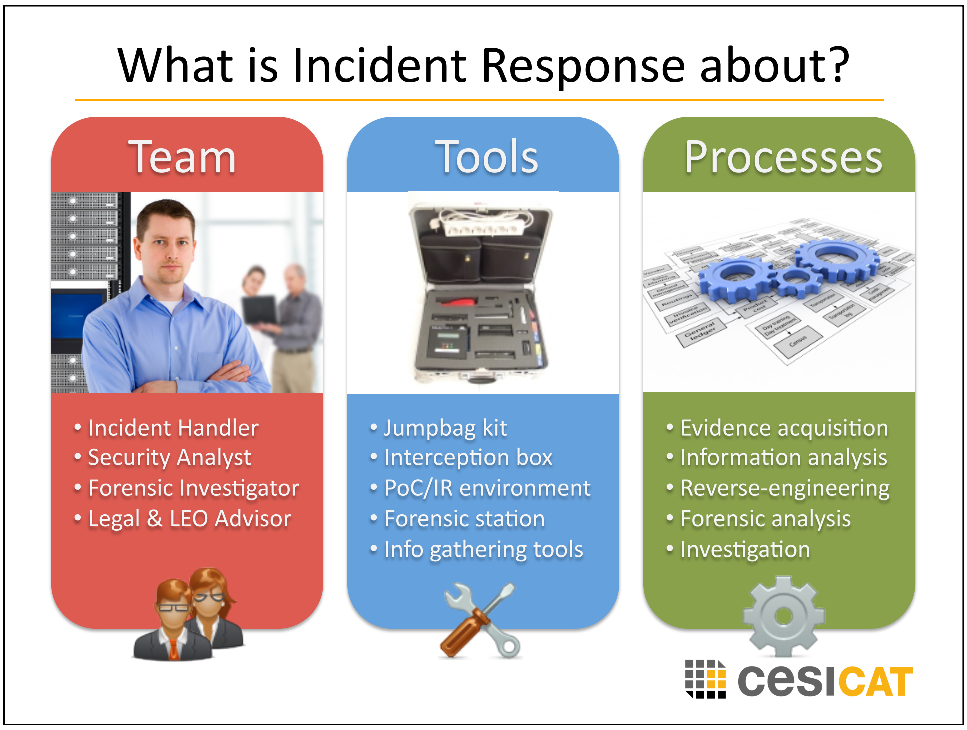
Incident Response!

... over the Clouds

Carles Fragoso Mariscal

ESNOG 6 · Madrid · 11-11-2010

cesiCAT



What is Incident Response about?

Team

- Incident Handler
- Security Analyst
- Forensic Investigator
- Legal & LEO Advisor

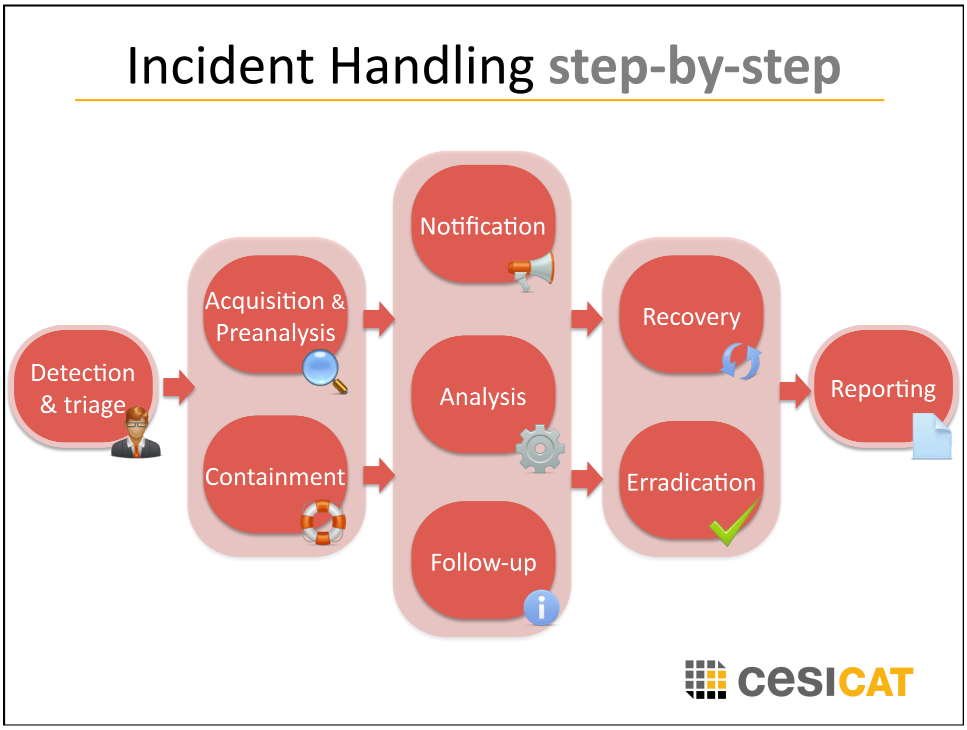
Tools

- Jumpbag kit
- Interception box
- PoC/IR environment
- Forensic station
- Info gathering tools

