

AUG 2017

# In the Boxing Ring

## Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

### Welcome to the August 2017 edition of In the Boxing Ring

This month, we discuss the growing issue of **Spear Phishing**. Since the early days of computer eMails, there has been spam, and one particular malicious form of spam is phishing. These are eMails that attempt to extract private information by deception and social engineering. The vast majority of these emails have been obvious to most, however, some are specifically targeted and composed to look like legitimate eMails, a process known as 'Spear Phishing.' This is discussed further 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 Germany signed a partnership agreement with Hannover-based cloud solution provider, **acmeo** GmbH, to offer cloud-based UTM+ protection to customers across Germany. In addition, Network Box was featured in various media outlets. You can find links to these articles on page 5.



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

You can contact us here at HQ by email ([nbhq@network-box.com](mailto: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>

**Linked in** <http://www.linkedin.com/company/network-box-corporation-limited>

**Google+** <https://plus.google.com/u/0/107446804085109324633/posts>

### In this month's issue:

2 – 3

#### Spear Phishing

Recently, Network Box Security Response has seen an upsurge in spear phishing attacks. On pages 2 to 3 we highlight the common patterns observed, and how to defend against such attacks. In the meantime, Network Box Security Response will continue to closely monitor the situation, track these attacks, and issue signature and heuristics for known patterns of attack.

