CIRA DNS UPDATES
RECURSIVE DNS FIREWALL

CANADA 150
THE NEXT
150
BELONGS TO
CANADA

cira

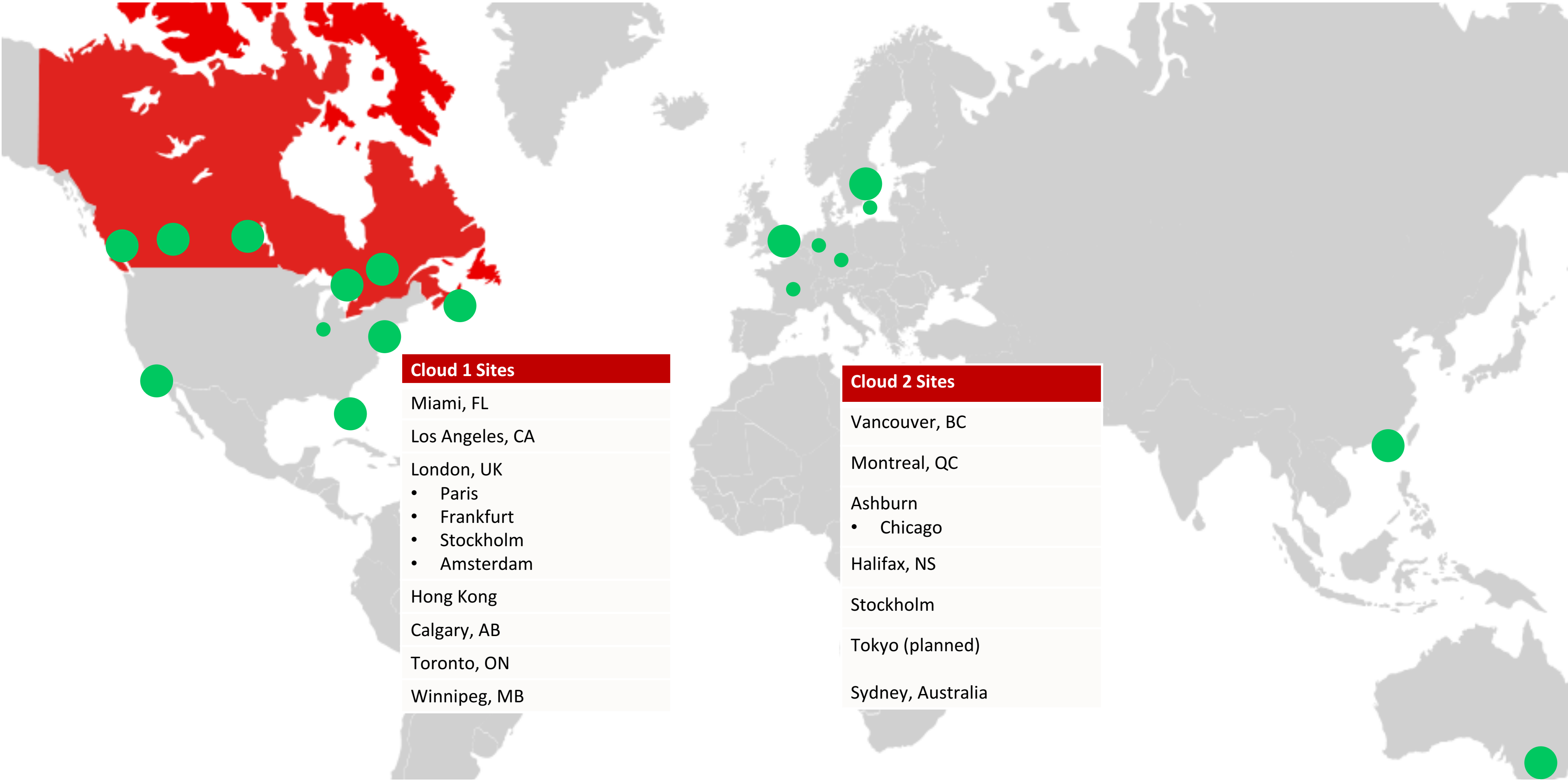
BUILDING A BETTER
ONLINE CANADA

Presented by: Mark Gaudet

AGENDA

- CIRA
- D-Zone Anycast DNS Update
- D-Zone Firewall
  - Overview
  - Architecture
  - Implementing

A GLOBAL ANYCAST DNS SERVICE



Cloud 1 Sites
Miami, FL
Los Angeles, CA
London, UK • Paris • Frankfurt • Stockholm • Amsterdam
Hong Kong
Calgary, AB
Toronto, ON
Winnipeg, MB

Cloud 2 Sites
Vancouver, BC
Montreal, QC
Ashburn • Chicago
Halifax, NS
Stockholm
Tokyo (planned)
Sydney, Australia

