

OVERVIEW OF DDOS, RANSOMWARE, MALWARE...& ALL THINGS GENERALLY UNPLEASANT

(HOPE YOU ENJOY IT!)



BCNET Conference – April 25th, 2017

shawn.beaton@cira.ca

AGENDA

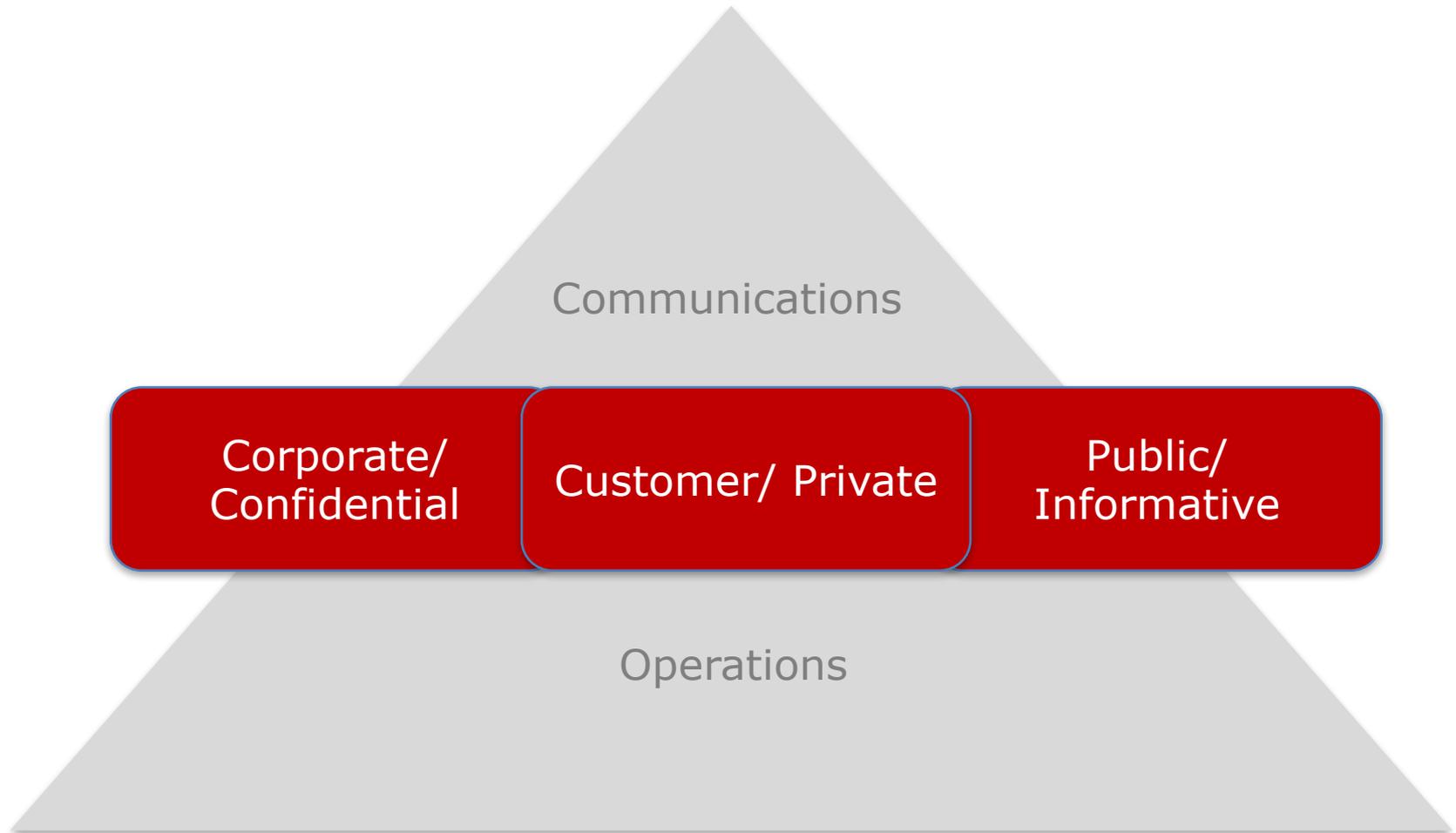
Lets start with the positive...

- Improvement of the Internet in Canada
- Just how do Internet Exchange Points help us all
- A series of unfortunate stats
 - DDoS
 - Malware
 - Data theft
- How CIRA is using the Internet to help you with D-Zone
 - Anycast DNS
 - DNS Firewall

ABOUT CIRA

- Self funded not for profit that manages the .CA domain as the country code domain registry
- Fund other non-profits through the CIRA Community Investment Program
 - over \$1 million annually in programs that range from setting up wireless towers in underserved areas to helping IV Drug users with an SMS system to alert them to problems
- Help build, deploy and manage technology that is good for the Canadian Internet, such as:
 - Internet governance (nationally and globally)
 - IPv6 and DNSSEC
 - Internet Exchange Points
 - Secondary DNS
 - Recursive DNS
 - Internet Performance and Quality testing
 - Research into Canadians use of the Internet

A SIMPLE MODEL FOR ORGANIZATIONAL DATA



ORGANIZATIONAL DATA

Corporate/
Confidential

Customer/
Private

Public/
Informative

Internet Governance

✓

Registry

✓

DNSSEC

✓

✓

✓

IPv6

✓

✓

✓

IXPs

✓

✓

Secondary DNS

✓

✓

DNS Firewall

✓

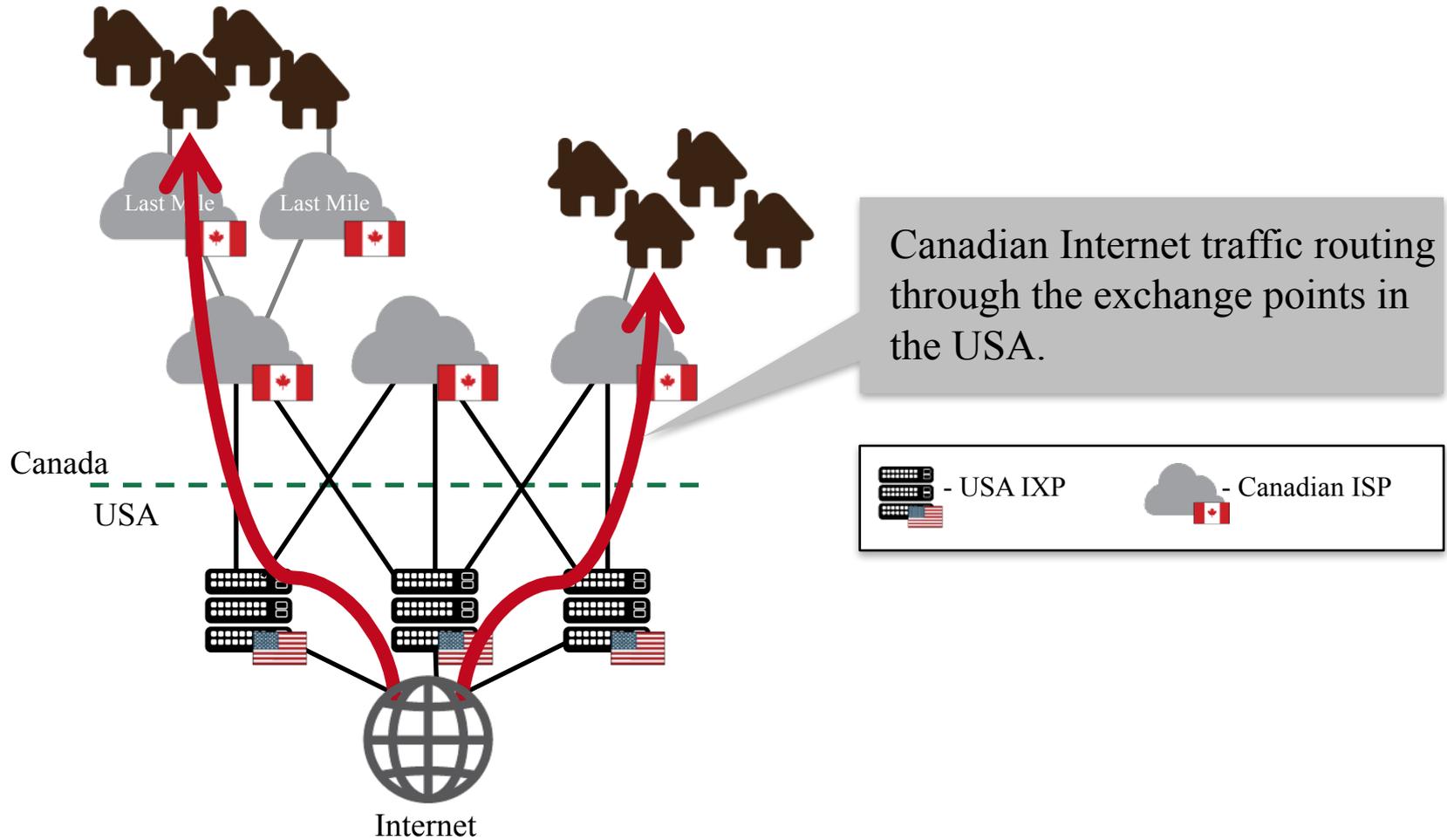
✓



INTERNET EXCHANGE POINTS

Sharing a vision for the Canadian Internet

IXPS AND TRAFFIC ROUTING



UNTIL RECENTLY CANADA HAD ONLY TWO INTERNET EXCHANGE POINTS

We were behind other countries in the world like:

- Cambodia (3)
- Philippines (5)
- Poland (12)
- Singapore (3)

We were on par with countries like:

