NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

# In the Boxing Ring JUN 2019

## Network Box Technical News

### from Mark Webb-Johnson

*Chief Technology Officer, Network Box*

### Welcome to the June 2019 edition of In the **Boxing Ring**

This month, we discuss the ongoing issue of **Administrative Systems access from the Internet**. This was highlighted by the recent **CVE-2019-0708**, a remote code vulnerability in Microsoft Remote Desktop Services. Whilst it is helpful to have such remote access, even with strong authentication enabled, permitting direct access to Administrative Systems from the public Internet is a very bad idea. You are reliant on your authentication system being perfect, reliant on your users never making mistakes, reliant on the software being perfect, and relying on credentials not having been leaked / discovered from other systems. On pages 2 to 3 we discuss our recommendations for CVE-2019-0708, and highlight how can Network Box securely provide remote administrative access, if required.

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

In other news, Network Box Managing Director was asked by **RTHK Radio 3** to share his opinion on growing concerns about the privacy issues raised by facial recognition technology. In addition, we present some upcoming Network Box events; and finally, we highlight security headlines which affecting: **Equifax, Salesforce, Cisco, UNIQLO, Binance,** and **SAP.**

**Mark Webb-Johnson**
*CTO, Network Box Corporation Ltd.*
June 2019

### 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

## In this month's issue:

**Page 2 to 3**

### Administrative Systems access from the Internet

On pages 2 to 3 we discuss the dangers of permitting direct access to Administrative Systems over the public Internet, and how (if required) Network Box securely provide remote administrative access.

**Page 4**

### Network Box 5 Features

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

**Page 5**

### Network Box Highlights:

- **RTHK Radio 3 Backchat**
  Surveillance and facial recognition technology
- **Upcoming Network Box Events**
  - Cyber Security Risk Management for the Hotel Industry
  - The Dark Web: The Dark Side of the Internet
- **Security Headlines**
  - Equifax
  - Salesforce
  - Cisco
  - UNIQLO
  - Binance
  - SAP

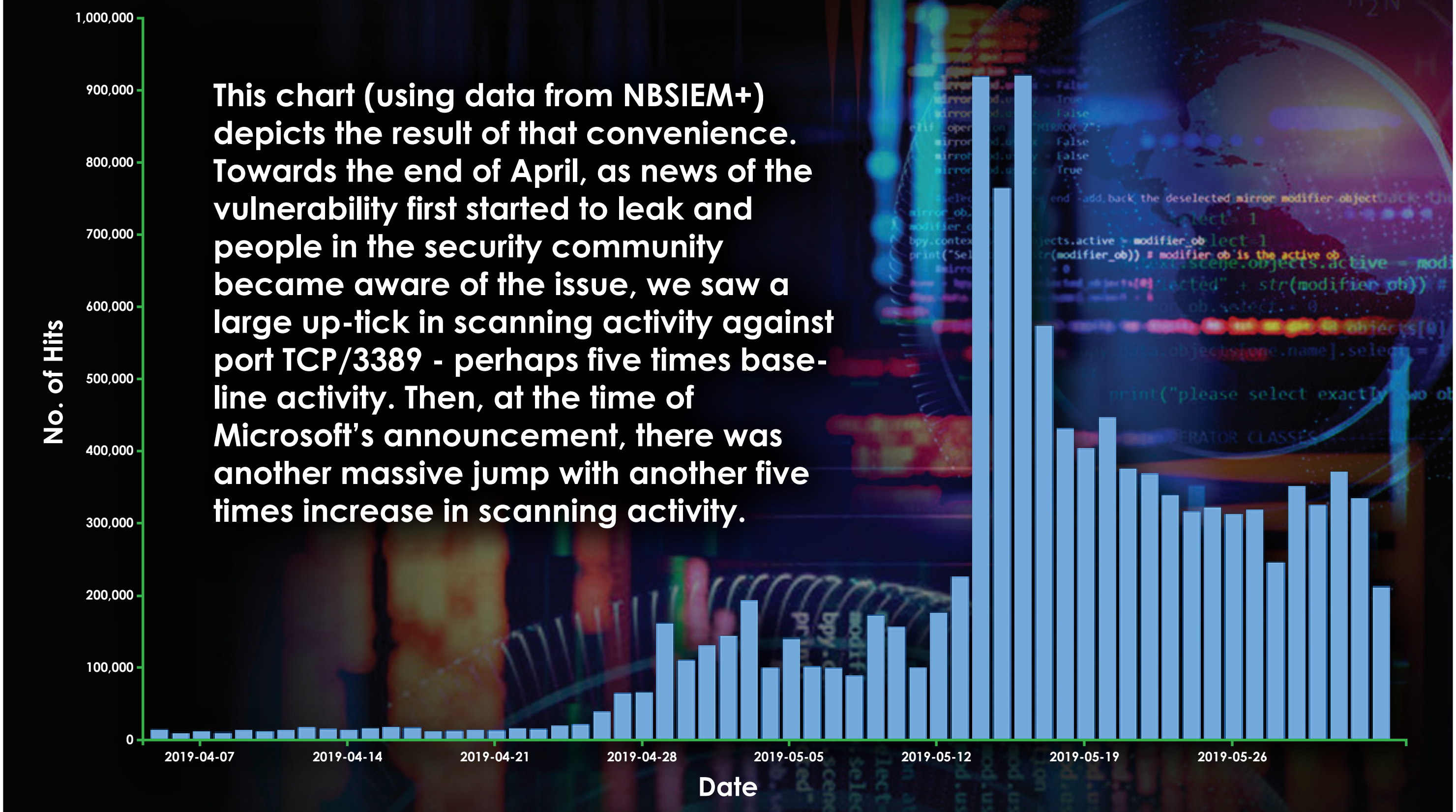
# Administrative Systems access from the Internet

