Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

TLS Trends:
A roundtable discussion on current usage and future directions

Communications Security Establishment Canada (CSEC)

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

1

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

This presentation is up to

TOP SECRET//SI
//REL TO
CAN, AUS, GBR, NZL, USA

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Outline

- Background

- Implementation

- Trend Report

- Success Stories

- Future Development

- Questions

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA   3

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Background

- Objectives:

    - Identify capabilities in existing warranted SSL/TLS traffic

    - Generate regular trend reports and analysis

    - Identify abnormalities and technology changes
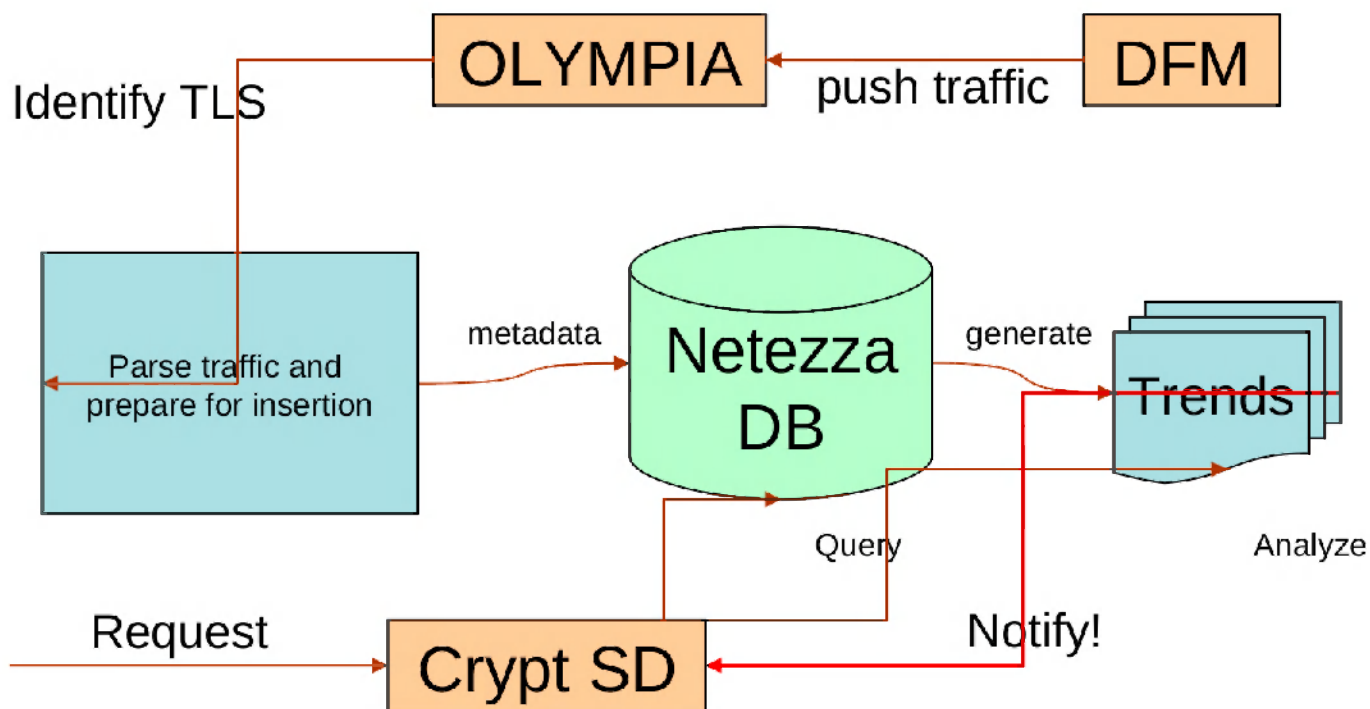
    - **Be proactive!**

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA   4

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Implementation – Warranted Collection

