

# Canadian Shield

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

Mark Gaudet

[mark.gaudet@cira.ca](mailto:mark.gaudet@cira.ca)

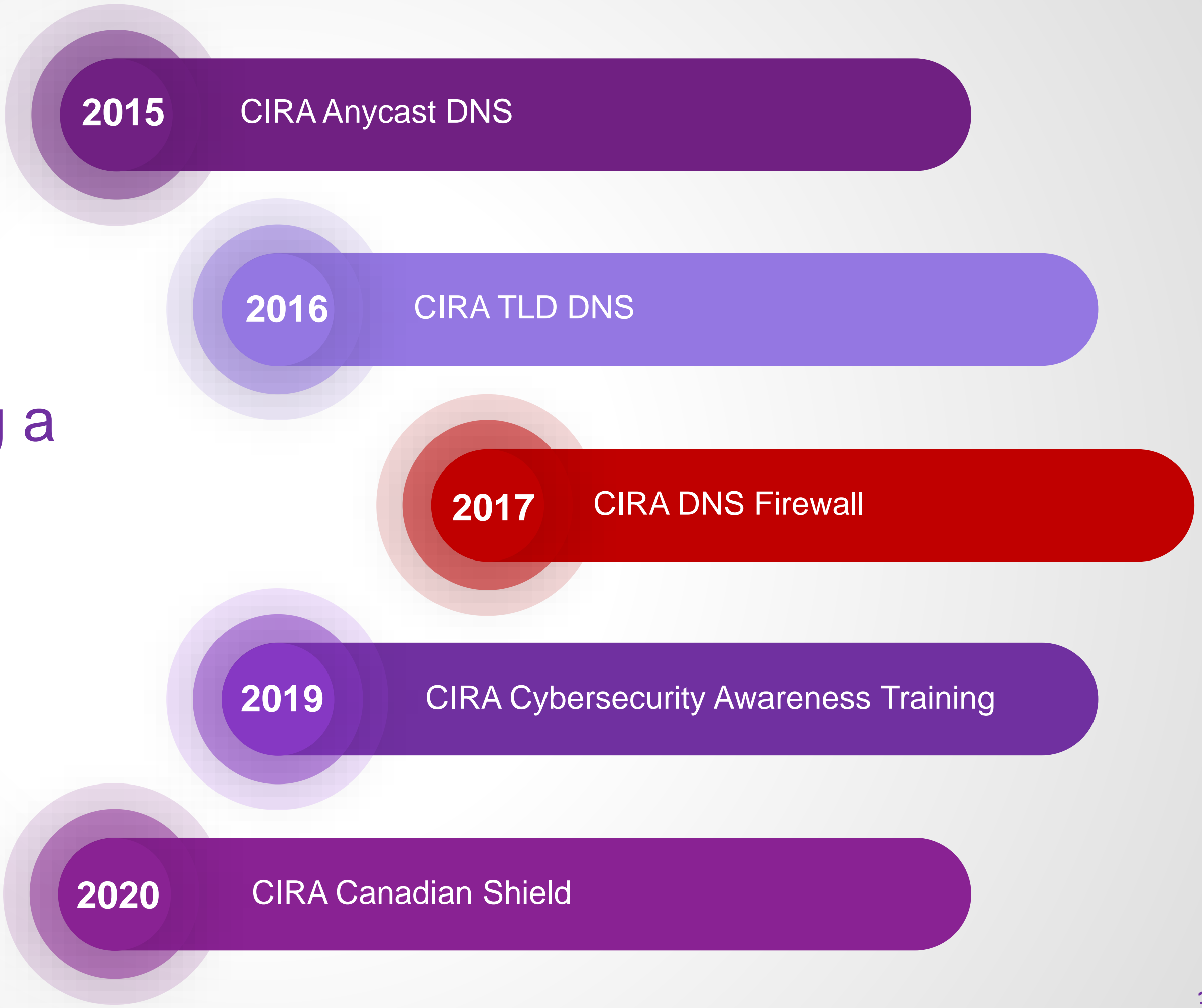
## ICANN IDS 2021

# Agenda

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

### CIRA Cybersecurity Services

Why is CIRA operating a national DNS security service.



