



Hey You **GET OFF MY CLOUD !**


P0WN the CLOUD : The Good, the Bad, and The Pugly
Dan Hubbard, CTO Websense

Kind of, sort of, an Agenda

- ⦿ Do believe the hype!
- ⦿ Cloud / grids have been around for a long time but now CPU cycles and software along with virtualization we have a new game
- ⦿ Grids are popping up all over the place. Changing the IT game and a number of things. Hint: Future / Present : Remember the green screen?
- ⦿ Its centralized - distributed computing
- ⦿ What are these grids? How do they work? What is the danger? How can I use them for good or....evil?

Buzzzzzzz.....

Software via the Internet: Microsoft in 'Cloud' Computing



By JOHN MARKOFF
Published: September 3, 2007

Corrections Appended

SAN FRANCISCO, Sept. 2 — The empire is preparing to strike back — again.

SIGN IN TO EMAIL OR SAVE THIS

PRINT
SINGLE PAGE
REPRINTS

InfoWorld

Does Yahoo reorg signal cloud computing move?

Announcement of a cloud computing and data infrastructure group has some wondering if Yahoo plans to enter the market for hosted IT services like Google and Amazon

By Juan Carlos Perez, ICG News Service
June 27, 2008

Under fire from angry shareholders and rocked by a stream of high-profile executive departures, embattled Yahoo on Thursday announced another reorganization, one which includes the formation of a cloud computing and data infrastructure group. The move has some analysts speculating that Yahoo may have plans to enter the market for hosted IT services like Google and Amazon have done.

Free IT resource

Whatever your role, there's a Sun solution for your business.

Sponsored by Sun

Free IT resource

Microsoft: Smart Ways

IBM opens cloud computing centre in Africa

Firm steps up investment in growth markets

Written by Ian Williams
www.ibm.com 27 Jun 2008

IBM is announcing on the continent the formation of a new centre for cloud computing in Johannesburg, Africa.

Have your say | Send to a friend | Share

IBM is to open a cloud computing centre in Johannesburg enabling a range of services to share computing resources and bandwidth from any location on a range of devices.

Big Blue is also building a similar centre in China, the second of its kind in the country.

These centres will enable our clients to better embrace the services-based global economy

Nick Donofrio IBM

The shift to cloud computing has been fuelled by dramatic growth in business collaboration, connected devices, real-time data streams and web 2.0 applications, the company said.

August 23rd, 2006

Google CEO's new paradigm: 'cloud computing and advertising go hand-in-hand'

Posted by Donna Bogatin @ 6:07 am

Categories: [Business Models](#), [Web 2.0](#), [Advertising](#), [Search](#), [Government](#), [Marketing](#)

Tags:


2 TalkBacks
ADD YOUR OPINION

SHARE

PRINT

E-MAIL

WORTHWHILE? 0 VOTES

 Google CEO Eric Schmidt, Ph.D. in computer science, has gotten "advertising religion." Schmidt may be an electrical engineer by trade, but he has become a marketer by vocation.

Schmidt extolls a newfound power of advertising to fund "all of the software innovation."

At the Search Engine Strategies Conference earlier this month, Schmidt described the "old" client/server computing business model, which he characterizes as "largely invented by Oracle":

It was a direct sales force that would go in and sell complicated software to enterprises that they would integrate and do important business

The Cloud is getting Crowded !

- Top players today are Amazon AWS and GoGRID
- Big players coming in: IBM, VMWARE, Xen, Redhat, Microsoft, Sun, etc...