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

5

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada
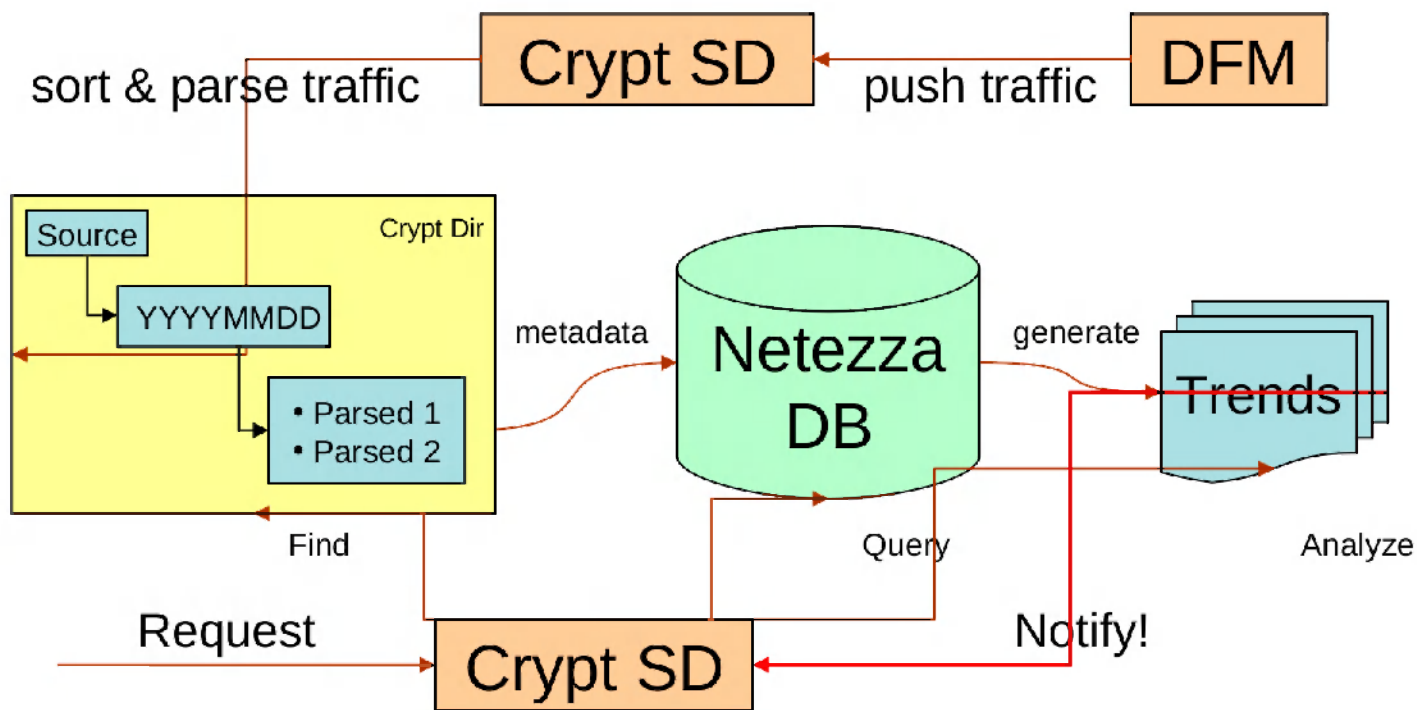
Implementation – Special Source

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

6

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Trend Report – Warranted Collection

