



In the Boxing Ring AUGUST 2020



Network Box Technical News

from **Mark Webb-Johnson**

Chief Technology Officer, Network Box

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

This month, we are talking about **Top-Level Domains**. At the dawn of what we know today as the Internet, the ARPA domain was the sole top-level domain. Next, five top-level domains were introduced: *.com*, *.edu*, *.gov*, *.mil*, and *.org*. Today, the root name servers serve 1,509 top-level domains, and below them are tens of thousands more secondary level domains. On pages 2 to 3, we discuss this in greater detail and highlight the security threat in all this.

In other news, Network Box is listed as a top player in the **Global Cloud Intrusion Detection and Prevention Market Research Report 2015-2027**. And in this month's Media Coverage, Network Box was featured in **TIME**, **South China Morning Post**, **The Standard**, **Asia Times**, and **it-daily.net**.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
August 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:

Page 2 to 3

Top-Level Domains

In our featured article, we outline the brief history of top-level domains, discuss the current landscape today, and highlight the security issues related to this.

Page 4

Network Box Highlights:

- Global Cloud Intrusion Detection and Prevention Market Research Report 2015-2027
- Network Box Media Coverage:
 - TIME
 - South China Morning Post
 - The Standard
 - Asia Times
 - it-daily.net

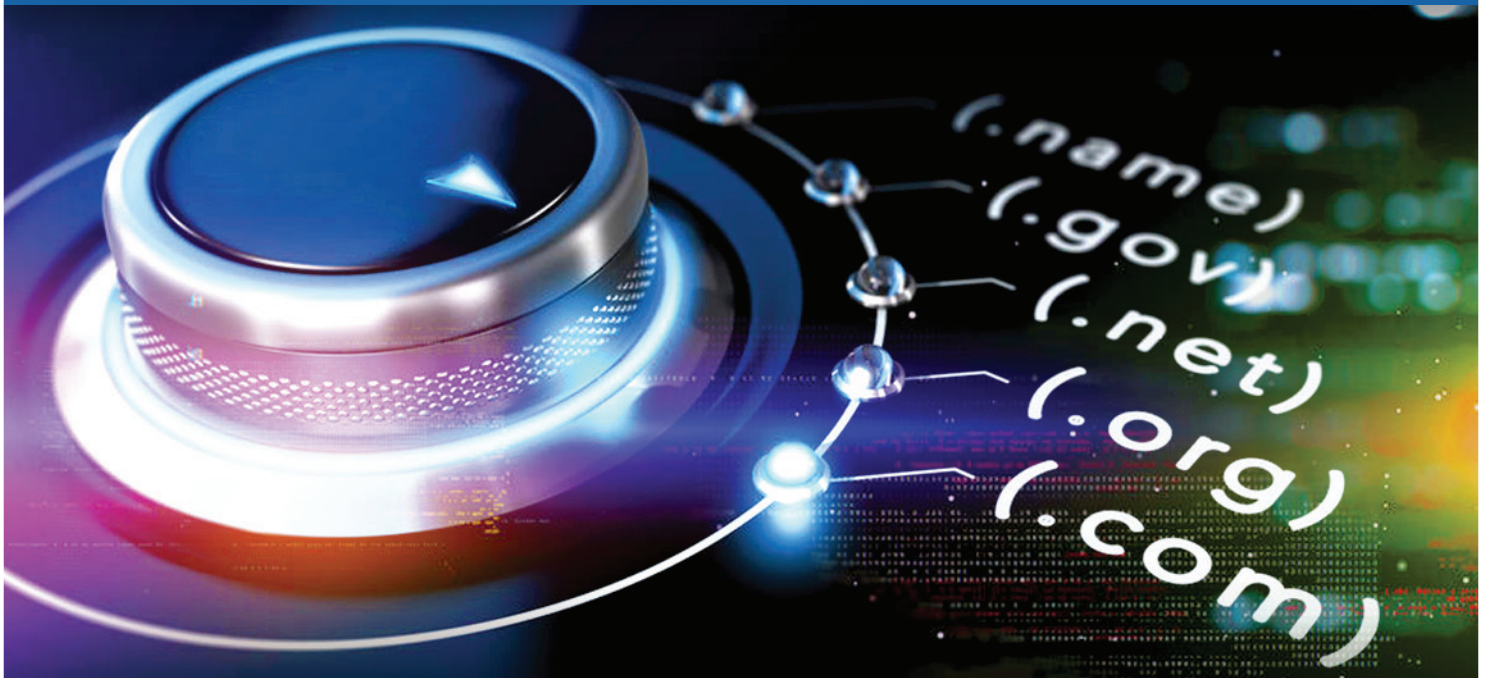
NOTE: With effect from January 2020 we have switched to a quarterly Patch Tuesday cycle for Network Box 5. However, essential security fixes will continue to be released out-of-cycle, if necessary.