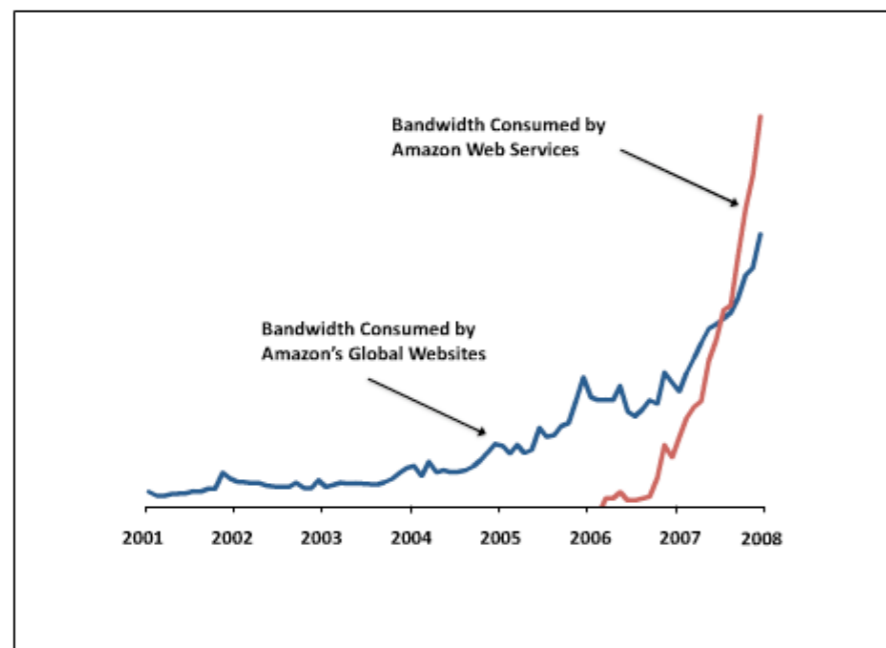
The screenshot displays two web pages side-by-side. On the left is the GoGrid website, featuring a navigation bar with 'How GoGrid Works', 'Pricing/Sign Up', and '24/7 Support'. The main heading is 'Control in the Cloud™' with a sub-headline 'GoGrid is the world's first multi-server control panel that allows you to deploy and scale load-balanced cloud server networks in minutes'. Below this is an illustration of servers and a database. A sidebar on the right mentions 'Award Win' and 'GUI | Windows'. A yellow starburst graphic advertises '\$50 FREE TRIAL'. At the bottom left of the screenshot is the 'websense' logo with the tagline 'ESSENTIAL INFORMATION PROTECTION™'. On the right is the Amazon AWS website, showing the 'amazon web services™' logo and a navigation menu with 'About AWS', 'Products', 'Solutions', 'Resources', 'Support', and 'Your Account'. The page title is 'Amazon Elastic Compute Cloud (Amazon EC2) BETA'. A 'Sign Up For Amazon EC2' button is visible. The main text describes Amazon EC2 as a web service for resizable compute capacity. A 'Related Services' section lists 'Amazon S3', 'AWS Premium Support', and 'Amazon DevPay'. At the bottom, a list of links includes 'Amazon EC2 Functionality', 'Service Highlights', 'Pricing', 'Resources', 'Detailed Description', and 'Intended Usage and Restrictions'.

Lots of uses....

- Some popular applications are web services, check into EC2's application they tout, and others.
- Also, centralized computing being used for applications
- Great for anything that needs a LOT of CPU cycles, memory, storage, etc..

Jeff Bezos, Founder of Amazon.com

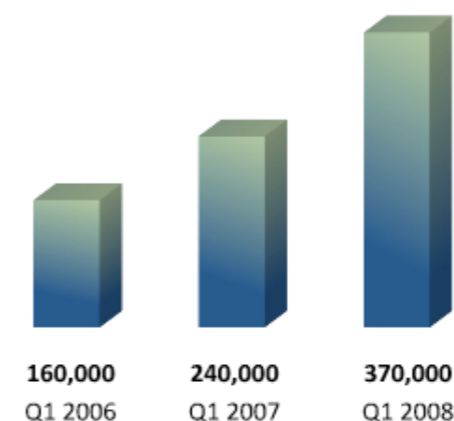
Jeff Bezos, Founder of Amazon.com, speaks at Startup School 2008



Jeff Bezos, Founder of Amazon.com

Jeff Bezos, Founder of Amazon.com, speaks at Startup School 2008

Registered AWS Developers



Fundamentals: What is good for business can be bad for security. No change here!

- Frictionless business systems
- Anonymity
- Anywhere, all the time, endless supply (pay per drink)
- Large systems, inexpensive, easy to use, 'virtually spotless'
- Free trials
- Little monitoring
- Sound familiar ? AKIN to some name registrations, but we are talking horse power here!



Frictionless Business Systems = Friction

Billing Summary ▼

09/22/2008 to 10/22/2008 i

Promotion Code: **GOGOTRIAL50**
 Credit Remaining: **\$ 50.00**

Memory Plan: Trial Grid
 Memory Allotment: 0 GB/Hrs
 Transfer Plan: Trial Grid
 Transfer Allotment: 0 GB

Memory

GB in Use: N/A
 GB Hours to Date: 0
 Monthly Projected GB Hrs: N/A
 Today's Overage GB Hrs: 0
 Today's Overage Charge: \$ 0.00

Transfer (GB)

Transfer to Date: N/A
 Projected Transfer: N/A
 Today's Transfer Overage: 0
 Today's Overage Charge: \$ 0.00

Account Activity

[view Previous Statement](#)

Summary of This Month's Activity as of September 24, 2008

Billing Cycle for this Report: September 1 - September 30, 2008

[Expand All](#) | [Collapse All](#)

Rate	Usage	Totals
Amazon Elastic Compute Cloud		
View/Edit Service		
\$0.10 per Small Instance (m1.small) Instance-hour (or partial hour)	4 Hrs	0.40
View Usage Report		0.40
Amazon Simple Storage Service		
View/Edit Service		
\$0.15 per GB-Month of storage used	0.722 GB-Mo	0.11
View Usage Report		0.11
Taxes		0.00
Estimated Taxes (Due October 1, 2008)		
Charges due on October 1, 2008+		0.51

† All charges for this billing cycle will be charged to your credit card on your next billing date, October 1, 2008. These charges include 1) next billing cycle's subscription charges due on the next billing date and 2) usage charges from the current billing cycle. Not included in the charges displayed here are any additional usage charges you will accrue this billing cycle. Visit the Amazon Web Services FAQs to learn more about web services pricing models and billing.

