Gaining Security Insight Through DNS Analytics

Scott Penney

Director of Cyber Security Solutions, BlueCat Networks
Agenda

- Welcome to the Jungle
- Why DNS Matters
- Deal with the Facts
- The Power of DNS
- Q&A
Welcome to the Jungle
IT Sprawl is out of Control

4.9 Billion
“Things” Connected in 2016

480 Million
Smart Phones Delivered in 2016

70%
of Mobile Professionals Work on Personal Devices

2 Billion
Mobile Devices Shipped in 2016

65%
of Smart Phones used in BYoD Environments

Only 1 in 3 Companies Know How Many Vendors Use their Infrastructure

Source: Gartner (http://www.gartner.com/newsroom/id/3165317)
IT Moving from CENTER to the EDGE…

Business drivers demand DISTRIBUTED RESOURCES to meet local needs, which brings additional CHALLENGES.

**Added Risk**
- More attack surface is exposed
- Untrusted/managed devices
- Loss of visibility

**Reduced Control**
- Costly infrastructure to deploy
- Absence of standards & practices
- Lack of policy enforcement
And What is the Result?

- Security spending has increased by 49% from 2010 to 2014
- The number of records stolen and exposed through security breaches has increased 200x over same period
- Increasing spending on more solutions isn’t working; we need a new paradigm

Sources: Verizon, Information is Beautiful, RBS, Gartner, Forrester
Where to Focus?

“Prevention is a failed strategy.”

Amit Yoran, President, RSA
RSA Conference 2016
Prevention or Detection?

- Organizations are focused on PREVENTION of breaches
  - 93% use Anti-virus/Anti-malware tools
  - 82% use Perimeter Firewalls
  - 65% use Intrusion Prevention Systems
  - 52% use Unified Threat Management (UTM) Systems
- But when breached, attackers have 200-250 days before they are DETECTED
- Organizations need to leverage the power of what they already have to address this detection gap
Why DNS Matters
DNS is Foundational

Perimeter Security: Firewalls, Content Filters, Honeypots, etc.

Endpoint Security: AV, DLP, Patch Mgmt., Client Firewalls, IDS/IPS, etc.

Data Security: Encryption, IDAM, DLP, Integrity, DRM

Network Security: IDS/IPS, NAC, DLP, Messaging, etc.

Application Security: WAF, DB Security, Code Scanners, etc.
DNS is Foundational

Perimeter Security: Firewalls, Content Filters, Honeypots, etc.

Endpoint Security: AV, DLP, Patch Mgmt., Client Firewalls, IDS/IPS, etc.

Data Security: Encryption, IDAM, DLP, Integrity, DRM

Network Security: IDS/IPS, NAC, DLP, Messaging, etc.

Application Security: WAF, DB Security, Code Scanners, etc.

DNS Security: Foundation/Visibility/Enforcement
DNS is a PERVERSIVE SENSOR

- DNS signals INTENT
- DNS shows BEHAVIOR
  - All device types
  - All protocols
  - All locations
  - Managed AND Unmanaged
  - Corporate AND Guest
  - Center AND Edge
- DNS is REAL TIME
DNS is an IDEAL ENFORCER

- Enforce at every level
  - Client
  - Network
  - Enterprise

- Configurable Policies
  - White & Black Lists
  - Geographic
  - Time-based
  - Risk-based
DNS is Untapped Potential

56% of Large Orgs Don’t Capture DNS Data

63% of Small Orgs Don’t Capture DNS Data

Of Those Paying Attention – only 75% actually look at it

Source: BlueCat Networks/UBM Survey
Insight Through DNS Analytics

The Power of DNS Lets You:

1. See threats emerge before they become “known”
2. Gain equal visibility into internal and external activity
3. Understand who (and what) is accessing your infrastructure
4. Monitor the activity of all users and devices in real time
5. Protect and control across all device types
Deal with the FACTS
Gain insights to improve security
Data Versus Facts

“Data is of course important in manufacturing, but I place the greatest emphasis on facts.”