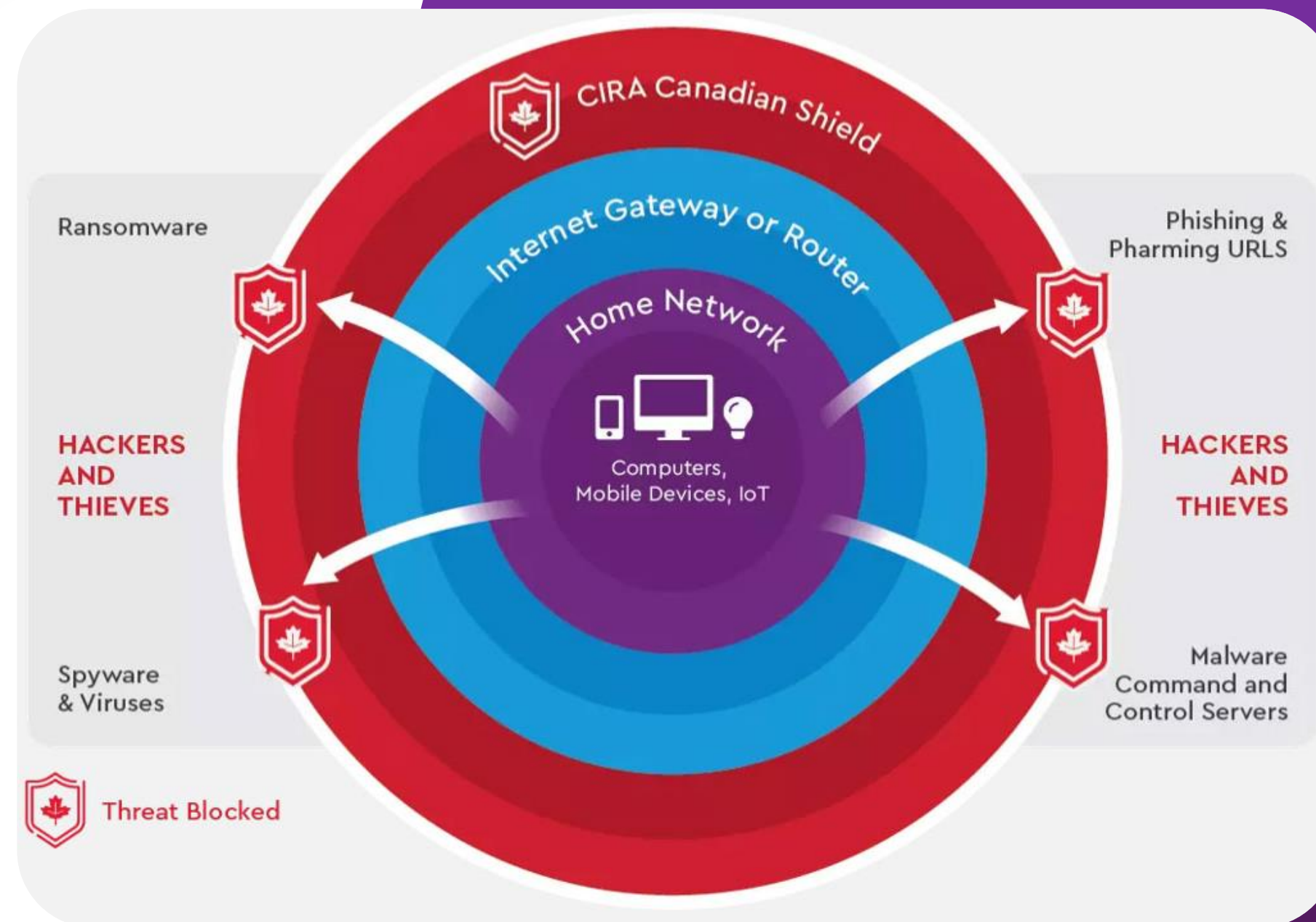
Happy First Birthday

# 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!



## Open recursive service

### Three options

**Private** – provides DNS resolution only

**Protected** – includes malware and phishing protection

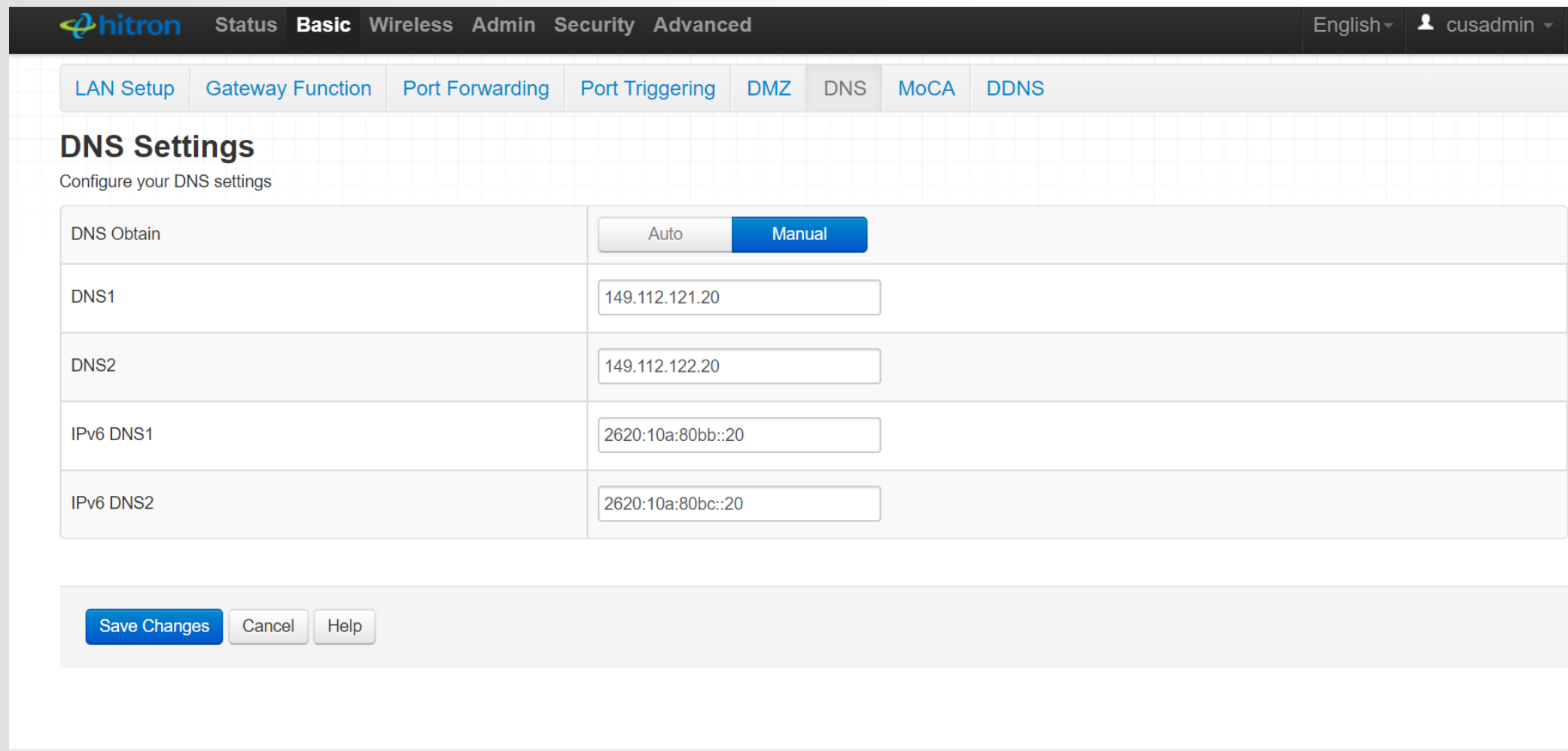
**Family** – includes protected plus blocking pornographic content



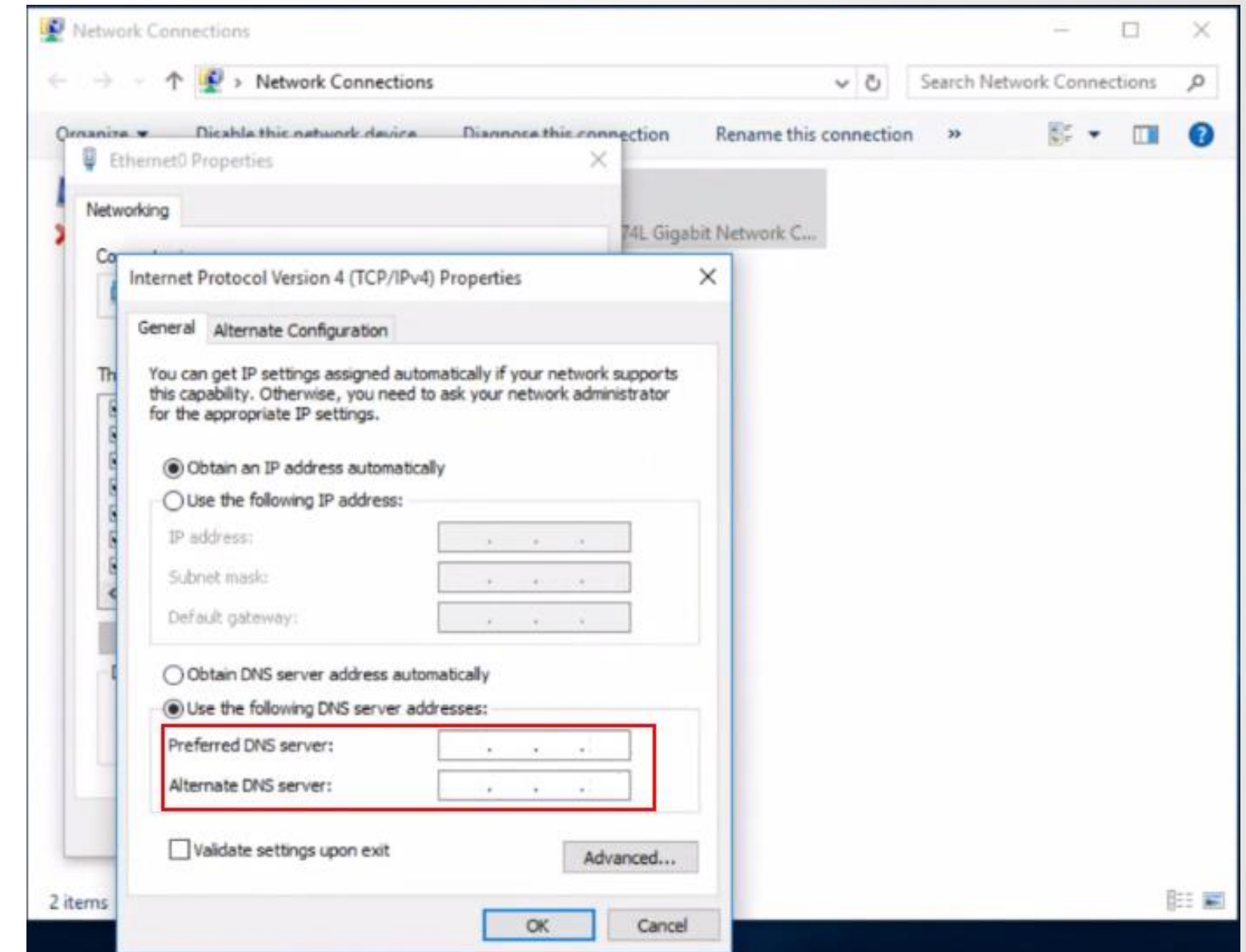
# Malware Blocked by CIRA Canadian Shield