The ongoing issue of access to Administrative Systems over the public Internet has again been highlighted by the recent announcement of CVE-2019-0708 (a remote code execution vulnerability in Microsoft Remote Desktop Services).

**Even with strong authentication enabled, permitting direct access to Administrative Systems from the public Internet is a very bad idea.**

I understand that it is helpful to have such remote access (particularly in times of emergency), but opening up those ports is simply too risky. You are reliant on your authentication system being perfect, reliant on your users never making mistakes, reliant on the software being perfect, and relying on credentials not having been leaked / discovered from other systems. You have to be perfect, 100% of the time, while the remote hacker only has to find that one mistake you (or one of your suppliers) made.

When we deploy Network Box devices at network perimeters, it is fairly common for us to find a request to open TCP/3389 and NAT forward it to an internal server. It is so very convenient for administrators to have remote access to screen sharing on that server.



This chart (using data from NBSIEM+) depicts the result of that convenience. Towards the end of April, as news of the vulnerability first started to leak and people in the security community became aware of the issue, we saw a large up-tick in scanning activity against port TCP/3389 - perhaps five times base-line activity. Then, at the time of Microsoft's announcement, there was another massive jump with another five times increase in scanning activity.

That is why Network Box pushes back against requests to open TCP/3389, TCP/22, TCP/23 (yes, we still see these), and other common administrative ports. If you really want it, we will open it (as you the customer are in charge of policy), but we warn you of the possible consequences and suggest you alternative, more secure, ways of remaining secure (while still enjoying the convenience of remote access).

## How can Network Box securely provide remote administrative access?

- So long as the traffic passes over the TCP protocol, we can permit access only via specific source IP addresses. With modern equipment, it is pretty hard to successfully spoof TCP/IP nowadays (especially over the public Internet).
- A VPN is the most common approach. It can be used to provide a second layer of authentication and encryption, through which administrative traffic can be tunneled. Open SSL VPNs can be configured with a fingerprint at the packet level, to further protect access.
- Using dual factor authentication can help, but will probably not be of much use in the case of exploit of a vulnerability (such as with CVE-2019-0708).
- Using non-standard ports is one approach that can help against mass scanning, but not against a determined hacker targeting your network. So long as your services can be fingerprinted, they can still be exploited (and even without fingerprint, brute force exploits are still a possibility).