- Inspired by GCHQ weekly TLS Trend Reports

- What we're tracking:
  - Amount of SSL/TLS traffic seen
  - Cipher Suite Breakdown (RSA vs EC vs DH)
  - SSL/TLS Version Breakdown
  - Top Certificates seen by Common Name
  - Top RSA Certificate Moduli seen
  - Top DH Moduli seen
  - Percentage of Resumed Session
  - Session Ticket Usage, Elliptic Curve Usage
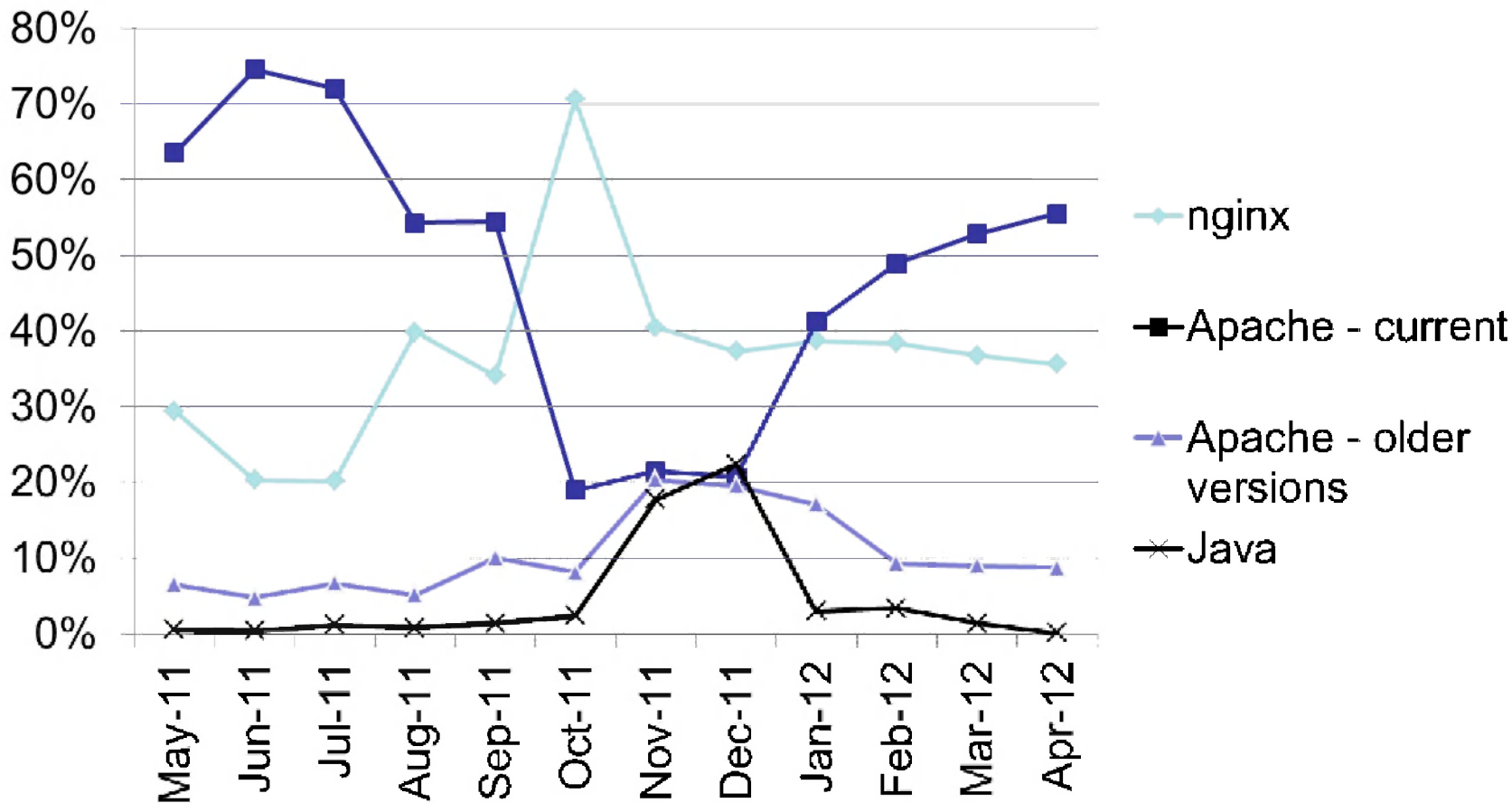 - RSA & DH Modulus Size Breakdown
  - New DH moduli
  - Top new RSA moduli