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                              |
|------------------|---|----------------------------------|--|--|----------------------------------|
| <b>Private</b>   | DNS resolution only                       | 149.112.121.10<br>149.112.122.10 | 2620:10A:80BB::10<br>2620:10A:80BC::10 | https://private.canadianshield.cira.ca/dns-query   | private.canadianshield.cira.ca   |
| <b>Protected</b> | Malware and phishing protection           | 149.112.121.20<br>149.112.122.20 | 2620:10A:80BB::20<br>2620:10A:80BC::20 | https://protected.canadianshield.cira.ca/dns-query | protected.canadianshield.cira.ca |
| <b>Family</b>    | Protected + blocking pornographic content | 149.112.121.30<br>149.112.122.30 | 2620:10A:80BB::30<br>2620:10A:80BC::30 | https://family.canadianshield.cira.ca/dns-query    | family.canadianshield.cira.ca    |

WWW.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](#)

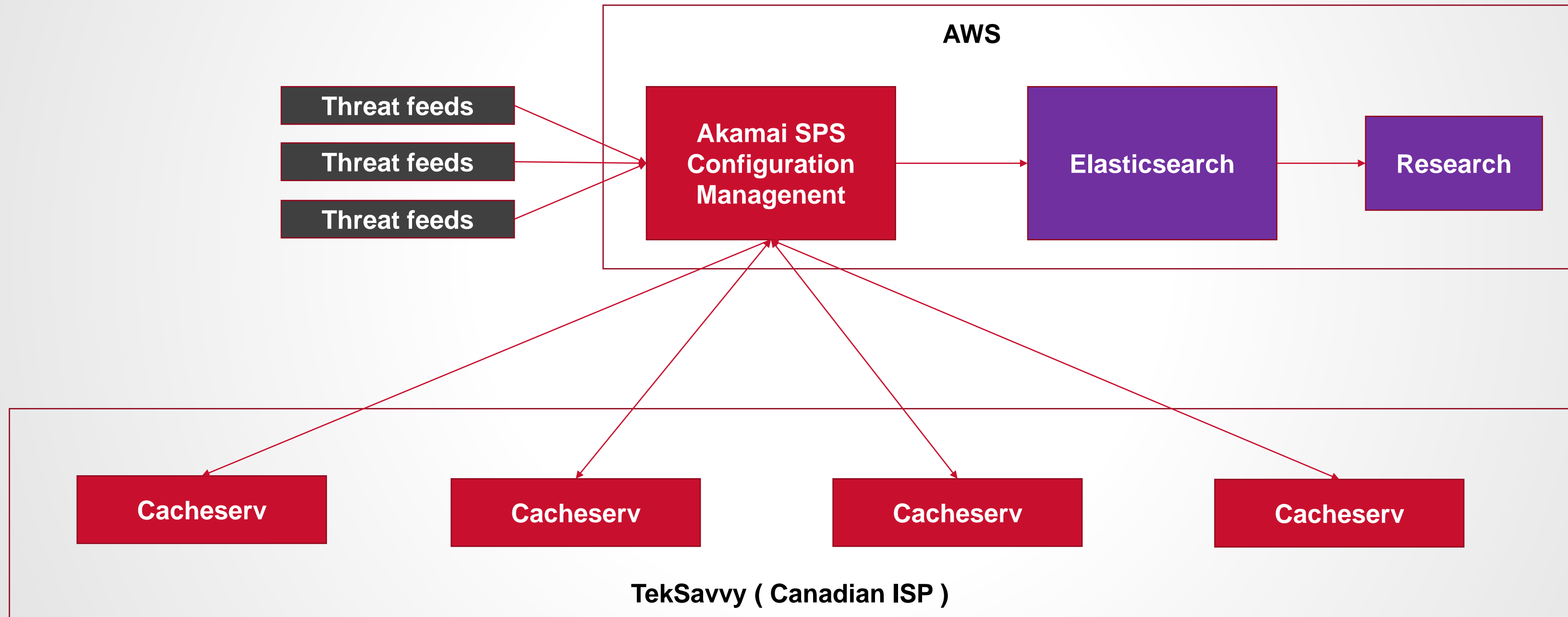
At Mozilla, we believe that [DNS over HTTPS \(DoH\)](#) is a feature that everyone should use to enhance their privacy. By encrypting these DNS requests, DoH hides your browsing data from anyone on the network path between the you and your nameserver. For instance, using standard DNS queries on a public 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