D-ZONE DNS UPDATE

- Infrastructure
  - Vancouver upgrade to 10G transit
  - Japan node, planned
  - South America node, planned
- Features
  - DNS diversity, Bind + NSD
  - Reporting enhancement (location, query type, response type, protocol, operation type, IP version)
  - Email alerts

D-ZONE DNS UPDATE - FEATURES

- Notify to API
  - Automatic addition of zones by sending notifies to special server
  - Checks if zones are configured in D-Zone and adds them
  - Additional filtering of adds
    - Name servers
    - TLD
- Auto expire zones
  - Expired zones go to “to be deleted” state
  - Deleted after 7 days

GROWTH INTO TLD MARKET

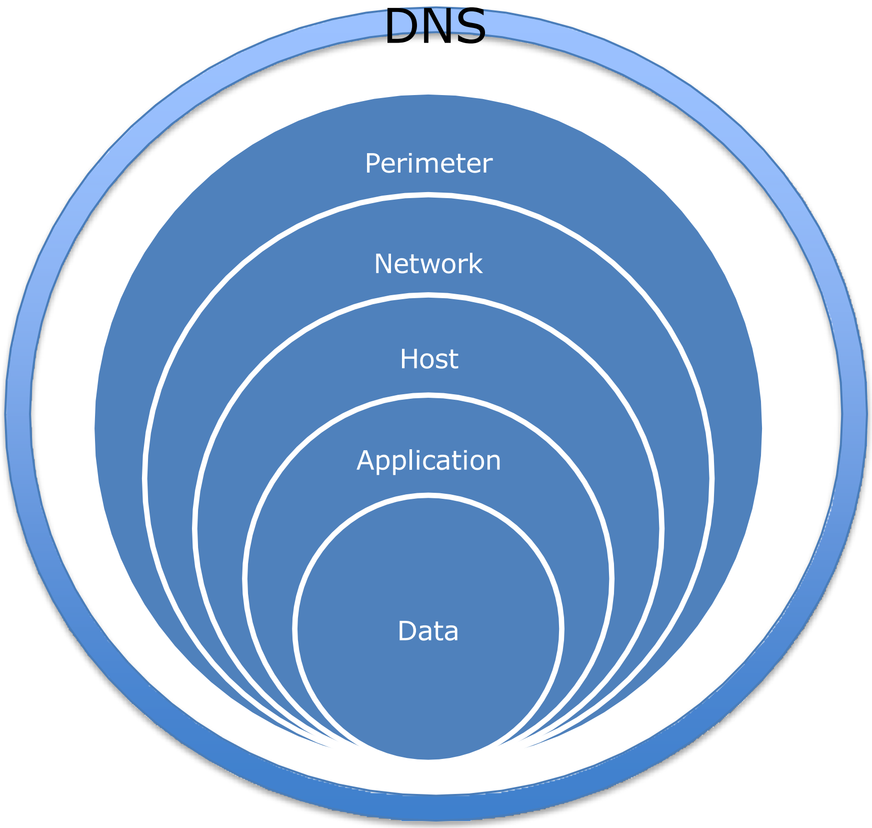
- Growth into TLD DNS
  - ccTLDs
    - .dk, .pt, .nl, .nz, .cr, .sx, .aw
  - gTLDs
    - .kiwi, amsterdam, politie
    - Uniregistry - .link, .click, .mom, .lol, .sexy, .photo, .help and more
- Innovation in TLD reporting

