Canadian Shield

A Year of Experience Operating a Secure National DNS Infrastructure for Canada

Mark Gaudet mark.gaudet@cira.ca

ICANN IDS 2021

Agenda

- Background
- Canadian Shield
- Architecture
- Threat feeds
- Data Privacy
- Security
- Results
- Partners/Ecosystem

WWW.CIRA.CA

CIRA Cybersecurity Services

Why is CIRA operating a national DNS security service.

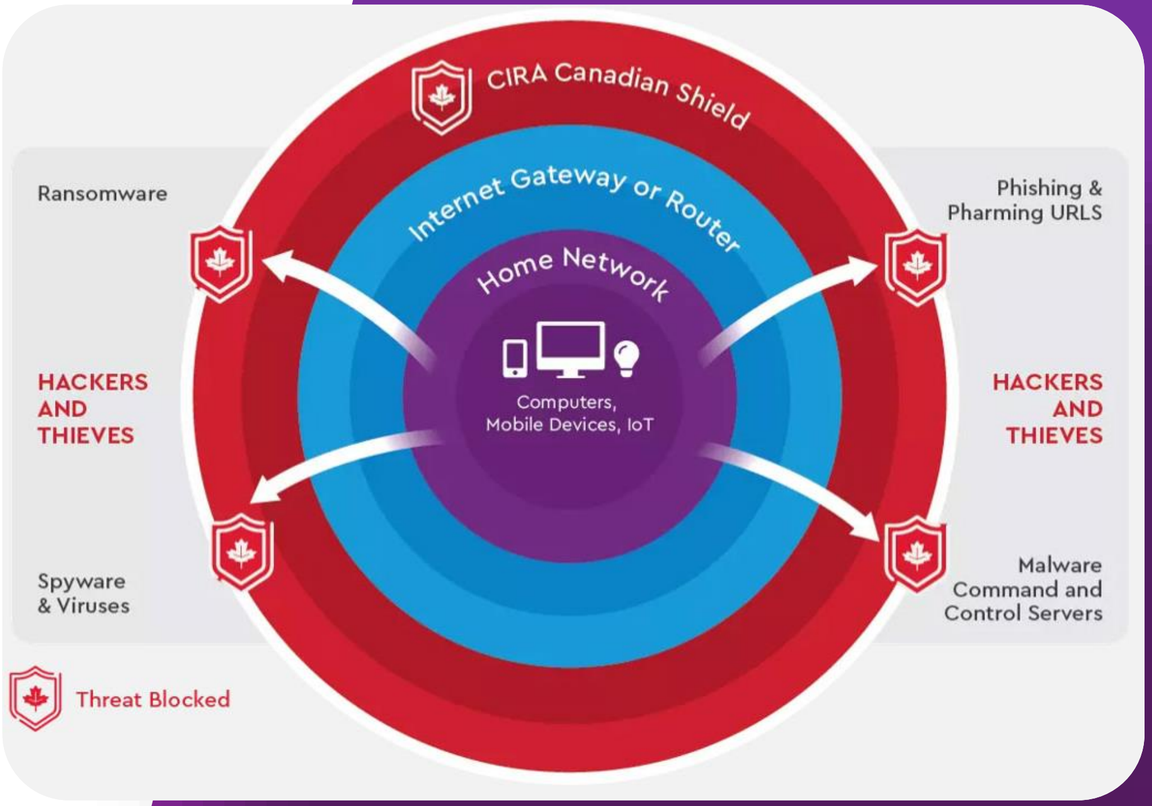
Happy First Birthday

CIRA Canadian Shield

Free DNS service that extends the core threat blocking capability to home users.

No personal data is used, or resold.

Launched April 23, 2020!



Same benefits DNS Firewall provides but with the home network at the center

Open recursive service

Three options

Private – provides DNS resolution only

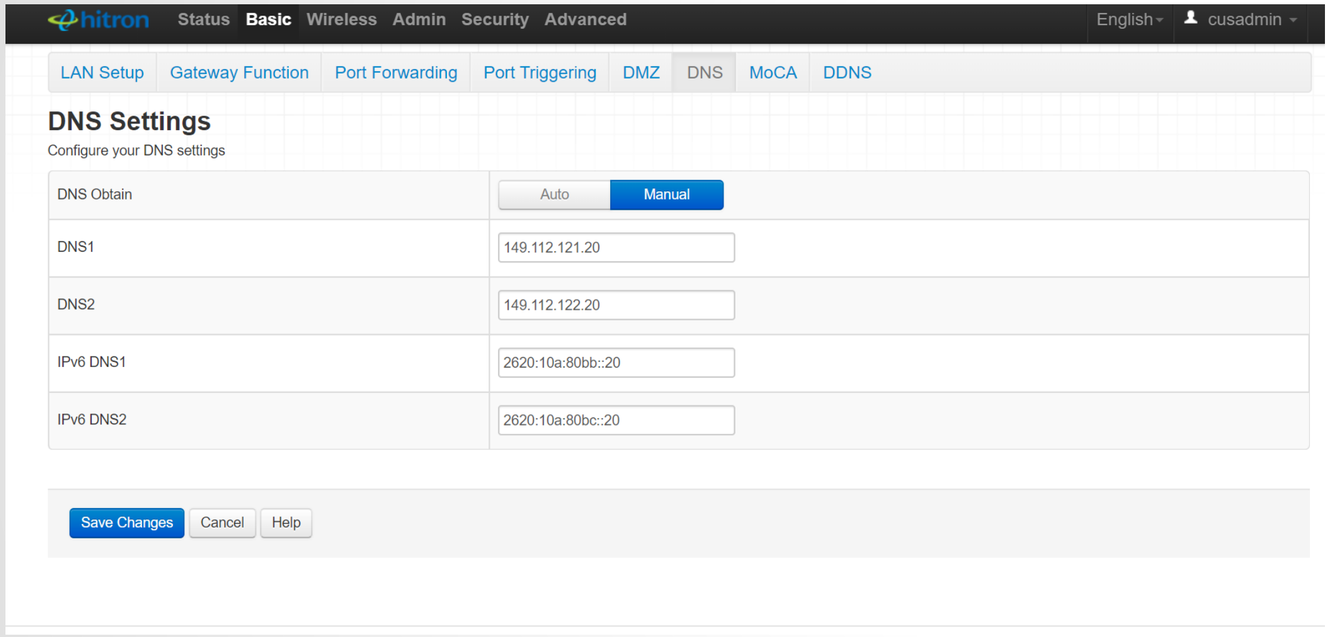
Protected – includes malware and phishing protection