## As a reminder, our recommendations for CVE-2019-0708 are:

- If you have RDS ports (by default tcp/3389) open to the Internet, we recommend that you immediately close those down.
- If you have RDS ports open to the LAN/DMZ, for administrative purposes, we recommend that you immediately close those down as well.
- We recommend that you either close the ports entirely, or restrict access to specifically identified administrative source IP addresses or VPN connections.
  - If you have no requirement for RDS services, you should disable them completely on your servers.
  - Network Box can assist with this, and we will be contacting customers we have identified to have tcp/3389 open to the Internet directly.
  - Microsoft has released patches for this, and these should be applied as a matter of urgency.

**For those of you subject to PCI compliance, the above controls should already have been applied as part of your network segmentation exercise.**

**Should you have any questions, please don't hesitate to contact your local Network Box Security Operation Centre for assistance.**

# Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th June 2019, 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

## June 2019

This month, for Network Box 5, these include:

- Global release of InfectedLAN URL categorisation engine
- Web client performance improvements (when large number of policy rules enabled)
- Support for time ACLs in IPv6 firewall
- Include source IP address in wording of cached RBL block message
- Release support for authentication policies (including PCI requirement)
- Admin web portal support for authentication policies
- Experimental support for sub-url extraction and categorisation (proxies, translators, etc)
- Experimental support for scan clustering
- Change scan job dispatcher to use a prioritised round robin algorithm
- Add support for 'dlp' classification in policy rules
- Improved BEATS protocol support for ack:0 back-off messages in NBSIEM+
- Add support for PCI network interface naming convention
- Improvements to Box History report in admin 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 HIGHLIGHTS

NETWORK BOX

## Network Box Upcoming Events

### Cyber Security Risk Management for the Hotel Industry

Hotel ICON

Network Box will be taking part in Hotel ICON's upcoming **Cyber Security Risk Management Workshop** on the 3rd July 2019. The event will cover the entire spectrum of cyber-threats facing the Hospitality Industry, and beyond.

**LINK:** https://bit.ly/2JSuL9H

### The Dark Web: The Dark Side of the Internet

ISACA

On 6th June 2019, Network Box has been invited by ISACA China Hong Kong Chapter, to talk about the threats posed by the Dark Web, and how organizations can protect themselves by leveraging Network Box's new **Dark Web Monitoring Service**.

**LINK:** https://bit.ly/2XoYUQZ

### RTHK Radio 3 Backchat

Network Box Managing Director, Michael Gazeley, was asked by RTHK to share his views about the privacy issues raised by facial recognition technology.

**LINK:** https://bit.ly/2JX7pPY

Radio3

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

## Security Headlines

EQUIFAX

**Equifax just became the first company to have its outlook downgraded for a cyber attack**

**LINK:** https://cnb.cx/2Z6n4QI

salesforce

**Faulty database script brings Salesforce to its knees**

**LINK:** https://zd.net/2Ig6JlE

CISCO

**Critical Flaw in Cisco Elastic Services Controller Allows Full System Takeover**

**LINK:** https://bit.ly/2WmdlZy

**Thrangrycat flaw lets attackers plant persistent backdoors on Cisco gear**

**LINK:** https://zd.net/2WimqT4

UNI QLO

**UNIQLO says Japan online stores hacked, more than 460,000 accounts affected**

**LINK:** https://bit.ly/2QMldxl

BINANCE

**Hackers steal $40 million worth of bitcoin in massive security breach**

**LINK:** https://cnn.it/2Wevu6C

SAP

**50,000 enterprise firms running SAP software vulnerable to attack**

**LINK:** https://zd.net/2W9YMDj