HEY! YOU! GET OFF MY CLOUD!
ATTACKS AGAINST CLOUD HONEYPOTS
Cloud Adoption

Choose two:

Fast  Cheap  Good
IaaS Cloud Security Layers

SECURE

- API / GUI
- Application Code
- Operating System
- Virtual Machine
- Hypervisor
- Device
- Network
- Facility

Your problem

Provider’s responsibility
Elastic Computing

Development

Low utilisation
Low cost

Deployment

Heavy utilisation
High cost
My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above $350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a $50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at $15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay.
Threat Types - Customers

Cloud Environment
- application-attack
- brute-force
- suspicious-activity
- recon
- trojan-activity
- denial-of-service
- other

On Premise Environment
- application-attack
- brute-force
- trojan-activity
- suspicious-activity
- recon
- denial-of-service
- other

Source: Alert Logic ASR 2015
Relative Threats - Cloud vs On Premise

- denial-of-service: 5
- suspicious-activity: 2
- recon: 2
- brute-force: 1
- application-attack: 1
- other: 1
- trojan-activity: 0

Source: Alert Logic ASR 2015
Cloud Threats by Customer Industry Vertical

Source: Alert Logic ASR 2015
Subtle Differences

Cloud threats ≠ On premise threats

Your threats ≠ Your neighbour’s threats
Honeypot Infrastructure

Cloud Honeypot

123.45.67.88
share.example.com

Cloud Production System

123.45.67.89
sys.example.com

123.45.67.90
db.example.com

Cloud Honeypot

Increased Protection

Threat Intelligence

threat intelligence

Threat Intelligence
Honeypot Types

Low Interaction
- Simulates high level services
- Collects basic information

Medium Interaction
- Simulates generic functions
- Records interaction

High Interaction
- Simulates specific environment
- Collects details of attack
Kippo – medium interaction

https://github.com/desaster/kippo

- Simulates SSH shell
- Fake file system
- Easily detected! – we use heavily modified version
- We used to log brute force attacks & replay session
Dionaea – medium interaction

http://dionaea.carnivore.it/

- Simulates network services
- SMB / HTTP / FTP / MySQL / SIP (VOIP)
- Simulates shellcode execution
- We see mostly SMB activity
Amun – low interaction

http://amunhoney.sourceforge.net/

- Modular Honeypot
- Simulates vulnerable services
- We see mostly SMB activity
Low Interaction

p0f – low interaction

http://amunhoney.sourceforge.net/

• Fingerprint connecting IPs
• Run in tandem
Custom Interaction

Create your own

- Modify modular honeypot
- Reflect your environment
- Respond to new threats
- Research attacks against specific vulnerabilities
What do we find?

April 2015
Findings – Top 20 IP Addresses

198.101.193.22
177.143.161.1
177.143.167.30
186.92.57.234
43.255.190.130
43.255.190.119
186.92.180.244
186.92.122.154
177.143.161.164
190.204.147.44
43.255.190.167
186.92.36.215
186.92.51.249
36.236.150.66
190.37.94.20
93.118.46.197
186.92.54.111
186.92.57.234
61.227.174.2
114.47.9.182
82.211.147.147

Number of Attacks
Findings – Top 20 Source Countries

- Japan
- Taiwan
- Venezuela
- China
- Brazil
- Georgia
- Unknown
- Romania
- United States
- Russian Federation
- Bulgaria
- Armenia
- Kazakhstan
- Ukraine
- Korea, Republic of
- Iran, Islamic Republic of
- Mexico
- Netherlands
- United Kingdom
- India
Findings – Attacker OS

- Linux 2.4.x
- Windows XP
- Linux 3.1-3.10
- Linux 2.2.x-3.x
- Windows 7 or 8
- Linux 2.6.x
- Linux 3.11 and newer
- Linux 2.4.x-2.6.x
- Linux 2.2.x-3.x (no timestamps)
- Linux 3.x
- Linux 2.2.x-3.x (barebone)
- Windows NT kernel
- Linux 2.0
Findings – Top 20 Destination Ports

- Secure Shell (SSH)
- Microsoft Directory Service
- Remote Desktop Protocol
- NETBIOS Session Service
- SMTP
- HTTP
- Active API Server Port (Proxy)
- Telnet
- POP3
- HTTP Alternate (Proxy)
- MySQL
- Microsoft SQL Server
- Abyss Web Server
- HTTPS
- FTP
- Socks (Proxy)
- Universal Plug 'N Play (UPnP)
- Microsoft DCOM
- IMAP
- Apple OSX RPC Services
Findings – Top 20 Brute Forced Usernames

- root (98.5%)
- admin
- ubnt
- user
- guest
- ubuntu
- operator
- PlcmSplp
- Administrator
- db01
Findings – Top 20 Brute Forced Username/Password

- root/admin
- admin/admin
- root/123654
- root/default
- root/zaq1xsw2
- root/a123456
- root/11111111
- root/changeme
- root/qwerty
- root/qwerty
- root/meiyoumima
- root/admin1
- root/123456]
- root/654321
- root/administrator
- root/qazwsx
- root/888888
- root/aaaaaa
- root/root
- root/159357
- root/meiyoumima
- root/vision
Findings – Top 20 Uploads

<table>
<thead>
<tr>
<th>Malware Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troj/Agent-AMRO</td>
<td>12</td>
</tr>
<tr>
<td>PsExec</td>
<td>7</td>
</tr>
<tr>
<td>Mal/HckPk-A</td>
<td>2</td>
</tr>
<tr>
<td>Mal/PWS-JJ</td>
<td>2</td>
</tr>
<tr>
<td>Mal/Spy-Y</td>
<td>2</td>
</tr>
<tr>
<td>Unknown</td>
<td>6</td>
</tr>
</tbody>
</table>

- **Troj/Agent-AMRO**
- **PsExec**
- **Mal/HckPk-A**
- **Mal/PWS-JJ**
- **Mal/Spy-Y**
- **Unknown**
Deployment

Honeypots in Operation
Honeypots for Managed Services

Connecting IPs

Cloud Honeypot

Customer Cloud System

Security Agent

Blocklist update

Threat Intelligence
Honeypots for Managed Services

- Malware
- Cloud Honeypot
- Customer Cloud System
  - Security Agent
  - Correlate
- Threat Intelligence
Cloud environments have a specific threat profile. Well placed honeypots provide timely intelligence. Apply intelligence to protect production systems.
Thank you

Will Semple – VP ActiveIntelligence
Brian Wilson – Director, Intelligence
Michael Laughlin – Tools Engineer
Thank you.