CIRA/ITWC WEBINAR

Preparing for the Big Hack in Healthcare

WEDNESDAY, MARCH 20, 2019

Today’s Program

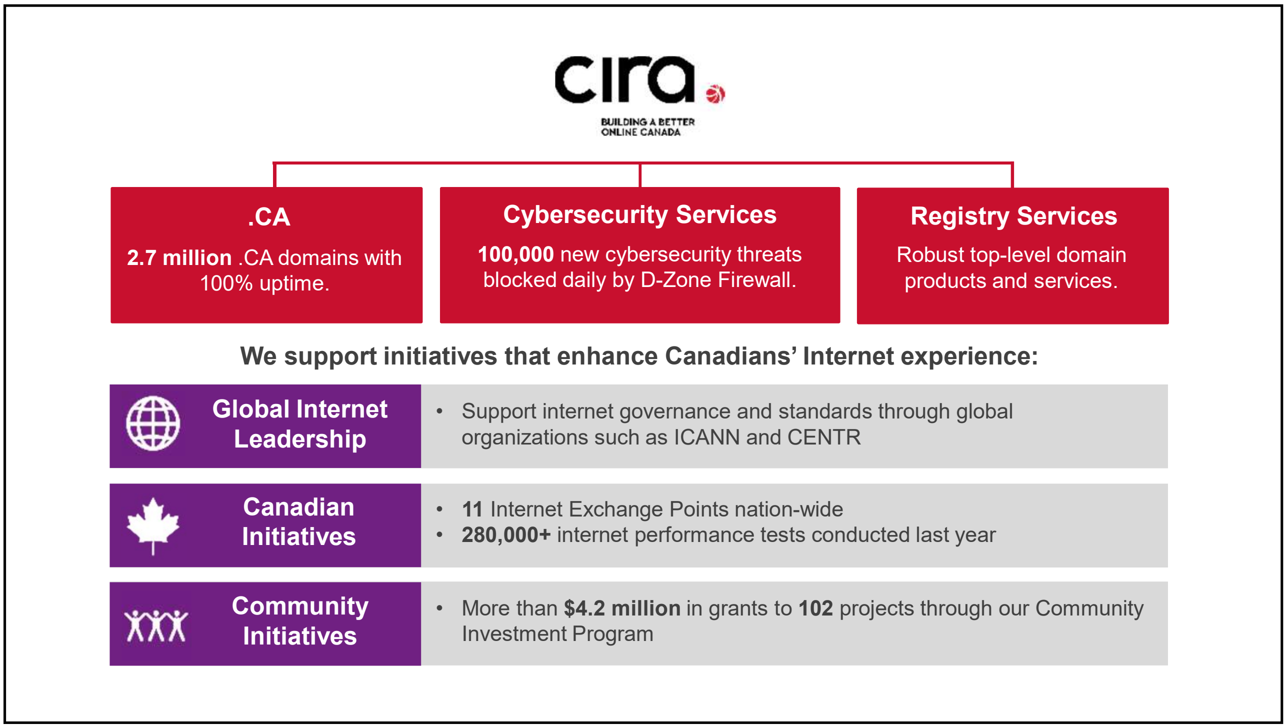
- Welcome, Introduction
- Presentation
- Q&A
- Evaluation

Poll Question

Defending Health Care with DNS

cira

BUILDING A BETTER
ONLINE CANADA



cira
BUILDING A BETTER ONLINE CANADA

.CA

2.7 million .CA domains with 100% uptime.

Cybersecurity Services

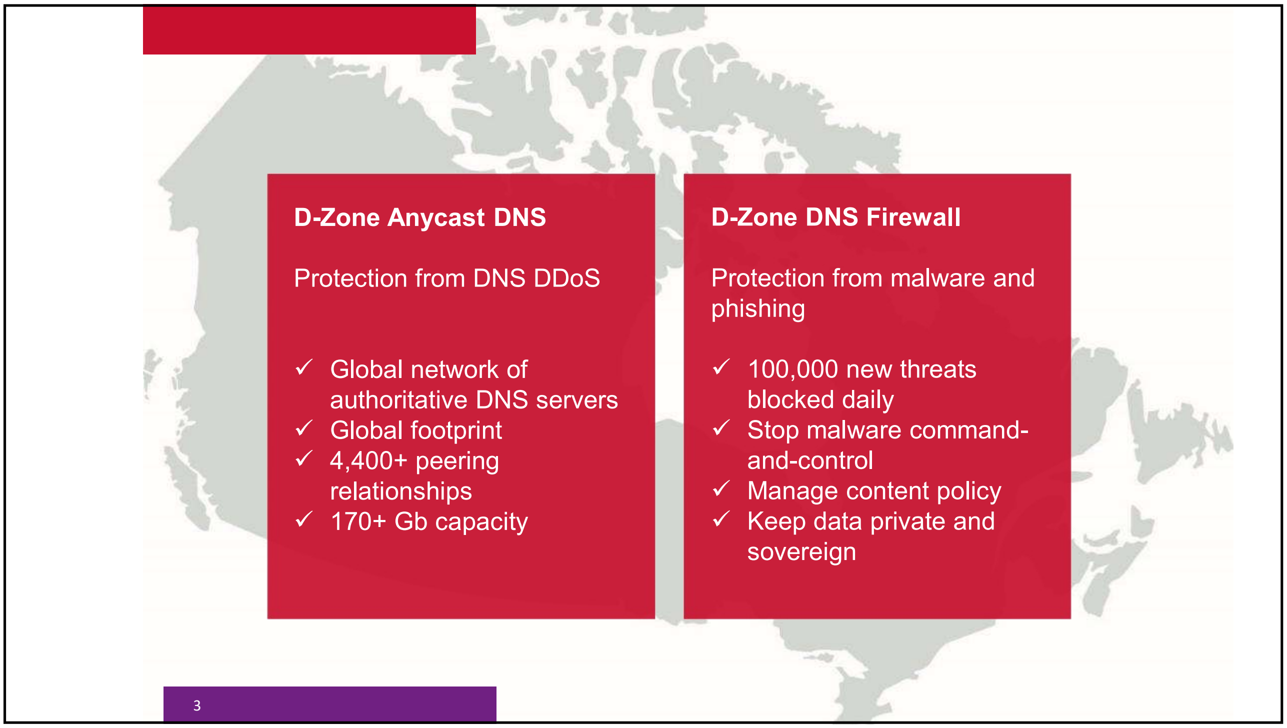
100,000 new cybersecurity threats blocked daily by D-Zone Firewall.