4

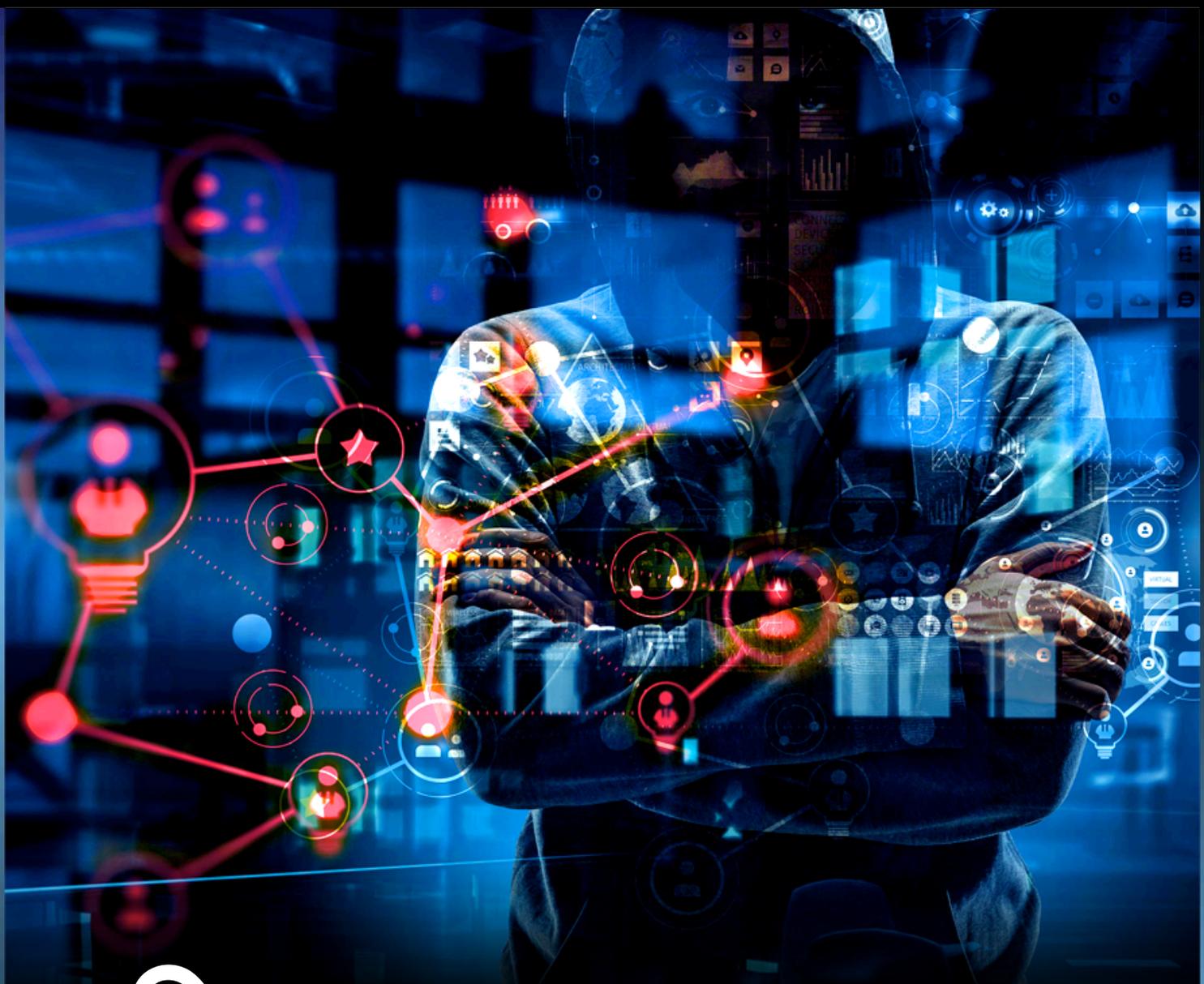
#### Network Box 5 Features

The features and fixes to be released in this month's patch Tuesday for Network Box 5.

5

#### Network Box Highlights:

- **Network Box Germany**  
acmeo Partnership
- **Network Box Media Coverage:**
  - ❖ *Global Cyberattack: What you need to know*
  - ❖ *Cyber Sleuths at Work*
  - ❖ *What is Ransomware?*



# Spear PHISHING

Since the early days of computer eMail, there has been spam, and one particularly malicious form of spam is *phishing* - attempts to extract private information by deception and social engineering.

The vast majority of these eMails have been obvious to most (and often the senders of these eMails make them obvious on purpose, to only solicit responses from the most gullible of recipients), but some are specifically targeted and craftily composed. These we call 'spear phishing'; while some cast nets wide into a sea, hoping to catch a random fish, spear phishers target one specific fish.

A spam/phish sender typically only has the recipient eMail address to work from, and relies on mass eMailing to get a response from a tiny fraction of recipients. But spear phishing works by the sender first identifying his target and gathering information to craft his attacks. Information such as names of executives, bank details, addresses and telephone numbers; all are commonly available on corporate websites, press releases, LinkedIn, Facebook, and Internet searches. As eMail sender addresses are typically trivially spoofed, given this information it is easy for the attacker to craft his eMail in a very precise way.

Recently, we've seen an upsurge in such attacks, and they are very hard to stop in any automated way. Patterns commonly seen are:

- ❖ The eMails are sent from compromised corporate computers never previously used for spam/phishing, with good reputation, and not listed in any blacklists. If you are going to this trouble to send a targeted attack, it is trivial to ensure that the address you use to send from is clean.
- ❖ The sender names are spoofed as high level executives in the target company. Most eMail clients nowadays adopt so-called 'smart addressing'; they don't show the sender eMail address, only the name presented. "Mark Webb-Johnson" not "mark@acme.com". Similarly, when replying to such eMails, only the name is shown not the address.
- ❖ The sender addresses are throwaway gmail or other public webmail style accounts. Attackers avoid using real eMail addresses in the target domain as (a) using gmail they can receive replies to intercept confirmation requests, and (b) they avoid any issues with SPF on the target domain.
- ❖ The recipients are accounts / Human Resources employees in the target company. Here, full names are used along with the correct matching eMail address.
- ❖ The messages use real names in greetings and sign-offs, and are perfectly written. Often, short-form names are used to further reinforce the deception (such as Mike instead of Michael, or Tom instead of Thomas).
- ❖ The messages usually contain either requests for information, or instructions to perform a bank transfer to a fictitious, but believable, supplier.

Defending against such attacks is not at all trivial. While eMail scanning (for malware, spam, known phish patterns, and policy enforcement) can go some way towards defending, such eMails are specifically manually crafted to bypass such defenses. The most effective defense is User Education (particularly for key individuals in your organization such as those listed on corporate websites). Train users to be suspicious of ALL incoming eMails, as well as how to use facilities in their eMail clients to check headers to see the real sender and other headers of incoming eMails.