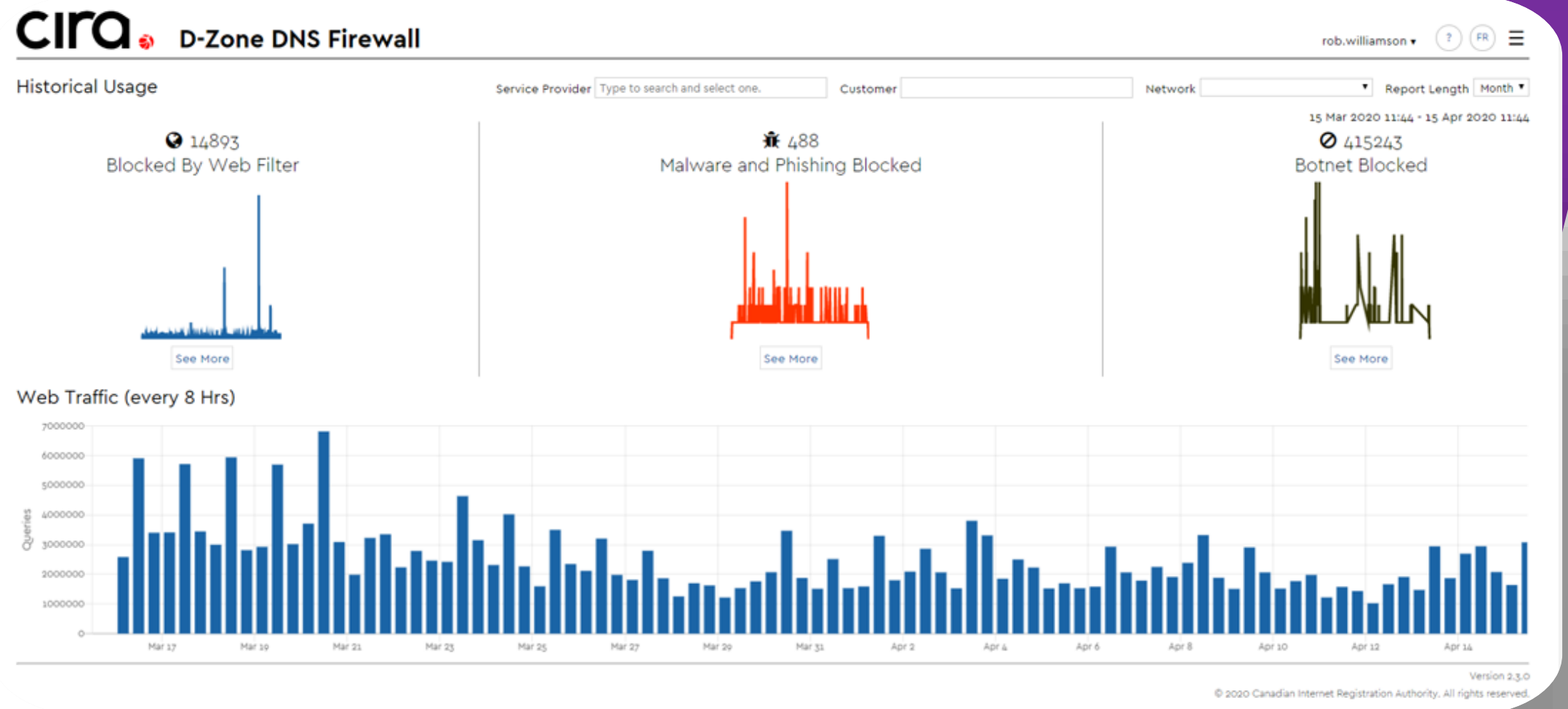
WWW.CIRA.CA



## DNS Firewall

### Threat detection

- ✓ Incorporates Akamai data science with 3<sup>rd</sup> 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

NEW CORE DOMAINS FOUND

Since Jan 22nd 10:01 UTC

QUARANTINED CORE DOMAINS

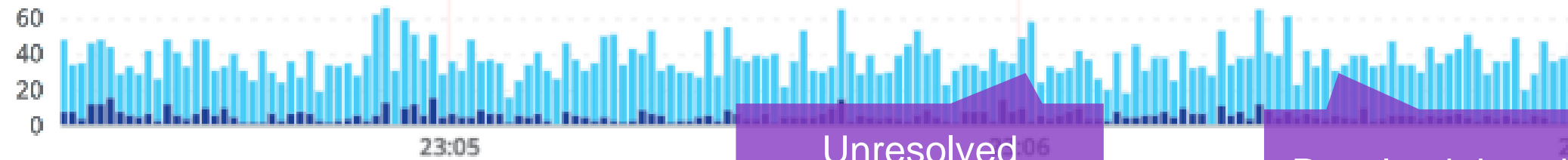
Since Jan 22nd 10:01 UTC

TOTAL QUERIES PROCESSED

Since Jan 22nd 10:01 UTC

60 DAY UNIQUE CORE DOMAIN COUNT

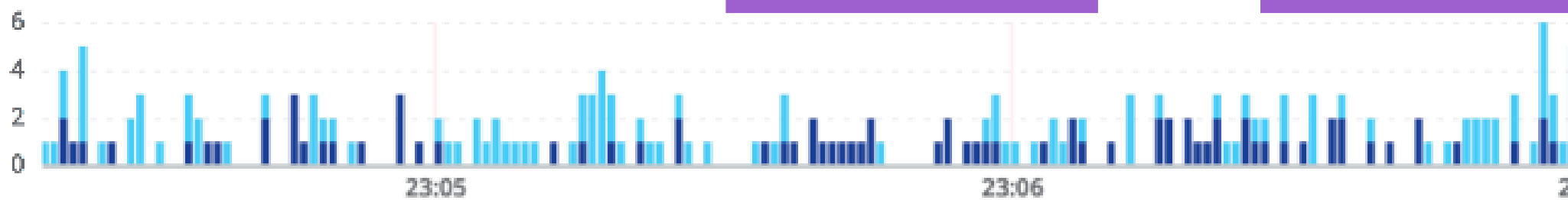
NEW CORE DOMAINS, PER SECOND



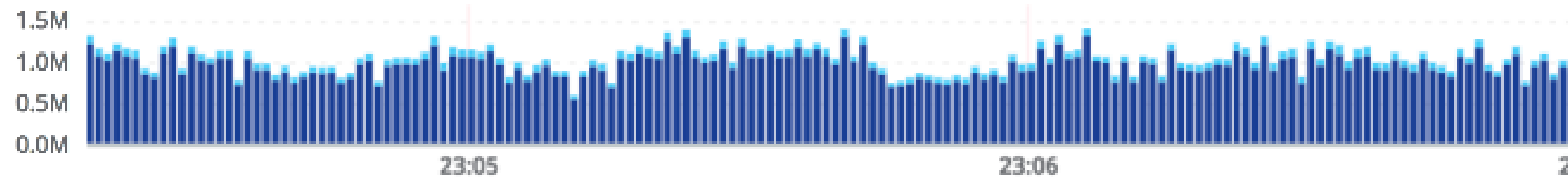
Unresolved domains

Resolved domains

CORE DOMAINS TO BE QUARANTINED, PER SECOND



DNS QUERY STREAM, QPS



RCODE >= 1

banfalabella.com.pe.  
ninpjq.net.  
cuoehzyfnajwerf.com.  
ftuooaftgs.com.  
DIRECTLYSHIPPED.COM.directl...  
conslogic.com.au.  
apoloogroup.com.au.  
woodpecker.au.  
Hww.6138388.cc.  
appollogroup.com.au.  
dashconcepts.com.au.  
clickng.com.au.  
sksjnlonol.biz.  
xn--80aj9g.com.  
cleveruraltraders.com.au.  
www.ermanence.com.br.  
www.Cgj.jhfy.WIn.jhfy.win.  
ingest.au.  
bualik.vlc.edu.au.  
WWW.Jyjtsw.cn.jyjtsw.cn.  
solarsnartaust.com.au.  
XN----itBBL6aCeFQq.Xn--P1Ai...  
egg.au.  
directmodels.com.au.  
tyreprotector.com.au.  
dehange.com.au.

