In the Boxing Ring November 2020

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

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

This month, we are talking about **Virtual Patching**. When a vulnerability is discovered, it is a race between releasing and installing patches and the attackers exploiting the vulnerability. Virtual Patching aims to deploy early virtual patches on the affected devices themselves or at the gateway, before formal patches can be released to stop attackers from compromising protected systems. On pages 2 to 3, we discuss Virtual Patching in greater detail and the Network Box approach to it.

In other news, Network Box is pleased to announce the opening of two new offices in **Austria** and **Spain**. Security issues were discovered in tech giant **Software AG** and cryptocurrency exchange **KuCoin**. In this month's Media Courage, Network Box was featured in **Harbour Times** and **Asia Times**. Finally, episode #3 of **HPCC Hackpod Club** is now available for listening.

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

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:

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.

Virtual PATCHING

From the time a vulnerability is announced, a race starts between developing, testing, releasing, and installing the patches to fix it; and the attackers developing their exploits to take advantage. Virtual Patching aims to deploy early patches 'virtually.' Sometimes on the affected devices themselves, but more often at the gateway, before formal patches can be released or installed, and before the attackers can compromise protected systems.

The Technology

Virtual patches target network traffic attempting to exploit a known vulnerability. They often start with signatures to detect the vulnerability, or exploit behaviors, and then actively interrupt the traffic and block it before it affects the target system. They are a 'quick-and-dirty' solution to a complex problem, as they can usually be deployed without reboot or interruption to services. Due to limitations inherent in the technology, they are often only short-term stop-gaps, gaining time for formal patches to be deployed.

Think of the vulnerability akin to a leaky pipe, the exploit being the resulting flood, and the virtual patch being a temporary tape to fix the leak. The permanent solution would be to replace that part of the broken pipe, but the virtual patch gains you time and avoids the damage that a flood would cause. It is certainly better than having to turn off the water.

Virtual Patching allows the user to maintain their own patching cycle, not dependent on the various manufacturers of equipment, systems, and applications that they run. They are much simpler to deploy, as they are typically installed at just a few centralized/gateway locations, rather than on every potentially affected device.

Limitations of Virtual Patching Technology

- **The virtual patch must be deployed between the attacker and the attacked device or service.**
  For it to be effective, this protection must be inline or at least able to block malicious traffic with very little latency. Encrypted traffic may need special handling to be accurately analyzed for exploits.

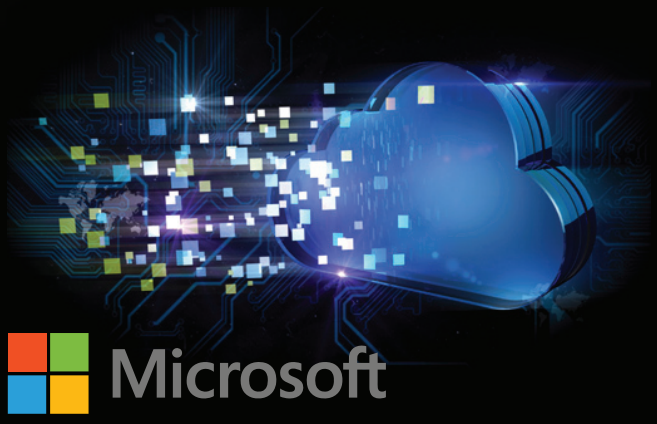
- **A virtual patch must be accurate.**
  It must detect exploits of the vulnerability without affecting legitimate traffic while being broad and comprehensive enough to detect new emerging variants of exploits (not just an initial specific one). In cases where the exploit is non-trivial and in particular, where it involves multiple requests in a network traffic session, this may not be possible, and the virtual patch only partially effective.

- **False positives may be a problem.**
  As the virtual patches need to be deployed quickly, there may not be adequate time for testing. Depending on the severity and impact of the vulnerability, this may be considered an acceptable risk to the alternative of shutting down all services until formal patches can be deployed. Deployment of manufacturer patches is also not without risk.

The Network Box Approach

The Network Box approach to virtual Patching is that we have many layers of protection. From frontline IPS, through firewall, IDS/IPS, application proxies, protocol scanners, and hardened services. We implement Virtual Patching technology at each of these layers - choosing the best approach for each particular vulnerability and often deploying protections with multiple technologies to protect against different attack vectors.

Network Box maintains partnerships with dozens of security organizations and works with these to gather and share threat intelligence. For example, we work with Microsoft's Active Protections Program (MAPP) to synchronize our virtual patch releases to Microsoft's own Patch Tuesday schedule. Last year Microsoft listed Network Box as one of their top threat indicator contributors.



Virtual Patching is not a perfect solution and cannot protect every vulnerability from every possible exploit. However, it is a good solution that is effective in most cases, particularly those identified as high severity. The technology does provide a comprehensive and effective first line of defense against network-based exploits and is valuable as one tool of many in your arsenal.

Network Box HIGHLIGHTS

Network Box
New offices in Austria and Spain

Network Box is pleased to announce the opening of two new offices in Austria and Spain to provide multi-award-winning world-class Managed Security Services to new and existing Network Box customers in those regions.

Network Box Austria
Marktplatzstrasse 18
8861 Sankt Georgen ob Murau
(+43) 720 500243
info@network-box.at

Network Box Spain
Paseo Ibaialde 204
31192 Mutilva Navarra
(+34) 638 948 739
info@network-box.eu

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 Media Coverage and Security Headlines

Harbour Times
Death by cyberattack should motivate Hong Kong hospitals to lock down on cybersecurity – they haven't
LINK: https://bit.ly/35SyrAJ

Asia Times
New privacy tech has pros and cons
LINK: https://bit.ly/3jV8GVy

HPCC Hackpod Club
Episode #3: The Human Firewall
LINK: https://bit.ly/3mK8ha5

ZDNet
German tech giant Software AG down after ransomware attack
LINK: https://zd.net/383ydJx

Decrypt
Cryptocurrency Exchange KuCoin Hacked, $150 Million Moved
LINK: https://bit.ly/3ej3lpI