Malware, Ransomware, Phishing Protection

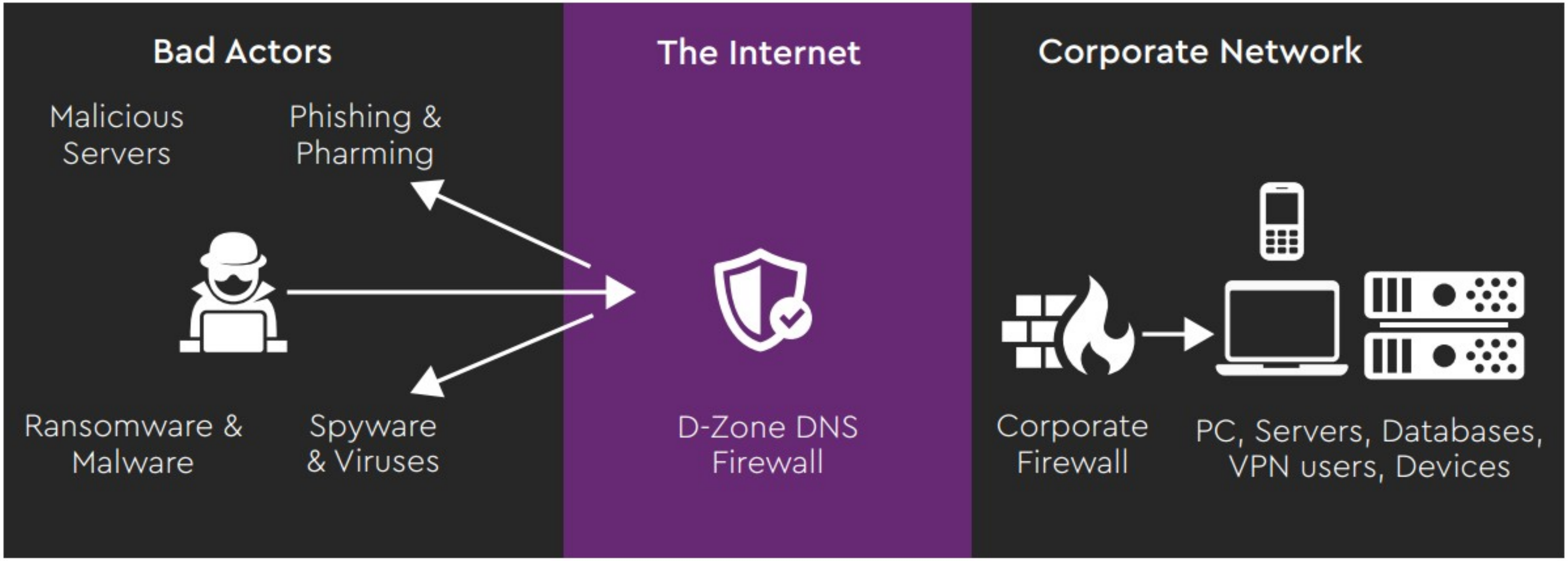
Keep malware off the network and block communication to command and control with the D-Zone DNS Firewall

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



D-ZONE DNS FIREWALL



Bad Actors

Malicious Servers

Phishing & Pharming

Ransomware & Malware

Spyware & Viruses

The Internet

D-Zone DNS Firewall

Corporate Network

Corporate Firewall

PC, Servers, Databases, VPN users, Devices

Detect

Real time and analysis of global DNS data to detect threats

Feed

Policy enabled recursive DNS servers are updated with threat feeds

Enforce

Servers examine DNS transactions and block domain and IP security threats

Report

Malicious activity is identified and reported

Mitigate

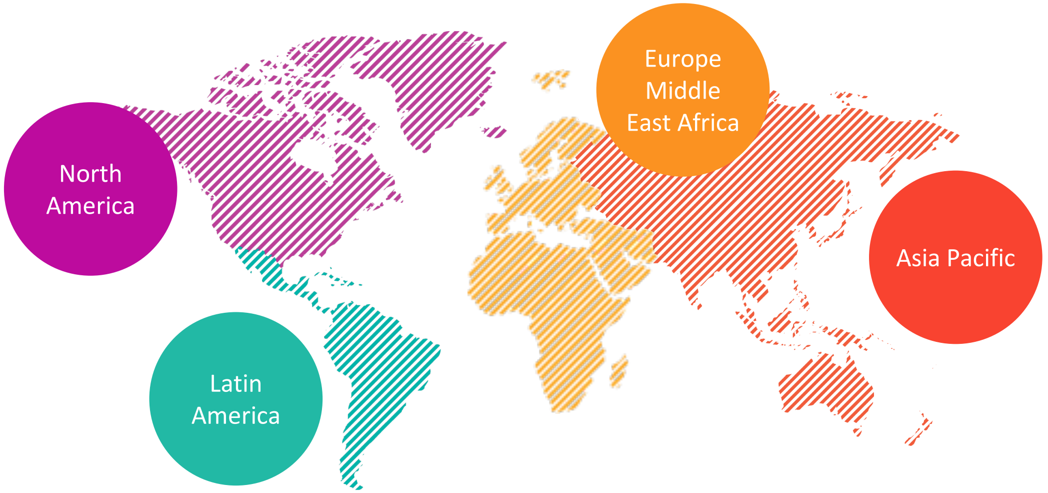
IT managers can located and quarantine infected devices

Leader in DNS - Nominum

100+ **providers**
40+ **countries**

Charter Spectrum
verizon
cox
eastlink
VIDÉOTRON
COMCAST
TELUS
CABLEVISION
Walmart

kpn
proximus
Telefónica
STC
الاتصالات السعودية
BT
orange
Virgin media
altice
swisscom
vodafone

