NOV 2015

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the November 2015 edition of In the Boxing Ring

This month, we highlight a very serious security vulnerability that affects us all. Imagine, one day you you discover that your office computer has been wiped clean. Next, your iPhone goes blank. You go to another workstation and find that your company website looks completely different. Could this quite possibly be the worst day of your life? In pages 2 to 3 we talk about the ONE vulnerability that could have caused all this.

On pages 4–5, 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 Germany was at IT-SA 2015, the largest and probably the most important IT Security Exhibition and Conference in the German speaking world. Also, Network Box Singapore participated at GovWare 2015, jointly organized by the Singapore CSA, MHA and IDA.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
November 2015

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:

2–3
The ONE Vulnerability
Quite often we are asked "what should we focus on, in terms of security?" If there is only ONE vulnerability you should focus on, this is it. To find out what this is, read our feature article on pages 2 to 3.

4–5
Network Box 5 and Network Box 3 Features
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.

5
Network Box Highlights:
- **Network Box Germany**
  IT-SA 2015
- **Network Box Singapore**
  GovWare 2015

NETWORK BOX

The ONE Vulnerability

At Network Box, quite often we are asked "what should we focus on, in terms of cyber security?" Whilst there is a whole catalogue of potential threats and vulnerabilities, if there is only ONE vulnerability you should do something about before the end of this year, this is it...

The Story

Joe is the sys admin at a small textile company. He's worked there for 15 years, and pretty much runs the place. Sure, he's got some help for changing printer toner, updating workstation patches, etc. But, for the servers and security, he is it.

One day, Joe gets to his office for the worst day of his life. The first thing he notices is that his office desktop Apple iMac has been wiped clean. Next, his iPhone goes blank. He rushes to another workstation and finds his company website looks completely different. He doesn't understand it – that uses HTTPS SSL and can't have been hacked! He can't get to his local eMail, and can't even get into his gmail as it says his password is incorrect. His facebook wall is messed up, instagram wiped, and his twitter is a never ending stream of adult links.

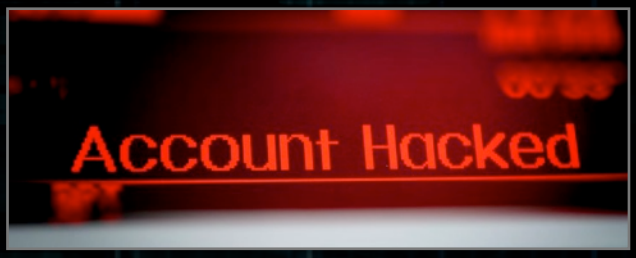
Joe really can't understand what happened. Every service he uses (Apple iCloud, his company active directory login, facebook, instagram, twitter, etc) has different usernames and passwords. How could this have happened?

The fix takes days, and both Joe and his company suffer incalculable damage to their reputations. Without an on-line way of fixing the issue, Joe has to contact each and every provider by telephone (have you ever tried to contact Instagram, Facebook, etc, by phone?) to resolve the situation. He has a horrendous time even proving who he is, in order to get back in control.

The Vulnerability

While Joe is a fictitious character, the key points of the above story are true and represent a very real threat to everyone online today. So, how did this happen, and what was the vulnerability?

Joe had correctly setup each of his on-line accounts with individual usernames and different passwords. That way, if one service was hacked (as seems to happen so often nowadays), it couldn't affect the others. The problem is that all these services offer a 'password recovery' feature. The password can be reset using a secret link sent to the registered eMail address.



The eMail address Joe used was his office one. But, that is secure. It is long and complex, with mixed case letters and numbers. He changes it every few months.

Being a busy on-the-go type of guy, Joe uses his iPhone to remotely access his eMail when out of the office. When he set it up, he entered his username and password, and assumed that was secure. He also setup his outbound SMTP server to be his office server, using the same credentials for SMTP AUTH. He didn't realize that both IMAP4 and SMTP AUTH can send those credentials in clear text, not even protected by SSL.

A couple of weeks ago, he was in an airport lounge. He connected to the free airport wifi, retrieved his eMail and sent some replies. That was his mistake.

