APR 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the April 2016 edition of In the Boxing Ring

Last month, the Internet was subjected to large volumes (and different types of) **Ransomware**, leading to Network Box to raise the threat level to 4. On pages 2-3 we discuss the measures you can take to ensure you are protected from these increased threats.

Following on from the main article, on page 4 we discuss the multi-layered approach to mitigate the malware variants that are executed from ransomware and phishing emails.

On pages 5–6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. Based on Sunset Policy, we will continue to support, Network Box 3 until at least late 2018.

Finally, Network Box was awarded a Grand Trophy and two Gold Awards at the Silicon Valley Communications Info Security Global Excellence Awards. In addition, Network Box was named a winner for the second consecutive year at this year's IT Innovations Awards.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2016

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

In this month's issue:

NETWORK BOX

SECURITY ALERT CONDITION:

THREAT LEVEL 4

The Internet is under attack.

There is serious malicious activity affecting Internet service globally.

Last month, due to the massive increase in the amount of **RANSOMWARE** on the Internet, Network Box Security Response raised its alert condition to **THREAT LEVEL 4**.

NETWORK BOX

Every few hours, there were new variations of delivery mechanisms for these ransomware. Most of it coming via email, using trojan downloaders to download the actual malware over the HTTP/HTTPS protocol, but Network Box Security Response also saw techniques such as advertising network compromise on popular HTTP/HTTPS web sites. *(Both the New York Times and BBC websites are well known examples.)*

In light of these threats, Network Box advises you to check your gateway security, and ensure that the following best practices are being followed. If they are not, you are kindly advised to follow them now.

1. The majority of this ransomware is coming in as trojan downloaders, or links, in emails. The email attachment contains just a downloader, and the malware itself is downloaded using the HTTP or HTTPS protocols. Accordingly, please ensure that both email and web traffic is scanned.

2. Due to the common use of the SSL encrypted HTTPS protocol for this, and other, malware, please also ensure that you are using HTTPS scanning for your workstations and servers, so as to protect your HTTPS traffic.

3. Network Box recommends that you follow our suggested policy of blocking executable attachments for incoming email.

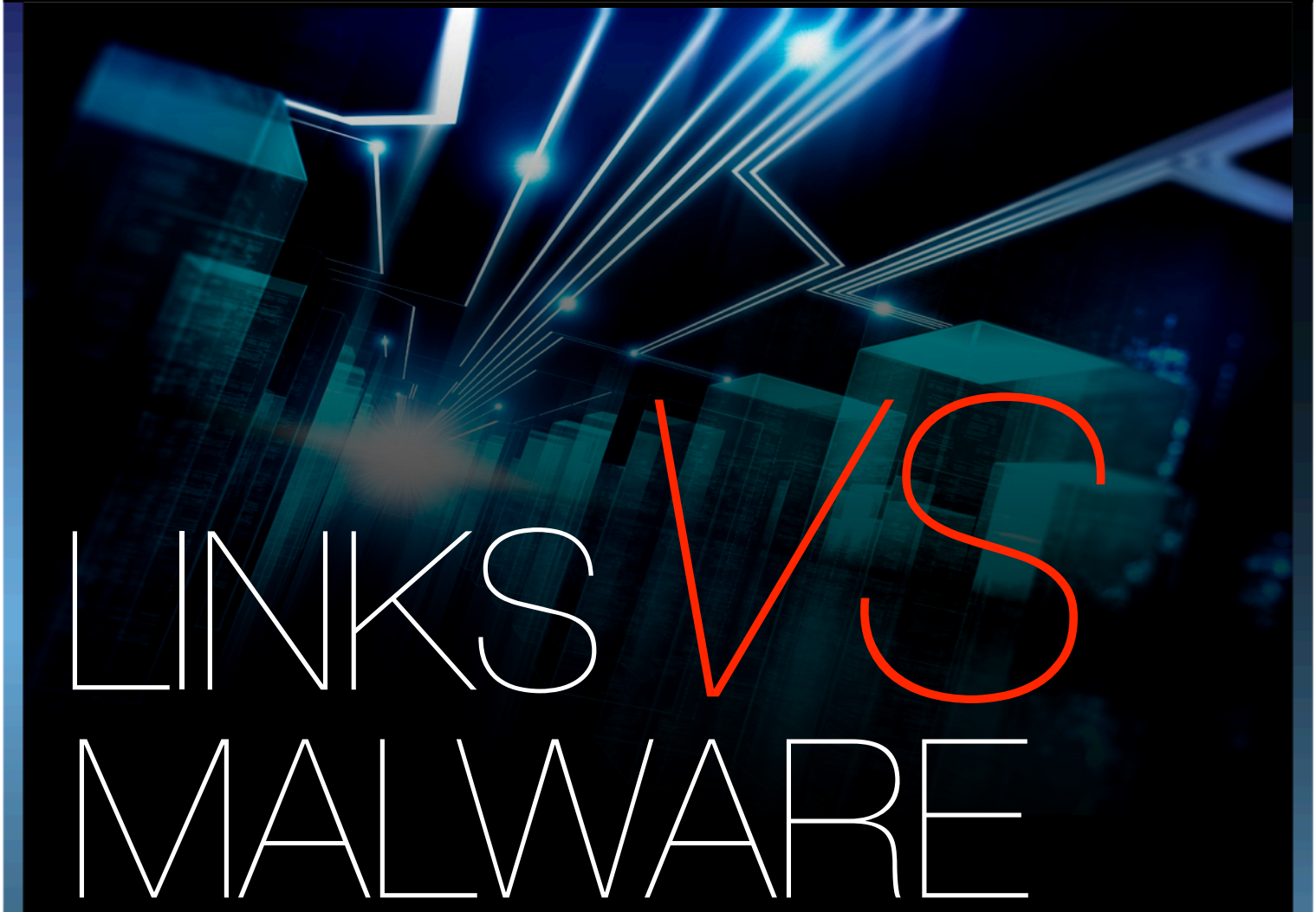
(All Network Box systems can do this, either by simple extension block, or by smart content recognition. The '.js' extension (javascript) should, in particular, be blocked as an email attachment. The Network Box 5 platform offers additional heuristics for detection of executable code in email messages, and we recommend all Network Box 5 customers to take advantage of this facility, as part of their default incoming policy.)

