DNS as a National Defense Layer

Presented by: Mark Gaudet

ICANN61 – TechDay
DNS as National Defense Layer

Agenda

• DNS as part of a defense in depth strategy
• CIRA DNS Firewall
• What we learned
• Vision for the service
Cybersecurity Challenge in Canada

Extensive use of antivirus software and firewalls
- 90% use firewalls
- 85% use antivirus software

Ransomware and phishing attacks still getting through
- 19% were victims of a ransomware attack
- 32% fell victim to a phishing attack and divulged information to hackers

Results from the 2018 CIRA Canadian Internet Security Survey
Defense in Depth with DNS

- DNS is the fabric of the internet
- 91% of malware uses DNS for command and control
- No additional hardware or software
- Covers all devices
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 locate and quarantine infected devices
Build versus Partner

• DNS Software
  – BIND RPZ
  – Custom DNS development

• Threat feeds
  – Public feeds
  – Commercial feeds

• Value of a DNS security product is the threat feed
Competitive Value is Data Science

Analyze **100 billion queries** every day.

On average **100,000 new domains** are dynamically added to the block list daily.
Advanced, Predictive Intelligence

DATA SCIENCE METHODS
Anomaly Detection & Pattern Recognition

SERVICE PROVIDER DATA
DNS AND PROXY

MOBILE + FIXED
SUBSCRIBERS + BUSINESSES
= 100B QUERIES DAILY

COMMERCIAL DATA SOURCES

PUBLIC DATA SOURCES

BUSINESS CUSTOMERS

SUBSCRIBERS

NETWORK

Streaming Threat Intelligence
CIRA D-Zone DNS Firewall

Launched June 2017 → 80 Live Customers → 500,000 Network Users

3000 QPS Peak → 1M Blocks Per Month → 5M new domains added monthly

100% of customers see blocks → DNS as a defense layer accepted → False positives not an issue
What We Learned

- Operational Requirements
- Customer experience and benefit
- Threat Landscape
- Benefits to CIRA
Recursive DNS services need to be DDoS resilient
Operational - Capacity

Need to understand the query traffic and required capacity
Operational - Modeling Capacity (QPS/1,000 users)

We can map our 200,000 QPS operational capacity in to number of network users for each type of organization.
D-Zone DNS Firewall – Customer Value

Need for additional malware phishing protection
# Customer Value - Hospital

<table>
<thead>
<tr>
<th>Address</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Threat Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-09-13 16:50 UTC</td>
<td>2018-03-09 22:55 UTC</td>
<td>Palevo</td>
<td>24 352</td>
<td></td>
</tr>
<tr>
<td>2017-09-18 14:10 UTC</td>
<td>2018-03-08 22:00 UTC</td>
<td>Malware Call Home</td>
<td>1443</td>
<td></td>
</tr>
<tr>
<td>2017-10-01 12:10 UTC</td>
<td>2018-02-27 13:30 UTC</td>
<td>Malware-Adware/A</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>2017-11-15 16:35 UTC</td>
<td>2018-03-02 17:10 UTC</td>
<td>Ransomware</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>2017-12-04 23:55 UTC</td>
<td>2018-03-09 22:50 UTC</td>
<td>Suspected Malware</td>
<td>4034</td>
<td></td>
</tr>
<tr>
<td>2018-01-03 19:50 UTC</td>
<td>2018-03-09 19:25 UTC</td>
<td>Bitcoin Miner</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>2018-01-30 18:30 UTC</td>
<td>2018-02-17 21:30 UTC</td>
<td>RoughTed</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>2018-02-28 15:35 UTC</td>
<td>2018-02-28 15:40 UTC</td>
<td>Mirai</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2018-03-08 03:30 UTC</td>
<td>2018-03-09 22:50 UTC</td>
<td>Ramnit</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>
Threat Landscape – Aggregate Threats
Threat Landscape – Malware

Number of Queries

Time

DDoS SubDomGen  Bitcoin Miner  Malware Call Home  Mirai  Other  Conficker B  Palevo  Bedep  DNS Tunneling  Suspected Malware  ZeroDayCluster
Benefits to CIRA

• View of threat landscape in Canada
• Ability to identify threats specific to Canada
• Inform and educate
• Protection for Canadians
• Create communities of interest to share threat data
• Elevates CIRA to a national Cybersecurity Role in Canada
DNS Firewall Vision

- Make D-Zone DNS Firewall a critical part of Canada’s cybersecurity
- Create communities of interest to share threat data
- Improve data sovereignty
- Augment service with Canadian Threat Data
- A secure recursive DNS available to all Canadians
Conclusion

• Partnership with Nominum/Akamai helped us move quickly with a carrier grade service
• DNS is gaining momentum as a critical part of a defense in depth strategy
• Operating a national DNS is great fit with CIRA’s mandate for a better online Canada
• DNS service and data is a valued resource that can be leveraged to improve national cybersecurity
Questions?

Mark Gaudet
mark.gaudet@cira.ca