Processes

- Evidence acquisition
- Information analysis
- Reverse-engineering
- Forensic analysis
- Investigation

cesiCAT



Incident Handling step-by-step

Detection & triage

Acquisition & Preanalysis

Containment

Notification

Analysis

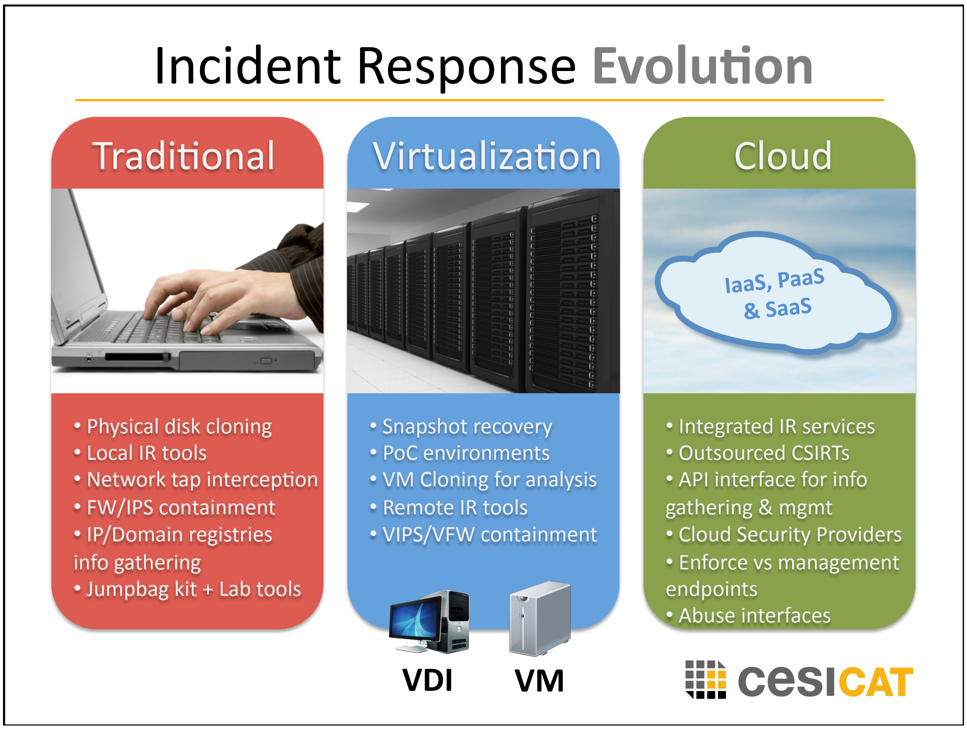
Follow-up

Recovery

Erradication

Reporting

How virtualization and Cloud Computing changed the way it works?



Incident Response Evolution

Traditional

- Physical disk cloning
- Local IR tools
- Network tap interception
- FW/IPS containment
- IP/Domain registries info gathering
- Jumpbag kit + Lab tools

Virtualization

- Snapshot recovery
- PoC environments
- VM Cloning for analysis
- Remote IR tools
- VIPS/VFW containment

