YOU’VE GOT 99 PROBLEMS AND A BUDGET’S ONE
Rebekah Brown | @PDXBek

Threat Intelligence Lead at Rapid7

But before that…

• Gunnery Sergeant United State Marine Corps
• Chinese Crypto linguist and Network Warfare Analyst
• Policy Developer
• Liaison to State and Local Governments
• Threat Intelligence in the private sector
Why are budgets such a problem?
We are living in a material world…

- Feeds - $$- $$$$$
- Platform - $$$- $$$$$
- Reports - $$-$$$$$
- Analyst on Demand - $$$
- Social Media Analysis - $$- $$$$$
2015 Global Study on IT Security Spending & Investment – Ponemon Institute

• 50% security budget is stalled or declining
• 19% IT security leadership has a say in resource allocation
• 37% of investments in security investments did not meet expectations
• Many organizations do not have the budget to even stay in compliance with regulations
Frugal Girl’s Guide to Threat Intelligence

• Solid Foundation - FREE
• Open-source Feeds – FREE*
• Open-source Platforms – FREE*
• Open-source reports – FREE
• Community Tools – FREE*
• Smart friends - PRICELESS
Retreat, hell! We're not retreating, we're just advancing in a different direction.

— Oliver P. Smith —
That all sounds well and good… but how?

COMMUNICATE

- Find the problems
- Identify solutions
- Implement
- Gather feedback
- Adjust as needed
• CERT-UK and the Centre for the Protection of National Infrastructure

• https://www.cpni.gov.uk/advice/cyber/Threat-Intelligence/

• Strategic
• Operational
• Tactical
• Technical
Security Functions

• Risk and Priority Assessment
• Situational Awareness
• Threat Identification and Alerting
<table>
<thead>
<tr>
<th>Risk and Priority Assessment</th>
<th>Strategic Intelligence</th>
<th>Operational Intelligence</th>
<th>Tactical Intelligence</th>
<th>Technical Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess threats facing similar businesses. <strong>Source:</strong> DBIR, industry reports, annual reports</td>
<td>Assess whether ongoing attacks would impact business operations. <strong>Source:</strong> News, industry reports, internal reports</td>
<td>Evaluate threats have been seen in the past and how to best respond and prioritizing intel. <strong>Source:</strong> Log Data, internal reports</td>
<td>Identify what technologies should be in place to counter the most likely threats. <strong>Source:</strong> industry reports, internal reports</td>
<td></td>
</tr>
</tbody>
</table>

| Situational Awareness | Understand the implications of emerging or high profile threats or vulnerabilities. **Source:** News, blogs, Industry reports | Understand current or planned campaigns and how to respond **Source:** News, blogs, Industry reports, forums, social media | Identify TTPs or indications of a threat and determine how to alert and respond. **Source:** News, Blogs, industry reports | Technical details of threats, including exploitation of a vulnerability. **Source:** News, Blogs, industry reports |

| Threat Identification and Alerting | Provide trending data on what threats are impacting operations and actionable advice for decision makers. **Source:** News, blogs, Industry reports | Identify whether a current or planned attack is impacting you and determine how to respond. **Source:** Blogs, social media, forums. | Alert on TTPs and mechanisms associated with known threats, including implications. **Source:** News, blogs, industry reports, internal reports | Provide automated alerting on high fidelity threat information and help validate and interpret alerts. **Source:** News, blogs, industry reports, internal reports |