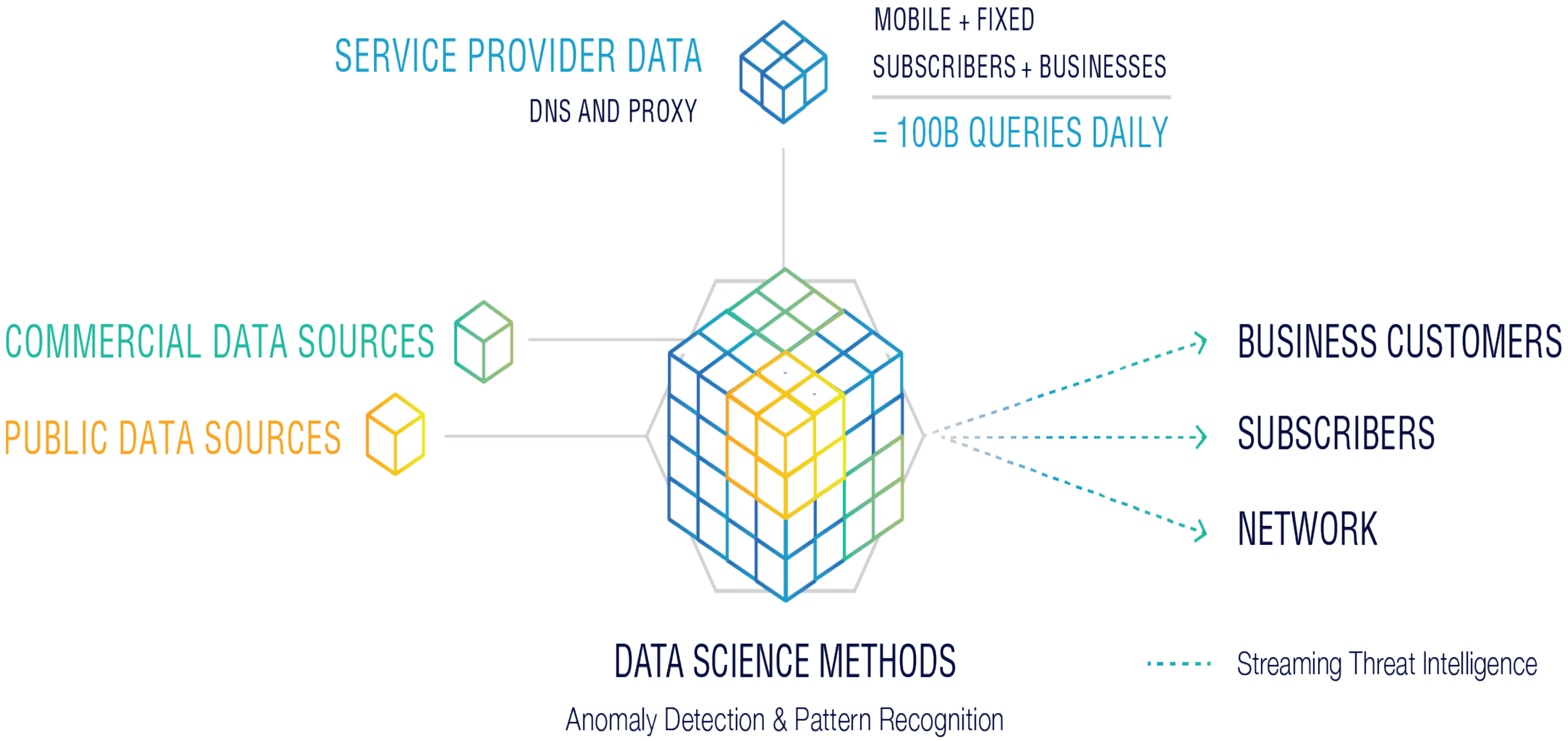


AIS
airtel
Rakuten
StarHub
!dea
NTT Communications
中華電信
TELSTRA
KDDI
SMART
Spark
Singtel

Televisa
Telefónica
CABLEVISION
oi
TELECOM
telcel
vivo
TIM
TELMEX
Cablevisión
Claro

