The Time Is Now—A New Era for Cybersecurity

Ashok Sankar
Senior Director Cyber Strategy
Raytheon|Websense

Neil Thacker
Information Security & Strategy Officer, EMEA
Raytheon|Websense
The Time Is Now—A New Era for Cybersecurity

Ashok Sankar
Senior Director – Cyber Strategy
Raytheon | Websense
@ashoksankar
In 2014 has your enterprise experienced an increase or decrease in security attacks as compared to 2013?

- More Attacks: 76.57%
- Fewer Attacks: 23.43%

Enterprises expect to be breached in 2015: 82.5%

## The New Adversaries

Which of the following threat actors exploited your enterprise in 2014?

<table>
<thead>
<tr>
<th>Threat Actor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Criminals</td>
<td>45.6%</td>
</tr>
<tr>
<td>Non Malicious Insiders</td>
<td>40.72%</td>
</tr>
<tr>
<td>Hackers</td>
<td>40.09%</td>
</tr>
<tr>
<td>Malicious Insiders</td>
<td>28.62%</td>
</tr>
<tr>
<td>Hactivists</td>
<td>19.81%</td>
</tr>
<tr>
<td>Nation/State</td>
<td>17.45%</td>
</tr>
</tbody>
</table>

The New Enterprise Landscape

Evolving Business Environment
- Dissolving Security Perimeter
- Embracing Mobility and Cloud Computing
- Extending Value Chain of Partners / Supply Chain / Contractors

More Dangerous Threat Landscape
- More Than Just Malware
- Threats Vectors Span Multiple Channels
- Insider Threat Widening

Complexity & Fragmentation
- Too many tools
- Too many alerts
- Not enough skills and manpower to deal with this complexity
### Cybersecurity Skills Gap Grows

The shortage of skills compounds the rise in security incidents.

<table>
<thead>
<tr>
<th>Year</th>
<th>Projection</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>2.25 million</td>
</tr>
<tr>
<td>2017</td>
<td>4.25 million</td>
</tr>
</tbody>
</table>

*Source: 2013 (ISC)2 Global Information Workforce Study*
Chasing Alerts is a Failing Strategy

Malware Containment Survey Results:

- **198.8** Approximate # of hours per week spent investigating infections
- **229.9** Approximate # of hours per week spent cleaning or fixing infected devices
- **395** Approximate # of hours per week wasted chasing erroneous alerts

Malware Containment Survey Results: Malware Alerts Per Week

- **4%** Alerts that get investigated
- **19%** Reliable alerts
- **40%** Infections that go undetected

Source: Ponemon Institute, 2015
How Do We….

- Continue to fuel business velocity?
- Absorb innovations as needed for the business?
- Stop the adversary from dictating our priorities?
- Confidently navigate the risks in today’s changing IT environment?
- Become resilient?
Need a Strategic Response

1. **ADVANCED THREAT PROTECTION**
   Threat defenses that model the behavior of complex multi-stage attacks.

2. **END-TO-END VISIBILITY**
   Continuously monitor activities including user behaviors across your enterprise.

3. **ADVANCED ANALYTICS**
   Intuitively turn data into insights and answers that drive action.

4. **ADAPTIVE SECURITY**
   Apply context rich intelligence to stop and contain emerging threats.
Focus: Dwell Time Reduction

206 Days Mean time to identify a breach¹ 69 Days Mean time to contain a breach¹

“It is better to have 100 attackers on your network for 10 minutes than a single attacker for 6 months. If dwell time trends down then cyber security is improving”

Jeff Brown, Raytheon CISO

¹Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2015
End-to-end Visibility

- The digital revolution has obfuscated visibility
- Organizations cannot manage threats they cannot see

But is visibility really just more content?
“Context is critical to turning huge amounts of security data into actionable insight and identifying those things that represent the most risk in an organization.”

