RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

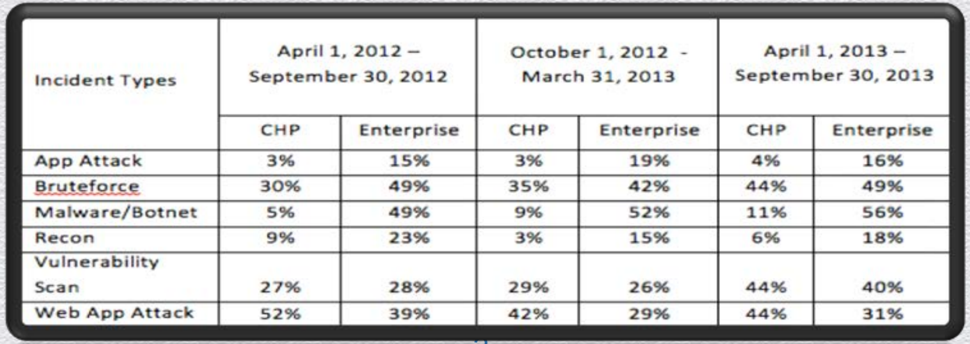
Computer Forensics and Incident Response in the Cloud

SESSION ID: ANF-T07A

Stephen Coty
AlertLogic, Inc.
@Twitter AlertLogic_ACID

Why forensics in the cloud?

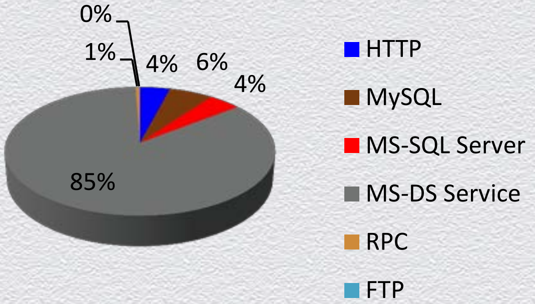
- Cloud market revenue will increase at a 36% annual rate, PR News
- Analysts expect AWS revenues to hit $6 billion - $10 billion in 2014
- Microsoft Azure to reach $1 billion in annual sales
- Oracle Cloud bookings increase by 35% in the 3rd quarter this year
- VDI (Desktop as a Service) market reached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



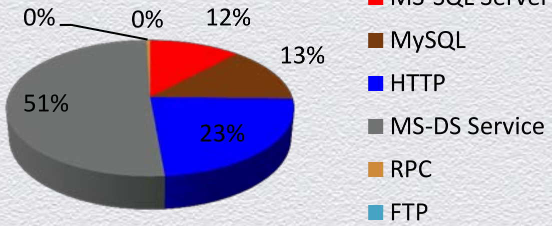
Incident Types	April 1, 2012 – September 30, 2012		October 1, 2012 - March 31, 2013		April 1, 2013 – September 30, 2013	
	CHP	Enterprise	CHP	Enterprise	CHP	Enterprise
App Attack	3%	15%	3%	19%	4%	16%
Bruteforce	30%	49%	35%	42%	44%	49%
Malware/Botnet	5%	49%	9%	52%	11%	56%
Recon	9%	23%	3%	15%	6%	18%
Vulnerability Scan	27%	28%	29%	26%	44%	40%
Web App Attack	52%	39%	42%	29%	44%	31%

