Defending a Cloud

• MSRC | Azure
  • Security incident response investigations.
    • Compromise | Intrusion | Breach.
    • Forensics @ Microsoft.
  • Making forensics and incident response work in the *Cloud*.
    • Global.
    • Scale.
    • Borders and boundaries.
    • Fast and accurate.
Defending a Cloud

• What is cloud computing?

• Defending a cloud:
  • Brief overview.
  • Challenges.
  • Opportunities.
Defending a Cloud

• What is a cloud?
What is a cloud?

- *Automated* datacenter, where *machines* are-
  - Deployed by machine;
  - Managed by machine; and
  - Monitored by machine.
What is a cloud?

- Collection of automated datacenters.
  - Primary resources:
    - Compute.
    - Storage.
    - Network.
Azure Internals

• Datacenters:
  • Clusters.
  • Nodes (blades).
Azure Internals

• Compute node:
Azure Internals

• **Azure Compute**.
  • **PAAS**—*Platform as a Service*:
    • VM OS provisioned and serviced by Azure infrastructure.
    • Customer runs its own applications on top.
    • Persistent data goes to Storage.
    • PAAS VMs are *stateless*.
  • **IAAS**—*Infrastructure as a Service*:
    • Customer provisions and services the VM OS and applications.
    • IAAS VMs are *stateful*—data are persisted to disks (VHDs).
Azure Internals

• PAAS VM:

   C:\ Resource Disk
   Dynamic VHD

   D:\ Windows
   Differencing Disk

   E:\ or F:\ Role Image
   Differencing Disk

   Windows VHD

   Role VHD
Azure Internals

• PAAS VM:

 Restart in a clean state:
Azure Internals

• IAAS VM:

C:\ OS Disk
RAM Cache
Local Disk Cache

D:\ Resource Disk
Dynamic VHD

E:\, F:\, etc. Data Disks

Blobs

Blob
Azure Internals

• *Persistent Disk.*
Azure Internals

• Big picture:
  • Physical infrastructure.
  • Hosting Environment.
  • Services VMs.
  • Tenant VMs.
Defending a Cloud

Tenant VMs

Services

HE Infra
Defending a Cloud

- Challenges:
  - Ownership.
  - Security.
  - Boundaries.
  - Time.
  - Scale.
Defending a Cloud

• Ownership:
Defending a Cloud

• Ownership:

Privacy: You own and control your data

For more than 20 years, Microsoft has been a leader in creating robust online solutions designed to protect the privacy of our customers. Our time-tested approach to privacy and data protection is grounded in our commitment to organizations’ ownership of and control over the collection, use, and distribution of their information.

We strive to be transparent in our privacy practices, offer you meaningful privacy choices, and responsibly manage the data we store and process. One measure of our commitment to the privacy of customer data is our adoption of the world’s first code of practice for cloud privacy, ISO/IEC 27018.

You own your own data. With Azure, you have ownership of customer data—that is, all data, including text, sound, video, or image files and software, that are provided to Microsoft by you, or on your behalf, through the use of Azure. You can access your customer data at any time and for any reason without assistance from Microsoft. We will not use customer data or derive information from it for advertising or data mining.

You are in control of your data. Because the customer data you host on Azure belongs to you, you have control over where it is stored and how it is securely accessed and deleted.
Defending a Cloud

• Security:
Defending a Cloud

- Security.
  - *Shared Security Model.*
  - Management.
  - Ownership.
Defending a Cloud

• Security.
  • Shared Security Model.
    • Management.
    • Ownership.
Defending a Cloud

• Boundaries:
Defending a Cloud

• Boundaries:
  • We go to the data.
Defending a Cloud

• Time:
  • Here today,
  • Gone tomorrow.
    • VMs.
    • VHDs.
    • Storage.
    • IP address assignments.
Defending a Cloud

• Scale and scalability:
Defending a Cloud

• Scale and scalability:
  • Scale of responsibility requires a scalable response.
Defending a Cloud

• A cloud can be attractive to adversaries.
  • Take up residence:
    • Free trials.
    • Compute power.
    • Storage.
    • Bandwidth.
  • Attack:
    • Internet-exposed services.
    • Internet exposed VMs.
Defending a Cloud