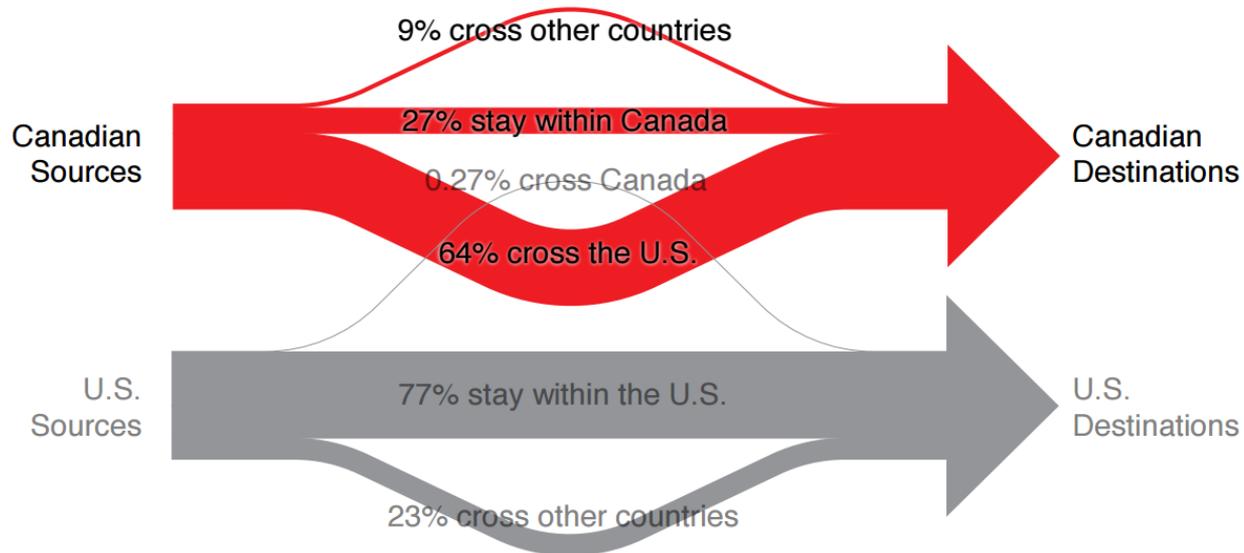
- Tanzania, Latvia, Tunisia, Peru

CIRA helped to fund the start-up of new IXPs across Canada

- The goal of the program is to keep Canada's traffic in the country, reduce latency, and increase end-user experiences

HOW LARGE IS THE DATA FLOW ISSUE?

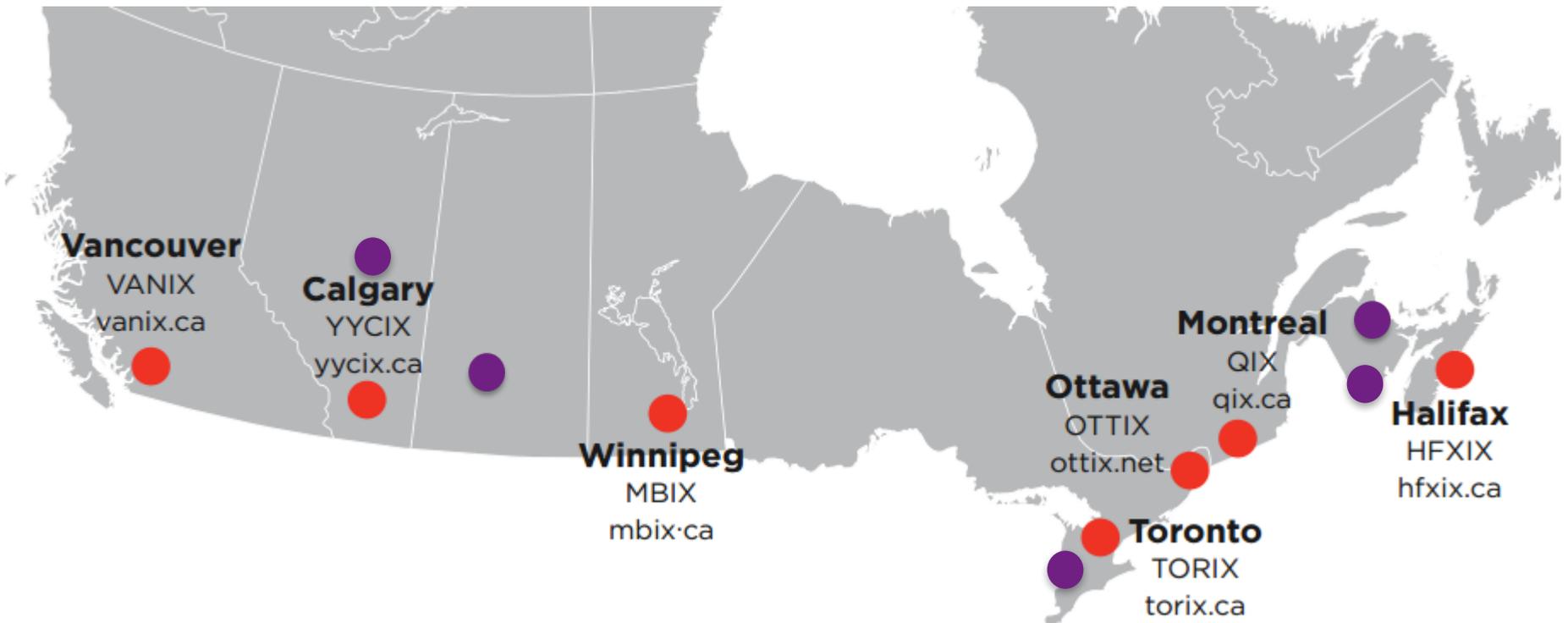
The majority of data flowing from an end user location to a server and back goes through another country



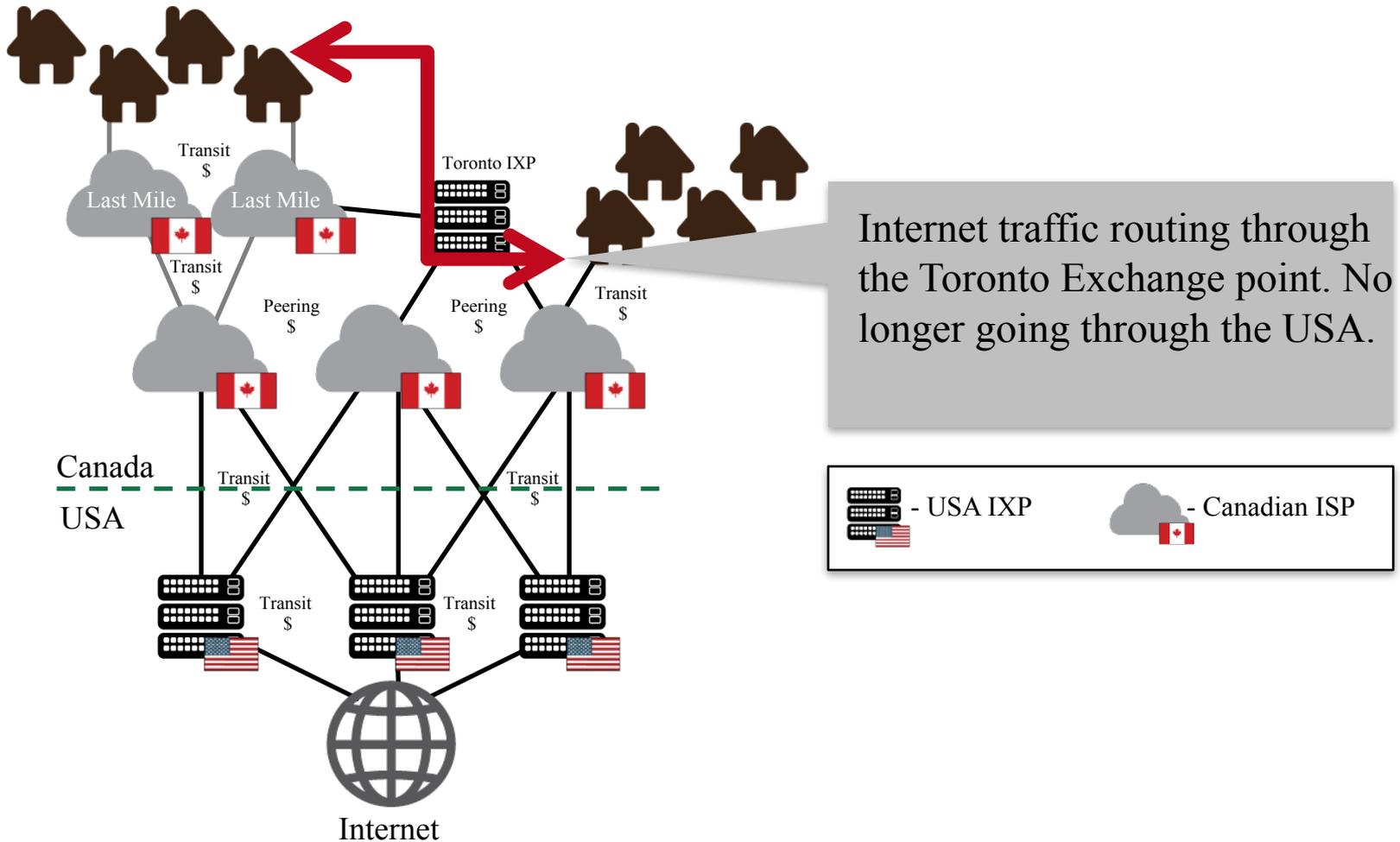
PCH & CIRA research on Internet traffic flow – preliminary data

