OPERATION: TUNA

MTA Configuration, Info Leakage, and you.

AKA

Happy Fun MTA Exploration

It started so innocently.

“dude, mail headers leak a lot of info”

Hmm…

Rapid7?

Delivered-To: jcran@0x0e.org
Received: by 10.52.163.6 with SMTP id ye6cs23091vdb;
Sat, 12 Mar 2011 10:56:29 -0800 (PST)
Received: by 10.101.32.10 with SMTP id k10m1224100anj.159.1299956188566;
Sat, 12 Mar 2011 10:56:28 -0800 (PST)
MIME-Version: 1.0
Return-Path: <>
Received: by 10.101.32.10 with SMTP id k10mr1703754anj.159; Sat, 12 Mar 2011
10:56:28 -0800 (PST)
From: Mail Delivery Subsystem <mailer-daemon@googlemail.com>
To: jcran@0x0e.org
X-Failed-Recipients: alsdjflkdasjflkjsadfjlsdafj@rapid7.com
Subject: Delivery Status Notification (Failure)
Message-ID: <0016367d6154d7d2d2049e4da2e4@google.com>
Date: Sat, 12 Mar 2011 18:56:28 +0000
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable

Delivery to the following recipient failed permanently:

alsdjflkdasjflkjsadfjlsdafj@rapid7.com

Technical details of permanent failure:=20
Google tried to deliver your message, but it was rejected by the recipient =
domain. We recommend contacting the other email provider for further inform=
ation about the cause of this error. The error that the other server return=
ed was: 554 554 5.7.1 <alsdjflkdasjflkjsadfjlsdafj@rapid7.com>: Recipient a=
ddress rejected: Access denied (state 14).

Not much.

Qualys?

Not much.

Tenable?

Delivered-To: jcran@0x0e.org
Received: from mail1.dmz.tenablesecurity.com ([172.20.210.11]) by mta1.tenable.com with ESMTP id lu4rFDf2w5F6TEtT for <jcran@0x0e.org>; Wed, 23 Feb 2011 18:39:07 -0500 (EST)
X-Barracuda-Envelope-From:
X-Barracuda-RBL-Trusted-Forwarder: 172.20.210.11
Received: by mail1.dmz.tenablesecurity.com (Postfix)
id D2B593144003; Wed, 23 Feb 2011 18:39:07 -0500 (EST)
Date: Wed, 23 Feb 2011 18:39:07 -0500 (EST)
Message-Id: <20110223233907.D2B593144003@mail1.dmz.tenablesecurity.com>
X-Barracuda-Connect: UNKNOWN[172.20.210.11]
X-Barracuda-Start-Time: 1298504347
X-Virus-Scanned: by bsmtpd at tenable.com
X-Barracuda-Spam-Score: 0.20
X-Barracuda-Spam-Status: No, SCORE=0.20 using global scores of TAG_LEVEL=1000.0 QUARANTINE_LEVEL=1000.0 KILL_LEVEL=9.0 tests=ANY_BOUNCE_MESSAGE, BOUNCE_MESSAGE, BSF_SC0_SA590, EMPTY_ENV_FROM
X-Barracuda-Spam-Report: Code version 3.2, rules version 3.2.2.56209
Rule breakdown below
pts rule name description
---- ---------- ----------
0.00 EMPTY_ENV_FROM Empty Envelope From Address
0.20 BSF_SC0_SA590 Custom Rule SA590
0.00 BOUNCE_MESSAGE MTA bounce message
0.00 ANY_BOUNCE_MESSAGE Message is some kind of bounce message

This is a MIME-encapsulated message.

--CADCB3144002.1298504347/mail1.dmz.tenablesecurity.com
Content-Description: Notification
Content-Type: text/plain; charset=us-ascii

Hmm, I wonder…

What if i?..

Send email?

Receive email?

Well, that seems easy enough.

But where to get the email addresses?

top-1m.csv.zip

Thank you Alexa :]

1,google.com
2,facebook.com
3,youtube.com
4,yahoo.com
5,live.com
6,blogspot.com
7,wikipedia.org
8,baidu.com
9,twitter.com
10,qq.com
11,msn.com
12,yahoo.co.jp
13,google.co.in
14,taobao.com
15,amazon.com
16,sina.com.cn
17,linkedin.com
18,bing.com
19,google.de
20,wordpress.com
21,google.com.hk
22,google.co.uk
23,yandex.ru
24,microsoft.com
25,ebay.com
26,google.co.jp
27,google.fr

```
aesop@bolivia:~operation_tuna$ cat gen_email.rb
#!/usr/bin/ruby

def random_alphanumeric(size=16)
 s = ""
 size.times { s << (i = Kernel.rand(62); i += ((i < 10) ? 48 : ((i < 36) ? 55 : 61 ))).chr }
 s
end

f = File.open("domains.txt")
out = File.open("emails.txt", "w")
emails = []


f.each_line do |domain|
                domain.chomp!
                name = random_alphanumeric(30)
                out.puts "#{name}, #{name}@#{domain}" ## probably won't work
end
```