• Digital forensics and incident response challenge:
  • Infrastructure: Internal cloud network is not a domain network.
    • Segmented.
    • Firewalled.
    • No domain authentication.
  • Standard enterprise DF/IR procedures:
    • May work well in the tenant space.
    • But not in the hosting environment.
Defending a Cloud

• Opportunities:
  • VM forensics.
  • Cloud resources.
  • Time.
  • Scale.
Defending a Cloud

• Virtual machine forensics.
  • Near perfect evidence:
    • Virtual disks are files on disk.
    • Guest physical address space.
  • Acquisition:
    • Saved states.
    • Snapshots.

VMs permit evidence acquisition that is not generally possible with physical machines.
Defending a Cloud

• Virtual machine forensics:
  • Virtual disk, differencing disk;
  • Deployment disk, as-found disk.

VHD as deployed  VHD at later time  Possible bad stuff.
Defending a Cloud

• Cloud resources:
  • Unlimited compute.
  • Unlimited storage.
  • Bandwidth.
• Cloud services:
  • Tables and databases;
  • Distributed processing;
  • Search.
• Geographical reach.

To defend a cloud, you need to use the cloud.
Defending a Cloud

• Time:
  • Remediation and stateless machines:
    • PAAS: a redeployment is a clean deployment.
    • DF/IR in a world of stateless machines?

Forensics answers questions. Is there a question to answer?
Defending a Cloud

• Time:
  • Ephemeral nature of assets and addresses.
  • Auditing and event logging provide durable evidence.

To defend a cloud, you must learn to think cloud.
Defending a Cloud

• Opportunities of Scale:
  • Machines have scores to thousands of identical twins.
  • Deployment.
  • Roles.
    • Role instances.
      • xyz-service-1_of_200
      • xyz-service-2_of_200
      • xyz-service-3_of_200
      • ...
      • xyz-service-256_of_200
Defending a Cloud

• Opportunities of Scale.
  • Deployment/Role/Role Instances:
    • Same OS VHD.
    • Same applications and Application VHD.
    • Same configuration and deployment settings.
    • Same hardware.
    • Same accounts.
    • Same function and intended use.
    • Same processes.
Defending a Cloud

• Opportunities of Scale.
  • Deployment/Role/*Role Instances*.  
    • Compare:
      • File properties—names, paths, dates, version, code signing, hash.  
      • Registry key value data and metadata.  
      • Accounts, account properties, and account activity.  
      • Loaded/running code or mapped files.  
      • *Events*.  

Defending a Cloud

• Logging at scale.
  • Process creation events (security event ID 4688):

<table>
<thead>
<tr>
<th>EventData</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SubjectUserSid</strong></td>
</tr>
<tr>
<td><strong>SubjectUserName</strong></td>
</tr>
<tr>
<td><strong>SubjectDomainName</strong></td>
</tr>
<tr>
<td><strong>SubjectLogonId</strong></td>
</tr>
<tr>
<td><strong>NewProcessId</strong></td>
</tr>
<tr>
<td><strong>NewProcessName</strong></td>
</tr>
<tr>
<td><strong>TokenElevationType</strong></td>
</tr>
<tr>
<td><strong>ProcessId</strong></td>
</tr>
<tr>
<td><strong>CommandLine</strong></td>
</tr>
</tbody>
</table>
Defending a Cloud

• Logging at scale.
  • Process creation events (security event ID 4688):
    • Subject User Account.
    • New Process Name (and path).
    • Token Elevation Type.
    • Parent Process.
    • Command Line.
  • What processes should run, how, by what account, and (sometimes) when.
Defending a Cloud

• Opportunities of Scale.
  • *Runtime, role-specific, event baselines.*
    • For any deployment:
      • *Cf.* Events from any role instance,
      • With events common to all role instances:
        = What should be normal; and
        = What is unique.
  • White listing
  • Hunting
Defending a Cloud

• Automating DF/IR:
  • Scale provides approximation of normal in operation.
  • Deviations from normal may be evidence of compromise.
  • Difference the individual against the herd.
  • Does a deviation indicate compromise?
Defending a Cloud

• Time!