Successful Non-Governmental Threat Attribution, Containment and Deterrence: A Case Study

Joe St Sauver, Ph.D.

joe@internet2.edu or joe@uoregon.edu

Internet2 Nationwide Security Programs Manager

November 2nd, 2010, 1:15-2:30 PM, Chancellor I

http://pages.uoregon.edu/joe/attribute-contain-deter/

Disclaimer: The opinions expressed are those of the author and do not necessarily represent the opinion of any other party.

I. Introduction

Cyberspace: Anonymous and Undeterred?

- General Keith Alexander, Director of the National Security Agency (DIRNSA), recently commented [1] that in cyberspace:

> **“It is difficult to deliver an effective response if the attacker's identity isn't known,” and**
>
> **“It is unclear if the government's response to cyber threats and attacks have deterred criminals, terrorists, or nations.”**

- That's a provocatively framed (if equivocal) assessment, and one worthy of careful consideration given its source.

Is The Concept of Deterrence Even Relevant to Attacks on Private Critical Cyber Infrastructure?

- In pondering that quote, I also note the National Research Council's (NRC's) "Cyber Deterrence Research and Scholarship" question number 39, [2] which asked:

> **How and to what extent, if at all, is deterrence applicable to cyber attacks on private companies (especially those that manage U.S. critical infrastructure)?**

- Since the Office of the Director of National Intelligence (ODNI) requested the NRC's inquiry into cyber deterrence, and since General Alexander is now leading the new United States Cyber Command as well as the National Security Agency, it is appropriate to consider these two questions jointly.

Can We Identify An Example of Successful Attribution and Cyber Deterrence?

- If we are to prove that cyber deterrence is both relevant and possible, and that the difficulties associated with attribution can be overcome, we must be able to point to at least <u>one</u> example of successful attribution and cyber deterrence.

- I believe that there is at least one noteworthy example of successful non-governmental cyber threat attribution, containment and deterrence, and that's in the area of spam.

- I refer, of course, to **the Spamhaus Project's global anti-spam efforts.**

But Is *ANY* Part of Information Technology Really “Critical Infrastructure?”

- There's a temptation to paraphrase Mr. Justice Stewart's famous remark from his concurring opinion in *Jacobellis v. Ohio* [3] -- when it comes to critical infrastructure, like some other things, "we know it when we see it.”
- For example, if you were to ask average Americans to describe some "critical infrastructure," their responses would surely includes things such as the national power grid and key energy pipelines, dams, major airports, our interstate highways and critical bridges, banks and stock exchanges, chemical plants and refineries, etc.
- It is inconceivable that anyone responsible for our homeland security would disagree that those facilities are part of our nation’s "critical infrastructure.”

Formal Definitions of Critical Infrastructure

- But did you know that critical infrastructure has a formal definition which has evolved over time? E.G., in 2004, in "Critical Infrastructure and Key Assets: Definition and Identification," the Library of Congress Congressional Research Service examined the evolution of the term "critical infrastructure" over a period of 20 years. [4] While infrastructure components were added or subtracted overt that time span, "information systems" (or "information technology") has been part of all definitions of "critical infrastructure" since 1998, and "telecommunications" has been part of "critical infrastructure" since at least 1996.
- Some, such as Theodore Gyle Lewis, go so far as to assert that telecommunications was the earliest critical infrastructure sector, dating to the telecommunication failures of the Cuban Missile Crisis in 1962. [5]

Information Technology Unequivocally Remains Part of "Critical Infrastructure" Today

- The Department of Homeland Security makes it clear that "Information Technology" remains a key part of critical infrastructure sector today. According to DHS, the Information Technology sector plays a role which is...

> *central to the nation's security, economy, and public health and safety. Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. These virtual and distributed functions produce and provide hardware, software, and IT systems and services, and -- in collaboration with the Communications Sector -- the Internet. [6]*

Critical IT Infrastructure Isn't Just Hardware

- In thinking about information technology and telecommunications, it is tempting to focus on just tangible assets -- computers, fiber and copper circuits, routers, switches, and other hardware.
- "Infrastructure" unquestionably includes those sort of physical assets, but is that ALL it includes?
- We must remember that physical information technology assets have little intrinsic value in and of themselves, divorced from the protocols, operating systems, and applications running on those assets, and the information, transactions, and relationships that that software and hardware combine to enable.
- Applications can be critical, too.
- So what happens if email isn't available?

Email Outages Can Be Paralyzing

- Consider the January 2009 White House email outage which lasted over eight hours. [7]

- While it was reported that "there was no indication that the outage caused any sort of national calamity," it was also reported that "several administration officials said that business had ground to a halt because of the disruption."

- In general, however, because email is architected as a distributed and survivable service, even if email service fails at a single site (even a site as important as the White House), email usually continues to be available elsewhere.

How Might You “Kill” Email Worldwide?

- We can, however, imagine scenarios under which email would NOT be available/usable worldwide.
- Prime among those scenarios would be a failure of spam filtering.
- Email may not be the New York Stock Exchange (NYSE) or the international air traffic control system, but email is unquestionably essential to every modern organization, a point which is quickly driven home when even brief partial outages occur.
- Without effective anti-spam measures, email would quickly degenerate into unusability. Skeptics can verify this by briefly disabling their own spam filtering!
- Spamhaus is a key part of protecting the email infrastructure worldwide. Let’s review a little about what Spamhaus offers to the community.

II. Understanding Spamhaus

A Brief Overview of the Spamhaus Project

- Because many may never have heard of the Spamhaus Project, and even among those who have heard of it, there are often misconceptions about what the Spamhaus Project is, how it operates, the size of its user base, etc., let's begin with a brief overview of it.

- Since we're not members of the Spamhaus Project team, for the purpose of this talk we'll primarily rely on the description of the Spamhaus Project that's available from its website. [8]

- Condensing that description into bullet format…

Spamhaus Organization and Mission

- **Organization:** The Spamhaus Project is an international nonprofit organization, founded in 1998, and based in Geneva and London.

- **Mission:** The Spamhaus Project's mission is to:

  -- track the Internet's spam operations,
  -- to provide dependable real time anti-spam protection for Internet networks,
  -- to work with law enforcement agencies to identify and pursue spammers worldwide, and
  -- to lobby governments for effective anti-spam legislation.

Spamhaus Funding, Staffing and Leadership

- **Funding:** Funding for operations is through sponsors and donations from industry, including from The Spamhaus Foundation, a private Foundation whose charter is to assure the long-term security of The Spamhaus Project and its work.

- **Staffing:** The Spamhaus Project is staffed by volunteers, including 28 investigators and forensic specialists located in 8 countries.

- **Leadership:** Steve Linford, Founder and CEO

Spamhaus Infrastructure, Market Presence, And Information Products

- **Infrastructure:** Spamhaus has built one of the largest DNS infrastructures in the world. Its network of over 60 public DNSBL servers spread across 18 countries serves many billions of DNSBL queries to the public every day, free of charge.

- **Market Presence:** The mailboxes of over **1.4 billion** Internet users are currently protected by Spamhaus DNSBLs. [9]

- **Information Products:** Spamhaus is best known for its real time block lists, such as the SBL (Spamhaus Block List).

SBL (The Spamhaus Block List)

- Operationally, the Spamhaus Project provides its six primary anti-spam block lists via the domain name system (high volume sites make arrangements to do zone transfers and run private mirrors of the Spamhaus block list zones locally).

- The first of those six block lists is the SBL. [10]

> *The Spamhaus Block List ("SBL") Advisory is a database of IP addresses which do not meet Spamhaus's policy for acceptance of inbound email and therefore from which Spamhaus does not recommend the acceptance of electronic mail.*
>
> *IP addresses are listed on the SBL because they appear to Spamhaus to be under the control of, or made available for the use of, senders of Unsolicited Bulk Email ("spammers").*
>
> *The SBL database will normally include IPs identified to Spamhaus's best ability as likely direct spam sources, spammer hosting/DNS, spam gangs and spam support services. [...]*

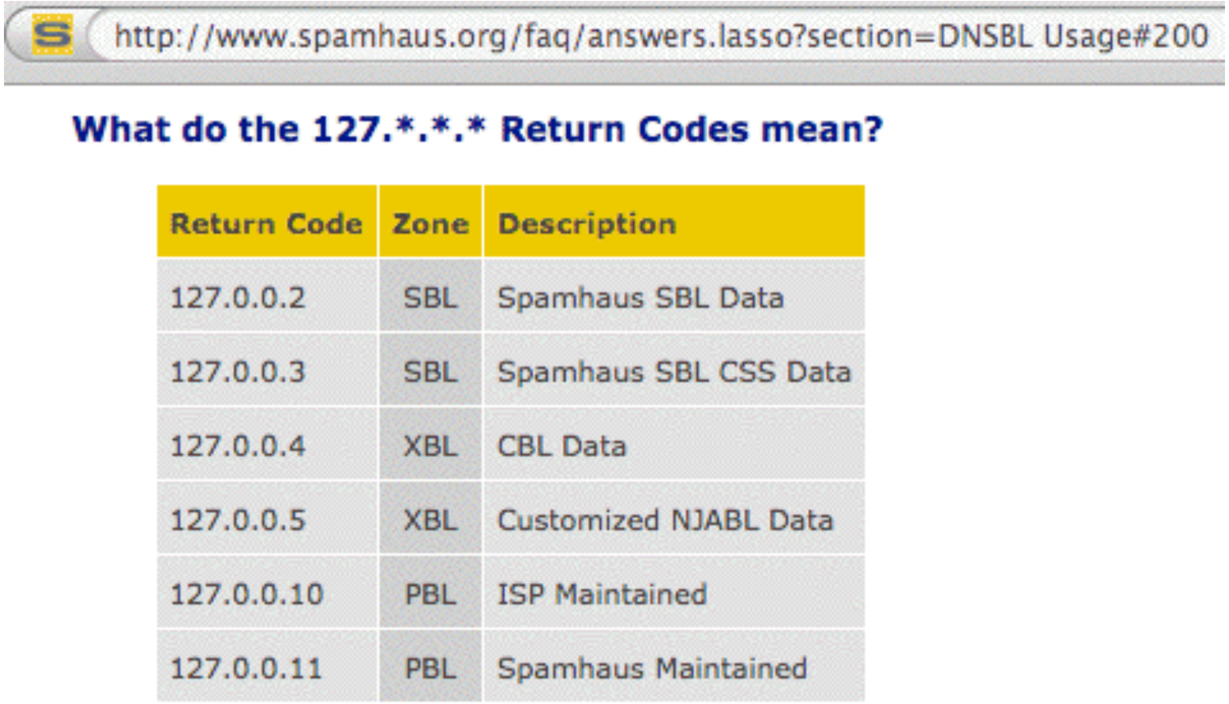
SBL (The Spamhaus Block List) (cont.)

- *The criteria for listing IP addresses in the SBL are:*
  - ***Spam Sources:*** *Sources of unsolicited bulk email sent to Spamhaus spamtraps or submitted to Spamhaus by trusted 3rd party intelligence.*
  - ***Spam Services:*** *Servers, including mail, web, dns and other servers identified as being an integral part of a spam operation or being under the direct control of spammers.*
  - ***Spam Operations:*** *Known spam operations and gangs listed in Spamhaus ROKSO registry, including preemptively listing new IPs each time known spammers move to new hosts.*
  - ***Spam Support Services:*** *Services providing service to known spam operations listed on ROKSO, services providing 'bullet-proof hosting' for spam service purposes, services obfuscating or anonymising spam senders, services selling or providing hosting for the sales or distribution of spamware or address lists, and networks knowingly hosting spammers as either stated or de facto policy.*

SBL Values Returned via DNS

- The SBL returns coded DNS values to signal when a site has been listed. For example, manually checking 88.255.78.101:

```
% dig +short 101.78.255.88.sbl.spamhaus.org
127.0.0.2
```