AZWOfUWdjXUDxD0PJZzatzu97ham4G, AZWOfUWdjXUDxD0PJZzatzu97ham4G@google.com
mLdLJYH0gKE61eXp9a8f5VwvT02FAs, mLdLJYH0gKE61eXp9a8f5VwvT02FAs@facebook.com
7eePLejlvZh1EyMcmyStv1nLCsgPGX, 7eePLejlvZh1EyMcmyStv1nLCsgPGX@youtube.com
dIHHVdlQk6PwLlDGPPHILcCTgrP5Hs, dIHHVdlQk6PwLlDGPPHILcCTgrP5Hs@yahoo.com
4fcLsjXyM8u0Mu5e0gGUsHunMR414g, 4fcLsjXyM8u0Mu5e0gGUsHunMR414g@live.com
w9lDwET4SCGjcGChLb2Vy0hdFoEPsH, w9lDwET4SCGjcGChLb2Vy0hdFoEPsH@blogspot.com
uhRuwht5cAwTstdbJY3gWnXMeI4s8L, uhRuwht5cAwTstdbJY3gWnXMeI4s8L@wikipedia.org
WF0jJ2zAmyYyWEw3pNeIHTHAk93Q3T, WF0jJ2zAmyYyWEw3pNeIHTHAk93Q3T@baidu.com
UPm7eHu1scRoyPQRQCsP1QFetK6ejs, UPm7eHu1scRoyPQRQCsP1QFetK6ejs@twitter.com
2hBUCYzpI18VMsCuLN6fopJ465YOqy, 2hBUCYzpI18VMsCuLN6fopJ465YOqy@qq.com
uL3YTsHH7qnbF01186yHNROGhSuMVT, uL3YTsHH7qnbF01186yHNROGhSuMVT@msn.com
XAUXp3gwS6MhOWfDTsojdiwqt0lhkc, XAUXp3gwS6MhOWfDTsojdiwqt0lhkc@yahoo.co.jp
FNv7T9wdkEvxuyuDn6pPVKlc0Cuiki, FNv7T9wdkEvxuyuDn6pPVKlc0Cuiki@google.co.in
Pov60wAdp8cfEiX6WKg1zGstjKu6rv, Pov60wAdp8cfEiX6WKg1zGstjKu6rv@taobao.com
ujfF8HjlZIQkfqo5TraGzhBe9SWaud, ujfF8HjlZIQkfqo5TraGzhBe9SWaud@amazon.com
0hM6fmphoGt21KttYQXbj3GkHtvmhi, 0hM6fmphoGt21KttYQXbj3GkHtvmhi@sina.com.cn
xS3QVNHXolfn2qgYEIwna7Wcp2towv, xS3QVNHXolfn2qgYEIwna7Wcp2towv@linkedin.com
4LMVDySGgfo0SQW9Tty7AANiLEp3JK, 4LMVDySGgfo0SQW9Tty7AANiLEp3JK@bing.com
h3EwfrfTr4F95M5Lu741XBuo9Acwzs, h3EwfrfTr4F95M5Lu741XBuo9Acwzs@google.de
QQ0ha2yQHhfNDLoczRHrbePU6HO9Gs, QQ0ha2yQHhfNDLoczRHrbePU6HO9Gs@wordpress.com
zrMcbAf1XnqCKR7rad03ExPfgFpKP2, zrMcbAf1XnqCKR7rad03ExPfgFpKP2@google.com.hk
3BKXd4IbLOhwHJ31RekSFr4gGVP4Zm, 3BKXd4IbLOhwHJ31RekSFr4gGVP4Zm@google.co.uk
LcEjGPqgAIvSs204uVlD7TUcw1UpZb, LcEjGPqgAIvSs204uVlD7TUcw1UpZb@yandex.ru

Use auxiliary/client/smtp/emailer

Hfs, simplify simplify!

Let’r rip!

Your Linode, linode84209, has exceeded the notification threshold (1000) for disk io rate by averaging 10073.11 for the last 2 hours.

20k/emails sent in the first day

1500 ~interesting replies

A quick note on pulling down mail

larch --from imaps://imap.gmail.com --all --from-user aesopisthename@gmail.com --to imap://localhost --to-user aesop

You’ve got mail!

Abuse@linode.com?!?

Aww, crap.

Yo, I’m not a spammer!

