FEB 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the February 2017 edition of In the Boxing Ring

This month, Network Box USA's Chief Technology Officer, Pierluigi Stella, discusses the very serious issue of **Spear Phishing**. Unlike most spam emails which use a shotgun approach to lure unsuspecting victims, spear phishing attacks are specifically aimed at targeted victims, whereby a wrong click on the email can inflict serious damage. It is by no means random and these emails are usually made to appear as though they are coming from a legitimate sender. This, and Network Box's approach to mitigate this threat is discussed further on pages 2 to 4.

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

Finally, at the end of last year, Network Box was interviewed by the **HKTDC** for a series of videos titled 'Cyber Belt and Road.' These videos are now available and can be viewed by following the links on page 6.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 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

In this month's issue:

NETWORK BOX

Spear PHISHING

by Pierluigi Stella

Chief Technology Officer
Network Box USA

One of the dangerous issues we currently face with spam emails is that of spear phishing – a type spam email targeting a specific recipient.

While most spam deploy a shotgun approach (send billions of emails and see what sticks), spear phishing attacks are specifically aimed at the recipient, requiring hackers to do homework on the targeted victim. It is by no means random. If their efforts are to be handsomely rewarded, they must target Executive and C levels, whereby a click on the wrong email can inflict serious damage. These emails are usually made to appear as though they are coming from one C level, to either another C level or someone else with authority to act upon the request.

Most of our clients are financial institutions (banks and CUs), and as such, a frequent phishing attempt we see in this particular sector is an email appearing to originate from the CEO. The request likely to be to execute a wire transfer, with the intended target being the CFO, or the person in the bank who oversees such wires.

NETWORK BOX

To be convincing, hackers need to imitate the CEO as much as possible which, at first glance, may seem a daunting task. Unfortunately, given how we are all far too eager to share as much of ourselves as possible these days, through various social media platforms, it isn't as impossible a task as it might appear. Hackers can quickly find out the name of the CEO, they know the address of the business and the main phone number; thus crafting a false signature isn't all that difficult. If the recipient has never received an email from the CEO before, he/she may well fall into the trap.

The second step is to find out who's doing the wire transfers. That's why the CFO might be the target here; because he has the authority to forward that email and ask for the wire to be executed. However, we've also seen such emails directly targeting the employee who can run the wire. In such instances, it means hackers have invested a little more time researching the company, perhaps through connections on LinkedIn. However they went about it, they now have the information they need, and have placed a bullseye on that person.

To understand how this could be technically possible, we first need to understand how email works, and what the SMTP protocol specifies and doesn't specify (SMTP stands for Simple Mail Transfer Protocol and is the protocol used on the internet to send emails). When SMTP was devised about 40 years ago, security wasn't at all a concern. Therefore, the creators of the protocol simply set out to model electronic communications in the image of physical mail. When we write a letter, we have an envelope and a page where we compose the 'body' of our letter. On the envelope, we write the name of the recipient, with the actual address we want it to go to. We then pen our own name and address as the sender, so if the letter cannot be delivered, it is returned to us.

On the inside, however, we do not replicate all this. Depending on the person to whom we're writing, we may say "Dear Larry", or "Hello son", or something to that effect. When we're done, we end by signing the letter. NOTHING says we _have_ to use our name. We could be signing "Dad"; or "Pierluigi", or use a nickname.

The SMTP protocol accounts for this and allows it in electronic format. An email is comprised of 2 parts – the envelope and the body. Users who never deal with email scanning, never see the envelope. Your email server behaves like JARVIS, opens the "letter" for you, discards the envelope. So you, as a user, most likely are unawares this part of the email even exists. I personally know I didn't, that is, before I started dealing with spam and malware.

What you receive in your inbox is what we call the body of the email, which is the electronic equivalent of the actual physical letter of old times. The body is, in turn, divided into three areas:

- **Headers**
- **Actual body**
- **Attachments**

We all know what attachments are. We can easily understand which part is the 'body'. The headers contain a few, well specified, fields, the following being relevant to our current discussion:

- **From:**
- **To:**
- **Subject:**
- **Reply-to:**

The **From:**, **To:**, and **Subject:** are those that email software, including webmail, shows you at the top of the email. NONE of these fields is mandatory. The reason why your email server sent that email to you and not to someone else is because of what was written in the envelope; and not because of the **To:** field in the headers of the body.

This also means that these fields can be entirely different from those in the envelope. And that's where the phishing trick comes into play. You as a user only see the **From:** and **To:**. Therefore, if I'm a hacker, I can write the following into the email:

From: *Tim Cook (CEO of Apple)*

To: *Luca Maestri (CFO of Apple)*

Subject: *Wire*

If Mr Maestri isn't careful, he'll think the email originates from Mr. Cook and will execute the order. However, if we analyze the envelope logged into the server, we will likely find:

- The originating IP of the email does not belong to Apple.
- The server sending the email (identified by something called "EHLO") isn't Apple's.
- The sender in the envelope may or may not say *cook@apple.com*, and most likely it does not.