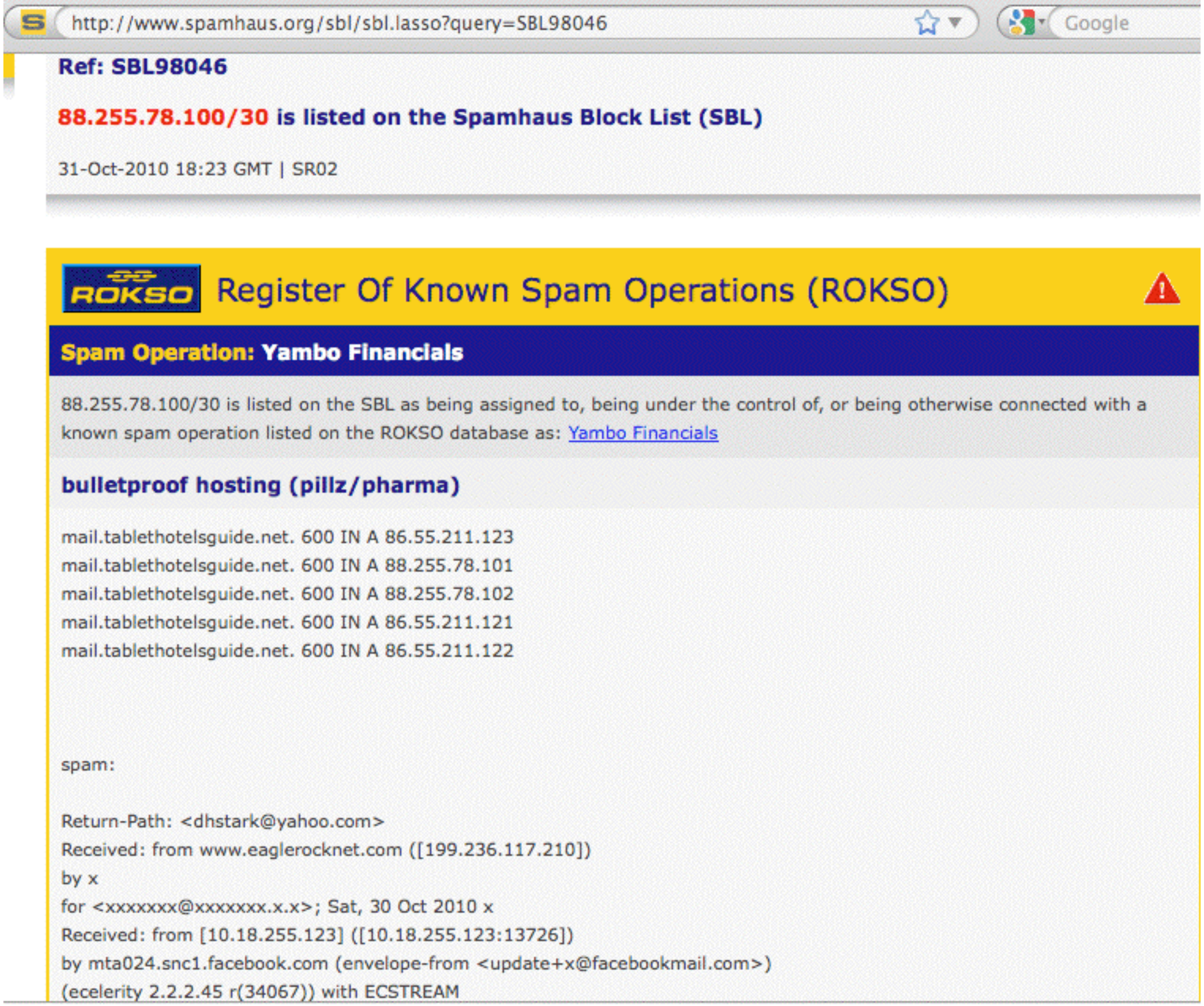


http://www.spamhaus.org/faq/answers.lasso?section=DNSBL Usage#200

What do the 127.*.*.* Return Codes mean?

Return Code	Zone	Description
127.0.0.2	SBL	Spamhaus SBL Data
127.0.0.3	SBL	Spamhaus SBL CSS Data
127.0.0.4	XBL	CBL Data
127.0.0.5	XBL	Customized NJABL Data
127.0.0.10	PBL	ISP Maintained
127.0.0.11	PBL	Spamhaus Maintained

Sample SBL Listing Web Page



Ref: SBL98046

88.255.78.100/30 is listed on the Spamhaus Block List (SBL)

31-Oct-2010 18:23 GMT | SR02

Register Of Known Spam Operations (ROKSO)

Spam Operation: Yambo Financials

88.255.78.100/30 is listed on the SBL as being assigned to, being under the control of, or being otherwise connected with a known spam operation listed on the ROKSO database as: Yambo Financials

bulletproof hosting (pillz/pharma)

```
mail.tablethotelsguide.net. 600 IN A 86.55.211.123
mail.tablethotelsguide.net. 600 IN A 88.255.78.101
mail.tablethotelsguide.net. 600 IN A 88.255.78.102
mail.tablethotelsguide.net. 600 IN A 86.55.211.121
mail.tablethotelsguide.net. 600 IN A 86.55.211.122
```

spam:

```
Return-Path: <dhstark@yahoo.com>
Received: from www.eaglerocknet.com ([199.236.117.210])
by x
for <xxxxxxx@xxxxxxx.x.x>; Sat, 30 Oct 2010 x
Received: from [10.18.255.123] ([10.18.255.123:13726])
by mta024.snc1.facebook.com (envelope-from <update+x@facebookmail.com>)
(ecelerity 2.2.2.45 r(34067)) with ECSTREAM
```

Key SBL Take-Aways

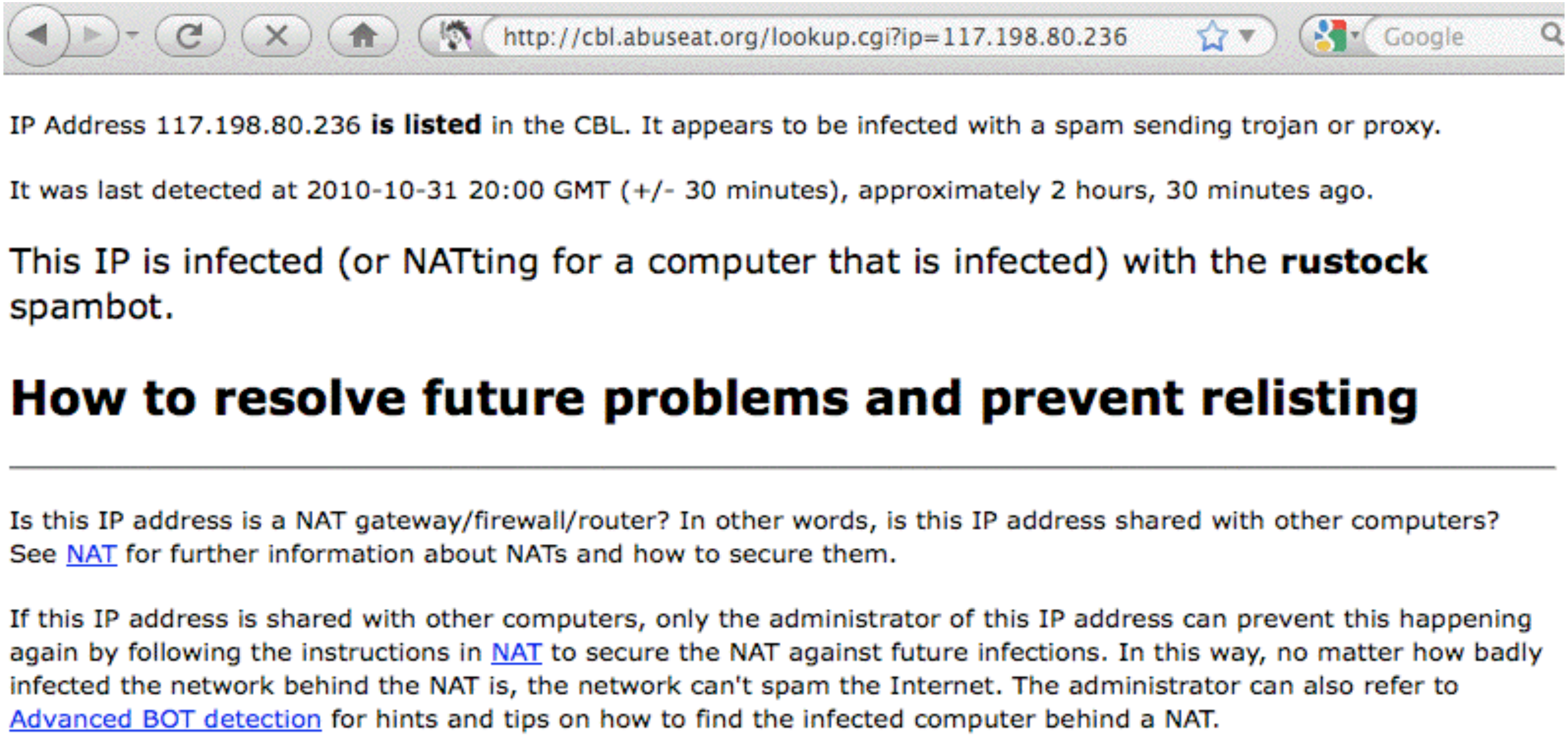
- IP address ranges are manually added to the SBL (removal requests are also handled manually)
- SBL listings list spammer controlled network resources
- All SBL listings are documented on the Spamhaus web site
- SBL listings are attributed/associated with spammers by name or spam outfit when that connection can be made
- If spammers only spammed from their own dedicated address space, this would be all we'd need to block spam
- But, because spammers find it difficult to spam once their network addresses have been listed, most spammers send via bots. Individual botted hosts are not listed on the SBL.
- Botted hosts spewing spam are addressed via the XBL, derived from the CBL, which we'll cover next.

XBL (The Spamhaus Exploits Block List)

- *The Spamhaus Exploits Block List (XBL) [11] is a realtime database of IP addresses of hijacked PCs infected by illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, wingate, etc), worms/viruses with built-in spam engines, and other types of trojan-horse exploits. [...]*

- *The XBL wholly incorporates data from two highly-trusted DNSBL sources, with tweaks by Spamhaus to maximize the data efficiency and lower False Positives. The main components are:*
  *- **the CBL (Composite Block List)** from cbl.abuseat.org*
  - the NJABL Open Proxy IPs list from www.njabl.org.

Sample CBL/XBL Listing



IP Address 117.198.80.236 **is listed** in the CBL. It appears to be infected with a spam sending trojan or proxy.

It was last detected at 2010-10-31 20:00 GMT (+/- 30 minutes), approximately 2 hours, 30 minutes ago.

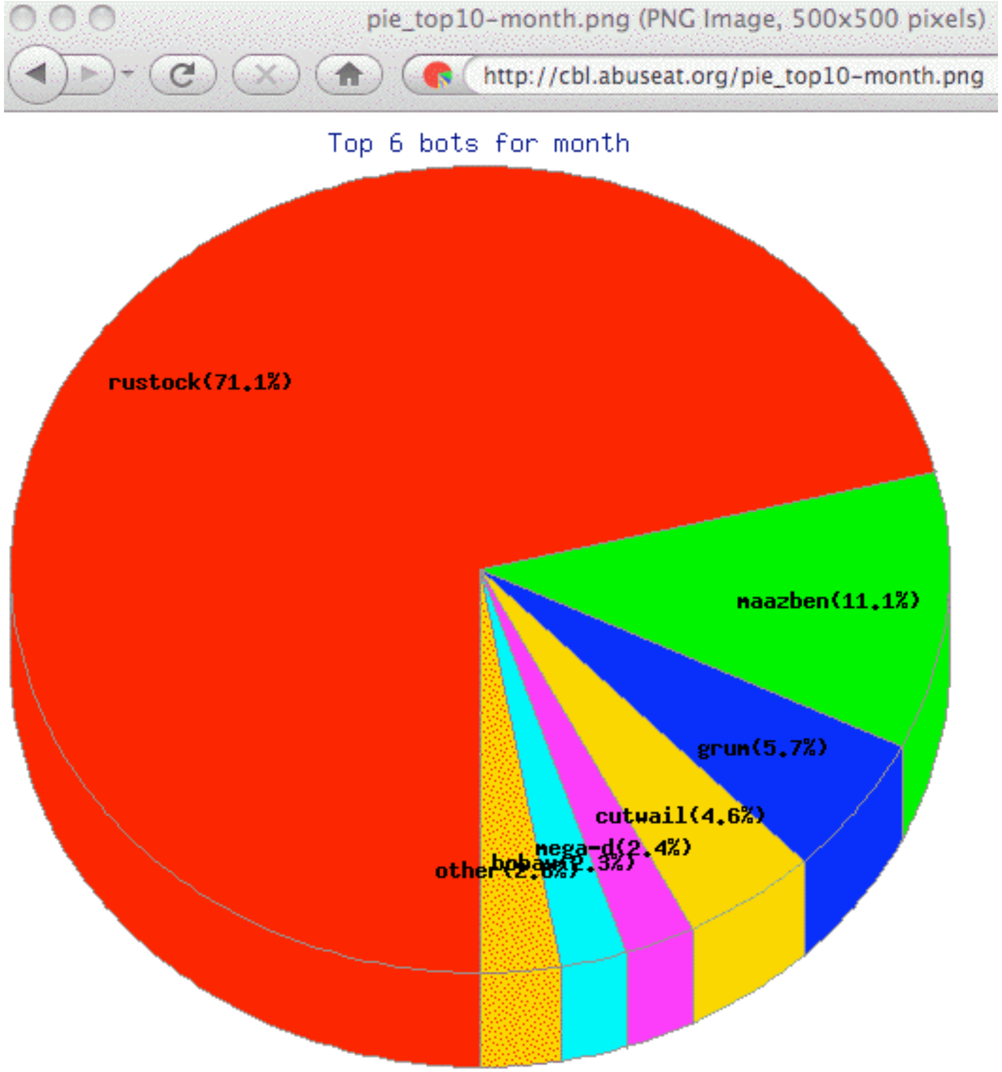
This IP is infected (or NATting for a computer that is infected) with the **rustock** spambot.

