

Cloud IDS

Intrusion Detection for Shared Hosting

Josh Pyorre

OpenDNS

Security Analyst

Previously:

Threat Analyst at NASA

Threat Analyst at Mandiant

Cloud Hosting

- Convenient
- Cheap
- Common

Security features

What kind of people would do this?

Why bother?

Hacked websites are used for phishing



Stats

Online, valid phishes

30,768

Total Submissions

3,156,797

Total Votes

11,463,012

Phishes Verified as Valid

Total:

1,777,180

Online:

30,771

Offline:

1,746,409

Suspected Phishes Submitted

Total:

3,157,209

Online:

33,678

Offline:

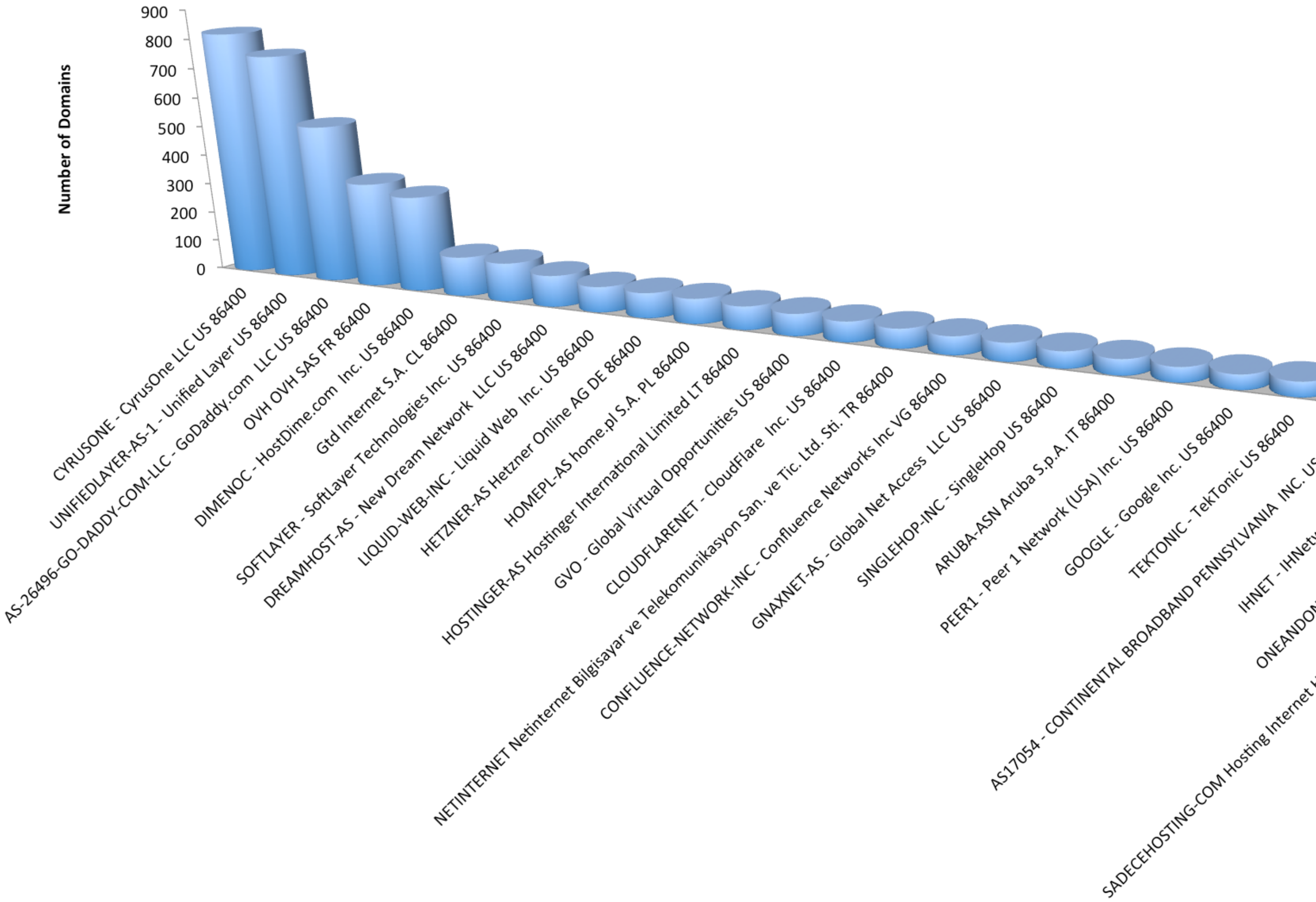
3,123,221

```

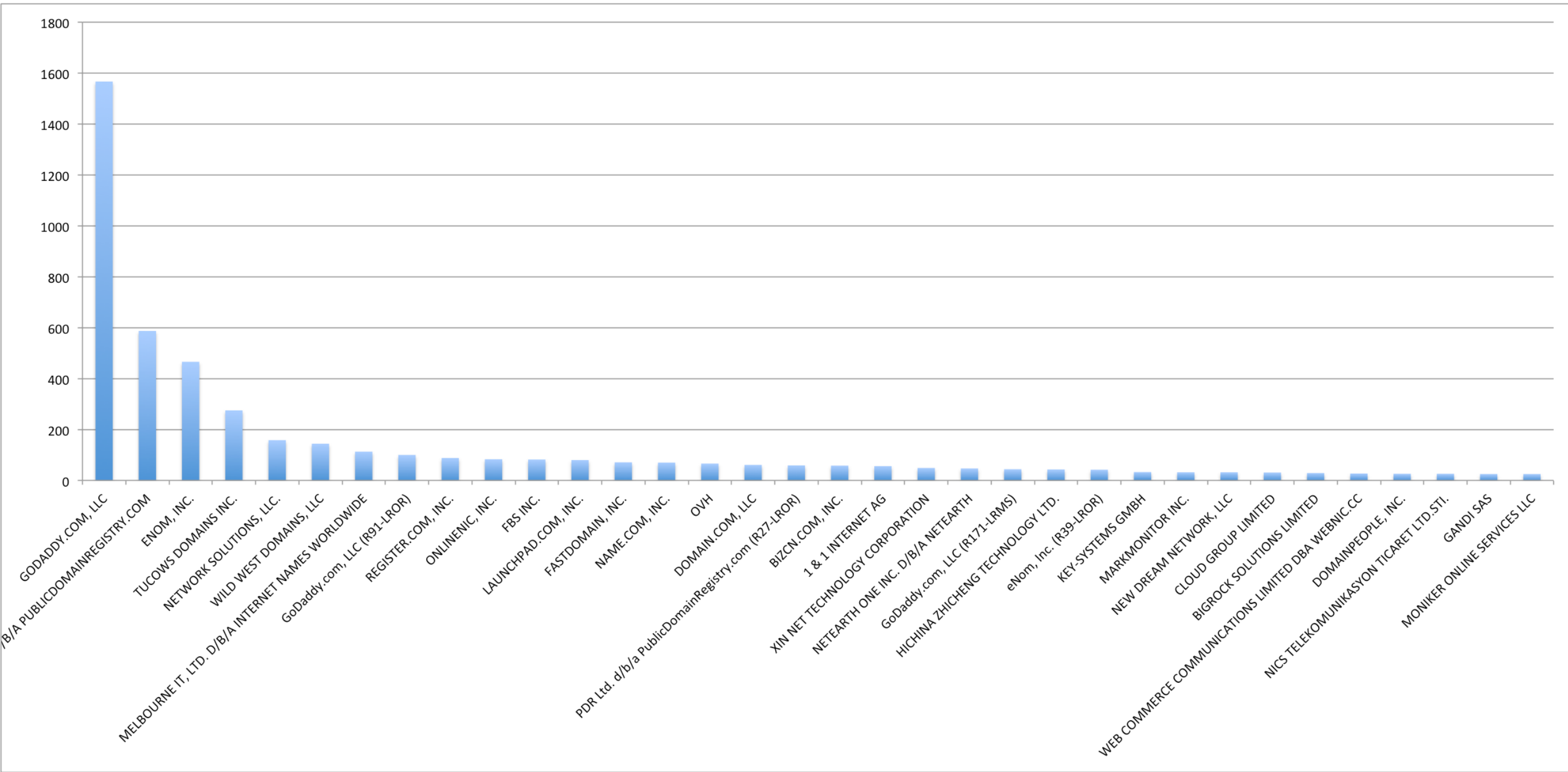
1
2 123NET - 123.Net
3 180SERVERS - 180Servers.com
4 1TELECOM SERVICOS DE TECNOLOGIA EM INTERNET LTDA
5 24SHELLS - 24 SHELLS
6 3M-HDQ-AS - 3M Company
7 4-RWEB - 4RWEB
8 A. P. OLIVEIRA & CIA. INFORMATICA LTDA.
9 A1COLO-COM - A1COLO.COM
10 A2HOSTING - A2 Hosting
11 AAMRA-NETWORKS-AS-AP aamra networks limited
12 AAPT AAPT Limited
13 AARNET-AS-AP Australian Academic and Research Network (AARNet)
14 ABCOM-AS ABCOM Shpk
15 ABCONNECT AB CONNECT
16 ABOUTIT-ONLINE
17 ABOVENET - Abovenet Communications
18 ABQG - New Mexico Lambda Rail
19 ACCELERATED-IT Accelerated IT Services GmbH
20 ACCESSKENYA-KE ACCESSKENYA GROUP LTD is an ISP serving
21 ACEDATACENTERS-AS-1 - Ace Data Centers
22 ACENS_AS acens Technologies
23 ACS-SK-AS ACS Ltd.
24 ACTIVE-SERVERS Dennis Rainer Warnholz trading as active-servers.com
25 ACTIVEHOST-RU-AS Activehost RU Ltd.
26 ADANET-TR ADA-NET Internet ve Iletisim Hizmetleri Tic. A.S.
27 ADDD2NET-COM-INC-DBA-LUNARPAGES - Lunar Pages
28 ADELPHIA-AS2 - Time Warner Cable Internet LLC
29 ADF01 - EBOUNDHOST.com
30 ADHOST - Adhost Internet Advertising
31 ADK-AS-AP AS Data(Hong Kong)Limited
32 ADMONET-LLC - Admo.net LLC
33 ADNET-TELECOM SC AD NET MARKET MEDIA SRL
34 ADSNET TELECOM LTDA ME
35 ADVANCED1 - Advanced Cable Communications
36 ADVANCEDHOSTERS-AS Haldex ltd
37 AECF-AS - American Eagle Computer Products
38 AEROTEK-AS Aerotek Bilisim Taahhut Sanayi ve Ticaret Limited Sirketi
39 AFRANET AFRANET Co. Tehran
40 AGARIK-NETWORK AGARIK SA
41 AGAVA3 Agava Ltd.
42 AGUIARI E AGUIARI PROVEDOR DE INTERNET
43 AI-NET Ai Networks Limited
44 AIRCEL-IN Aircel Ltd.
45 AIRNET-HB-AS-AP NOW
46 AIRSTREAMCOMM-NET - Airstream Communications
47 AIRTELBROADBAND-AS-AP Bharti Airtel Ltd.
48 AIS-WEST - American Internet Services
49 AIST CJSC AIST
50 AITNET - Advanced Internet Technologies
51 AKAMAI-AS - Akamai Technologies
52 AKAMAI-ASN1 Akamai International B.V.
53 AKNET Educational and Science Network
54 ALABANZA-BALT - Alabanza
55 ALASTYR Alastyr Telekomunikasyon A.S.
56 ALCHEMYNET - Alchemy Communications