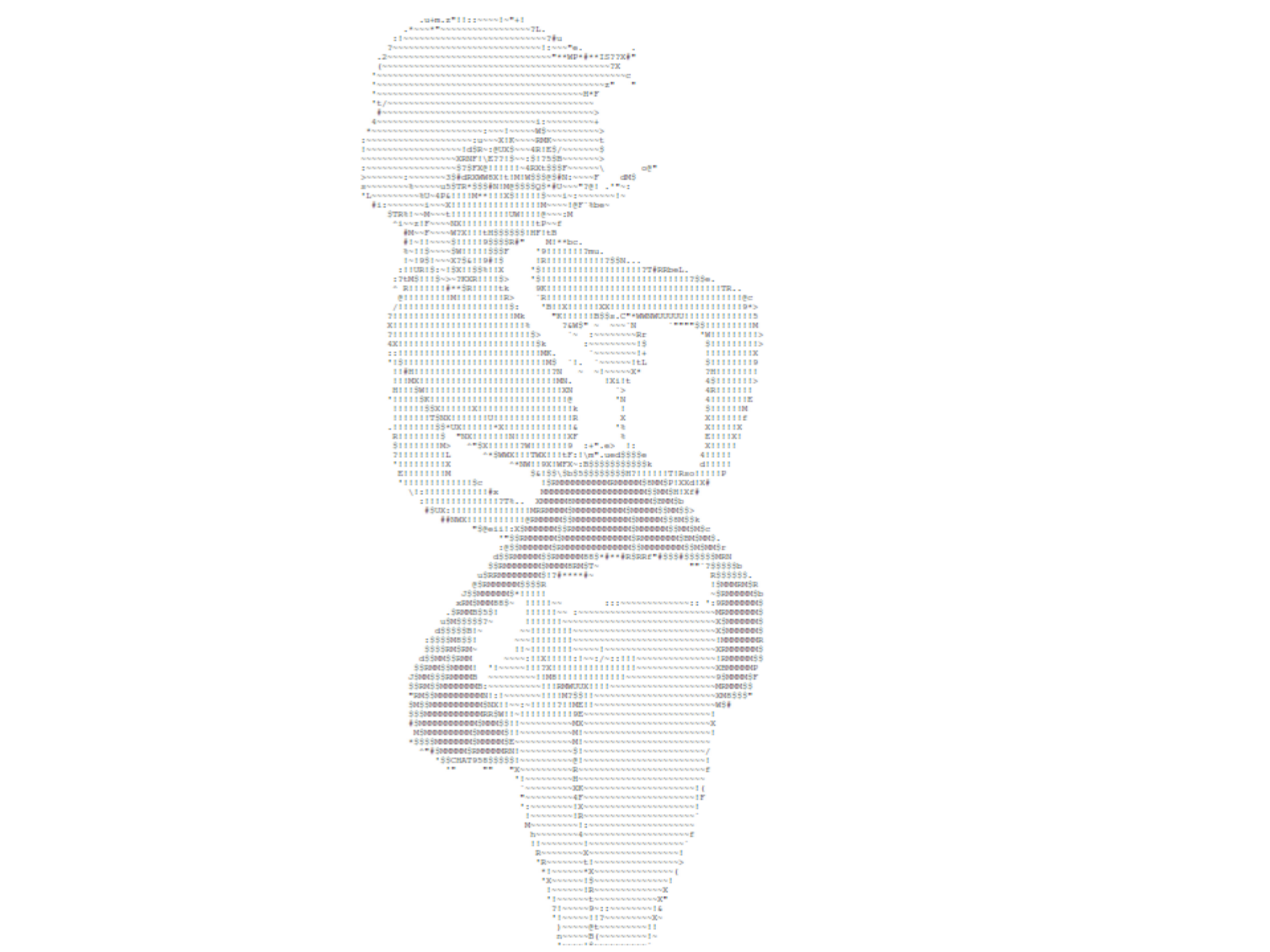

I’m tuna fishing!