How to resolve future problems and prevent relisting

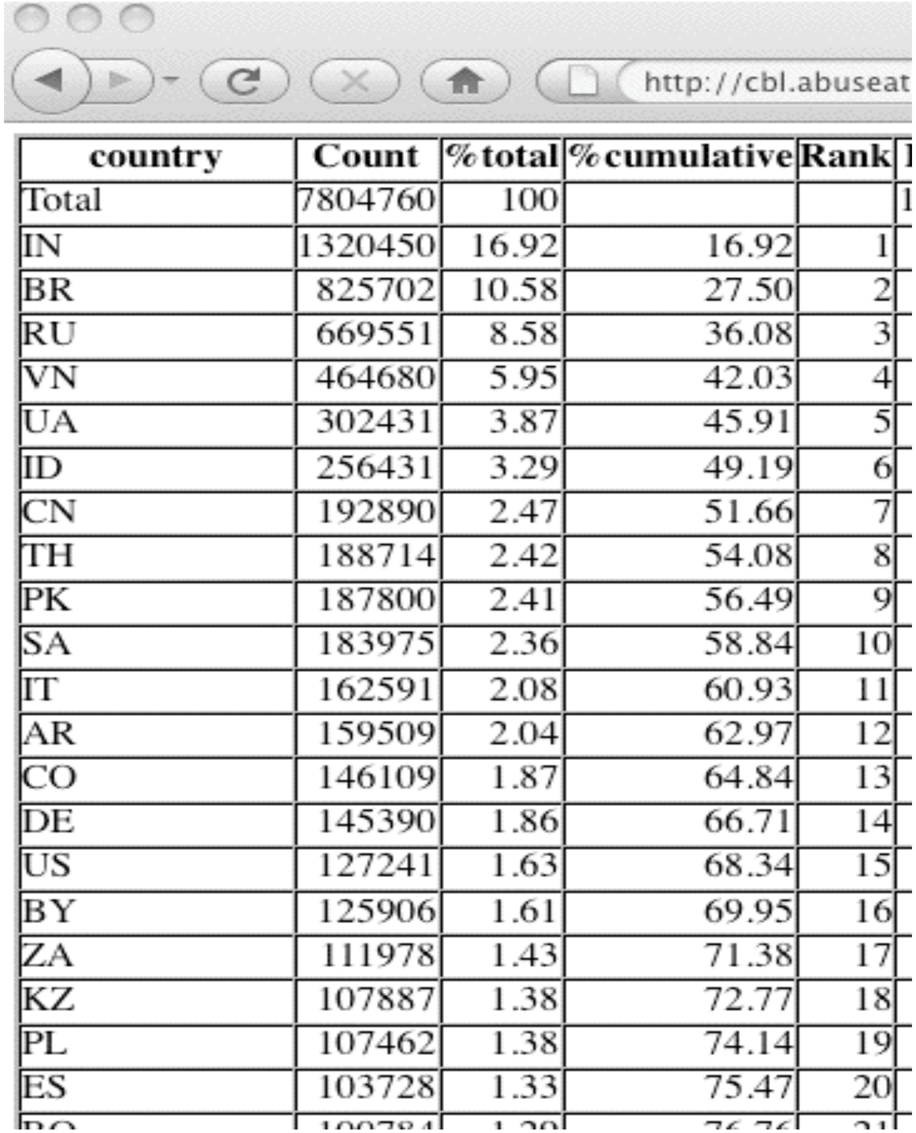
Is this IP address is a NAT gateway/firewall/router? In other words, is this IP address shared with other computers? See NAT for further information about NATs and how to secure them.

If this IP address is shared with other computers, only the administrator of this IP address can prevent this happening again by following the instructions in NAT to secure the NAT against future infections. In this way, no matter how badly infected the network behind the NAT is, the network can't spam the Internet. The administrator can also refer to Advanced BOT detection for hints and tips on how to find the infected computer behind a NAT.

The CBL Has Many Interesting Statistics… E.G., One Bot Dominates All Bot Spam Output



Bots in Just 20 Countries Do 75% of Bot Spam



country	Count	%total	%cumulative	Rank	I
Total	7804760	100			1
IN	1320450	16.92	16.92	1	
BR	825702	10.58	27.50	2	
RU	669551	8.58	36.08	3	
VN	464680	5.95	42.03	4	
UA	302431	3.87	45.91	5	
ID	256431	3.29	49.19	6	
CN	192890	2.47	51.66	7	
TH	188714	2.42	54.08	8	
PK	187800	2.41	56.49	9	
SA	183975	2.36	58.84	10	
IT	162591	2.08	60.93	11	
AR	159509	2.04	62.97	12	
CO	146109	1.87	64.84	13	
DE	145390	1.86	66.71	14	
US	127241	1.63	68.34	15	
BY	125906	1.61	69.95	16	
ZA	111978	1.43	71.38	17	
KZ	107887	1.38	72.77	18	
PL	107462	1.38	74.14	19	
ES	103728	1.33	75.47	20	
RO	100784	1.29	76.76	21	

Key XBL Takeaways

- XBL lists individual IP addresses (not IP address ranges, as the SBL does)
- XBL listings list compromised (or "botted") malware infected end user hosts observed to be sending spam
- IPs are mechanically/automatically listed on the XBL based on non-disclosed but apparently quite reliable indicia
- IPs can be manually delisted by the system owner (after all, if they get used to send spam again, they'll just end up quickly relisted).
- IP addresses that haven't been seen spamming for some time will be automatically "aged out"
- Roughly **8 million** hosts are currently on the XBL
- Botted computers in just 20 countries account for 3/4ths of all the botted computers sending spam worldwide.

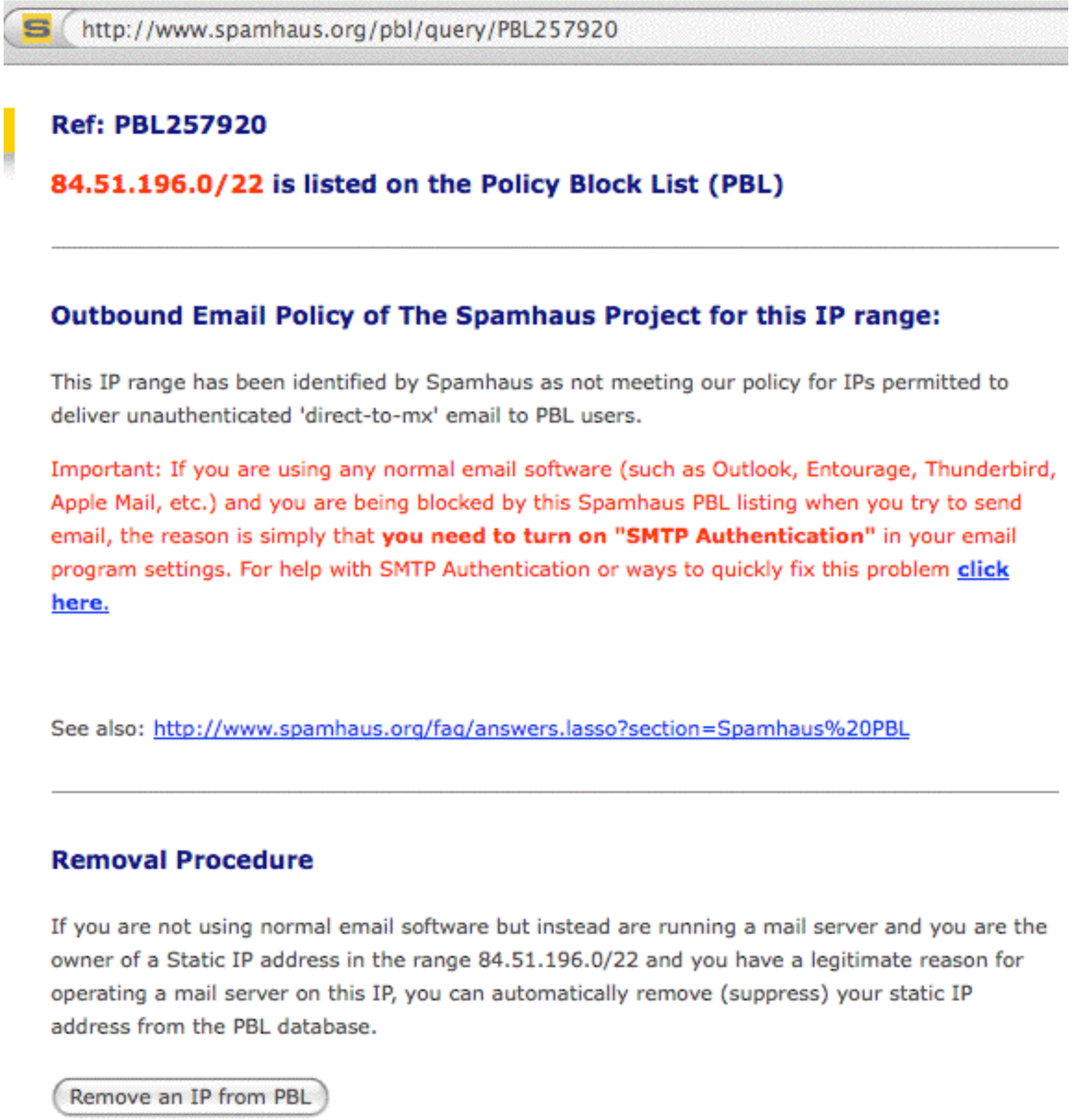
Non-Mail-Server Address Space

- Consumer PCs normally get their IP address via DHCP.
- This means that the address I use today may have been used by you an hour ago, and someone else yesterday, and still another person may use it tomorrow. There's no way to meaningfully accumulate "reputation" information about senders on dynamic addresses because so many different people may sequentially be using a single IP.
- Moreover, many ISPs prohibit consumers from running connections on dynamic addresses – if you want to run a mail server or web server, you're supposed to be paying more to get a static IP address and a "business-class" connection which will explicitly permit you to run servers.
- Consumers on dynamic addresses, therefore, should not be running servers on dynamic addresses.
- The Spamhaus PBL (Policy Block List) formalizes that…

PBL (The Spamhaus Policy Block List)

- *The Spamhaus PBL [12] is a DNSBL database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use.*
- *The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges. [...]*
- *The PBL lists both dynamic and static IPs, any IP which by policy (whether the block owner's or -interim in its absence- Spamhaus' policy) should not be sending email directly to the MX servers of third parties.*

Sample PBL Listing



http://www.spamhaus.org/pbl/query/PBL257920

Ref: PBL257920

84.51.196.0/22 is listed on the Policy Block List (PBL)

Outbound Email Policy of The Spamhaus Project for this IP range:

This IP range has been identified by Spamhaus as not meeting our policy for IPs permitted to deliver unauthenticated 'direct-to-mx' email to PBL users.

Important: If you are using any normal email software (such as Outlook, Entourage, Thunderbird, Apple Mail, etc.) and you are being blocked by this Spamhaus PBL listing when you try to send email, the reason is simply that **you need to turn on "SMTP Authentication"** in your email program settings. For help with SMTP Authentication or ways to quickly fix this problem **click here.**

See also: http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20PBL

Removal Procedure

If you are not using normal email software but instead are running a mail server and you are the owner of a Static IP address in the range 84.51.196.0/22 and you have a legitimate reason for operating a mail server on this IP, you can automatically remove (suppress) your static IP address from the PBL database.

How *Are* End Users Supposed To Send Email Then???

- End users should be sending their outbound email via the ISP's own customer-facing mail server, and that customer-facing mail server should be accepting that end user email traffic on port 587 (the "Submit" service).
- Port 587 traffic should be authenticated (e.g., the user should need to supply their username and password before being allowed to hand off their email traffic), and the port 587 traffic should be employing TLS encryption to protect those credentials from eavesdropping.
- Note that email coming from sites that follow this recommendation will be attributable since those messages will have been injected by an authenticated user, and the ISP could record that identity as part of a clear text or cryptographic X-header added to each message.