CA-IX : CANADIAN IXP ASSOCIATION

- 7 established and operational IXPs
- Engaged Canadian IXP community 😊



IXPS AND TRAFFIC ROUTING IMPROVED

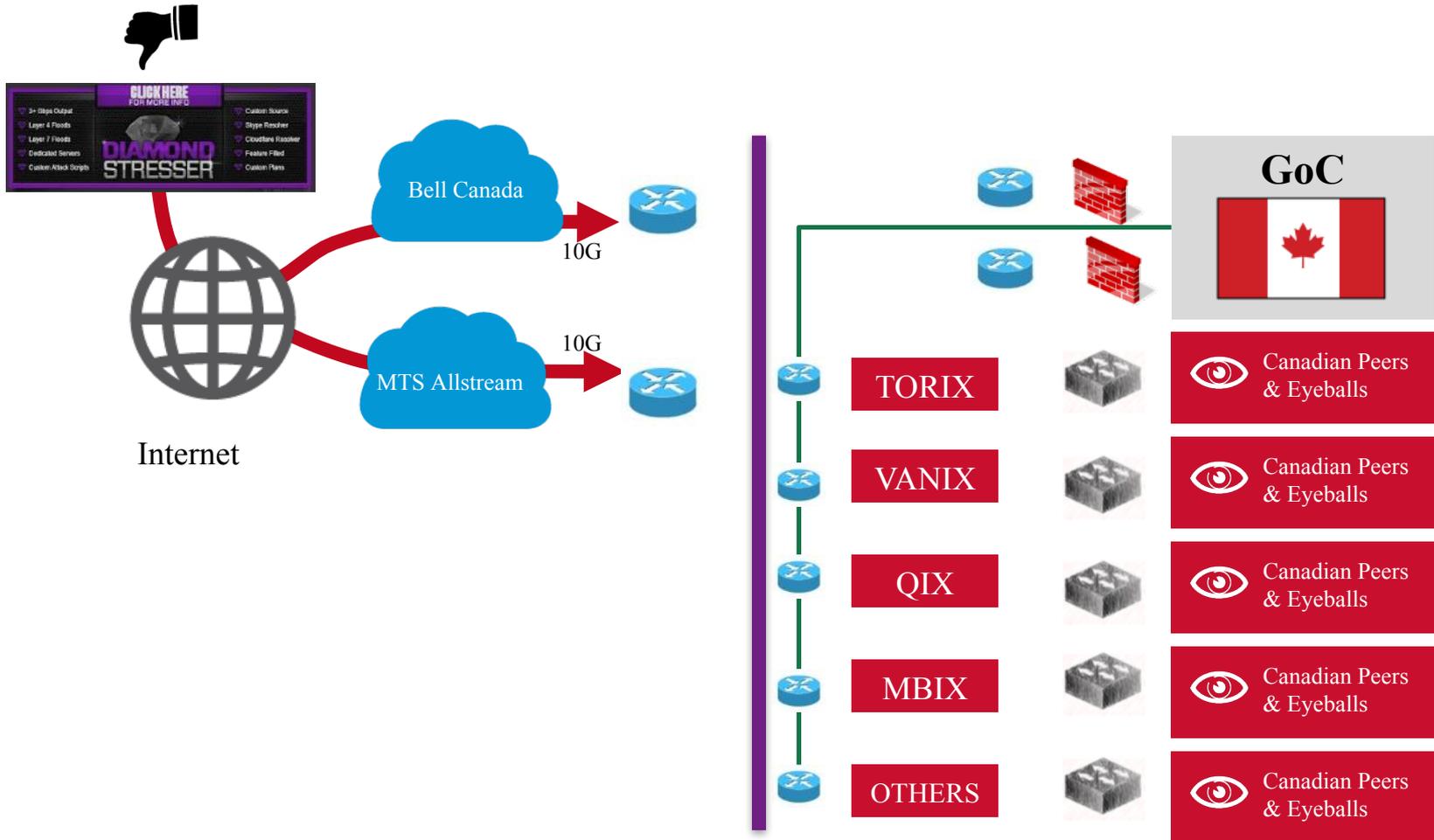




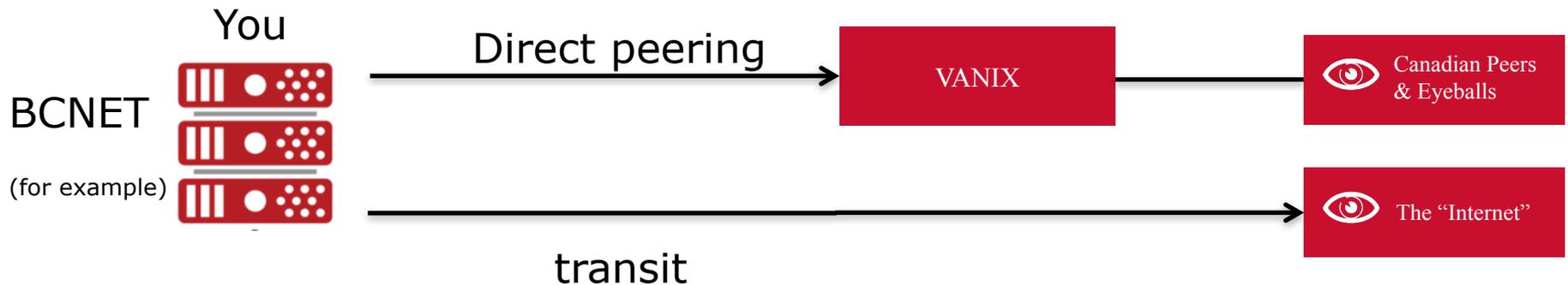
CASE STUDY

In the summer of 2015 the Government of Canada was hit with a massive DDoS attack that brought down its web presence globally

HOW MIGHT HAVE THIS BEEN MITIGATED



WHY DO YOU CARE: EXAMPLE VANCOUVER INTERNET EXCHANGE



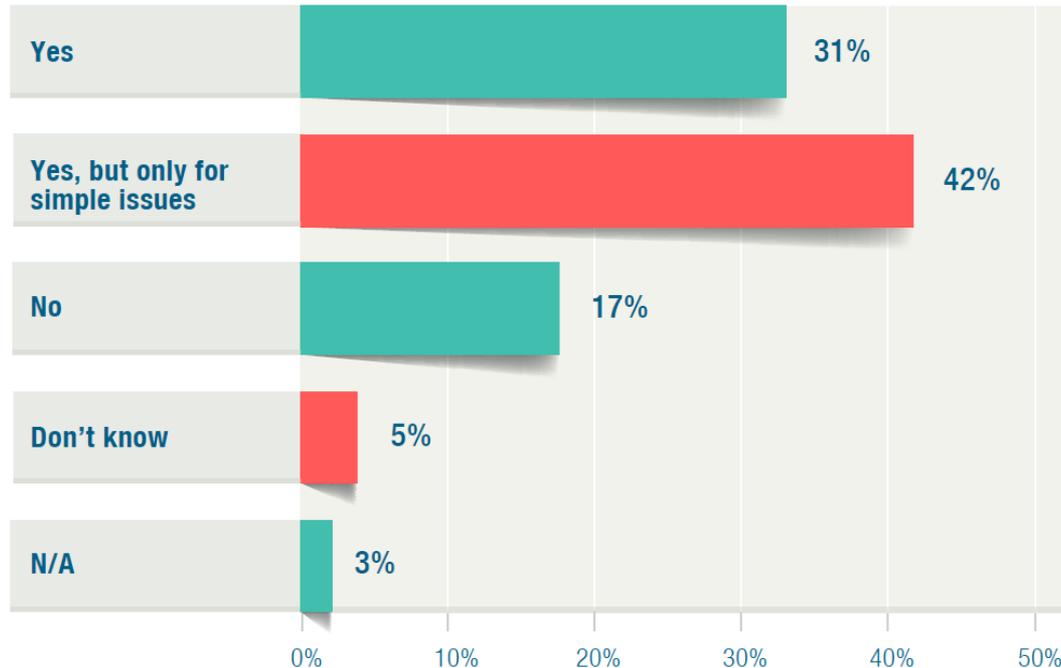
- ✓ You now have two routes to area networks and all of their peers
- ✓ One dedicated to local traffic and one dedicated to global



A SERIES OF UNFORTUNATE STATS

ARE YOU COMFORTABLE?

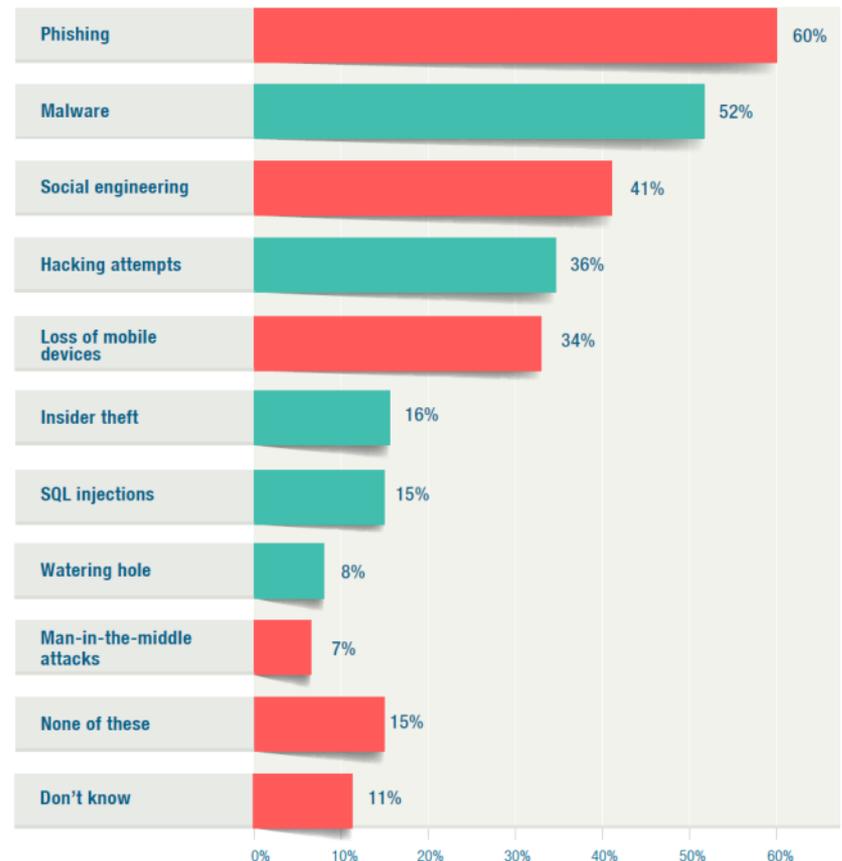
Percentage of survey respondents that felt comfortable with their teams ability to handle cybersecurity issues