Top-Level Domains

At the dawn of what we know today as the Internet, the ARPA (United States Defense Advanced Research Project Agency) domain was the sole top-level domain - used to help transition from ARPANET to the new domain name system. Today, the remnants of this still exist as .arpa; used for reverse DNS lookups (converting IP addresses to domain names).

Next, five top-level domains were introduced: **.com**, **.edu**, **.gov**, **.mil**, and **.org**. As the Internet grew and expanded beyond the USA's borders, this was accompanied by the country-level top-level domains, roughly following the ISO 3166-1 standard. With each country free to sub-delegate under their own top-level country code.

At this point, things were already starting to get complex. Should a company in, say Hong Kong, register under **.hk**, **.com.hk**, or **.com**? To protect its trademarks, perhaps it should be registered under all three? Then what about the hundreds of other country-level domains for countries the company did business in or hoped to do business in the future? At this point, each country was permitted to set the rules for their own domains, such as residency or business registration conditions, resulting in the popularity of the **.com** domain. Nowadays, there 137+ million sub-domains under **.com**. There were further complexities when people realized that they could sub-assign sub-domains and hence was born domain registrars such as **.hk.com**.



In the late '90s, ICANN (Internet Corporation for Assigned Names and Numbers) was created to manage these top-level domains, and within a few years, many more new top-level domains started to appear: **.aero**, **.biz**, **.coop**, **.info**, **.museum**, **.name**, **.pro**, and others. ICANN also started to accept sponsored top-level domains (**.asia**, **.cat**, **.jobs**, **.mobi**, **.tel**, **.travel** were the first). Controversially, in 2011 the **.xxx** top-level domain was approved (and quickly categorized as Adult/Sexually Explicit by Network Box). The introduction and adoption of the Punycode standard paved the way for non-roman characters in domain names.

Under the stewardship of ICANN, the number of top-level domains has exploded in the past ten to twenty years. Today, the root name servers serve 1,509 top-level domains - each with their own sub-assigned registrars, registration mechanisms, name servers, whois servers, and support infrastructure. And that is just for the top-level domains, below them are tens of thousands more secondary level domains.



■ ICANN headquarters, Los Angeles, California.

So what is the problem?

Where is the security threat in all this? To some extent, this made things easier for security companies. Domains under **.biz** were most likely business sites, **.xxx** adult/sexually explicit, and categorization was similarly trivial for **.arts**, **.shop**, **.museum**, etc. (so long as the domain registrars did their job correctly). But a more sinister problem started to appear. With the proliferation of available top-level domain names, and the hundreds of top-level registrars, costs came down, and the level of abuse went up. Some registrars were less diligent in their approach to security than others, and the spammers, phishers, and hackers took advantage.

Throwaway domains started to be created, be used in spam campaigns for a matter of hours, and then disappear to only 'live' a few days. Credit card fraud was often used to purchase these throwaway domains. Brand name protection became impossible for all but the largest of companies with teams of lawyers on staff. Phishing also became a problem, as a company's brand name would appear under a top-level domain of some faraway country's ISO 3166-1 code that doesn't look like a country to typical users. Domains like **.to** (Tonga), **.ly** (Libya), **.jo** (Jordan), **.io** (British Indian Ocean Territory), etc., are often used for other than their intended purpose.

Is there a solution?

Probably not. Pandora's box has been opened, and it would be hard to put this back in. It seems that as quickly as abused registrars tighten down to bring things under control, new vulnerable top-level domains and their registrars pop up. ICANN could try to impose strict regulations on how registrars conduct business. With hundreds of countries, all with their own legal and privacy protection systems in place, that is unlikely to happen. Step #1 would be for ICANN to stop issuing new top-level domains for a while to allow those that are already live to improve their systems.



Network Box HIGHLIGHTS



Global Cloud Intrusion Detection and Prevention Market Research Report 2015-2027



Network Box is listed as a top player in the **Global Cloud Intrusion Detection and Prevention Market**

Research Report. The report provides today's industry data, as well as future developments. In-depth analysis of key drivers, leading market players, key segments, and geographical regions. Other notable players in the list included: *AT&T, McAfee, Dell, IBM, Juniper Networks, Symantec, Cisco, and Check Point.*

LINK: <https://bit.ly/2ECIBeR>



■ Network Box USA, Houston, Texas.

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



TIME

Twitter Massive Breach Undermines Trust in the Platform, Experts Say

LINK: <https://bit.ly/3hYkYM4>



South China Morning Post

SCMP

Hongkongers, spooked by Beijing's new national security law, are scrubbing their digital footprints

LINK: <https://bit.ly/33idbEQ>



The Standard

Police interception fears boost Signal messaging

LINK: <https://bit.ly/2PgdrRh>



Asia Times

VIRUSES:
Biological versus computer

LINK: <https://bit.ly/3k5SNwM>



it-daily.net

[Network Box offers free phishing awareness workshop for customers]

LINK: <https://bit.ly/2PfxRoO>