Family – includes protected plus blocking pornographic content

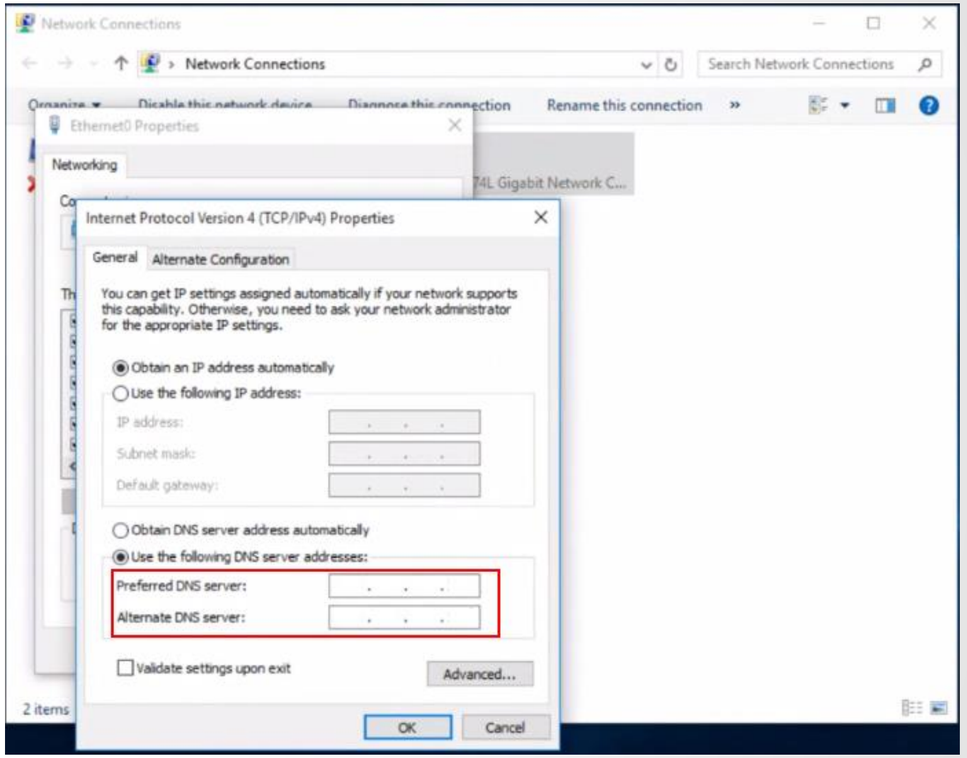
Malware Blocked by CIRA Canadian Shield

The site you are trying to visit contains malicious content. It has been blocked to avoid causing harm your computer, device, or network or subject your personal information to theft.

Why am I seeing this page?



Rogers Hitron Router



Windows Operating System

Mobile Apps

- Partnership with Mobolize and Akamai
- Providing the Android and IoS for free for use with Canadian Shield
- Redirect queries to Canadian Shield automatically
- In app upgrades
  - Encryption on wifi
  - Bonding

Summary of resolvers

This open recursive service is accessed via DNS settings in the router or operating system. It also supports DNS encryption.

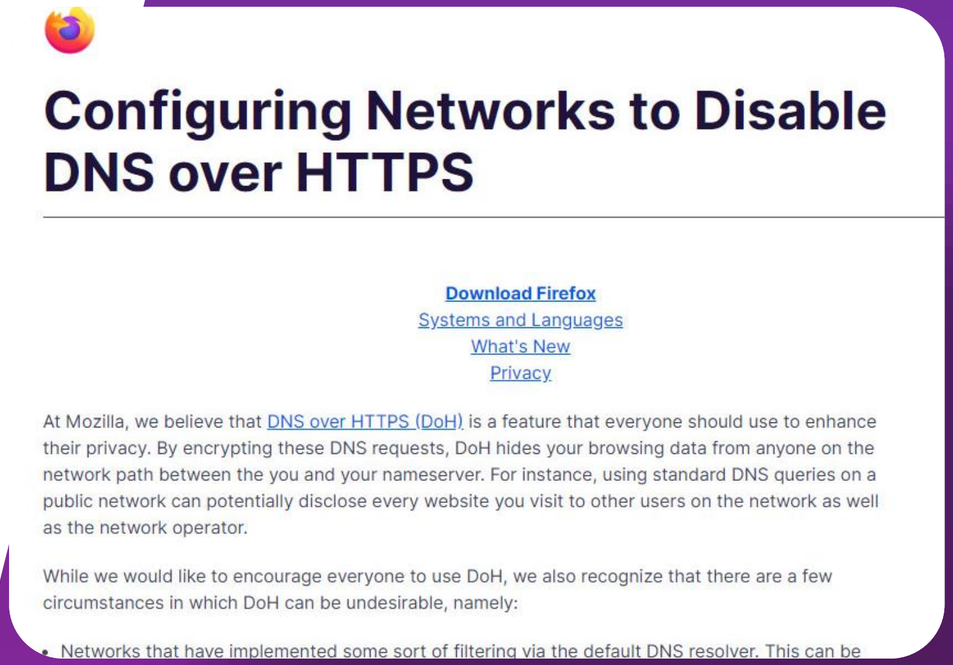
	Features	IPv4	IPv6	DoH	DoT
Private	DNS resolution only	149.112.121.10 149.112.122.10	2620:10A:80BB::10 2620:10A:80BC::10	https://private.canadianshield.cira.ca/dns-query	private.canadianshield.cira.ca
Protected	Malware and phishing protection	149.112.121.20 149.112.122.20	2620:10A:80BB::20 2620:10A:80BC::20	https://protected.canadianshield.cira.ca/dns-query	protected.canadianshield.cira.ca
Family	*Protected* + blocking pornographic content	149.112.121.30 149.112.122.30	2620:10A:80BB::30 2620:10A:80BC::30	https://family.canadianshield.cira.ca/dns-query	family.canadianshield.cira.ca

+ Apple iOS and Play store downloads for mobile clients

DNS encryption

DNS over HTTPs and DNS over TLS are fully supported by CIRA Canadian Shield.