RCODE: NOERROR

kendramaynard.com.  
jjmtd.com.  
xn--80aafxj1aahhddjl2n.xn--...  
www.debtfreeagain.co.uk.  
xn--b1aaocxjaaccldfxbuo8jb...  
www.body-space.co.uk.  
oft.cr.  
mri.net.au.  
xn--90a0MAH.xn--P1ai.xn--90...  
HDCam.mp.hdcam.mp.  
kompakt-bibelschule.de.  
xn--80acq4ak.xn--j1anh.  
gwellis.com.  
findyourfabulousthailand.com.  
fatgoaway.eu.  
www.fpcar.it.  
mail.carnendeaguirre.com.  
www.thesafest-content4video...  
cinnabar.com.au.  
xn--h1aakfa.xn--p1ai.  
wfxko4g1k9.download.  
www.private-cloud-solutions...  
knjdb.com.  
www-1jn-com.us.  
www.tatjiana.com.  
www.kfv331.loan.

## Working with Canadian organizations

Cybertip.ca

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

WWW.CIRA.CA

The screenshot shows the Cybertip.ca website. At the top, the logo 'cybertip!ca' is displayed with the tagline 'CANADA'S NATIONAL TIPLINE FOR REPORTING THE ONLINE SEXUAL EXPLOITATION OF CHILDREN'. To the right of the logo are buttons for 'DONATE' and 'EN FRANÇAIS'. Below the logo is a large banner with a photograph of a child's feet and hands on pavement, with a red button that says 'CLICK HERE TO REPORT'. A navigation menu includes links for 'ABOUT US', 'CHILD SEXUAL ABUSE', 'INTERNET SAFETY', 'PROJECTS', 'PARTNERS', and 'REPORTING'. The main content area features a 'Welcome to Cybertip.ca' heading and the text 'Canada's tipline to report the online sexual exploitation of children.' Below this is a large blue-tinted image of a child's face with a quote: '“You're not just clicking something, downloading it, and watching it. You are harming somebody. That child is hurting.” - SURVIVOR OF CHILD SEXUAL ABUSE MATERIAL'. A 'CLICK TO LEARN MORE' button is positioned below the quote. To the right of the main content is a sidebar with a search bar, a 'Supported By: Manitoba' logo, and three call-to-action boxes: 'Sign up to receive Cybertip.ca ALERTS!', 'Do you provide an Internet Service? REPORT HERE', and 'Concerned about a sexual (or nude) picture being shared online?'. At the bottom of the page, there is a row of small thumbnail images.

## 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.

The screenshot shows the Canadian Centre for Cyber Security website. At the top, there is a navigation bar with the text "Government of Canada" and "Gouvernement du Canada" on the left, and "Canada.ca | Services | Departments | Français" on the right. The main header features the "Canadian Centre for Cyber Security" logo and a search bar. Below the header, there is a navigation menu with options: "Information & Guidance", "Services", "Cyber Incidents", "Education & Training", and "Building the Community".

The main content area features a prominent "ALERT" banner with the title "Cyber threats to Canadian health organizations". The alert text states: "This Alert is intended for IT professionals and managers of notified organizations. Recipients of this information may redistribute it within their respective organizations." Below the alert is a "Read More" link.

Below the alert is a large banner titled "STAYING CYBER-HEALTHY DURING COVID-19". Below this banner is a sub-header: "The Canadian Centre for Cyber Security offers the following tips to help Canadians stay cyber-healthy during the COVID-19 pandemic." Below this is a carousel navigation with "Item 1 of 3" and a "Play" button.

At the bottom, there is a section titled "Cyber Centre Expertise" with four featured articles:

- An Introduction to the Cyber Threat Environment**
- Alerts & Advisories**: The Cyber Centre issues alerts and advisories on potential, imminent or
- How to Shop Online Safely (ITSAP.00.071)**: Ways you can keep yourself safe
- Cyber Security Tips for Remote Work (ITSAP.10.116)**

## DNS Privacy

# What does privacy mean

DNS data combined with IP address is private data

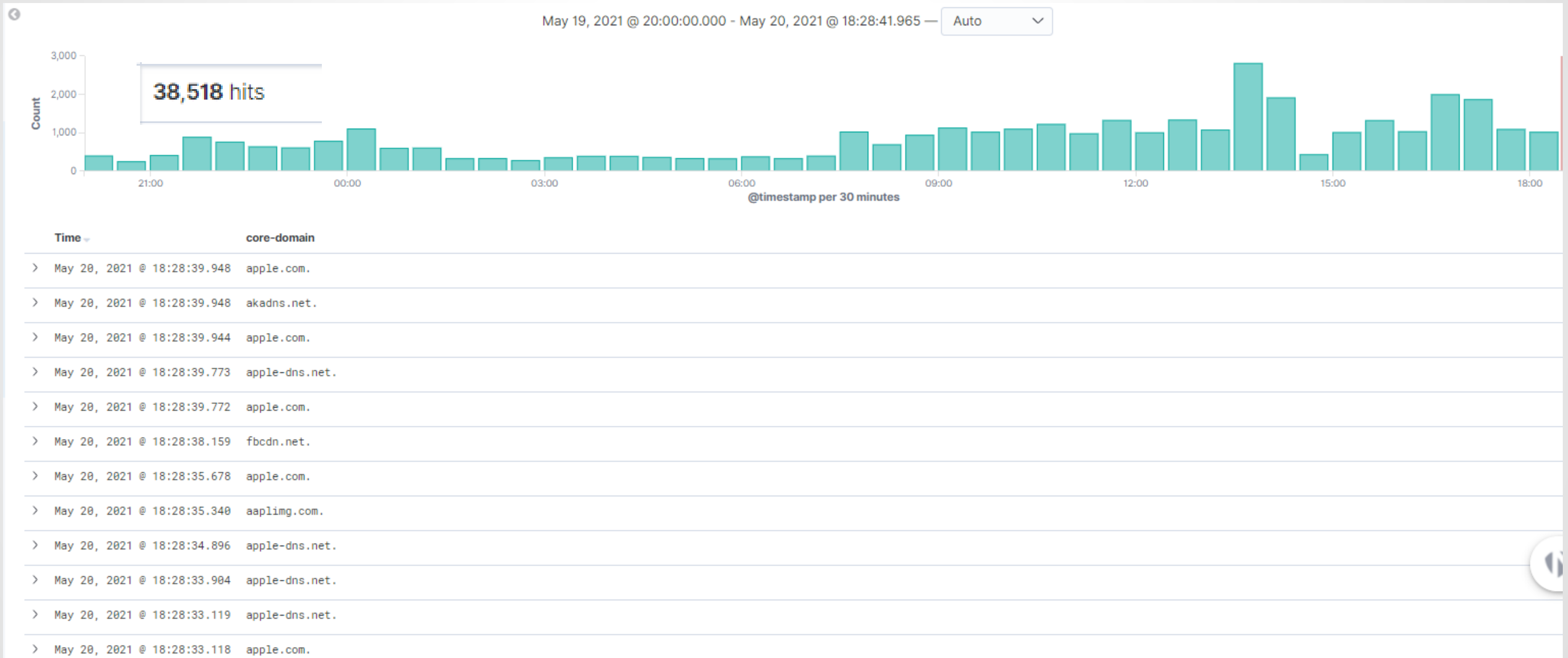
The DNS is a record of everything you do online.