All web services are sold by Amazon Web Services LLC

Summary of Last Month's Statement

Billing Cycle for this Report: August 1 - August 31, 2008

[View Full Statement](#)

Total Charges **0.14**

Demo 1: Spinning up VM manually

- GoGrid login and spinning up...
- `file:///Users/websense/Desktop/presentations/p0wn_cloud/p0wn_gogrid_setup.mov`

Demo 1: Mmmmm. auto API's

- Web Service API's allow you to spin up VM's in near real-time!

The screenshot shows a web browser displaying the GoGrid API Wiki page for the endpoint `grid.server.add`. The page is titled "API" and includes a navigation bar with links for "page", "discussion", "view source", and "history". The main content area describes the `grid.server.add` endpoint, stating: "This call will add a single `server` object to your grid. This method follows a common add pattern." Below this, a "Request" section is shown with a "URL" subsection containing the endpoint: `https://api.gogrid.com/api/grid/server/add`. The page also features a sidebar with navigation links, a search box, and a "Contents" table of contents.

API

API

Welcome to the GoGrid API Wiki. Check out the Getting Started Guide below for an overview of the API. When you are ready to start coding take a look at the pages under Language Resources to see how to use the API in your favorite language.

Start Here

- Getting Started Guide
- Anatomy of GoGrid API Call
- Common API Call Patterns
- Download a GoGrid API Quick R

Language Resources

- Java
- bash

REST Interface

The GoGrid API is a REST-like Quer can be used to communicate over Python, Perl, Ruby, C#, or even shi

GOGRID WIKI

Log in / create account

API

grid.server.add

This call will add a single `server` object to your grid. This method follows a common add pattern.

Request

URL

- `https://api.gogrid.com/api/grid/server/add`

Contents [hide]

- 1 Start Here
- 2 Language Resources
- 3 REST Interface
- 4 API Methods

Contents [hide]

- 1 Request
 - 1.1 URL
 - 1.2 Role Based Access Control Permissions
 - 1.3 Input Request Query Parameters
 - 1.4 Sample Request
- 2 Response
 - 2.1 JSON Response
 - 2.2 XML Response
 - 2.3 CSV Response
 - 2.4 Error Codes

Shazam....zero to 16 in 15min!

The screenshot displays the GOGGRID web management interface. At the top, there are navigation links for "Grid", "My Account", "Support", and "Log Off". The main content area is divided into three sections: "Load Balancers", "Web/App Servers", and "Database Servers". Each section contains a grid of server icons, each labeled "own me". The "Load Balancers" section has 6 servers, "Web/App Servers" has 12 servers, and "Database Servers" has 4 servers. On the left side, there is a "Billing Summary" section for the period "09/22/2008 to 10/22/2008" with a promotion code "GOGOTRIAL50" and a credit remaining of "\$ 50.00". Below this is a "Network" section showing a public network with IP addresses ranging from 173.1.14.48 to 173.1.14.58. A green plus sign and the word "add" are visible next to the billing summary.

Spinning up EC2

```
#!/usr/bin/perl -w
use strict;

# number of instances wanted
my $instances = 1;

# Ubuntu 8.04 image ID
my $image = "XXXXXXX";

# local keypair file
my $auth_keys = "XXXXXXX";

# set environments for EC2
my $PATH = $ENV{PATH};
my $SEC2_HOME = "/usr/local/websense/blueshift/ec2/ec2-api-tools-1.3-19403";

$ENV{EC2_PRIVATE_KEY} = "~/.ec2/XXXXXXX.pem";
$ENV{EC2_CERT} = "~/.ec2/cert-XXXXXXXXXXXXXXXXXXXXX.pem";
$ENV{EC2_HOME} = $SEC2_HOME;
$ENV{PATH} = "$PATH:$SEC2_HOME/bin";
$ENV{JAVA_HOME} = "/usr";

# below is just for testing to make sure everything works
#my $out = `ec2-describe-images -o self -o amazon | grep machine`;
#print "$out\n";

open (FILE, ">/tmp/instances");

# build VMs
for (my $i = 0; $i < $instances; $i++)
{
    my $out = `ec2-run-instances $image -k $auth_keys`;
    $out =~ s/.*\nINSTANCE\t(i-\w+)\tami.*//;
    print "EC2 image $1 created\n";
    print FILE "$1\n";
}
}
```

⊙ How many VM's (20 per account unless U r special)

⊙ What image and keys

⊙ Report on success!