CIRA fully supports DNS privacy and security.



Configuring Networks to Disable DNS over HTTPS

Download Firefox
Systems and Languages
What's New
Privacy

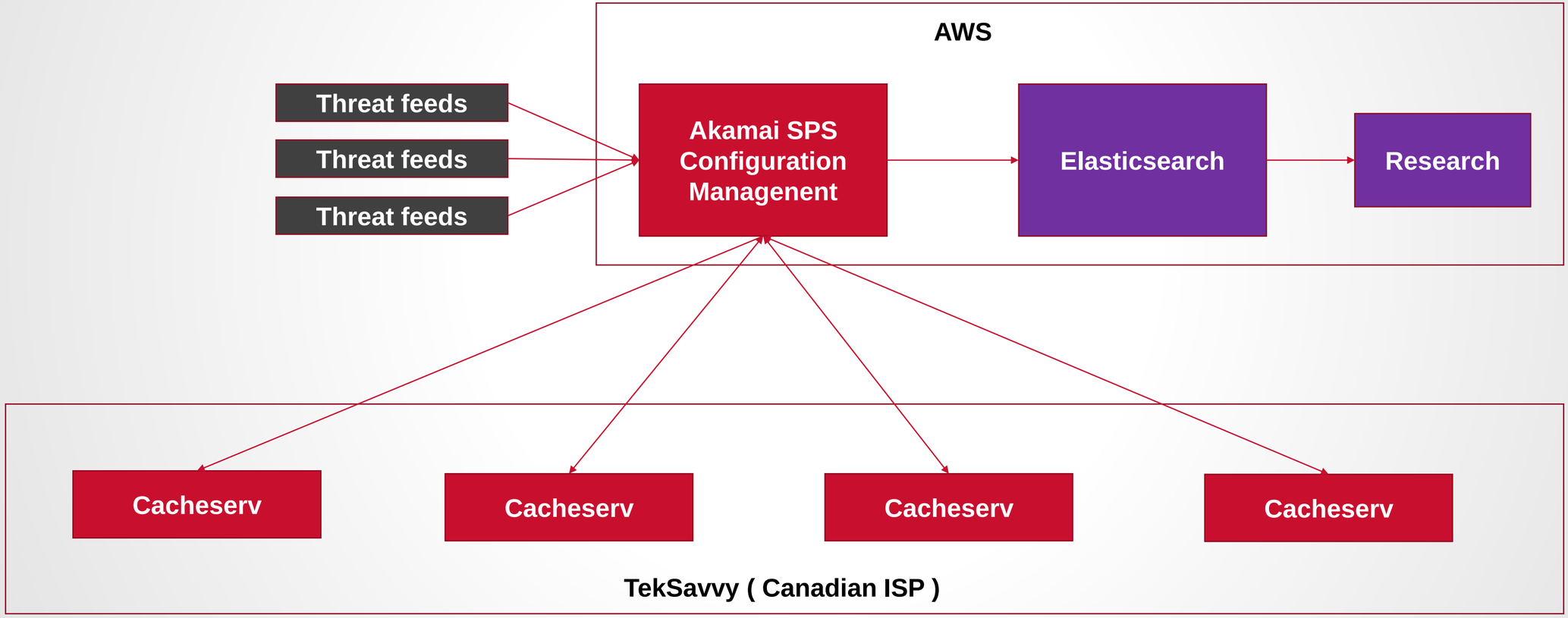
At Mozilla, we believe that DNS over HTTPS (DoH) is a feature that everyone should use to enhance their privacy. By encrypting these DNS requests, DoH hides your browsing data from anyone on the network path between the you and your nameserver. For instance, using standard DNS queries on a public network can potentially disclose every website you visit to other users on the network as well as the network operator.

While we would like to encourage everyone to use DoH, we also recognize that there are a few circumstances in which DoH can be undesirable, namely:

- Networks that have implemented some sort of filtering via the default DNS resolver. This can be

Canadian Shield

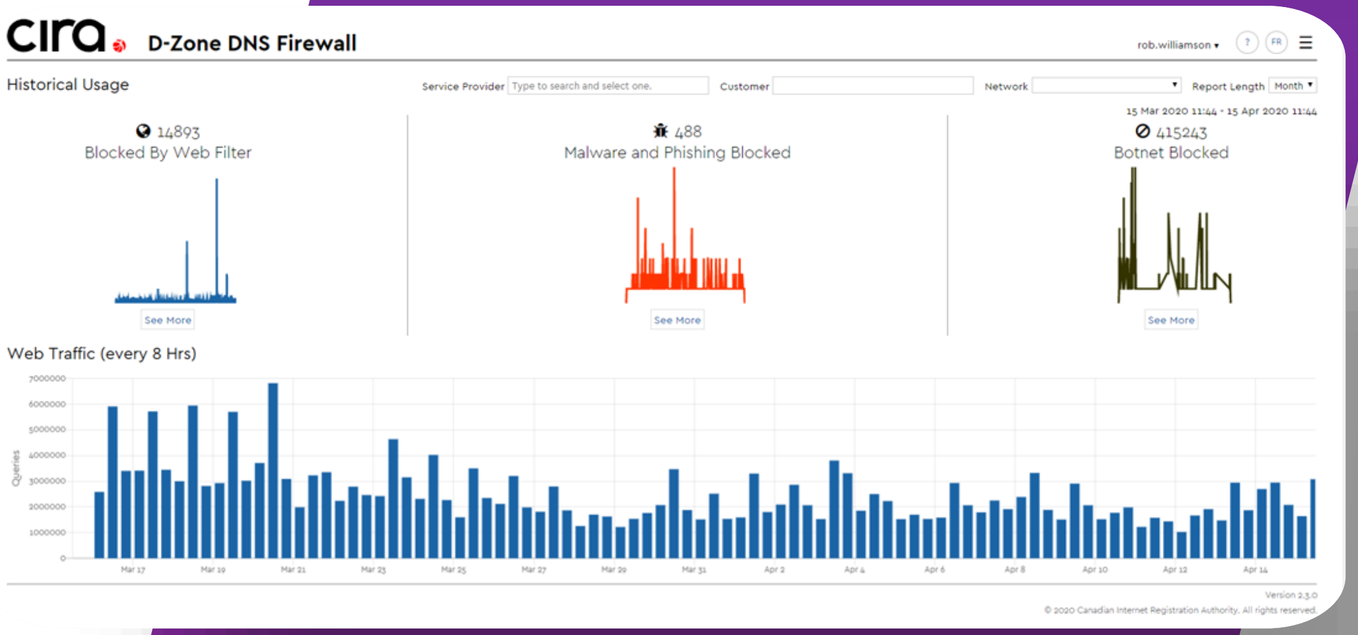
Architecture



DNS Firewall

Threat detection

- ✓ Incorporates Akamai data science with 3rd party threat feeds
- ✓ Over 100,000 net new domains are added to the block list every day
- ✓ Time from first query to block list is minutes