<p>| Hunting Operations | Conduct threat trend analysis for your company - what you typically see - to identify when something deviates from the normal. <strong>Source:</strong> Social media, forums. | Information about attackers, where and how they communicate, who they target. <strong>Source:</strong> News, blogs, industry reports | Identify and search for new anomalous activity based off of previously identified known TTPs. <strong>Source:</strong> News, blogs, industry reports | Compare large quantities of technical data to look for outliers or anomalies. <strong>Source:</strong> News, blogs, industry reports, internal reports |</p>
<table>
<thead>
<tr>
<th>Risk and Priority Assessment</th>
<th>Strategic Intelligence</th>
<th>Operational Intelligence</th>
<th>Tactical Intelligence</th>
<th>Technical Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess threats facing similar businesses.</td>
<td>Assess whether ongoing attacks would impact business operations.</td>
<td>Evaluate threats have been seen in the past and how to best respond and prioritizing intel.</td>
<td>Identify what technologies should be in place to counter the most likely threats.</td>
<td></td>
</tr>
<tr>
<td>Source: DBIR, industry reports, annual reports</td>
<td>Source: News, industry reports, internal reports</td>
<td>Source: Log Data, internal reports</td>
<td>Source: industry reports, internal reports</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Situational Awareness</th>
<th>Understand the implications of emerging or high profile threats or vulnerabilities.</th>
<th>Understand current or planned campaigns and how to respond</th>
<th>Identify TTPs or indications of a threat and determine how to alert and respond.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Source: News, Blogs, industry reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Threat Identification and Alerting</th>
<th>Provide trending data on what threats are impacting operations and actionable advice for decision makers.</th>
<th>Identify whether a current or planned attack is impacting you and determine how to respond.</th>
<th>Alert on TTPs and mechanisms associated with known threats, including implications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: News, blogs, Industry reports</td>
<td>Source: Blogs, social media, forums.</td>
<td>Source: News, blogs, industry reports, internal reports</td>
<td>Source: News, blogs, industry reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hunting Operations</th>
<th>Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.</th>
<th>Information about attackers, where and how they communicate, who they target.</th>
<th>Identify and search for new anomalous activity based off of previously identified known TTPs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: Social media,</td>
<td>Source: News, blogs,</td>
<td>Source: News, blogs,</td>
<td>Source: News, blogs,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk and Priority Assessment</strong></td>
<td><strong>Strategic Intelligence</strong></td>
<td><strong>Operational Intelligence</strong></td>
<td><strong>Tactical Intelligence</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
| **Assess threats facing similar businesses.**  
*Source: DBIR, industry reports, annual reports* | Assess whether ongoing attacks would impact business operations.  
*Source: News, industry reports, internal reports* | Evaluate threats have been seen in the past and how to best respond and prioritizing intel.  
*Source: Log Data, internal reports* | Identify what technologies should be in place to counter the most likely threats.  
*Source: industry reports, internal reports* |

| **Situational Awareness** | **Understand the implications of emerging or high profile threats or vulnerabilities.**  
*Source: News, blogs, Industry reports* | **Understand current or planned campaigns and how to respond**  
*Source: News, blogs, Industry reports, forums, social media* | **Identify TTPs or indications of a threat and determine how to alert and respond.**  
*Source: News, Blogs, industry reports* | **Technical details of threats, including exploitation of a vulnerability.**  
*Source: News, Blogs, industry reports* |

| **Threat Identification and Alerting** | **Provide trending data on what threats are impacting operations and actionable advice for decision makers.**  
*Source: News, blogs, Industry reports* | **Identify whether a current or planned attack is impacting you and determine how to respond.**  
*Source: Blogs, social media, forums.* | **Alert on TTPs and mechanisms associated with known threats, including implications.**  
*Source: News, blogs, industry reports, internal reports* | **Provide automated alerting on high fidelity threat information and help validate and interpret alerts.**  
*Source: News, blogs, industry reports, internal reports* |

| **Hunting Operations** | **Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal.**  
*Source: Social media, forums.* | **Information about attackers, where and how they communicate, who they target.**  
*Source: Social media, forums.* | **Identify and search for new anomalous activity based off of previously identified known TTPs.**  
*Source: News, blogs,* | **Compare large quantities of technical data to look for outliers or anomalies.**  
*Source: News, blogs, industry reports, internal reports* |
Strategic Intel for Risk and Priority Assessment

“What threats are facing us? What can we do to prevent it?”