```

Hosting Providers (by ASN) with Phishing Domains



Top Registrars for Domains used in Phishing Attacks



★★★★★

hackeado por **HighTech Brazil HackTe**

h4x0r3d por *CrazyDuck*

n0s s0m0s

[@byCrazyDuck - @synchr0nlze - @Thiago_0k]
[s2] Lua (@luanerocha)



[+] Hacked By Xranger Super [+]



★★★★★

Hacked by KkK1337

by **KkK1337**

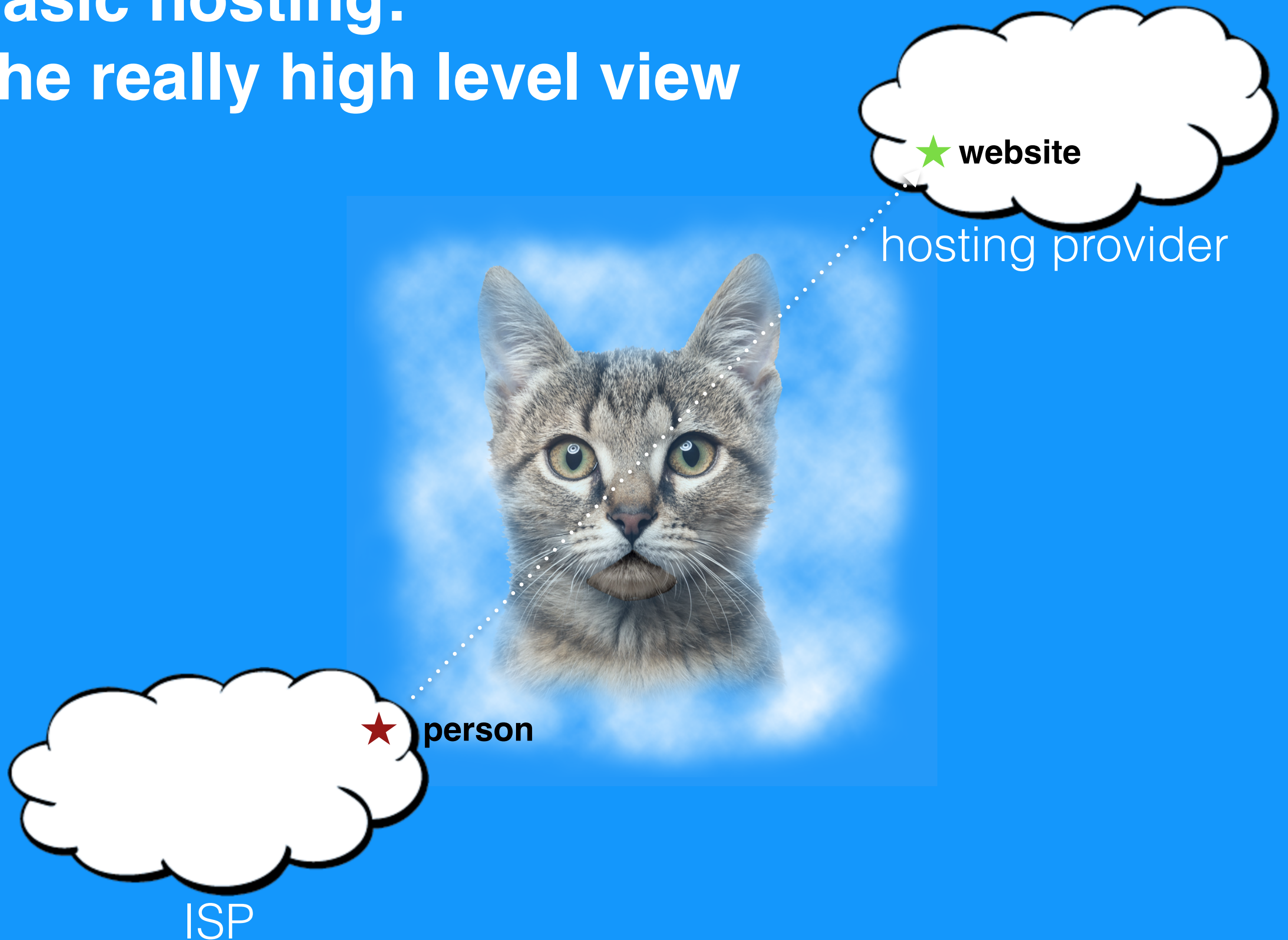


SCARY CLOWN!!!

WordPress Vulnerabilities

Version	Added	Title
4.0	2014-11-20	WordPress <= 4.0 - Long Password Denial of Service (DoS)
4.0	2014-11-25	WordPress <= 4.0 - CSRF in wp-login.php Password Reset
4.0	2014-11-30	WordPress <= 4.0 - Server Side Request Forgery (SSRF)
4.0	2014-11-30	WordPress 3.9, 3.9.1, 3.9.2, 4.0 - XSS in Media Playlists
3.9.2	2014-09-17	WordPress 3.4.2 - 3.9.2 Does Not Invalidate Sessions Upon Logout
3.9.2	2014-11-20	WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
3.9.2	2014-11-20	WordPress <= 4.0 - Long Password Denial of Service (DoS)
3.9.2	2014-11-25	WordPress <= 4.0 - CSRF in wp-login.php Password Reset
3.9.2	2014-11-30	WordPress <= 4.0 - Server Side Request Forgery (SSRF)
3.9.2	2014-11-30	WordPress 3.9, 3.9.1, 3.9.2, 4.0 - XSS in Media Playlists
3.9.1	2014-09-16	WordPress 3.9 & 3.9.1 Unlikely Code Execution
3.9.1	2014-09-16	WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing
3.9.1	2014-09-16	WordPress 3.0 - 3.9.1 Authenticated Cross-Site Scripting (XSS) in Multisite
3.9.1	2014-09-16	WordPress 3.6 - 3.9.1 XXE in GetID3 Library
3.9.1	2014-09-17	WordPress 3.4.2 - 3.9.2 Does Not Invalidate Sessions Upon Logout
3.9.1	2014-11-20	WordPress 3.0-3.9.2 - Unauthenticated Stored Cross-Site Scripting (XSS)
3.9.1	2014-11-20	WordPress <= 4.0 - Long Password Denial of Service (DoS)
3.9.1	2014-11-25	WordPress <= 4.0 - CSRF in wp-login.php Password Reset
3.9.1	2014-11-30	WordPress <= 4.0 - Server Side Request Forgery (SSRF)
3.9.1	2014-11-30	WordPress 3.9, 3.9.1, 3.9.2, 4.0 - XSS in Media Playlists
3.9	2014-09-16	WordPress 3.9 & 3.9.1 Unlikely Code Execution
3.9	2014-09-16	WordPress 2.0.3 - 3.9.1 (except 3.7.4 / 3.8.4) CSRF Token Brute Forcing

Basic hosting: The really high level view



Basic hosting:
The really high level view

Hacker version!



Exactly the same

Let's hack

...the Slider Revolution Wordpress plugin

Dashboard

Posts

Media

Pages

Comments

Appearance

Plugins

Installed Plugins

Add New

Editor

Users

Tools

[WordPress 4.1.1](#) is available! [Please update now.](#)

Plugins [Add New](#)

Plugin activated.

All (1) | [Active \(1\)](#)

Bulk Actions

Apply

☐

Plugin

Description

☐

Revolution Slider

Revolution Slider - Premium res

[Deactivate](#) | [Edit](#)

Version 3.0.95 | By [ThemePunch](#)

☐

Plugin

Description

Bulk Actions

Apply

[illegible]

WPScan

@WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart


[+] Finished: Tue Apr 14 18:15:55 2015

Video of an attack on my website hosted on Hostgator. The attack is not successful because Hostgator uses Mod_security, an Apache module.

- mod_security!
- We have no idea

The Neighborhood!



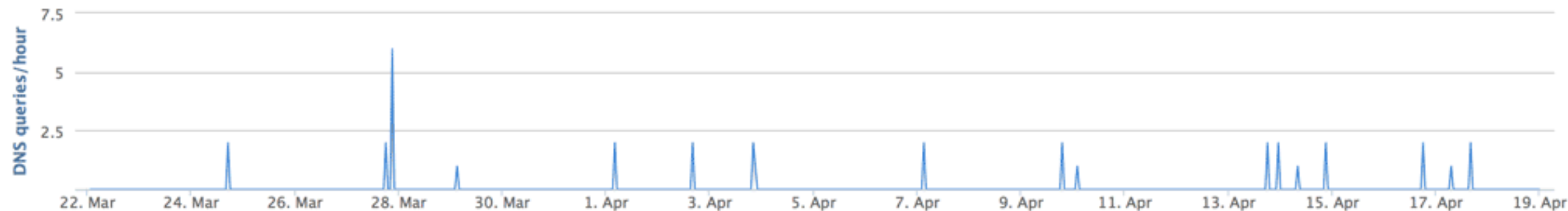
 Abandoned Building
Cause: Too many deaths

Hostgator

Details for jpyorre.com

This domain has IPs listed in 3rd-party threat intelligence databases

DNS queries



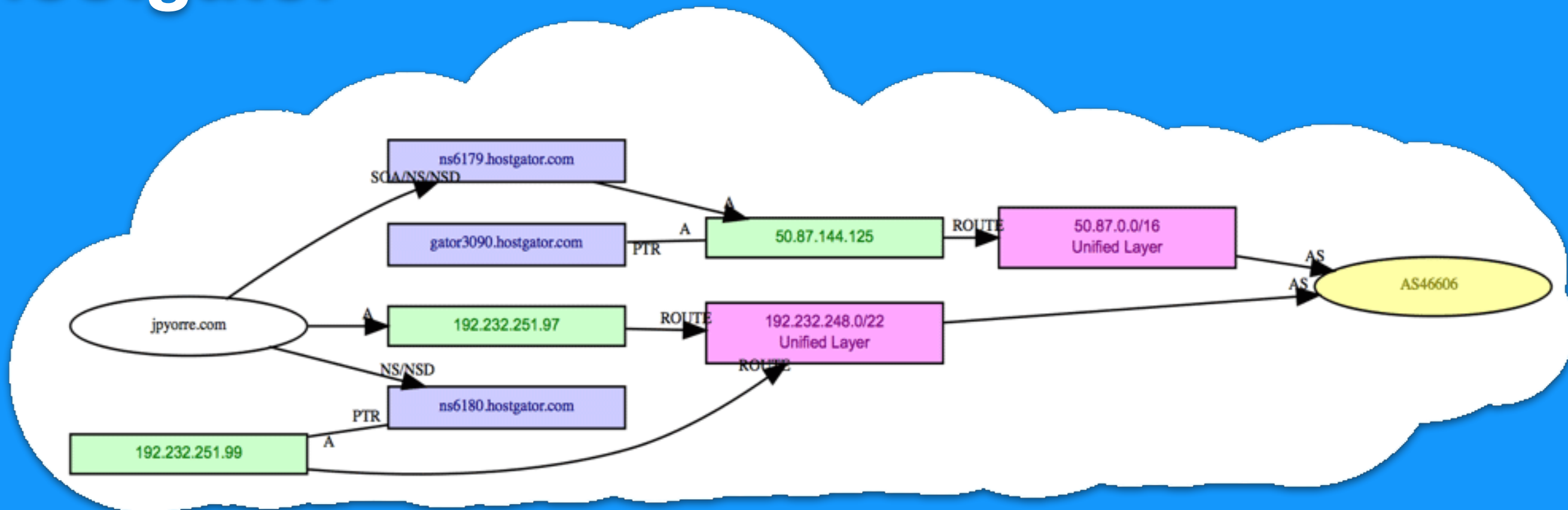
3rd-party threat intelligence

IP	Last update	Direction	Description	Source
192.232.251.97	2/18/15	outbound	Malware Domain	http://reputation.alienvault.com/reputation.data

IP addresses

First seen	Last seen	IPs
2/18/15	4/19/15	192.232.251.97 (TTL: 14400)

Hostgator



Domain Name:	JPYORRE.COM
Registrar:	NETREGISTRY PTY. LTD.
Sponsoring Registrar IANA ID:	677
Whois Server:	whois.netregistry.net
Referral URL:	http://www.netregistry.com.au
Name Server:	NS6179.HOSTGATOR.COM
Name Server:	NS6180.HOSTGATOR.COM
Status:	ok http://www.icann.org/epp#OK
Updated Date:	26-nov-2014
Creation Date:	26-nov-2014
Expiration Date:	26-nov-2015
>>> Last update of whois database:	Fri, 30 Jan 2015 18:25:56 GMT <<<

Who else is at 192.232.251.97?