ZEN: SBL+XBL+PBL

- Q. "I've heard we use the Spamhaus 'Zen' block list – what's that?"
- A. For efficiency sake, Spamhaus offers a combined zone the includes all three of their main block lists: Zen is the union of the SBL+XBL+PBL, which means that a mail server can query all three lists with a single DNS lookup.

DBL (The Spamhaus Domain Block List)

- The preceding block lists were all oriented toward IP addresses, or IP address ranges. But what about domain names? Domain names can accrue reputation as well…
- *The Spamhaus DBL [13] is a realtime database of domains (typically web site domains) found in spam messages.*
- *Mail server software capable of scanning email message body contents for URIs can use the DBL to identify, classify or reject spam containing DBL-listed domains.*
- *The DBL is queriable in realtime by mail systems throughout the Internet, allowing mail server administrators to identify, tag or block incoming email containing domains which Spamhaus deems to be involved in the sending, hosting or origination of Unsolicited Bulk Email (aka "Spam"). [...]*

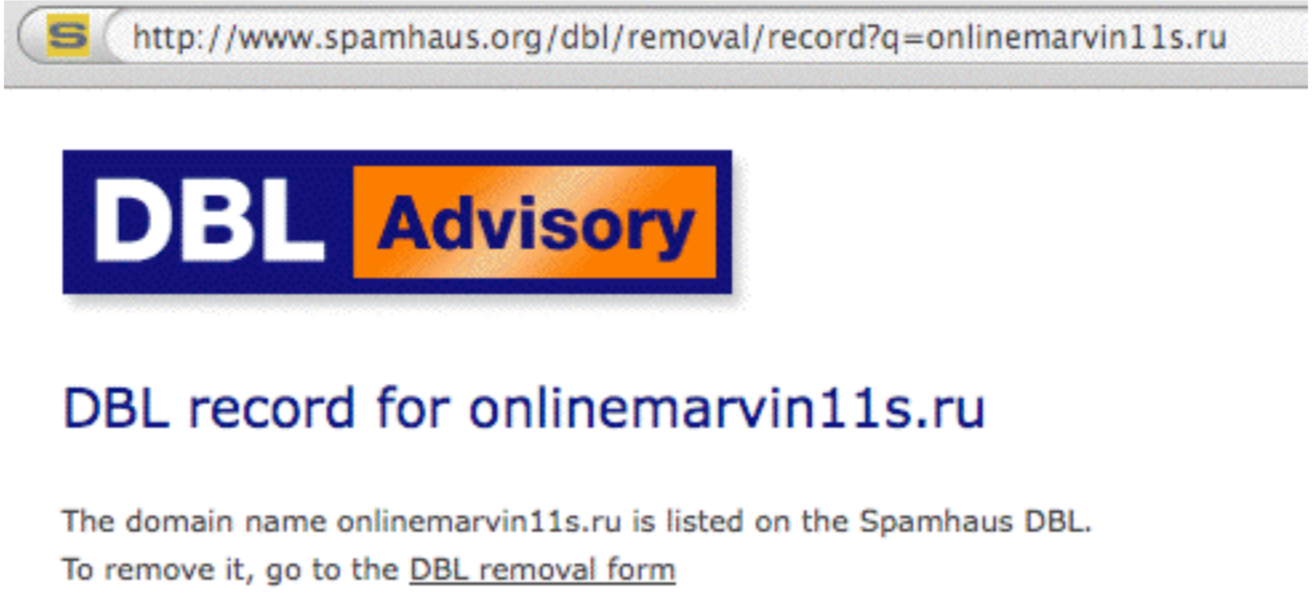
DBL (The Spamhaus Domain Block List) (cont.)

- *The DBL is both a domain URI Blocklist and RHSBL ["right hand side block list"].*

- *It is intended primarily for message body URI checks but it can additionally be used for connection checks at the SMTP level and header domain checks (HELO, connecting IP rDNS domain, From & Reply-To domains, Message-ID domain) and other checks involving domains.*

- In a nutshell, if you see a domain in a mail message's headers or a mail message body, think,
  "I wonder if it's on the Spamhaus DBL?"

Sample Spamhaus DBL Entry



http://www.spamhaus.org/dbl/removal/record?q=onlinemarvin11s.ru

DBL record for onlinemarvin11s.ru

The domain name onlinemarvin11s.ru is listed on the Spamhaus DBL.

To remove it, go to the DBL removal form

Spamhaus Whitelists: The SWL

- *The Spamhaus Whitelist [14] is a realtime database of IP addresses and domains which have passed security checks and whose owners/operators agree to the strict terms of the Spamhaus Whitelist program.*
- *It allows internet mail servers to separate incoming email traffic into 3 categories: Good, Bad and Unknown, allowing mail server operators to block known bad email traffic, let known good email traffic pass safely, and heavily filter unknown email sources. [...]*
- *The IP Address whitelist, the SWL, is designed to contain both IPv4 and IPv6 addresses. Although initially it will contain predominantly IPv4 addresses, it's future primary intended usage is to enable networks to implement IPv6 mail services with control over IPv6 spam.*

Whitelists: DWL

- *The Domain element of the whitelist, the DWL, enables automatic certification of domains with DKIM signatures.*
- If you're not familiar with DKIM, it is a cryptographic signature applied to mail by an ISP when the ISP is willing to attest that the mail came from them (or more accurately one of their users). For more on DKIM, see [15].
- See also Author Domain Signing Practices ("ADSP") as described in RFC5617. ADSP is a related protocol which, if used, describes the ISP's intentions when it comes to DKIM signing messages from its domain. Put simply, ADSP answers the question, "If there's no DKIM signature on a message, should I accept it anyway?"

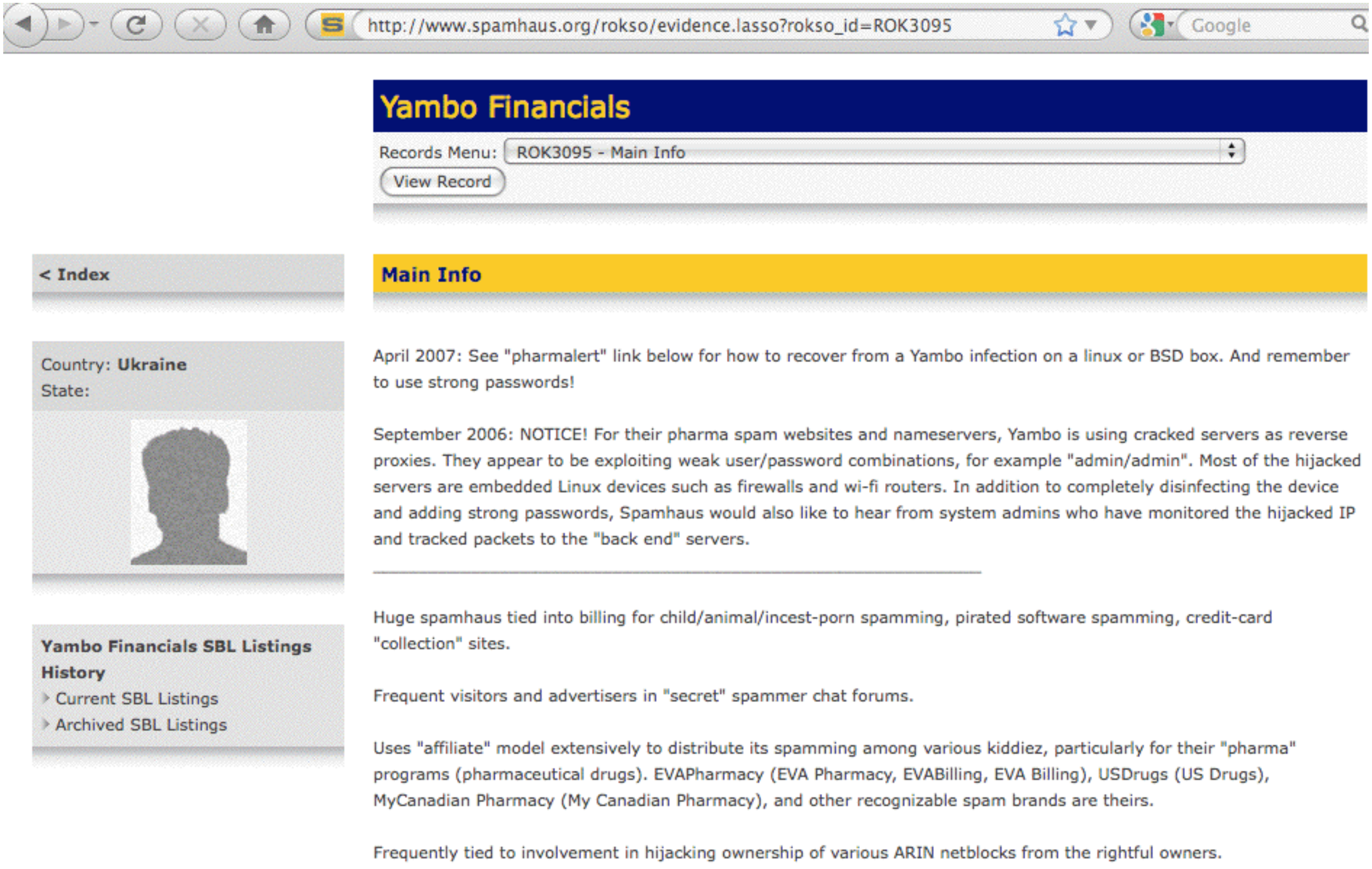
ROKSO

- Two other Spamhaus information products are also available, although they are delivered via the world wide web, rather than via DNS:

- **ROKSO (The Spamhaus Register of Known Spam Operations):** [16]

  The Register of Known Spam Operations (ROKSO) database collates information and evidence on known professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses.

Sample ROKSO Entry


http://www.spamhaus.org/rokso/evidence.lasso?rokso_id=ROK3095
Google
Records Menu: ROK3095 - Main Info
View Record
< Index

Yambo Financials

Country: **Ukraine**
State:

Yambo Financials SBL Listings History

- Current SBL Listings
- Archived SBL Listings

Main Info

April 2007: See "pharmalert" link below for how to recover from a Yambo infection on a linux or BSD box. And remember to use strong passwords!

September 2006: NOTICE! For their pharma spam websites and nameservers, Yambo is using cracked servers as reverse proxies. They appear to be exploiting weak user/password combinations, for example "admin/admin". Most of the hijacked servers are embedded Linux devices such as firewalls and wi-fi routers. In addition to completely disinfecting the device and adding strong passwords, Spamhaus would also like to hear from system admins who have monitored the hijacked IP and tracked packets to the "back end" servers.

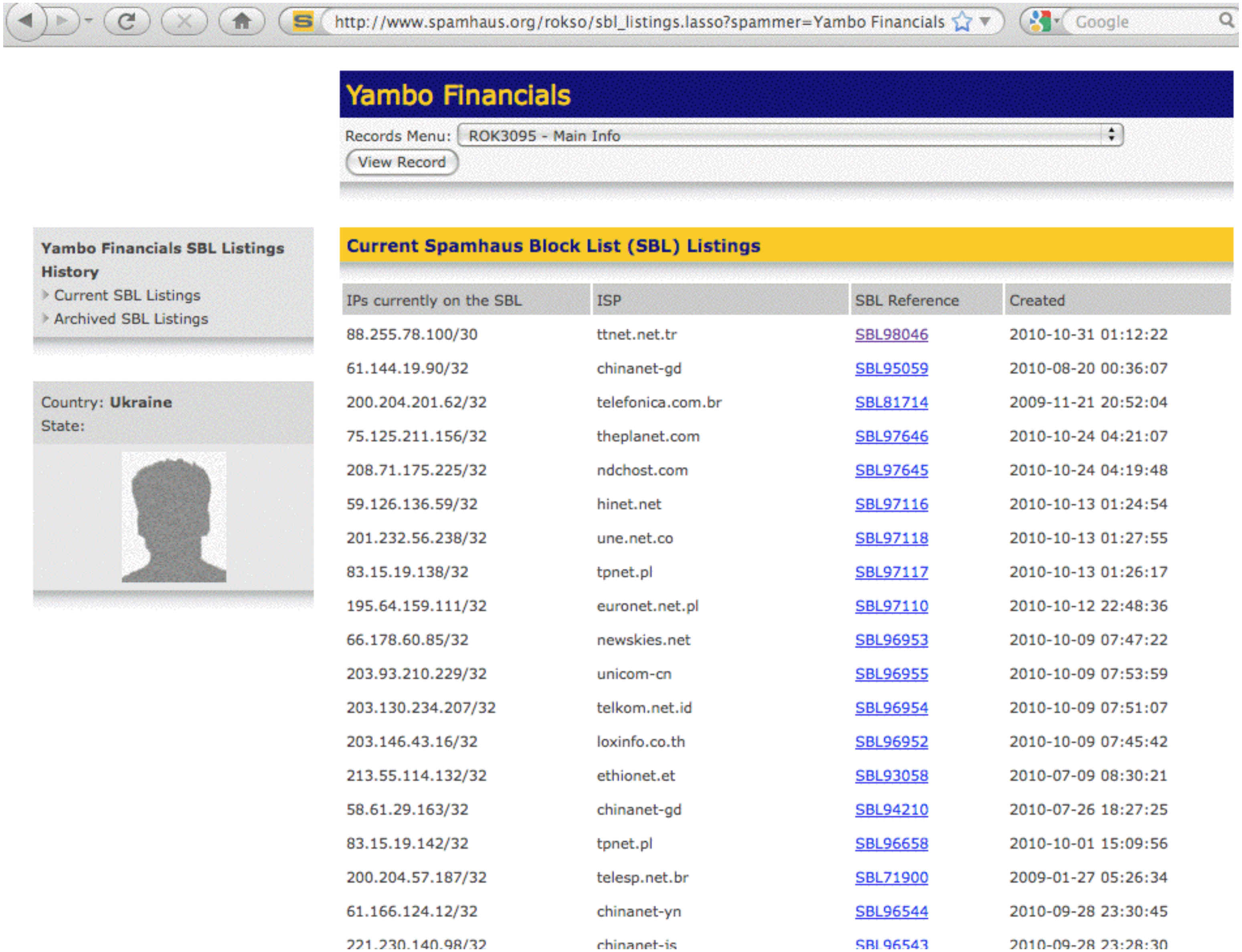
Huge spamhaus tied into billing for child/animal/incest-porn spamming, pirated software spamming, credit-card "collection" sites.