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

7

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

RSA Key Size Trends
(warranted only)
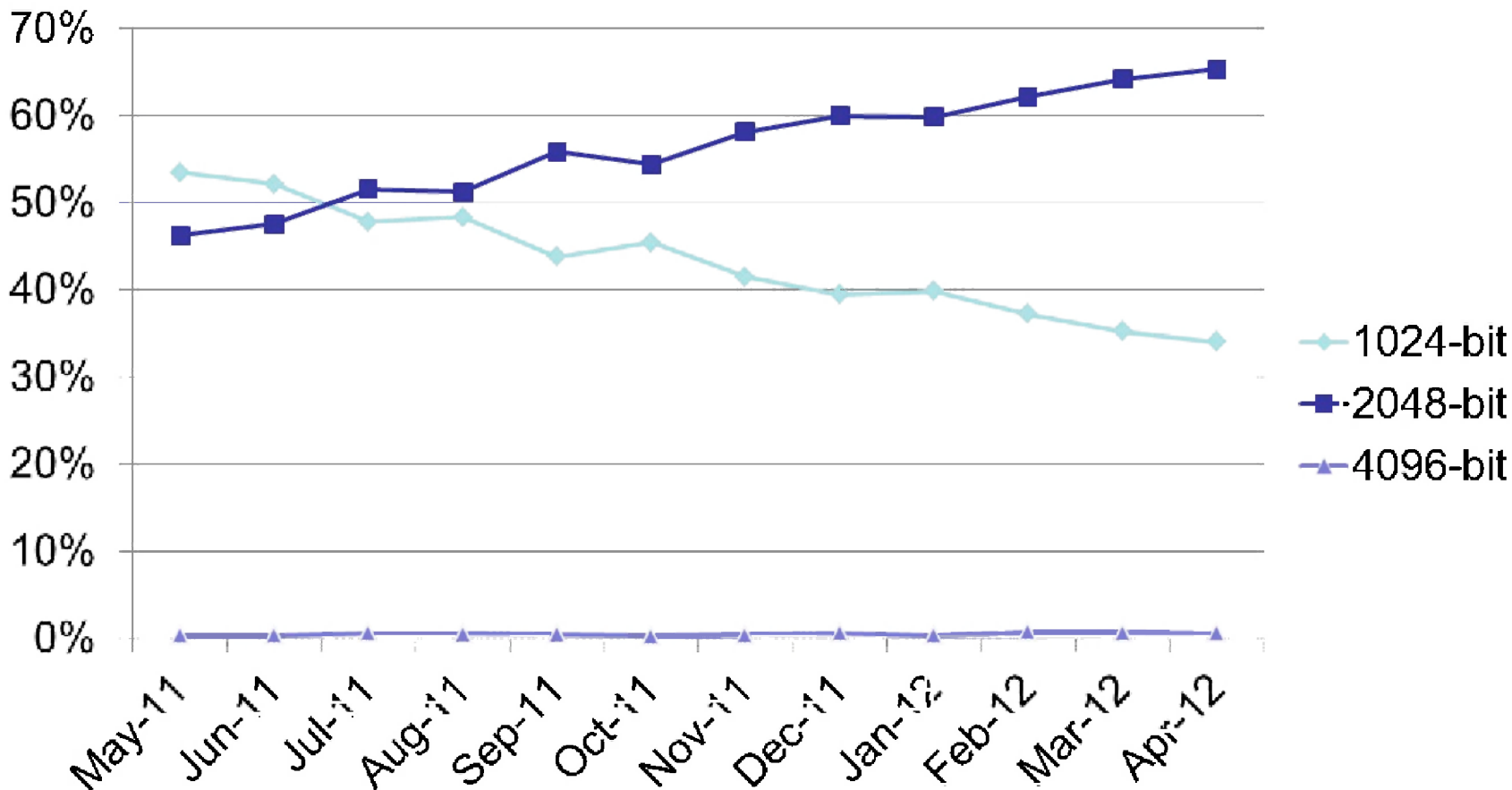
Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

8

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

DH Modulus Trends
(warranted only)