Details for 192.232.251.97

This IP is listed in 3rd-party threat intelligence databases

3rd-party threat intelligence

Last update	Direction	Description	Source
2/18/15	outbound	Malware Domain	http://reputation.alienvault.com/reputation.data

Known domains hosted by 192.232.251.97

viralsoil.com unicorndartssandiego.com beginnerboxadventures.com thebikerweb.com www.c2mtech.com foamrubbersponge.com bryanleeart.com renown-travel.com bestpoolcue.com absolutefitnesspeoria.com neckbeard.org reiaofmacomb.com chinachieve.com cbportraits.com cynergymail.com hummingbirdtechnologies.com market-africa.com faerimoon.com yourdailymediafix.com exotic-fish.org barstoolsandiego.com medfieldhighschoolalumni.org celesteholeman.com bestbackmassager.com sbothaicenter.com menopausalweightloss.com drevon.org cinnamonspice.com.au goldsilverupdates.com sandiegopoolcuerepair.com julianearl.com customsuperhomes.com amazinglightphoto.com ericamsimmons.com 3qadvisors.com www.2.sbothaicenter.com life-madebetter.com selfdefense.alertwebmarketing.net jsoclan.com buildingtopcompanies.co.uk cnlap.com manualtutor.com prettymichiganhomes.com edigitalsolutions.org venasylaser.com newenglandgirl.com oyunf1.com versarailattic.com perukokusai.com elcaminowoodworking.org limitationsofjustice.com bestphotoprinter.org ethiopian-business-development.com thebluepig.com www.acne.alertwebmarketing.net silverbullionprices.org www.pregnant.alertwebmarketing.net autismalternativesolutions.com jobs.cloudanalyticssolutions.com construction-contractors-uk.co.uk idibujo.com dubaitouchscreenkiosk.com bottlesendartssandiego.com karengrove.com sandiegobarstool.com unjustecuador.com ccontractors.co.uk babycarehandbook.com medicarepart.net jliremodeling.com breastenlargementwithoutsurgery.com newsite.belladodds.com luminvisionasia.com lifetechhk.com cinnamonsugar.com.au agssocialmedia.ca dessme.com Julesprokop.com roop.dk bcgs-law.com fireboyandwatergirl2.com texasmedicareplan.com skyhold.east-of-paradise.com cynergysair.com rubbersheetroll.com oasisdentistry.org alertwebmarketing.net daylaraephotoagency.com bjrdefiningmoments.com amazinglightphotography.com buyclear.net skinrefined.com splashinginsunshine.com iheartreviewsblog.com kayamaya.com test.arissabrown.com sliemahotsticks.com arissabrown.com pandaswordoftheday.com.au texasmedicareadvantage.com fieldhockeyforum.com huahcoding.com lmsadministrator.com best-epilator.com andreaandreasen.com mezzcuesandiego.com britishsportscar.org bikingtolive.com impactleadershipforum.com cellphonecasesforwomen.com alexeipatrascudesign.com consejos-relacion-pareja.com coupongold.ca bcnlabs.com assurancehabitationmoinischer.com www.allergy.alertwebmarketing.net cynergyfitness.com unyha.com east-of-paradise.com suirealty.com iguanalittle.com entredosmundos.net bestlaptopcooler.org bryandewberry.com affportaltools.com 707ave.com www.cake.alertwebmarketing.net geoffreysweeney.com comparatiffavevaisselle.com blight.east-of-paradise.com granmesonmirador.com dedicated.com.sa islam webmail.lisabelcastro.com webmail.bioscreen.com highermindhealth.com practicalchristianwoman.com www.bioscreen.com reiaofmacomb.dylantanaka.com asuttlepursuit.com driftwood-pieces.com thepersonalcaresite.com qualityfamilyphotos.com www.credit.alertwebmarketing.net adivinaadivanzas.com fricentary.com touchwood-homes.co.uk dev.jpfirm.com electrictoothbrushreviews.org routertech.com tigerminds.com pechaueruesandiego.com theurbanfestivalcollective.ineedadate.info corecareadvocates.com vidboxvideos.com ilovesticks.com selfesteem-from-inside-out.com coachingispower.com best-epilator.com americanfamilyblog.com ethniderm.com mail.brasseriekensington.com highlandsclothingresale.org versaliftrviews.com electricshaver.com karewfound.com reynolds.sinp.it neillryanjoinery.com eastkoastparanormal.com smtp.jpfirm.com recetasmascomidas.com entrenamientoespoder.com karewfound.com reynolds.sinp.it clickbucks.com mypetsangel.com skyycamstudio.com www.blight.east-of-paradise.com houseofluc.com www.personalcaresite.com webmarketing-reselection.bufomarinus.com 37itemstohoard.com n0jiveturkey.com cynergylifts.com lilbluepig.com houseofluc.com www.personalcaresite.com webmarketing-reselection.penguinsoftsol.com sandiegopoolcuecase.com greenburialsasheville.com mainstreetart.com centerispabe.com shaneduran.com fireboyandwatergirl4.net snailbob3.com wx9.org aquarium-calculator.com cryogenic10.com www.2.sbobetchamp.com polarisproperty.com.au anubians.com anubians.com anubians.com bunnyduster.com.au goldenmumbai.com doin Jupiter.com elsabah.net hendersonville.dentalspa.com ingenieriatdf.com.au andthehorizon.com.au min.ac.th panic.alertwebmarketing.net kaydickey.com county-legal.com pregnant.alertwebmarketing.net encuentratuparejajamora.com suchstonesanctuary.com freshwater-sharks.com onyxarmor.com absinthe.east-of-paradise.com dfwapartmentslocator.com www.houseofluc.com unpoco-design.com griffithkllc.com doin Jupiter.mobi enigmabb.com reedlaplant.com lavoiedesplantes.com fireboyandwatergirl5.net smtp.bcgs-law.com taylorfuentesantana.com mysportsstation.com webmail.brasseriekensington.com cleftstories.com modeltrainguide.org gameofthronescentral.org karewfound.com www.houseofluc.com wstaartclub.nl thenmaschinen-vergleich.de blackwidowdartssandiego.com landoftravel.com northcoastsigns.net thatmomentebook.com salsadartsupplies.com salsadartsupplies.com salsadartsupplies.com www.lespetitscherubs.com anadool.com footpathpictures.com beststyle.com dubstep-art.com east-of-paradise.com senconsultingservices.com lagranlucha.com predatorcuesandiego.com poolcuecasesandiego.com dfr4.com absentfaith.com ingrochester.com healingana.com twhomes.co.uk rates.goldenmumbai.com detailingknights.com mipsrestaurant.com miketagg.com txtqpsinc.com shuttershadez.com edaraty.com lcrlegal.com cynergycorp.org suzyscove.net improvingourhome.com smtp.jpfirm.com blackdogtag.com ethiopian-property.com goldprice.ie www.photos.alertwebmarketing.net buildingtopcompanies.com bhk-health.com policacidp.com shedweight.net psolano.com weekenz.com businesstrendsblog.org wesleymcintyre.com thecynergygroup.com m-hk-photos.com hammerheadart.com jealousmycat.com mental-skills.com salesbooster4u.co.uk thetechnologicalchemist.com landconsulting.com alexeipatrascu.com 32ndallament.com fonoonit.com smtp.bioscreen.com 365onlineresults.com rubberepdmroofing.com ymersh.net jaypilates.info versalift.com pensplac.com le-college.com heroelite.viveyopal.co work-from-home-ideas.org nahra.org hostheaven.co.uk bioscreen.com anubians.com ericavid.com autograding.com insurancemedicalsupplementtexas.com 2manyshoes.ie casanarebilingue.com.co whataboutmaddie.com bestbeardtrimmer.com c2mtech.com webdesigner.com neondecoration.com cpanel.thebluepig.com bibletranslation.ws www.arthritis.alertwebmarketing.net thecynergygroup.com b-kensington.com voteapril.com plusbeard.com imap.bioscreen.com howtobuildalistreview.com casamotosyamaha.viveyopal.co vas-school.com thecynergygroup.com alertwebmarketing.com smith.info auto-diagnostics.com estime-de-soi-amour-propre.com bestgarmentsteamer.org www.resume.alertwebmarketing.net derelation.com roadysnews.com www.hendersonvilledentalspa.com jacquelineadooley.com veterinariawalac.com thecoachingpower.com marathonstadium.com mozillafirefoxazoth.fr oyun.sarkioyunlari.org hammerheadpvp.com autoclubadvantage.com predatorchalk.com 20twelvedubstep.com online-bible.bibletranslation.ws ezmoney.us trust.com insanovision.com alexeipatrascu.com alrightgraphix.com sub-domain.net viveyopal.co denverautorepairshop.org agtfze.com topclasscompanies.com footprintsLtd.net deathxdeath.com prettyhomes.com turtlesantsetup.com projecttuts.com goldenlondon.com bestfriendpizza.com uhohmom.com ohitsdana.com alertwebmedia.info bensproperties.co.uk vikingcuesandiego.com ouroffridsolarcabin.com agscanada.ca tshirtarabia.com wickedthicketfurniture.com alertwebmarketinggold.com weekendlonden.net keepitgolden.com sixtytozeromusic.com mominacentury.com pydaw.org thebikinibabes.net svhomeforaged.com amateur-webcamgirl.com stephenmccloughlinsound.com studio421blog.com esmecakes.com christinemasonphotography.com hiddenassetsmalta.com hairclipperreviews.org beardgrooming.com c2mtech.com webdesigner.com neondecoration.com cpanel.thebluepig.com bibletranslation.ws www.arthritis.alertwebmarketing.net cellphonecoversandcases.com bluemedicasesupplement.com dartsupliessandiego.com reviewingdogfood.com midgard.east-of-paradise.com garrettgriess.com internationalenterprise.org ryanoneilknight.com carvacuums.org happier-dog.com alanpsi.com rantingpanda.com titan-avto.net fenironline.com hazeltineholdings.com djalright.com livingstonpaint.com anarouges.com lespetitscherubs.com bazalamazingoptionstrading.com howtotalkdirtytoyourman.net guinea-pigs.org bestsumppump.org bikini-trimmer.com jamesbrowne.net coppercladfr4.com cararadioclub.org dylantanaka.com tegansweeney.com www.panic.alertwebmarketing.net oyuntanitimi.com free-bible.bibletranslation.ws doorwaystoarkomo.com internetmarketingadvice.net www.brasseriekensington.com m-memorials.com webmail.footpathpictures.com katchamama.com velocejewelry.com freshfusion.us silverbullionrate.com e-booksdownloaden.net couplingboringservicesinc.com sbobetchamp.com studiorennewyoga.com ethiopian-properties.com zab-zab.com frasesdecarinho.net hartzenterprises.com gameclay.com magiclyric.com ashia.org www.2.sboextra.com gothcoven.com reikinatualhealing.ca alinavlaicu.com bikerseek.com lifeyoulovenow.com agssocialmedia.info onegreatgift.org bestbeardtrimmer.org vsecretmd.com torressonido.com suzyscove.org www.preforeclosure.alertwebmarketing.net stepstosuccessnj.com createsuccessathome.com steveoliverrealestateacademy.com guppy-fish.com www.guitar.alertwebmarketing.net veronicabane.com koreyconnolly.com dearbluelovegreen.com cuscohome.com agssocialmedia.com goddessastraea.com organicmalta.com reptilehaven.eu ashiaconsulting.com lisabelcastro.com babadballi.com ihacer.com smallonlinebusinessforwomen.com floresdesignstudio.com cizastore.com thewinmedia.com melissamillerstudios.com divorceinjurylaw.com frasesdealiento.info aupronailsupply.com ugliestanimals.com novasity.com consultecsoftware.com lucasicuesandiego.com afrugalwedding.net jguzman.com designarnedia.com classifieds.goldenmumbai.com webmaster365.email pattillowebdesigns.com petclipper.org suzyscove.ca jpfirm.com joshevol.com sell-house-fast-hawaii.com cheapchampionshipsrings.com paintsprayerreviews.net www.sweating.alertwebmarketing.net bible-verses.bibletranslation.ws dtlandgroup.com thebeepetest.com celebrateincorporated.com www.time.alertwebmarketing.net cloudanalyticssolutions.com maryrileyfitness.com daniefabricatore.com natalieobermaier.com universalsanitizers.com pitstopmontreal.com www.selfdefense.alertwebmarketing.net local.goldenmumbai.com burlesqueduction.com internetmarketingadvice.jacquelineadooley.com yellowpages.goldenmumbai.com sell-my-house-in-hawaii.com poolcuecasesandiego.com broodco.ca sandiegodarts.com clearskiesphotography.ca poderdelcoaching.com alacritis.east-of-paradise.com customtelsys.com aliciaszot.com phenolicmaterials.com restocapucine.com old.thebluepig.com knightbg.com sarkioyunlari.org zcstudenica.org amharicquran.com fixmyzippo.com jlkarmoring.com dpm-rks.org www.jpfirm.com viewhwall.com electricicus.com googlesniperreview.ca petemt.com goldfish-forum.com printingtshirtsdubai.com webmail.katchamama.com pilatesphuket.com king-james-bible.bibletranslation.ws nose-hair-trimmers.org alertwebmarketing.com gulfsolvents.com uspronailsupply.com foursomeresor.com sandiegodartboards.com backspacedatasolutions.com backtoearthherbs.com androidxx.info freegolis.com sitedirectory.us info.w3realtysolutions.com dartboardssandiego.com pornxx.info summitdallas.com webmail.chikamura.com bigrevenge.cl piranha-fish.com aquarium-geek.com americanxx.info termites-pictures.com freeusaporn.com mobilexx.info funxx.info sbototal.com asianxx.info