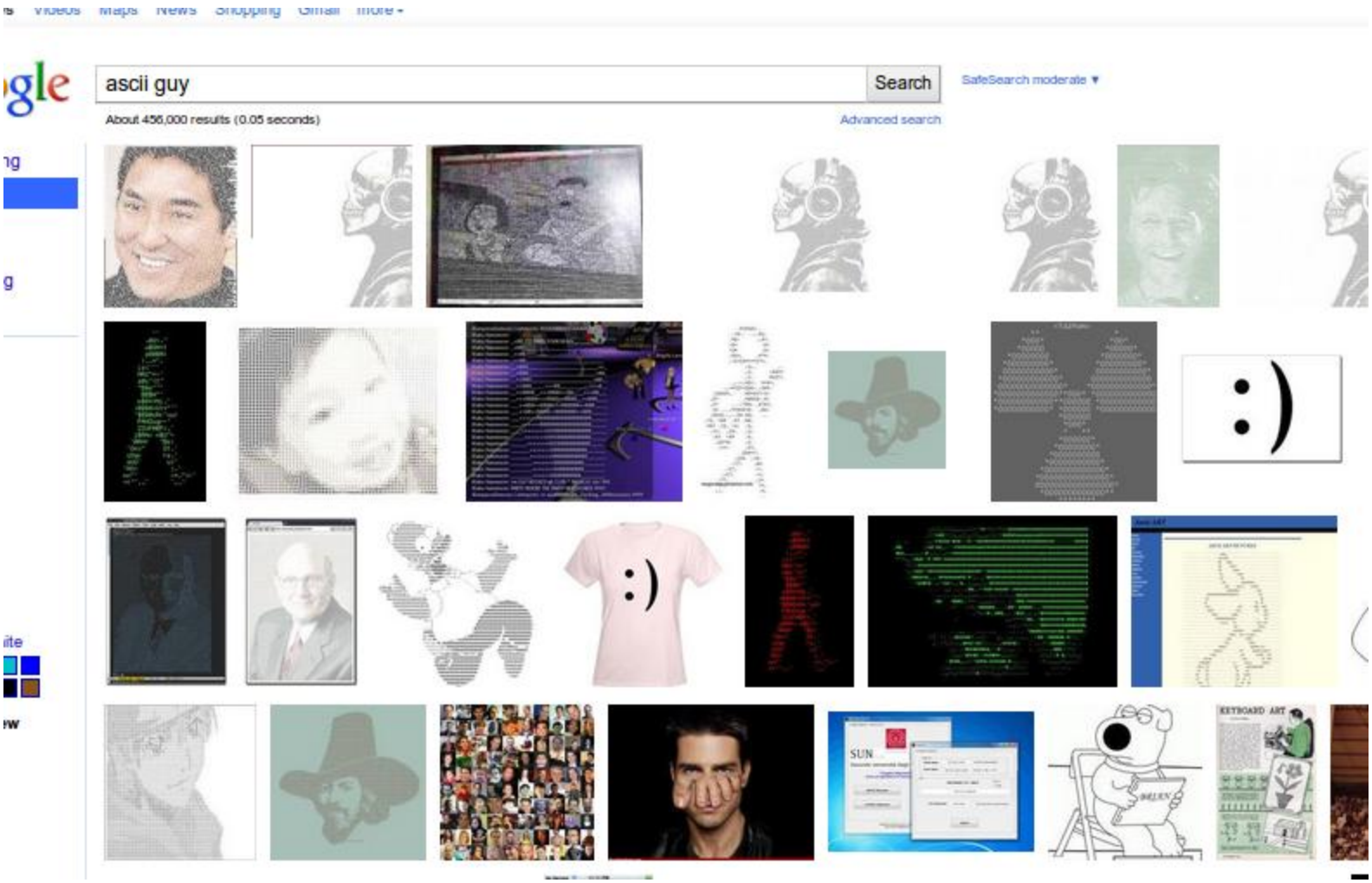
Clean-mx.de

auto-complaint on a 550?

Quick review of SMTP errors

550 Requested action not taken: mailbox unavailable (E.g., mailbox not found, no access)




ascii guy
Search
SafeSearch moderate
About 456,000 results (0.05 seconds)
Advanced search
:)
:)
SUN
KEYBOARD ART