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



## Normal Activity

# Typical Household – 38,000 DNS queries per day



## Data Privacy

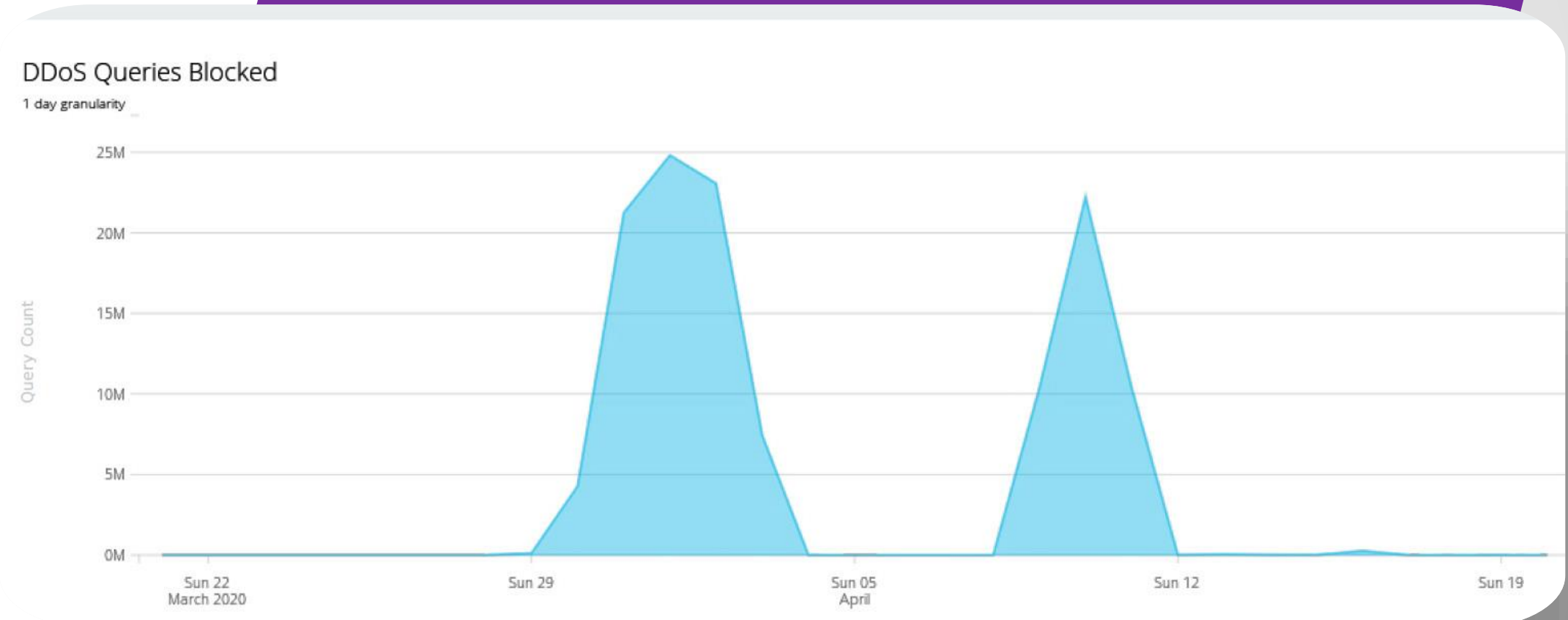
# Data Collection and Usage

- 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

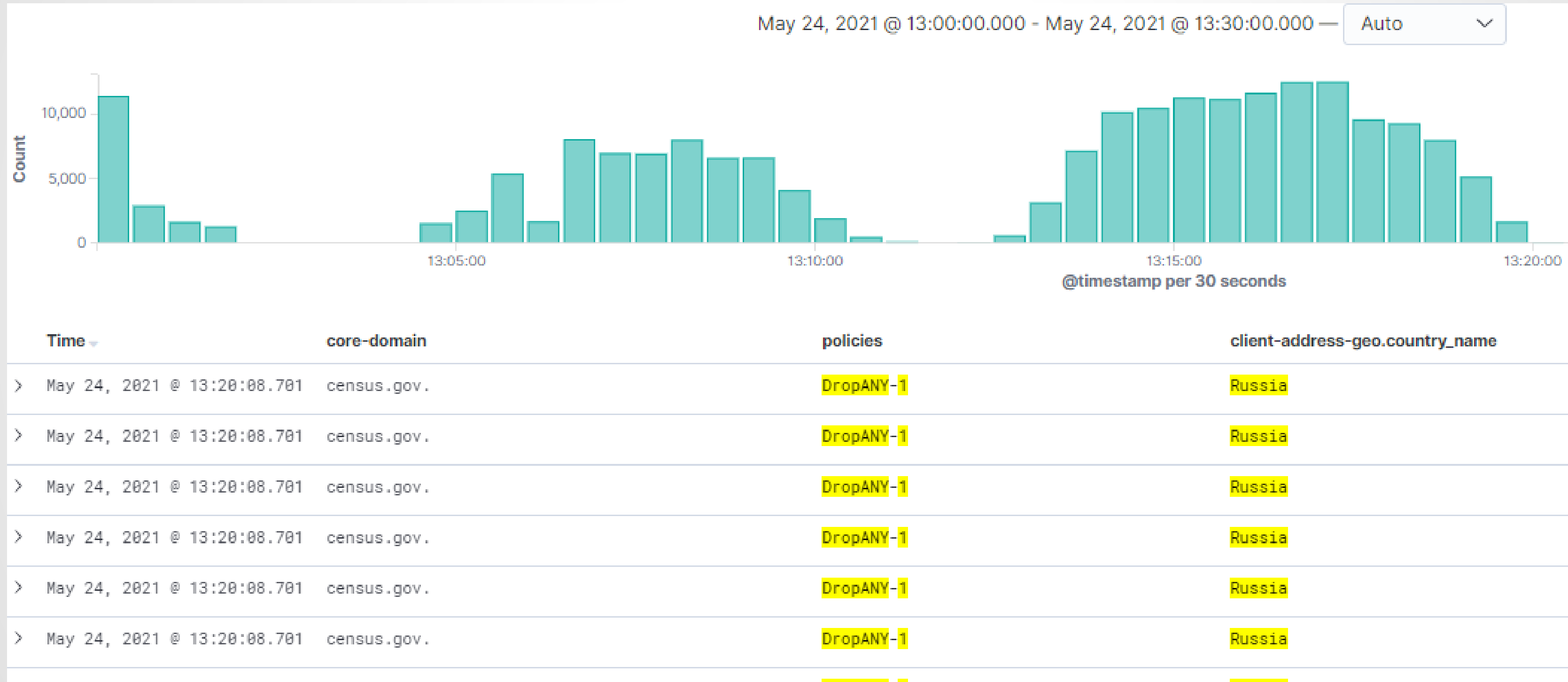
IP blocking

High Capacity

# Malicious Activity

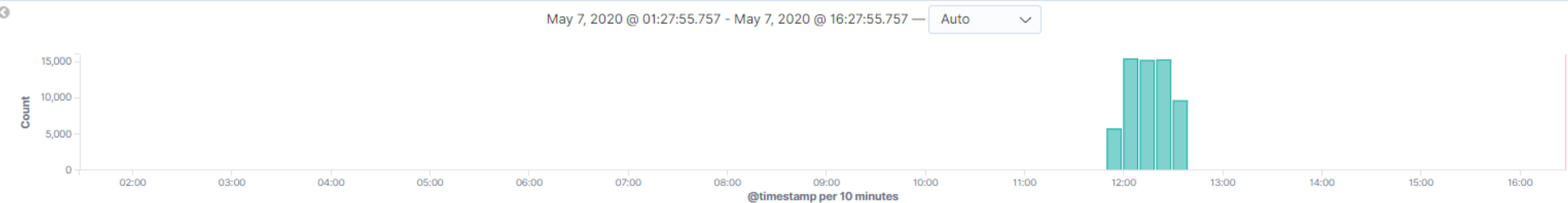
## Amplification – Any Attacks

WWW.CIRA.CA



## 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                  | zz157.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