What Attacks are hitting the Cloud Space

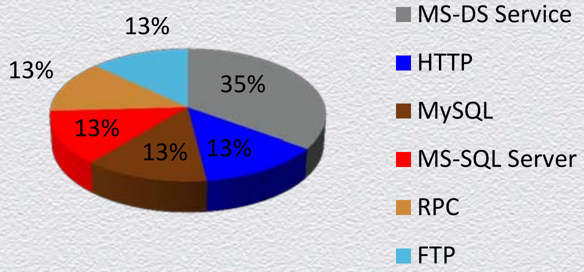
Asia Honeypots



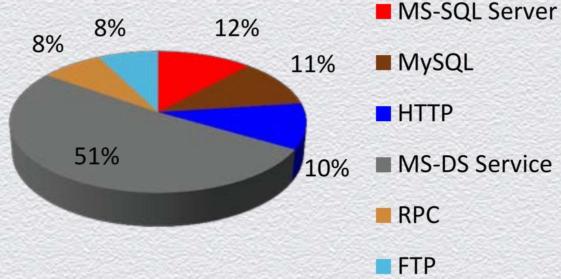
US Honeypots



Europe Honeypots

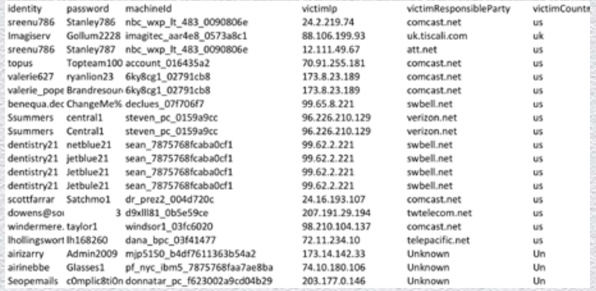


Global Honeypots

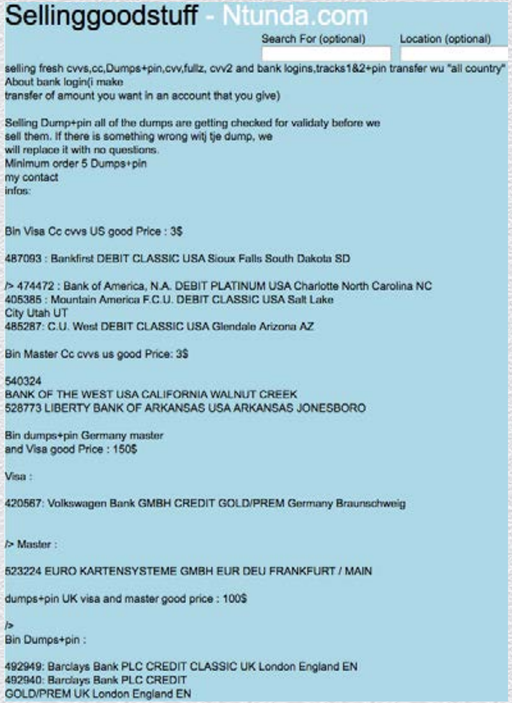


When is digital forensics in the cloud required

- 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



identity	password	machineId	victimIp	victimResponsibleParty	victimCount
sreenu786	Stanley786	nbc_wxp_lt_483_0090806e	24.2.219.74	comcast.net	us
Imagiserv	Gollum2228	imagitec_aar4e8_0573a8c1	88.106.199.93	uk.tiscali.com	uk
sreenu786	Stanley787	nbc_wxp_lt_483_0090806e	12.111.49.67	att.net	us
topus	Topteam100	account_016435a2	70.91.255.181	comcast.net	us
valerie627	ryanlion23	6ky8cg1_02791cb8	173.8.23.189	comcast.net	us
valerie_pope	Brandresoun	6ky8cg1_02791cb8	173.8.23.189	comcast.net	us
benequa.dec	ChangeMe%	declues_07f706f7	99.65.8.221	swbell.net	us
Ssummers	central1	steven_pc_0159a9cc	96.226.210.129	verizon.net	us
Ssummers	Central1	steven_pc_0159a9cc	96.226.210.129	verizon.net	us
dentistry21	netblue21	sean_7875768fcaba0cf1	99.62.2.221	swbell.net	us
dentistry21	jetblue21	sean_7875768fcaba0cf1	99.62.2.221	swbell.net	us
dentistry21	Jetblue21	sean_7875768fcaba0cf1	99.62.2.221	swbell.net	us
dentistry21	Jetbule21	sean_7875768fcaba0cf1	99.62.2.221	swbell.net	us
scottfarrar	Satchmo1	dr_prez2_004d720c	24.16.193.107	comcast.net	us
dowens@soı	3	d9xlll81_0b5e59ce	207.191.29.194	twtelecom.net	us
windermere.	taylor1	windsor1_03fc6020	98.210.104.137	comcast.net	us
lhollingswort	lh168260	dana_bpc_03f41477	72.11.234.10	telepacific.net	us
airizarry	Admin2009	mjp5150_b4df7611363b54a2	173.14.142.33	Unknown	Un
airinebbe	Glasses1	pf_nyc_ibm5_7875768faa7ae8ba	74.10.180.106	Unknown	Un
Seopemails	c0mplic8ti0n	donnatar_pc_f623002a9cd04b29	203.177.0.146	Unknown	Un