sourced from Nominum

COMPETITIVE ADVANTAGE IS DATA SCIENCE



SERVICE PROVIDER DATA

DNS AND PROXY

MOBILE + FIXED
SUBSCRIBERS + BUSINESSES

= 100B QUERIES DAILY

COMMERCIAL DATA SOURCES

PUBLIC DATA SOURCES

DATA SCIENCE METHODS

Anomaly Detection & Pattern Recognition

BUSINESS CUSTOMERS

SUBSCRIBERS

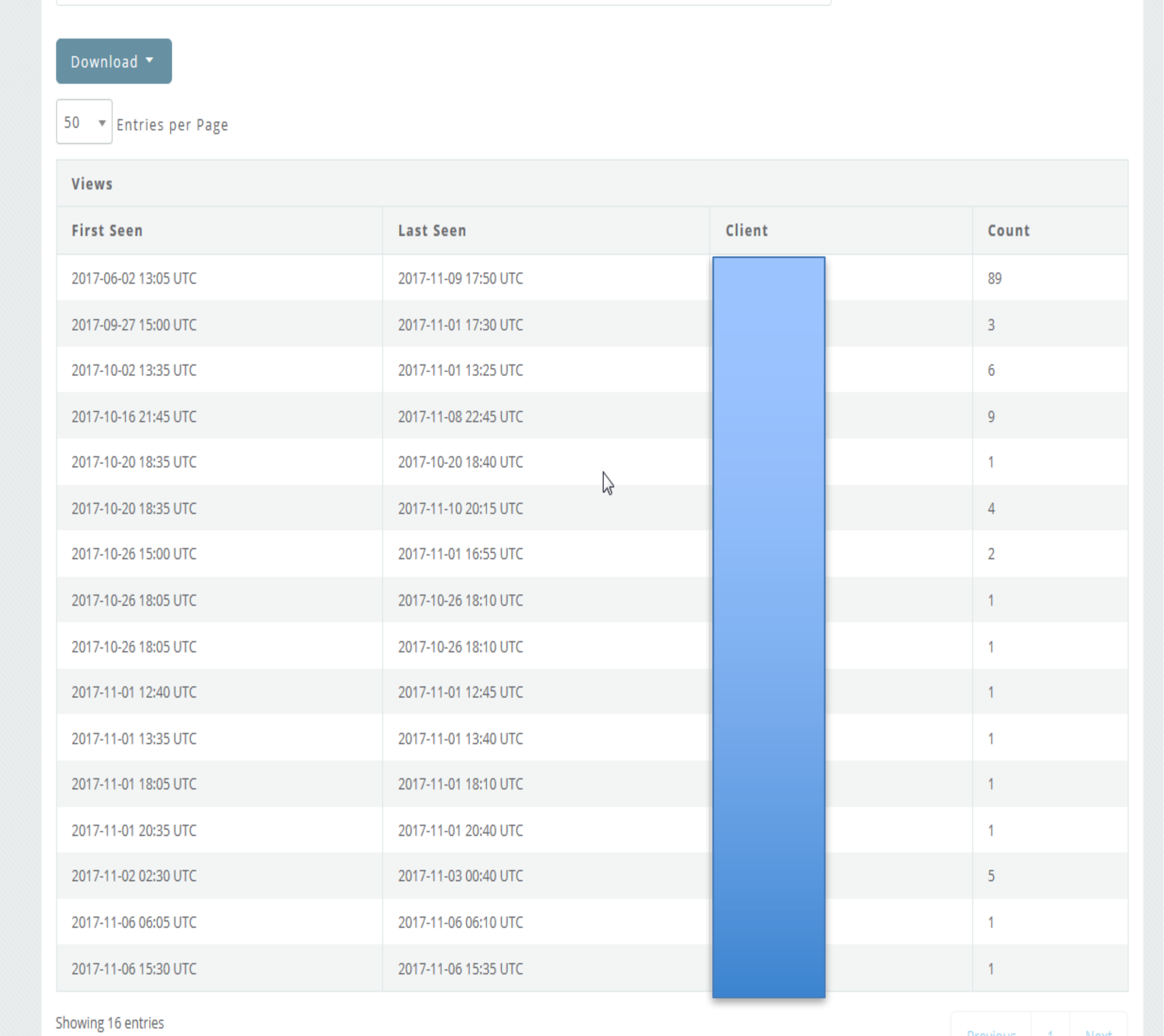
NETWORK

······ Streaming Threat Intelligence

D-ZONE DNS FIREWALL RESULTS

- Over 225,000 users
- 2000 queries per second
- All using malware, phishing and ransomware protection
- 30% using content filtering with the majority using custom filters appropriate to their organizations
- Many use blacklist feature to selectively block things that have gotten through their network