Spinning up...doing damage...tearing down

🕒 file:///Users/websense/Desktop/presentations/p0wn_cloud/p0wn_ec2.mov

Service	Operation
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances
AmazonEC2	RunInstances



The screenshot shows the 'Account Activity' page for a billing cycle ending on September 24, 2008. It lists usage for Amazon Elastic Compute Cloud (2.51 units) and Amazon Simple Storage Service (0.11 units). Taxes are listed as 0.00, and charges due on October 1, 2008, are 2.62.

Account Activity

[View Previous Statement](#)

Summary of This Month's Activity as of September 24, 2008

Billing Cycle for this Report: September 1 - September 30, 2008

[Expand All](#) | [Collapse All](#)

		Totals
+ Amazon Elastic Compute Cloud	View/Edit Service	
	View Usage Report	2.51
+ Amazon Simple Storage Service	View/Edit Service	
	View Usage Report	0.11
Taxes		
Estimated Taxes (Due October 1, 2008)		0.00
Charges due on October 1, 2008+		2.62

† All charges for this billing cycle will be charged to your credit card on your next billing date, October 1, 2008. These charges include 1) next billing cycle's subscription charges due on the next billing date and 2) usage charges from the current billing cycle. Not included in the charges displayed here are any additional usage charges you will accrue this billing cycle. Visit the Amazon Web Services FAQs to learn more about web services pricing models and billing.

This is pretty cool! What is the problem?

- ⦿ Pseudo code...
- ⦿ `/bin/pseudocode>`
 - ⦿ `blacklist = false`
 - ⦿ `while blacklist = true; do`
 - ⦿ *spin up new virtual machine with new IP address*
 - ⦿ *change DNS resolver to match*

With power comes responsibility...or NOT

- Some Grids have default no Firewalls inbound!
- Incident response teams ???
- SSH simple pass / auth on all systems
- How about Grid Hijacking? Key Guessing? Social Engineering? Phishing for Grid credentials?
- How long can one go under the radar in this frictionless system?

Onslaught of fake Microsoft patch spam

Date:06.30.2008

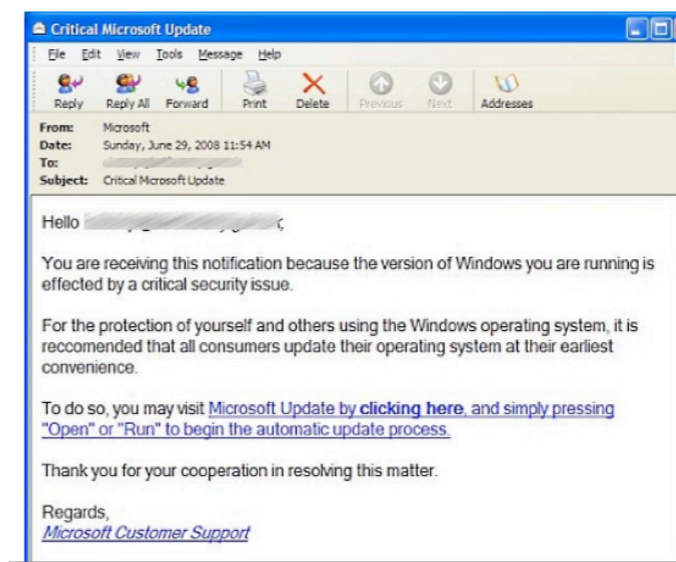
Threat Type: Malicious Web Site / Malicious code

BOOKMARK THIS ALERT

digg | del.icio.us | reddit
newsvine | furl | technorati

Websense® Security Labs™ ThreatSeeker™ Network has discovered a substantial number of spam messages utilizing a reliable social engineering trick that lures users to download a Microsoft critical security update.

The intercepted emails typically look like the following:



If I only had my own grid....

- ⦿ Password Cracking
- ⦿ Key / Authentication Cracking
- ⦿ Key / Crypto Creation, random file creation / modification
- ⦿ Storing large amounts of other peoples information for small amounts of \$\$\$ or nothing
- ⦿ DDOS (less likely but could do some damage for small amount of time)
- ⦿ Hosting Phishing, Malicious Code, binary files, etc...
- ⦿ Web Service to register infections and update
- ⦿ Captcha Farms

Danger Will Danger!

- ⦿ Perhaps one could “in theory” perform MITM attacks on the grid and own machines / grids, etc...
- ⦿ What is you could escape your VM !
- ⦿ Eavesdropping could be possible
- ⦿ Possible compromise could allow someone to silently watch traffic, redirect users, etc..
- ⦿ How about data tainting if you compromise their cloud

