Computer Forensics and Incident Response in the Cloud

SESSION ID: ANF-T07A

Stephen Coty
AlertLogic, Inc.
@Twitter AlertLogic_ACID
Why forensics in the cloud?

- Cloud market revenue will increase at a 36% annual rate, PR News
- Analysts expect AWS revenues to hit $6 billion - $10 billion in 2014
- Microsoft Azure to reach $1 billion in annual sales
- Oracle Cloud bookings increase by 35% in the 3rd quarter this year
- VDI (Desktop as a Service) market reached $13.4 billion in 2013
- Gartner predicts 60% of banking institutions to migrate to the cloud
What Attacks are hitting the Cloud Space

**Asia Honeypots**
- 85% MS-SQL Server
- 6% MySQL
- 4% MS-DS Service
- 4% RPC
- 1% HTTP
- 0% FTP
- 0% FTP

**US Honeypots**
- 51% MS-SQL Server
- 23% MySQL
- 12% HTTP
- 13% MS-DS Service
- 13% RPC
- 13% FTP

**Europe Honeypots**
- 35% MS-SQL Server
- 13% MySQL
- 13% HTTP
- 13% MS-DS Service
- 13% RPC
- 13% FTP

**Global Honeypots**
- 51% MS-SQL Server
- 10% MySQL
- 11% HTTP
- 12% MS-DS Service
- 8% RPC
- 8% FTP
When is digital forensics in the cloud required

- Investigation into organized cyber crimes
- Investigation into Acceptable Use Policy violations
- Data Recovery, Intentional or Accidental
- 3rd Party reports of suspicious activity
- Fraudulent builds for malicious activity
- Data Breaches

**WARNING**
---------------
Adults Only
Challenges with Digital Forensics in the Cloud

- Investigators do not have the physical control of the media nor the network.
- Massive database infrastructure uses customer relationship management systems and social graphs that current forensics cannot address.
- With the nature of cloud computing there are challenges with the chain of custody.
- Who owns the data and what is the expectation of privacy as a customer.
- Oregon State vs Bellar
  - Judge Timothy Sercombe wrote “Nor are a person’s privacy rights in electronically stored personal information lost because that data is retained in a medium owned by another.”
Why Digital Forensics will not work?

Challenges in Collection

- Seize servers containing files from many users creates privacy issues with others
- Trustworthiness of evidence is based on the cloud providers “word”
- Investigators are dependent on cloud providers to acquire evidence
- Technician collecting data may not be qualified for forensic acquisition
- Unknown location of the physical data can hinder investigations
Think Network Forensics, it’s the only way

- Traditional digital forensic data collection is still appropriate for many investigations.
- There is a growing number of cases, with the adoption of virtual technology and the cloud, where it is not practical or impossible to conduct digital forensics
- Relies on Limited data to examine
  - Captured Packets
  - Reviewing Log Data
  - Cloned Servers from Server Administrators
  - Looking for key words in parsed data
  - Reviewing any type of IDS or WAF event data
Understanding your Service Provider

Service Provider Responsibility

Foundation Services
- Compute
- Storage
- DB
- Network

Hosts
- Secure coding and best practices
- Software and virtual patching
- Configuration management
- Hardened hypervisor
- System image library
- Root access for customer

Apps
- Secure coding and best practices
- Software and virtual patching
- Configuration management
- Access management
- Application level attack monitoring

Networks
- Logical network segmentation
- Perimeter security services
- External DDoS, spoofing, and scanning prevented
- Network threat detection
- Security monitoring

Customer Responsibility
- Access management
- Patch management
- Configuration hardening
- Security monitoring
- Log analysis

- Root access for customer
- Access management
- Application level attack monitoring
- Network threat detection
- Security monitoring
Shared Customer and Service Provider Responsibility

- Enabling a logging solution of the virtual server
- Amazon Cloud has Cloud Trail that logs API calls to your instance
- Providing an IDS designed for the cloud can provide a level of protection and logging of security related events.
- Ability to perform deep packet forensics in a virtual environment
- Researchers have proposed various applications to conduct forensic memory analysis in virtual environments
- Multi Jurisdiction and multi-tenancy Service Level Agreements (SLA)
Forensic Process and tools in the Cloud

- Have Primary server relocated in the cloud
  - Keep compromised device online while you move the customer to a new instance
  - Have service provider take a “Snap Shot” of the compromised server
  - Run Forensic Investigation on the compromised device live

- Tools
  - WireShark – Collects Packets
  - Network Miner – Collects Data about the Host
Credits


Link to Ciphx and other Open Source Tools

- http://df.shsu.edu/ciphix.html