Frequent visitors and advertisers in "secret" spammer chat forums.

Uses "affiliate" model extensively to distribute its spamming among various kiddiez, particularly for their "pharma" programs (pharmaceutical drugs). EVAPharmacy (EVA Pharmacy, EVABilling, EVA Billing), USDrugs (US Drugs), MyCanadian Pharmacy (My Canadian Pharmacy), and other recognizable spam brands are theirs.

Frequently tied to involvement in hijacking ownership of various ARIN netblocks from the rightful owners.

Sample ROKSO Current SBL Listing (Partial)



http://www.spamhaus.org/rokso/sbl_listings.lasso?spammer=Yambo Financials
Google

Yambo Financials

Records Menu: ROK3095 - Main Info

View Record

Yambo Financials SBL Listings History

- Current SBL Listings
- Archived SBL Listings

Country: **Ukraine**

State:

Current Spamhaus Block List (SBL) Listings

IPs currently on the SBL	ISP	SBL Reference	Created
88.255.78.100/30	ttnet.net.tr	SBL98046	2010-10-31 01:12:22
61.144.19.90/32	chinanet-gd	SBL95059	2010-08-20 00:36:07
200.204.201.62/32	telefonica.com.br	SBL81714	2009-11-21 20:52:04
75.125.211.156/32	theplanet.com	SBL97646	2010-10-24 04:21:07
208.71.175.225/32	ndchost.com	SBL97645	2010-10-24 04:19:48
59.126.136.59/32	hinet.net	SBL97116	2010-10-13 01:24:54
201.232.56.238/32	une.net.co	SBL97118	2010-10-13 01:27:55
83.15.19.138/32	tpnet.pl	SBL97117	2010-10-13 01:26:17
195.64.159.111/32	euronet.net.pl	SBL97110	2010-10-12 22:48:36
66.178.60.85/32	newskies.net	SBL96953	2010-10-09 07:47:22
203.93.210.229/32	unicom-cn	SBL96955	2010-10-09 07:53:59
203.130.234.207/32	telkom.net.id	SBL96954	2010-10-09 07:51:07
203.146.43.16/32	loxinfo.co.th	SBL96952	2010-10-09 07:45:42
213.55.114.132/32	ethionet.et	SBL93058	2010-07-09 08:30:21
58.61.29.163/32	chinanet-gd	SBL94210	2010-07-26 18:27:25
83.15.19.142/32	tpnet.pl	SBL96658	2010-10-01 15:09:56
200.204.57.187/32	telesp.net.br	SBL71900	2009-01-27 05:26:34
61.166.124.12/32	chinanet-yn	SBL96544	2010-09-28 23:30:45
221.230.140.98/32	chinanet-js	SBL96543	2010-09-28 23:28:30

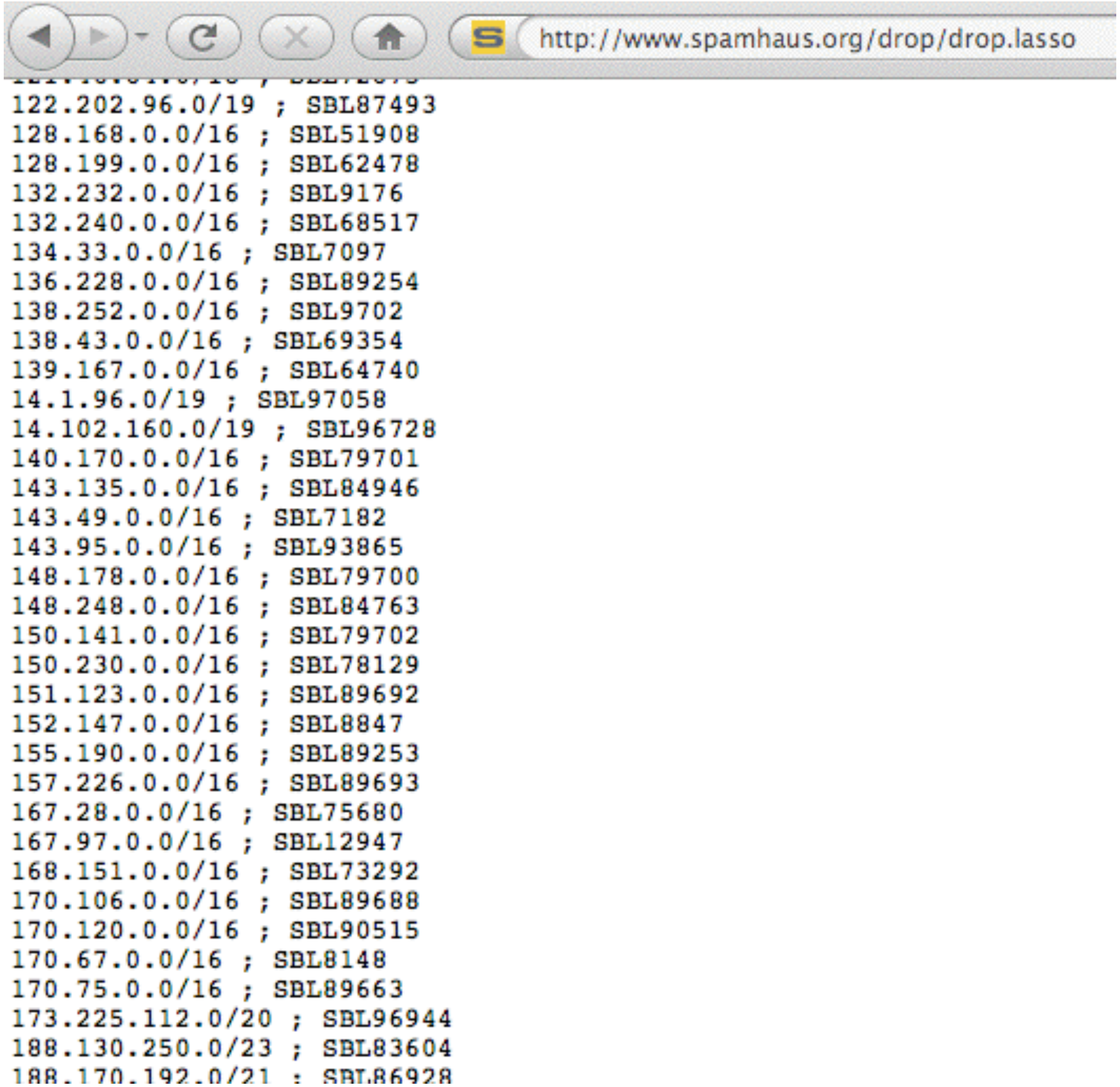
DROP

- *DROP (Don't Route Or Peer) [17] is an advisory "drop all traffic" list, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by professional spammers. DROP is a tiny subset of the SBL designed for use by firewalls and routing equipment.*
- *The DROP list will not include any IP address space under the control of any legitimate network [...] DROP will only include netblocks allocated directly by an established Regional Internet Registry (RIR) or National Internet Registry (NIR) such as ARIN, RIPE, AFRINIC, APNIC, LACNIC or KRNIC or [...] "hijacked" IP address blocks that have been snatched away from their original owners (which in most cases are long dead corporations) and are now controlled by spammers or netblock thieves who resell the space to spammers.*

Why Would A Site Use DROP?

- *When implemented at a network or ISP's 'core routers', DROP will help protect the network's users from spamming, scanning, harvesting, DNS-hijacking and DDoS attacks originating on rogue netblocks.*

Part of the Current DROP List



```
122.202.96.0/19 ; SBL87493
128.168.0.0/16 ; SBL51908
128.199.0.0/16 ; SBL62478
132.232.0.0/16 ; SBL9176
132.240.0.0/16 ; SBL68517
134.33.0.0/16 ; SBL7097
136.228.0.0/16 ; SBL89254
138.252.0.0/16 ; SBL9702
138.43.0.0/16 ; SBL69354
139.167.0.0/16 ; SBL64740
14.1.96.0/19 ; SBL97058
14.102.160.0/19 ; SBL96728
140.170.0.0/16 ; SBL79701
143.135.0.0/16 ; SBL84946
143.49.0.0/16 ; SBL7182
143.95.0.0/16 ; SBL93865
148.178.0.0/16 ; SBL79700
148.248.0.0/16 ; SBL84763
150.141.0.0/16 ; SBL79702
150.230.0.0/16 ; SBL78129
151.123.0.0/16 ; SBL89692
152.147.0.0/16 ; SBL8847
155.190.0.0/16 ; SBL89253
157.226.0.0/16 ; SBL89693
167.28.0.0/16 ; SBL75680
167.97.0.0/16 ; SBL12947
168.151.0.0/16 ; SBL73292
170.106.0.0/16 ; SBL89688
170.120.0.0/16 ; SBL90515
170.67.0.0/16 ; SBL8148
170.75.0.0/16 ; SBL89663
173.225.112.0/20 ; SBL96944
188.130.250.0/23 ; SBL83604
188.170.192.0/21 ; SBL86928
```

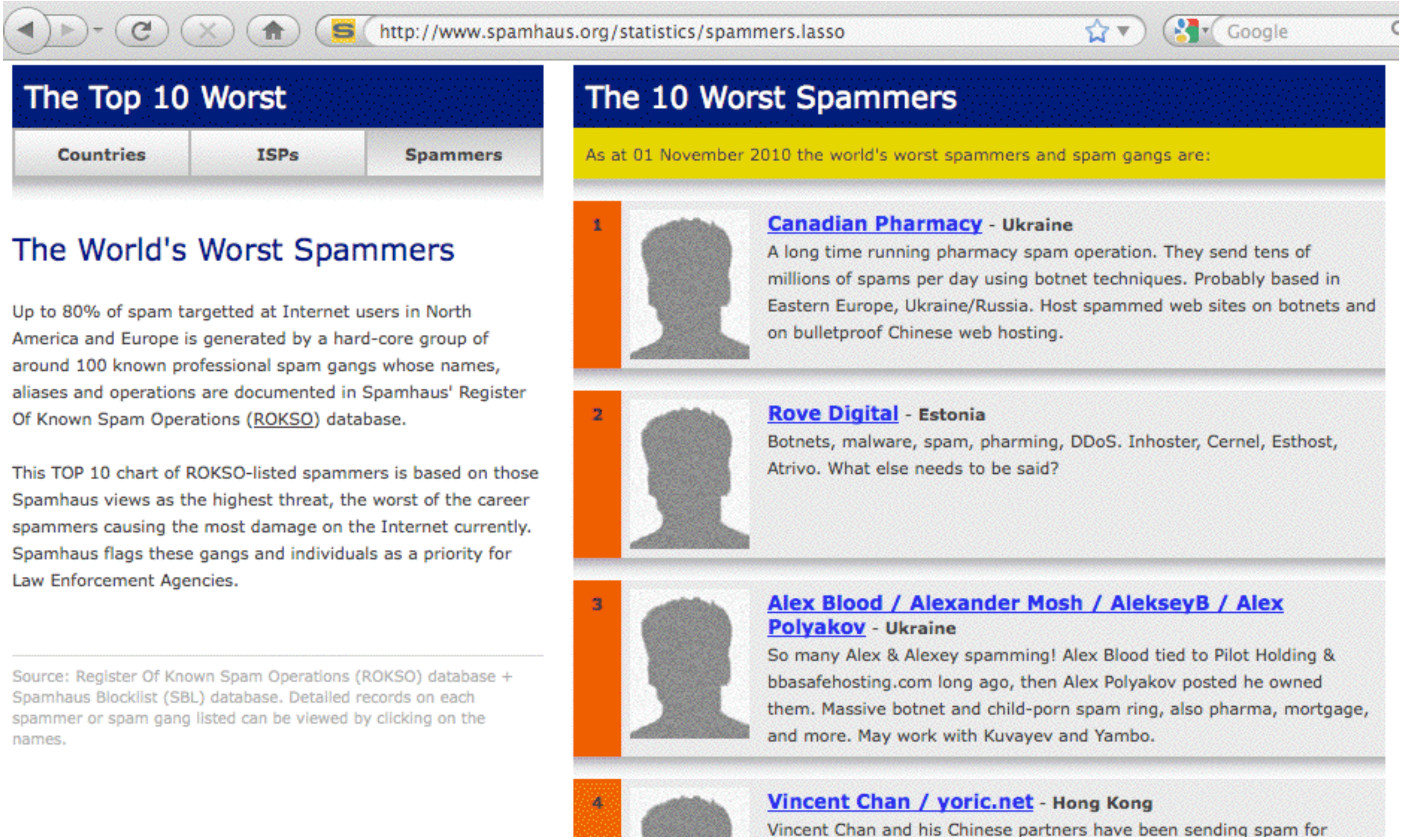
Spamhaus Also Tabulates Three "Top Ten" Lists

- In addition to everything else Spamhaus produces, they also produce three "top ten" summary lists based on SBL listings.