• Goal: Assess threats facing business similar to yours and present that information in a digestible format

• Resources:
  – Verizon Data Breach Investigations Report
  – DBIR Industry Snapshot
  – Congressional Research Service
  – Internal resources
DBIR Industry Snapshot - Healthcare

Close to two-thirds of all breaches go on for months before the victim learns that they’ve been compromised.

Table 1. Threat action varieties by percent of breaches in the Healthcare industry

<table>
<thead>
<tr>
<th>Rank</th>
<th>Variety</th>
<th>Category</th>
<th>Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exploitation of default or guessable credentials</td>
<td>Hacking</td>
<td>72%</td>
</tr>
<tr>
<td>2</td>
<td>Backdoor (allows remote access/control)</td>
<td>Malware</td>
<td>49%</td>
</tr>
<tr>
<td>3</td>
<td>Exploitation of backdoor or command and control channel</td>
<td>Hacking</td>
<td>49%</td>
</tr>
</tbody>
</table>
Cybersecurity: Authoritative Reports and Resources, by Topic

- Cybersecurity Policy
- Critical Infrastructure
- Cybercrime and Data Security
- Cybersecurity framework
- Reports by federal agency
Internal Resources

- Business Priorities
- Asset Management
- Third Party Outsourcing
- Security Posture
Key Points:

• What are the largest threats to organizations similar to yours?
• What types of threat actors target your organization?
• What actions do they take?
• Where do they attack?
• Are we positioned to identify and defeat an attack?
Tips for Reporting to the Board:

- Do not use jargon or overly technical terms
- Discuss business impact of threats
- Be prepared to answer questions
- Tell the story
- Keep it simple
<table>
<thead>
<tr>
<th>Strategic Intelligence</th>
<th>Operational Intelligence</th>
<th>Tactical Intelligence</th>
<th>Technical Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk and Priority Assessment</strong></td>
<td>Assess threats facing similar businesses.</td>
<td>Evaluate threats have been seen in the past and how to best respond and prioritizing intel.</td>
<td>Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports</td>
</tr>
<tr>
<td>Source: DBIR, industry reports, annual reports</td>
<td>Assess whether ongoing attacks would impact business operations.</td>
<td>Source: Log Data, internal reports</td>
<td></td>
</tr>
<tr>
<td><strong>Situational Awareness</strong></td>
<td>Understand the implications of emerging or high profile threats or vulnerabilities.</td>
<td>Identify TTPs or indications of a threat and determine how to alert and respond.</td>
<td>Technical details of threats, including exploitation of a vulnerability.</td>
</tr>
<tr>
<td>Source: News, blogs, Industry reports</td>
<td><strong>Understand current or planned campaigns and how to respond</strong></td>
<td>Source: News, Blogs, Industry reports reports, forums, social media</td>
<td>Source: News, Blogs, industry reports</td>
</tr>
<tr>
<td><strong>Threat Identification and Alerting</strong></td>
<td>Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports</td>
<td>Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, Industry reports, internal reports</td>
<td>Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, Industry reports, internal reports</td>
</tr>
<tr>
<td><strong>Hunting Operations</strong></td>
<td>Conduct threat trend analysis for your company - what you typically see to identify when something deviates from the normal. Source: Social media, forums</td>
<td>Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs, Industry reports, internal reports</td>
<td>Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, Industry reports, internal reports</td>
</tr>
</tbody>
</table>
Operational Intel for Situational Awareness

“Is this attack that is happening going to impact us? Do we need to change anything to be prepared?”

• Goal: Understand ongoing or pending attacks and be prepared to respond.