Registry Services

Robust top-level domain products and services.

We support initiatives that enhance Canadians' Internet experience:

Global Internet Leadership	• Support internet governance and standards through global organizations such as ICANN and CENTR
Canadian Initiatives	• **11** Internet Exchange Points nation-wide • **280,000+** internet performance tests conducted last year
Community Initiatives	• More than **$4.2 million** in grants to **102** projects through our Community Investment Program



D-Zone Anycast DNS

Protection from DNS DDoS

- ✓ Global network of authoritative DNS servers
- ✓ Global footprint
- ✓ 4,400+ peering relationships
- ✓ 170+ Gb capacity

D-Zone DNS Firewall

Protection from malware and phishing

- ✓ 100,000 new threats blocked daily
- ✓ Stop malware command-and-control
- ✓ Manage content policy
- ✓ Keep data private and sovereign

3

HEALTHCARE IS A TARGET

Hospitals a 'magnet' for cyberattacks: health care expert

How Ransomware and Data Theft will Change the Face of Dentistry

Computer virus causes delays at dozens of Northern Ontario hospitals

Oshawa hospital among thousands of global 'ransomware' cyberattack victims

'Doctors are under attack': Group says medical offices are regularly hit by ransomware

In the best-case scenario after the incidents, medical offices spend two or three days restoring their systems from backup sites

CBC INVESTIGATES

Thousands of patient records held for ransom in Ontario home care data breach, attackers claim

7

PATIENT DATA IS A HIGH VALUE ASSET

- **Move to electronic health records**
- **Healthcare data** – from patient records and clinician information
  - Identity theft
  - Insurance Fraud
  - Personal information
- **Patient records are critical infrastructure**
  - Encrypt patient records for ransomware
- **High resale value**
  - Ranges from $1 (in bulk) to $1,000 for individual