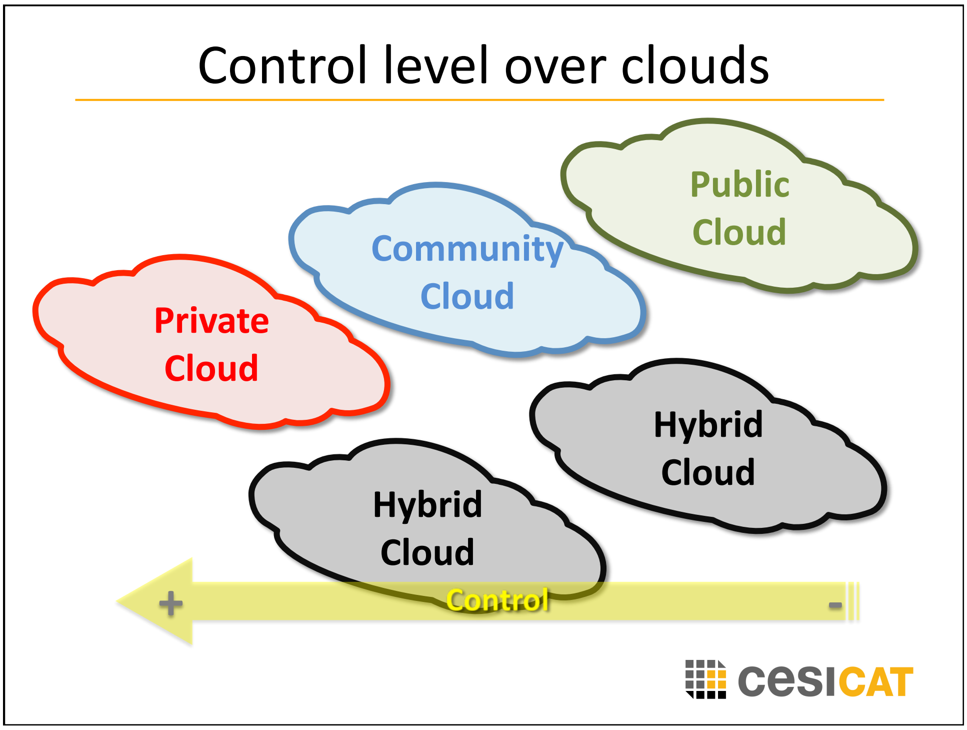
VDI VM

Cloud

IaaS, PaaS & SaaS

- Integrated IR services
- Outsourced CSIRTs
- API interface for info gathering & mgmt
- Cloud Security Providers
- Enforce vs management endpoints
- Abuse interfaces