- Neil MacDonald, Gartner
Analytics Takes Center Stage

Understand and Prioritize

- Automation can help plow through mountains of information
- Discover more about an entity that you know about (reactive/prevent)
- Investigate to understand patterns, find anomalies (proactive/detect)
Adaptive Security boosts Resiliency

Feedback for prediction and preventative action
Cyber Risk Management Approach

PRESENTATION LAYER
- Visibility
- User Experience
- Intuitive

CONTEXT LAYER
- Unstructured Data
- IP Addresses
- Relational Databases
- HR, Travel and other applications
- End User Activity

ANALYTICS LAYER
- Machine Learning
- Heuristics
- Behavior Analysis
- Link Analysis
- Temporal
- Geospatial
- Statistical

CONTENT LAYER
- Mobile
- SIEM
- Network Visibility
- Web Gateway
- Directory Services
- Traditional Security (AV, Scanners, Etc)
- Email Gateway
- Other Data Sources
- Threat Intelligence
Take Aways

- A determined adversary will break in – not a matter of ‘If’ but ‘When’

- Prevention is ideal but need containment strategies

- Rethink cyber strategies to adapt to the landscape

- Resiliency is key to operation in the new normal
Ashok Sankar
Raytheon | Websense
ashok.sankar@raytheon.com
@ashoksankar
The Time Is Now—A New Era for Cybersecurity

Neil Thacker
Information Security & Strategy Officer EMEA
Raytheon | Websense
@nt_hacker
Intelligence, Visibility & Prediction (2000-2015)

Detect
Prevent
Respond

EVOLVED TO

Visibility
Intelligence
Response
Predict
Prevent

#RSAC
From infrastructure security to risk management

- Breach detection
- Malware forensics
- Threat intel feeds
- Threat modelling

- Full DLP/DTP
- Data discovery
- Data encryption
- Behavior analysis
- Predictive analytics

Maturity

1. Perimeter Infrastructure
   - FW/NGFW/UTM
   - SIEM
   - Anti-Virus
   - Device Encryption

2. Baseline Compliance

3. Business Threat
   - Breach detection
   - Malware forensics
   - Threat intel feeds
   - Threat modelling

4. Business Risk
   - Full DLP/DTP
   - Data discovery
   - Data encryption
   - Behavior analysis
   - Predictive analytics

Time
## Threat landscape

<table>
<thead>
<tr>
<th>Top Threats</th>
<th>Current Trends</th>
<th>Top 10 Threat Trends in Emerging Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Malicious code: Worms/Trojans</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>2. Web-based attacks</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>3. Web application attacks /Injection attacks</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>4. Botnets</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>5. Denial of service</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>6. Spam</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>7. Phishing</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>8. Exploit kits</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>9. Data breaches</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
<tr>
<td>10. Physical damage/theft /loss</td>
<td>🟢</td>
<td>🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢 🟢</td>
</tr>
</tbody>
</table>

Threat landscape

Country Report: United Arab Emirates

<table>
<thead>
<tr>
<th>Trend</th>
<th>Identifier</th>
<th>Stages Identified</th>
<th>Detections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic</td>
<td></td>
<td></td>
<td>1567</td>
</tr>
<tr>
<td>R3dom</td>
<td></td>
<td></td>
<td>965</td>
</tr>
<tr>
<td>Proxy</td>
<td></td>
<td></td>
<td>507</td>
</tr>
<tr>
<td>Injection</td>
<td></td>
<td></td>
<td>491</td>
</tr>
<tr>
<td>Dyre</td>
<td></td>
<td></td>
<td>364</td>
</tr>
<tr>
<td>FraudKit</td>
<td></td>
<td></td>
<td>174</td>
</tr>
<tr>
<td>FakeSoftware</td>
<td></td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>Mal_TDS</td>
<td></td>
<td></td>
<td>28</td>
</tr>
<tr>
<td>FakeEmailPortal</td>
<td></td>
<td></td>
<td>23</td>
</tr>
<tr>
<td>Vawtrak</td>
<td></td>
<td></td>
<td>13</td>
</tr>
</tbody>
</table>

Stage Definitions:
- Recon: Research performed by cybercriminals to gather intelligence that improves the probability...
- Lure: An inducement, such as a targeted email or manipulated search engine result (SEO), designed...
- Redirect: When a link in an email or on a web page (visible or hidden) leads to an unexpected...
- Exploit Kit: A packaged set of tools designed to analyze target systems for open vulnerabilities, ...
- Dropper File: The file downloaded onto the victim’s computer that contains the malware. It is a ...
- Call Home: The malware contacts command and control servers (C&C) for instructions, updates, and ...
- Data Theft: The malware sends targeted data to the cybercriminals. Common tactics include slow...
Threat actors
Demo
Analytics & Context in action
Demo
A Layered Approach for the New Normal