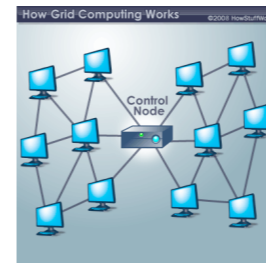
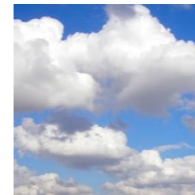
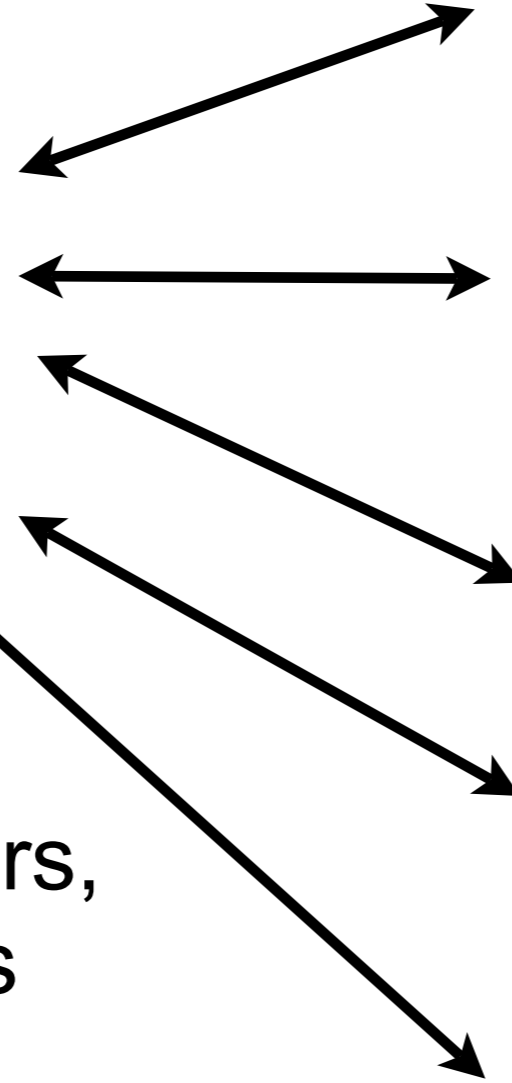
Best Defense is a GOOD OFFENSE!

- ⦿ Cracking code, crypto, etc.
- ⦿ Image analysis farm
- ⦿ Large corpus abstraction / correlation / scoring
- ⦿ Fuzzing / Vuln research
- ⦿ Movie / Animation analysis
- ⦿ Large data sets for link analysis, de-compilation, static analysis
- ⦿ Large data set behavior analysis, code analysis, comparison across large sample sets
- ⦿ Distributing HoneyClients

Honeyclient Distribution

- ⦿ Continual cat and mouse game as attackers maintain blacklist of who we are and where we come from (note: not just for security...lots of content is changed based on who you are)
- ⦿ Cloud distribution is economical way to distribute clients without the need for infrastructure
- ⦿ Current IP space is known of common cloud providers but they are adding IP space and distributing also. This is a bigger problem for their customers. As people virtualize apps, etc, it will be harder to know if its a VM or a “real” machine
- ⦿ Currently mine > 190M per day in distributed manner

Honeyclient Distribution (how)



Data Miner
Clusters

Data Miner
Clusters

Data Miner
Clusters

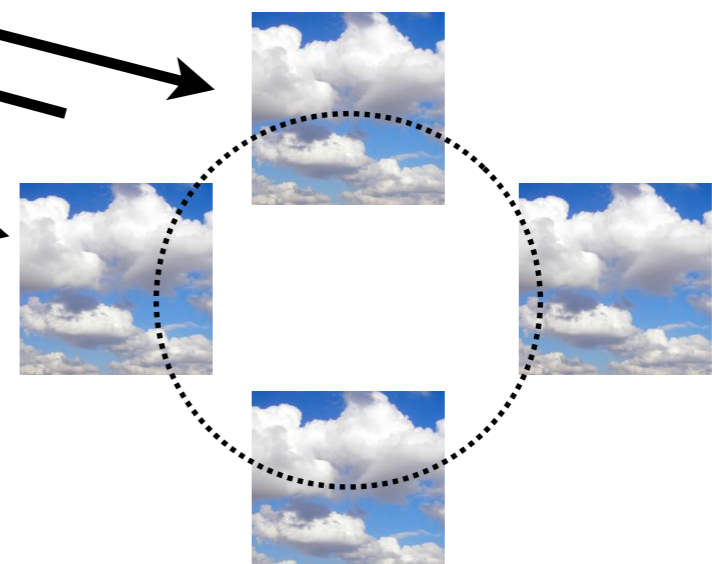
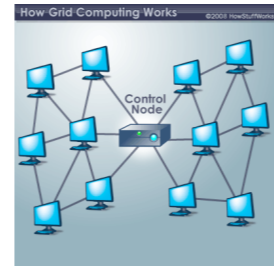
Grid/Cloud Clusters

Controller, Dispatchers,
Reporting, Analysis

Honeyclient Distribution (how)