4. Often, email messages containing broken malware fragments will be blocked as spam. That is expected, and an effective anti-spam policy, to quarantine spam messages, should be enforced.

5. This is a good time to remind End Users not to open attachments in incoming emails, even if that email says it is from someone they know. Double-check with the sender, if you are not 100% confident.

Be suspicious, be vigilant, keep your data and systems safe.

NETWORK BOX



LINKS VS MALWARE

We are often asked why we can't just block links to malware. The answer is that while there is a limited amount of malware, the number of links and trojan downloaders is growing exponentially. Quite simply, it is hard to generate a new variant of malware. It is much easier to generate hundreds of thousands of unique links to that one single malware variant.

Most ransomware we see nowadays starts with an email. The email itself will be a short message containing either a link to an external site, or a small piece of script / office macro (the trojan downloader). Both the link and the script/macro operate in the same way - they download the malware executable usually using the HTTP or HTTPS (SSL) protocols.

Network Box offers, and recommends, a multi-layered approach to Internet perimeter security, best exemplified by our response to such malware.

- The original incoming email will be subjected to anti-malware and anti-spam scans. We'll catch the majority of them in this way, but we can never be 100% successful against such simple links/scripts in spam email. This is the first line of defence.
- The second line of defence is that a policy can be applied to incoming eMail, to block executable attachments. In most business use cases, you can simply block executable attachments, and then whitelist those senders you trust. This is affective against both script and office macro attachments.
- Should the email pass through and be read by a user, education is your third line of defence. Spend time talking to your users about this issue, and make them wary of clicking on links or trusting some random email that comes in.
- Should the user click on the link (or open the office document and enable macros, or execute the script), the network Box HTTP/HTTPS scanning forms the fourth line of defence. Again a full anti-malware scan is performed - but this time against the actual executable itself (not just the link to it).
- For users of the Network Box 5 system, a fifth line of defence is available in policy for HTTP/HTTPS downloads. Just like in emails, you can policy block executable code from being downloaded by your users.

Leveraging all these layers of defence is important to ensure a safe network. Nowadays, it is not sufficient to rely on just one layer.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th April 2016, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
April 2016

This month, for Network Box 5, these include:

- Include 'last update' column in NOC administrative console report for managed boxes.
- Improvements to multiple box selection and maintenance for NOC administrative console.
- Performance improvement in signature push system.
- Improvements to performance and reliability of database query system.
- Enhanced configurable logging limits in network firewall.
- Enhanced configurable logging limits in network frontline intrusion prevention.
- Enhanced configurable logging limits in network infected lan.
- Introduction of an optional bridge routed mode in base network layer.
- Change memory display on LCD front panel to show percentage used.
- Support for SMTP authentication option added to mail server module.
- Improvements to translation in long wrapped headers of user and admin web portals.
- Improvements to icons regarding mail quarantining, to better reflect quarantine status.
- Reliability improvements to network trace route, to better reflect alternate route hops and route changes.
- Improved fine grained control of release and whitelist options for policy, spam, malware in user portal web interface.
- Change to use latest (rather than earliest) message for user portal security token.
- Include emails classified as executable, in user portal mail report.
- Improve compatibility between NBRS-3 and NBRS-5 anti-spam signatures.
- Improved detection and extraction of Microsoft Office textual content.

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 SOC will contact you to arrange this if necessary.

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

NETWORK BOX

Network Box 3 Features April 2016

On Tuesday, 5th April 2016, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office and Response web sites
- Various (mostly internal) enhancements to several internal 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 SOC will contact you to arrange this if necessary.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	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 2736-2083 Fax: +852 2736-2778 www.network-box.com

Silicon Valley Communications Info Security Global Excellence Awards 2016

Network Box won several key awards at the Silicon Valley Communications Info Security Global Excellence Awards 2016, held in San Francisco, USA. Network Box walked away with the **Gold Award** in the coveted categories of **Integrated Security & Unified Threat Management (UTM)** and **Security Products & Solutions for Healthcare**, as well as a **Grand Trophy** which recognizes overall outstanding leadership and achievement in information security.

LINK:

http://www.network-box.com/sites/default/files/files/Info%20Sec%20Global%20Excellence%20Awards%202016.pdf

INNOVATIONSPREIS-IT IT Innovation Award 2016

Network Box has received an Initiative Mittelstand INNOVATIONSPREIS-IT 2016 Award in the **IT Security** category. Several thousand companies submitted their innovative IT solutions for the coveted IT Innovation Awards 2016, and for the second consecutive year, Network Box has won the highly coveted award.

LINK:

http://www.network-box.com/sites/default/files/files/IT%20Innovation%20Award%202016.pdf