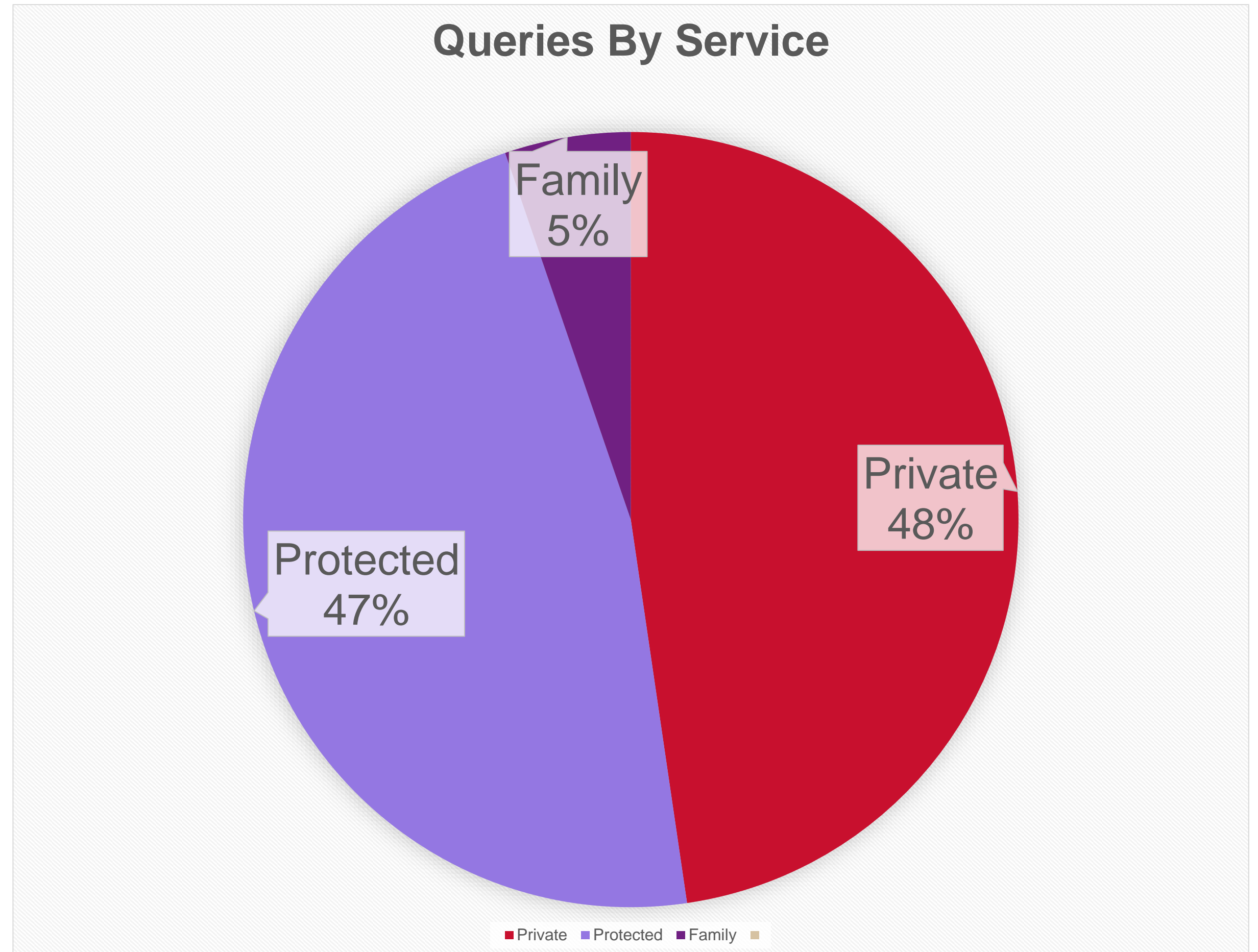
## Day In The Life ( DITL ) Results

# DITL Queries By Service Type

---

732,344,413 Queries

- 80.1% Canada
- 4.1% United States

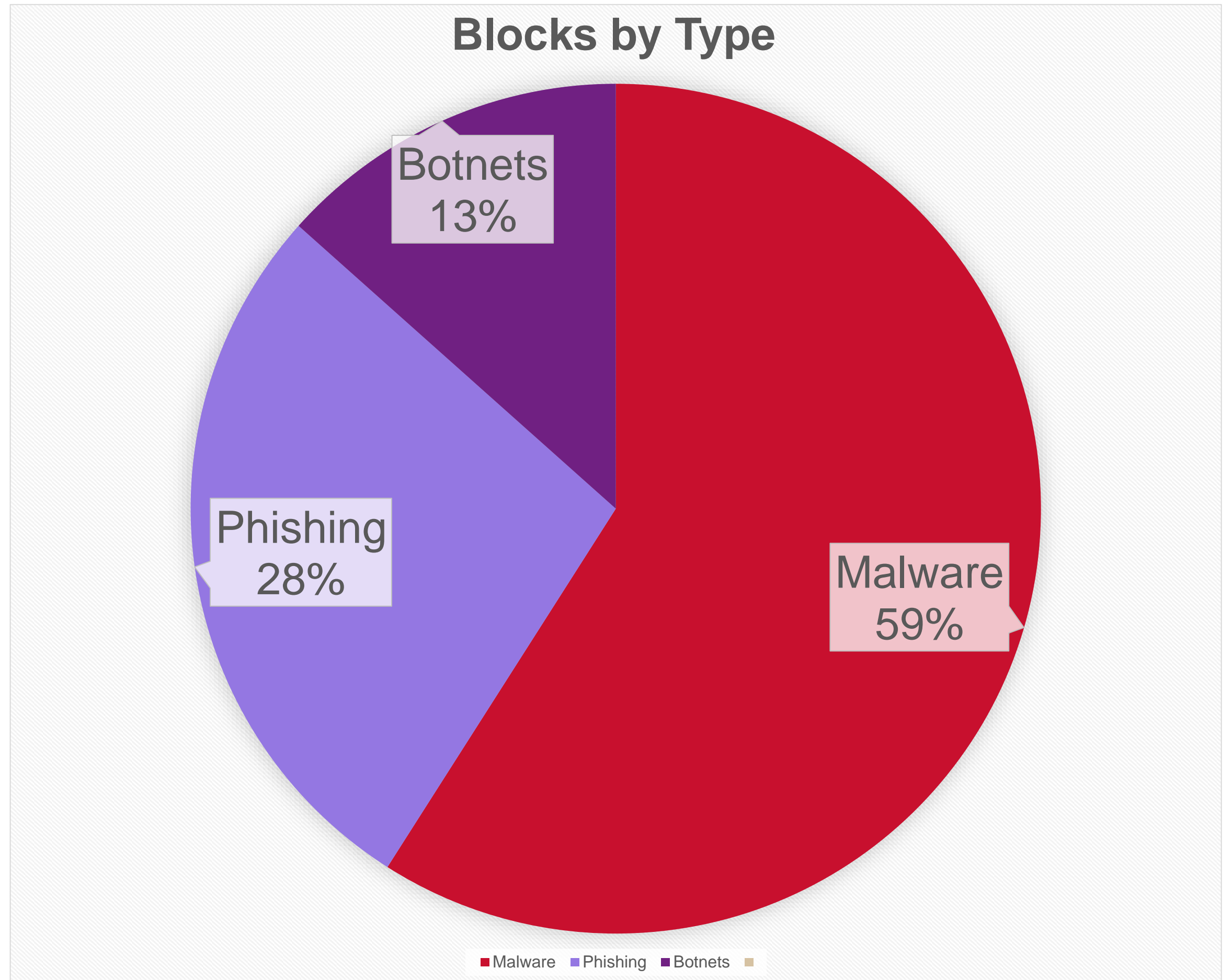




# DITL Blocks by Type

---

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



## Canadian Shield A Day in the Life

### Top Blocks

WWW.CIRA.CA

| 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 |
| klkjwt9fqwieluoi.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