THERE IS A REASON FOR DISTRESS

There are many vectors and many successful attacks

- Criminals, nuisance hackers, hacktivists, nation-states, insiders are all players where once only hackers lived
- Volume and impact is on the rise in almost every category
- 30% of organizations report attacks at least quarterly



Organizations reporting successful attacks in the prior year, ISACA (Information Systems Audit and Control Association)

DDOS





Widespread cyberattack takes down sites worldwide

by Sara Ashley O'Brien @saraashleyo

October 21, 2016: 8:11 PM ET

Recommend

13K



Social Surge - What's Trending



Mercedes-Benz unveils first pickup truck



Fixing this would boost U.S. economy by \$1.2 trillion



This is the easiest place in the world to do business



DEVELOPING STORY

U.S. GOVT. INVESTIGATING MASSIVE CYBERATTACK

LIVE

CNN

DOW ▼ -16.64

00:04 / 03:22

Massive cyber attack takes down major websites

ATTACK ON DYN DNS

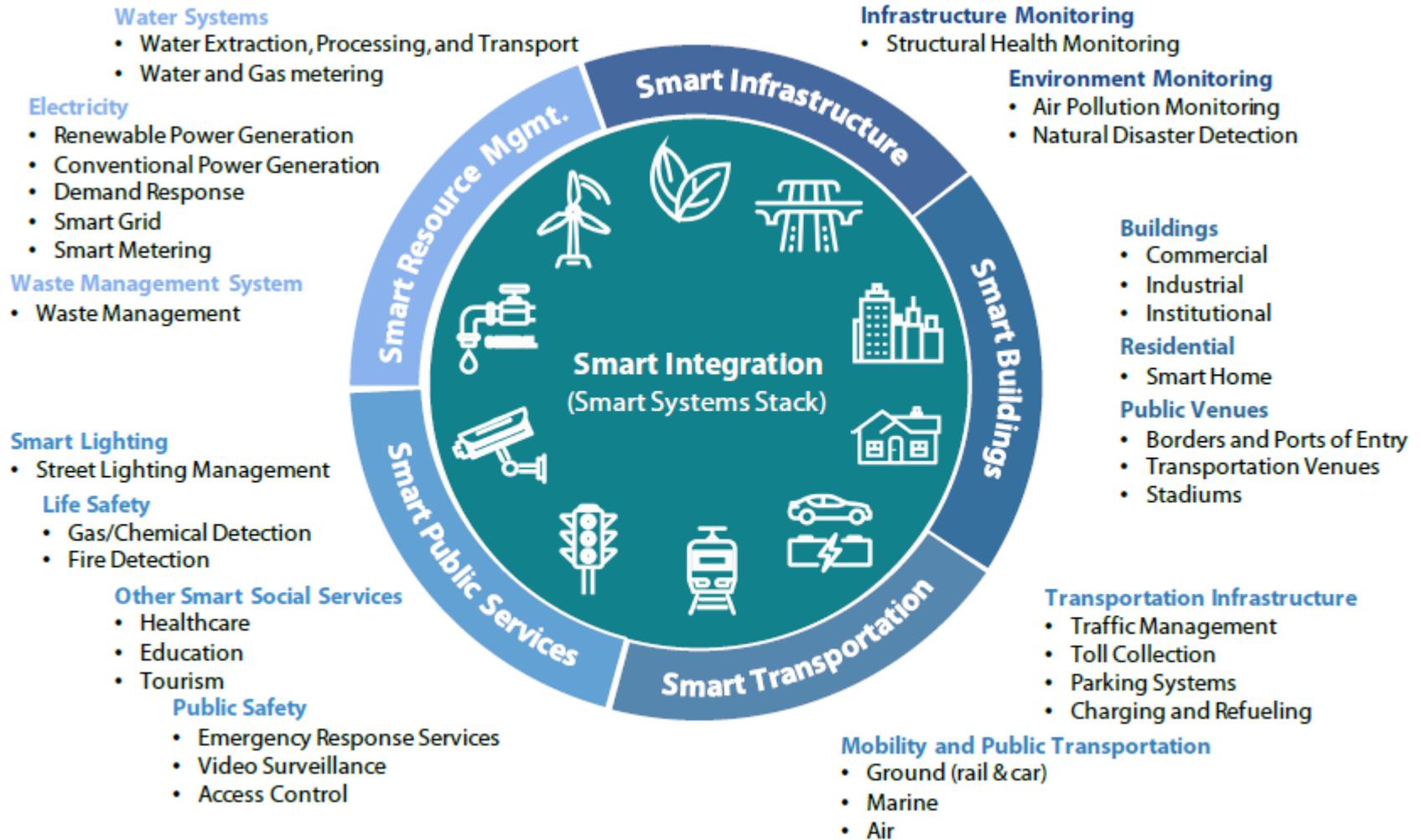
Mirai turned the “Internet of things” into the “botnet of things”

- Mirai source code was published in 2016
- Generated a massive 1.2 TBPS attack on DYN that was the new record
 - Took advantage of tens of millions of unique IP addresses
 - Webcams by Hangzhou Xiongmai were cited as the primary target*
 - Previously hit Krebs security with a record 665 GBPS, then hit OVH with new record 1 TBPS

“IoT devices are cheap and don’t necessarily have the necessary memory or processing to secure properly.”