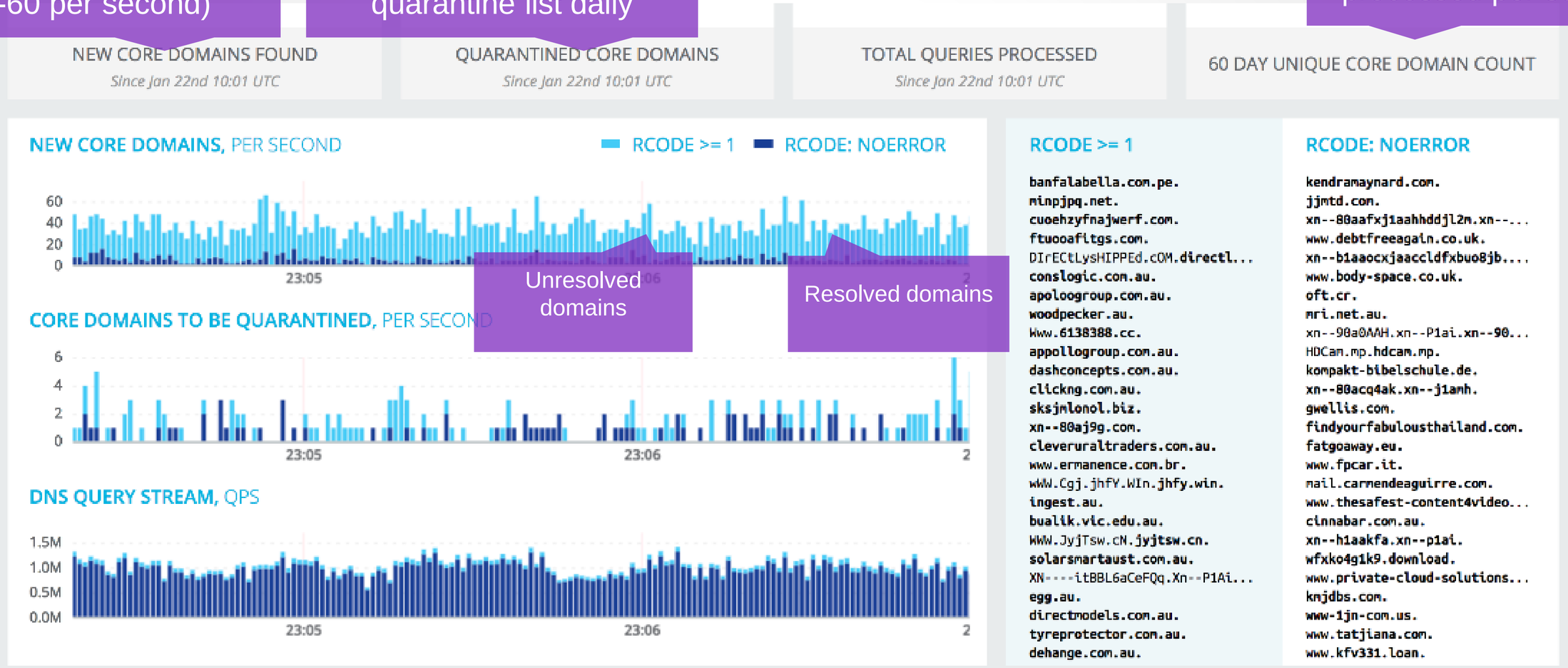
One month view into a firewall customer

Akamai Threat feed Dashboard

New core domains filtered (50-60 per second)

4-5 % of domains added to quarantine list daily

1 million queries processed per second



13

Working with Canadian organizations

Cybertip.ca

Includes the child exploitation list from the Canadian Center for Child Protection

Working with Canadian organizations

CCCS Threat Feed

Threat feed includes Indicators of Compromise (IoCs) derived from many sources such as Canadian cyber incidents, malware analysis and strategic partnerships.

CIRA is sharing back threat blocking activity in Canada.

No personally identifiable information (PII) of any kind is transmitted back to the Canadian Centre for Cyber Security.