  Those three top ten lists are:

  -- the ten worst spam gangs
  -- the ten worst spam support ISPs, and
  -- the ten worst spam countries

Spamhaus List of Top 10 Worst Spammers



The Top 10 Worst

Countries | ISPs | Spammers

The World's Worst Spammers

Up to 80% of spam targetted at Internet users in North America and Europe is generated by a hard-core group of around 100 known professional spam gangs whose names, aliases and operations are documented in Spamhaus' Register Of Known Spam Operations (ROKSO) database.

This TOP 10 chart of ROKSO-listed spammers is based on those Spamhaus views as the highest threat, the worst of the career spammers causing the most damage on the Internet currently. Spamhaus flags these gangs and individuals as a priority for Law Enforcement Agencies.

Source: Register Of Known Spam Operations (ROKSO) database + Spamhaus Blocklist (SBL) database. Detailed records on each spammer or spam gang listed can be viewed by clicking on the names.

The 10 Worst Spammers

As at 01 November 2010 the world's worst spammers and spam gangs are:

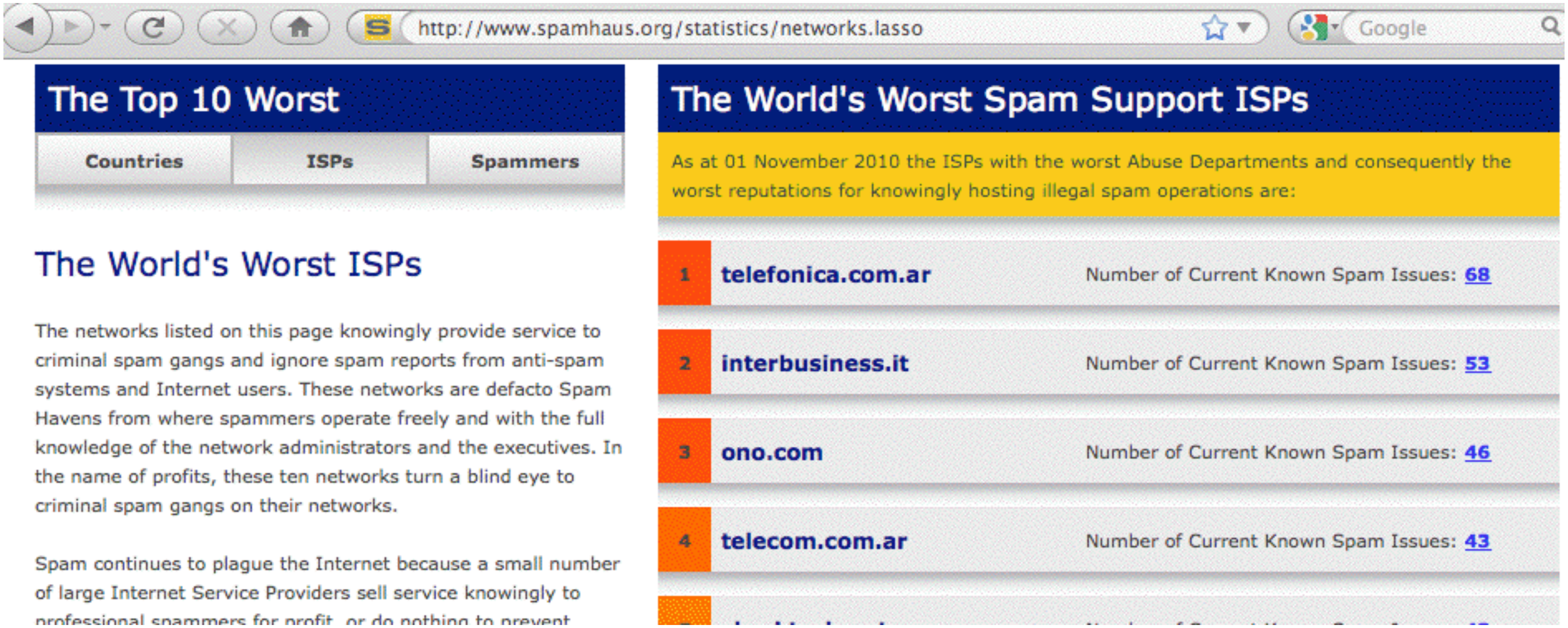
1 **Canadian Pharmacy** - **Ukraine**
A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.

2 **Rove Digital** - **Estonia**
Botnets, malware, spam, pharming, DDoS. Inhoster, Cernel, Esthost, Atrivo. What else needs to be said?

3 **Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov** - **Ukraine**
So many Alex & Alexey spamming! Alex Blood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.

4 **Vincent Chan / yoric.net** - **Hong Kong**
Vincent Chan and his Chinese partners have been sending spam for

Spamhaus List of Top 10 Worst Spam Support ISPs



The Top 10 Worst

Countries | ISPs | Spammers

The World's Worst ISPs

The networks listed on this page knowingly provide service to criminal spam gangs and ignore spam reports from anti-spam systems and Internet users. These networks are defacto Spam Havens from where spammers operate freely and with the full knowledge of the network administrators and the executives. In the name of profits, these ten networks turn a blind eye to criminal spam gangs on their networks.

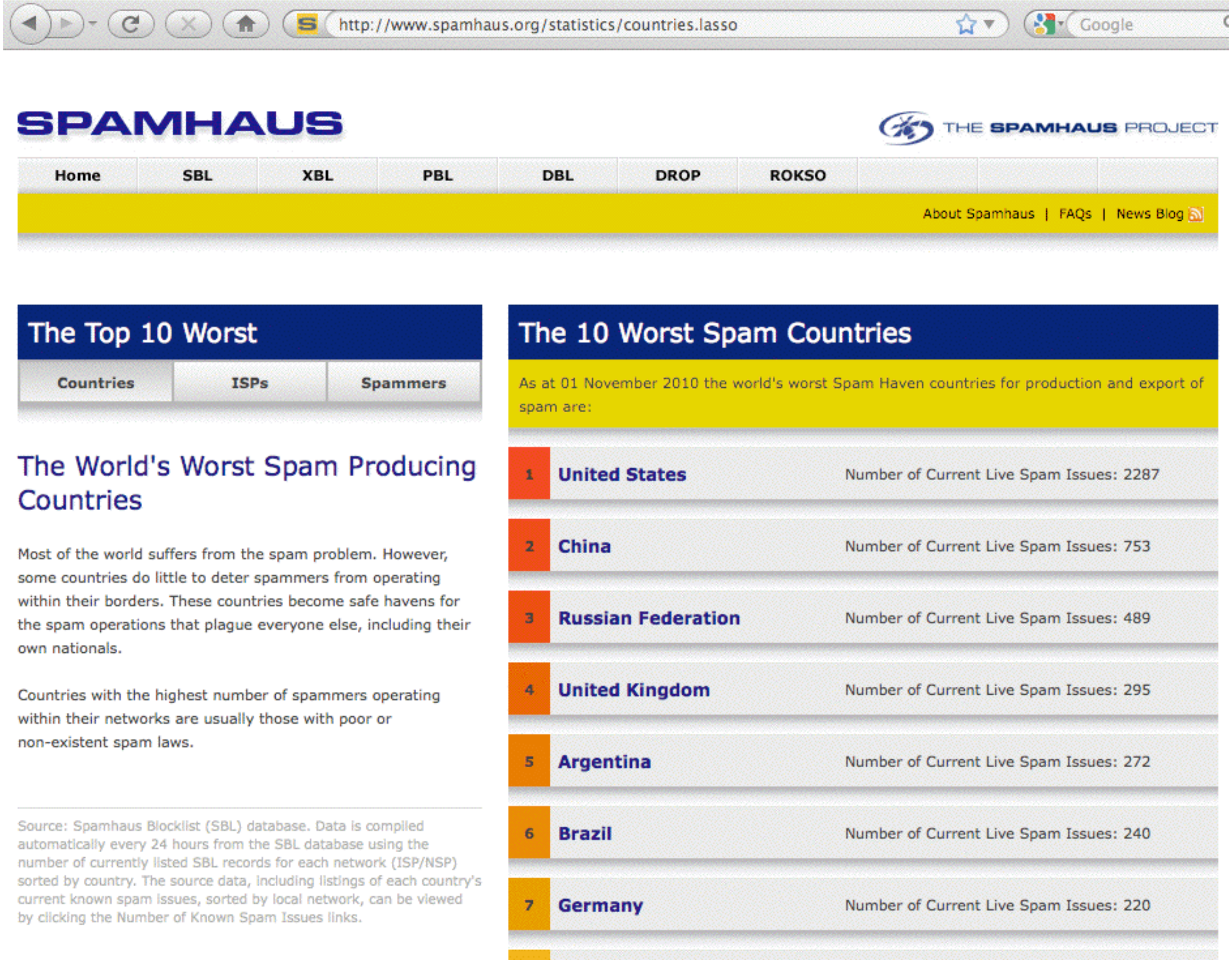
Spam continues to plague the Internet because a small number of large Internet Service Providers sell service knowingly to professional spammers for profit, or do nothing to prevent

The World's Worst Spam Support ISPs

As at 01 November 2010 the ISPs with the worst Abuse Departments and consequently the worst reputations for knowingly hosting illegal spam operations are:

1	telefonica.com.ar	Number of Current Known Spam Issues: 68
2	interbusiness.it	Number of Current Known Spam Issues: 53
3	ono.com	Number of Current Known Spam Issues: 46
4	telecom.com.ar	Number of Current Known Spam Issues: 43

Spamhaus List of Top 10 Worst Spam Countries



http://www.spamhaus.org/statistics/countries.lasso

The Top 10 Worst

The World's Worst Spam Producing Countries

Most of the world suffers from the spam problem. However, some countries do little to deter spammers from operating within their borders. These countries become safe havens for the spam operations that plague everyone else, including their own nationals.

Countries with the highest number of spammers operating within their networks are usually those with poor or non-existent spam laws.

Source: Spamhaus Blocklist (SBL) database. Data is compiled automatically every 24 hours from the SBL database using the number of currently listed SBL records for each network (ISP/NSP) sorted by country. The source data, including listings of each country's current known spam issues, sorted by local network, can be viewed by clicking the Number of Known Spam Issues links.

The 10 Worst Spam Countries

As at 01 November 2010 the world's worst Spam Haven countries for production and export of spam are:

1	United States	Number of Current Live Spam Issues: 2287
2	China	Number of Current Live Spam Issues: 753
3	Russian Federation	Number of Current Live Spam Issues: 489
4	United Kingdom	Number of Current Live Spam Issues: 295
5	Argentina	Number of Current Live Spam Issues: 272
6	Brazil	Number of Current Live Spam Issues: 240
7	Germany	Number of Current Live Spam Issues: 220

We Recognize That's a Blizzard of Data…

- It is easy to be overwhelmed by the sheer volume of spam-related intelligence that Spamhaus tracks.