cesiCAT



Control level over clouds

Private Cloud

Community Cloud

Public Cloud

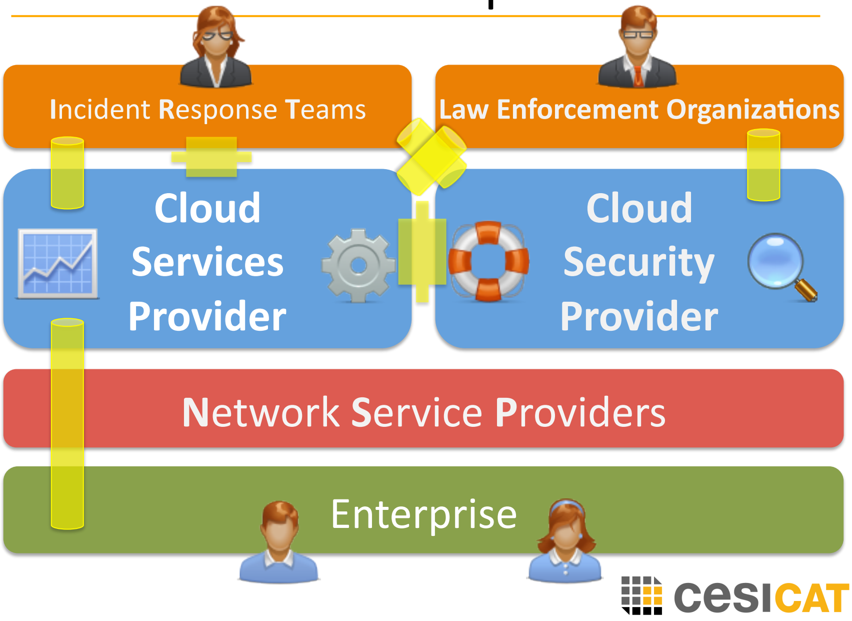
Hybrid Cloud

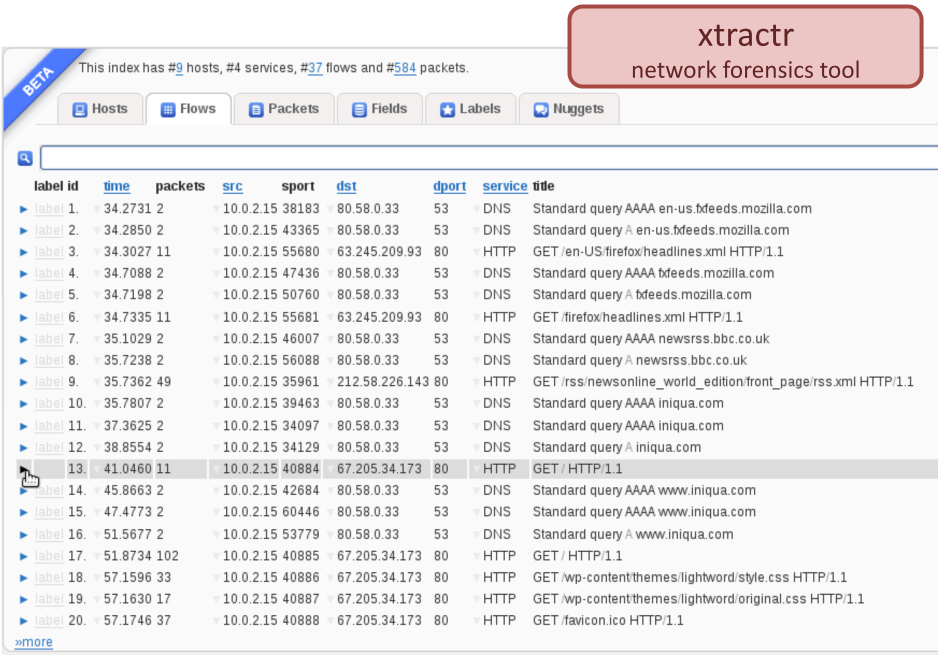
Hybrid Cloud

+ Control -

cesiCAT

Cloud Incident Response Puzzle



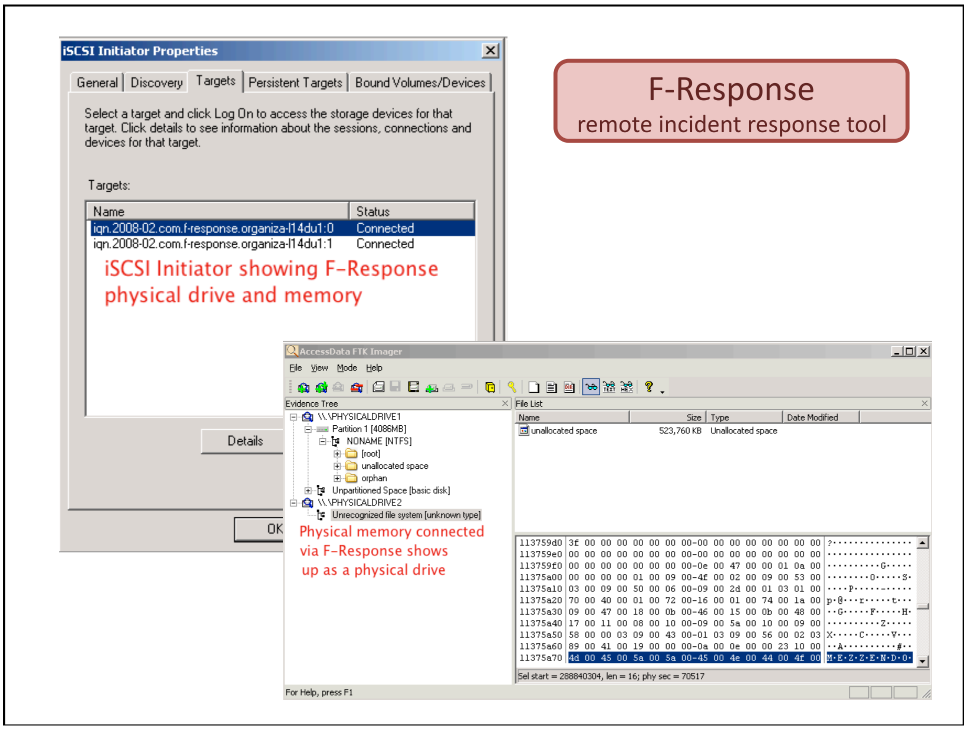


xtractr
network forensics tool

This index has #9 hosts, #4 services, #37 flows and #584 packets.

label	id	time	packets	src	sport	dst	dport	service	title
label	1.	34.2731	2	10.0.2.15	38183	80.58.0.33	53	DNS	Standard query AAAA en-us.fxfeeds.mozilla.com
label	2.	34.2850	2	10.0.2.15	43365	80.58.0.33	53	DNS	Standard query A en-us.fxfeeds.mozilla.com
label	3.	34.3027	11	10.0.2.15	55680	63.245.209.93	80	HTTP	GET /en-US/firefox/headlines.xml HTTP/1.1
label	4.	34.7088	2	10.0.2.15	47436	80.58.0.33	53	DNS	Standard query AAAA fxfeeds.mozilla.com
label	5.	34.7198	2	10.0.2.15	50760	80.58.0.33	53	DNS	Standard query A fxfeeds.mozilla.com
label	6.	34.7335	11	10.0.2.15	55681	63.245.209.93	80	HTTP	GET /firefox/headlines.xml HTTP/1.1
label	7.	35.1029	2	10.0.2.15	46007	80.58.0.33	53	DNS	Standard query AAAA newsrss.bbc.co.uk
label	8.	35.7238	2	10.0.2.15	56088	80.58.0.33	53	DNS	Standard query A newsrss.bbc.co.uk
label	9.	35.7362	49	10.0.2.15	35961	212.58.226.143	80	HTTP	GET /rss/newsonline_world_edition/front_page/rss.xml HTTP/1.1
label	10.	35.7807	2	10.0.2.15	39463	80.58.0.33	53	DNS	Standard query AAAA iniqua.com
label	11.	37.3625	2	10.0.2.15	34097	80.58.0.33	53	DNS	Standard query AAAA iniqua.com
label	12.	38.8554	2	10.0.2.15	34129	80.58.0.33	53	DNS	Standard query A iniqua.com
	13.	41.0460	11	10.0.2.15	40884	67.205.34.173	80	HTTP	GET / HTTP/1.1
label	14.	45.8663	2	10.0.2.15	42684	80.58.0.33	53	DNS	Standard query AAAA www.iniqua.com
label	15.	47.4773	2	10.0.2.15	60446	80.58.0.33	53	DNS	Standard query AAAA www.iniqua.com
label	16.	51.5677	2	10.0.2.15	53779	80.58.0.33	53	DNS	Standard query A www.iniqua.com
label	17.	51.8734	102	10.0.2.15	40885	67.205.34.173	80	HTTP	GET / HTTP/1.1
label	18.	57.1596	33	10.0.2.15	40886	67.205.34.173	80	HTTP	GET /wp-content/themes/lightword/style.css HTTP/1.1
label	19.	57.1630	17	10.0.2.15	40887	67.205.34.173	80	HTTP	GET /wp-content/themes/lightword/original.css HTTP/1.1
label	20.	57.1746	37	10.0.2.15	40888	67.205.34.173	80	HTTP	GET /favicon.ico HTTP/1.1