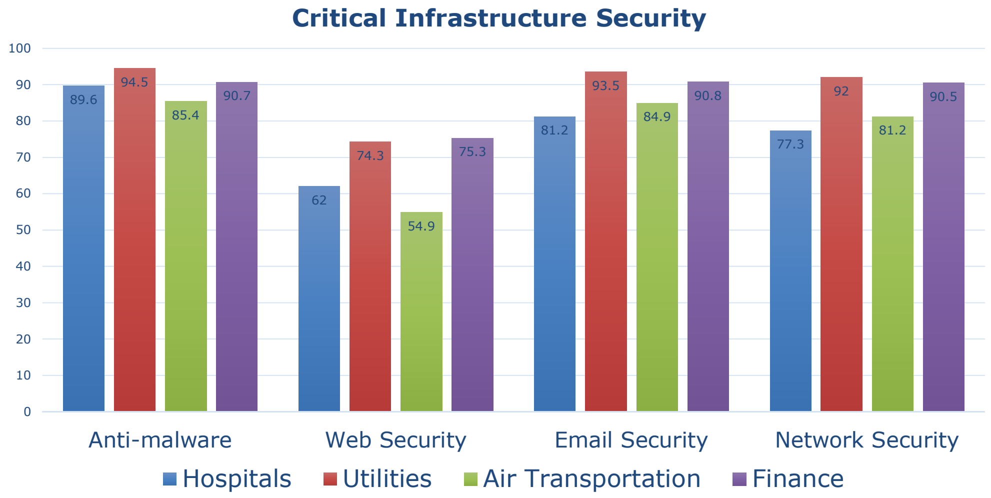
8

HIGH COST OF DATA BREACHES IN CANADA

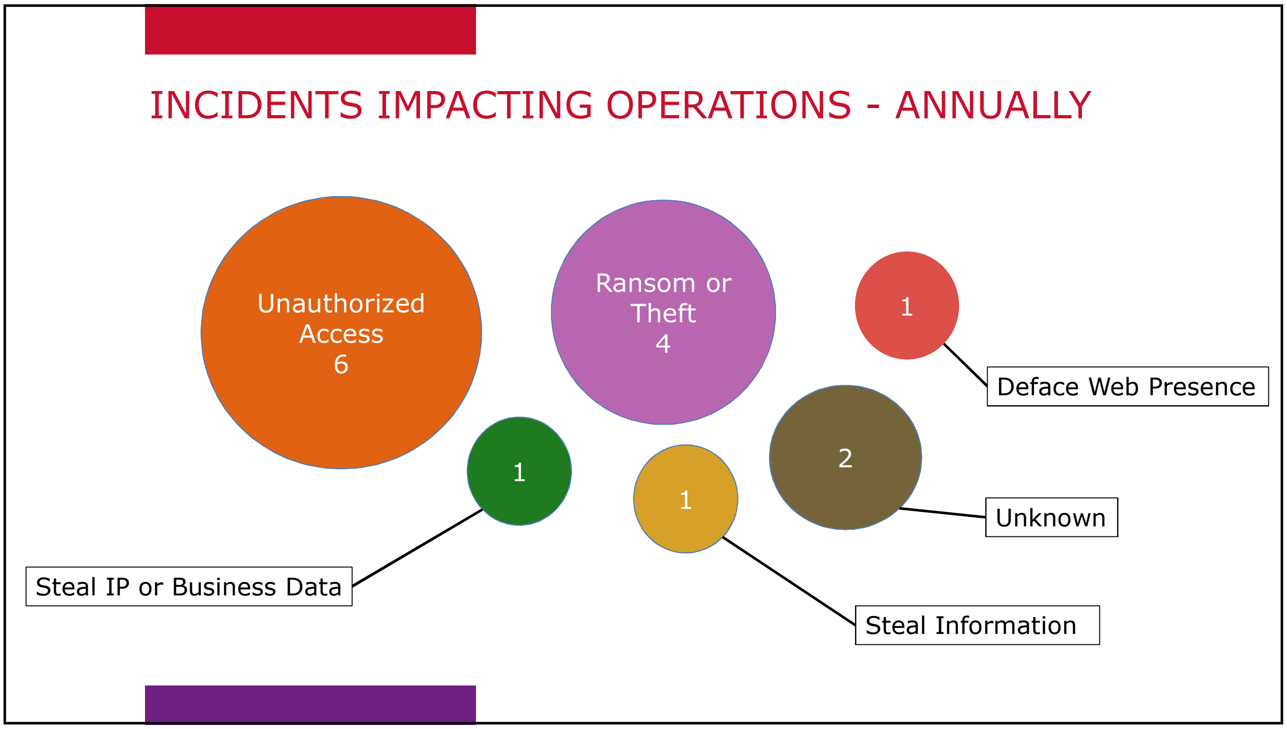
- Highest **direct costs** at **$81 per record**
  - – engaging forensic experts,
  - – specialist law firm assistance,
  - – purchase of identity protection services.
- Second highest **indirect costs** at **$116 per record**
  - – employees' cost and effort to notify victims
  - – employee cost to investigate the breach,

The 2018 Cost of Data Breach Study: A Global Overview was released by Ponemon Institute, LLC.