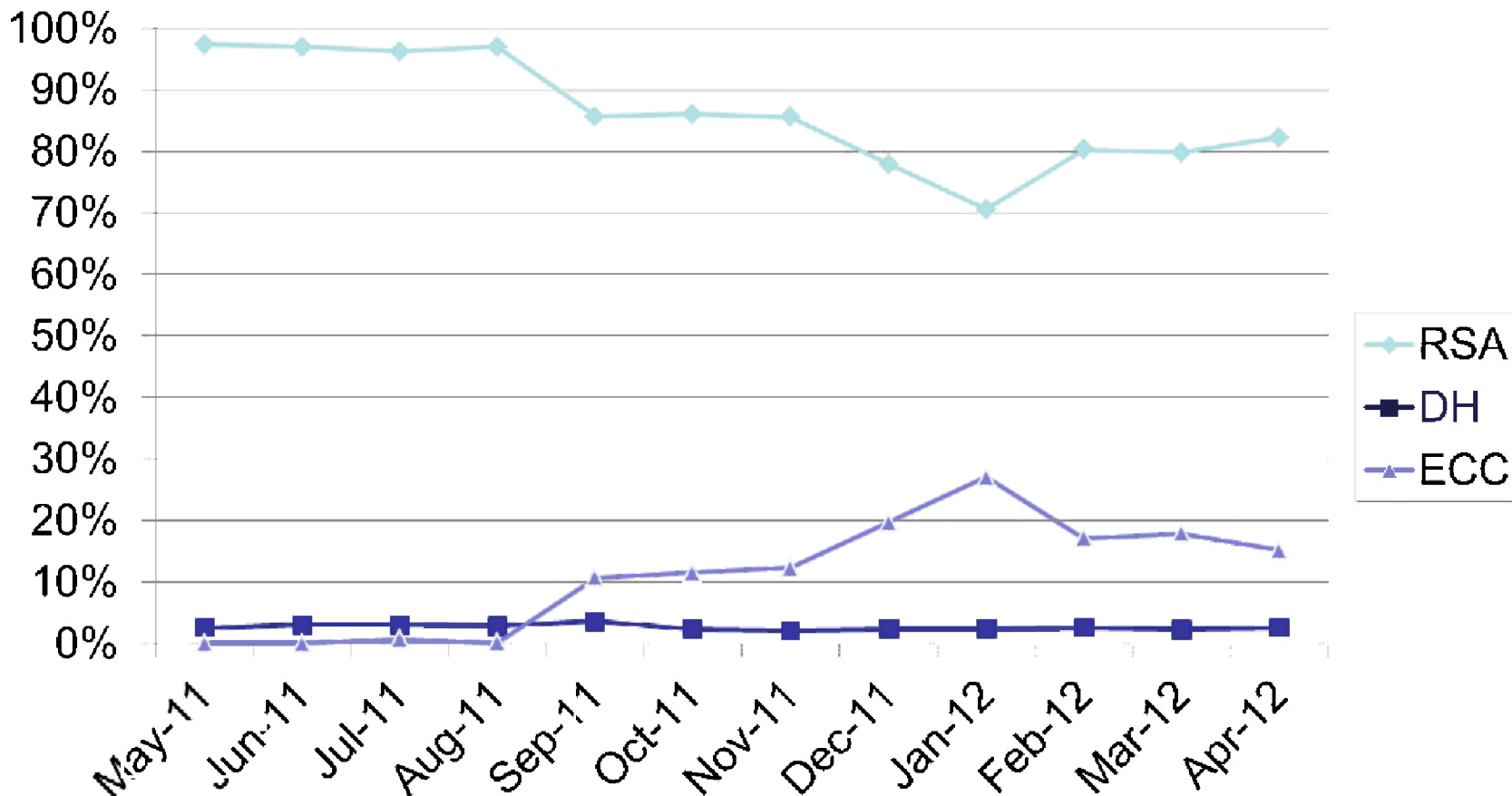*Safeguarding Canada's security through information superiority*
Préserver la sécurité du Canada par la supériorité de l'information

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA   9

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Public Key Exchange Methods
(warranted only)

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

10

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Target Specific reporting (warranted only)

- Intended to engage analysts in identifying traffic of interest
  - Show the known services their target is using
  - Ask them to help identify unknown services
  - Identify changes in their target's use of TLS

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

11

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Sample Report

Trends Report for Canuckistan in the month of April

Table 1. Types of TLS traffic in working hours (7am to 6pm) and out of hours

```
         WHO           | OUT_HOURS | IN_HOURS | TOTAL
-----------------------+-----------+----------+------
Google                 |      1479 |     2782 |  4261
Hotmail/Live           |       455 |      934 |  1389
Advertising            |       401 |      139 |   540
Foreign government sites |     338 |       97 |   435
Canuckistan Social Media |      59 |       90 |   149
Facebook               |        38 |       82 |   120
Apple                  |        12 |        2 |    14
Banking                |         5 |        4 |     9
Transportation sites   |         3 |        0 |     3
Microsoft              |         1 |        0 |     1
```

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canadä

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Sample Report (cont'd)

Table 2. Sites visited from the Canuckistan Social Media group

```
    WHO     |         SITES         | OUT_HOURS | IN_HOURS | TOTAL
------------+-----------------------+-----------+----------+------
hockeytalk  | login.hockeytalk.com  |         3 |       10 |   13
hockeytalk  | chat.hockeytalk.com   |        31 |       44 |   75
hockeytalk  | mail.hockeytalk.com   |        25 |       36 |   61
```

Comments:

We have noticed a large increase in chat activity on the hockeytalk sites. This is
likely due to the beginning of playoff season.

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Success Stories

- Easily identified current capabilities in warranted traffic

- Verified certificate being phased out and identified possible replacements

- Corroborated with GCHQ on discovering frequent Google moduli changes

- Currently pushing new moduli for testing against publicly known weaknesses (PHOENIX)

- Identified use of Elliptic Curve Certificates

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada

Future Development

- Trends reports on Special Source collection

- New types of metadata added to database

- Collaboration with CSEC's Data Mining team

- Improve efficiency, stability of solutions

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

TOP SECRET//SI//REL TO CAN, AUS, GBR, NZL, USA

15