DNS Privacy

What does privacy mean

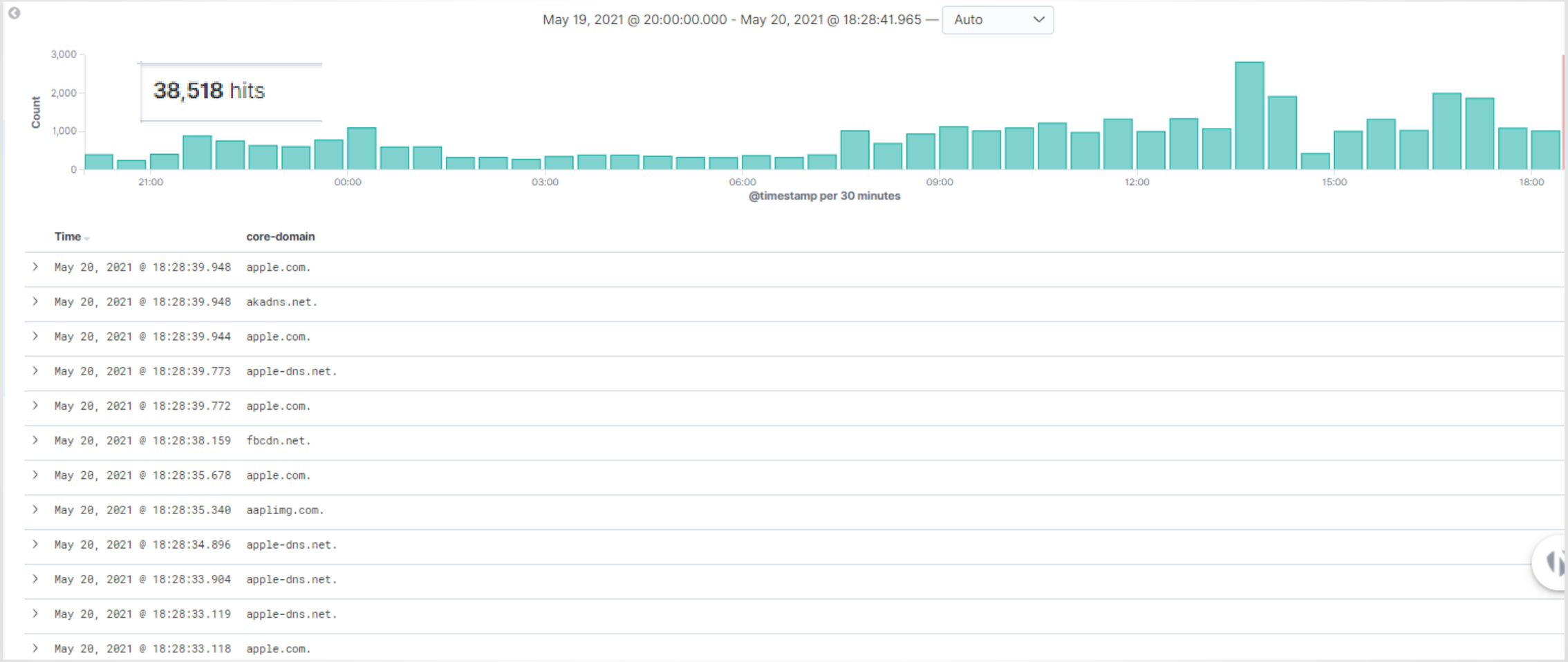
DNS data combined with IP address is private data

The DNS is a record of everything you do online.

Most are unaware of who has their DNS data and how it used

Normal Activity

Typical Household – 38,000 DNS queries per day



Time	core-domain
May 20, 2021 @ 18:28:39.948	apple.com.
May 20, 2021 @ 18:28:39.948	akadns.net.
May 20, 2021 @ 18:28:39.944	apple.com.
May 20, 2021 @ 18:28:39.773	apple-dns.net.
May 20, 2021 @ 18:28:39.772	apple.com.
May 20, 2021 @ 18:28:38.159	fbcdn.net.
May 20, 2021 @ 18:28:35.678	apple.com.
May 20, 2021 @ 18:28:35.340	aaplimg.com.
May 20, 2021 @ 18:28:34.896	apple-dns.net.
May 20, 2021 @ 18:28:33.904	apple-dns.net.
May 20, 2021 @ 18:28:33.119	apple-dns.net.
May 20, 2021 @ 18:28:33.118	apple.com.

Data Collection and Usage

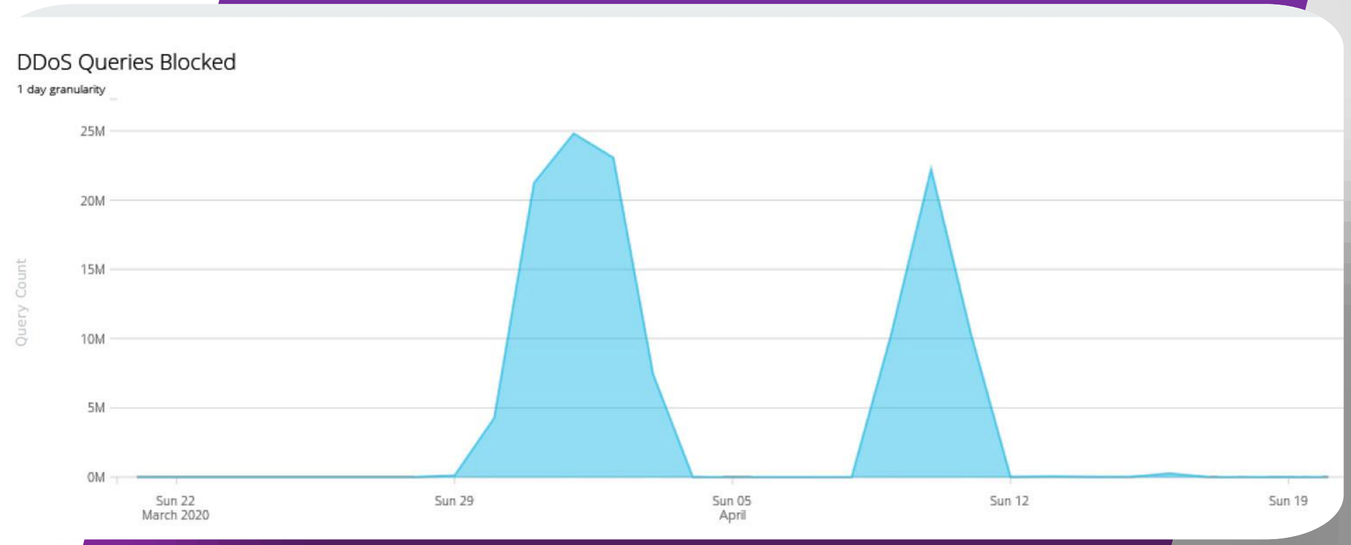
- Detailed DNS is collected and stored for less than 24 hours in ELK stack
- Detailed query and response data
- Used for protecting the service and estimating usage
- 24 hour indexes are auto deleted
- List of blocked domains without source IP data is stored longer
- We share block counts against threat feeds provided without IPs
- We do not censor content
- Privacy policy was audited by Deloitte

Protecting Canadian Shield

Threats

An open recursive service is target for abuse

- Ran full suite of tests using RIPE and held internal hack-a-thons
- Within minutes of going live the service was already being probed