RANSOMWARE BLOCKS – 30 DAYS

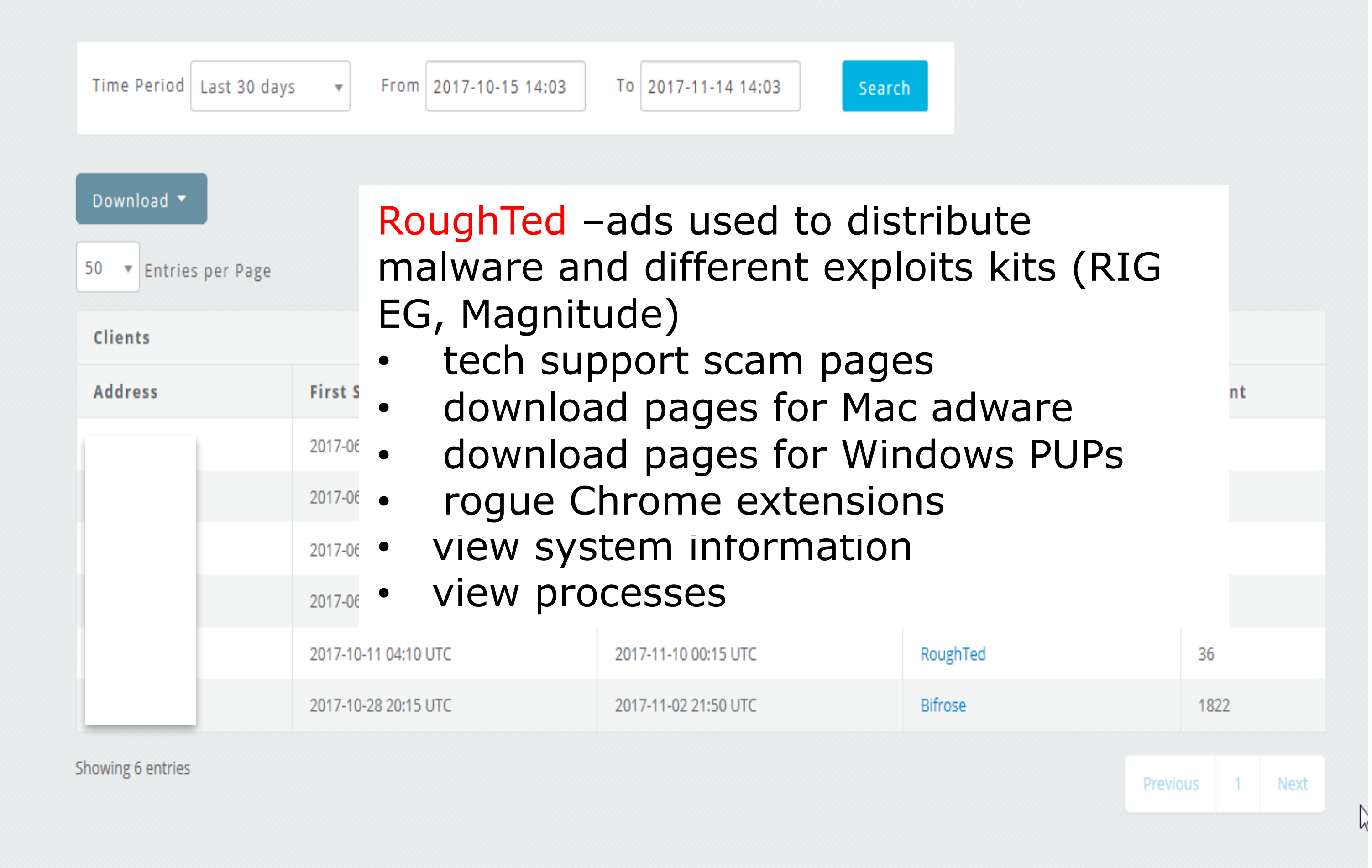


Views

First Seen	Last Seen	Client	Count
2017-06-02 13:05 UTC	2017-11-09 17:50 UTC	[redacted]	89
2017-09-27 15:00 UTC	2017-11-01 17:30 UTC	[redacted]	3
2017-10-02 13:35 UTC	2017-11-01 13:25 UTC	[redacted]	6
2017-10-16 21:45 UTC	2017-11-08 22:45 UTC	[redacted]	9
2017-10-20 18:35 UTC	2017-10-20 18:40 UTC	[redacted]	1
2017-10-20 18:35 UTC	2017-11-10 20:15 UTC	[redacted]	4
2017-10-26 15:00 UTC	2017-11-01 16:55 UTC	[redacted]	2
2017-10-26 18:05 UTC	2017-10-26 18:10 UTC	[redacted]	1
2017-10-26 18:05 UTC	2017-10-26 18:10 UTC	[redacted]	1
2017-11-01 12:40 UTC	2017-11-01 12:45 UTC	[redacted]	1
2017-11-01 13:35 UTC	2017-11-01 13:40 UTC	[redacted]	1
2017-11-01 18:05 UTC	2017-11-01 18:10 UTC	[redacted]	1
2017-11-01 20:35 UTC	2017-11-01 20:40 UTC	[redacted]	1
2017-11-02 02:30 UTC	2017-11-03 00:40 UTC	[redacted]	5
2017-11-06 06:05 UTC	2017-11-06 06:10 UTC	[redacted]	1
2017-11-06 15:30 UTC	2017-11-06 15:35 UTC	[redacted]	1