• Resources:
  – Social Media
  – Blog Posts
  – Government Alerts
  – Partners and peers
Operational Intel for Situational Awareness

Identify that there is a threat

Gather information

Make recommendations on actions
Threat Identification

Security Tip (ST14-001)
Sochi 2014 Olympic Games

Original release date: February 04, 2014 | Last revised: March 10, 2014

CyberJihadHelp
@Anony_Caucasus

#Paybackforsochi Warning our attack Its revenge
For the Stupid games in our Land the circassian land 1.5 million people dead in 1864
9:07 AM - 5 Feb 2014

ē  t 5  ❤ 2
Social Mention

0% strength
0% passion
2 days avg. per mention
last mention 8 days ago
1 unique authors
1 retweets

1:0 sentiment
2% reach

Google Alerts

Alerts
Monitor the web for interesting new content

Search: Sochi Olympics AND DDOS

How often: As-It-happens
Sources: Automatic
Language: English
Region: Any Region
How many: Only the best results
Deliver to: RSS feed

CREATE ALERT
Hide options
Key Points:

• What is the operation?
• Who is the target?
• How have they attacked in the past?
• Are we vulnerable to any of those attacks?
• What are we seeing now that could help us defend ourselves?
Tips for Reporting

• Be objective
• Identify triggers
• Identify constraints – if this is serious what do you need to do your job?
• Provide updates
<table>
<thead>
<tr>
<th>Risk and Priority Assessment</th>
<th>Strategic Intelligence</th>
<th>Operational Intelligence</th>
<th>Tactical Intelligence</th>
<th>Technical Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess threats facing similar businesses.</td>
<td>Assess whether ongoing attacks would impact business operations.</td>
<td>Evaluate threats have been seen in the past and how to best respond and prioritizing intel.</td>
<td>Identify what technologies should be in place to counter the most likely threats.</td>
<td></td>
</tr>
<tr>
<td>Source: DBIR, industry reports, annual reports</td>
<td>Source: News, industry reports, internal reports</td>
<td>Source: Log Data, internal reports</td>
<td>Source: industry reports, internal reports</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Situational Awareness</th>
<th>Understand the implications of emerging or high profile threats or vulnerabilities.</th>
<th>Understand current or planned campaigns and how to respond</th>
<th>Identify TTPs or indications of a threat and determine how to alert and respond.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Threat Identification and Alerting</th>
<th>Provide trending data on what threats are impacting operations and actionable advice for decision makers.</th>
<th>Identify whether a current or planned attack is impacting you and determine how to respond.</th>
<th>Alert on TTPs and mechanisms associated with known threats, including implications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: News, blogs, Industry reports</td>
<td>Source: Blogs, social media, forums.</td>
<td>Source: News, blogs, industry reports, internal reports</td>
<td>Source: News, blogs, industry reports, internal reports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hunting Operations</th>
<th>Conduct threat trend analysis for your company - what you typically see - to identify when something deviates from the normal.</th>
<th>Information about attackers, where and how they communicate, who they target.</th>
<th>Identify and search for new anomalous activity based off of previously identified known TTPs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: Social media,</td>
<td>Source: News, blogs,</td>
<td>Source: News, blogs,</td>
<td>Source: News, blogs,</td>
</tr>
<tr>
<td>Industry reports</td>
<td></td>
<td>industry reports, internal reports</td>
<td>industry reports, internal reports</td>
</tr>
</tbody>
</table>
Tactical Intel for Situational Awareness

“Is this new tactic/tool/methodology going to impact us? How quickly do we need to respond?”

Goal: Identify TTPs or indications of a threat and determine how to alert and respond.

Resources:
  – News
  – Social Media
  – Blog Posts
  – Internal Resources
Tactical Intel for Situational Awareness

1. Identify threat
2. Identify key factors
3. Are you vulnerable?
4. Report
HD Moore’s Law

“Casual Attacker power grows at the rate of Metasploit”

• Pay special attention to vulnerabilities with Metasploit modules
• More attacker activity
• Check your vulnerability
• Identify artifacts and IOCs to monitor
New Modules

This update also comes with a fun privilege escalation exploit for OSX where an environment variable ends up on a commandline. I love these kinds of bugs because people have been screwing up environment variables since the invention of shells.