- Let me make a shot at summarizing all those information products in a single table for you…

Spamhaus Information Product Summary

Name	Focus	Listing?	Auto?	Approx. Size?	DNS or HTTP?	Black or White?
SBL	Spammer Resources	CIDR	No	N Thousands	DNS	Black
XBL	Botted Hosts	IP	Yes	N Millions	DNS	Black
PBL	Non-Mail Server Addrs	CIDR	No	N Thousands	DNS	Black
DBL	Spam Domains	Domain	No	N Thousands	DNS	Black
SWL	*Good* IPv4/IPv6 IPs	CIDR	No	N Thousands	DNS	White
DWL	*Good* Domains	Domain	No	N Thousands	DNS	White
ROKSO	Professional spam gangs	Identity	No	~Hundred	HTTP	Black
DROP	100% Bad Netblocks	CIDR	No	~Hundred	HTTP	Black
	Top 10 Worst Spammers	Identity	Yes	Ten	HTTP	Black
	Top 10 Worst ISPs	Identity	Yes	Ten	HTTP	Black
	Top 10 Worst Countries	Identity	Yes	Ten	HTTP	Black

Those Information Products Are The Key To Spamhaus’ Online Impact and Influence

- Collectively, that set of privately operated and maintained anti-spam information products comprise the most widely used and most widely respected cyber threat detection, attribution, containment and deterrence activity in existence on the Internet today.
- Some Spamhaus resources, such as the industry-wide intelligence collected and presented in the Spamhaus Project's ROKSO database, literally exists nowhere else on the public Internet.
- As a result, many ISPs rely on the SBL and the ROKSO in deciding what new customers to accept, and what existing customers to drop

ISPs Using the Spamhaus Lists For Customer AUP/TOS and Vetting Purposes

- If you're a ROKSO-listed spammer, you may find it hard to find an ISP which will let you sign up. For example, consider the following excerpts from a number of providers' acceptable use policy/terms of service (emphasis added in each case by me):

- **Comcast Business:** [18]
  *[...] any use of the Service or its features that results in your business' Service account, or any associated Comcast information, being listed on, for example, spam reporting web sites such as **Spamhaus, SBL, ROKSO,** TrendMicro Maps, or SenderScore Blocklist, or anti-phishing or anti-spyware services, may result in Comcast suspending or terminating your business' Service account.*

- **Hostgator:** [19]
  *No organization or entity listed in **the ROKSO** may be hosted on our servers. Any account which results in our IP space being blacklisted will be immediately suspended and/or terminated.*

More Examples

- **Hurricane Electric:** [20]

  *Blacklists - No customer shall do anything that could get any portion of Hurricane's IP space (or address space announced by Hurricane on behalf of Customer) put on blacklists such the **SBL (Spamhaus Block List) as maintained by Spamhaus (http://www.spamhaus.org/)** or other similar organizations, or perform activities that would cause portions of the Internet to block mail or refuse to route traffic to any portion of Hurricane's IP space (or address space announced by Hurricane on behalf of Customer).*

- **Level 3:** [21]

  *Level 3 may in its sole discretion rely upon information obtained from anti-spamming organizations (including for example and without limitation **spamhaus.org,** spamcop.net, sorbs.net, and abuse.net) as evidence that a User is an active "spam operation" for purposes of taking remedial action under this Policy.*

More Examples (2)

- **Limestone Networks:** [22]

  If any client or any third-party user that is a customer of our client uses Limestone Networks services, network, or its physical infrastructure in a manner that causes Limestone Networks, or any IP addresses issued by Limestone Networks to be "blacklisted" or "blocked", Limestone Networks reserves the right to suspend or terminate services of such client and/or suspend or terminate the access to services, network, and/or its physical infrastructure. Operating Limestone Networks service on behalf of, or in connection with or reselling any service to persons or firms listed in the ***Spamhaus Register of Known Spam Operations database at www.spamhaus.org*** *shall constitute a violation of this AUP.*

More Examples (3)

- **Rackspace:** [23]

  Complaints from email recipients and third party abuse agencies (e.g. ***SpamHaus*** *or Spamcop) shall be deemed proof of the facts stated therein unless you provide compelling evidence to the contrary.*

- **ThePlanet:** [24]

  Operating The Planet Service on behalf of, or in connection with, or reselling any service to persons or firms listed in the ***Spamhaus Register of Known Spam Operations database at www.spamhaus.org*** *shall constitute a violation of this AUP. Block Removal – If, as a result of a Customer's actions, The Planet's mail servers or IP address ranges are placed on black hole lists or other mail filtering software systems, The Planet shall charge Customer $100 upfront and $100 per hour thereafter for any necessary remedial actions.*

This Sort of Screening Is Partially A Matter of ISP Self-Preservation

- Once address space has gotten listed on block lists, it is most definitely "damaged goods," and these days, as we get close to running out of IPv4 address space, no ISP wants to be stuck with huge blocks of IP addresses that have been abused into unusability by spammers.
- After all, what "lucky" new customer would want to be reassigned some previously damaged block of addresses, and then have to spend substantial time and effort "rehabilitating" those addresses by getting them delisted from block lists all over the world?
- Some IP addresses may even be on non-public block lists -- how would you even know to ask to have your addresses delisted at those sites, eh? There's no way you'd even know you had a delivery problem there...

III. Why Has Spamhaus Been Able To Be So Influential?

1.4 Billion Users Are Protected by Spamhaus

- Why are over 1.4 billion users protected by Spamhaus?

- Why do ISPs rely on Spamhaus Project intelligence when vetting their potential customers?

- Could the United States government (or the European Union, or any government or consortium of governments elsewhere in the world) ever field an equally influential cyber security reputation resource?

- If they wanted to even try, what would be the key success factors they'd need to heed?

Spamhaus Meets An Otherwise Unmet Need

- Spam is a huge problem, and in blocking much spam outright, Spamhaus met an otherwise unsatisfied important need.

- Since Spamhaus is effectively the "state of the art" for anti-spam block lists, any potential competitor to Spamhaus would need to offer at least as competitive a service, or at least help with some area they haven't already covered (is there any such area? I'd love to hear your thoughts about anything they may have missed).

- Let's take a minute to talk about some other specific attributes.

High Level of Accuracy

- Spamhaus is very, very, careful, and has an excellent reputation for "getting it right."
- While no system maintained by humans can ever be totally error free, it is extremely rare for Spamhaus Project data to have "false positives," whether due to typos or other errors.
- If a mistake does occur, it can be corrected, and typically does get corrected, extremely rapidly.
- In some cases a user can even automatically de-list a listed IP (this is not as daring as it sounds because if the de-listed host is still spamming, it will rapidly be redetected and re-listed, with subsequent auto-delisting suppressed for that IP).

Well Documented

- With the exception of the XBL, which uses proprietary methods (aka "secret sauce") to detect and list botted hosts, [25] Spamhaus is meticulous when it comes to documenting the basis for each of its block list entries, usually showing at least one example for each SBL listing.

- In the XBL's case, because it is listing botted hosts, you will normally be able to scan a listed system with multiple anti-malware products, detecting viruses or other malware and thereby confirming the appropriateness of the listing.

Minimal Collateral Damage

- The Spamhaus Project strives to minimize collateral damage by listing the absolute smallest range of IPs needed.

- "Escalated" listings, (e.g., listing of larger encompassing network ranges or listings of corporate mail servers), tend to be used only when an ISP is completely recalcitrant and totally disinterested in addressing its abuse issues.

Timeliness

- The Spamhaus Project is very quick when it comes to listing new sources of spam and other abuse.

- Because of that quickness, spam from many sources ends up getting blocked while spam runs from those IPs or domains are still in progress.

- After all, it wouldn't do much good to list spam sources a week after spam was last seen – by then, the spammer would have moved on to still other hosts.

- Crisp operational execution is key when combating spam.

Equally Quick DE-listing

- Spamhaus is unquestionably quick to list new abuse resources, but Spamhaus is also equally quick to delist abused resources once the problem with those resources has been resolved. This is important, because being block listed can really make things screech to a halt until that block listing gets resolved.

- Spamhaus does not tend to accumulate a backlog of listings that should have been delisted days earlier.

- Spamhaus also has never requested payment of a fee for delisting a site, unlike some other DNS block lists.

Fairness/Evenhandedness

- Everyone gets treated the same way by Spamhaus. Spamhaus doesn’t play games and they don't play favorites.

- Spamhaus has demonstrated a willingness to list the largest of well known ISPs on terms exactly the same as those applied to the smallest and most obscure.

Reliability and Availability

- Due to the Spamhaus Project's distributed and replicated architecture (and the availability of data via zone transfers for use in private mirrors), the Spamhaus Project is highly available and reliable, even in the face of determined network attacks.

- This is another critical factor. If you're relying on a 3rd party resource for critical protective functions such as spam filtering, that data has got to be reliably available. (If spam filtering were suddenly to fail, email might overwhelm provisioned resources, backlogging or crashing critical mail servers)

High Performance

- The Spamhaus Project's chosen data distribution mechanism, the domain name system, is capable of delivering very high performance with very low latency.

- If Spamhaus had chosen a higher-overhead, lower performing distribution channel (such as http), it is unlikely that they would have been able to achieve the performance that they currently deliver.

Coverage

- The Spamhaus Project's coverage is worldwide.

- It is not narrowly scoped to just cover one country or some small subset of providers or just one bot.

- Its coverage is part of its impact, even though biting off a worldwide task isn't a minor undertaking, particularly considering things such as language-related issues, time zone issues, etc.

An Ecosystem-Wide Approach

- The Spamhaus Project understands that spammers need a variety of services to be able to successfully spam, and thus their coverage spans the breadth of that ecosystem, including things like spamware vendors, so-called "bullet proof hosting," and DNS providers.

- Spammers would have a significantly easier time of it if they only had to worry about their actual mail emitting hosts getting block listed.

Standard Setting

- Because Spamhaus is so broadly used, it has the ability to establish de facto standards industry wide, including things such as:
  -- what constitutes reasonable email sending practices,
  -- what's acceptable for list management practices, etc.
- Spamhaus does a good job of documenting those best common practices on its website, and because they do, many senders follows those practices and avoid getting listed in the first place.
- Spamhaus is also active in the Messaging Anti-Abuse Working Group (MAAWG), the carrier anti-spam forum.
- Spamhaus has *not* been active in the IETF standardizing things such as block list response codes, however (block lists just return response codes as normal A records).

Willingness to Evolve

- Spamhaus has been good about evolving its offerings as spammers have evolved their sending sending techniques.

- This process has insured that the Spamhaus Project's data remains relevant and efficacious against newly emerging spam threats.

- For example, Spamhaus just recently announced their new SWL and DWL white lists, a new approach that's designed at least to part to allow sites to deal with the potential problem of spam from IPv6 addresses, given that traditional IP-by-IP block lists will scale poorly to the huge address spaces associated with IPv6.

“Best Choice of Multiple Alternatives”

- As frustrating as it may be for an ISP to end up listed on any block list, being listed by Spamhaus is still far preferable to other alternatives.

- For example, if the Spamhaus block lists didn't exist, a plethora of less professionally run block lists would probably get created, and getting delisted from myriad *ad hoc* block lists would be orders of magnitude higher than getting delisted from just one professionally administered source.

IV. Discouraging Problems When Possible; When Deterrence Fails, Containment

Spamhaus Works Best When Its Sheer Existence Deters Misbehavior

- Like any international control regime, Spamhaus workS best when its sheer existence deters abuse.

  For example:

  -- Because Spamhaus is standing watch, ISPs avoid selling connectivity or web hosting to spammers.

  -- Because Spamhaus cooperates with law enforcement, and law enforcement has been prosecuting botmasters, malware authors may be less likely to code and release new spam bots.

When Deterrence Fails, Containment

- As influential as Spamhaus is, and it truly is very influential, a small number of spam gangs, typically less than a hundred worldwide, resist playing by the rules. When that happens, and they fail to be deterred from spamming, it is necessary to contain their misbehavior.
- Blocking spam by listing IP addresses and domain names is the "stick" that backs up or "enforces" the Spamhaus Project's anti-spam policies. Once that happens, as far as the vast majority of the Internet is concerned, your mail traffic no longer exists. You may be able to try to send it, but most of the Internet simply won't accept it.
- This voluntary "blockade," this global "banishment," dwarfs anything that a national government might be able to orchestrate. That abuse has been effectively contained.

Containment at Origin, En Route, or at Destination?

- When we talk about containment, we should recognize that we can potentially contain abuse at the point where it originates, or we can try to interdict that traffic while it is in transit, or we can contain that abuse at its destination network.
- Traditional block lists (such as the SBL) protect destination networks by blocking unwanted traffic just before it would enter that destination network.
- DROP (do not route or peer) is aimed at interdicting worst-of-the-worst traffic enroute, breaking connectivity between the source of the abuse and the destination.
- The XBL and PBL potentially help ISPs to identify and contain unwanted customer traffic at its source.