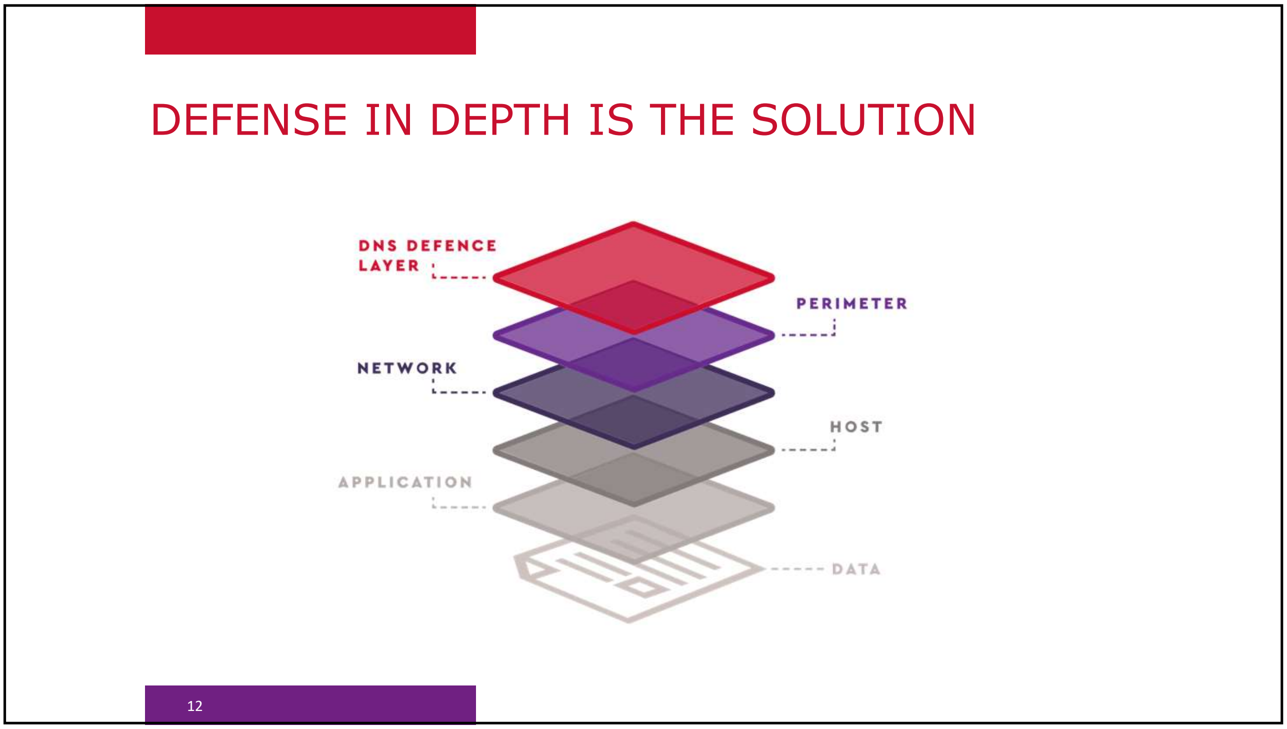
HOW HOSPITALS COMPARE



https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210000101



INCIDENTS IMPACTING OPERATIONS - ANNUALLY

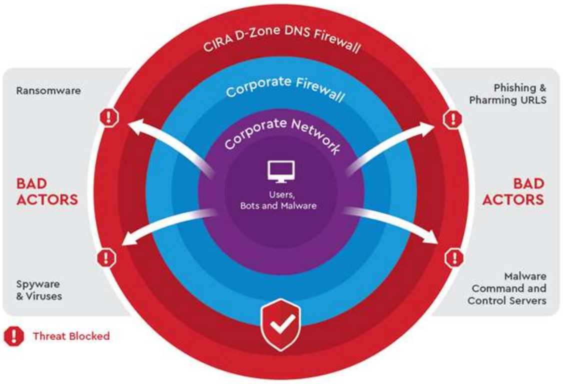


DEFENSE IN DEPTH IS THE SOLUTION

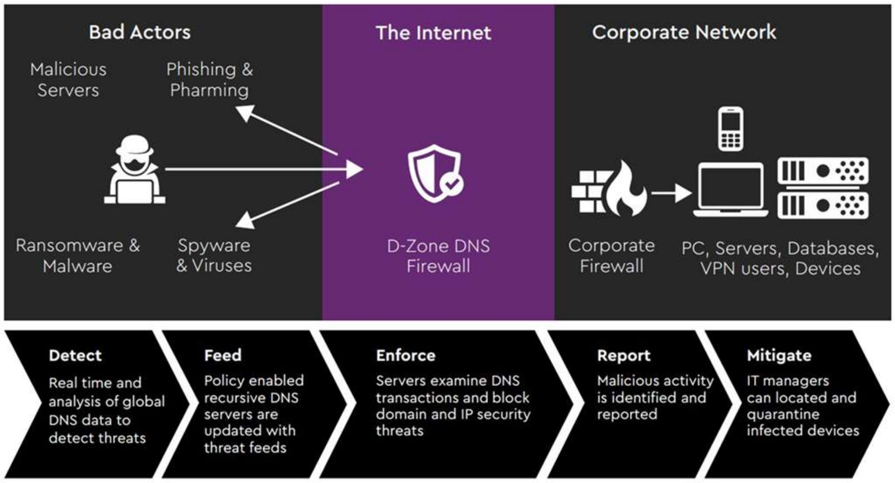
12

DNS AS A LAYER OF DEFENCE & INTELLIGENCE

- DNS can both keep malware off the network and block its command and control function
- DNS is part of a multi-layer defence in depth approach
  - 91.3% of malware uses DNS
  - DNS is used for command and control
  - IoT
  - BYOD



DNS FIREWALL AS LAYER OF DEFENSE



Detect Real time and analysis of global DNS data to detect threats

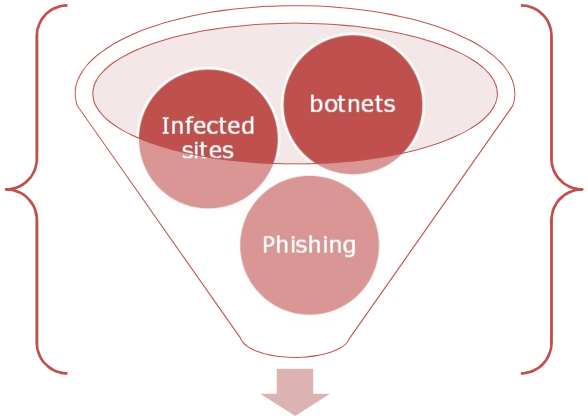
Feed Policy enabled recursive DNS servers are updated with threat feeds

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

GLOBAL DNS DATA FOR THREAT INTELLIGENCE



Infected sites

botnets

Phishing

Commercial & Public
Threat Data

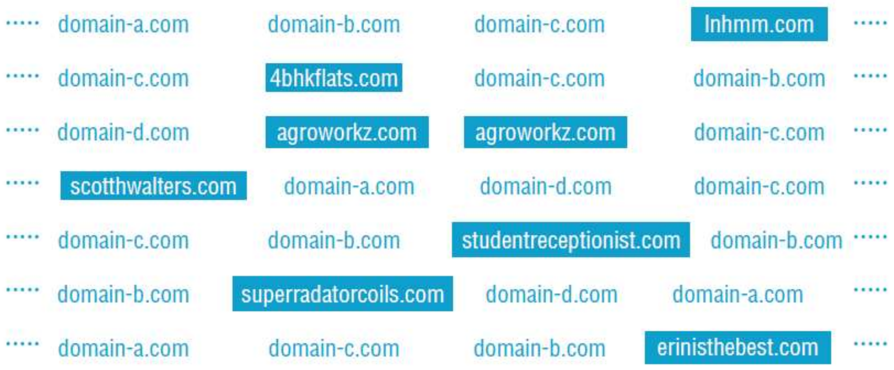
Data Science
Anomaly Detection
& Machine Learning

D-Zone DNS Firewall
Real-Time Threat Feed

AKAMAI DATA SCIENCE

- **Machine learning on new domains**
  - Unsupervised learning is applied to the mega groups of resolved and unresolved domains
  - Clusters of associated domains are identified
- **Known threats** – if any cluster member is on known threat lists this elevates the whole cluster
- **Unknown** – cluster members do not match known threats but the characteristics indicate maliciousness
- 4 to 5% of new core domains are blocked

ZERO DAY QUARANTINE



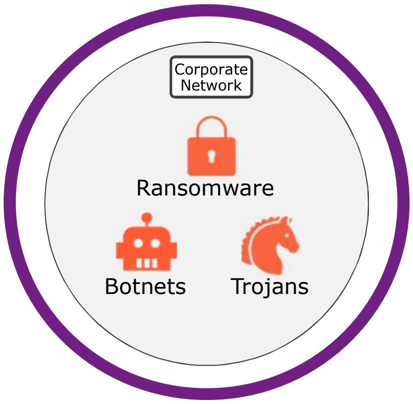
·····	domain-a.com	domain-b.com	domain-c.com	**lnhmm.com**	·····
·····	domain-c.com	**4bhkflats.com**	domain-c.com	domain-b.com	·····
·····	domain-d.com	**agroworkz.com**	**agroworkz.com**	domain-c.com	·····
·····	**scotthwalters.com**	domain-a.com	domain-d.com	domain-c.com	·····
·····	domain-c.com	domain-b.com	**studentreceptionist.com**	domain-b.com	·····
·····	domain-b.com	**superradatorcoils.com**	domain-d.com	domain-a.com	·····
·····	domain-a.com	domain-c.com	domain-b.com	**erinisthebest.com**	·····