Screenshot of Email:
Welcome to the American Airlines AAdvantage(R) program, the first and largest loyalty program in the world! We are proud to inform you that today June 23 2008 AmericanAirlines.com launch a new reward program. Please log in to your American Airlines account and take the 5 questions survey. For your effort you will be rewarded with \$50.
Your 50 dollars bonus code is AA-001NDX-2008ND22. Please log in to: <http://aa.americanairlines.com/bonus/> and follow the steps.
Thank you very much for your help and your patient and hope you will enjoy the American Airlines reward program in the future.
Sincerely,
American Airlines Reward Department
Please do not reply to this auto-answer message.
Discover the rewards that come with AAdvantage membership and start earning miles toward AAdvantage elite status today. Members can also earn miles at more than 1,500 participating companies including:
* over 20 participating airlines
* leading hotel chains
* car rental agencies
* credit/debit cards
* dining
* financial services
* retail and gifts
* telecommunications companies
* vacations and cruises



test again at another time to see if its content is still there

HoneyClient Distribution: Uses

- *Evasion: We are being blacklisted*
 - If access results = “suspicious” then ... spin up X, etc..
- *Load / More results faster: Zero-day out, web worm, BIG phish outbreak*
 - If load = XX then spin up 50 additional clients
- *Geography specific content delivery: Geo-based attack*
 - If site location = Y , then spin up client y in geography Z
- *Fail-over and redundancy: Systems down or we are being DDOS'd*
 - If network A = down then spin up VM cluster B
- *Extra processing needed: We need more horsepower!*
 - Add to test corpus, run against large sample set for analysis, add to confirmed corpus, re-tune classifier, release
 - If binary file, static analysis, test sigs, compare to LARGE FP corpus, test against heuristics, re-tune heuristic, test against product performance

Honeyclient Distribution / Stats



Allows you to start/stop Blueshift2 process, or stop process on any machine.

Process	Status
Blueshift2 Process	● ● ● ●

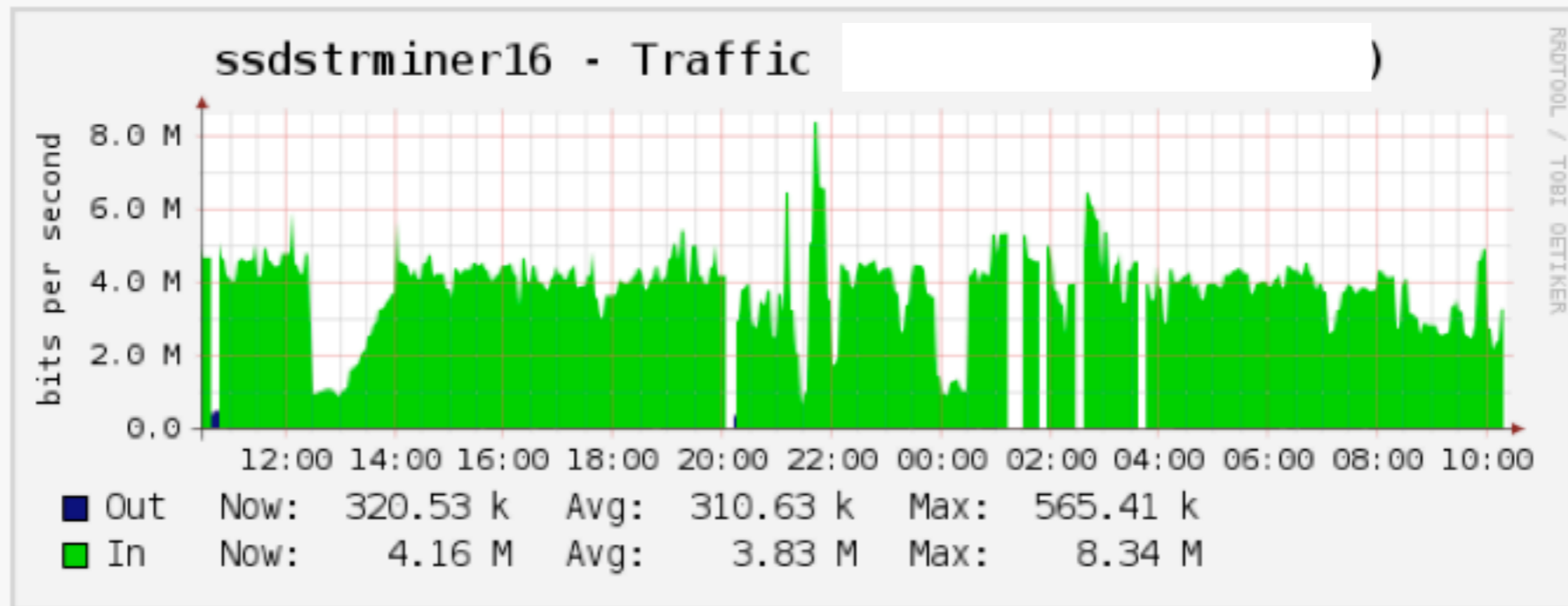
dns servers		
Machine Name	Type	Machine Status
ssdstrdns1	dns	● ● ● ●

