In the Boxing Ring
FEB 2019

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

Welcome to the February 2019 edition of In the **Boxing Ring**

This month, in our feature article, Network Box's Managing Director, Michael Gazeley, talks about **The Dark Side of the Internet**. Whenever there is a massive data breach, that personal data usually ends up on the Dark Web. There are currently over **6.5 billion** sets of hacked credentials already posted on the Dark Web, and the number is growing fast. On pages 2 to 3 we discuss how hackers and cyber criminals can leverage these stolen credentials for malicious activities, and how does this all impact you.

Also this month, **DNS Flag Day** was on 1st February 2019. This change only affect sites operating non-compliant software, and will make most DNS operations slightly more efficient, and also allow operators to deploy new functionality, including new mechanisms to protect against DDoS attacks.

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

In other news, Network Box USA's CTO, Pierluigi Stella, gave a cybersecurity webinar to various universities in the USA title, **"The importance of security in today's tech-driven world"**. In addition, Network Box was interviewed by numerous media outlets about the latest security issues including the **SCMP**, **The Standard**, and **RTHK Radio 3**. Finally, the 2018 edition of the **Network Box Technology Review** is now available for download.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2019

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://plus.google.com/u/0/107446804085109324633

In this month's issue:

The DARK SIDE

What do bomb threats, webcam hoaxes, fake credit cards, identity theft, and targeted hacking, increasingly have in common?

The Dark Web

by Michael Gazeley
Managing Director
Network Box

The Dark Web is the deliberately hidden part of the Internet, which is the natural habitat of of hackers and cyber criminals. This 'dark side' of the Internet, can only be accessed with specialist knowledge, and specific software tools. Perhaps the most famous such tool is TOR (The Onion Router). Other examples include Riffle, Freenet, and I2P (Invisible Internet Project).

Whenever there is a massive data breach, that personal data usually ends up on the Dark Web. There are currently over 6.5 billion sets of hacked credentials already posted on the Dark Web, and the number is growing fast.

In most cases, the companies and organizations who suffered these breaches, clearly didn't do enough to secure themselves from cyber-criminals.

Far from leveraging critical cyber-security systems and services to protect their client data effectively, many firms' customer data was compromised, because databases were put online without having had security patches applied for up to a year, or in some cases, because databases were put online without even basic password protection.

We are talking about certain banks and credit card companies, making millions of their customers' private data available online, with literally no security at all.

Many managers wring their hands and say, 'it's impossible to protect our networks from EVERY kind of attack,' but in reality, there are far too many cases, where networks are not properly protected from ANY kind of attack.

So how does all this impact you?

First, there is the loss of privacy. If your doctor, bank, credit card company, travel agency, hotel, children's school, lawyer, accountant, or a government department, leaks your private data onto the Dark Web, then your data is out there forever. Everything from how much money you have, to your children's identities, to your medical condition, to your travel itinerary, to your photos and videos, to your physical location, maybe compromised.

Second, there is the potential for direct access to critical accounts, especially if you have reused passwords. It maybe that your bank, credit card company, or your workplace, has been hacked. In such a case, a hacker could just login to your accounts, and directly take advantage. This is why dual factor authentication, is so important. It is also possible, if you have reused passwords, that a hacker can try a password they took from a third-party data breach, on your bank or workplace. This is why reusing the same password on multiple accounts, is a very bad idea.