Taiichi Ohno, Toyota Motor Corporation
Father of Lean Manufacturing
The Big Data Challenge
A Cautionary Tale

3.8 Trillion
Queries Per Week

- Actual query volume from a very large financial institution
- All of which is logged in a very expensive database
- And all they have is a really big log file, **but no FACTS**
Deriving FACTS from DNS Data
Deriving FACTS from DNS Data

Activity Signature Identified:
Start-up sequence for application
Deriving FACTS from DNS Data


ACTIVITY SIGNATURE IDENTIFIED:
Start-up sequence for application

FACT CATALOGED
• 07-Oct-2015
• Client Application Identified: Instagram

CATALOG

<table>
<thead>
<tr>
<th>LOGGED FACT SIGNATURE</th>
<th>ACTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-Oct-2015 APP: Dropbox Communication Fre...</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: WhatsApp Startup Sequence</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: Instagram Startup Sequence</td>
<td></td>
</tr>
</tbody>
</table>
Deriving FACTS from DNS Data

Deriving FACTS from DNS Data

ACTIVITY SIGNATURE IDENTIFIED:
Repeated query intervals – Beaconing

FACT CATALOGED
• 07-Oct-2015
• Security Threat Identified: MALWARE [whatsmyip.net]

CATALOG

<table>
<thead>
<tr>
<th>LOGGED FACT SIGNATURE</th>
<th>ACTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-Oct-2015 APP: Dropbox Communication Fre...</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: WhatsAPP</td>
<td></td>
</tr>
<tr>
<td>Startup Sequence</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: Instagram Startup Sequence</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 MALWARE: whats... Query Intervals</td>
<td></td>
</tr>
</tbody>
</table>
Deriving FACTS from DNS Data

ACTIVITY SIGNATURE IDENTIFIED:
Newly Observed Domain

<table>
<thead>
<tr>
<th>LOGGED FACT SIGNATURE</th>
<th>ACTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-Oct-2015 APP: Dropbox Communication Fre...</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: WhatsApp Startup Sequence</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 APP: Instagram Startup Sequence</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 MALWARE: whats... Query Intervals</td>
<td></td>
</tr>
</tbody>
</table>
Deriving FACTS from DNS Data

ACTIVITY SIGNATURE IDENTIFIED:
Newly Observed Domain

FACT CATALOGED
- 07-Oct-2015
- Security Threat Identified: Suspect Activity [leet.cc]

CATALOG

<table>
<thead>
<tr>
<th>LOGGED FACT SIGNATURE</th>
<th>ACTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-Oct-2015 APP: Dropbox Communication Fre...</td>
<td>Startup</td>
</tr>
<tr>
<td>07-Oct-2015 APP: WhatsApp Sequence</td>
<td>Startup</td>
</tr>
<tr>
<td>07-Oct-2015 APP: Instagram Sequence</td>
<td>Startup</td>
</tr>
<tr>
<td>07-Oct-2015 MALWARE: what... Query Intervals</td>
<td></td>
</tr>
<tr>
<td>07-Oct-2015 Suspect: leet.cc Observed Domain</td>
<td></td>
</tr>
</tbody>
</table>
The Power of DNS
Analytics to drive better security
DNS as a Sensor and Enforcer

What can DNS do for you?

- Provide instant VISIBILITY into what’s on your infrastructure
- Identify BEHAVIOR that is suspicious, regardless of the cause
- CONTROL access to resources or data
- BLOCK known threats before they manifest
DNS Gives the Facts You Need to Secure Your Network

#1
Leverage What You Have
• Avoid complexity & cost
• No more “layers”
• Mine the data you already have

#2
Increase Your Visibility
• Use a pervasive technology to gain insight
• Detect events faster to save time, money, and reputation
• Utilize the adaptive nature of DNS
• Stop playing catch-up to new threats

#3
Get More Control
• Enforce policies across any device or user type
• Use DNS to assess risk and decide on action
• Secure remote locations without costly infrastructure
• Use dependence on DNS against the bad guys
Questions?