17

DISABLING THREATS ALREADY INSIDE

- D-Zone DNS Firewall shows malware and botnets inside the network
- D-Zone picks the malware as it tries to call home to the host server
- Botnets that get inside the network are disabled

D-Zone DNS Firewall



15

PREDICTIVE BLOCKING

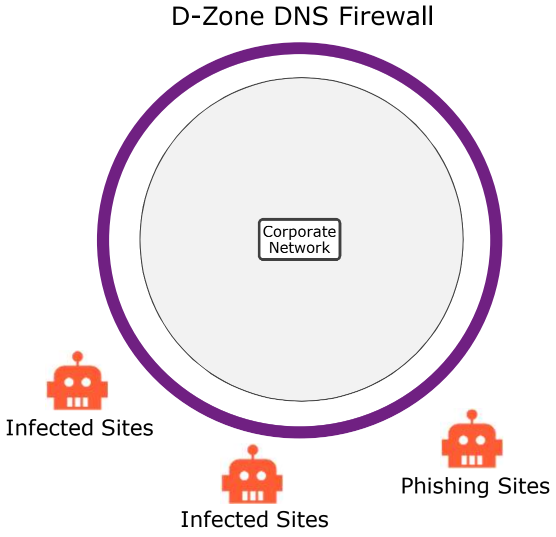
Algorithmically generated domain names

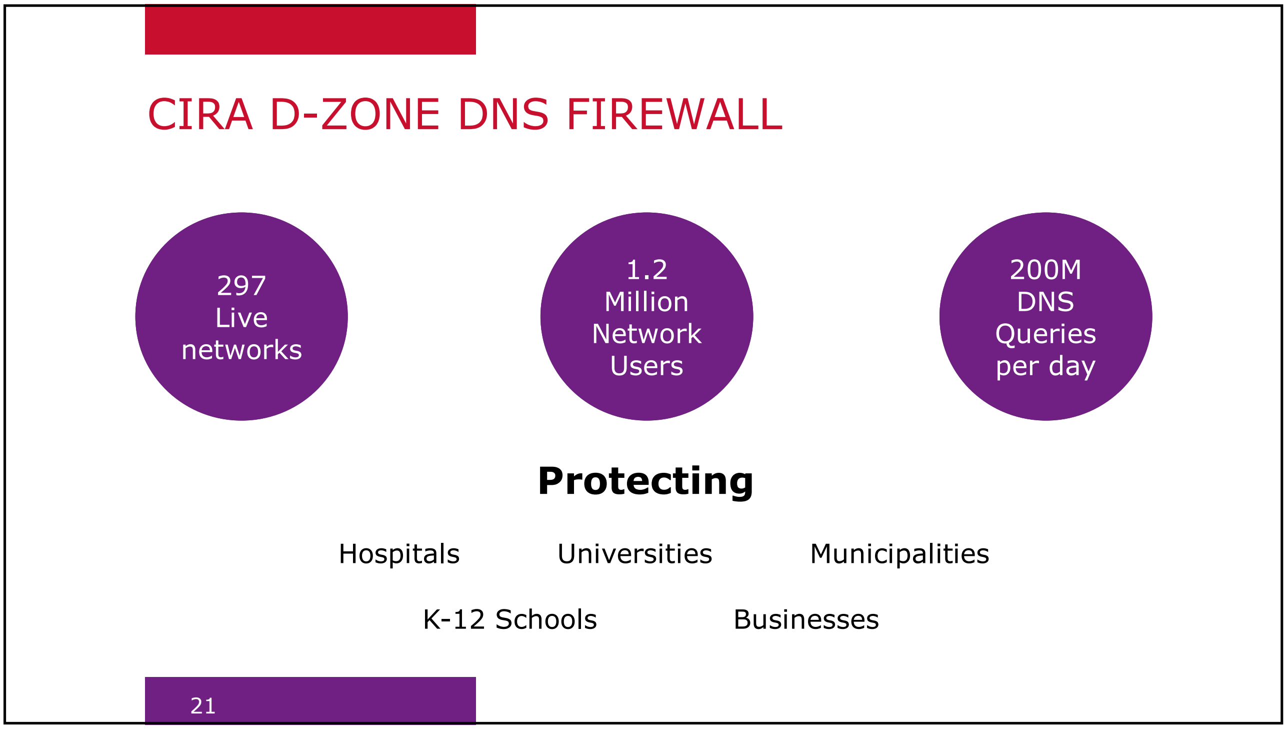
Botnet	Trojan	Fraud	Ransomware	Worm	PUA
Necurs	Sphinx	Tofsee	Locky*	Proslikefan	Chinad
NewGOZ	Sinowal**	Bamital*	Dorifel		
Virut**	Bedep**		Reveton		
	Dyre		Cryptowall		
	Suppobox		Cryptolocker		

We know how they are generated

PREVENTING THREATS FROM GETTING INSIDE

- D-Zone DNS Firewall prevents access to infected sites and phishing domains
- D-Zone blocks access at the DNS level
- Reduces load and alerts from firewalls
- Typically legitimate websites that have been compromised