»more



F-Response
remote incident response tool

iSCSI Initiator Properties

Select a target and click Log On to access the storage devices for that target. Click details to see information about the sessions, connections and devices for that target.

Targets:

Name	Status
iqn.2008-02.com.f-response.organiza-l14du1:0	Connected
iqn.2008-02.com.f-response.organiza-l14du1:1	Connected

iSCSI Initiator showing F-Response physical drive and memory

AccessData FTK Imager

```
\\.\PHYSICALDRIVE1
  Partition 1 [4086MB]
    NONAME [NTFS]
      [root]
      unallocated space
      orphan
  Unpartitioned Space [basic disk]
\\.\PHYSICALDRIVE2
  Unrecognized file system [unknown type]
```

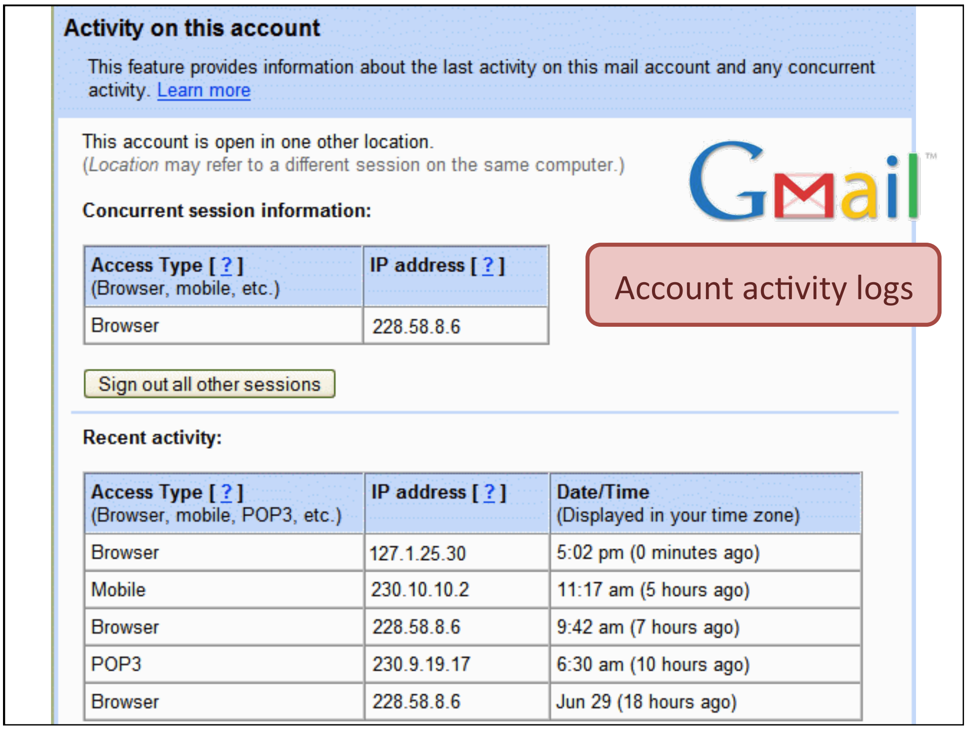
Physical memory connected via F-Response shows up as a physical drive

