

# In the Boxing Ring

## APR 2021



## Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

### Welcome to the April 2021 edition of In the **Boxing Ring**

In our current COVID-19 times, this month, we are talking about **Herd Immunity from Computer Worms**. The term Herd Immunity is all about reducing the Effective Reproduction Number (the average number of new infections caused by a single infected individual in a partially susceptible population) of a virus by reducing the percentage of individuals it can infect. On pages 2 to 3, we discuss the similarities of how Herd Immunity can be applied for both human and computer viruses.

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

In other news, Network Box was named a **Globee® Awards Grand Winner** at the 17th Annual 2021 Cyber Security Global Excellence Awards. Besides taking home a Grand Award, Network Box also took home Gold Awards and Silver Awards in various security categories. Finally, Network Box was listed in the **Frost & Sullivan** and **Garner Insights** market reports.



**Mark Webb-Johnson**  
CTO, Network Box Corporation Ltd.  
April 2021

### Stay Connected

You can contact us here at Network Box HQ by email: **[nbhq@network-box.com](mailto: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

#### **Herd Immunity from Computer Worms**

In our featured article, we discuss how Herd Immunity can be applied to stop the spread of computer virus worms.

#### Page 4

#### **Network Box 5 Features**

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

#### Page 5

#### **Network Box Highlights:**

- **Globee Awards:**  
17th Annual Cybersecurity Global Excellence Awards
- **Frost & Sullivan Market Report:**  
Increasingly Sophisticated Threat Landscape Drives the Uptake of Managed Security Services in APAC
- **Garner Insights:** Cloud Intrusion Detection and Prevention Market Research Report 2021-2027

# Herd Immunity from Computer Worms

**Remember computer virus worms? That nasty form of malware that crawled around the Internet, infecting everything it could find and then forcing those infected hosts to continue the virus's spread? Recalling these, in our contemporary context of COVID-19 and vaccination programs, made us think about herd immunity and how that term applies equally to both computer and human viruses.**

## Reproduction Number

The Basic Reproduction Number (**R<sub>0</sub>**) of a virus is a term used to describe the expected number of cases directly generated by one case in a population where all individuals are susceptible to infection. SARS-CoV-2 (the virus that causes the COVID-19 disease) has an **R<sub>0</sub>** somewhere between 2 and 3, Polio about 5 to 7, Mumps 10-12, and Measles (one of the most infectious of viruses) around 12 to 18. **Think about those numbers for a minute.**

Each case of Measles goes on to infect 12 to 18 other people in a population without protection. Then each of those 12 to 18 people goes on to infect another 12 to 18, etc. Exponential growth, and pretty scary when you think about it.

Now, in any population, the Effective Reproduction Number (**R<sub>e</sub>**) - the average number of new infections caused by a single infected individual in a partially susceptible population; should be less than **R<sub>0</sub>**. Some individuals either have natural immunity or gain immunity through previous infection, vaccination, or isolation. With computer viruses, immunity is achieved either by patching the flaw the virus is exploiting (by anti-malware technology) or by network isolation/firewalling (the computer equivalent of social distancing). In both humans and computers, quarantine is an effective technique to limit the number of hosts an infected individual can contact to further reduce the disease's spread.

If the **R<sub>e</sub>** stays above 1, then the number of hosts infected increases, and the virus spreads. If the **R<sub>e</sub>** remains below 1, then the virus peters out and disappears. In reality, the number goes up and down over time, resulting in the waves of infection we so often see.



## Herd Immunity

Herd Immunity is all about reducing the **Re** of a virus by reducing the percentage of individuals it can infect.

Think about a virus with an **Ro** of 2 and a population with no protection (100% susceptible to infection). A single infected host passes on the infection to two others. Now, in a population where more than 50% of people are immune, the **Re** would fall below 1 (as more than half of those two previously susceptible to infection are no longer in danger), and the virus would slowly go away. When less than 50% are immune, the virus will continue to spread (**Re** > 1) at a rate dependent on the inverse of the percentage of population immune. You can see how the magic number for Herd Immunity depends on the infectiousness of the disease and the effectiveness of the protection.



## Computer Virus Worms

Now, let's bring this back and look at how this affects computer virus worms' behaviour. While human viruses typically have incubation periods (the time between infection and infectiousness to others) of days, weeks, or years; computer viruses are commonly instantly infectious. So while the transmission time of the infection may be similar, this lack of incubation period, coupled with the speed of light transport, means computer viruses spread much more rapidly than human viruses.

