Taking A Closer Look

Integrated Intelligence From RSA Live
Integrated Intelligence

How Do I Know What To Look For?

- Intelligence gathered from global security community and RSA FirstWatch
  - Aggregated and consolidated
    - Converted into alerts, parsers, blacklists, views and correlation rules
      - Fused with your organization’s data
        - Applied to current & historical data to look for matches
          - Additional intelligence gained during investigation
            - Internal intelligence, custom reports and alerts created

© Copyright 2012 EMC Corporation. All rights reserved.
Fusion of Threat Intelligence With Your Data

- Automatically enrich data with intelligence to help level playing field
- Integrate custom feeds
- Centralize intelligence
- Take advantage of the best 3rd party and RSA First Watch Intelligence
RSA Live In Action

- Definitively classify computers associated with illegal third party exploits, open proxies, worms/viruses, spam engines, Botnets and other current and zero-day exploits
- Prioritize intersection of threat indicators
- Provides real-time, full content navigation of enterprise security intelligence
- Synchronize with RSA FirstWatch and global content derived from best of breed sources
RSA Live In Action – Threat Prioritization

- **Risk: Warning** – high likelihood of malicious activity (botnet, malicious obfuscation, and other malware activity).

- **Risk: Suspicious** – not overtly malicious, but suspicious when combined with other behaviors (known malware filenames, non-standard exe structure, pdfs with javascript, etc.).

- **Risk: Informational** – notable when combined with other behaviors. (hits to file sharing sites, bittorrent activity, social networking use)

  - Prioritized alerts to guide analysis based on intersection / threshold of indicators
# RSA Live Subscription Offering

<table>
<thead>
<tr>
<th>CONTENT CLASSIFICATION</th>
<th>BASIC</th>
<th>ENHANCED</th>
<th>PREMIUM*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informer Threat / Security Reports</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Open Source Community Intelligence</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Core Content for Common Protocols / C&amp;C Reports</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Exploit Kit Identification</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Zero-Day Indicators / Compromise Indicators</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Prioritized Risk Levels</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>RSA Security Threat Blacklist</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>APT Tagged Domains</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Suspicious Proxies</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Malicious Networks</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>NetWitness Identity (AD Integration)</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
<tr>
<td>Verisign® iDefense®</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
<td>![CheckMark]</td>
</tr>
</tbody>
</table>
RSA Live – System Metrics

• 1000+ pieces of content
• 100+ Distinct feed sources
  – Over 5 million IP’s and Domains tracked
  – 20% grown in unique feed sources over past 6 months
• Content library grew by aggregate 30% over past 6 months

• Average of 1.4 million new data points imported and processed week over week
• Live Content Library updated dynamically every hour
  – 8760 updates over past year
• Support for 2 new platforms added over past year
  – RSA for Logs
  – Spectrum