Sellinggoodstuff - Ntunda.com

Search For (optional) Location (optional)

selling fresh cvvs,cc,Dumps+pin,cvv,fullz, cvv2 and bank logins,tracks1&2+pin transfer wu "all country"
About bank login(i make
transfer of amount you want in an account that you give)

Selling Dump+pin all of the dumps are getting checked for validaty before we
sell them. If there is something wrong witj tje dump, we
will replace it with no questions.
Minimum order 5 Dumps+pin
my contact
infos:

Bin Visa Cc cvvs US good Price : 3$

487093 : Bankfirst DEBIT CLASSIC USA Sioux Falls South Dakota SD

/> 474472 : Bank of America, N.A. DEBIT PLATINUM USA Charlotte North Carolina NC
405385 : Mountain America F.C.U. DEBIT CLASSIC USA Salt Lake
City Utah UT
485287: C.U. West DEBIT CLASSIC USA Glendale Arizona AZ

Bin Master Cc cvvs us good Price: 3$

540324
BANK OF THE WEST USA CALIFORNIA WALNUT CREEK
528773 LIBERTY BANK OF ARKANSAS USA ARKANSAS JONESBORO

Bin dumps+pin Germany master
and Visa good Price : 150$

Visa :

420567: Volkswagen Bank GMBH CREDIT GOLD/PREM Germany Braunschweig

/> Master :

523224 EURO KARTENSYSTEME GMBH EUR DEU FRANKFURT / MAIN

dumps+pin UK visa and master good price : 100$

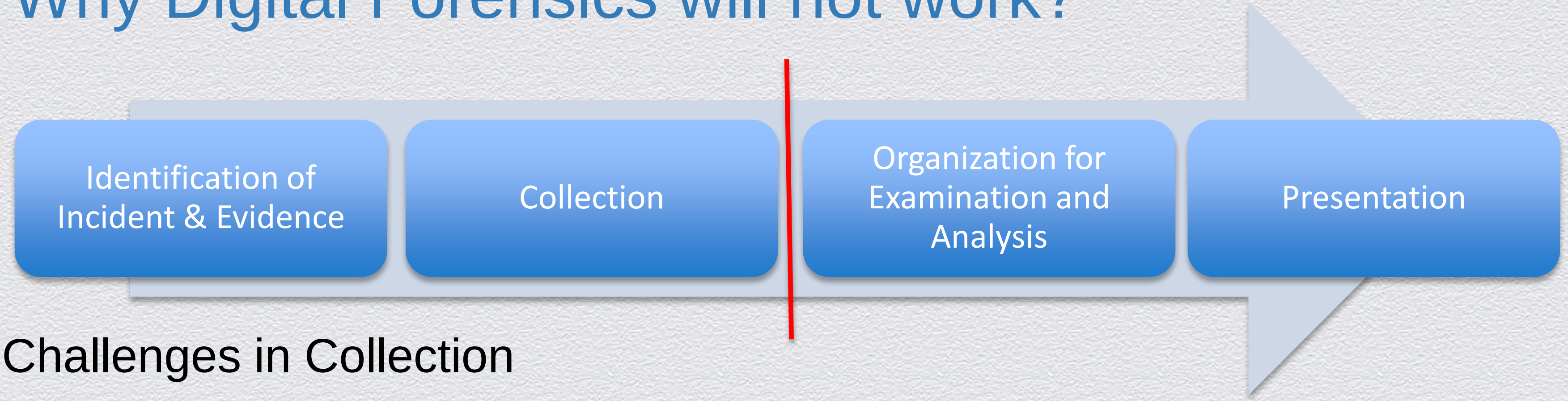
/>
Bin Dumps+pin :

492949: Barclays Bank PLC CREDIT CLASSIC UK London England EN
492940: Barclays Bank PLC CREDIT
GOLD/PREM UK London England EN

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?