Showing 16 entries

BLOCKS FOR AN ONTARIO CITY



Time Period: Last 30 days | From: 2017-10-15 14:03 | To: 2017-11-14 14:03

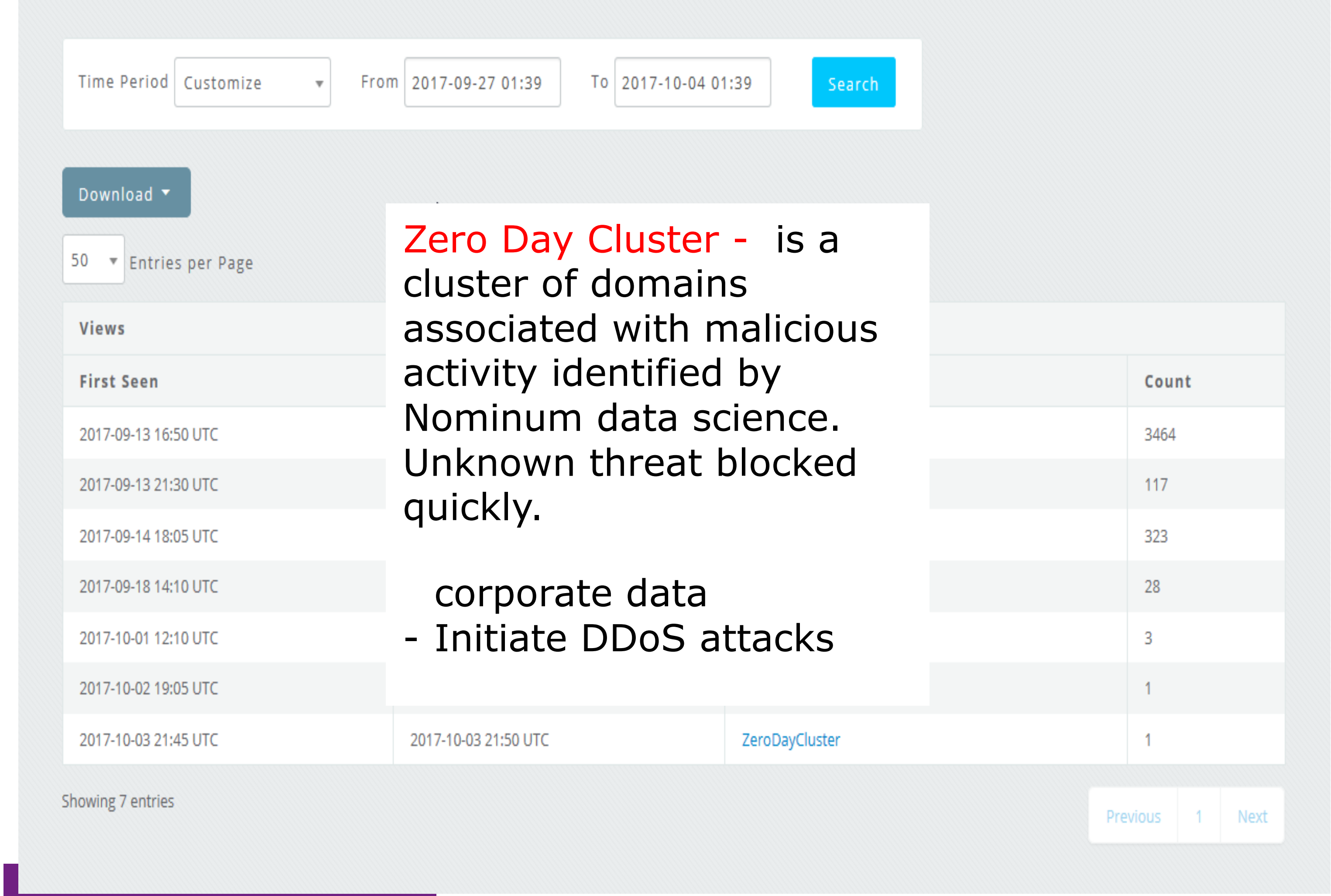
RoughTed –ads used to distribute malware and different exploits kits (RIG EG, Magnitude)

- tech support scam pages
- download pages for Mac adware
- download pages for Windows PUPs
- rogue Chrome extensions
- view system information
- view processes

Address	First S			nt
[redacted]	2017-06			
	2017-06			
	2017-06			
	2017-06			
	2017-10-11 04:10 UTC	2017-11-10 00:15 UTC	RoughTed	36
	2017-10-28 20:15 UTC	2017-11-02 21:50 UTC	Bifrose	1822