A typical zero-day computer virus worm will exploit a vulnerability in a particular version of an operating system or application to infect a remote host and then use that host to continue to spread the virus. For such viruses, the **Ro** is usually extremely high and dependent only on network and CPU host bandwidth (how fast it can scan and how many vulnerable hosts there are). These viruses can bring networks to a standstill just with their scanning and infection activity as they try to spread. In the early stages of the virus worm launch, the effective reproduction number is usually similarly high (particularly for those viruses targeting popular applications or operating systems).

Hosts gain immunity, or at least stop being infectable and infectious, in one of a few ways:

1. Not running those vulnerable operating systems or applications.
2. Applying patches to protect against the vulnerabilities being exploited (either on the host itself or via virtual patching).
3. Anti-malware signatures or heuristic protection.
4. Isolation from the infected networks (either via firewall or physical controls).
5. Being taken offline due to system damage caused by the infection (aka death).

So what we see when such virus worms are launched is an immediate and rapid increase in scanning activity from the virus looking for hosts to infect. At this stage, as so many targets without protection exist, the rate of infection is often exponential and dramatic. For many worms, this brings networks to a crawl and is so very obvious. Then, typically within a few hours, the anti-malware companies start to release and distribute signatures (aka vaccines). One by one, infected hosts are brought offline and cleaned (cured), while others are protected by their anti-malware systems (vaccination).

Smart and pro-active administrators start isolating their vulnerable systems to prevent and/or contain infections, and the effective reproduction rate starts to fall. Manufacturers release patches to fix the vulnerabilities, and these are installed. As time goes by, the population of potentially infectable hosts falls, and it takes longer for the worm to scan to find each new vulnerable target. The effective reproduction number continues to fall until the magic point of Herd Immunity is reached, the number falls below 1, and the virus worm slowly disappears into obscurity.

Unlike human viruses (where most are commonly suppressed by our immune systems to stop us from being infectious during recovery in some days/weeks), infected computers continue to be infectious until their owners take active steps to stop them. That can take months, or years in some cases, so flare-ups of old viruses can still happen long after the initial release. But eventually, the worm dies off to obscurity, only to be revived in bar room stories told by hard-working network administrators.

**The simple steps of isolation/quarantine, patching vulnerabilities, and updating anti-virus, have brought the reign of that virus worm to an end. If only it were so easy to defeat COVID-19.**

# Network Box

5

## NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th April 2021, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOC's will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

## Network Box 5 Features 2021 Q2

This quarter, for Network Box 5, these include:

- Support for upcoming cloud services release
- Enhancements to entity system in proxy services
- Improvements to box image display in admin web portal
- Release support for new V-38 box model
- Release support for new E-2000i and E-4000i 2021 box models
- Support for Microsoft Hyper-V
- Enhanced capabilities for WAF HTTP path redirection



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



## Globe Awards 2021 17th Annual Cybersecurity Global Excellence Awards



Network Box is extremely proud to announce that it was named a **Globe® Awards Grand Winner** at the 17th Annual 2021 Cyber Security Global Excellence Awards.

In addition to taking home a Grand Award, Network Box also took home Gold Awards for Security Monitoring, and Software-Defined Networking (SDN) and Network Function Virtualization (NFV) Security. Furthermore, Network Box received Silver Awards for Managed Security Services, Secure Web Gateways, and Security Information and Event Management (SIEM).

**LINK:**  
<https://globeawards.com/cyber-security-global-excellence-awards/winners/>

## Frost & Sullivan Market Report: Increasingly Sophisticated Threat Landscape Drives the Uptake of Managed Security Services in APAC



Network Box was in **Frost & Sullivan's Market Report**. The company was listed as a managed security service provider (MSSP) that offers managed security services (MSS) that help manage and monitor their customers' IT infrastructure's security posture.

**LINK:**  
<https://bit.ly/2O8OV2R>

FROST & SULLIVAN

## Garner Insights: Cloud Intrusion De- tection and Prevention Market Re- search Report 2021-2027

Network Box was listed as a **Top Key Player** in **Garner Insights's** Cloud Intrusion Detection and Prevention Market Research Report 2021-2027.

**LINK:** <https://bit.ly/2PcL9pL>



### 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](mailto: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](http://www.network-box.com)