MAY 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the May 2017 edition of In the Boxing Ring

This month, we are releasing a releasing a specific content classification for **Encrypted eMails** for Network Box 5. This new classification gives the IT administrator fine-grained control by allowing them to define polices on whether to permit or deny encrypted content to enter their networks. This is discussed in detailed on pages 2 to 3.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Network Box is proud to announce that the company won *The Best Network Security Provider* at the **Capital Outstanding Enterprise Awards**. In addition, Network Box Australasia was at the **Cyber Law Conference** held in Wellington, New Zealand; and Network Box Hong Kong hosted a cyber security seminar for the **Hong Kong Management Association**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
May 2017

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

ENCRYPTED eMAIL

It seems that every few years spammers and malware writers circle back to trying the old ‘and the password is’ technique to get their stuff past content filters and protection systems. The technique normally involves an encrypted attachment to an eMail message, with the body of the message telling the user what the password is. The password is usually either plaintext or contained in an obfuscated image. In recent weeks, Network Box Security Response has seen an upsurge in such activity; primarily using encrypted Microsoft Office documents.

While Network Box obviously cannot scan inside such encrypted content, there is still a large amount of meta data around the content that can be used to detect malicious activity or spam. Things such as URLs, IP addresses, and textual content in the message itself.

We often also have plaintext content directories (while the content itself is encrypted, the directory is not).

For example, here is the directory listing for an encrypted ZIP file:

```
$ zipinfo  sample.zip
Archive:  sample.zip
Zip file size: 3492 bytes, number of entries: 3
-rw-r--r--  3.0 unx     2731 TX defN 17-May-02 09:54 file1.exe
-rw-r--r--  3.0 unx     2680 TX defN 17-May-02 09:54 file2.exe
-rw-r--r--  3.0 unx     1898 TX defN 17-May-02 09:54 file3.txt
3 files, 7309 bytes uncompressed, 2948 bytes compressed:  59.7%

$ unzip sample.zip
Archive:  sample.zip
[sample.zip] file1.exe password:
```

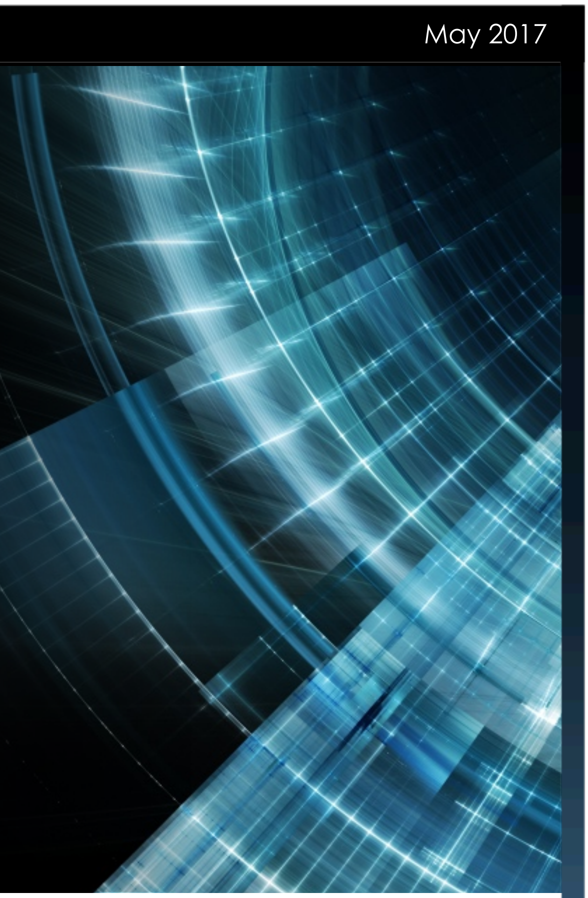
While the files inside the ZIP archive are encrypted, the directory listing is not.

This month, as part of the May 2017 patch tuesday, we are releasing a specific content classification for encrypted content in our Network Box 5 product. Our design guideline for this classification is to identify content that is encrypted in such a way that the content cannot be effectively and completely scanned. If such content is found, the mail message will be classified as 'encrypt'.

This new classification allows organizations to define a policy whether to permit or deny such encrypted content to enter their networks. This is a policy decision and it is common to deny encrypted content other than from specifically whitelisted senders. Remember that Network Box 5 is a content classification system; we classify the content, then apply organizational policy as to whether to permit or deny each classification. This new 'encrypt' classification fits nicely into this content classification system and allows for fine-grained control of such encrypted content.

Network Box 5

NEXT GENERATION MANAGED SECURITY



On Tuesday, 2nd May 2017, 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
May 2017

This month, for Network Box 5, these include:

- Improvements to logging to external syslog server over TCP/IP protocol
- Smarter truncation of long messages sent to external syslog server over UDP/IP protocol
- Improvements to Geographic IP mapping system (IP address to country/city)
- Introduction of an optional alternative (v7) network interface naming convention
- Permit configuration of source address parameter for network routes
- Support new 'encrypt' classification for eMail (indicates one or more message parts are encrypted)
- Improve display of system device attribute configuration
- Improve the section arrangement for configuration display
- Add support for transport mode in IPSEC tunnels
- Improvements to alignment of filter forms in the administrative web portal
- Improvements to table/chart interactivity in web portals
- Standardization on field naming for User/Entity in administrative web portal

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 ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box
Capital Outstanding Enterprise Awards 2017

Network Box has received the Capital Outstanding Enterprise 2017 Award for *The Best Network Security Provider*. This is the seventh Outstanding Enterprise Award that Network Box has received from Capital Magazine.

Network Box Managing Director, Michael Gazeley, collected the award on behalf of the company at the awards ceremony took place on 11 April 2017, at the Island Shangri-La, Hong Kong.

LINK: http://www.network-box.com/sites/default/files/files/Capital_Outstanding_Enterprise_2017_Award.pdf

Network Box Hong Kong
Cyber Security Seminar: The Vulnerability of Everything

The Hong Kong Management Association (HKMA) visited Network Box, for a talk on 'The Vulnerability of Everything.' As more and more smart connected devices are being installed in homes and offices, they are becoming vulnerable to cyber criminals and hackers. The talk highlighted the dangers, and how organizations can protect themselves from these vulnerabilities.

Network Box Australasia
Cyber Law Conference 2017

Network Box Australasia was at the Cyber Law Conference 2017, held in Wellington, New Zealand.

Organized by the New Zealand Law Society (NZLS), it aims to highlight the cyber risk for organizations and businesses, and to develop an understanding of the impact, and challenges they present.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Nick Jones
Kevin Hla
Production Support

Network Box HQ
Network Box USA
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 2736-2083
Fax: +852 2736-2778

www.network-box.com