Videos Maps News Shopping Gmail more

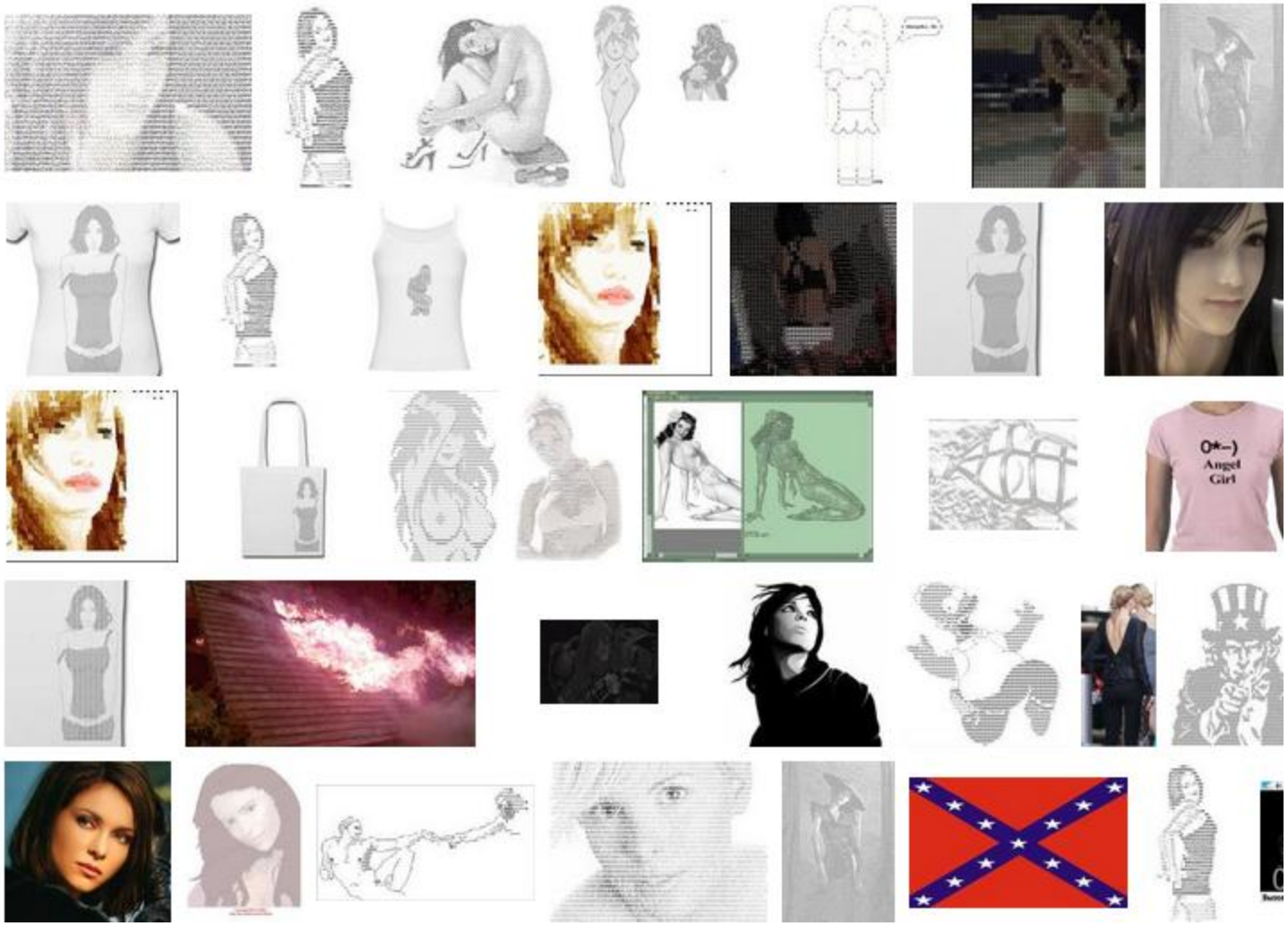
gle

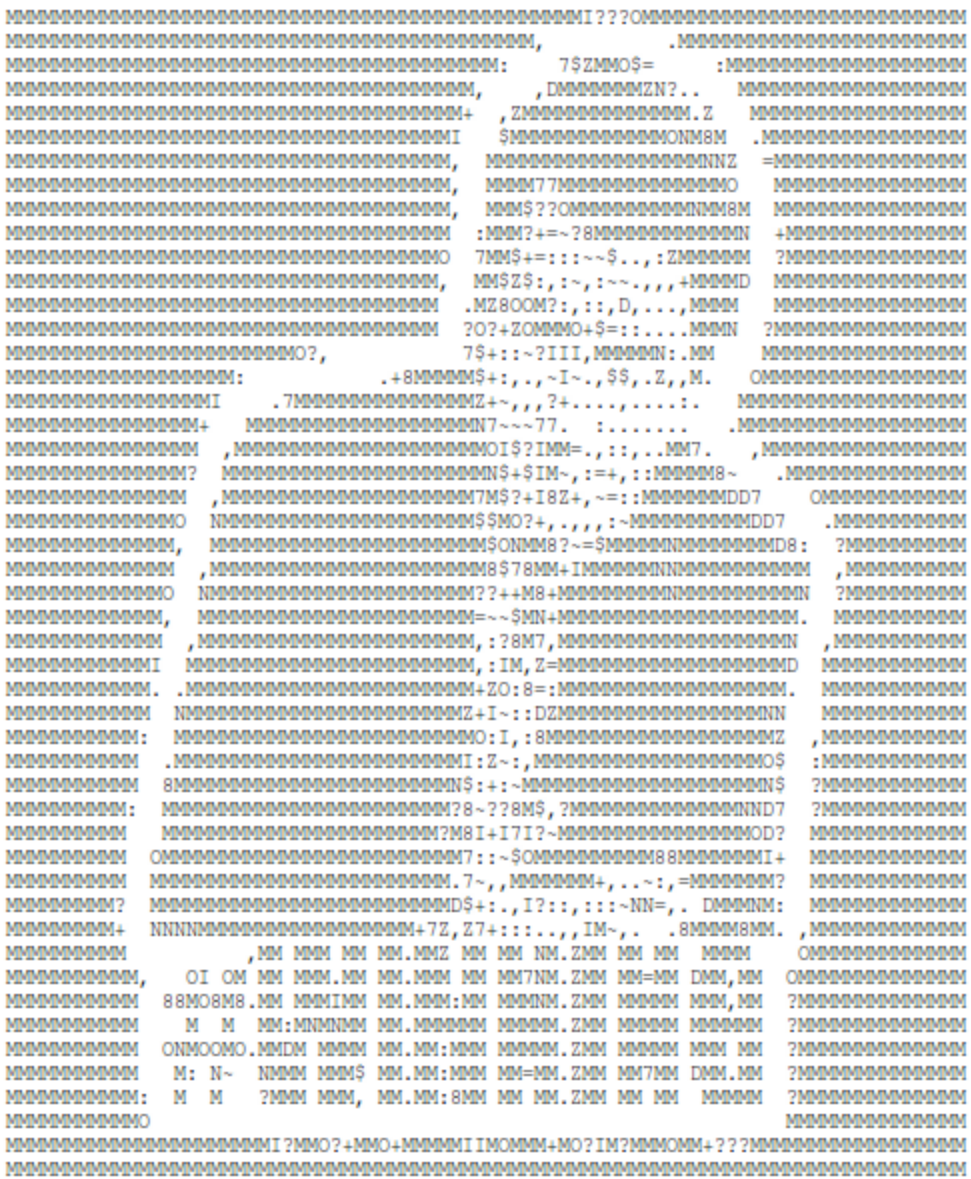
ascii girl Search

SafeSearch moderate

About 269,000 results (0.34 seconds)

Advanced search




GlassGiant.com

400k emails.
3 complaints.

<lyu9MpLX25Hv5rr2mulSW9Ma20iBrO@press1.de>
<vmySmBDV0XxDrjLR0g3nKN6WQznifS@clean-mx.de>
fVoRYQNejjA2mFF3cQGFjdpDSJKZ1d@ibusiness.de


FACEPALM
Because expressing how dumb that was in words just doesn't work.

apologize for the confusion -- you've provided more than enough information, thank you! However in the past, we have had security researches block hosts/ranges of companies who have these types of reporting systems in place to minimize the amount of complaints generated by their Linode(s). At the moment, it appears that these complaints are mainly coming from hosts that operate within netpilot's network (netpilot.net) -- perhaps you could exclude hosts netpilot's network from your tests? This is just a suggestion, however it may help to minimize the frequency of these tickets!

In any case, I have also gone ahead and made a note on your account to let members of our support team know about the security research your are carrying out, which should make future reports a lot easier to deal with.

Once again, I apologize for the confusion. Feel free to resumeyour mailer script :)!