- Chris Sullivan,
Core Security

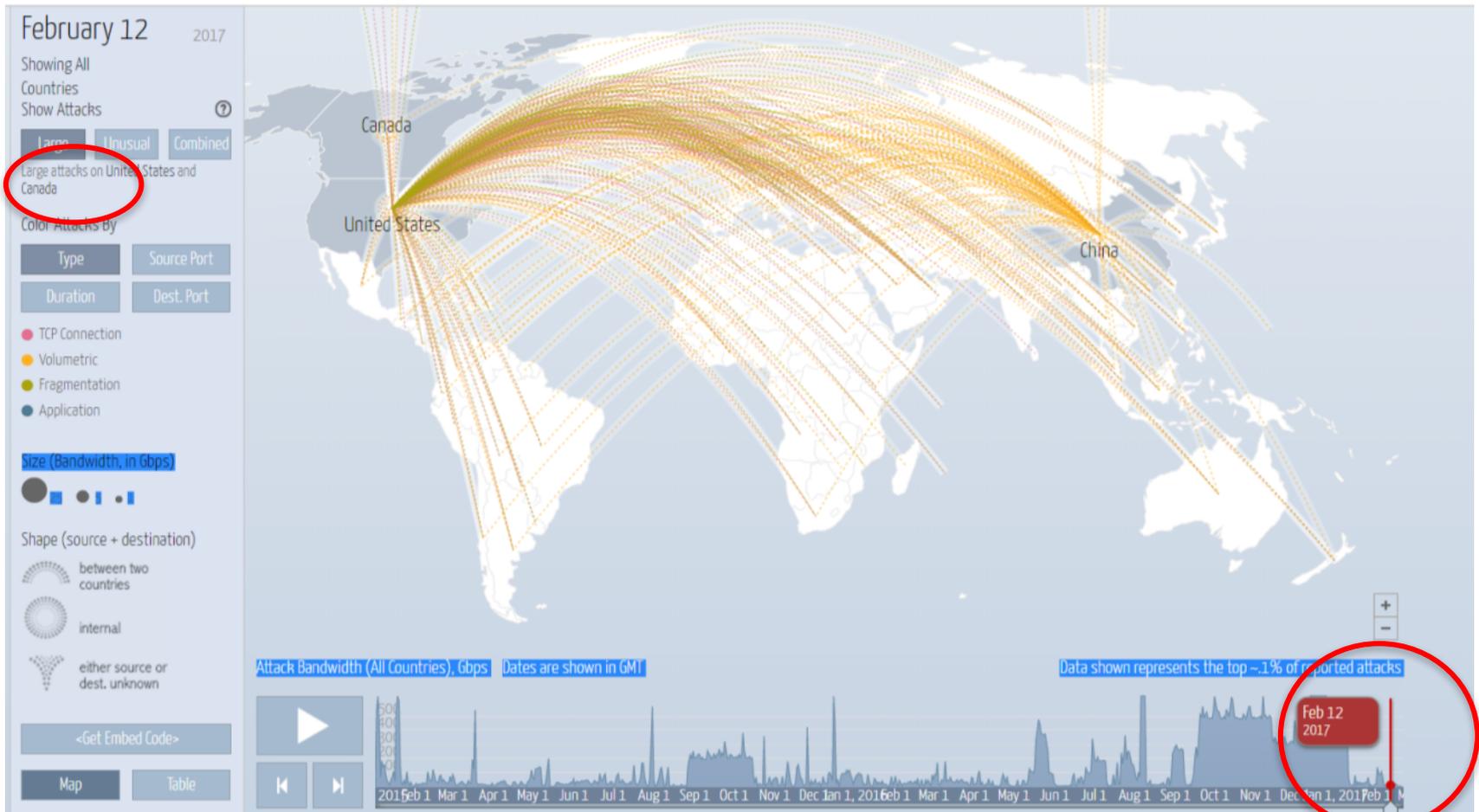
SMART CITY MARKET STRUCTURE



CANADIAN ORGANIZATIONS ARE ROUTINELY IN THE TOP 3 TARGETED GLOBALLY

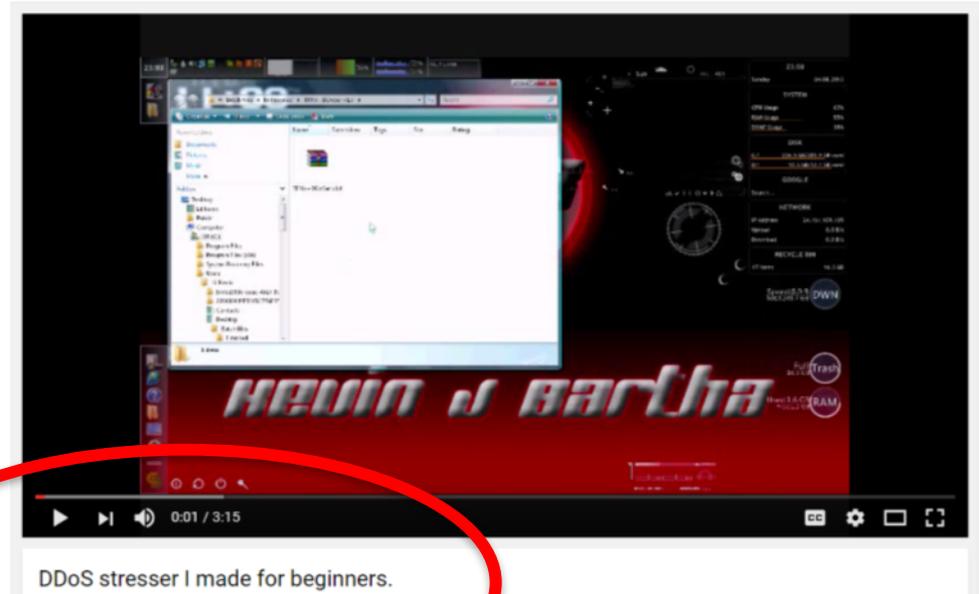
Digital Attack Map Top daily DDoS attacks worldwide

[Map](#) · [Gallery](#) · [Understanding DDoS](#) · [FAQ](#) · [About](#) · [G+](#) [Twitter](#) [Facebook](#)



BECAUSE IT IS EASY

- There are professional quality tools...
- ...and tools for noobs



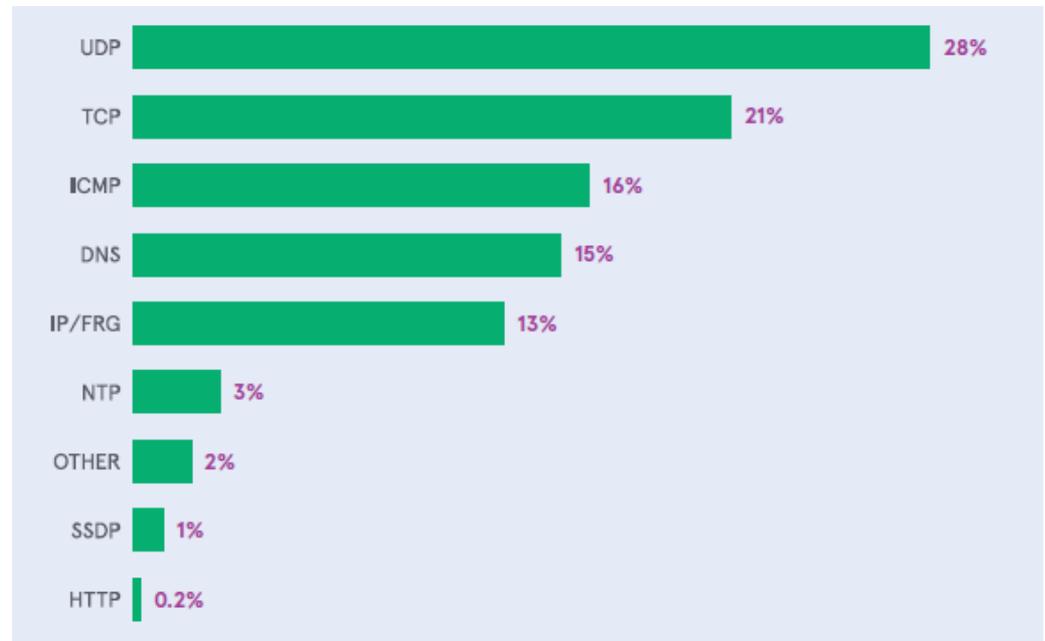
THE DOMAIN NAME SYSTEM

93% of organizations report DDoS attacks in 2016 up from 86% in 2013*

- Arbor networks world-wide infrastructure security reports that DNS is the most common service targeted by application layer attacks
 - Multi-vector attacks reported up to 56%
 - Cloud service attacks reported up to 33%
 - 27% report DDoS as a distraction while hackers attempt malware infiltration or data extraction

ACCORDING TO ONE VENDOR ATTACKS ARE UP 40% VS 2016

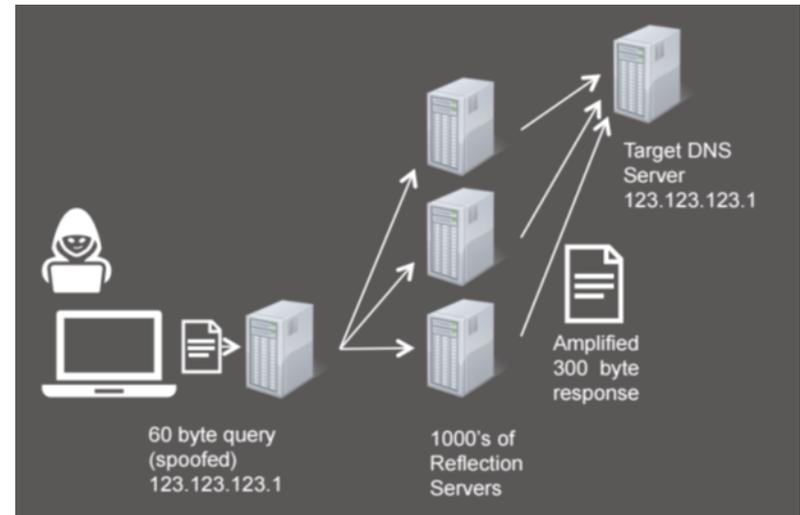
- Multi-vector attacks up 322%
- DNS-based attacks among the fastest rising



Neustar Q3 DDoS Security Insights Report showing attack vectors seen to Nov 2016

THE DNS IS A POPULAR TOOL

- The DNS is a popular choice because a small query can be amplified approx. 30x
- With the growth of the DNSSEC standard this potential is increased with a response that can be 300% the size of the query
- Organizations need to be responsible for their DNS not being part of the problem



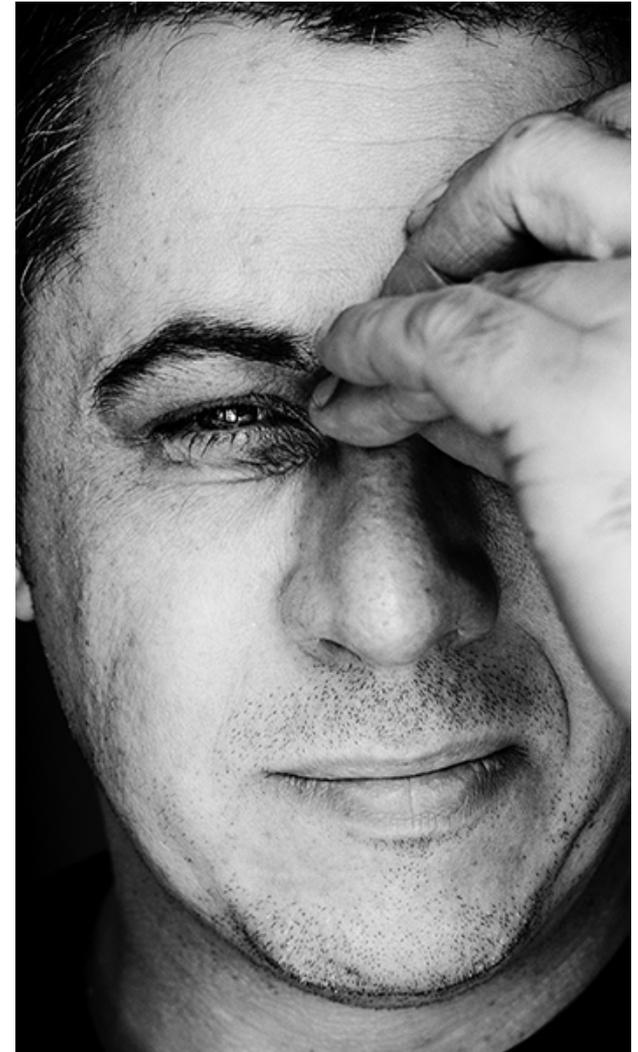
Malware



MALWARE

A rose by any other name still has thorns

- Remember when we just had “virus” protection
- Now the simple virus has branched into families under the umbrella of “Malware”:
 - Virus
 - Worm
 - Trojans
 - Bots
 - Spyware
 - Ransomware
 - Adware





LETS START WITH THE VECTORS

Exposure - Have always been around

- Clickbait
- USB drops
- Open networks

Where - Growing risks

- Rise in remote/home office workers and their poorly secured home networks
- Rise in BYOD
- Rise in available properties

HOME OFFICE WORKERS, BYOD AND SO-CALLED "SHADOW IT"