Starting Nmap 6.00 (<http://nmap.org>) at 2015-03-05 14:34 PST

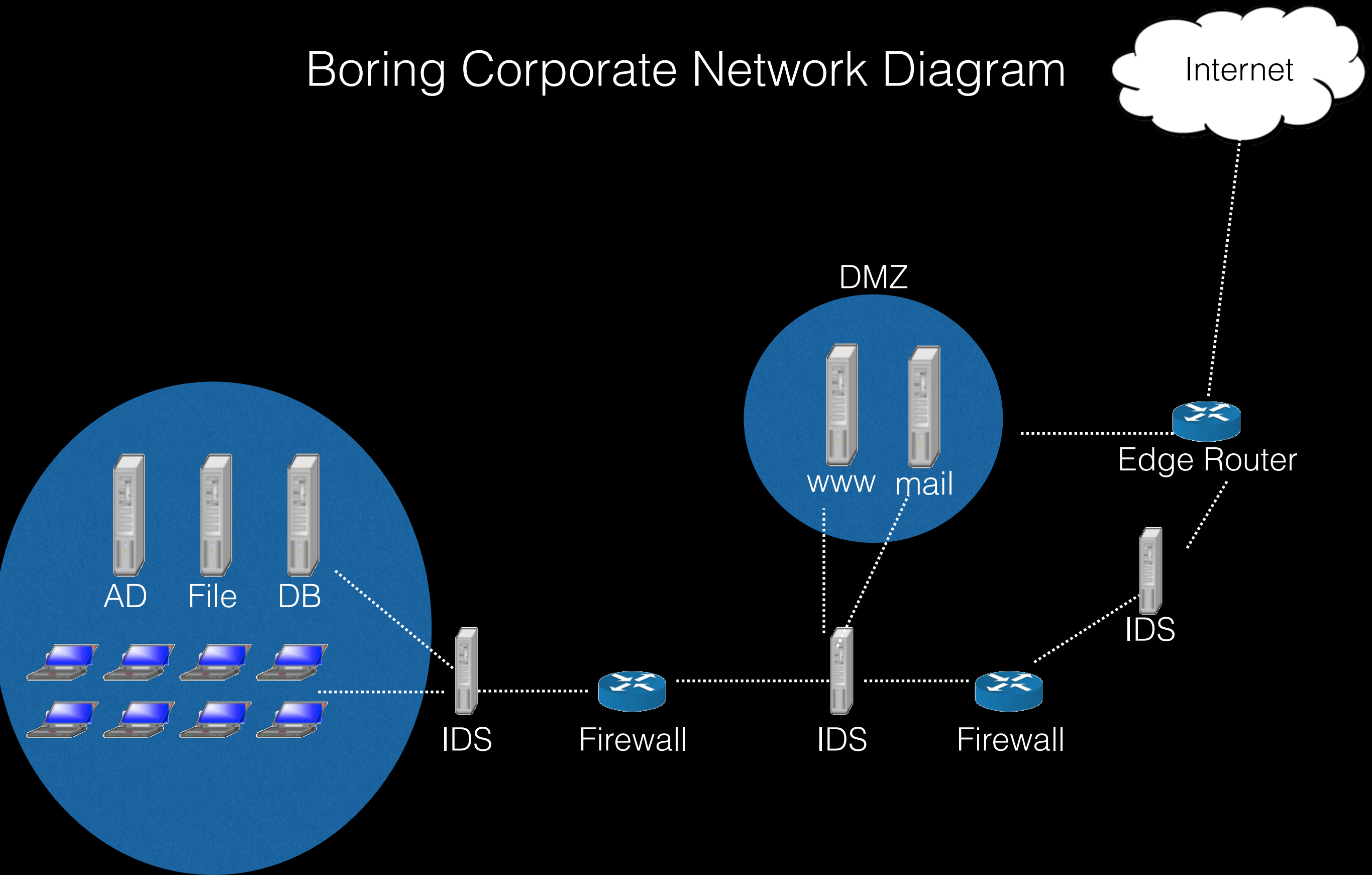
Nmap scan report for 192.232.251.97

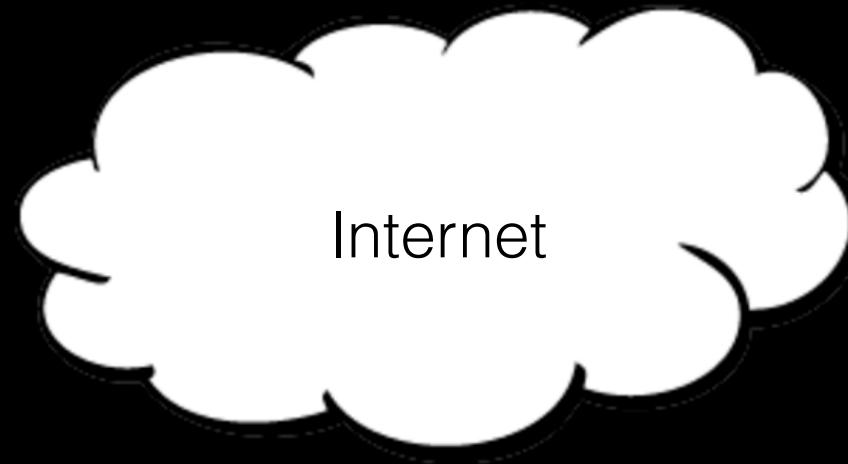
Host is up (0.040s latency).

Not shown: 966 closed ports

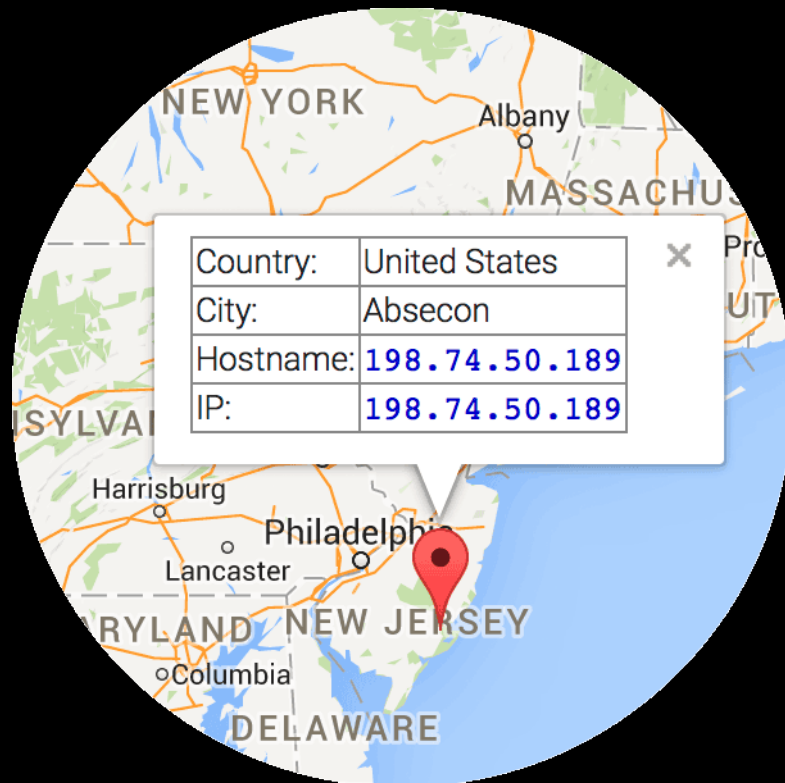
PORT	STATE	SERVICE
1/tcp	filtered	tcpmux
3/tcp	filtered	compressnet
4/tcp	filtered	unknown
6/tcp	filtered	unknown
7/tcp	filtered	echo
9/tcp	filtered	discard
13/tcp	filtered	daytime
17/tcp	filtered	qotd
19/tcp	filtered	chargen
21/tcp	open	ftp
22/tcp	filtered	ssh
23/tcp	filtered	telnet
25/tcp	filtered	smtp
26/tcp	open	rsftp
53/tcp	open	domain
80/tcp	open	http
110/tcp	open	pop3
111/tcp	filtered	rpcbind
135/tcp	filtered	msrpc
139/tcp	filtered	netbios-ssn
143/tcp	open	imap
179/tcp	filtered	bgp
443/tcp	open	https
445/tcp	filtered	microsoft-ds
465/tcp	open	smtps
514/tcp	filtered	shell
587/tcp	open	submission
993/tcp	open	imaps
995/tcp	open	pop3s
1080/tcp	filtered	socks
2049/tcp	filtered	nfs
2222/tcp	open	EtherNet/IP-1
3306/tcp	open	mysql
8080/tcp	open	http-proxy

