In the Boxing Ring
JUNE 2022

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

Welcome to the June 2022 edition of In the **Boxing Ring**

This month, we are talking about **Ransomware and the Dark Web**. Most companies nowadays gather, store, and handle highly confidential client information. Such personal data is an integral part of almost every company's day-to-day existence. However, imagine needing some crucial data only to find access to your server, desktop computer, laptop, data file, backup file, or cloud backup file encrypted and blocked by Ransomware. Additionally, picture a situation where a hacker gains access to your network using a password that other hackers had stolen from your staff posted on the Dark Web. These aren't just hypothetical problems. Many businesses worldwide have been forced to face precisely such a nightmare in real life. On pages 2 to 4, we discuss this in greater detail.

In other news, Network Box was listed as a *Top-Tier Player* in the **Cloud Intrusion Detection and Prevention Market**. Additionally, Network Box was featured in **it-daily**, and the latest episode of **HPCC Hackpod Club** is now available. Finally, in this month's Network Box customer testimonial, *Andrew Powner,* Managing Partner of **Haldanes Solicitors & Notaries**, shares his experience of how Network Box has helped with their cybersecurity.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2022

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:

RANSOMWARE and the Dark Web

Most companies nowadays gather, store, and handle highly confidential client information. Such personal data is an integral part of almost every company's day-to-day existence. There is a self-evident need to ensure that such data hasn't been altered. Continued and timely access to any required documents, emails, and plans, are also critical.

Imagine needing some crucial data only to find access to everything blocked by Ransomware. Everything is encrypted and inaccessible. Every server, desktop computer, laptop, data file, backup file, and even cloud backup file is rendered useless. This isn't just a hypothetical problem. Many businesses worldwide have been forced to face precisely such a nightmare in real life. Just as an arsonist can burn down your office, a hacker can delete your entire digital existence.

This isn't just a hypothetical problem. Many businesses worldwide have been forced to face precisely such a nightmare in real life. Just as an arsonist can burn down your office, a hacker can delete your entire digital existence.

Hackers leverage panic. Hackers leverage value. Hackers leverage the fact that the last thing any business wants or can afford, is to suffer the massive reputational loss of being successfully breached by a hacker. And once a hacker has had control of a company's computer systems, it becomes difficult to assess if something has been stolen or to trust any of the data stored on those systems has not been tampered with, even if control has been supposedly restored.

Yet, so few companies seem to take cybersecurity seriously. Despite being extremely practical for protection against cyber threats, it also can relieve the danger of being sued by angry clients.

Hackers have changed

Some thirty years ago, their goal was to (perhaps) delete your data and (somehow) make themselves 'famous.' But over time, hackers realized they could use their technical skills to make a lot of money. Ransomware alone is now estimated to be a USD 10 billion-a-year industry.

Over time, even Ransomware itself has evolved

Traditionally, Ransomware encrypted your data, displayed a countdown clock on your computer screens, and threatened to delete all of your files if you didn't pay the hackers if and when the countdown clock hit zero.

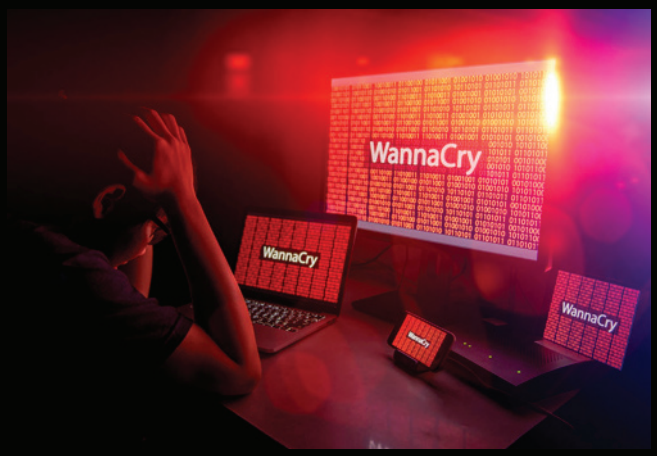
However, companies soon learned that having a good data backup was adequate protection from such an attack. Formatting all infected devices, and restoring them from a recent high-quality data backup, would render the Ransomware attack ineffective.

This has led to modern Ransomware variants, which infect networks, taking their time to spread to every device connected to these infected networks, targeting any backup systems possible, including backup systems in the cloud, and then stealing as much confidential data as possible.

The confidential data is sent back to the hackers, usually overseas, in a country that the police have no jurisdiction over. Only then does the Ransomware encrypt and make access to the victim's confidential data impossible.

This kind of double-edged attack gives the hacker two different bargaining chips. The first is the stranglehold on the victim's operational continuity and access to its critical confidential data. The second, and probably even more critical, is the threat of publishing the stolen confidential data on the Internet, giving the whole world access to their data.

Cyber attacks can come in the form of direct disruptions to a company's on-premises physical file servers. Still, they can equally be attacks on servers located at a third-party data centre or virtual servers located in the cloud. There are computer servers located somewhere, running some form of the operating system and storing some form of the digital data file. Hackers can go after these, wherever they happen to be.