- Telecommuting is offered by 59 percent of companies*
- Full time telecommuting by 20 percent
- 72% of organizations offer at least some BYOD**
- Home users install all kinds of things on their home networks, part of the shadow IT dilemma

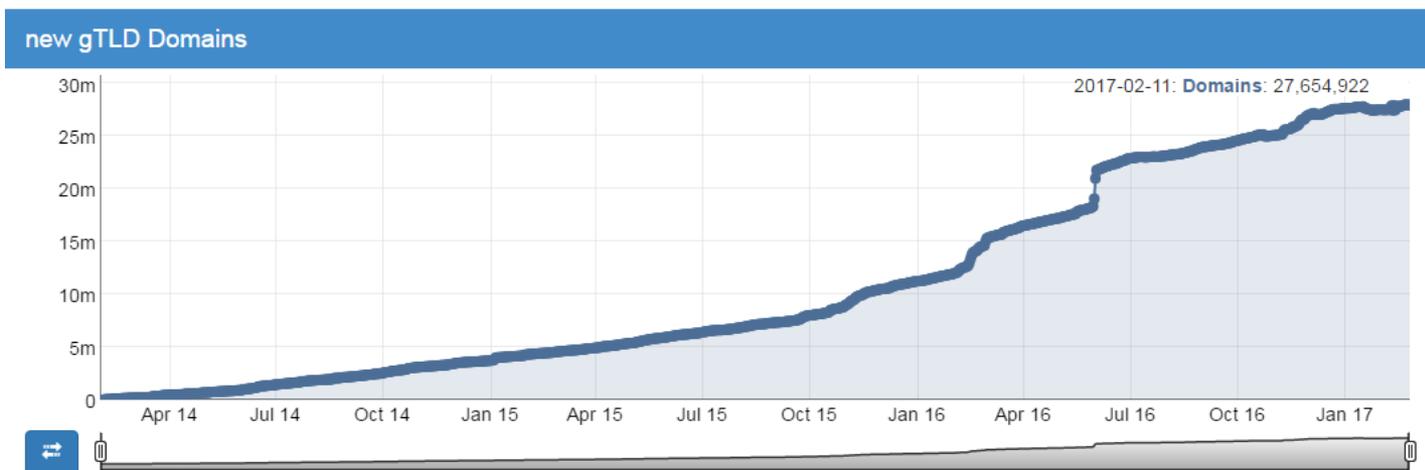


*2014 the Society for Human Survey Resource Management
** Teneble 2016 Mobile and BYOD security report

NEW PLACES TO HIDE – TLDS

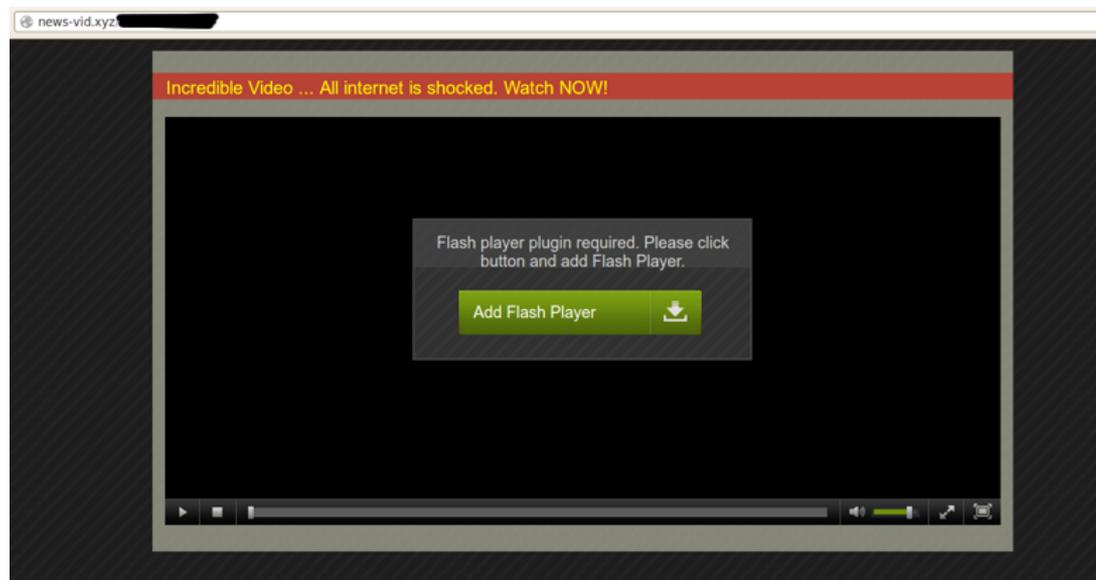
Free domains have always been a problem for security

- The new gTLD marketplace started in 2014 and now brings .sucks, .club, .guru, .xyz, and over 1,000 new top-level domains to the world as market penetration is close to 30 million globally
- In the race to build market-share many have offered low-cost or free promotions which attracts the baddies
- The old world of ccTLDs like .CA, .uk, .de, and others had presence requirements to deter problems. .com had scarcity. All had a \$.



.XYZ – ONE EXAMPLE

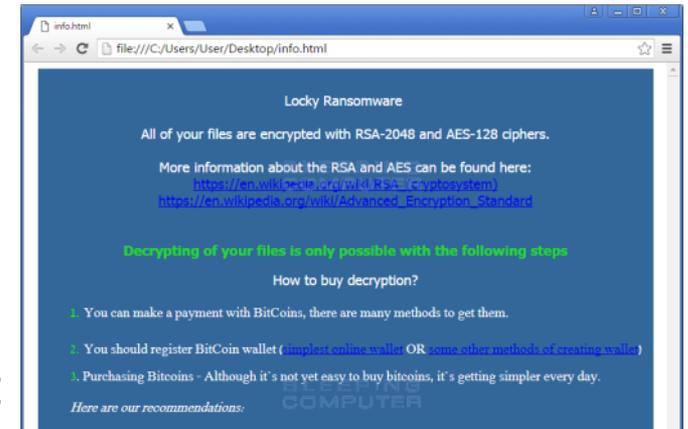
- .xyz is one of the more successful gTLDs from a total domains under management perspective
- BlueCoat networks determined that during their explosive growth phase, 97% of .xyz sites were being used for nefarious purposes



CRIME PAYS IN THE (PROBABLY) FASTEST GROWING IT SECTOR

Nuisance hackers and hacktivism seem like old friends when compared to the latest growth sector

It's estimated that **last year saw cybercrime victims pay out \$24 million to hackers** deploying ransomware. According to the Herjavec Group, the amount paid out by victims of ransomware in just the first three months of this year came to a total of \$209 million. The report suggests that at that rate, the **total cost of ransomware is set to reach \$1 billion for all of 2016.**



BOTNETS, MALWARE, RANSOMWARE

There are more attack vectors than ever with a clear path to profitability and/or hacktivism.

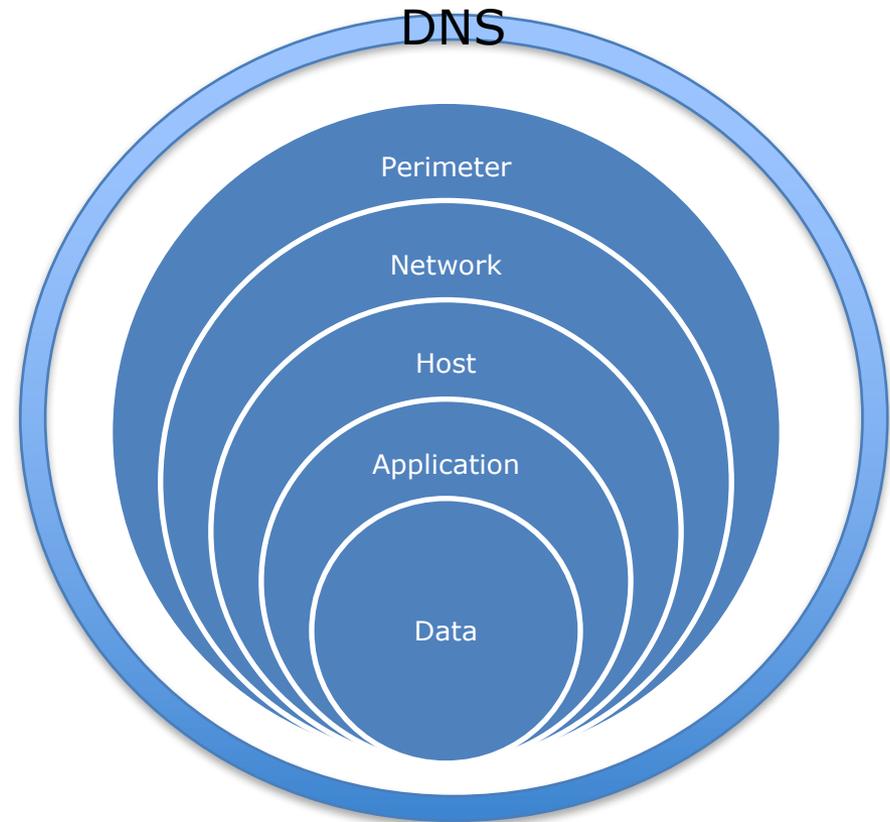
- ✓ Botnets are on the rise with Necurs reaching up to **59 million queries per-day** with Mirai a close second¹
- ✓ Ransomware like Locky, CryptXXX, Cerber, Ghost Push, and now Spora are providing plenty of “professional” tools for hackers
 - ✓ Locky alone is estimated to be generating an average of **\$1.6 million dollars** per day in bitcoin “revenue”¹