Boring Corporate Network Diagram

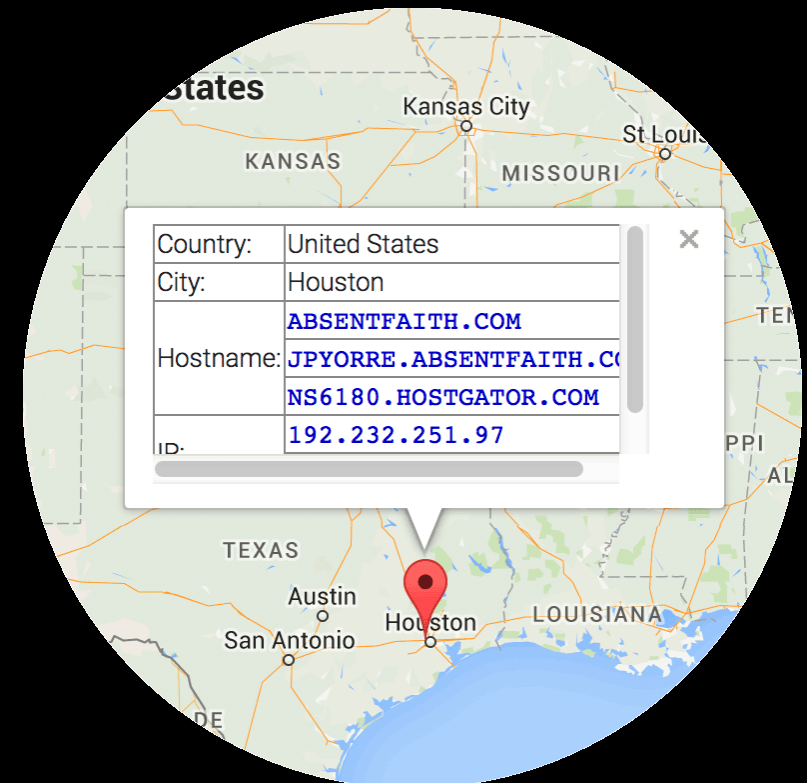




Internet



IDS at Linode




jpyorre.com at hostgator

The IDS

The IDS

Linode Manager

 pyorre | [my profile](#) | [log out](#)

[Linodes](#) [NodeBalancers](#) [Longview](#) [DNS Manager](#) [Account](#) [Support](#) [Documentation](#) [Community](#)

[Dashboard](#) [Remote Access](#) [Rebuild](#) [Rescue](#) [Resize](#) [Clone](#) [Graphs](#) [Backups](#) [Settings](#) [Extras](#)

[Linodes](#) » **mship**

Dashboard

Select	Configuration Profiles	Options
<input checked="" type="radio"/>	My Debian 7.3 Profile (Latest 64 bit (3.18.5-x86_64-linode52))	Edit Remove

[Reboot](#)

[Rebuild](#) | [Deploy an Image](#) | [Create a new Configuration Profile](#)

Disks

	Debian 7.3 Disk Image (48640 MB, ext3)	Edit Remove
	512MB Swap Image (512 MB, swap)	Edit Remove

[Create a new Disk](#)

Host Job Queue ([more](#))

Server Status

Your Linode is currently

Running

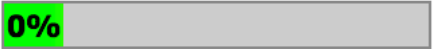
[Shut down](#)

5 days uptime

Network


- Transfer/mo: 3000 GB
- Incoming: 106 MB
- Outgoing: 149 MB
- Total: 255 MB

You have used

0% 
of your monthly transfer

The IDS

Linode Manager

 pyorre | [my profile](#) | [log out](#)

[Linodes](#) [NodeBalancers](#) [Longview](#) **DNS Manager** [Account](#) [Support](#) [Documentation](#) [Community](#)

DNS Manager

Domain Zone	Type	Last Modified	Status	Options
jpyorre.com	master	2015-02-24 17:11:15	ACTIVE	Edit Remove Check Zone file
Import a zone Clone an existing zone Add a domain zone				

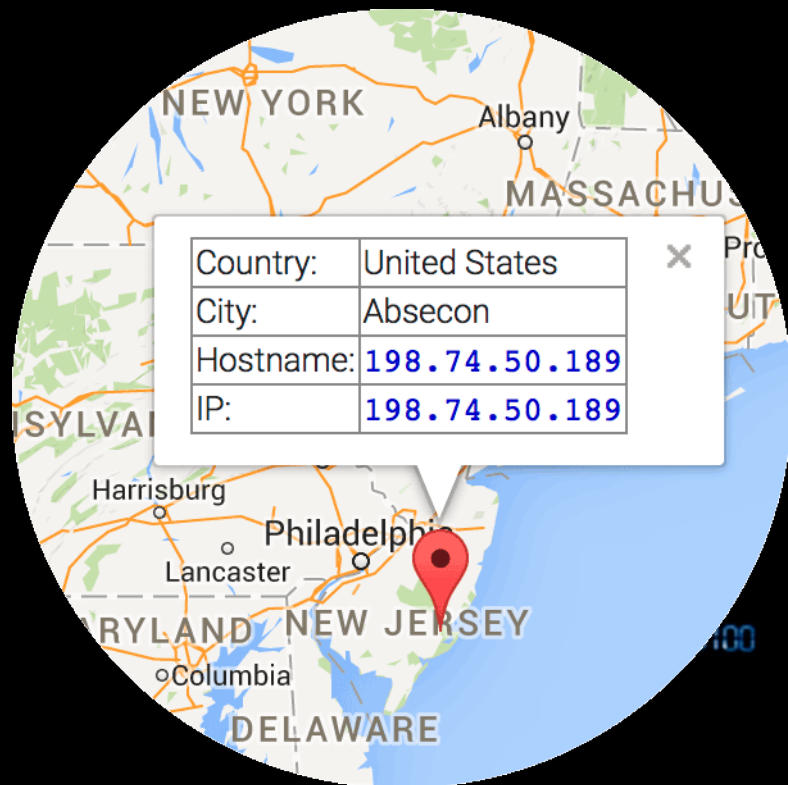
[DNS Manager](#) » **jpyorre.com**

A/AAAA Records

Hostname	IP Address	TTL	Options
	198.74.50.189	Default	Edit Remove
ids	198.74.50.189	Default	Edit Remove
mail	198.74.50.189	Default	Edit Remove
www	198.74.50.189	Default	Edit Remove

Open proxy?

Open proxy?



IDS at Linode

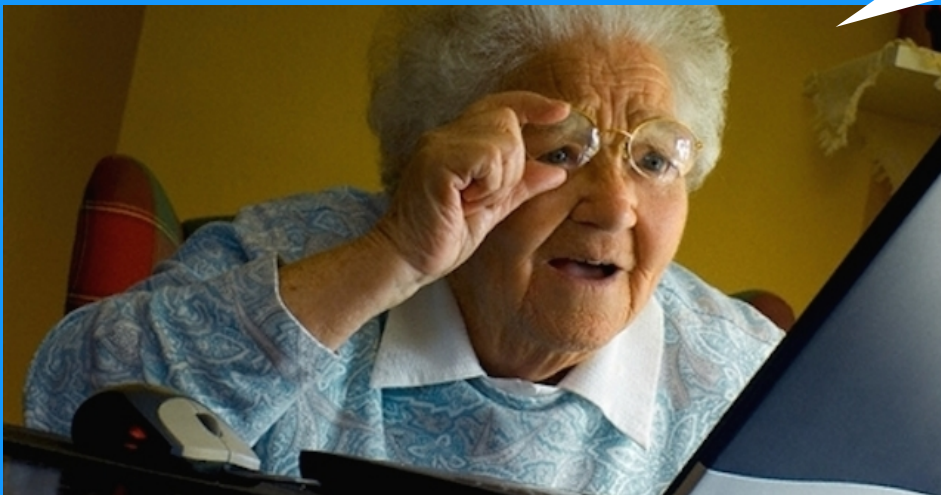
Configuration

DNS

The normal route to the server

Internet. Take me to
jpyorre.com

jpyorre.com
is at
192.232.251.97

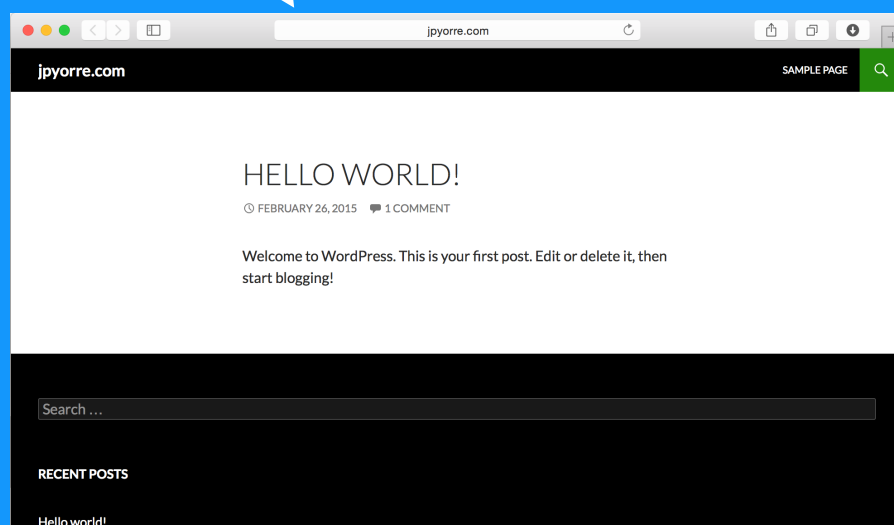


1: jpyorre.com?



2: 192.232.251.97

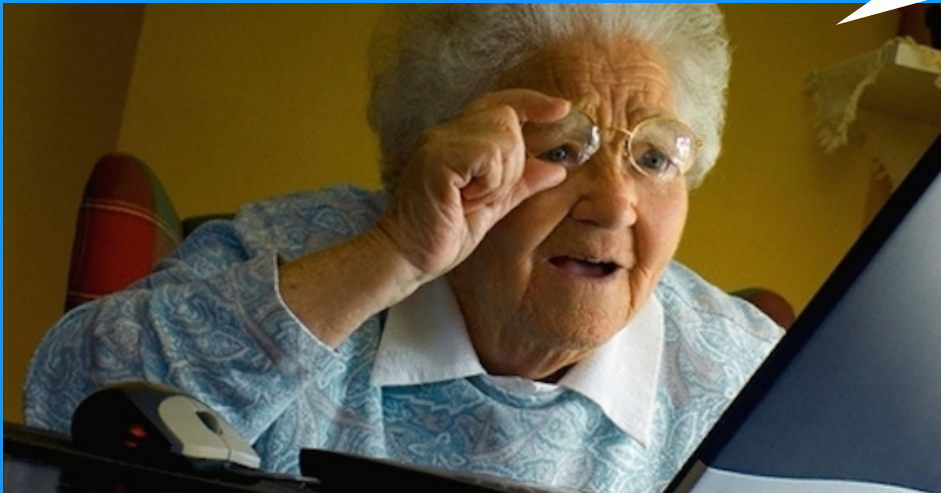
3: 192.232.251.97 / Hostgator



The modified route to the server

Internet. Take me to
jpyorre.com

jpyorre.com
is at
198.74.50.189



1: jpyorre.com?



