Did I Block That?
Five (or so) Things Organizations Botch During a Compromise

Chris Bream, Director
Agenda

- Introduction
- Common Incident Response Mistakes
  - Data
  - Leadership
  - Focus
  - Intensity
  - Information Management
  - Remediation
- Conclusion
Introduction
We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- Targeted Threat and CDT experts
- Located in
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education
Our Team: Industry Leaders

- Extensive information security experience, primarily focused on incident response
- 10 security books authored or co-authored
- Testified about targeted threats to the Permanent Select Committee on Intelligence
Common Incident Response Mistakes
ISSUE

- Forensic and log data can be the source of issues
  - Quality
  - Quantity
  - Blind spots
  - Accessibility

RECOMMENDATION

- Move from getting data to getting the right data
  - Find your blind spots and address them
  - Identify the data that matters and collect it
  - Make the data that matters easily accessible
  - All team members have access to data sources
Leadership

ISSUE

- Organizations struggle with IR leadership
  - No leaders
  - Too many leaders
  - Ineffective leaders
  - Groups or individuals “going rogue”

RECOMMENDATION

- Assign a single IR lead
  - Knowledge of IR not IT or security
  - Full spectrum authority
  - Final decision maker
  - Decisions made with consultation, not agreement
Focus

ISSUE

- Participant focus can be misdirected
  - Resources not dedicated to response
  - Individual on periphery focusing on IR
  - Investigating hunches not leads

RECOMMENDATION

- Dedicate an investigative team during an incident
  - Sole focus on the incident
  - IR lead directs team efforts exclusively
  - Team members have necessary authority during incident
Intensity

ISSUE

- Organizations don’t manage the intensity of the incident
  - Investigation and response are too intense
  - IR fatigue
  - Leadership does not take incidents seriously enough

RECOMMENDATION

- Manage efforts and expectations effectively
  - Set realistic expectations with management
  - Ensure leadership is aware but not overly informed
  - Monitor workload and length of shifts, enforce balance as necessary
ISSUE

- Large amounts of IR data is not properly managed
  - Information is not normalized for efficient consumption
  - Information is provided without context
  - Incomplete information leads to incorrect conclusions

RECOMMENDATION

- Build mechanisms to manage information
  - Settle on a standard time zone for **all** timestamps
  - Develop an information tracking tool before an incident
  - Create a mechanism for information sharing
  - Set a standard for minimum context
Remediation

ISSUE
- Remediation activities can make investigation efforts meaningless
  - Misunderstanding scale of compromise
  - Inappropriate remediation activities
  - Overreaching remediation activities
  - Failure to verify

RECOMMENDATION
- Take a measured, complete remediation approach
  - Full-scale compromise means full-scale remediation
  - Targeted remediation for targeted compromises
  - Test, test, and test again
  - Set a date, miss it, set a second date, make it
Conclusion
Organizations make mistakes in a number of areas
- Data
- Leadership
- Focus
- Intensity
- Information management
- Remediation

Once an incident happens, it’s too late to fix your issues
Understanding what happens during an incident is key
M-Trends 2013

Download the full report
http://www.mandiant.com
STATE OF THE HACK
- Designed for all technical levels
- Case study format
- Illustrates the latest attacks we are seeing

FRESH PRINTS OF MALWARE
- Designed for the technical user
- Case study format
- Digs deeper into the technical aspects of the incidents we respond to
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOCFinder</td>
<td>look for evil on your endpoints</td>
</tr>
<tr>
<td>Redline</td>
<td>answers the question: are you compromised?</td>
</tr>
<tr>
<td>Web Historian</td>
<td>browser analysis</td>
</tr>
<tr>
<td>Memoryze</td>
<td>memory forensics</td>
</tr>
<tr>
<td>Mac Memoryze</td>
<td>memory forensics for MacOS</td>
</tr>
<tr>
<td>Highlighter</td>
<td>log analysis</td>
</tr>
<tr>
<td>IOCe</td>
<td>indicator of compromise editor</td>
</tr>
<tr>
<td>OpenIOC</td>
<td>common language to describe IOCs</td>
</tr>
<tr>
<td>Heap Inspector</td>
<td>detect heap spray in memory</td>
</tr>
<tr>
<td>Shim Cache Parser</td>
<td>look for trace evidence of executing evil</td>
</tr>
</tbody>
</table>
Mandiant is Hiring

- Positions in
  - Intel
  - MCIRT
  - Product development
  - Sales

- Locations
  - Alexandria, VA
  - New York
  - Los Angeles
  - San Francisco
  - Reston, VA

- http://www.mandiant.com/careers
Questions?

- **Chris Bream**
  - chris.bream@mandiant.com

- **More MANDIANT info**
  - [http://www.mandiant.com/](http://www.mandiant.com/)
  - [http://www.twitter.com/mandiant](http://www.twitter.com/mandiant)
  - info@mandiant.com