Best Regards,
Danny Ariti

Linode rocks.

Linode rocks.

This is where the AHA left off.

And this is where the fun begins.

379702 emails sent

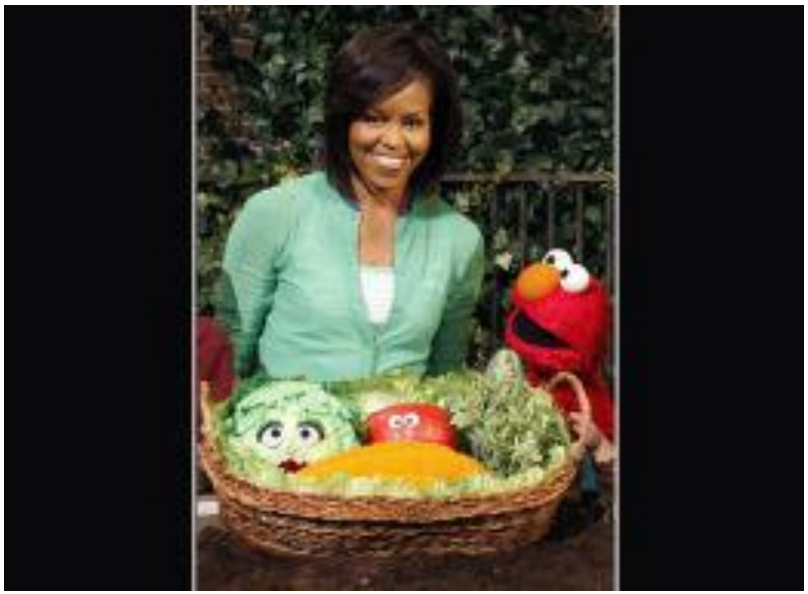
You are currently using 4995 MB (66%) of your 7560 MB.

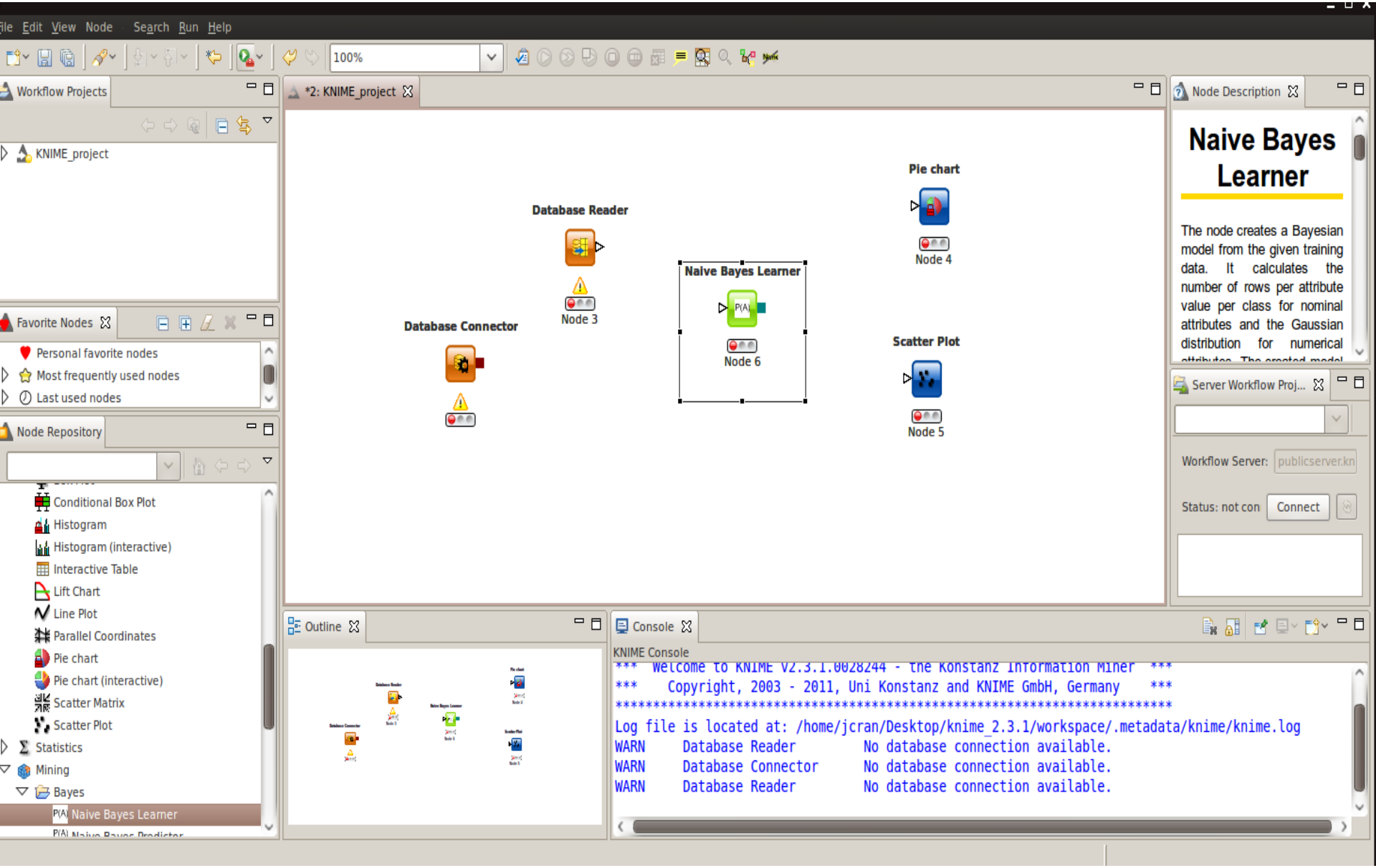
Processed ~100k

~20,000 “interesting”responses

The numbers are fail.