Name	Size	Type	Date Modified
unallocated space	523,760 KB	Unallocated space	

```
113759d0  3f 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ?···············
113759e0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ················
113759f0  00 00 00 00 00 00 00 00-0e 00 47 00 00 01 0a 00  ··········G·····
11375a00  00 00 00 00 01 00 09 00-4f 00 02 00 09 00 53 00  ········O·····S·
11375a10  03 00 09 00 50 00 06 00-09 00 2d 00 01 03 01 00  ····P·····-·····
11375a20  70 00 40 00 01 00 72 00-16 00 01 00 74 00 1a 00  p·@···r·····t···
11375a30  09 00 47 00 18 00 0b 00-46 00 15 00 0b 00 48 00  ··G·····F·····H·
11375a40  17 00 11 00 08 00 10 00-09 00 5a 00 10 00 09 00  ··········Z·····
11375a50  58 00 00 03 09 00 43 00-01 03 09 00 56 00 02 03  X·····C·····V···
11375a60  89 00 41 00 19 00 00 00-0a 00 0e 00 00 23 10 00  ··A··········#··
11375a70  4d 00 45 00 5a 00 5a 00-45 00 4e 00 44 00 4f 00  M·E·Z·Z·E·N·D·O·
```

Sel start = 288840304, len = 16; phy sec = 70517

For Help, press F1



Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. Learn more

This account is open in one other location.
(*Location* may refer to a different session on the same computer.)

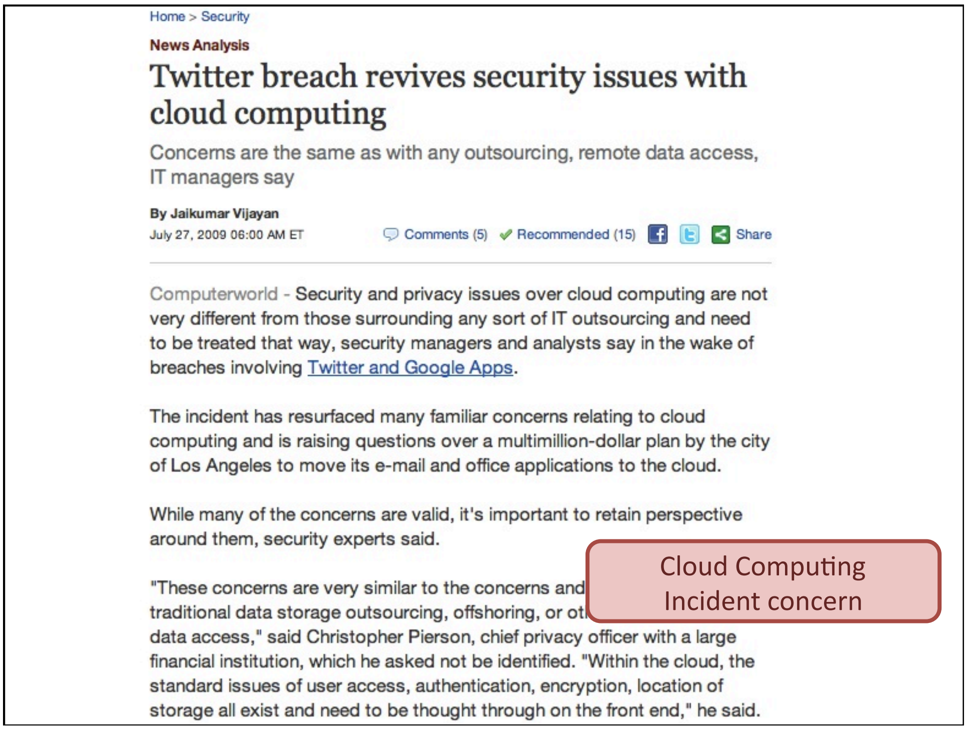
Concurrent session information:

Access Type [?] (Browser, mobile, etc.)	**IP address [?]**
Browser	228.58.8.6

Account activity logs

Recent activity:

Access Type [?] (Browser, mobile, POP3, etc.)	**IP address [?]**	**Date/Time** (Displayed in your time zone)
Browser	127.1.25.30	5:02 pm (0 minutes ago)
Mobile	230.10.10.2	11:17 am (5 hours ago)
Browser	228.58.8.6	9:42 am (7 hours ago)
POP3	230.9.19.17	6:30 am (10 hours ago)
Browser	228.58.8.6	Jun 29 (18 hours ago)



Home > Security

News Analysis

Twitter breach revives security issues with cloud computing

Concerns are the same as with any outsourcing, remote data access, IT managers say

By Jaikumar Vijayan
July 27, 2009 06:00 AM ET

Computerworld - Security and privacy issues over cloud computing are not very different from those surrounding any sort of IT outsourcing and need to be treated that way, security managers and analysts say in the wake of breaches involving Twitter and Google Apps.

The incident has resurfaced many familiar concerns relating to cloud computing and is raising questions over a multimillion-dollar plan by the city of Los Angeles to move its e-mail and office applications to the cloud.

While many of the concerns are valid, it's important to retain perspective around them, security experts said.