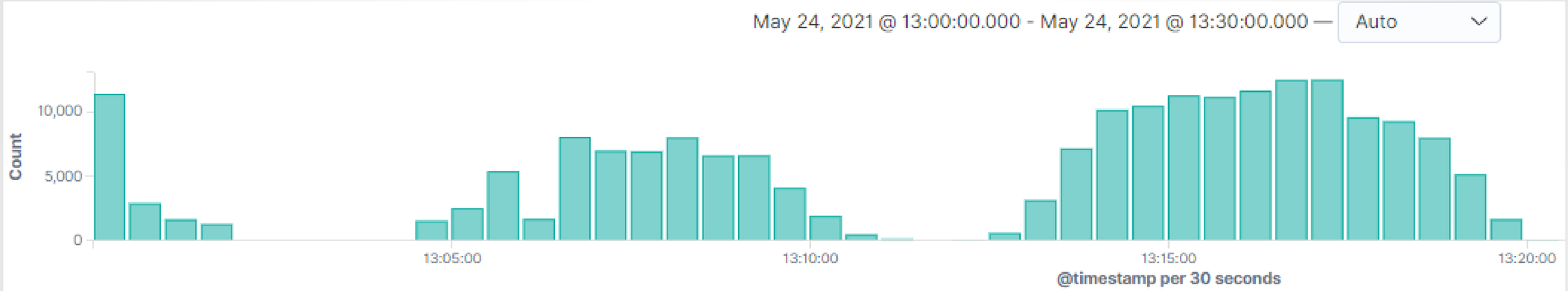
Protecting Canadian Shield

Akamai Threat Avert

Reflection	Amplification	Any	Pseudo Random Subdomain Attacks
Rate limiting	Automatic protection	IP blocking	High Capacity

Malicious Activity

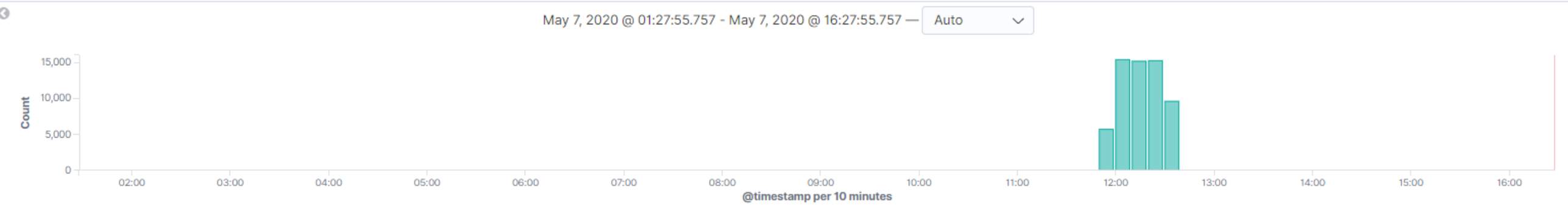
Amplification – Any Attacks



Time	core-domain	policies	client-address-geo.country_name
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia
May 24, 2021 @ 13:20:08.701	census.gov.	DropANY-1	Russia

Malicious Activity

Pseudo Random Subdomain Attacks



Time	core-domain	client-address-geo.country_name	dns-message.rdtype	dns-message.qname	policies	client-address
May 7, 2020 @ 12:36:09.799	elstc.co.	Netherlands	A	zzwpq.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.786	elstc.co.	Netherlands	A	zzw5l.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.786	elstc.co.	Netherlands	A	zza-a.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.655	elstc.co.	Netherlands	A	zzl57.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.655	elstc.co.	Netherlands	A	zzvyn.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.654	elstc.co.	Netherlands	A	zzyav.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.572	elstc.co.	Netherlands	A	zzp0h.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.571	elstc.co.	Netherlands	A	zzlxn.elstc.co.	vta-rsd-1	108.61.166.9
May 7, 2020 @ 12:36:09.563	elstc.co.	Netherlands	A	zzac4.elstc.co.	vta-rsd-1	108.61.166.9