As always, you can see all the changes since the last wrapup on github: 4.11.4-2015102801...4.11.5-2015103001

Exploit modules

- Th3 MMA mma.php Backdoor Arbitrary File Upload by Jay Turla
- Mac OS X 10.9.5 / 10.10.5 - rsh/libmalloc Privilege Escalation by rebel and shandelman116 exploits CVE-2015-5889

Auxiliary and post modules

- Joomla Real Estate Manager Component Error-Based SQL Injection by Nixawk and Omer Ramic
- Joomla com_contenthistory Error-Based SQL Injection by Asaf Orpani, Nixawk, and bperry exploits CVE-2015-7297
If you are vulnerable:

• Overview of the threat
• Details of how it operates
• What systems are at risk
• How those systems fit into operations
• Available remediation or workarounds
If you are NOT vulnerable:

• Not every threat will impact every organization!!!
• Provide an overview of the threat
• Details of how it operates
• WHY it should not impact you
• What to continue to look for
Tips for Reporting

• Technical terms are fine, but define if you have a broad audience
• Provide links to sources
• Use bullet points to call out important details
• TIMELINESS IS KEY
• Control the spin
• Update as needed
<table>
<thead>
<tr>
<th></th>
<th>Strategic Intelligence</th>
<th>Operational Intelligence</th>
<th>Tactical Intelligence</th>
<th>Technical Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk and Priority</strong></td>
<td>Assess threats facing similar businesses. Source: DBIR, industry reports, annual reports</td>
<td>Assess whether ongoing attacks would impact business operations. Source: News, industry reports, internal reports</td>
<td>Evaluate threats have been seen in the past and how to best respond and prioritizing intel. Source: Log Data, internal reports</td>
<td>Identify what technologies should be in place to counter the most likely threats. Source: industry reports, internal reports</td>
</tr>
<tr>
<td><strong>Assessment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Situational</strong></td>
<td>Understand the implications of emerging or high profile threats or vulnerabilities. Source: News, blogs, Industry reports</td>
<td>Understand current or planned campaigns and how to respond Source: News, blogs, Industry reports, forums, social media</td>
<td>Identify TTPs or indications of a threat and determine how to alert and respond. Source: News, Blogs, industry reports</td>
<td>Technical details of threats, including exploitation of a vulnerability. Source: News, Blogs, industry reports</td>
</tr>
<tr>
<td><strong>Awareness</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Threat Identification</strong></td>
<td>Provide trending data on what threats are impacting operations and actionable advice for decision makers. Source: News, blogs, Industry reports</td>
<td>Identify whether a current or planned attack is impacting you and determine how to respond. Source: Blogs, social media, forums.</td>
<td>Alert on TTPs and mechanisms associated with known threats, including implications. Source: News, blogs, industry reports, internal reports</td>
<td>Provide automated alerting on high fidelity threat information and help validate and interpret alerts. Source: News, blogs, industry reports, internal reports</td>
</tr>
<tr>
<td><strong>and Alerting</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hunting</strong></td>
<td>Conduct threat trend analysis for your company - what you typically see- to identify when something deviates from the normal. Source: Social media, forums.</td>
<td>Information about attackers, where and how they communicate, who they target. Source: News, blogs, industry reports</td>
<td>Identify and search for new anomalous activity based off of previously identified known TTPs. Source: News, blogs, industry reports</td>
<td>Compare large quantities of technical data to look for outliers or anomalies. Source: News, blogs, industry reports, internal reports</td>
</tr>
</tbody>
</table>
Technical Intelligence for Threat Alerting

“What is this thing??!?!?”

Goal: Make sense of alerts that the SOC has to deal with because of you

Resources:
- Virus Total
- Blogs
- Reports
- Maltego
What can you do?

• You alerted on something for a reason – I hope

• Key Details:
  – Where did the alert come from?
  – When was it flagged as malicious?
  – What activity is it associated with?

