NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring FEB 2024

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the February 2024 edition of In the **Boxing Ring**

This month, we are talking about **Ransomware Delivery Protocol (RDP) and others.** Whilst this is a play on words for Remote Desktop Protocol, the security risks that it represents cannot be overlooked. Among every ransomware case that Network Box has been called in to assist with over the past five years, RDP has been the #1 mechanism for network infiltration and eventual ransomware delivery. Whilst being the worst offender, RDP is far from the only problematic such service. On pages 2 to 3, we discuss this in greater detail and provide a few best practices to alleviate these threats.

In other news, Network Box's Managing Director, Michael Gazeley, participated in a cybersecurity panel discussion titled, **Building Network Security Barriers Together - Creating a New Chapter for Smart Cities.** Additionally, as a special end-of-year summary, Network Box has compiled all the key events of the last year in the 2023 edition of **Year in *Focus*.** And in this month's Global Security Headlines, there were security issues with **Cisco**, **TeamViewer**, **Ivanti**, and **Cloudflare**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2024

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

Ransomware Delivery Protocol (RDP) and others

This is a play on words for Remote Desktop Protocol. Over the past five years, RDP has been the #1 mechanism for network infiltration and eventual ransomware delivery. In almost all of these cases, the RDP service was completely unprotected - no source IP limits, no effective password policy, no password lockout policy, and no restrictions. However, RDP is far from the only problematic such service. In our featured article, we talk about this in greater detail.

Page 4

Network Box Highlights:

- **Network Box Hong Kong:** Cyberport Cybersecurity Panel Discussion
- **Network Box Year in *Focus* 2023**
- **Global Security Headlines:**
  - Cisco
  - TeamViewer
  - Ivanti
  - Cloudflare

Ransomware Delivery Protocol (RDP) and others

Imagine leaving your laptop out on the front porch of your home. It is secured against theft, but any passerby can use the screen, mouse, and keyboard to access the login screen and 'try their luck.' Repeatedly guessing usernames and passwords until they finally manage to log in and have access to all your files and applications. Worse yet, they can then use your laptop's network connection to access all the other computers in your home (bypassing the protection of your front door firewall).

Sounds ridiculous, right? No sane person would do this, right? Well, today, a quick Shodan search for port tcp/3389 shows over 4.6 million such computers (with mouse, keyboard, and screen) open to the public Internet and bypassing firewall controls.

Top Countries with tcp/3389 RDP open to the Internet

#1	China	1.5 million
#2	USA	1.2 million
#3	Germany	214,000
#4	Japan	115,000
#5	Hong Kong	109,000

Using our internal ***Nidan*** tool (similar to Shodan, but just covering Network Box managed networks) shows several dozen tcp/3389 ports open to the public Internet. And this is despite multiple warnings and best practice recommendations for years.

Admittedly, we are calling tcp/3389 RDP the Ransomware Delivery Protocol, as a tongue-in-cheek phrase (its proper name is Remote Desktop Protocol), but I am sure you get the point. Among every ransomware case that Network Box has been called in to assist with over the past five years, RDP has been the #1 mechanism for network infiltration and eventual ransomware delivery. Nothing else comes even close. And in almost all of these cases, the RDP service was completely unprotected - no source IP limits, no effective password policy, no password lockout policy, and no restrictions.

Whilst being the worst offender, RDP is far from the only problematic such service. Among our managed networks, we see more than 1,000 tcp/22 (SSH), 700 Cisco, 300 Fortinet, 200 tcp/23 (TELNET), 150 Sonicwall, 150 tcp/5900 (VNC), and a dozen Palo Alto, administrative interfaces directly open to the public Internet.

Globally, the situation is much worse: 25 million SSH, 6 million Cisco, 670,000 Fortinet, 2 million TELNET, 860,000 Sonicwalls, and 600,000 VNC. Understandably, many of these are in ISP-provided router equipment - unforgivable given the trivial simplicity of the ISP locking those down to their SOC address ranges. But many are also deliberately opened to allow remote access (especially post-COVID and the associated work-from-home arrangements).

Network Box and others recommend Best Practices for securing your networks, and amongst all these, the #1 is the prevention of **'Remote Administrative Access Open to the Internet.'**

Remote Administrative Access Open to the Internet

In general, Remote Administrative Access services that provide administrative access (such as SSH, RDP, VNC, etc.) should not be open to the Internet. Opening such services to the Internet directly exposes the network to the exploitation of vulnerabilities or insecure credentials, and brute force attacks. Even those services restricted to user-only (non-administrative) access are discouraged due to privilege escalation issues.

As an alternative, it is recommended that VPN/SDWAN services be deployed. These remote administrative services should only be made available over secure VPN/SDWAN links to specific user accounts, VPN endpoints, or source IP addresses.

We've written about this in the past and, no doubt, will write about it again in the future. In the end, the security policy is maintained by our customers; Network Box can only point out the dangers and recommend changes. That said, if you have these administrative services open to the Internet, and in particular RDP tcp/3389, then if there is only one change you make to tighten the security of your network, irrespective of whether it is protected by Network Box or not, it should be to lock this down.

> **It is relatively simple to deploy and use SSL VPN technology to provide a layer of authentication on top of these protocols - and putting these services behind such a VPN is the same as moving that laptop off your front porch, back safe where it cannot be trivially tampered with by passersby.**

Network Box HIGHLIGHTS

NETWORK BOX

Network Box Hong Kong Cybersecurity Panel Discussion

Network Box's Managing Director, Michael Gazeley, participated in a cybersecurity panel discussion titled, **Building Network Security Barriers Together - Creating a New Chapter for Smart Cities**, at HK Cyberport. During the discussion, panelists shared cases and experiences in enhancing cybersecurity to enable a safer and more conducive network environment for applying technological innovations, thus advancing smart city development.

同建網絡安全屏障 共譜智慧城市新章
Building Network Security Barriers Together - Creating a New Chapter for Smart Cities
Felix Kan

Global Security Headlines

Dark Reading

Critical Cisco Unified Communications RCE Bug Allows Root Access

LINK: https://bit.ly/42nKsep

Bleeping Computer

TeamViewer abused to breach networks in new ransomware attacks

LINK: https://bit.ly/3wcGhpt

Security Week

After Delays, Ivanti Patches Zero-Days and Confirms New Exploit

LINK: https://bit.ly/3Ut31vv

The Hacker News

Cloudflare Breach: Nation-State Hackers Access Source Code and Internal Docs

LINK: https://bit.ly/3SKB5Sx

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

Network Box Year in *Focus* 2023

As a special end-of-year summary, Network Box has compiled all the key events of the last twelve months in the 2023 edition of **Year in *Focus*.**

LINK:
https://bit.ly/3w16TKi