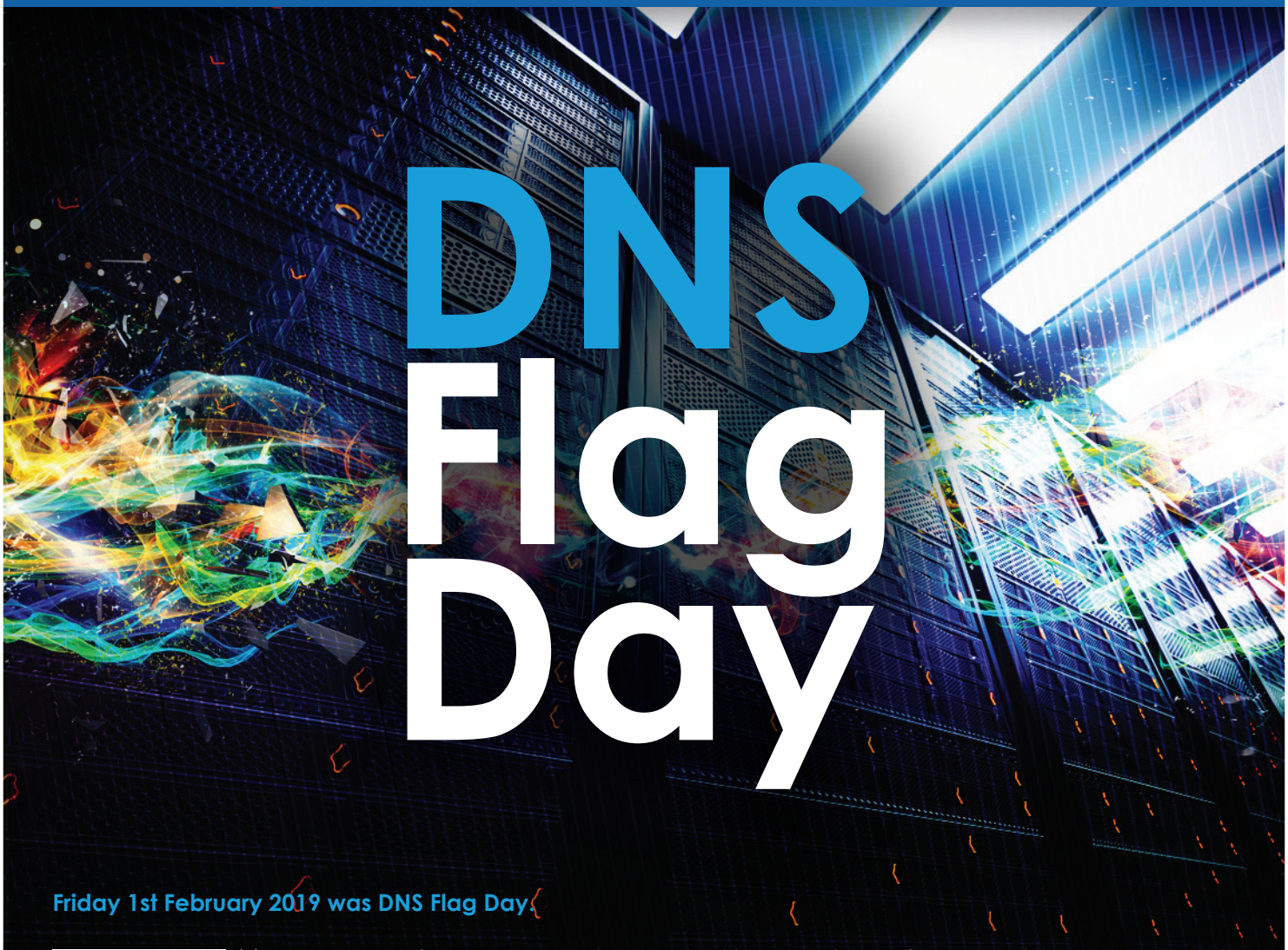
Third, are 'hoaxes.' Although that actually might not be the right word, to describe what criminals are actually doing. After all, a criminal may say they have hacked your webcam, when they haven't, making the claim a 'hoax,' but on the other hand the blackmail being carried out is very 'real.'

There have now been millions of emails sent out to people, claiming that a hacker has captured them on video, while they were browsing an Adult Website, using their hacked webcam. These evolved into physical bomb threats as well.

The connection to the Dark Web is both the email address to send the blackmail to, and also, and this is the key, the person's actual password, which will often scare the potential victim into thinking everything else written, must be 'real' too.

Given the number of panic calls for help, which Network Box has received over the last few months, we have rapidly developed, and will be offering, an optional Dark Web Monitoring Service very soon. This is so that our clients can receive continual automated updates, highlighting which of their organization's people, have hacked sets of credentials, posted on the Dark Web.

This will allow IT Departments to educate their users, so they can further appreciate the importance of cyber-security, and help to defend their devices, networks, and data, even more comprehensively. Additional Cyber-Threat Intelligence, and Cloud Reputation monitoring, will also be part of this new Dark Web Monitoring Service.