Identification of Incident & Evidence

Collection

Organization for Examination and Analysis

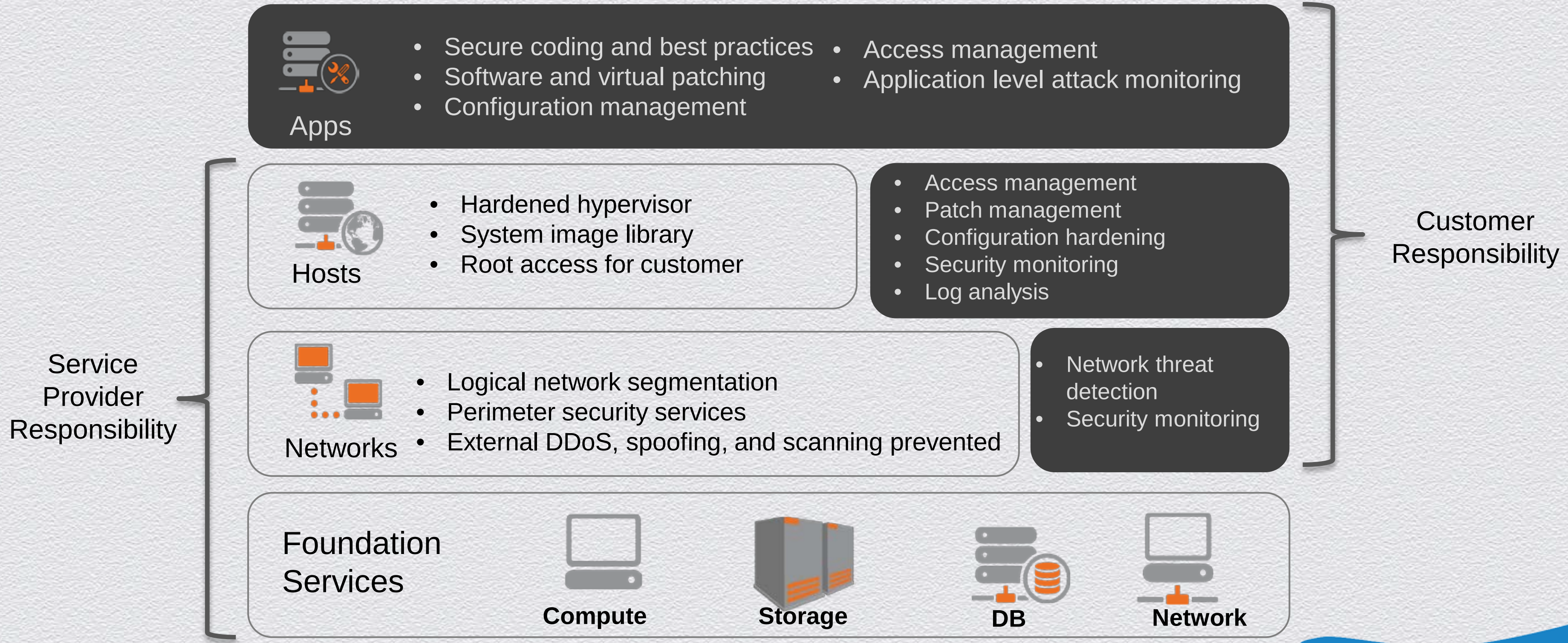
Presentation

- 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



Apps

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

Hosts

- Hardened hypervisor
- System image library
- Root access for customer

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

Networks

- Logical network segmentation
- Perimeter security services
- External DDoS, spoofing, and scanning prevented

- Network threat detection
- Security monitoring

Foundation Services

Compute

Storage

DB

Network

Service Provider Responsibility

Customer Responsibility

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

- http://www.securitywizardry.com/index.php/products/forensic-solutions/remote-forensics.html
- http://www.linkedin.com/pub/andrew-bennett/4/193/203
- https://www.asdreports.com/news.asp?pr_id=2116
- http://www.dfrws.org/2012/proceedings/DFRWS2012-10.pdf
- https://www.alertlogic.com/resources/cloud-security-report/

Link to Ciphx and other Open Source Tools

- http://df.shsu.edu/ciphix.html
- http://www.mcafee.com/us/downloads/free-tools/index.aspx

Q&A