CIRA D-ZONE DNS FIREWALL

297 Live networks

1.2 Million Network Users

200M DNS Queries per day

Protecting

Hospitals Universities Municipalities

K-12 Schools Businesses

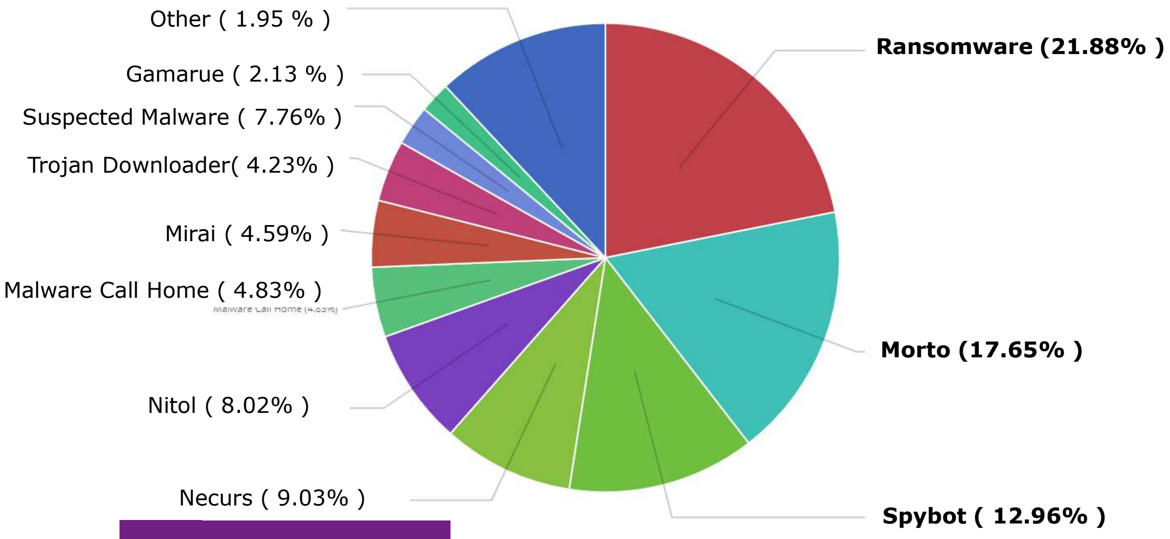
21

Poll Question

24 HOURS OF THREATS IN CANADA

32,087	3,926	6,515
Malware	Phishing	Botnets

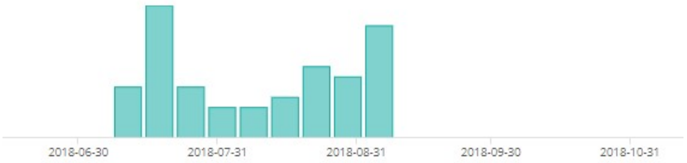
BOTNET LANDSCAPE IN CANADA



HOSPITAL THREAT DATA

MIRAI

- Major hospital implemented DNS Firewall
  - Discovered C&C for Mirai botnet
- Able to mitigate and remove
- Medical and IoT devices targets of Mirai
- Prevented further infections at DNS level



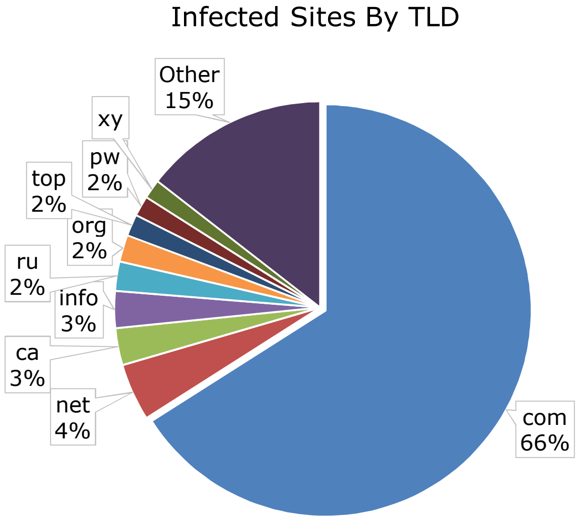
DNSespionage

'Unprecedented' DNS Hijacking Attacks Linked to Iran

- This threat was blocked in Canadian Hospital
- Targets – Libya, UAE
- Malware distribution domains
  - hr-wipro.com
  - hr-suncor.com
- Domain high jacking

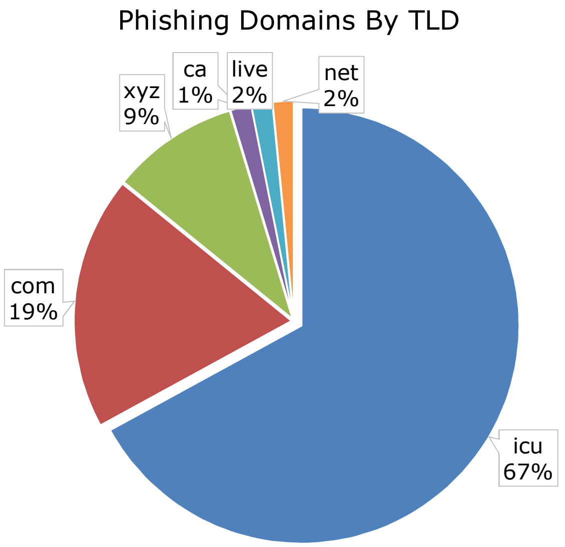
TOP INFECTED SITES

Domain Name	Count
sadfashdf8oasdfhasdf.site	573
img1.cfcdn.club	304
t1.contentgreat.com	251
cdn-102.statdynamic.com	181
cdn-104.statdynamic.com	154
cdn-101.statdynamic.com	144
cdn-103.statdynamic.com	127
im.gwsanguo.com	55
restat.info	35
mediaply.net	24
t1.contentnice.com	24
chabadavenue.com	23
home.h5play.top	21



