DIY DNS DFIR: You’re Doing it WRONG

Andrew Hay, CISO
DataGravity, Inc.
ahay@datagravity.com
twitter.com/andrewsmhay
About Me

• Andrew Hay
  – Chief Information Security Officer (CISO) @ DataGravity
  – Former:
    • Director of Research @ OpenDNS
    • Chief Evangelist & Director of Research @ CloudPassage
    • Senior Security Analyst @ 451 Research

  – Wrote some books, blog occasionally, and give Rob a hard time on Twitter
Overview

• Whirlwind tour of DNS
• Why DNS is so valuable for TH and IR
• Real world example
• Available tools
• Summary
Whirlwind tour of DNS
Hang on tight!
The Domain Name System (DNS) is one of the most essential parts of the Internet’s infrastructure—Some might say it’s the plumbing 😊

By using DNS, you can connect to a website without having to know the website’s IP address.

After all, who wants to remember every website’s IP address

Recursive vs. Authoritative

Authoritative DNS nameservers are responsible providing answers to recursive DNS nameservers with the IP “mapping” of the intended website
What DNS Looks Like

• Recursive DNS nameservers
  – Responsible for providing the proper IP address of the intended domain name to the requesting host.

• Authoritative DNS nameservers
  – responsible for providing answers to recursive DNS nameservers with the IP “mapping” of the intended website
Why DNS is so valuable
For threat hunting and incident response
Why DNS is so valuable

• The more data you have, the better suited you are to **CONSTRUCT A TIMELINE** of events

• At the **VERY LEAST** you should be able to **MAKE MORE INFORMED DECISIONS**

• DNS traffic is often the most overlooked and undervalued network-based data source
Why DNS is so valuable

• DNS shows you...
  – What domains are being looked up by humans and machines
  – The frequency at which domains are being looked up
  – What parts of the world (based on TLD) your systems are trying to hit
  – Whether or not the domains being queried are live
  – If subsequent queries (redirects) are made as a result of a particular query
  – Whether or not the queries are attempting to resolve fraudulent/phishing sites
Why DNS is so valuable – DGA Detection

• Domain Generation Algorithm (DGA)
  – Used to generate domains programmatically
• Typically rely on a seed of some sort
  – Date, time, keyword, etc.
• Allows for the registration of domains that no human would ever type
Why DNS is so valuable – DGA Detection

- Frequently used by malware for dynamic C&C generation
- Example
  - Dyre DGA algorithm
  - Provided by Talos
Why DNS is so valuable – DGA Detection

- Also used for marketing campaigns
  - e.g. Marketo
  - `http://100-AEK-913.mktorest.com/rest/v1/lead/{id}.json`
Why DNS is so valuable – Redirects

1. domain.com
2. redir -> domain2.com
3. domain2.com

www.domain.com
exploit delivery
Real world example
Of using DNS for threat hunting and incident response
Real World Example: Xerox Printers

• Noticed a rather odd domain name being beaconed out to: xeroxdiscoverysupernode3.com
  – Malware?
  – Phishing?
  – Drive update site?
  – Too long to be valid, right?
• Domain was not even registered!
  – Used OpenDNS Investigate
  – xeroxdiscoverysupernode[1-3].com were each seeing ~2,000 queries per hour
Real World Example: Xerox Printers

- Google showed these domains as being related to Xerox® WorkCentre® 5845/5855/5865/5875/5890 and 7000-series line of printers
- Origin of beaconing was from the McAfee ePolicy Orchestrator (ePO) security module
Real World Example: Xerox Printers

**WorkCentre™ 5865/5875/5890**
- New!
- Xerox ConnectKey Controller
- Copy, print, scan, fax, email
- Speed: up to 65 / 75 / 90 ppm
- Maximum paper capacity: 6,700 sheets
- **List Price:** $25,245