USING THE INTERNET'S INFRASTRUCTURE TO HELP – WITH CIRA

DNS IS THE FABRIC OF THE INTERNET

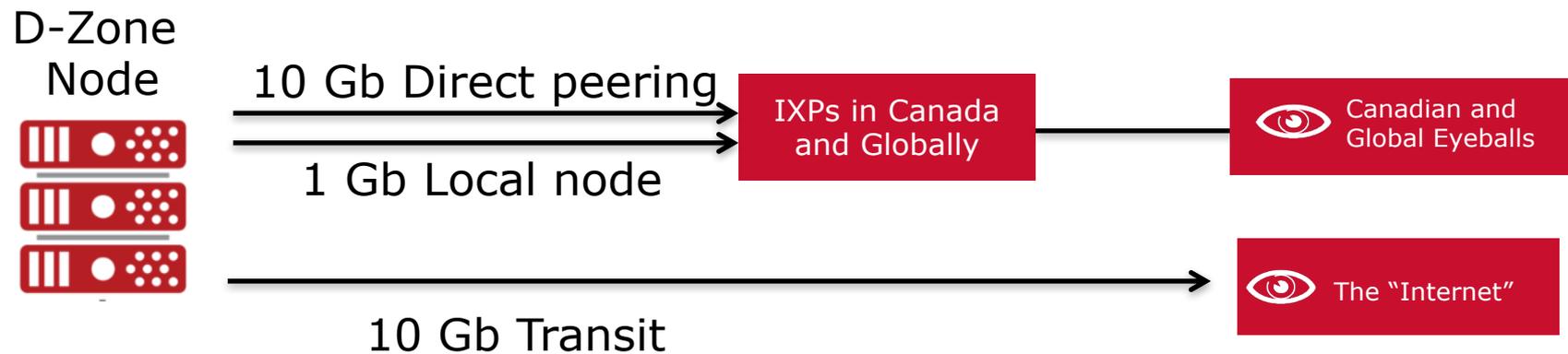
- DNS is part of a multi-layer “defence in depth” approach
 - 91.3% of malware uses DNS
 - DNS is used for command and control
 - Endpoint protection is limited
 - IoT
 - BYOD



SERVICE 1: D-ZONE ANYCAST DNS TO HELP KEEP YOU ONLINE



D-ZONE GLOBAL NODE CONFIGURATION



Look familiar?

D-Zone leverages the same footprint that we recommend for maximum resilience with your Internet "connection"



D-ZONE ANYCAST ARCHITECTURE HIGHLIGHTS

- 2 Anycast Clouds
 - 2 diverse transit providers
 - Hurricane Electric
 - Hibernia
 - 2,400 peering relationships globally
 - Diverse management transit
 - 2 load shared DNS servers at each site
 - Out of band reporting and data collection
- 

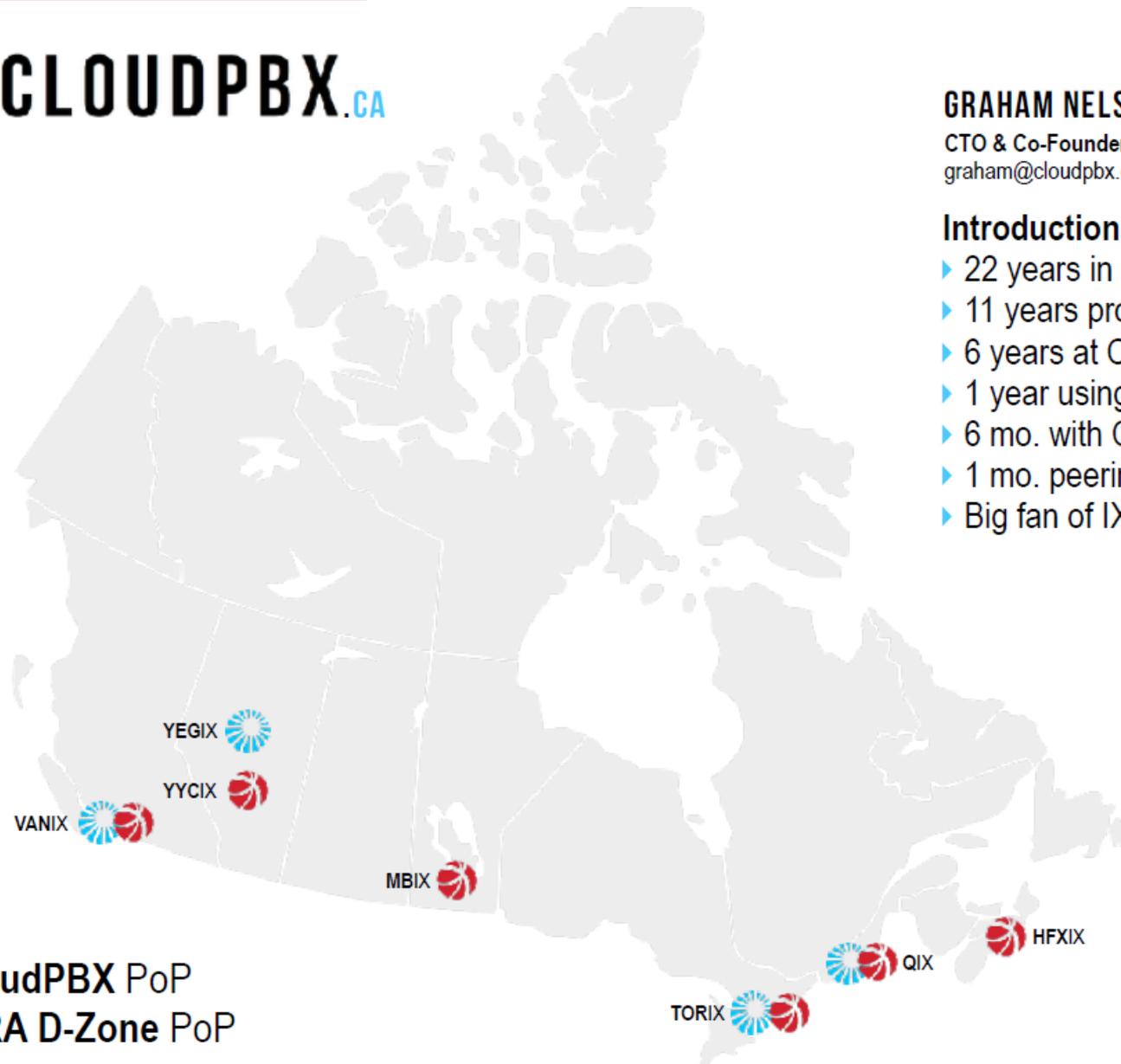
D-ZONE ANYCAST DNS SOAKS UP DDOS WHERE IT STARTS



We are continuing to work with partners around the world to add capacity



CLOUDPBX.CA



GRAHAM NELSON-ZUTTER

CTO & Co-Founder
graham@cloudpbx.ca

Introduction:

- ▶ 22 years in IT
- ▶ 11 years providing VoIP
- ▶ 6 years at CloudPBX
- ▶ 1 year using BGP
- ▶ 6 mo. with CIRA D-Zone
- ▶ 1 mo. peering on VANIX
- ▶ Big fan of IXPs!!!

 **CloudPBX PoP**

 **CIRA D-Zone PoP**

GRAHAM NELSON-ZUTTER

CTO & Co-Founder
graham@cloudpbx.ca

How do we build:

- ▶ scalable,
- ▶ multi-tenant,
- ▶ carrier-grade,
- ▶ high call quality,
- ▶ distributed load,
- ▶ geo-optimized,
- ▶ fault-tolerant,
- ▶ *enterprise VoIP*
- ▶ for **Canadians.**

EDM1

Upgraded:
▶ 2014
Location:
▶ 10250 101 St NW
Transit:
▶ Telus, Bell...
Local IX / Peering:
▶ YEGIX 2018

VAN1

Upgraded:
▶ 2016
Location:
▶ 1050 W. Pender
Transit:
▶ Telus, Bell...
Local IX / Peering:
▶ VANIX April '17
▶ AS395152