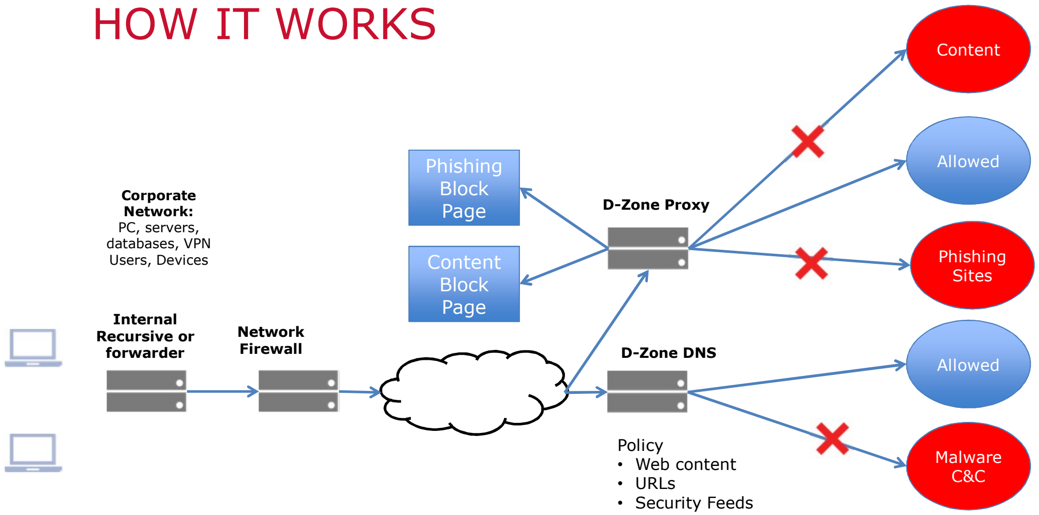
TOP PHISHING DOMAINS

Phishing Domain	Count
m.zr9f7.cn	226
ai51q.cn	148
visit.net-cb15.stream	19
www.geniustrainer.net	16
clk.rtpdn10.com	15
ticketswestjet.com	15
www.ilovekickboxing.com	8
mediaasktype-theclicks.icu	6
originallyknown.com	6
extremepita.com	5
shoppingemail.info	3
wamb.wei21234.cn	3
coots.ml	2
strandgossamer.xyz	2



29

HOW IT WORKS



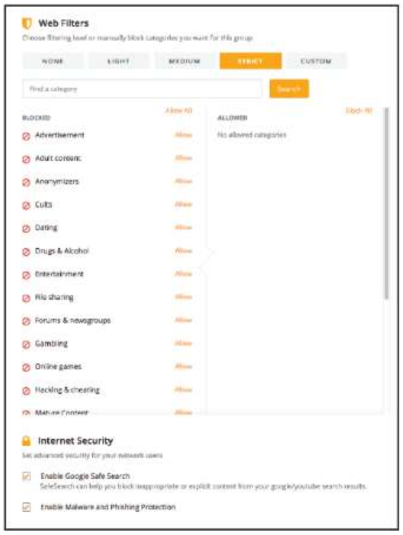
Policy
- Web content
- URLs
- Security Feeds
- Auto detected

Reporting
- Activity
- Blocked Content
- Malware

30

CONTENT FILTERING

- Set global content policies based on common categories like, gambling, dating, social pornography, cults, etc.
- Block and unblock individual domains at admin level



Web Filters

Choose filtering level or manually block categories you want for this group

BLOCKED	Allow All	ALLOWED	Block All
Advertisement	Allow	No allowed categories	
Adult content	Allow		
Anonymizers	Allow		
Cults	Allow		
Dating	Allow		
Drugs & Alcohol	Allow		
Entertainment	Allow		
File sharing	Allow		
Forums & newsgroups	Allow		
Gambling	Allow		
Online games	Allow		
Hacking & cheating	Allow		
Mature Content	Allow		