**WorkCentre™ 7755/7765/7775**
- Copy, print with optional scan, fax, email
- Best for high-volume jobs of any size with great color when you need it
- Color: up to 40 / 50 ppm
- Black: up to 55 / 65 / 75 ppm
- Standard paper capacity: 3,260 sheets
- Maximum paper capacity: 5,260 sheets
- **List Price:** $34,100

**Xerox® Color 560/570**
- Copy, print, scan, fax, email
- Best for graphics-intensive and short-run production applications
- Color: up to 60/70 ppm
- Black: up to 65/76 ppm
- Maximum paper capacity: 7,260 sheets
- **List Price:** $39,995

Not inexpensive printers...
Real World Example: Xerox Printers

• So what were they doing?

• They were trying to do a handshake
  – ...over the Internet
  – ...because that’s where DNS said the server was.
Real World Example: Xerox Printers

• Printers querying from all over the world!

• Long story short...
  – Xerox printers querying out to the Internet
  – Documentation says to configure the xeroxdiscoverysupernode[1-3] domains to point internally
  – Obviously not everyone read the instructions
Real World Example: Xerox Printers

• Registered the domains, pointed to a VPS, and monitored traffic.
Real World Example: Xerox Printers

• Domains sinkholed (at OpenDNS)

• Blog post released
  – http://labs.opendns.com/2014/05/01/xerox-printer-beacons/

• All fixed now, right?
### Real World Example: Xerox Printers

**Bytes**

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Time</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>05/05/14 19:00:00</td>
<td>0 bps</td>
</tr>
<tr>
<td>Max</td>
<td>05/05/14 12:00:00</td>
<td>2.12 Mbit</td>
</tr>
<tr>
<td>Last</td>
<td>05/05/14 19:03:51</td>
<td>75.4 bps</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td>1.62 Mbit</td>
</tr>
<tr>
<td>Total Traffic</td>
<td></td>
<td>240.09 GB</td>
</tr>
<tr>
<td>Selection Time</td>
<td></td>
<td>Wed Apr 30 2014 17:00:00 GMT-0700 (PDT)</td>
</tr>
</tbody>
</table>

*NOTE: Click on the graph to zoom.*
Available tools
Free and commercial
Free Tools

• PassiveTotal
  – Passive DNS threat-analysis platform
  – https://www.passivetotal.org/

• Site24x7
  – Generate a DNS Report for a domain

• DNSstuff Toolbox
  – Various tools related to DNS intelligence
  – http://www.dnsstuff.com/tools
Free Tools (Continued…)

- Domaintools
  - Whois lookup, other features for a price
  - http://research.domaintools.com/

- Elasticsearch, Logstash, Kibana (ELK)
  - Take data from any source, any format and search, analyze, and visualize it
  - https://www.elastic.co/

- Graylog
  - “Open source log management that actually works.”
  - https://www.graylog.org/
Commercial Tools

- PassiveTotal Enterprise (by RiskIQ)
  - Geared towards the enterprise
  - https://www.passivetotal.org/enterprise

- Domaintools
  - Domain, DNS and Internet OSINT-based cyber threat intelligence (14yrs worth)
  - http://domaintools.com/

- OpenDNS Investigate
  - View of Internet domains, IPs, and ASNs
Summary
This is the end my friends...
Collect DNS query logs

Isolate queries related to investigation

Observe network/malware/system comms during incident

Eliminate irrelevant communications and investigation targets

Query/Reference stored DNS to determine scope and scale of exposure

Use third-party tools to enrich your findings

• I wanted to leave you with a workflow for THIR w/DNS
• Hopefully this helps you wrap your heads around how to employ DNS logs during investigations
Summary

• DNS is one of the core protocols used on the Internet
  – And by Internet-connected devices
  – So...like...use it to your benefit, bro!

• DNS can be used to focus your investigation and create a timeline of related events/actions

• Wealth of tools (free and commercial) available to help generate intelligence and corroborate information for use in your investigations
Questions?

Contact me at
ahay@datagravity.com
@andrewsmhay