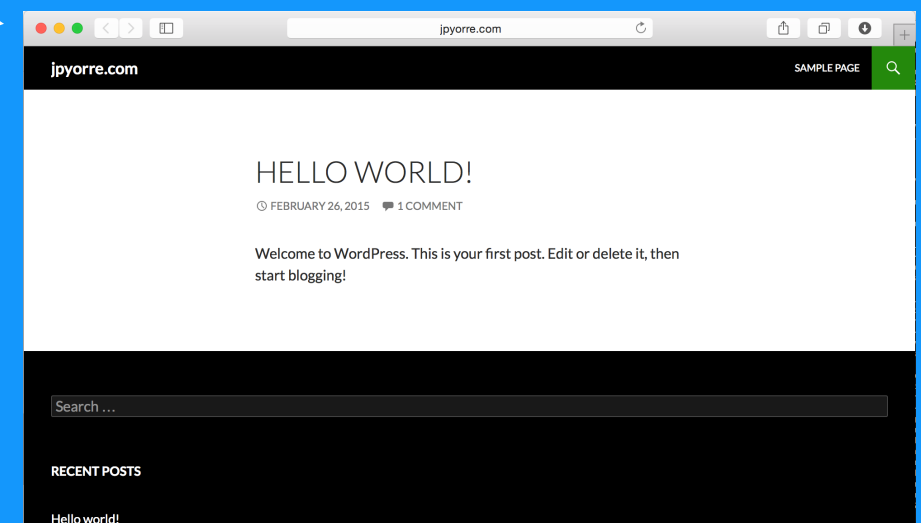
2: 198.74.50.189

3: 198.74.50.189 / Linode

198.74.50.189
(VPS at Linode)



4: 192.232.251.97 / Hostgator



Manage a domain

jpyorre.com

Domain expires 27/11/2015 [[Renew](#)]
[Visit jpyorre.com](#)

[Dashboard](#)

[Domain Name](#)

[Zone Manager](#)

[Domain Delegation](#)

[Domain Redirector](#)

[Business Profile](#)

[Hosting](#)

[Email](#)

[Payment Gateway](#)

[SSL Certificates](#)

[Online Marketing](#)

[Website Security](#)

Manage your domain delegation ?

To delegate your domain name you'll require both primary and secondary name servers and, if you have any, they must be added.

Important: If you no longer require the services associated with this domain, they must be cancelled via the [Domain Delegation](#) page. Delegating your domain away will not cancel any associated services.

[How to modify your nameservers](#) ▶

Important information before you proceed

Name servers ?

Point your domain to your website or web hosting space.

NAME SERVER 1

ns6179.hostgator.com

NAME SERVER 2

ns6180.hostgator.com

[Set default](#)

[Update](#)

Actual Website Location



Host Gator

Control Panel

[Register](#)[Transfer](#)[Whois](#)[Register](#)

Find

Find functions quickly by typing here.

WordPress Hosting



Get Started With
WORDPRESS
Today!

[Install Now](#)

Install An SSL!

Stop Evil-Doers!

[Add SSL Today!](#)

Special Offers



Cloud
Backup



SEO Gears
- Promote
your site



Beautiful
Premium
WordPress
Themes



SiteLock:
Protect
Your Site
from
Hackers



Mojo
Graphics &
Logos



WordPress
Themes &
Templates



WordPress
Services



Get Started
With
WordPress
Today



Cloud
Desktop
Storage



Bing Ad
Credits



Accept
Credit
Cards with
TransFirst



Google
AdWords
Credit

Security



Password
Protect
Directories



IP Deny
Manager



HotLink
Protection



GnuPG
Keys

Domains



Subdomains



Addon
Domains



Parked
Domains



Redirects



Simple DNS
Zone Editor



Advanced
DNS Zone
Editor



Dns Tool

Mail



Get it Now

An SSL!

op
Doers!



L Today!

With
WordPress
Today

Desktop
Storage

Credits

Credit
Cards with
TransFirst

AdWords
Credit

Security



Password
Protect
Directories



IP Deny
Manager



HotLink
Protection



GnuPG
Keys

Domains



Subdomains



Addon
Domains



Parked
Domains



Redirects



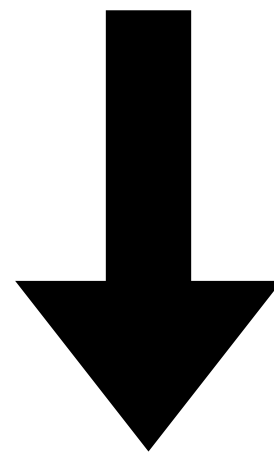
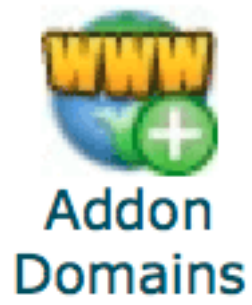
Simple DNS
Zone Editor





Dns Tool

Mail





jpyorre.com	 /public_html/domains/jpyorre 	jpyorre	not redirected	Remove	Manage Redirection
-------------	--	---------	----------------	------------------------	------------------------------------

Put an IDS in there!

Demo:

IDS Configuration and Hacking RevSlider

josh@zvmship: ~

Evol:~ josh\$ █

I





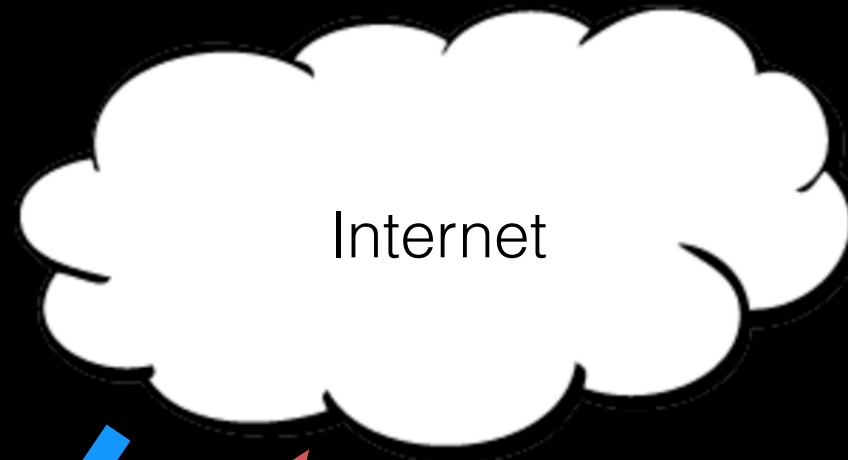
Default

Last login: Fri May 15 23:03:49 on ttys000

Evol:~ josh\$ █

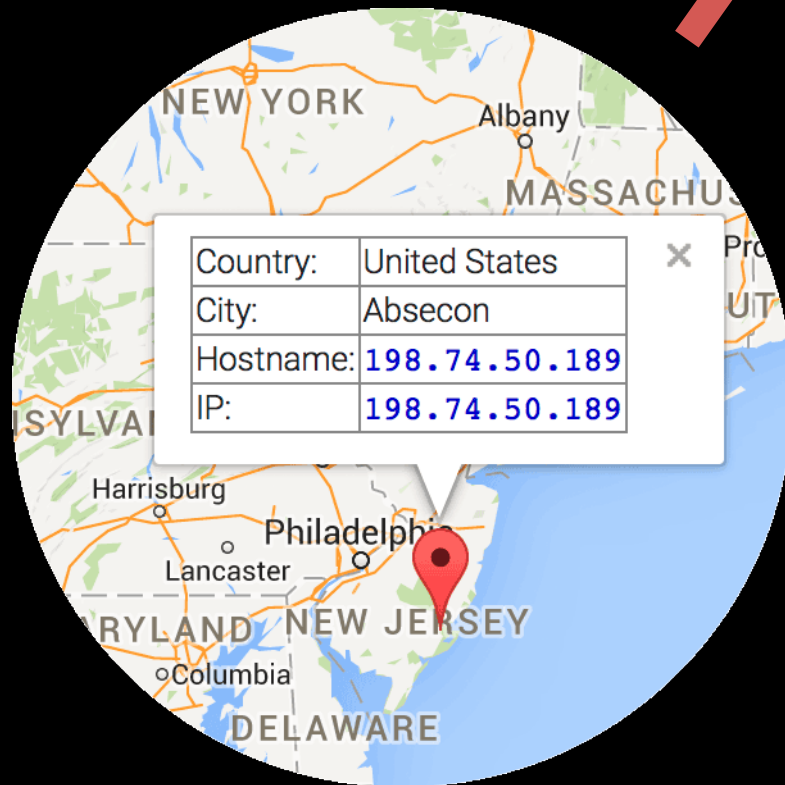
Another Hosting Provider

Without mod_security



Internet

Changes made here



IDS at Linode



jpyorre.com at Digital Ocean

Manage a domain

jpyorre.com

Domain expires 27/11/2015 [[Renew](#)]
[Visit jpyorre.com](#)

[Dashboard](#)

[Domain Name](#)

[Zone Manager](#)

[Domain Delegation](#)

[Domain Redirector](#)

[Business Profile](#)

[Hosts](#)

[Email](#)

[Payment Gateway](#)

[SSL Certificates](#)

[Online Marketing](#)

[Website Security](#)

Manage your domain delegation ?

To delegate your domain name you need to add primary and secondary name servers and, if you want, you can add additional name servers.

Important: If you no longer require the services associated with this domain, they must be cancelled via the [Domain Cancellation](#) page. Delegating your domain away will not cancel any associated services.

[How to modify your nameservers](#)

Important information before you proceed

Name servers ?

Point your domain to your website or web hosting space.

NAME SERVER 1

ns1.linode.com

NAME SERVER 2

ns2.linode.com

[Set default](#)

[Update](#)

Digital Ocean Local DNS

jpyorre.com

A

@

192.241.237.32

✖

NS

ns1.digitalocean.com.

✖

NS

ns2.digitalocean.com.

✖

NS

ns3.digitalocean.com.

