

In the Boxing Ring JUNE 2021



Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

Welcome to the June 2021 edition of In the **Boxing Ring**

This month, we are talking about **Security Hesitancy**. As the COVID-19 pandemic continues to rage around the world, a solution in the form of vaccines has arrived. However, the trend of vaccine hesitancy is emerging; a significant percentage of the population simply won't accept the vaccine. In the IT Security Industry, we've seen similar behavior regarding security solutions. On pages 2 to 3, we will continue our discussion of biological epidemics and how they compare to IT Security issues.

In other news, we are pleased to announce that **Armadillo Networks** now offers Network Box's *Dark Web Monitoring Services* in Spain. And in this month's security headlines, **Swatch Group**, **Colonial Pipeline**, and **AXA** were all hit by ransomware attacks; an **unpatched Fortinet VPN** was leveraged to attack a US municipal government; and the US, with the help of Denmark, were accused of spying on certain European governments.



Mark Webb-Johnson

CTO, Network Box Corporation Ltd.
June 2021

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

Security Hesitancy

In our featured article, we continue our discussion of biological epidemics and how they compare to IT Security issues. This month, we are focusing on the similarities between vaccine hesitancy and security hesitancy.

Page 4

Network Box Highlights:

- **Network Box Dark Web Monitoring Services**
Armadillo Networks
- **Global Security Headlines:**
 - Swatch Group
 - Colonial Pipeline
 - AXA
 - Unpatched Fortinet VPN
 - NSA



Security Hesitancy

As the COVID-19 pandemic continues to rage around the world, with more than half a million new infections and ten thousand deaths each day, a solution in the form of vaccines has arrived. To date, close to two billion of these vaccine doses have been administered globally. However, in countries rich and poor, the trend of vaccine hesitancy is emerging; a significant percentage of the population simply won't accept the vaccine. In the IT Security Industry, we've seen similar behavior regarding security solutions, so this month we will continue our discussion of biological epidemics and how they compare to IT Security issues.

The Risk

A virus such as COVID-19 has associated risks that are not the same for everybody. Aspects of your genetic makeup, your age, and your general health level, all affect your immune system; resulting in your overall susceptibility to a specific disease. That is your risk from the disease, and should be combined with your risk of exposure and infection (which is related to your activities, personal protective measures, and the general level of infectious disease in your community) to determine your overall risk level.

Computer viruses, worms, ransomware, and other attacks, also have associated risks dependent on many of the same types of factors. The type of operating system you are running, whether it is still supported with security updates, how recently security updates were applied, etc. Combine this with your risk of exposure (security policies, acceptable use practices, protective technologies in place, as well as the general level of attack in the wild) to come up with your overall risk.



No solution is 100% perfect, and the solution itself may have associated risks. Vaccines have side effects, which, in very rare cases, may be serious or even cause death. Anti-malware signatures may lead to false-positives and block important messages, while patch updates may break compatibility with important applications.

Classification

We can typically classify hesitancy into three groups:

1. Those that will turn up early and accept on day 1.
2. Those that are undecided and may eventually accept, but see no hurry and are waiting to see what happens.
3. Those that will never accept, usually either because they distrust the technology / the companies behind it, or refute that the problem even exists.

Fundamentally, this is a risk vs. benefit equation, applied at a personal level according to an individual's specific personal circumstances. Those in group #1 typically have concluded that the risk of the problem outweighs the risk of the solution. Those in group #2 are undecided, and those in group #3 either reject the problem or consider the risks of the solution far greater.



The issue is that individuals have a hard time applying logic to balance these levels of risk sensibly. Emotions, fears (both real and imagined), misinformation, or lack of good advice; all get in the way of making the right decision. And fundamentally, the risk is all about percentages applied to a group. When we say there is a 50% chance of an event happening, we mean that half will have the predicted outcome when applied to thousands of events. But on an individual basis, you may simply be lucky and get away with it, or unlucky and succumb.

The Herd

For the most part, individuals only think about themselves in such situations, and fail to balance the risk to society (aka 'the herd'). If enough individuals are protected, the overall level of the virus (human or computer) in the community is reduced, and all are protected.

Paradoxically, the least risky approach to vaccination is for everyone else to be vaccinated (let them take the risk) to protect you (the unvaccinated) from the disease. Take that to the extreme, and you have the tragedy of the commons where nobody is vaccinated, and everybody is vulnerable.

Interestingly, the more virus in the community (be it COVID-19 or an outbreak of a new type of computer worm or ransomware attack), the greater the acceptance and take-up of protective measures (vaccination rates increase, sales of anti-malware go up). When we look at countries worldwide with the least number of COVID-19 infections (such as Australia, New Zealand, Vietnam, Thailand, Hong Kong, and many more in the Asia-Pacific region), they also have the greatest levels of vaccine hesitancy. Similarly, IT security sales ebb and flow with the latest computer worm or ransomware attack news reports.

While we appreciate that it is sometimes hard to do, we encourage everyone to take a step back and try to take on a broader view of IT Security issues. Don't be reactive to today's news headline, but take a longer-term pragmatic viewpoint. Implement the security technologies to suit the risk profile of your own organization. Always keep in mind the risks of the problem and how destructive this could be so that you can budget for and plan appropriately. Similar to insurance, protection needs to be in place before the infection occurs - calling the insurance agent when your house is already on fire is too late. If you can't patch early, then implement other protective measures (such as patch mitigation) to gain you time. Minimize your system's exposure to the Internet and to threat both external and internal. And if you can, think about your impact on others and what you can do for that (such as egress filtering, intrusion detection, and others).

As for COVID-19, please think about your community and balance not just the risk today but what the risk could be tomorrow. Above all, stay safe.



Network Box HIGHLIGHTS



Network Box Dark Web Monitoring Service | Armadillo Networks



Armadillo Networks now offers Network Box's *Dark Web Monitoring Services* in Spain. The Dark Web contains billions of people's hacked and posted confidential credentials. Typically, one-third of people use the same password at work, as they do on various third-party sites. Therefore, it is critical to monitor such data breaches, or it is possible an organization can be infiltrated by people who simply use passwords taken from the Dark Web.

- **More Information about Network Box Dark Web Monitoring Service:**
https://network-box.com/nb5-darkWeb_monitoring
- **Armadillo Networks:**
<https://www.armadillonetworks.es/soluciones/monitoreo-de-la-dark-web/>

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



Global Security Headlines



Infosecurity

Swatch Group Hit by Likely Ransomware Attack

LINK: <https://bit.ly/3vyFj1L>



Wired

The Colonial Pipeline Hack Is a New Extreme for Ransomware

LINK: <https://bit.ly/3i727BR>



BleepingComputer

Insurer AXA hit by ransomware after dropping support for ransom payments

LINK: <https://bit.ly/3c7iF8U>



Security Affairs

APT hacked a US municipal government via an unpatched Fortinet VPN

LINK: <https://bit.ly/3wRSTh7>



SCMP

US accused of spying on Angela Merkel and European allies with Denmark's help

LINK: <https://bit.ly/3p623Ut>