBCS database option for web proxy categorization.
- A change to the weekly report email encoding, to better specify the mime encoding of the email message itself and allow this to be better displayed in some mail clients.
- Support for the newly launched E-x series (E-1000x, E-2000x and E-4000x) Network Boxes.
- Various other minor enhancements affecting my.network-box.com, mail portal, and the front-panel display systems.

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

Patch Tuesday

Network Box has now 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 will be the first Tuesday of every month, and the first will be Tuesday 1\textsuperscript{st} 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 will be 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 entrusted 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