• Identify false positives
## Passive Total

<table>
<thead>
<tr>
<th>IP Address</th>
<th>CIDR</th>
<th>Date</th>
<th>Time</th>
<th>Source</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>50.57.19.16</td>
<td>50.57.0.0/16</td>
<td>2012-03-21</td>
<td>21:13:23</td>
<td>2013-03-27</td>
<td>riskiq</td>
</tr>
<tr>
<td>64.202.189.170</td>
<td>64.202.188.0/23</td>
<td>2011-02-12</td>
<td>17:02:20</td>
<td>2012-03-15</td>
<td>riskiq</td>
</tr>
<tr>
<td></td>
<td>Jul</td>
<td>Aug</td>
<td>Sep</td>
<td>Oct</td>
<td>Nov</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td><strong>S</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>M</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>W</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>T</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>F</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>S</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Dynamic/Registered**

- Green
- Light Green
- Light Green
- Light Green
- Light Green

**Dynamic**

- Blue
- Blue
- Blue
- Blue
- Blue

**Registered**

- Medium Brown
- Medium Brown
- Medium Brown
- Medium Brown
- Medium Brown

**First Seen**

- Red
**Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Seen</td>
<td>2009-09-01 05:24:22</td>
</tr>
<tr>
<td>Last Seen</td>
<td>2016-01-21 00:00:00</td>
</tr>
<tr>
<td>Resolutions</td>
<td>2096</td>
</tr>
<tr>
<td>Network</td>
<td>72.167.232.0/24</td>
</tr>
<tr>
<td>ASN</td>
<td>26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com)</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Ever Compromised</td>
<td>true</td>
</tr>
<tr>
<td>Sinkhole</td>
<td>true</td>
</tr>
</tbody>
</table>

**Heatmap**

<table>
<thead>
<tr>
<th>Source</th>
<th>Link</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocklist</td>
<td><a href="http://www.blocklist.de/en/export.html">http://www.blocklist.de/en/export.html</a></td>
<td>blocklist, apache</td>
</tr>
<tr>
<td>Blocklist</td>
<td><a href="http://www.blocklist.de/en/export.html">http://www.blocklist.de/en/export.html</a></td>
<td>blocklist, bruteforcelogin</td>
</tr>
</tbody>
</table>

Select a date or dates (shift-click) on the Heatmap to filter results.

<table>
<thead>
<tr>
<th>Resolve</th>
<th>First</th>
<th>Last</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>monumentalperformance.com</td>
<td>2016-01-21 00:00:00</td>
<td>2016-01-21 00:00:00</td>
</tr>
<tr>
<td>ATTRIBUTES</td>
<td></td>
<td>Heatmap</td>
<td>OSINT</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>First Seen</td>
<td>2009-09-01 05:24:22</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Last Seen</td>
<td>2016-01-21 00:00:00</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Resolutions</td>
<td>2096</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Network</td>
<td>72.167.232.0/24</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>ASN</td>
<td>26496 (AS-26496-GO-DADDY-COM-LLC - GoDaddy.com)</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Ever Compromised?</td>
<td>true</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td>Sinkhole</td>
<td>true</td>
<td></td>
<td>virustotal</td>
</tr>
<tr>
<td></td>
<td>false</td>
<td></td>
<td>virustotal</td>
</tr>
</tbody>
</table>
Maltego

• Passive Total
• Threat Crowd
• Paterva
• Build your own machines
• Developer Portal:
  
  http://dev.paterva.com/developer/
Passive Total Transforms
Tips for Reporting

• Develop a process
• Keep track of your findings
• Provide related indicators or behaviors
• Identify repeat offenders
• Refine your block or alert lists
Reporting on ROI (or lack thereof)

- Make summaries
- Capture the impact
- What worked?
- What didn’t?
- What needs to be changed?
- Where are the pain points?
Building a Community

• Who needs money when you have friends?
• Conferences
• Summits (like this one!)
• Working Groups
• Your organization!
You’ve still got 98 other problems…

…but you’re not alone.

Questions?