Internet Security

Set advanced security for your network users

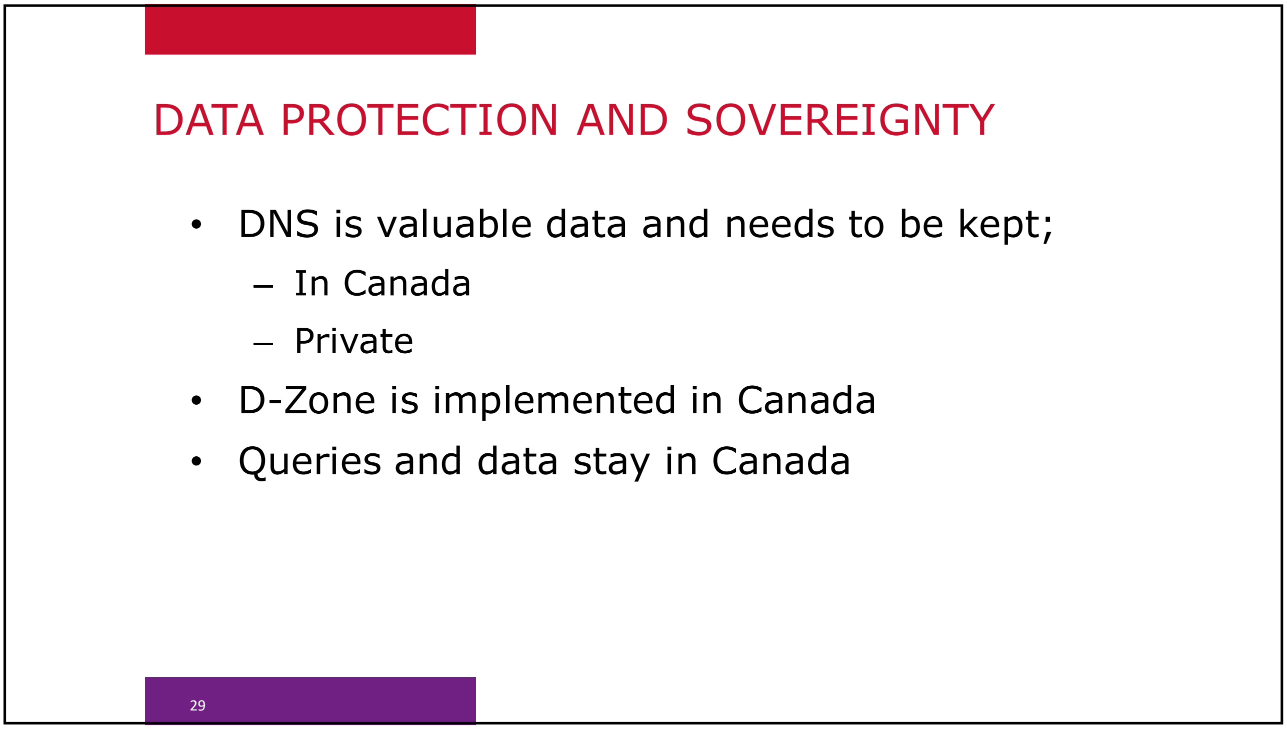
☑ Enable Google Safe Search
SafeSearch can help you block inappropriate or explicit content from your google/youtube search results.

☑ Enable Malware and Phishing Protection

FALSE POSITIVES?

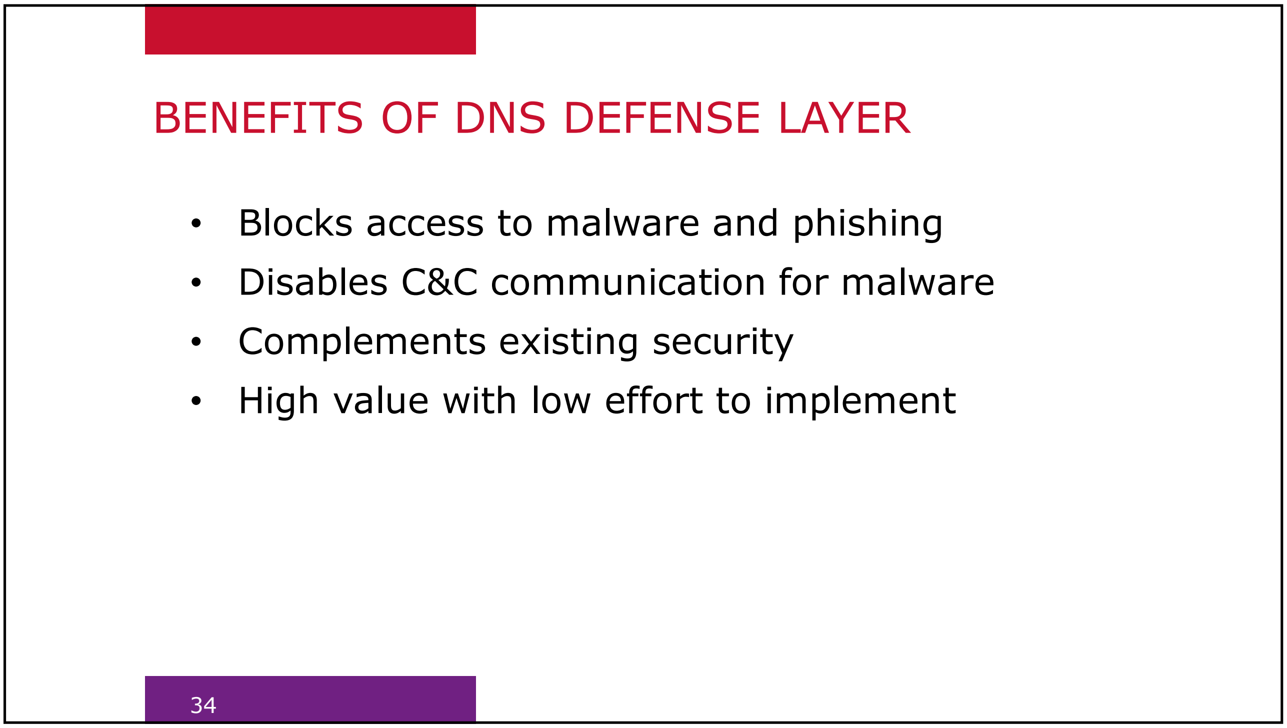
We have found multiple instances where cloud services or websites offering services were unaware of being hacked to distribute malware

- 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 PROTECTION AND SOVEREIGNTY

- DNS is valuable data and needs to be kept;
  - In Canada
  - Private
- D-Zone is implemented in Canada
- Queries and data stay in Canada



BENEFITS OF DNS DEFENSE LAYER

- Blocks access to malware and phishing
- Disables C&C communication for malware
- Complements existing security
- High value with low effort to implement

CONCLUSION

- Healthcare is a target
- Ransomware and malware are still a major issue
- Defense in depth with multiple layers is gaining momentum
- DNS is gaining momentum as critical layer of defense layer

THANK YOU

Mark Gaudet
CIRA Cybersecurity Services
Mark.Gaudet@cira.ca
613.799.5789

To start your free trial of D-Zone DNS Firewall visit cira.ca/trial.

ITWC
The Content Experts

Q&A

ITWC
The Content Experts

Thank You

Jim Love, ITWC
jlove@itwc.ca