In the Boxing Ring SEPTEMBER 2021

Network Box Technical News

from Mark Webb-Johnson
Chief Technology Officer, Network Box

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

This month, we are talking about the **Network Box Anti-Malware Solution**. In the early 1980s, there were less than 3,000 viruses known to exist. By 2020, over 3,000 new virus variants were seen every day. The Network Box anti-malware system deploys multiple approaches supporting more than 700 methods of archiving, encrypting, encoding, and packing viral code. On pages 2 to 4, we discuss the history and the global statics of malware today and highlight the various malware detection technologies deployed by Network Box.

Also this month, we are pleased to announce the latest revision to the Network Box M-395i. With upgraded hardware, the 2021 version of the unit provides enhanced performance.

In this month's media coverage, Network Box was featured in the SCMP, and the latest edition of the HPCC Hackpod is now available. Furthermore, there had been numerous security vulnerabilities in this month's global security headlines.

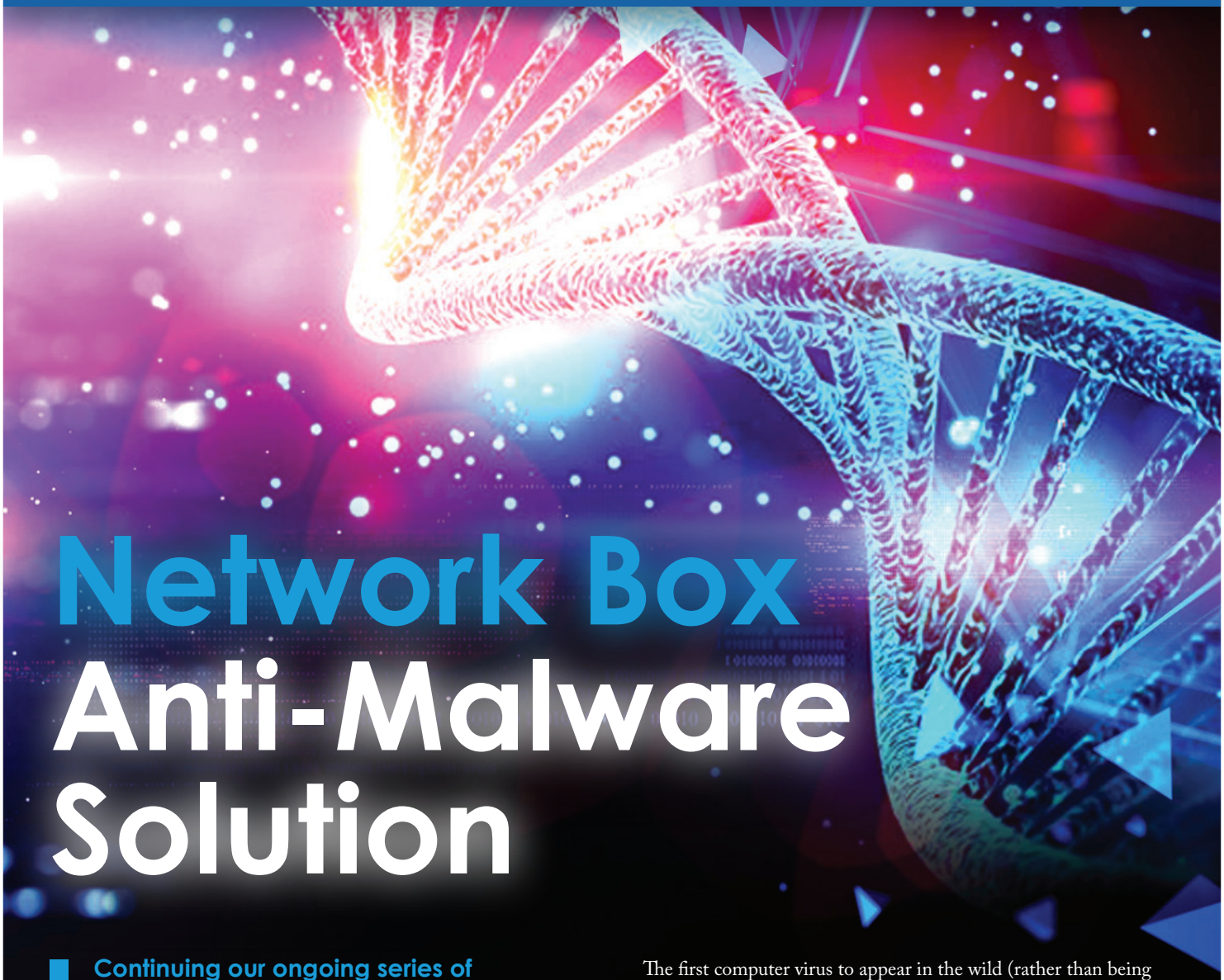
Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2021

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:



Network Box Anti-Malware Solution

Continuing our ongoing series of Network Box technology deep dives, we will be talking about the Network Box Anti-Malware solution in this article.