Network Box Security Response continues to closely monitor the situation, track these attacks, and issue signatures and heuristics for known patterns of attack. In particular, we're in the process of conducting beta testing of new policy controls regarding recipient names and permitted address enforcement, with the intent to release this publicly in the August timeframe. We will keep you informed as this becomes available.

# Network Box 5

## NEXT GENERATION MANAGED SECURITY

On Tuesday, 1st August 2017, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

### Network Box 5 Features August 2017

This month, for Network Box 5, these include:

- Improvements to DNS server support for active interface configuration
- Performance improvements to SSL connection acceptance rate and latency
- Improved support for policy configuration of SSL/TLS version and cipher control
- Support deferred client reads after SSL/TLS SNI categorization is complete
- Separate the NETWORK and NAT configuration sections, for improved legibility
- Introduction of a proxy capability to support modification of eMail headers
- Support for X-Forwarded-Protocol header modification in Web Application Firewall
- Add support for destination port mapping in SMTP server transport maps
- Enhanced reporting on configuration change history (now including change detail)
- Improved charting of disk utilization in admin web portal
- Improved reporting on mail utilization summary, when filtered by classification
- Improve the display of 'Record not found' in KPI reporting
- Move 'Add' to top of ACL pages
- Improved user experience on admin and user web portal menus

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 Germany acmeo Partnership



Network Box Germany recently signed a strategic partnership agreement with cloud solution provider, acmeo GmbH. The partnership will focus on the distribution of cloud solutions for managed IT security. Network box and acmeo would primarily offer UTM+ (Unified Threat Management plus) services from the cloud as a unique channel model to address the SME market.

*"By partnering with Network Box, we are now able to offer our customers a UTM firewall, which they can easily integrate into their existing managed service portfolio without having to invest in deep technical know-how."*

Udo Schillings  
acmeo, Head of Marketing and Manufacturing Management

*"We see this cooperation very positively as we are very similar in our concepts and ideas. acmeo can now offer reliable solutions, especially in the area of managed security services, to secure and promote the trust of their customers."*

Dariusz Ansari  
Network Box Germany, Chief Executive Officer

### 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](mailto: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](http://www.network-box.com)

## Network Box Media Coverage

During the past month, Network Box was featured in various media outlets and publications.



### Global cyberattack: What you need to know

Michael Gazeley, Network Box's Managing Director, was interviewed about the PetrWarp Ransomware attack by CNN.

*"There obviously are companies that will have been affected by this in Asia," said Michael Gazeley, managing director of Hong Kong-based cybersecurity provider Network Box. "But the success levels are lower, as they're attacking the same vulnerabilities as WannaCry."*

**LINK:** <http://money.cnn.com/2017/06/28/technology/ransomware-attack-petya-what-you-need-to-know/index.html>



### Cyber Sleuths at Work

The HKTDC (Hong Kong Trade Development Council) interviewed Michael Gazeley about cyber threats to SME operations.

*"Everyone always looks at the last attack, but they should be looking at the next attack, and all possible avenues of attack. You can plan to be safe, or you can risk being a victim."*

**LINK:** [http://hkmb.hktdc.com/en/1X0AAQ3X/first-person/Cyber-Sleuths-at-Work?utm\\_source=enews&utm\\_medium=email&utm\\_campaign=hkmb-edm](http://hkmb.hktdc.com/en/1X0AAQ3X/first-person/Cyber-Sleuths-at-Work?utm_source=enews&utm_medium=email&utm_campaign=hkmb-edm)



### What is Ransomware?

In addition, Michael Gazeley, was interviewed by CNN to share his view on the recent ransomware outbreaks.

*"It's only going to get worse and worse and worse," said Michael Gazeley, managing director of cybersecurity firm Network Box. "And it's absurd because companies have had years to prepare for this."*

**LINK:** <http://money.cnn.com/2017/05/15/technology/ransomware-wannacry-explainer/index.html>