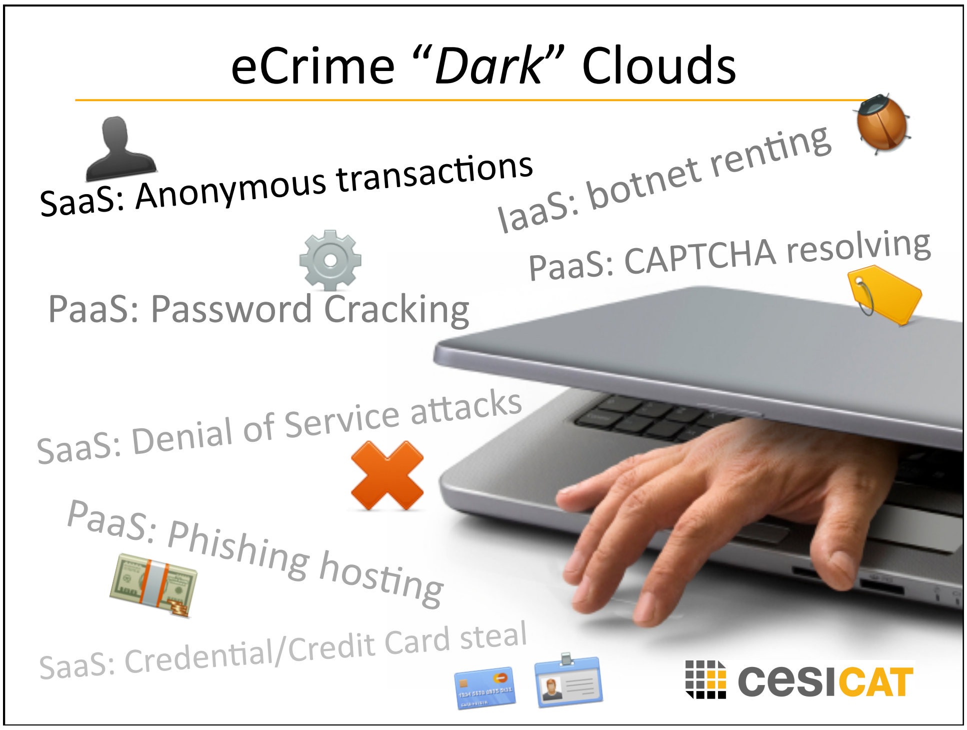
"These concerns are very similar to the concerns and traditional data storage outsourcing, offshoring, or ot data access," said Christopher Pierson, chief privacy officer with a large financial institution, which he asked not be identified. "Within the cloud, the standard issues of user access, authentication, encryption, location of storage all exist and need to be thought through on the front end," he said.

Cloud Computing
Incident concern

What about…

Dark Clouds

?



eCrime “*Dark*” Clouds

SaaS: Anonymous transactions

IaaS: botnet renting

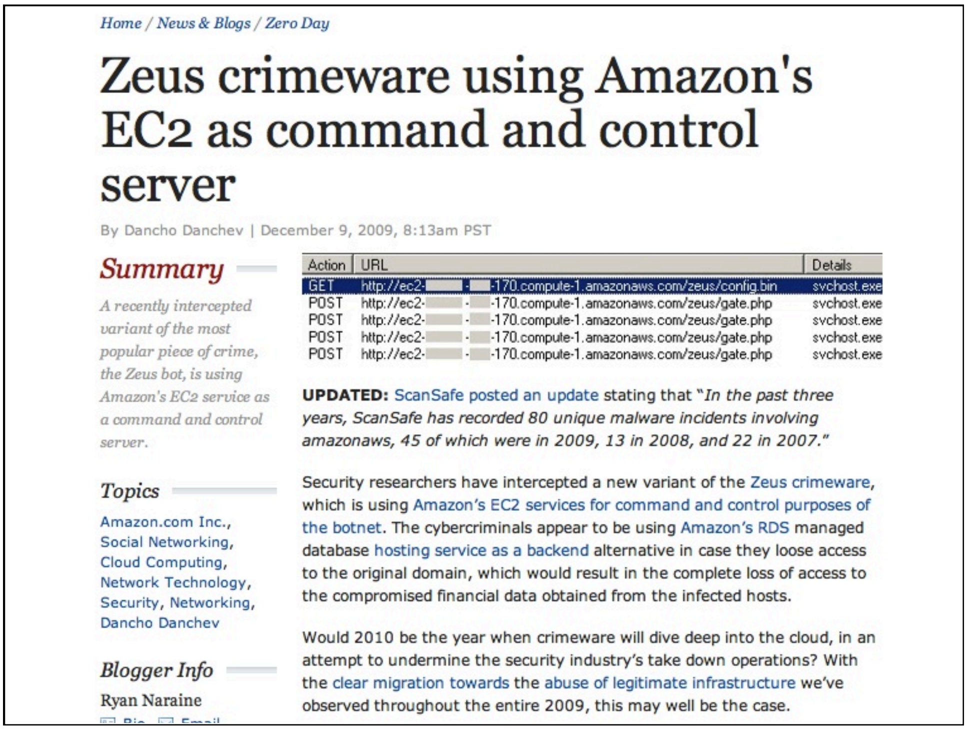
PaaS: CAPTCHA resolving

PaaS: Password Cracking

SaaS: Denial of Service attacks

PaaS: Phishing hosting

SaaS: Credential/Credit Card steal



Home / News & Blogs / Zero Day

Zeus crimeware using Amazon's EC2 as command and control server

By Dancho Danchev | December 9, 2009, 8:13am PST

Summary

A recently intercepted variant of the most popular piece of crime, the Zeus bot, is using Amazon's EC2 service as a command and control server.