control servers		
Machine Name	Type	Machine Status
ssdstrblshft1	control	● ● ● ●

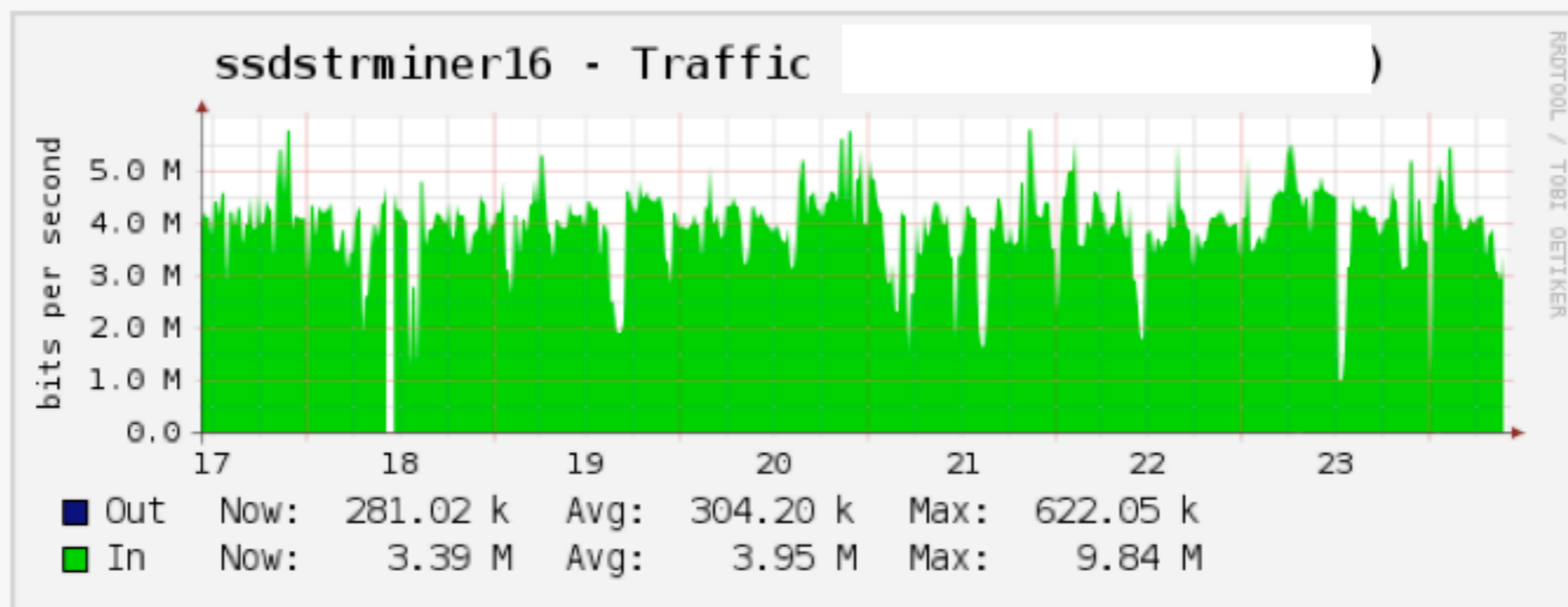
miner servers		
Machine Name	Type	Machine Status
miner10-blueshift	miner	● ● ● ●
miner11-blueshift	miner	● ● ● ●
miner12-blueshift	miner	● ● ● ●
miner14-blueshift	miner	● ● ● ●
miner15-blueshift	miner	● ● ● ●
miner7-blueshift	miner	● ● ● ●
miner8-blueshift	miner	● ● ● ●
miner9-blueshift	miner	● ● ● ●
ssdstrminer1	miner	● ● ● ●
ssdstrminer13	miner	● ● ● ●
ssdstrminer16	miner	● ● ● ●
ssdstrminer17	miner	● ● ● ●
ssdstrminer18	miner	● ● ● ●
ssdstrminer19	miner	● ● ● ●
ssdstrminer2	miner	● ● ● ●
ssdstrminer20	miner	● ● ● ●
ssdstrminer21	miner	● ● ● ●
ssdstrminer22	miner	● ● ● ●
ssdstrminer3	miner	● ● ● ●
ssdstrminer4	miner	● ● ● ●

Honeyclient Distribution / Stats

Traffic - 10.64.49.116 (eth0)



Daily (5 Minute Average)



Weekly (30 Minute Average)