A Quick PSA




File Edit View Node Search Run Help
100%
Workflow Projects
KNIME_project
Favorite Nodes
Personal favorite nodes
Most frequently used nodes
Last used nodes
Node Repository
Conditional Box Plot
Histogram
Histogram (interactive)
Interactive Table
Lift Chart
Line Plot
Parallel Coordinates
Pie chart
Pie chart (interactive)
Scatter Matrix
Scatter Plot
Statistics
Mining
Bayes
Naive Bayes Learner
*2: KNIME_project
Database Reader
Node 3
Database Connector
Naive Bayes Learner
Node 6
Pie chart
Node 4
Scatter Plot
Node 5
Node Description
Naive Bayes Learner
The node creates a Bayesian model from the given training data. It calculates the number of rows per attribute value per class for nominal attributes and the Gaussian distribution for numerical
Server Workflow Proj...
Workflow Server:
publicserver.kn
Status: not con
Connect
Outline
Console
KNIME Console
*** Welcome to KNIME V2.3.1.0028244 - the Konstanz Information Miner ***
*** Copyright, 2003 - 2011, Uni Konstanz and KNIME GmbH, Germany ***
Log file is located at: /home/jcran/Desktop/knime_2.3.1/workspace/.metadata/knime/knime.log
WARN Database Reader No database connection available.
WARN Database Connector No database connection available.
WARN Database Reader No database connection available.

lazy

Rails!

Rails =/= Analysis

pengwynn


creativ
xarxes
col·laboració
09-05-09 18:13

TUNA FACTORY!

Rapid7

When all you have is a hammer

Ghetto Mail Analytics

MTA?

```
aesop@bolivia:~/operation_tuna/mail$ cat * | grep Exchange | wc
1303   12023   84282
aesop@bolivia:~/operation_tuna/mail$ cat * | grep Postfix | wc
5447   36288  308272
aesop@bolivia:~/operation_tuna/mail$ cat * | grep -i sendmail | wc
15     141    1397
aesop@bolivia:~/operation_tuna/mail$ cat * | grep -i bigfish | wc
3090   18574  226804
aesop@bolivia:~/operation_tuna/mail$ cat * | grep -i sophos | wc
751    1624   40942
aesop@bolivia:~/operation_tuna/mail$ cat * | grep -i barracuda | wc
640    2942   43602
```

Antispam?

Antivirus?

Irancell.ir

X-QHPSI: clean
Received: (indimail 5206 invoked by uid 555); 17 Feb 2011 01:53:46 +0330
DKIM-Status: no signatures
DomainKey-Status: no signature
Received: from unknown (HELO drl423.irancell.ir) (::ffff:10.132.62.138)
  by 0 with ESMTPS; 17 Feb 2011 01:53:46 +0330
X-QHPSI: clean
Received: (indimail 19157 invoked by uid 555); 17 Feb 2011 01:53:46 +0330
DKIM-Status: no signatures
DomainKey-Status: no signature
Received: from unknown (HELO drl415.irancell.ir) (::ffff:10.132.62.138)
  by 0 with ESMTPS; 17 Feb 2011 01:53:46 +0330
X-QHPSI: clean
Received: (indimail 5182 invoked by uid 555); 17 Feb 2011 01:53:46 +0330
DKIM-Status: no signatures
DomainKey-Status: no signature
Received: from unknown (HELO drl423.irancell.ir) (::ffff:10.132.62.138)
  by 0 with ESMTPS; 17 Feb 2011 01:53:46 +0330
X-QHPSI: clean
Received: (indimail 19139 invoked by uid 555); 17 Feb 2011 01:53:46 +0330
DKIM-Status: no signatures
DomainKey-Status: no signature
Received: from unknown (HELO drl415.irancell.ir) (::ffff:10.132.62.138)
  by 0 with ESMTPS; 17 Feb 2011 01:53:46 +0330
X-QHPSI: clean

Remote host said: 554 too many hops, this message is looping (#5.4.6)

