In the Boxing Ring
JUNE 2020

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

This month, we are talking about **Viruses: Biological versus Computer**. During this time of the COVID-19 pandemic, those of us working with computer viruses continue to be amazed at the similarities between the techniques used by the medical community to fight SARS-CoV-2 (the virus that causes the COVID-19 disease) and the processes involved in our electronic anti-virus systems. On pages 2 to 3, we highlight the similarities and see how computer anti-virus researchers help protect.

In other news, Network Box has published materials and an executive summary video for the **Dark Web**. And in this month's Media Coverage, Network Box was featured in numerous media outlets, including: The **South China Morning Post**, **Cyber Houston**, and **Funkschau**. Furthermore, cybersecurity issues were found with the **German Government** and IT services giant, **Cognizant**.

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

VIRUSES: Biological versus Computer

During this time of the COVID-19 pandemic, those of us working with computer viruses continue to be amazed at the similarities between the techniques used by the medical community to fight SARS-CoV-2 (the virus that causes the COVID-19 disease) and the processes involved in our electronic anti-virus systems. Let's look at some of these similarities, and see how computer anti-virus researchers help protect.

What is the Virus?

SARS-CoV-2 is an RNA virus. Essentially, a strand of information wrapped up in a protective shell and a mechanism to infect cells - information, envelope, infection mechanism.

By comparison, a computer virus consists of the payload, a carrier, and an exploit mechanism. For example, the payload would be the malicious code, the carrier an email message, and the exploit mechanism something to take advantage of a vulnerability in a particular mail client. Another example would be script downloaded from a web page, taking advantage of a web browser exploit.

Replication

The virus's primary purpose is to replicate - to make copies of itself. SARS-CoV-2 does this by infecting cells (in the lungs, stomach, and other areas of the human body), then using the cell's own mechanisms to make copies of its RNA and make new virus particles.

Computer viruses have the same primary purpose of replication. They want to infect as many hosts as possible. Once in a computer system, they make multiple copies of themselves and transmit out to new hosts. It is this self-replication capability that defines this as a virus.

Identification and Testing

The gold standard for identifying viruses is the whole genome sequence. This maps the full sequence of the chemical components of the RNA (made up adenine, uracil, guanine, and cytosine; abbreviated as A, U, G, and C), and results in a very long string of these four letters. That is excellent for precise identification, but not so good for testing. Due to mutations, what we know of as SARS-CoV-2 is actually a collection of hundreds of different strains of the same fundamental virus, each with their own slightly different sequences (more on this later).

To test for the virus, researchers instead concentrate on relatively small portions of the full sequence. This way, they can extract samples from a potentially infected human, amplify the RNA in the sample to obtain enough to test with, and then compare that against the portion of the full sequence. That is the RT-PCR test.

Computer virus researchers work similarly. The payload of the virus itself is a sequence of computer code that can be expressed in binary, or more commonly in hexadecimal notation. Computer viruses are often intentionally self-encrypted and randomized (we call these polymorphic viruses) to avoid whole sequence detection. Nowadays, these are by far the most common form of computer virus seen.

Researchers extract portions of the sequence that don't change and use pattern matching techniques to detect those partial sequences in suspicious samples. We call these **signatures**, and they can be effectively used to detect known viruses in suspicious samples.

Immune Response and Vaccination

The human immune system has a component known as the **adaptive** immune system. The system works by identifying portions of viruses already in the body, and creating antigen-specific cells designed to identify, remember, and attack that specific antigen. These cells protect against future infections of the same virus and can survive in the body for some time (months, or years, typically). This is why after you've had the measles once, for example, you usually don't get it again. Vaccinations work by purposely injecting the body with antigens that will generate such an adaptive immune response, to protect you from future specific infections.

Computer anti-virus systems store databases of signatures of known viruses. When your computer receives a new file, it can scan it, look for a match against those signatures, and take action if a match is found (quarantine, etc). Such signature-based systems are the computer equivalent to the body's adaptive immune system.

Innate Immune Response

Another component in the human immune system is known as **innate**. This system can detect what is not '**you**', (what is foreign), and attack the invader. It relies on the antigen's chemical properties and doesn't need to have previously seen that specific antigen.

For computer anti-virus, this is extremely hard to achieve well. The capability to detect and block previously unknown viruses is what differentiates good anti-virus systems from the poor. Various techniques are used, but mostly revolve around: **a)** decoding the virus code to the rawest form, **b)** detecting suspicious encoding or exploit behavior, and **c)** using emulation or sandboxing techniques to see what the virus does when executed. Looking at behavior, rather than code sequences.

Mutations and the Future

RNA viruses such as SARS-CoV-2 are very poor at accurate replication, and sometimes the copies made are not perfect. Base pairs get flipped. Portions of the sequence are lost. Parts of other viruses are incorporated. Before long, you are dealing with bad copies of bad copies of a bad copy. It is like the story of a million monkeys with a million typewriters, eventually producing the works of William Shakespeare. Sometimes these viral mutations are beneficial to the virus, but most often not. Whatever the outcome, these mutations are the way the virus adapts to further its goal of replication.

Thankfully, we do not see the same with computer viruses. A computer virus can and does make perfect copies of itself, 100% of the time. Sure, we have self-encrypting polymorphic computer viruses, and randomizing fragments are often introduced, but the core code of the virus is not changed, and certainly not randomly. Perhaps in time, we will see this, but with today's non-forgiving computer CPU architectures, it is unlikely to be a successful approach. Of course, given enough monkeys and enough typewriters, anything is possible - perhaps even improve on Shakespeare.

BUT, if that day ever comes, you can be rest-assured that Network Box Security Response will be here to adapt and protect you.

Network Box HIGHLIGHTS

The Dark Web
the dark side of the Internet

LINK: https://youtu.be/KGZBrMGzDi8

The Dark Web is the deliberately hidden part of the Internet, which is the natural habitat of hackers and cyber criminals. Whenever there is a data breach, the stolen personal data usually ends up on the Dark Web. Today, there are several billion sets of hacked credentials already posted. To help you counter this, Network Box is offering **Dark Web Monitoring Service**.

LINK:
https://network-box.com/nb5-darkWeb_monitoring

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

SCMP
South China Morning Post

Hongkongers rush to download VPN tools amid fears of Beijing upping surveillance with national security law

LINK: https://bit.ly/2XdiDFG

Cyber Houston
CYBER HOUSTON

Cybersecurity Leadership Series: The Business Side of Cybersecurity

LINK:
https://youtu.be/ZGD5219pvSU

Funkschau
funkschau

CEO Fraud:
In the name of the boss

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

ZDNet
The Federal Government

German government might have lost tens of millions of euros in COVID-19 phishing attack

LINK: https://bit.ly/2TNUjIn

Bleeping Computer
Cognizant

IT services giant Cognizant suffers Maze Ransomware cyber attack

LINK: https://bit.ly/2yHUvRY