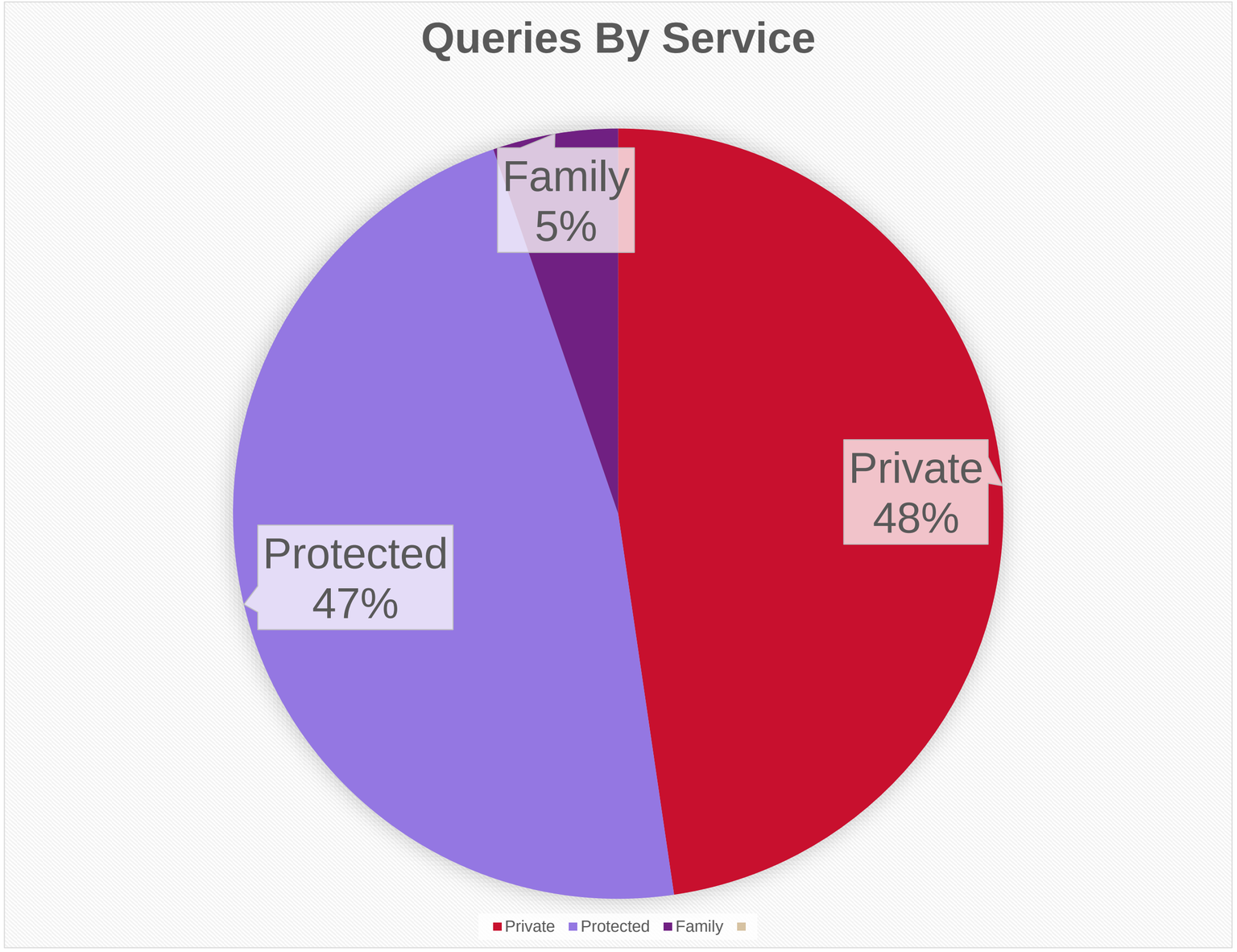
Canadian Shield

Day In The Life (DITL) Results

DITL Queries By Service Type

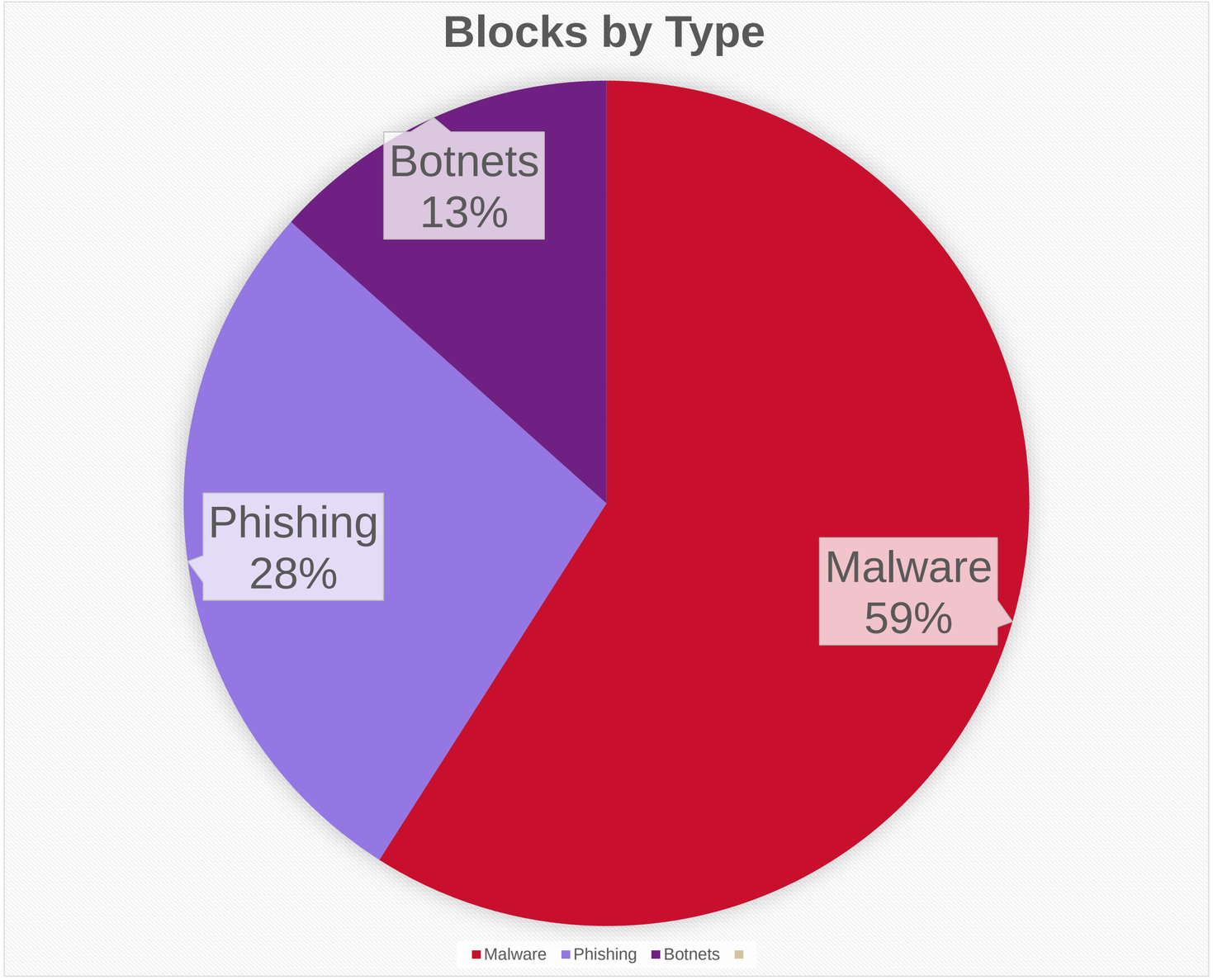
732,344,413 Queries

- 80.1% Canada
- 4.1% United States



DITL Blocks by Type

- **52,728** Blocks
- 0.5 blocks/user/day



Top Blocks

Top Malware	
microsip.org.	2,871
irc.zief.pl.	2,305
proxim.ircgalaxy.pl.	2,259
pool.minexmr.com.	1,583
mine.moneropool.com.	1,570
mine.xmrpool.net.	1,570
pool-vegas.xmrpool.net.	1,570
klkjwre9fqwieluoi.info.	825
tes.enterhere2.biz.	817
mudraorthotics.com.	532

Top Phishing	
robichakraborty.com.	370
desjardins-suspendu.xyz.	254
desjardinsvalid.xyz.	206
desjardins-vali.xyz.	198
ww16.signin-paypal.info.	196
www.bryantautocenter.com	190
presidentsbarberclub.com.	188
ghanahotgirls.com.	184
godeaug.org.	184
shred-of-dignity.org.	184