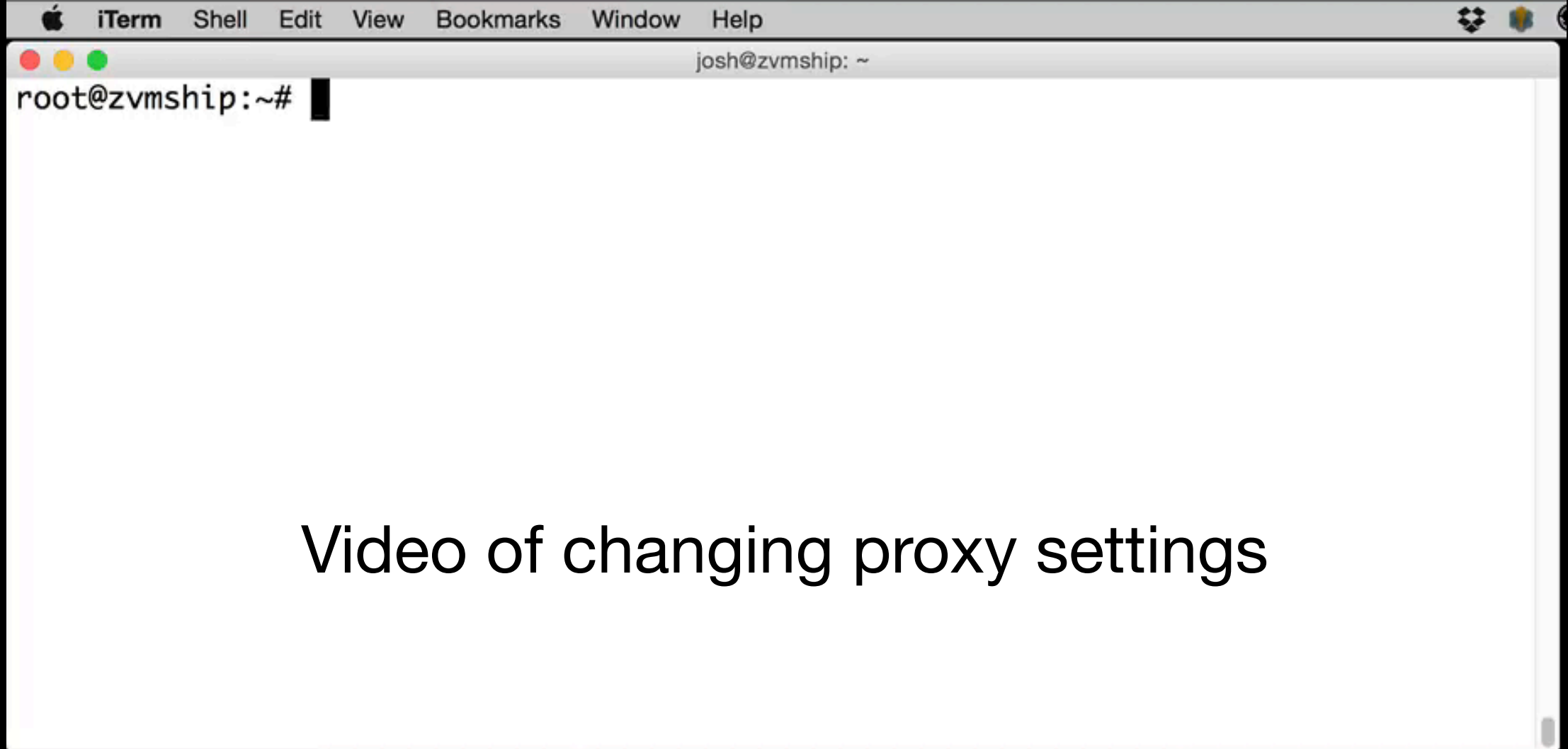
✖

Zone File

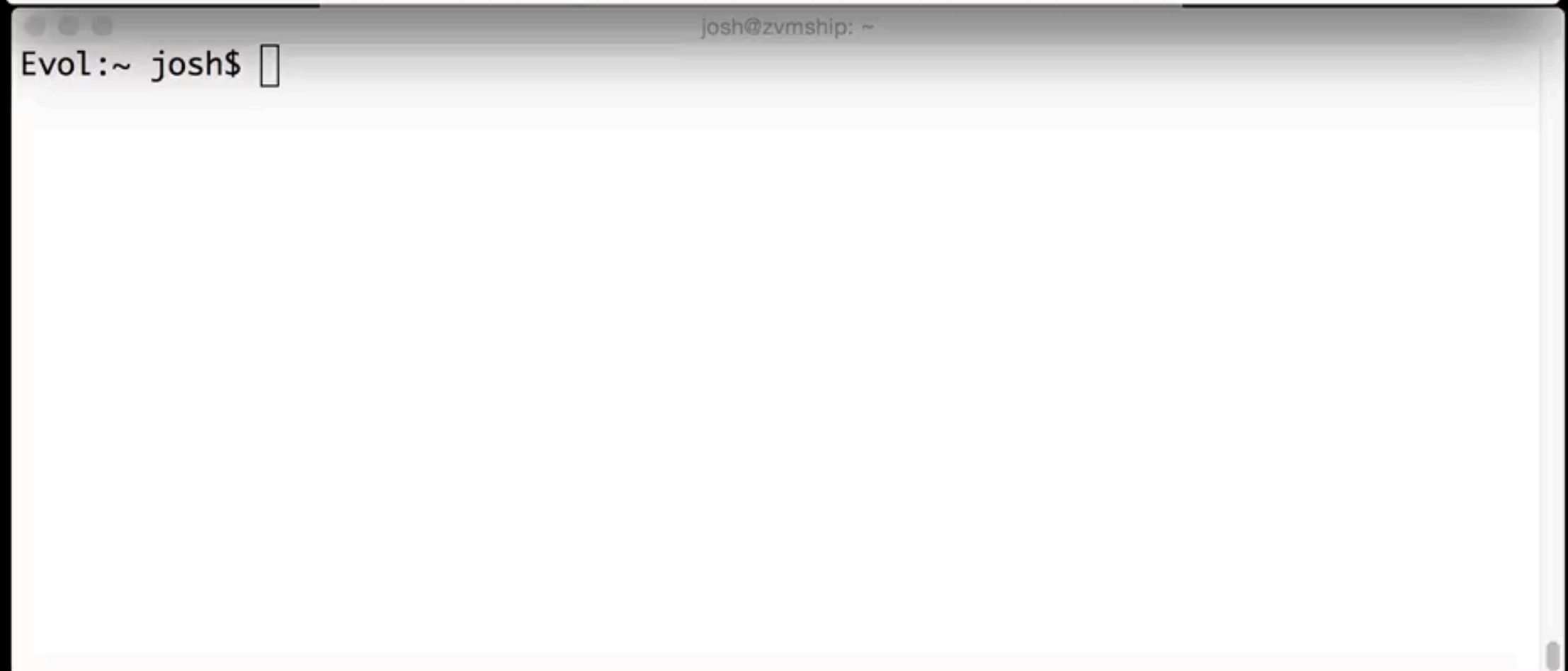
```
$ORIGIN jpyorre.com.  
$TTL 1800  
jpyorre.com. IN SOA ns1.digitalocean.com. hostmaster.jpyorre.com. 1425060087 10800 3600  
604800 1800  
jpyorre.com. 1800 IN NS ns1.digitalocean.com.  
jpyorre.com. 1800 IN NS ns2.digitalocean.com.  
jpyorre.com. 1800 IN NS ns3.digitalocean.com.  
jpyorre.com. 1800 IN A 192.241.237.32
```

Demo:

Visibility into an attack on the Digital Ocean website



Video of changing proxy settings



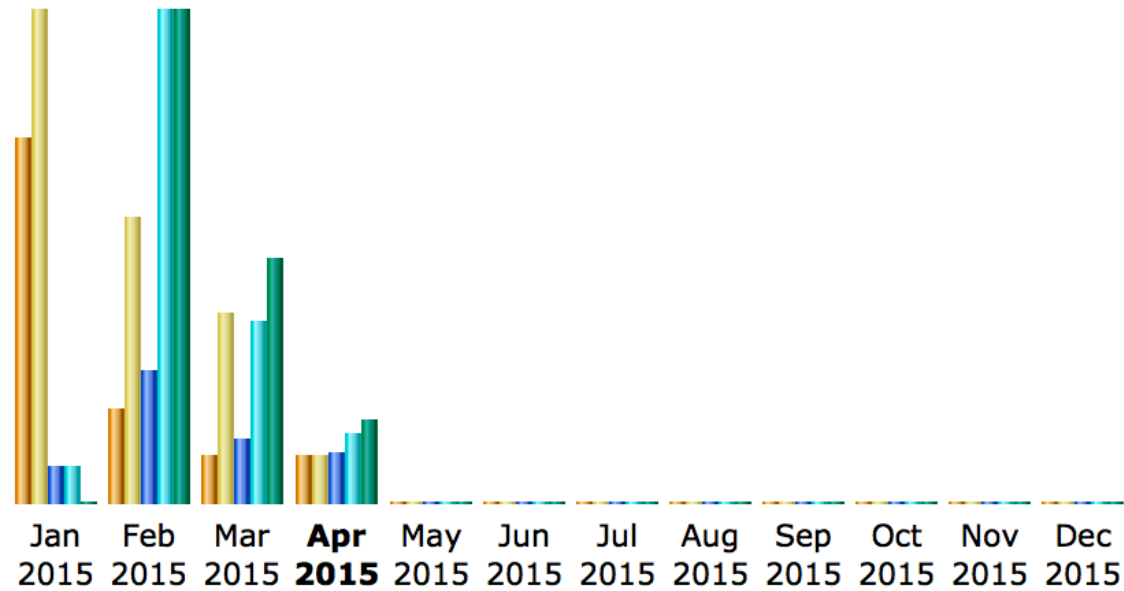
Potential Problems

Visitor Statistics

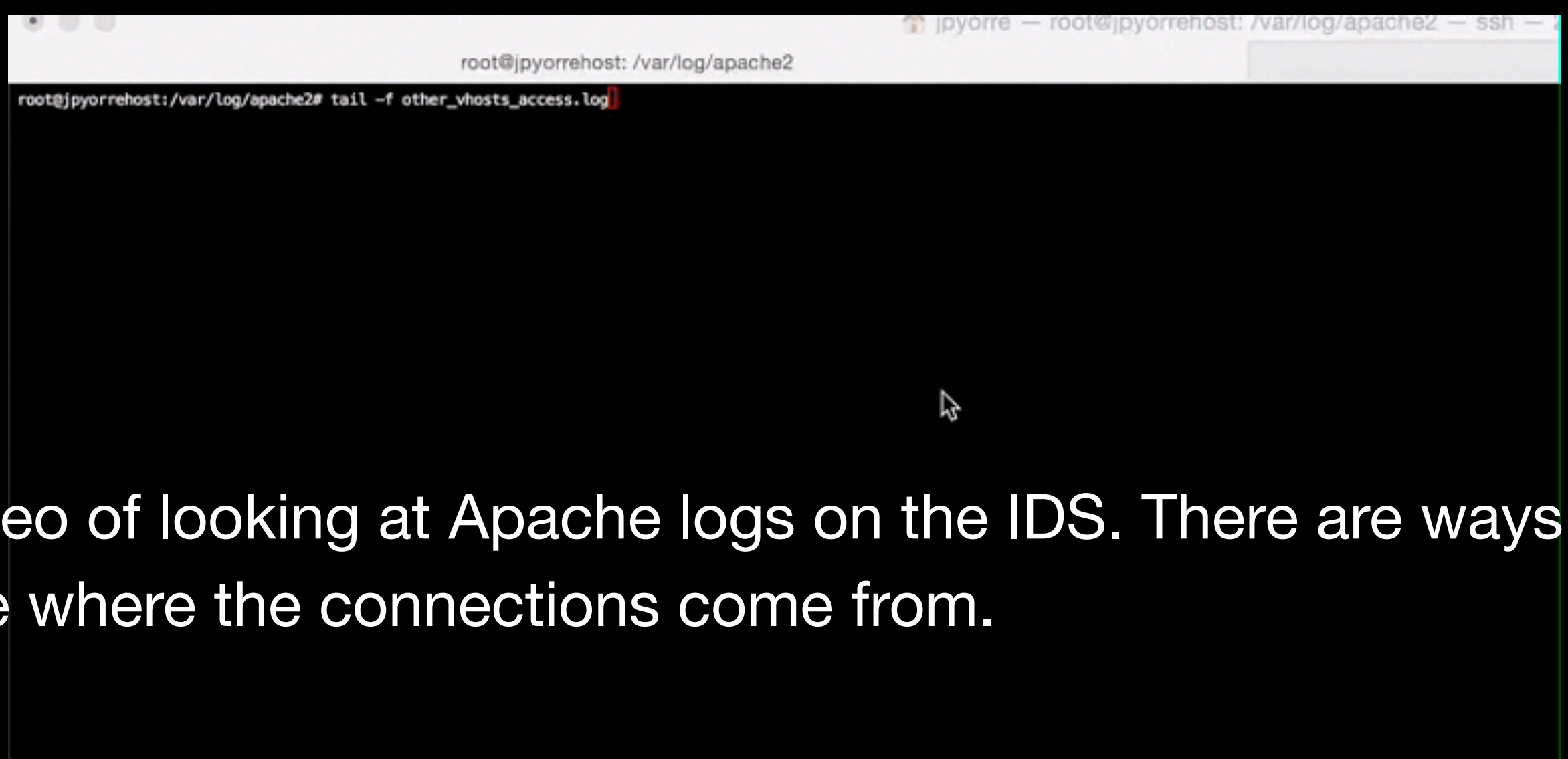
Hosts (Top 25) - [Full list](#) - [Last visit](#) - [Unresolved IP Address](#)