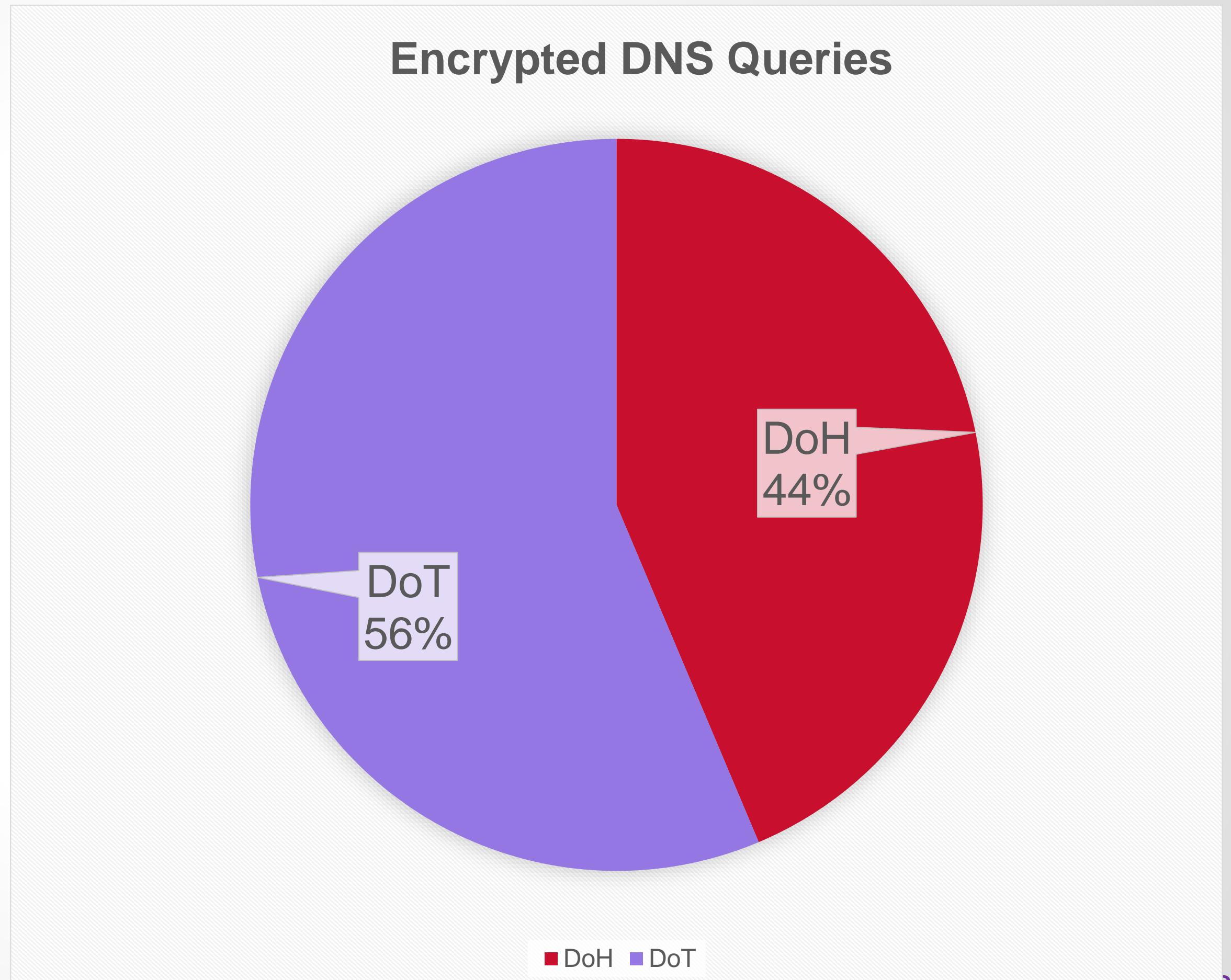
# Top Threats

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

# Encrypted DNS Queries

WWW.CIRA.CA

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



**Canadian Shield**

Ecosystem

---

Infrastructure

---

Threat Feeds

---

Research

---

Innovation

WWW.CIRA.CA

## Canadian Shield

# Summary

Protection

Benefit

Ecosystem

Resilient

Secure

Partnerships

# Questions?

Mark Gaudet,  
General Manager Cyber and DNS  
[mark.gaudet@cira.ca](mailto:mark.gaudet@cira.ca)