Action	URL	Details
GET	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/config.bin	svchost.exe
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe
POST	http://ec2-[redacted]-[redacted]-170.compute-1.amazonaws.com/zeus/gate.php	svchost.exe

UPDATED: ScanSafe posted an update stating that “*In the past three years, ScanSafe has recorded 80 unique malware incidents involving amazonaws, 45 of which were in 2009, 13 in 2008, and 22 in 2007.*”

Security researchers have intercepted a new variant of the Zeus crimeware, which is using Amazon’s EC2 services for command and control purposes of the botnet. The cybercriminals appear to be using Amazon’s RDS managed database hosting service as a backend alternative in case they loose access to the original domain, which would result in the complete loss of access to the compromised financial data obtained from the infected hosts.

Would 2010 be the year when crimeware will dive deep into the cloud, in an attempt to undermine the security industry’s take down operations? With the clear migration towards the abuse of legitimate infrastructure we’ve observed throughout the entire 2009, this may well be the case.

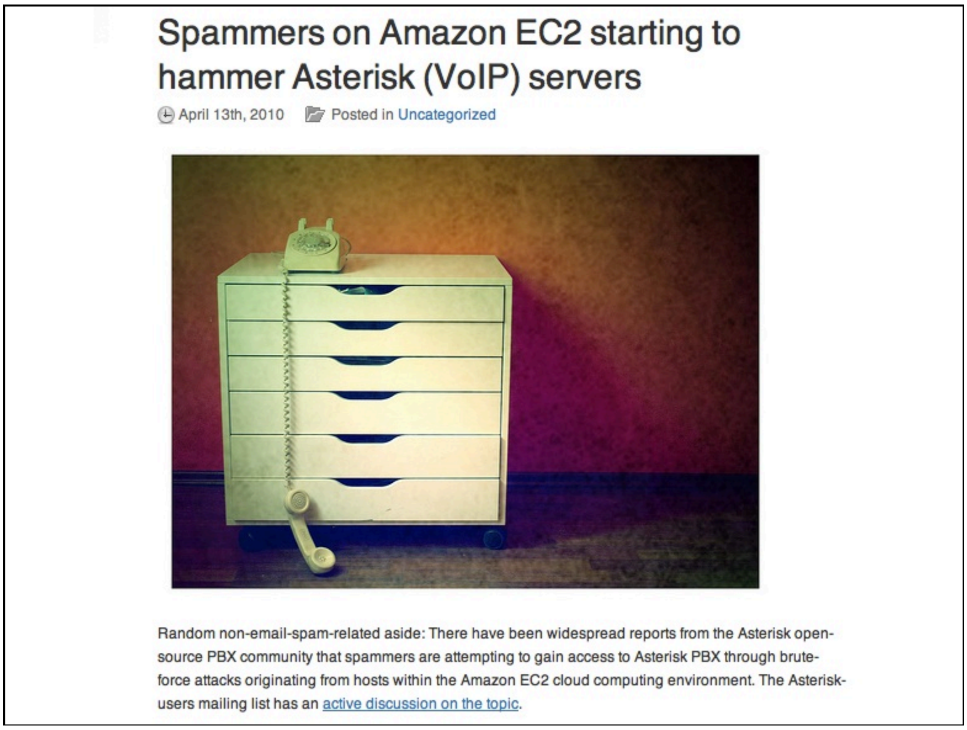
Topics

Amazon.com Inc., Social Networking, Cloud Computing, Network Technology, Security, Networking, Dancho Danchev

Blogger Info

Ryan Naraine

Bio Email



Spammers on Amazon EC2 starting to hammer Asterisk (VoIP) servers

April 13th, 2010 Posted in Uncategorized

Random non-email-spam-related aside: There have been widespread reports from the Asterisk open-source PBX community that spammers are attempting to gain access to Asterisk PBX through brute-force attacks originating from hosts within the Amazon EC2 cloud computing environment. The Asterisk-users mailing list has an active discussion on the topic.

cesiCAT

Helping to build a secure information society

info@cesicat.cat - www.cesicat.cat

Do not forget to follow us at your favourite social network…