Analytics-Based Security Service for the MOC

Alina Oprea
RSA Laboratories

November 19 2015
Risks in the cloud

Public cloud

User

VM

VM

VM

VM

VM

VM
### What are the threats?

<table>
<thead>
<tr>
<th>Cloud provider</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failures at scale</td>
<td>Co-location with malicious tenants</td>
</tr>
<tr>
<td>Configuration errors</td>
<td>Side-channel attacks (cache, network, storage)</td>
</tr>
<tr>
<td>Denial of service</td>
<td>Breach of confidential information</td>
</tr>
<tr>
<td>Server breaches</td>
<td>VMs infected with malware</td>
</tr>
<tr>
<td>Malicious tenants</td>
<td>Inaccurate billing</td>
</tr>
<tr>
<td>Insider attacks</td>
<td></td>
</tr>
<tr>
<td>Malware hosting infrastructure</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring infrastructure

Analytics for security
Analytics-based security service

• **Goals**
  – Real-time and historical analytics on multiple data sources
  – Early warning to cloud administrators and users of potential compromise

• **Use performance metrics**
  – Data already collected by monitoring infrastructure
  – Detect some attacks against the infrastructure and user VMs

• **Additional user protection**
  – Offer fine-grained monitoring service for opt-in users
  – Behavior-based network traffic analysis
Protect the cloud infrastructure

• Performance metrics for physical nodes
  – CPU, network usage, disk I/O, power consumption
• Time-series anomaly detection
• Is it a performance problem or security issue?
Attacks induce unique correlations!

- **Process\(\text{lsass}\)\% Processor Time**
- **Processor\(_\text{Total}\)\% Processor Time**
- **Processor\(_\text{Total}\)\% Idle Time**
- **LogicalDisk(C:)\ Free Megabytes 25466**
- **System\File Write Operations/sec**
- **Network Interface[Intel[R] PRO_1000 MT Network Connection]\ Bytes Total/sec**

- **NTDS\DS Search sub-operations/sec**
Insight: VMs running same application should behave similarly
Outlier detection reveals suspicious VMs
Additional user protection

MOC

VM

Proxy

Internet

Behavioral models

Classification
Clustering
Graph-based models
Markov models

Data collection HTTP headers

Storage
Summary

• Build analytics-based security service for MOC
• Early detection of attacks on cloud infrastructure or user VMs
• Initial stages of exploration

• Interested?
  – Alina Oprea (aoprea@rsa.com)
  – Monitoring team
    • Ayse Kivilcim Coskun
    • Orran Krieger
    • Ata Turk
    • Hua Li
    • Qingqing Li
    • Ozan Tuncer