

In the Boxing Ring

MARCH 2020



Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

Welcome to the
March 2020 edition of
In the **Boxing Ring**

This month, we will be talking about **when a password doesn't seem like a password, and you give it out to a stranger.**

Recently, Network Box has been helping with incidents involving *WhatsApp*, where victim's accounts have been hijacked by inadvertently giving hackers access to their account. On pages 2 to 3, we examine how hackers can do this, and discuss best practices and the measure you can take to prevent your account from being hijacked.

In other news, Network Box has released a brand new version of our executive summary newsletter, **Network Box Focus**. You can download the document from the link on page 4. And in this month's media coverage, Network Box was featured in the various media outlets including the **South China Morning Post**, **CRN** and **HK01**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
March 2020

In this month's issue:

Page 2 to 3

When a password doesn't seem like a password (and you give it out to a stranger)

On pages 2 to 3, we discuss how hackers are using social engineering techniques to hijack your *WhatsApp* account, and outline how you can prevent your account from being stolen by them.

Page 4

Network Box Highlights:

- **Network Box Focus**
New edition
- **Network Box Media Coverage and Security Headlines:**
 - SCMP
 - CRN
 - HK01
 - Forbes
 - Ars Technica

NOTE: With effect from January 2020 we have switched to a quarterly Patch Tuesday cycle for Network Box 5. However, essential security fixes will continue to be released out-of-cycle, if necessary.

Stay Connected

You can contact us here at Network Box 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:



<https://twitter.com/networkbox>



<https://www.facebook.com/networkbox>
<https://www.facebook.com/networkboxresponse>



<https://www.linkedin.com/company/network-box-corporation-limited/>



<https://www.youtube.com/user/NetworkBox>



PASSWORD

* * * * *

When a password doesn't seem like a password

and you
give it out to
a stranger

We've heard reports of, and helping resolve incidents with, WhatsApp account compromise. Not necessarily an issue that Network Box Security Operation Centres would usually be involved with, but an interesting lesson nonetheless.



The account hijack works as follows:

Step 1

A WhatsApp user (aka 'victim') receives a message from their contact friend saying that WhatsApp is asking him/her to get a friend to help verify their account. WhatsApp will SMS a code, and our victim will need to tell the friend that code to help get verified.

Step 2

Our victim receives an SMS from WhatsApp with a six-digit code, and helpfully forwards it on to their friend (via WhatsApp).

Step 3

Our victim is locked out of WhatsApp. He/she tries to go through the WhatsApp reset procedure but is told by WhatsApp that they need to wait 12 hours because they have failed to enter the verification code incorrectly too many times.

Step 4

The next day they try again, and the same lockout happens. Other contacts and friends of our victim start to receive messages asking them for help as WhatsApp is asking them to get a friend to verify their account.

Step 5

It takes 7 days for WhatsApp to free the account lock, and for ownership of the account to be recovered.

In hindsight, it seems clear that the 'friend' was a hacker who:

- a) used the victim's number to request an account transfer to his phone.
- b) hijacked the account with the PIN code helpfully provided.
- c) used another phone to repeatedly input incorrect PIN codes to lock out the victim.
- d) leveraged the attack further to the victim's other contacts.



The core problem is that six-digit WhatsApp verification code didn't feel like a password. That, coupled with the trust of a friend, led to a successful compromise.

The solution to this is **user education** to ensure that users:

- never give out passwords, PIN codes, authentication codes, etc., to third parties.
- enable dual-factor authentication, where available.

In particular, password authentication is weak and prone to compromise; dual-factor authentication is an essential part of modern computing and should be used wherever offered. WhatsApp has a robust dual-factor authentication mechanism that would have avoided this issue.

Network Box HIGHLIGHTS



Network Box Focus Executive summary newsletter

Network Box has launched a brand new edition of our executive summary newsletter, **Network Box Focus**. The publication highlights Network Box's key features and technologies, and covers the latest company news and events. Please use the link below to download the new version.

 **LINK:**
https://www.network-box.com/sites/default/files/files/NetworkBox_Focus-202002.pdf



Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
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

Copyright © 2020 Network Box Corporation Ltd.



Network Box Media Coverage and Security Headlines



**South China
Morning Post**

SCMP

Coronavirus: US cites Sars and 'ongoing uncertainty' as reasons for letting consulate staff leave Hong Kong, but business leaders say they are staying put

LINK: <https://bit.ly/38cWKZj>



CRN

Systemhäuser profitieren von der Zusammenarbeit mit MSPs
[System Integrators benefit from cooperation with MSSPs]

LINK: <https://bit.ly/38bC1oM>



HK01

24/7 Fitness adopts Network Box solution for for all-day protection of their IT network

LINK: <https://bit.ly/2Tu3EnB>



Forbes

Cisco Confirms 5 Serious Security Threats to 'Tens of Millions' of Network Devices

LINK: <https://bit.ly/2uJjr9I>



Ars Technica

New ransomware doesn't just encrypt data. It also meddles with critical infrastructure

LINK: <https://bit.ly/2PAhHXy>