Top Botnets	
jjckwupqrll.org.	886
nkkhsy.com.	37
tdzubx.net.	36
qed194.org.	36
avbllnjkt.ws.	13
avbllnj.ws.	13
8isbbs.cf.	13
6sv9ipbz.mx.	13
6sv9ip.mx.	13
0hkjbxu.rocks.	13

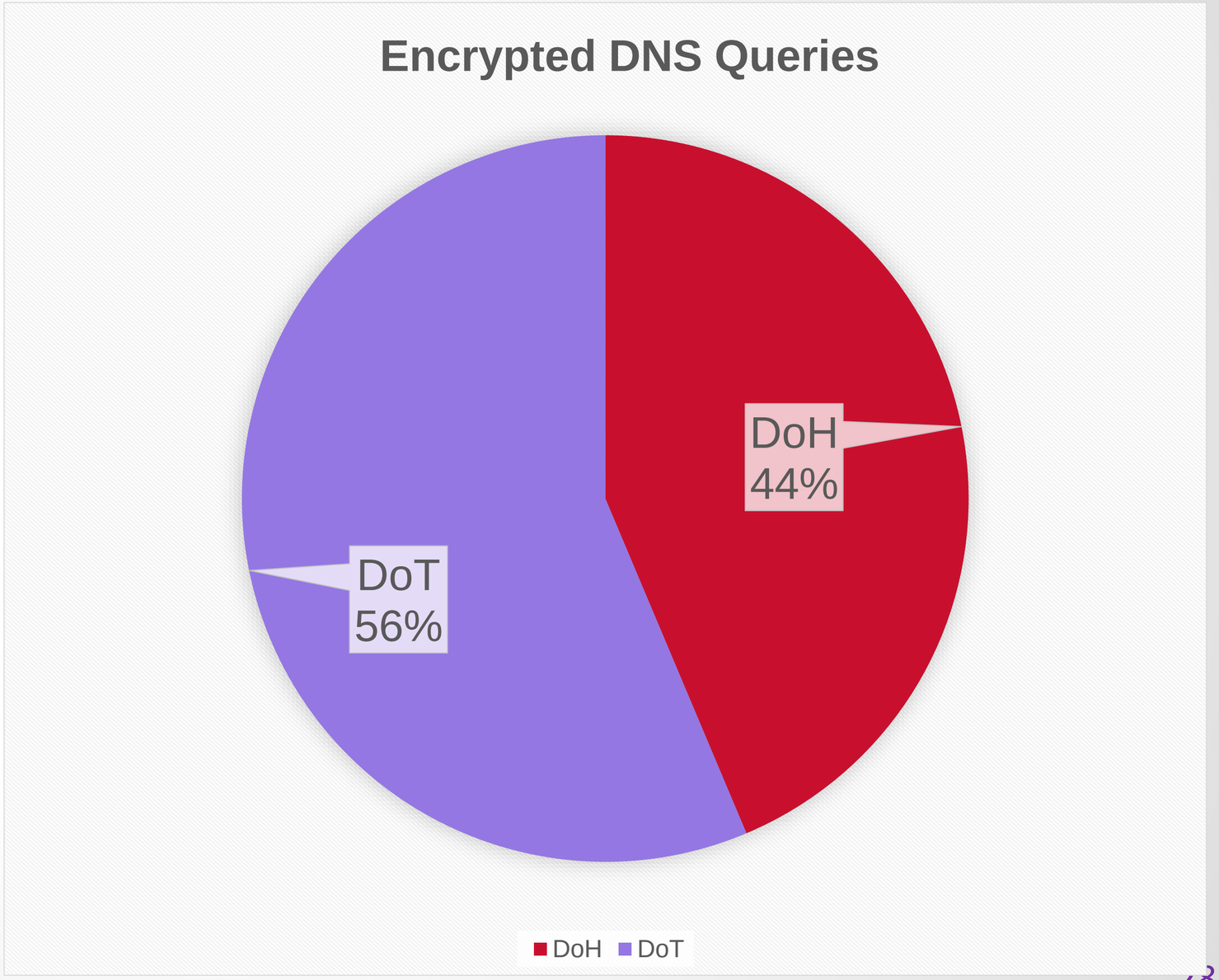
Canadian Shield

Top Threats

Threat Name	Description	Count
Simda	Known malware/botnet activity	2004
Qsnatch_v2	Backdoor malware tailored to attack QNAP storage hardware. Version 2 of DGA protocol	1890
Suspected Malware	Suspected malware/botnet activity that is in the process of being classified.	1204
MyDoom	Mass-mailing worm with variants that launch DDoS attacks or destroy local files	966
Nymaim	Known malware/botnet activity	885
Malware Call Home	Domains used for malware post-infection communications	30
Nymaim_v2	NyMaim Botnet. Version 2 of DGA protocol	25
Necurs	A very large botnet which is known mainly for the distribution of Locky ransomware and Dridex financial trojan	20
WPAD proxy hijack	Sites serving up WPAD configuration on sites likely to overlap with internal (or bogus) wpad domains	12
Agent Tesla	Information stealing malware (keystroke tracker).	8
Tinba	Malware used for financial fraud focusing on Turkey. Notable for being unusually small for banking malware. Also known as TinyBanker and Zusy.	6
Qakbot	Known malware/botnet activity	4
Conficker B	A worm that attacks old vulnerable versions of Microsoft Windows over the network.	3
Zeus	A Trojan/virus that records usernames/passwords and other sensitive data and transmits them to malicious sites over the Internet and can allow unrestricted remote access to infected computers.	2
Expiro	Family of malware used for data exfiltration.	2
Virut	A family of Windows malware that transmits sensitive user information over the network among other malicious activity.	2
FlubotMalware	Mobile spyware and botnet	1

Encrypted DNS Queries

- 1.4% encrypted
- DoH
  - 4,477,286
- DoT
  - 5,770,517



Canadian Shield

Ecosystem

Infrastructure

Threat Feeds

Research

Innovation

Summary

- Protection
- Benefit
- Ecosystem
- Resilient
- Secure
- Partnerships

Questions?

Mark Gaudet,
General Manager Cyber and DNS
mark.gaudet@cira.ca