TOR1

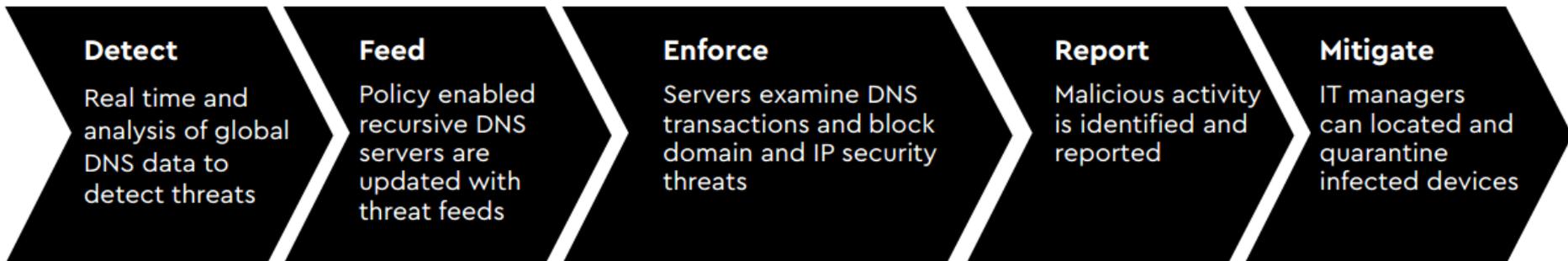
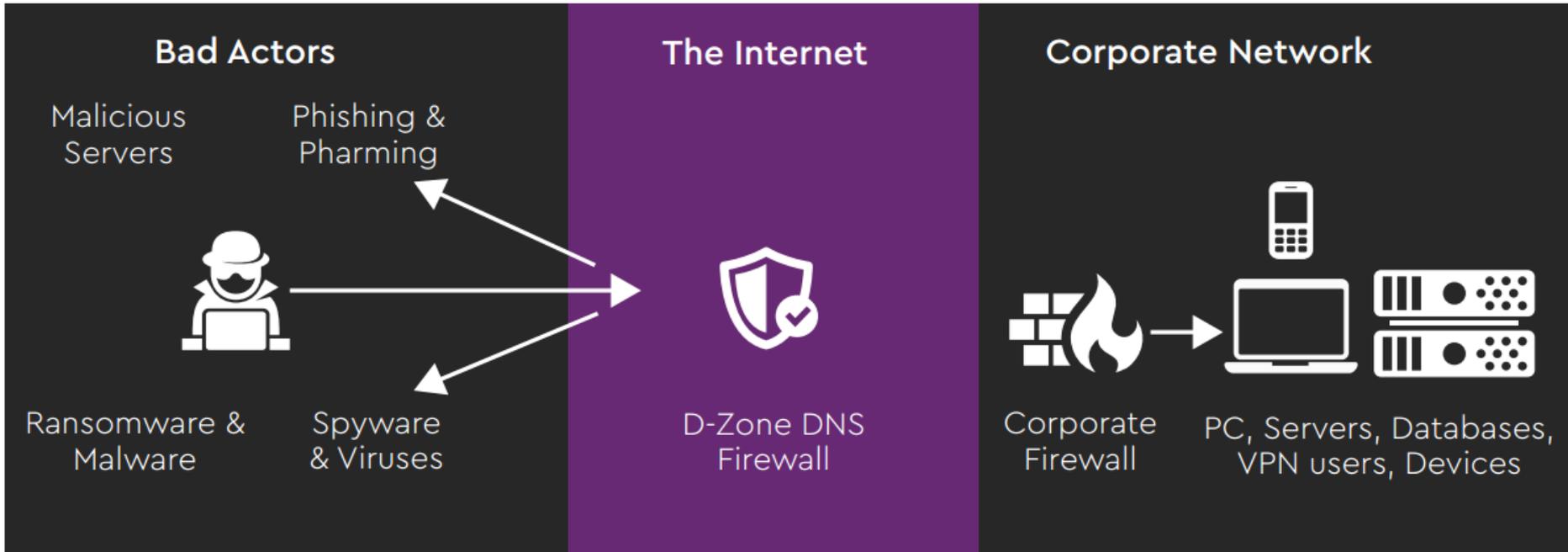
Upgraded:
▶ 2016
Location:
▶ 151 Front St. W.
Transit:
▶ Telus, Bell...
Local IX / Peering:
▶ TorIX May '17
▶ AS393755

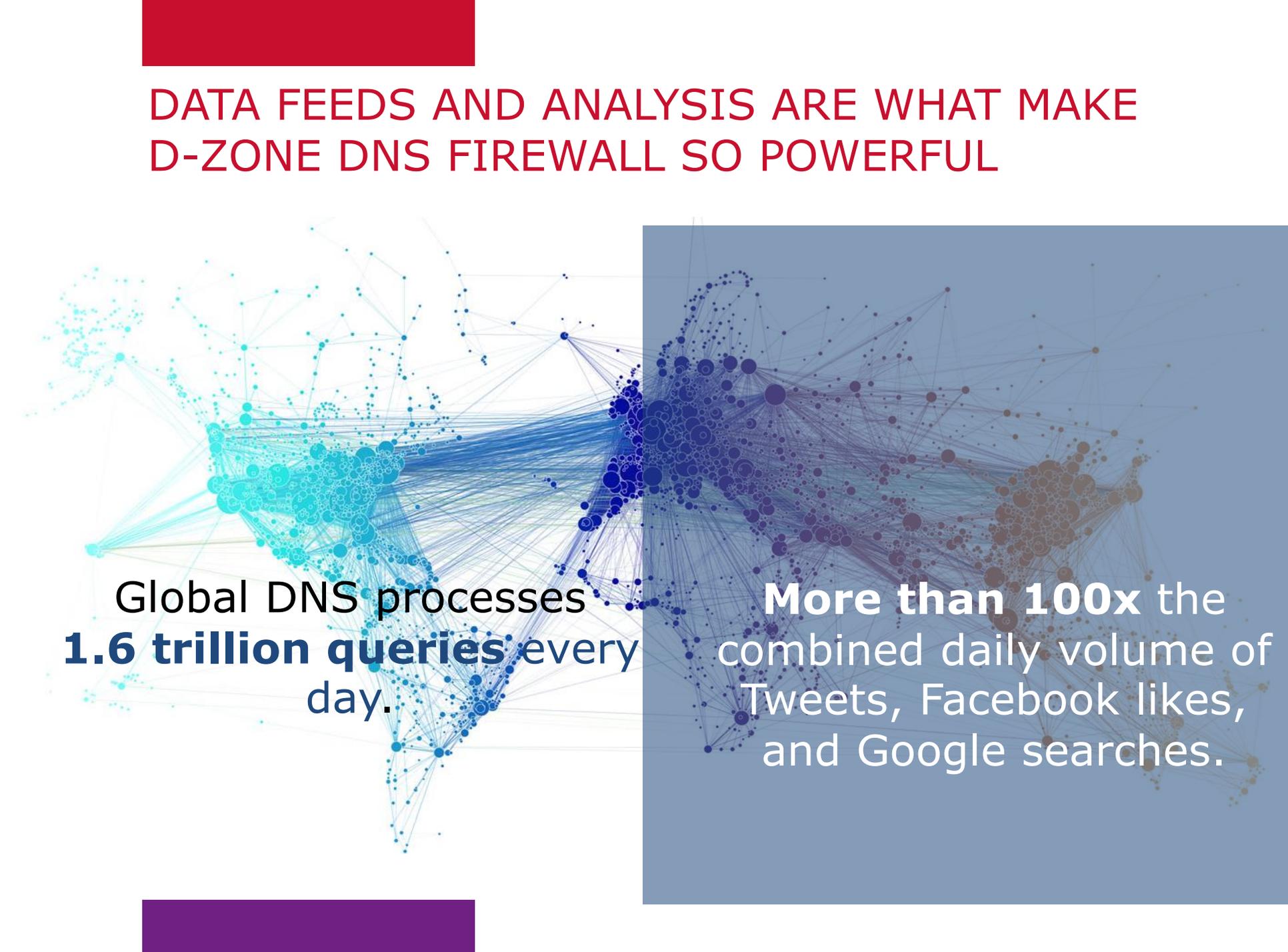
MTL1

Upgraded:
▶ 2017
Location:
▶ D2-3445 du Parc
Transit:
▶ Bell Peering...
Local IX / Peering:
▶ QIX July '17
▶ AS395152

Layer	Challenge	Standard	Solution	Notes
▶ Network	To remove single points of failure and to achieve low latency to subscribers and carriers.	BGP & IX	4 geo-redundant data-centres across Canada. Using BGP to peer on local IXs, multiple ASNs	Best latency is achieved on regional IXP's: VANIX, TorIX, QIX
▶ DNS	To enabled VoIP devices connecting to geo-redundant data-centres and to survive a DDoS.	NS SRV	SRV gives each client domain multiple SIP proxies. Canadian* NS authoritative SRV backup.	NS1.com with CIRA & D-Zone
Signalling	To bypass single SIP call signalling paths which can be disrupted by route failures.	Multiple Route SIP	2x Kamailio SIP proxies in each PoP each have dynamic routing to all FreeSWITCH media proxies	Geo and latency optimized.
Media	To bypass single RTP audio media stream paths which can be disrupted by route failures.	Multiple Route RTP	Our FreeSWITCH nodes ingest streams directly from our CLEC PSTN gateways with few hops.	Audit calls with MOS grading tool. Sponsor open-source tools to benefit others.
Data	To offer voicemail, IVR, DIDs, Extensions and callflows simultaneously in all PoPs.	JSON & NoSQL	Deploy self-healing many-master CouchDB nodes across 9 DB nodes in 3 PoPs	CouchDB is schema-less NoSQL based DB and follow revisions of each JSON doc.
Equipment	To purchase and provision enough muscle to handle 3x spikes in peak business hours usage.	x86 Linux	Deploy carrier-grade 3x Dell Cloud Servers 2U 4-Nodes, redundant power on A/B circuits.	Easily replaceable commodity parts with 3x extra capacity.
PSTN	To provide PSTN origination failover routing on media gateways between CLECs using SIP/RTP.	CLEC SS7 Failover	Originate calls from redundant Canadian CLECs using PSTN failover over SS7 circuits.	Ask CLECs if they have PSTN SS7 circuit layer failover routing.

SERVICE 2: D-ZONE DNS FIREWALL TO HELP PROTECT FROM MALWARE





DATA FEEDS AND ANALYSIS ARE WHAT MAKE
D-ZONE DNS FIREWALL SO POWERFUL

Global DNS processes
1.6 trillion queries every
day.

More than 100x the
combined daily volume of
Tweets, Facebook likes,
and Google searches.



D-ZONE DNS FIREWALL – BENEFITS

- Cloud based - easy to implement with no hardware or software install
- Subscriber protection from malware and phishing beyond your network
- Automatically updated block lists protect from new threats that appear globally within minutes
- Protects all devices
- Reduces support calls
- Cost effective

+ Bonus an enterprise-class recursive service that handles 2.4 million queries-per-second per server and has a cache hit-rate higher than non-cloud options



CONCLUSION

CIRA is using the Internet's fabric to deliver DNS services designed for Canadian organizations

- ✓ D-Zone Anycast DNS

An authoritative DNS designed to protect your websites and applications from DDoS

- ✓ D-Zone DNS Firewall

A recursive DNS designed to protect your users and network resources from malware



QUESTIONS ?

CONTACT ME:

Shawn Beaton, Business Development
Canadian Internet Registration Authority (CIRA)
Mobile: 613.799.5789
Shawn.beaton@cira.ca