Accenture.com

Received: from AMRXV1001.dir.svc.accenture.com ([10.10.160.61]) by mtahm1100.accenture.com (Lotus Domino Release 5.0.9a) with ESMTP id 2011021616494061:171546 ; Wed, 16 Feb 2011 16:49:40 -0600
Received: from AMRXH3004.dir.svc.accenture.com ([10.63.34.26]) by AMRXV1001.dir.svc.accenture.com with Microsoft SMTPSVC(6.0.3790.3959); Wed, 16 Feb 2011 16:49:38 -0600
Received: from AMRXH3006.dir.svc.accenture.com (10.63.34.50) by AMRXH3004.dir.svc.accenture.com (10.63.34.26) with Microsoft SMTP Server (TLS) id 8.3.106.1; Wed, 16 Feb 2011 17:49:38 -0500
Received: from EMEXH3001.dir.svc.accenture.com (10.134.3.22) by AMRXH3006.dir.svc.accenture.com (10.63.34.50) with Microsoft SMTP Server (TLS) id 8.3.106.1; Wed, 16 Feb 2011 17:49:37 -0500
Received: from EMEXE3001.dir.svc.accenture.com (10.134.4.201) by EMEXH3001.dir.svc.accenture.com (10.134.3.22) with Microsoft SMTP Server (TLS) id 8.3.106.1; Wed, 16 Feb 2011 23:49:36 +0100
Received: from mail63-tx2-R.bigfish.com (65.55.88.112) by emexe3141.accenture.com (10.134.4.141) with Microsoft SMTP Server (TLS) id 8.3.106.1; Wed, 16 Feb 2011 23:49:35 +0100
Received: from mail63-tx2 (localhost.localdomain [127.0.0.1]) by mail63-tx2-R.bigfish.com (Postfix) with ESMTP id 345A11720493 for <d5WPgvcCzuDVrcJxuZiDeXpdnXRcxm@accenture.com>; Wed, 16 Feb 2011 22:49:34 +0000 (UTC)
Received: from mail63-tx2 (localhost.localdomain [127.0.0.1]) by mail63-tx2 (MessageSwitch) id 1297896555693214_13963; Wed, 16 Feb 2011 22:49:15 +0000 (UTC)
Received: from TX2EHSMHS031.bigfish.com (unknown [10.9.14.240]) by mail63-tx2.bigfish.com (Postfix) with ESMTP id 1CF231C600CD for <d5WPgvcCzuDVrcJxuZiDeXpdnXRcxm@accenture.com>; Wed, 16 Feb 2011 22:48:41 +0000 (UTC)

Received: from AMRXV1001.dir.svc.accenture.com ([10.10.160.61]) by **mtahm1100.accenture.com (Lotus Domino Release 5.0.9a**) with ESMTP id 201102161649406l:171546 ; Wed, 16 Feb 2011 16:49:40 -0600

http://www.dominosecurity.org/A5581F/DominoSecurityOrg.nsf/c61b67c0b136c61e85256a00006c8d09/9709d3584b0fa22085256cde0069545b!OpenDocument

(01:21:32 AM) mubix: cat bigfish | sed 's/\ /\n/g' | grep bigfish | grep -P '^[0-9a-zA-Z]' | sed 's/[).;]$//' | sed 's/^dns;//' | xargs -I lookup dig lookup +short | sort | uniq -c | sort -n

(01:23:49 AM) mubix: 130 157.55.116.138
(01:23:49 AM) mubix: 144 94.245.120.74
(01:23:49 AM) mubix: 182 216.32.180.10
(01:23:49 AM) mubix: 342 65.55.88.10

What about shells, dude. shells.

Exim 4.72?

Displaying **all 14** emails

Domain	Path	Distance	Updated At		
caringbridge.org	webmail.caringbridge.org	1	2011-03-12 18:38:36 UTC	Edit	Destroy
rgu.ac.uk	194.66.84.76 -> gse-mta-09.mimesweeper.biz	2	2011-03-12 18:38:01 UTC	Edit	Destroy
prestigeshop.com.ua	[192.168.3.4] -> mail.prestigeshop.com.ua	2	2011-03-12 18:42:15 UTC	Edit	Destroy
eurotours.at	localhost -> mx1.eurotours.at	2	2011-03-12 18:39:26 UTC	Edit	Destroy
oeamtc.at	(unknown -> scm3.oeamtc.at	2	2011-03-12 18:39:55 UTC	Edit	Destroy
irctc.co.in	irctc.co.in -> sehdev.irctc.co.in	2	2011-03-12 18:40:46 UTC	Edit	Destroy
a-lehdet.fi	amme2.A-lehdet.fi -> smtp2.a-lehdet.fi	2	2011-03-12 18:40:50 UTC	Edit	Destroy
ope01.local	isjpissc69peh1.ope01.local -> mx2.sb-sys.info	2	2011-03-12 18:41:41 UTC	Edit	Destroy
yayoi-kk.co.jp	[219.101.215.123] -> smtp.ambisys.net	2	2011-03-12 18:39:20 UTC	Edit	Destroy
j2global.com	[204.11.170.19] -> worden.electric.net -> footwork.electric.net	3	2011-03-12 18:36:34 UTC	Edit	Destroy
stagecoachbus.com	unknown -> 12651 -> mail92.messagelabs.com	3	2011-03-12 18:40:36 UTC	Edit	Destroy
vvs.de	mail.ad.vvs.de -> [10.70.133.3] -> mail.vvs.de	3	2011-03-12 18:41:04 UTC	Edit	Destroy
mhro1b.mayo.edu	mhro1b.mayo.edu; -> mhro1b.mayo.edu -> mail9.mayo.edu	3	2011-03-12 18:36:00 UTC	Edit	Destroy
mail.sbigroup.co.jp	sbig-sc4.sbig.local -> mx5.sbigroup.co.jp -> mx8.sbigroup.co.jp -> mx8.sbigroup.co.jp	4	2011-03-12 18:39:44 UTC	Edit	Destroy


...brains...
Or tuna. Tuna is fine.
ICANHASCHEEZBURGER.COM

Creds & References:
Metasploit Team
Linode
http://www.marktheshark.com/
Michelle Obama