Honeyclient Distribution / Stats

Blueshift^2 Weather

Submission Stats | URLs/sec | URLs Processed | Bytes | URL Status

@ Week Overview

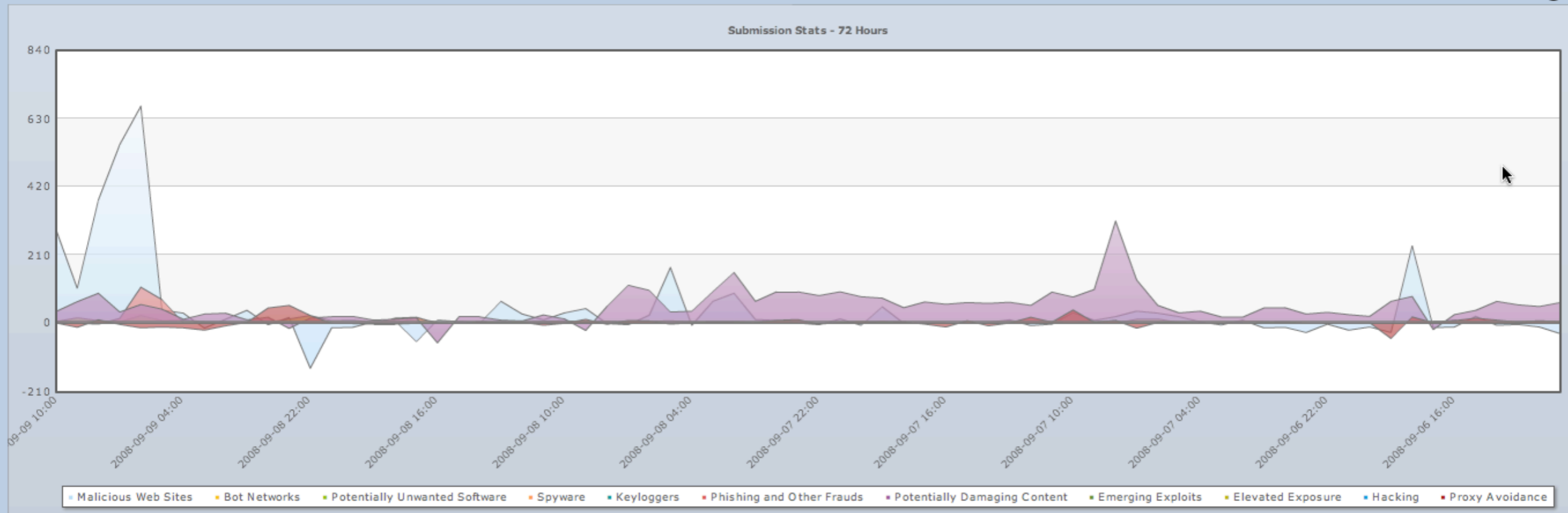
page 1 of 14 (97 rows) > >>

Add Date	URLs	Xfer Size	Xfer Rate	Miner Time	Avg URL/s	Total URL/s
2008-09-24	51.8 M	0.52 TB	551.5 KB/s	12 days + 17:38:53	53.79	1,972.41
2008-09-23	127.9 M	1.60 TB	519.2 KB/s	44 days + 17:39:24	39.49	1,482.03
2008-09-22	135.9 M	1.55 TB	518.2 KB/s	43 days + 3:45:57	44.66	1,576.68
2008-09-21	139.0 M	1.53 TB	511.0 KB/s	44 days + 18:37:51	45.01	1,613.02
2008-09-20	139.1 M	1.63 TB	548.2 KB/s	43 days + 0:49:35	45.74	1,612.43
2008-09-19	133.9 M	1.58 TB	528.9 KB/s	44 days + 4:28:47	43.47	1,550.29
2008-09-18	134.1 M	1.58 TB	533.1 KB/s	43 days + 9:57:4	44.20	1,552.40

Submission Stats | URLs/sec | URLs Processed | Bytes | URL Status

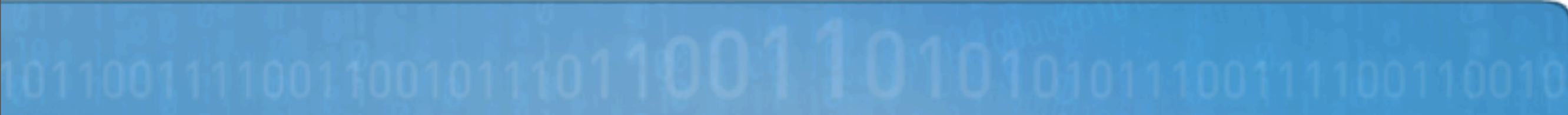
@ C Submission Stats

<< < page 6 of 31 (2163 rows) > >>



I am out of time : Conclusion...

- ⦿ Cloud / Grid computing is here to stay and is only going to get more popular
- ⦿ We need to assess the risk of the shift in models
- ⦿ Is your marketing department making VM's?
- ⦿ Attackers will look to the cloud just like researchers will
- ⦿ Cloud / Grid can be very useful for security research
- ⦿ Cloud / Grid can be very powerful for security products also
- ⦿ Do some research. Try them out, its will cost VERY little and I guarantee you will find your own use
- ⦿ Note: Watch EULA changes and AUP for Grid's and dont run with scissors, you may DDOS the GRID yourself



QUESTIONS ?