The Attack

The attacker was also on a flight that day, and for his idea of fun turned on his laptop's connection sharing advertised as 'free airport wifi', along with a data traffic logger. He recorded Joe's IMAP4 eMail retrieval, as well as SMTP AUTH credentials for sending eMail.

Armed with that, it was trivial for the attacker to get access to Joe's eMail account. From there he could change Joe's facebook, instagram, etc, passwords by simply using the 'lost password' link. Similarly, Joe's gmail account was compromised.

The website was compromised by DNS and SSL. Firstly, the attacker did a simple lookup on Joe's company domain to find the DNS provider, and then could 'lost password' Joe's account there to get control. By comparison, the SSL was trivial. He merely ordered a new SSL certificate online, using Joe's eMail to verify control of Joe's company domain. Now, he could setup his own version of the website, and all Joe's customers went to the attacker's version of the site.

But, why wipe Joe's iMac and iPhone? Well, just to make it harder for Joe to recover from the problem. To delay the fix. To keep the attacker in control for as long as possible. Nothing personal. Just business.

The ONE Vulnerability

So, what is that ONE vulnerability you should do something about before the end of this year? It is **protection of your email accounts.**

With almost all on-line services available today, your eMail address proves who you are, and the ability to view eMail you received on that address is all you need to reset online account security credentials.

It doesn't matter if you use different passwords, on different services. It doesn't matter if those passwords are long and complex. It all comes down to your one single password recovery eMail address.

Here are some simple steps you can take to improve your security:

- SSL secure your eMail (both SMTP and POP3/IMAP4). If you can't do this on your mail server, Network Box 5 can do this for you. We can front an SSL certificate for you, so the remote communications to your office are secure, even if your server is not.
- Choose secure password authentication options. Make sure your server supports them, and make sure you've enabled them on your mail clients. Never use BASIC AUTH or other plaintext authentication mechanisms, unless the session is protected by SSL. Again, Network Box 5 can assist with this by offloading the SSL to the perimeter protection.
- Choose online services that take this seriously and offer alternative security options. For example, Google offers Authenticator for two-factor authentication.
- Consider a separation of home/office roles, and don't cross-permit password recovery email address (especially not permitting your office services to be recovered with your personal email address).

In the above story, we've mentioned names and products for example only, and not to blame any one set of services. It matters little if Joe was using iPhone, Android, or Windows Phone. Pretty much all such online services suffer from these vulnerabilities, and many offer advanced protection capabilities that you can enable to help you stay secure.

Stay safe.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd November 2015, Network Box will release our patch Tuesday set of enhancements and fixes. This month, the regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
November 2015

This month, for Network Box 5, these include:

- Network firewall and proxy support for host ACLs
- Reduce memory requirements for report generation (in particular large PDFs)
- Display block rule on web client policy block pages
- Additional entity search options, by entity attribute types
- New GMS sensor for nbsyslog service
- New GMS sensor for provisioning service
- New GMS sensor for certificate issue service
- Enhanced support for policy control of SMTP TLS based on sender or recipient address
- Enhanced support for SMTP STARTTLS policy control for offloaded SSL configurations
- Support for wildcarding in application identifiers
- Support DNS forwarding on a per-domain basis
- Improvements to performance of top web client users displays in administrative web console
- Automated spam trap support
- Improvements to reliability in nbsync connections under high workload
- Improvements to anti-spam RBL caching mechanism
- Improvements to anti-spam URL extraction options
- 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.

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 November 2015

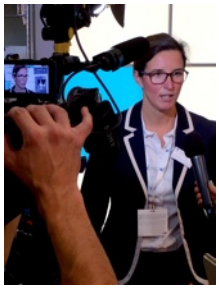
On Tuesday, 3rd November 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- 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

Network Box Germany
IT-SA 2015



Network Box Germany participated at IT-SA 2015, the largest IT Security Exhibition and Conference in the German speaking world, and certainly one of the most important IT Security Events anywhere across the globe.

During the event, Network Box Germany's General Manager, Jacqueline Voss, was interviewed for the trade show news.

Network Box Singapore
GovWare 2015

Network Box Singapore participated in Singapore's GovWare 2015. This event was jointly organized by the Cyber Security Agency of Singapore (CSA), in partnership with the Ministry of Home Affairs (MHA) and the Infocomm Development Authority of Singapore (IDA).