It is also crucial to note - Ransomware is only one form of cyber attack. Just as being shot using a gun is only one form of physical attack, if someone is trying to kill you, there are so many ways they can do so. They could burn you. They could stab you. They could drown you. They could poison you. They could push you down the stairs. The list is almost endless. In the digital world, hackers have an even broader spectrum of tools they can use to attack you or steal your confidential data. The number of potential cyber threats to businesses is legion.

The Dark Web

Some recent high-profile, successful cyber-attacks have stemmed from third-party data breaches, which had no direct relationship with the victim's company. The Colonial Pipeline in the United States, which was shut down by hackers using Ransomware, found that hackers had gained access using a password that other hackers had stolen from a member of their staff posted on the Dark Web. The Colonial Pipeline staff member had registered an account on a website belonging to a completely different organization (that was hacked) but had used exactly the same password they used at work.

Monitoring the Dark Web would almost certainly have prevented that shutdown.

In the end, the company paid a ransom of US$ 4.4 million to a Russia-linked cybercrime organization called ***Darkside*** before the critical network systems could be released and the oil pipeline reopened. Interestingly, the FBI managed to recover US$ 2.3 million in Bitcoin from the hackers. Ironically, this was also due to some poor password management on behalf of the hackers themselves.

Yet how many businesses are monitoring the Dark Web for credential leaks?

Hackers don't discriminate

Every company needs to protect itself. Small companies are not exempt from cyberattacks; hackers will not ignore your company just because it isn't famous or doesn't employ hundreds of staff.

In actuality, many cyberattacks, such as Ransomware attacks, are random in nature. An SME is just as likely to become a victim as a large global conglomerate. The most significant difference may be that a large organization will probably be more able to absorb the overall disaster, including the hit to its reputation, better than an SME.

In the USA, where reporting data breaches is required in certain cases, various companies have admitted to getting hacked and that hackers have published their confidential data. Yet, despite the obvious, undeniable, absolutely critical need for effective cybersecurity to be in place at every business, it simply isn't. Not even close.

When it comes to cybersecurity, one needs: real-time push updates to keep ahead of cyber-threats, cyber-security that is certified and audited to internationally recognized standards, and cybersecurity that is backed up by actual experts who monitor and manage the required systems around the clock.

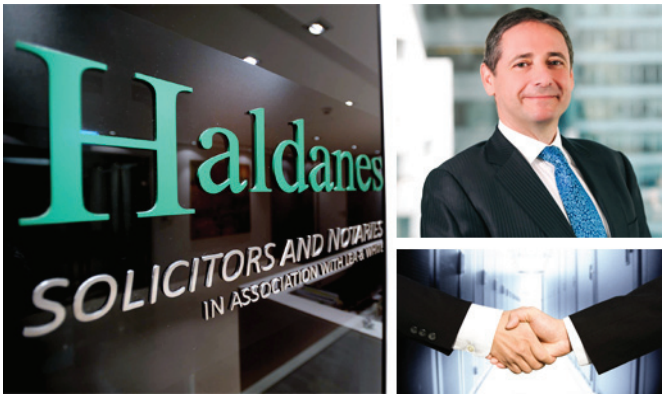
Most companies are simply not protecting themselves. It doesn't make sense, even from a purely financial perspective. For a small business to be professionally protected by a fully managed, certified cybersecurity service provider would cost them annually less than the monthly salary of a junior staff.

Every company's management should work out how much the utter disaster of being compromised would cost and how much being properly protected would cost. The two figures cannot even be remotely compared. Not just in financial terms either, one can lose a hard-won reputation gained over many decades in a single moment.

Get protected. Now.

Network Box HIGHLIGHTS

Network Box Customer Testimonial: Haldanes Solicitors & Notaries



LINK: https://mcdn.network-box.com/CS/Haldanes_Testimonial.pdf

"We asked Network Box to design a series of cybersecurity solutions suitable for our business and develop a Disaster Recovery Plan. These have been continuously updated and are used to this day. We feel very satisfied. Partnering with Network Box was the right investment for us."

Andrew Powner
Managing Partner of Haldanes Solicitors & Notaries

Haldanes www.haldanes.com

Haldanes Solicitors & Notaries is an award-winning Hong Kong-based law firm experienced in serving the needs of clients, both locally and throughout the Asia-Pacific.

Cloud Intrusion Detection and Prevention Market: In-Depth Industry Analysis 2026

The recent study on Cloud Intrusion Detection and Prevention Market scrupulously analyzes the workings of this industry vertical and its trajectory over 2020-2025. It expounds on the major trends, top growth indicators, profitable prospects, limitations, risks, and challenges that will mold the business dynamics in the forthcoming years.

Top-tier players in the Cloud Intrusion Detection and Prevention by market size are: Network Box, BAE Systems, Juniper Networks, AT&T, Cisco Systems, CounterSnipe Technologies, Alert Logic, Check Point Software Technologies, Dell SecureWorks, Clone Systems, Symantec, Extreme Networks, IBM and McAfee.

LINK: https://bit.ly/3GHW7cT

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

it-daily
Sensor takes over blacklist check
LINK: https://bit.ly/3tduwem

HPCC Hackpod Club
Episode #15: ***This is how security awareness becomes sexy***
LINK: https://bit.ly/3Q0nxiK