Allow me to share something which happened to one of our clients recently:

The sender "appeared" to be the CEO; but that was only the **From:**. The actual sender in the envelope was *mirza.shafgat@bingutab.com* – a fake sender. The originating IP address was 97.74.135.162; this IP is in Scottsdale, AZ, and corresponds to DNS name p3plsmtp09-01-2.prod.phx3.secureserver.net. The server connected to our device with a EHLO message of p3plwbeout09-01.prod.phx3.secureserver.net.

Our client's domain is none of this. However, the **From:** and **To:** fields appeared to be both from someone @ our client's domain.

The first reaction one could have would be to apply SPF (Sender Policy Framework, a type of DNS record that identifies which mail servers are permitted to send email on behalf of your domain) control. However, SPF is applied to the envelope, not to the body headers. The envelope shows bingutab.com as the sending domain, and secureserver.net as the EHLO domain. Upon checking the SPF record of the server, we note that the sending IP is included. So SPF did not fail. The email, on the surface, looked legitimate. Besides, SPF isn't mandatory. In this case, the server had one and it matched. In many other cases we've seen, there simply wasn't an SPF record to match. We cannot discard emails only based on that fact, because SPF isn't required. If it exists, it must be respected; but since it isn't a requirement, if a domain has no SPF record, we still need to accept emails from that domain.

In case it isn't clear, there's a specific reason why the envelope sender doesn't match the apparent sender (**From:**). Your domain _could_ have an SPF record; in which case, it'd be extremely easy for us to catch that email as a spoof, because it'd be originating from an IP address that isn't authorized. And if, by any chance, it did originate from an IP that you've authorized in your SPF record, then you've a much larger problem because one of your servers has been compromised!

So, how do you block such emails? Actually the answer is simpler than I've made it look so far. Network Box 5 has a 'mail sender match' policy rule that we can use to define the policy "if the header:from is from someone at my domain, the recipient is to someone at my domain, but the sender is not, block that email".

However, we cannot apply such a sweeping rule without thorough consideration. You may have hired a marketing firm to send emails on your behalf, including emails to your own employees/colleagues, and generally, they make it a habit of using a **From:** that makes them appear as though they're coming from your company. For example, I've seen emails from evite.com doing just this. You set up an invitation for your entire company, specify your own email address, and click GO. They'll generate an email to everyone on your list (your colleagues), the header:From will contain _your_ email address; but the envelope sender will be something random @evite.com.

To avoid catching such legitimate emails in the sweeping net of the rule above, we create a list of email addresses and domains that _you_ want to authorize to send such 'spoof looking' emails. So, say I were to do this for our company, the rule would look something like this:

config mail sender match rule require direction = server sender inacl mydomains sender notinacl authorized-spoofers

I know, it sounds/looks/reads strange. But it's a very effective way to solve the issue of spear phishing that's currently plaguing many companies. And the only input we need from you is that list of domains or companies you want to allow in the rule above.

Makes sense?
Has your company experienced Spear Phishing?
Or any other form of spam?

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th February 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
February 2017

This month, for Network Box 5, these include:

- Support for DHCP clients with default route suppressed
- Performance improvements in configuration handling
- Performance improvements in entity system
- Introduce logging of configuration changes as nbsyslog event.console_audit method ConfigChange
- Improvements to allocation of cpu utilization, for logging processes
- Introduce support for JSON messages in event log syslog via nxlog agent
- Introduce support for reception of syslog messages over TCP protocol (port 514 by default)
- Introduce support for entity learning from windows event log ID #4624
- Minor improvements and fixes to administrative web portal widget refresh
- Improved support for login to admin and user web portals from devices with very small screens
- Introduce configurable overall limits for proxy logging
- Enhancement to add a Received header to SMTP email, when source natting
- Improvements to proxy intermediate SSL certificate handling
- Improvements to web client safe search filtering

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
Technology Review 2016

2016 was another landmark year for Network Box. In addition to the launch of the Network Box Mobile App, last year also saw the release of many new features and enhancements to the Network Box 5 platform.

As a special end-of-year review, Network Box has complied the key *In the Boxing Ring* articles and technology news of 2016, for you. Please use the link below to download the **Network Box Tech Review 2016**:

http://www.network-box.com/sites/default/files/files/Technology_Review_2016.pdf

Network Box
HKTDC Video Series - *Cyber Belt and Road*

At the end of last year, Network Box was interviewed by the HKTDC (Hong Kong Trade Development Council) for a new series of videos titled 'Cyber Belt and Road.' These videos are now available and can be viewed using the links below:

Dream Connector for Cyber Belt and Road

Hong Kong has an online environment that other countries can "only dream about", says Michael Gazeley of global cyber security firm, Network Box. He says China's Belt and Road Initiative consists of online (as well as land and sea) trading links and Hong Kong can rely on its fast, stable Internet and world class infrastructure to safely connect up the cyber Belt and Road.

https://www.youtube.com/watch?v=clnRlcs5Ojg

Internet Security Advantage on the Belt and Road

China's Belt and Road Initiative provides countries with lagging technology the opportunities to install state-of-the-art systems, says Michael Gazeley of Network Box. With dangers to cyber security lurking across the Internet, Hong Kong has the environment to nurture talent locally and from around the world to keep systems safe.

https://www.youtube.com/watch?v=BheudKdiNe4

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