Showing 6 entries

BLOCKS FOR A HOSPITAL – 1 WEEK



Views

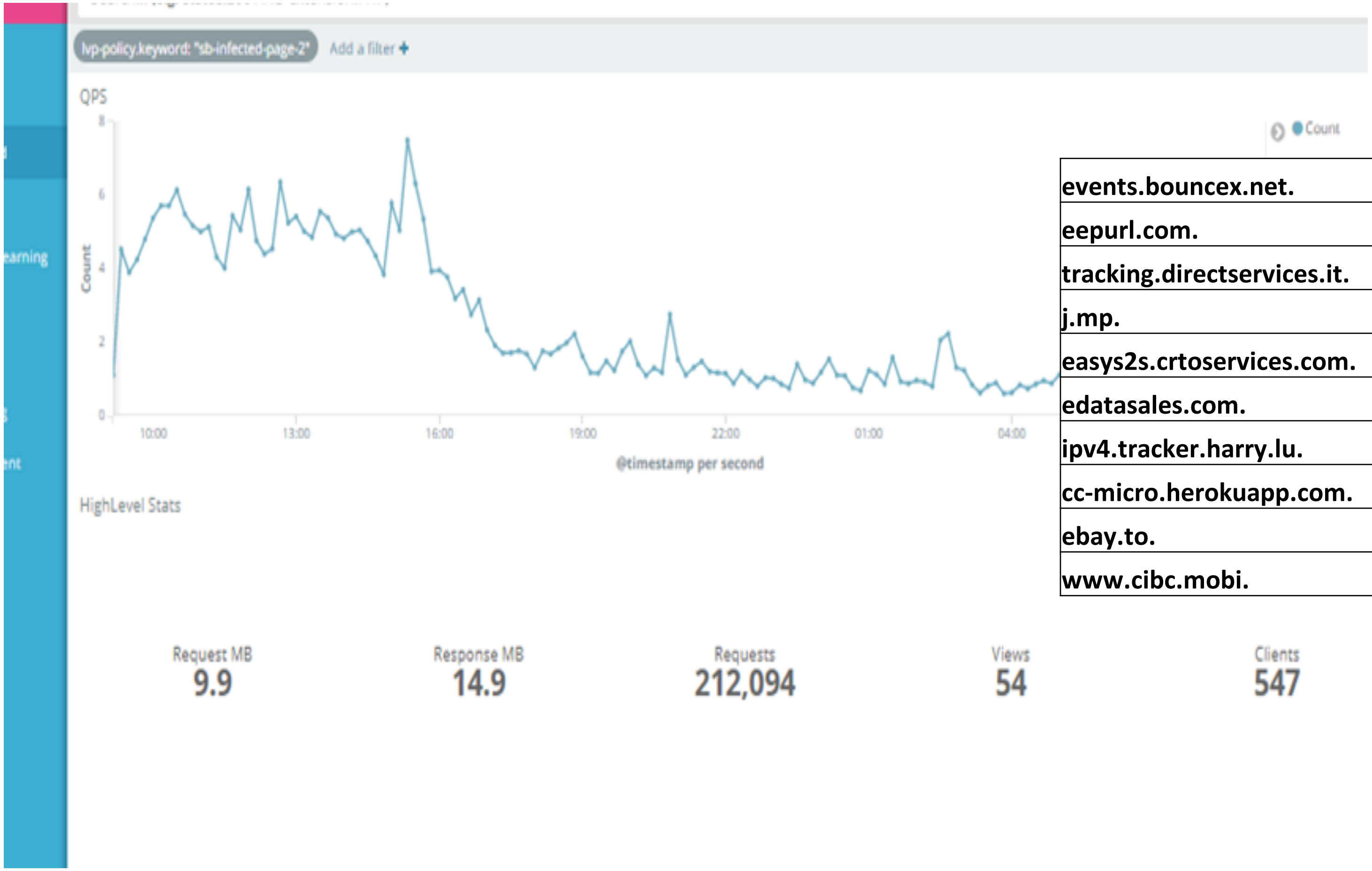
First Seen			Count
2017-09-13 16:50 UTC			3464
2017-09-13 21:30 UTC			117
2017-09-14 18:05 UTC			323
2017-09-18 14:10 UTC			28
2017-10-01 12:10 UTC			3
2017-10-02 19:05 UTC			1
2017-10-03 21:45 UTC	2017-10-03 21:50 UTC	ZeroDayCluster	1

Showing 7 entries

Zero Day Cluster - is a cluster of domains associated with malicious activity identified by Nominum data science. Unknown threat blocked quickly.

corporate data
- Initiate DDoS attacks

PHISHING BLOCKS



HighLevel Stats

Request MB
9.9

Response MB
14.9

Requests
212,094

Views
54

Clients
547

events.bouncex.net.	32,486
eepurl.com.	2,074
tracking.directservices.it.	1,138
j.mp.	877
easys2s.crtoservices.com.	768
edatasales.com.	744
ipv4.tracker.harry.lu.	696
cc-micro.herokuapp.com.	443
ebay.to.	378
www.cibc.mobi.	338

FALSE POSITIVES?

We have found multiple instances where cloud services or websites offering services were unaware of being hacked to distribute malware

- Seemingly safe educational game websites added to block lists and no longer accessible by users in a school board

- New Health Care portal riddled with “installment loan” hacks on launch

DATA IS GOLD!

Unique view on the Canadian Internet

- Visibility on Canadian Internet
- Ability to see new threats
- Trends in usage
- Communities of interest to share and block threats
- Linkage back to registry

QUESTIONS

Contact Me:
Mark Gaudet
Canadian Internet Registration Authority (CIRA)
979 Bank Street, Suite 400, Ottawa, Ontario, K1S 5K5
Office: 613.237.5335 x302
Email: mark.gaudet@cira.ca