DNS Flag Day

Friday 1st February 2019 was DNS Flag Day

The previous DNS was unnecessarily slow and inefficient because of efforts to accommodate a few DNS systems that are not in compliance with DNS standards established two decades ago.

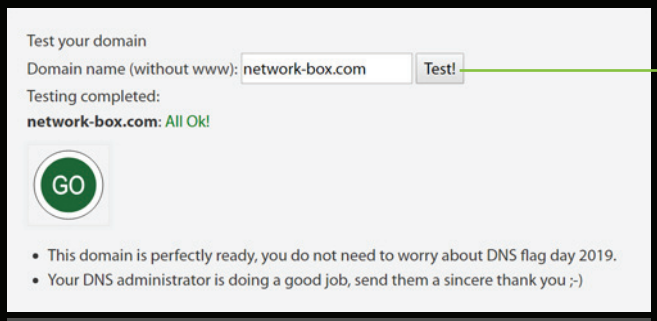
To ensure further sustainability of the system it was time to end these accommodations and remediate the non-compliant systems. This change will make most DNS operations slightly more efficient, and also allow operators to deploy new functionality, including new mechanisms to protect against DDoS attacks.

Major DNS software and service providers have agreed to coordinate removing accommodations for non-compliant DNS implementations from their software or services, on February 1st 2019. This change affects only sites operating non-compliant software.

All Network Box systems are now, up-to-date with this switchover. In particular, the Network Box NBRS-3 and Network Box 5 resolver and caching DNS servers, as well as our Cloud DNS servers. However, external DNS servers themselves (either on customer premises or in the cloud) may not have made the change. In particular, TCP port 53 should be opened to DNS servers, and those servers correctly configured to prevent unauthorised zone transfers.

If you have not yet made the transition, you can test the readiness of your domain(s) with the link below:

https://dnsflagday.net/



Enter your domain name into the test box provided, click Test! and view the results.

If you need assistance with firewall policy (for DMZ hosted DNS servers), please contact your regional SOC for support.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th February 2019, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
February 2019

This month, for Network Box 5, these include:

- Administrative improvements to scanning system maintenance
- Performance improvements in scanning system
- Enhanced logging support for multi-line replies in SMTP protocol
- Improvements to updating of kernel based IP address sets
- Enhanced support for policy control over permitted HTTP methods
- Improvements to policy control in WAF firewalls
- Enhanced support for NOC systems

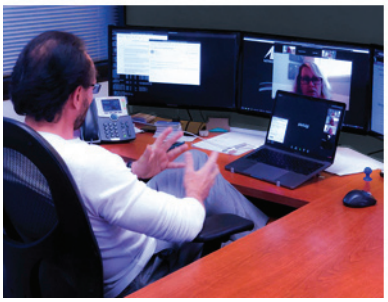
In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

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

Network Box USA
Cybersecurity Webinar

Network Box USA's CTO, Pierluigi Stella, gave a live, online talk and Q&A session to the University of Texas at Austin, UT Austin in Houston, Southern Methodist University and Washington University. The topic being, **"The importance of security in today's tech-driven world"**.



Network Box Media Coverage

South China Morning Post

Network Box's Managing Director, Michael Gazeley, and also Mark Webb-Johnson, Network Box's Chief Technology Officer, were interviewed, by Simone McCarthy, of the SCMP; covering the Dark Web, and its increasing impact and augmentation, on phishing, blackmail, and cyber-crime in general.

SCMP
Hong Kong's smaller businesses think 'we're too small to be hacked' despite hacking experience, insurer finds
LINK: https://bit.ly/2BcjQ4s

The Standard
Click clear of the dark side of life
LINK: https://bit.ly/2FVBpdb

RTHK Radio 3
Surging Cyberattacks
LINK: https://bit.ly/2RWX6A4

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	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
Tech Review 2018

As a special end-of-year review, Network Box has complied the key *In the Boxing Ring* articles and technology news of 2018. Please use the link below to download the 2018 edition of **Network Box Technology Review**.

LINK: https://bit.ly/2G9uooh