Background

The term 'computer virus' has evolved significantly over the years. While first it was used to refer to a specific set of self-replicating software programs, it is now commonly used to refer to a whole host of malicious software (malware), including:

- Email Worms
- Network Worms
- Trojan Horses
- Trojan Droppers
- Compromised website scripts and downloaded malware

Throughout the rest of this article, Network Box will refer to all these classes of malware as 'computer virus.'

The first computer virus to appear in the wild (rather than being created and staying in a laboratory) was known as **Elk Cloner**. Rich Skrenta wrote it in 1982, and it replicated by attaching itself to the Apple DOS 3.3 operating system passed around on floppy disks. Most of these early viruses were disk or file infectors and spread by file sharing.

As wide-area computer networks (such as bulletin boards) became popular in the 1980s and early 1990s, the number and spread of viruses increased dramatically. But, it was the advent of the Internet and the World-Wide-Web that provided the mechanism for the birth of the computer worm.

In the early 1980s, the vast majority of computer viruses were classic file and disk infectors. Today, over 99% of all viruses are email or network carried worms. In the early 1980s, it would take weeks for a new virus to propagate around the World. By 2020, computer worms often took less than 2.5 hours to reach their peak infection rate.

In the early 1980s, there were less than 3,000 viruses known to exist. By 2020, over 3,000 new virus variants were seen every day.

As the nature of the threat changes, so must the techniques used to fight that threat.

The Impetus for Change

More has changed in the past two years of computer virus protection than in the previous 20 years. Statistics from the global network of Network Box Security Response centers show:

- **A dramatic increase in the number of distinct threats seen**
  Years ago, one new variant of a particular virus would be seen, perhaps, once a month. Now, computer virus researchers are often seeing dozens of new variants in 24 hours.

- **A dramatic decrease in the time taken for a threat to reach peak infection levels**
  A standard measure is the time taken for the infection rate (detections/blocks per minute) to reach half its peak level. Virus variants now reach this point within less than 1 hour.

- **New techniques for bypassing protection devices have appeared**
  These include password-protected archives, vulnerability exploitation, social engineering, message fragmentation, and standards bypass.

- **The use of spamming techniques for the initial propagation stage of virus seeding**
  Thus, significantly increasing the initial rate of spread.

- **Forging of sender addresses**
  To obfuscate and confuse the tracking of messages and infected sources.

- **Commercial involvement**
  Primarily in setting up botnets and spamming sources, using trojan droppers and backdoor programs to maliciously take control of remote computers, establish a network of computers for criminal purposes, and install ransomware.

Technologies for Malware Detection

There are several technologies that can be used to detect whether a given object contains viral code or not. Prior to scanning for virus code, the object should be fully unpacked, using a combination of the following techniques:

1. **Object Archive Unpacking**
   Before scanning, objects should be unpacked using a selection of archive unpackers. This will extract sub-objects and add them to the set of objects to be scanned. Sample archive formats include MIME, ZIP, TNEF, RAR, etc. – several hundred different formats exist in the wild and should be supported for unpacking.

2. **Object Encrypted Archive Unpacking**
   Viral code can be hidden inside encrypted archive formats. Before scanning, objects should be unpacked using a selection of archive unpackers. This will extract sub-objects and add them to the set of objects to be scanned. Sample archive formats include MIME, ZIP, TNEF, RAR, etc. – several hundred different formats exist in the wild and should be supported for unpacking.

3. **Object Encoding Unpacking**
   Similar to Object Archive Unpacking, there exist several encoding formats, which should be supported. Sample encoding formats include base64, uuencode, binhex, quoted-printable, etc. – several dozen different formats exist in the wild and should be supported for unpacking.

4. **Object Packer Unpacking**
   Executable programs are rarely stored as straight binary; they are typically packed using various schemes. Some anti-virus scanners apply signatures against the unpacked object, but that is not a sensible long-term solution – merely choosing a different packing scheme and re-packing the object will cause the anti-virus signature to miss the new version. A better solution is to unpack the executable program to a raw binary stream (onto which signature, heuristic, or other anti-virus technologies can be applied).

There are more than 700 methods of archiving, encrypting, encoding, and packing viral code. A comprehensive anti-virus solution, such as the Network Box, must support all of these mechanisms to provide the best possible virus detection ability.

Once the object has been fully unpacked, to a set of binary streams ready for scanning, the following anti-virus techniques can be applied:

String Signature Scanning
This is the most basic technique used to detect known virus code. A set of string (text or binary) signatures is maintained, corresponding to known viral patterns. Each object to be scanned is compared against this signature set – a match is a positive indication of a virus. While powerful, simple, and quick, this technique is limited in detecting polymorphic or complex viruses.

Wildcard Signature Scanning
Similar to, but more sophisticated than, basic string signature scanning, wildcard signature scanning extends the signatures to support wildcards (matching one or more characters). This is typically slower than basic string scanning but provides a better ability to detect complex viruses.