Hosts : 0 Known, 3 Unknown (unresolved ip)
3 Unique visitors

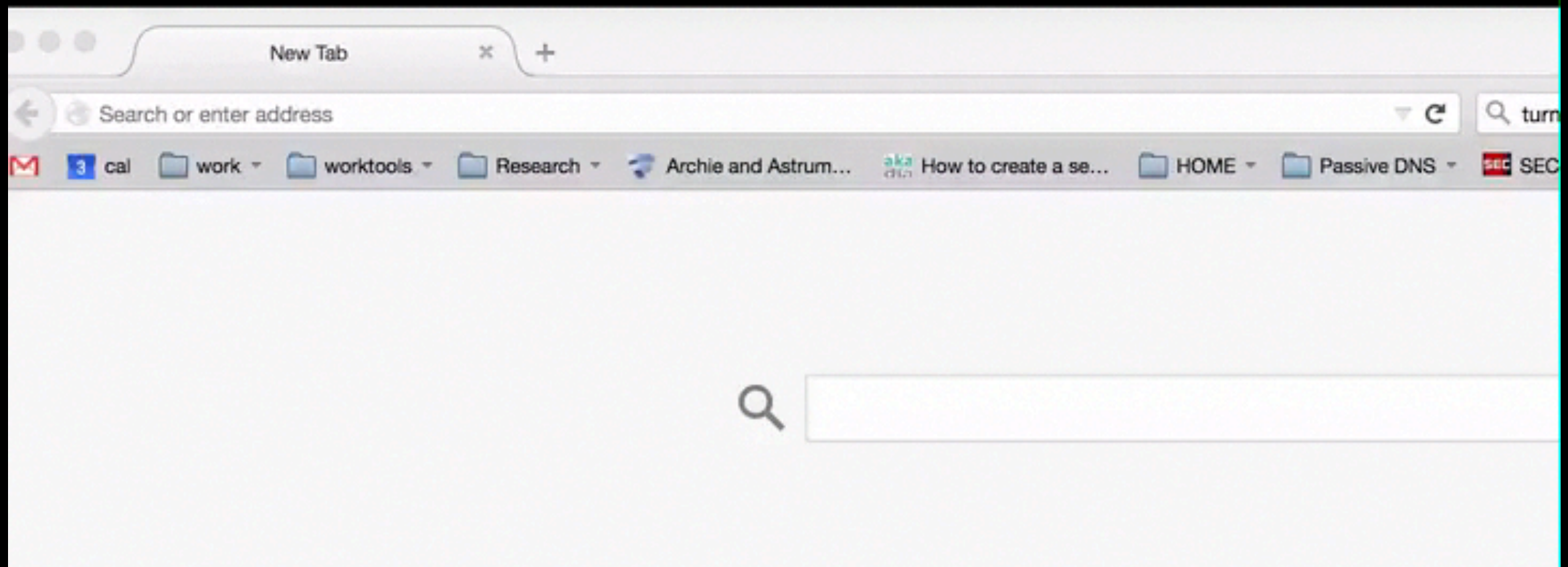
	Pages	Hits	Bandwidth	Last visit
198.74.50.189	30	48	1.34 MB	14 Apr 2015 - 20:16
50.131.187.245	20	21	35.14 KB	06 Apr 2015 - 23:00
67.215.89.46	1	1	7.46 KB	09 Apr 2015 - 14:23



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2015	23	31	37	37	0
Feb 2015	6	18	136	503	8.14 MB
Mar 2015	3	12	66	185	4.04 MB
Apr 2015	3	3	51	70	1.38 MB
May 2015	0	0	0	0	0
Jun 2015	0	0	0	0	0
Jul 2015	0	0	0	0	0
Aug 2015	0	0	0	0	0
Sep 2015	0	0	0	0	0
Oct 2015	0	0	0	0	0
Nov 2015	0	0	0	0	0
Dec 2015	0	0	0	0	0
Total	35	64	290	795	13.55 MB



Video of looking at Apache logs on the IDS. There are ways to see where the connections come from.



Other protocols

The Open Proxy

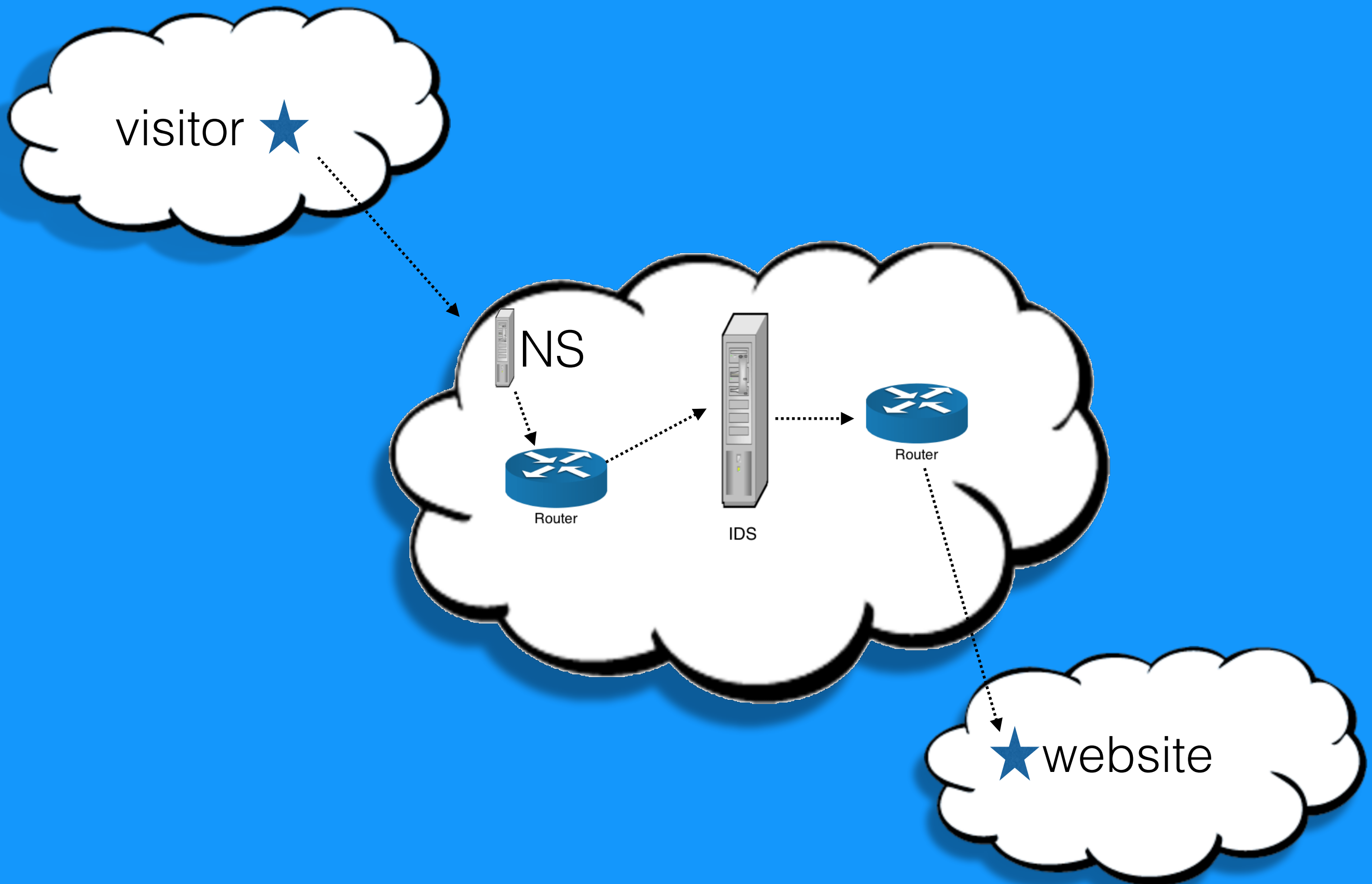
- Using IPTables
- Other protection mechanisms

```
RETURN      all  --  anywhere                anywhere

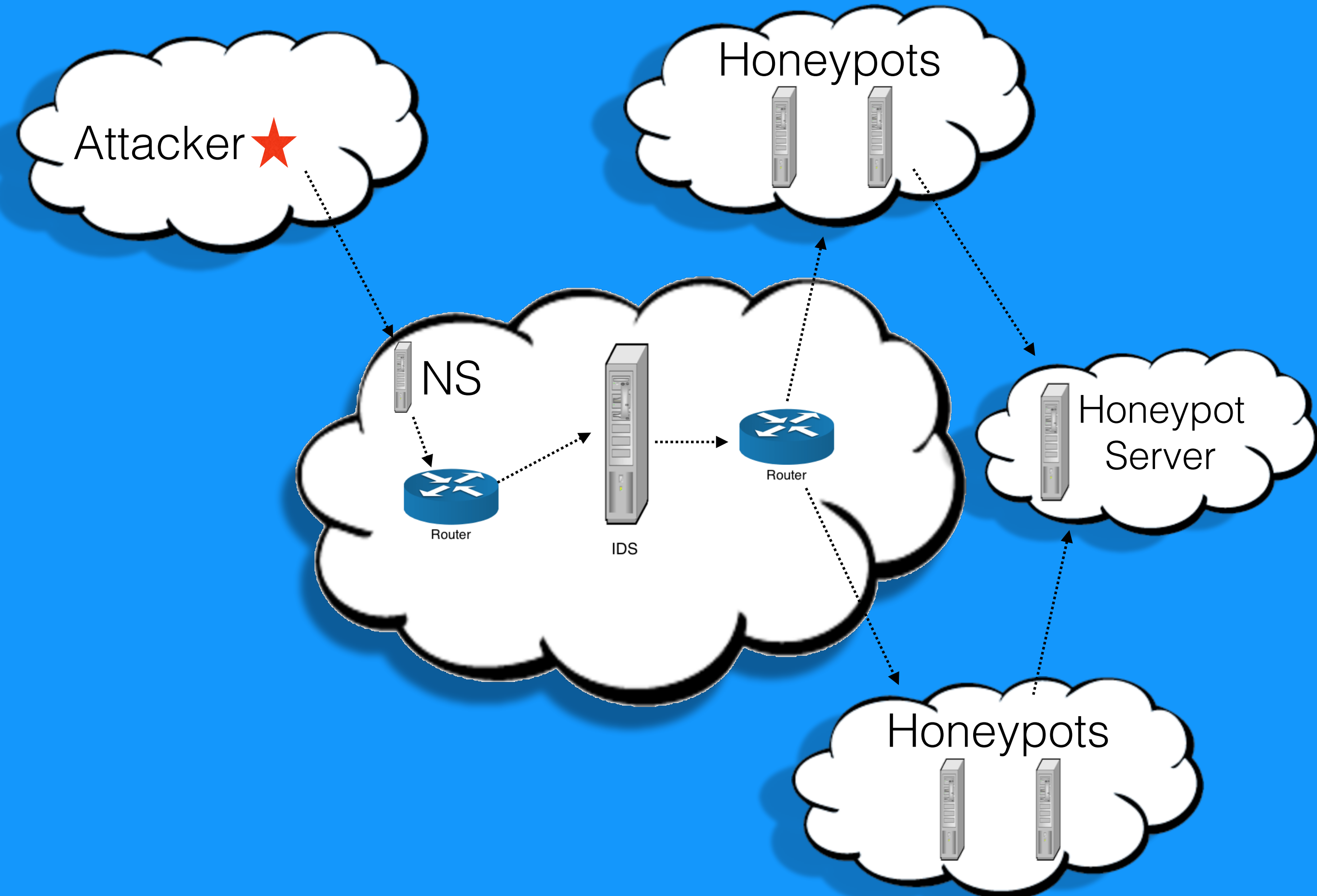
Chain fail2ban-ssh-ddos (1 references)
target      prot opt source                destination
DROP        all  --  c-67-180-177-204.hsd1.ca.comcast.net  anywhere
RETURN      all  --  anywhere                anywhere
```

Future Research

Future Research



Future Research



Questions?

Contact

jpyorre@gmail.com
jpyorre@opendns.com

 @joshpyorre