Regular Expression Signature Scanning
Similar to, but more sophisticated than, wildcard signature scanning, regular expression signature scanning extends the signatures to support full regular expressions (matching combinations, alternates, ranges, etc. of characters). This is typically slower than wildcard string scanning but further extends the power and flexibility of the anti-virus system to detect complex viruses and their variants. Often, regular expression signatures can be built to detect whole families of viruses in one signature set. These generic signatures are beneficial during outbreaks of new variants of existing viruses.

Hashing Signature Scanning
Cryptographic hashes of the entire or part of the object can be used to obtain digital signatures and quickly compare them against a database of known virus signatures. This can provide similar functionality to wildcarding and provides for accurate, positive identification of viral code.

Bookmarks (Fixed Offset Scanning)
Bookmarks (signatures at a specified offset and length) can be used to increase the accuracy and speed of signatures. These limit the scan to a specified portion of the object.

Mutation Avoidance Scanning
Virus mutator kits alter viral code by randomly adding nonsense and other useless instructions to viral code and cause standard signatures to miss. The mutation avoidance technique strips such useless instructions from the code stream before signature comparison and hence, works around the problems of virus mutator kits.

Virus-Specific Scanning
Often, new viruses use new techniques not immediately supported in the previous standard scanning techniques. Examples might include new encryption, polymorphism, or packing systems. To successfully detect and block such threats quickly, the anti-virus system code itself must be able to be updated with new algorithms and techniques. Such virus-specific scanning code will typically look for a particular, often emerging, virus family.

Detection Filtering
Primarily for performance reasons and for avoidance of false positives, the anti-virus system should be able to run specific technologies or signatures against specific object types or parts of objects.

Code Decryption
Viruses often include code to encrypt themselves. Coupled with a random polymorphic generation function and encryption key, this can effectively block effective viral signature matching. Anti-virus systems require the ability to decrypt either by algorithmic or brute-force such code to detect the virus contained within.

Code Emulation
This technique involves executing the segments of executable code in a protected and emulated environment. The emulation can either be used to determine the purpose (i.e., functions called) of the code or to allow the code to decrypt itself prior to conventional scanning. Such advanced techniques are heuristic in nature and often used for the detection of polymorphic and self-encrypted viruses.

Geometric Detection
In order to infect a file, a virus must alter the structure of that file. Often, these alterations to the geometry of the file's structures are detectable in a generic fashion. Such heuristic detection is excellent for detecting a family of viruses.

Executable Code Heuristic Analysis
Heuristic analysis is the detection of virus code by behavior, shape, or some such variable attribute. Heuristics are never 100% and often give a probability that the particular code is viral or not. Heuristics are essential for detecting macro, script, and other such highly variable viruses.

Standards Enforcement / Exploit Detection
Modern computer viruses often attempt to exploit known vulnerabilities in software applications: email clients, web browsers, or network applications. Standards enforcement coupled with exploit detection is a highly effective mechanism to detect and block such behavior.

Individually, each of the above techniques is of limited value. But, taken together, they form an effective anti-virus system. Nowadays, it is insufficient to merely apply one or two techniques or just basic string/wildcard signature scanning. An effective defense requires a complete package of technologies and the ability to detect and defend against previously unseen virus code proactively.

The Network Box anti-malware system deploys multiple approaches supporting more than 700 methods of archiving, encrypting, encoding, and packing viral code. Once the raw binary data stream has been obtained, a combination of signature, heuristic, and emulation technologies are used by multiple engines to detect malicious contents. This approach is used to protect traffic in network protocols such as web, email, and file transfer.

Network Box HIGHLIGHTS

Network Box
M-395i Hardware Upgrade

Network Box is pleased to announce our latest revision to the M-395i hardware unit with improved performance. In addition to an upgraded CPU, RAM, and Hard Disk, the new M-395i comes with 6 x 1Gb RJ45 and 2 x 1Gb SFP+ ports as standard, with further expansion options. Please use the link below to download the datasheet for technical specifications of the 2021 edition of the M-395i.

LINK:
https://www.network-box.com/sites/default/files/files/NetworkBox_M-395i_2021Edition.pdf

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

Media Coverage & Security Headlines

SCMP
South China Morning Post

China hatches a plan to lead in the adoption of new internet protocol as Beijing eyes internet of things
LINK: https://bit.ly/3yEyRa3

HPCC Hackpod Club
HPCC HACKPOD CLUB

Episode #11:
How to find the right cyber policy
LINK: https://bit.ly/3x7xuAV

CRN
accenture

Accenture Hit By Ransomware Attack, Latest Victim of 'Cyber-Pandemic'
LINK: https://bit.ly/3DHbXmn

The Hacker News
FORTINET

Unpatched Remote Hacking Flaw Disclosed in Fortinet's FortiWeb WAF
LINK: https://bit.ly/38zWtSM

Bleeping Computer
CISCO

Cisco won't fix zero-day RCE vulnerability in end-of-life VPN routers
LINK: https://bit.ly/3t9I750

CNBC
Microsoft

Microsoft warns thousands of cloud customers of exposed databases, email shows
LINK: https://bit.ly/2VcLZFP