Walled Gardens/Quarantines

- For example, an ISP might decide that if a customer ends up listed on the XBL, they'll automatically be shunted into a "walled garden" or quarantine VLAN, thereby insuring both:

  (a) once quarantined, the botted customer can't generate spam and other unwanted traffic and

  (b) even though they're quarantined, the botted customer can still access needed network resources to get themselves patched up-to-date and disinfected.

Managing Port 25

- In other cases, the PBL has influenced providers to actively manage their port 25 traffic, declining to permit random customers to source or sink port 25 traffic “direct-to-MX.”

- Providers who block port 25 traffic, requiring that their users authenticate and send their email via the email servers the provider creates for that purpose, are another nice example of containment at the origin.

Defense In Depth

- Because no single containment point can guarantee to provide "leak free containment," it is important to have "defense in depth."
- That way, if spam escapes from its origin network, it may still be blocked en route.
- If not blocked en route, the spam might at least be blocked when it attempts to be delivered to its destination.
- If it doesn't get blocked by a block list at its destination, it may still get filtered based on a more in-depth analysis of the URLs in the body of the message.

- This is effective containment via defense in depth.

V. Attribution

Spoofed Traffic

- Often when we think about network attack traffic, we worry about things like spoofed UDP traffic: if source networks don't filter spoofed traffic at their border, before it escapes, anyone can generate spoofed UDP traffic and use that traffic to attack other sites.
- For example, at one time it was common for attackers to fake DNS queries, setting those queries up to appear as if they came from some target they want to attack, a target that would then gets crushed with hundreds of thousands or millions of DNS "replies" for questions they didn't make in the first place.
- We're fortunate that email traffic is substantially more attributable, although it still suffers from spoofing issues.

You Shouldn't Trust From: Headers

- **"From:" Header Identities Are Not Trustworthy!**
- Each RFC2822-format [26] email message can be thought of as having two parts:

  -- the message headers, and

  -- an (optional) message body (including potentially attachments), which is separated from the message headers by a blank lines.
- Most email messages have a dozen or more lines worth of headers, with content that is largely cryptic or irrelevant to non-technical users.
- To avoid distracting or confusing typical non-technical users, most popular email clients automatically suppress the display of most headers present in messages, showing users only the most commonly used fields by default.

Condensed Headers

- For example, consider the condensed headers shown for a piece of pharmaceutical spam recently sent to my account:

  Date: Mon, 5 Jul 2010 02:26:19 -0700
  From: joe@uoregon.edu
  To: joe@uoregon.edu
  Subject: joe@uoregon.edu VIAGRA ? Official Site -29%

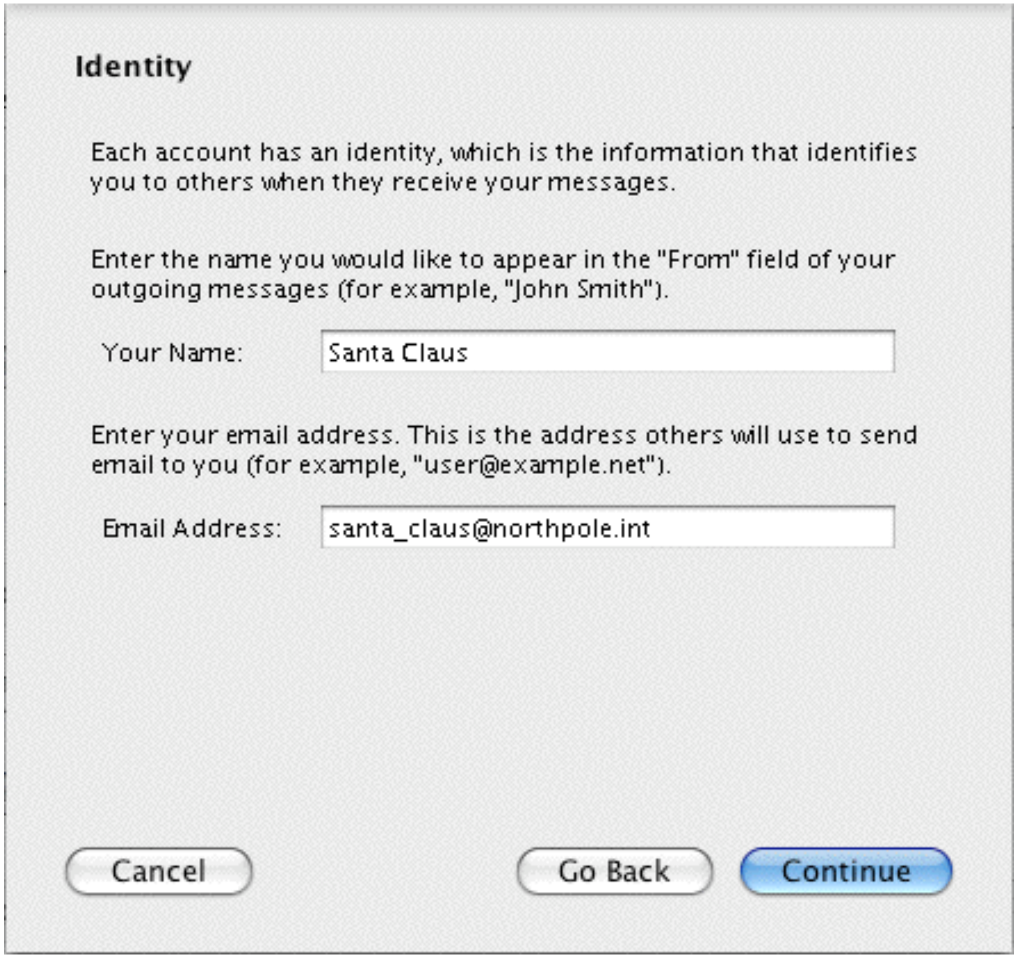
- Superficial inspection of the forged message body "From:" header might lead you to believe that I sent that spam to myself in the middle of the night (needless to say, I didn't).
- But, you might ask, how is it possible for that message body "From:" address to be forged and completely bogus?

Trusting The Untrustworthy

- You need to remember that the message body "From:" header values are constructed from user-supplied information, and can typically be set to any arbitrary value of the user's choosing.

- For example, any email user can pretend to be Santa Claus at the North Pole simply by plugging in suitably incorrect values of their choosing when configuring their email client…

Configuring Your Identity in Thunderbird



Identity

Each account has an identity, which is the information that identifies you to others when they receive your messages.

Enter the name you would like to appear in the "From" field of your outgoing messages (for example, "John Smith").

Your Name: Santa Claus

Enter your email address. This is the address others will use to send email to you (for example, "user@example.net").

Email Address: santa_claus@northpole.int

Bottom Line: Don't Trust "From:" Headers!

- The ease with which one's email identity can be spoofed, even on consumer grade network clients such as Thunderbird (much less purpose-built spamware), should leave no doubt in your mind that "From:" headers are routinely untrustworthy, and thus unusable for attribution purposes.

What About The Received: Headers?

- **Received: Headers and the IP Address of the SMTP Handoff Host**

  When we ask to see the full headers for a message we've received, additional, critically important, headers get displayed. The most critical of those additional headers is the "Received:" header added when the message gets handed off to our local SMTP server:

-
  ```
  Return-Path: <joe@uoregon.edu>
  Received: from chello062178014011.5.11.vie.surfer.at
     (chello062178014011.5.11.vie.surfer.at [62.178.14.11])
     by smtp.uoregon.edu (8.14.3/8.14.3) with SMTP id o659QJDq001292
     for <joe@uoregon.edu>; Mon, 5 Jul 2010 02:26:20 -0700
  Date: Mon, 5 Jul 2010 02:26:19 -0700
  Message-Id: <201007050926.o659QJDq001292@smtp.uoregon.edu>
  From: joe@uoregon.edu
  To: joe@uoregon.edu
  Subject: joe@uoregon.edu VIAGRA ? Official Site -29%
  MIME-Version: 1.0
  Content-Type: text/html; charset="utf-8"
  Content-Transfer-Encoding: 7bit
  ```

What About Received: Headers?

- We can trust the IP address shown in the handoff host's Received: header (bolded by us in the example shown above) because... [27]
- All SMTP connections take place over TCP, a connection-oriented protocol (rather than over UDP, a connectionless protocol). Each TCP connection requires that a full three-way TCP handshake (SYN, SYN-ACK, ACK) must take place before application layer packets can be exchanged, and thus we know that the IP address of the handoff host cannot be spoofed (if an attempt was made to spoof the IP address of the handoff host, the three-way TCP handshake could not be completed).
- At the time the handoff host connected to smtp.uoregon.edu, our server recorded the IP address associated with that connection, adding it to the message headers. (Other Received: headers, if any, may NOT be trustworthy since they're supplied along with the rest of the message by the external host).
- Thus, we do have confidence that this spam actually did come to us via [62.178.14.11]. [28]
- **That IP then becomes the basis for reputation accumulation, and ultimately traffic management.**

The Complication of Dynamic IP Addresses

- Looking at that IP address, it's a dynamic IP address, potentially used by different customers at different times, rather than a static IP address, dedicated to use by a single system or single customer.
- For example, when we check whois [29] for the IP address, we're told that that address is part of a DHCP address pool:

```
% whois -h whois.ripe.net 62.178.14.11
[whois.ripe.net]
<snip>
inetnum: 62.178.0.0 - 62.178.250.255
netname: CHELLO
descr: UPC Telekabel
descr: DHCP Range          <-- Note...
country: AT
admin-c: HMCB1-RIPE
tech-c: HMCB1-RIPE
remarks: Contact abuse@chello.at concerning criminal
remarks: activities like spam, hacks, portscans
<snip>
```

Dynamic Address? Sorry, Only Bad Reputations Will Accrue...

- Because different customers may briefly use the same IP address, if we do try to accumulate IP reputation about that IP, we may see dramatically different behavior: at one point in time, that IP may be associated with a totally secure host, while at other times that same IP may end up in use by a thoroughly infested botted host.
- Lacking any ability to externally identify the user of a dynamic IP address, and thus lacking the ability to meaningfully accumulate reputation (good or bad) for traffic from that dynamic IP, the community has no option but to "assume the worst" and block all email traffic sent directly from those IPs.
- Spamhaus does this via their PBL ("Policy Block List"), which we've previously mentioned above.

Web Email And Attribution

- We should also note one other attribution-related issue, and that relates to web email.
- When a user connects to a web email service and sends a mail message, what's the correct "origin" address for that message? Obviously it was composed at and sent from the web email server, but that's used by millions of customers. What we often want is the IP address (and time stamp) associated with the host that connected to the web email service to inject that message.
- Many web email services will include that IP address (and time stamp) in the headers. Sometimes it will be in plain text, other times it may be reversibly encoded, so that the user's privacy is protected, but the web email service provider can pierce that veil if they need to do so.
- Gmail is a notable exception to that general rule.

VI. A Government Role?

Should The U.S. Offer A National Blocklist?

- Let me rephrase that question.

- Should the world's critical email infrastructure rely on the efforts of a small handful of volunteers?

- Isn't it time for the US government to be at least as worrisome to gray or black hat ISPs as Spamhaus when it comes to deterring abusers?

Sharing Data With The Community

- The Internet community would love to know about the cybersecurity threats the federal government sees, if only as a result of attacks on federal systems and networks, but the data that the federal government currently share with the community is too little, too late, and is not subject to public documentation and public scrutiny the way the Spamhaus Project's data is.

- Federal cyber security data is also not delivered in an immediately operationally useful way (such as via a DNS block list); when I see data from federal authorities it is often embedded in a PDF-formatted report released days or weeks after the threat it describes ceases to be of primary concern. That's just too dang slow.

These Issues Translate to a Lack of Influence

- Because of these factors, the United States government's public attribution, deterrence and containment efforts in the cyber security realm have had limited operational impact to date, and objectively far less influence than what the private Spamhaus Project has been able to accomplish on shoestring resources.
- If the United States is to ever have the ability to publicly attribute and deter unacceptable cyber behaviors itself, and to contain cyber malicious activity which empirically cannot be deterred, it needs to begin to publicly share timely, high quality, actionable, cyber intelligence much in the way that Spamhaus currently does.
- Nothing less will give it the operational influence it wants and need.

Thanks For the Chance To Talk Today!

- Are there any questions?

[bracketed references follow]

References

- [1] Lolita C. Baldor, "Military asserts right to return cyber attacks", My Way News, April 14, 2010. http://apnews.myway.com/article/20100414/D9F2PLP00.html

- [2] "NRC Prize for Cyberdeterrence Research and Scholarship", Mar 11, 2010. http://sites.nationalacademies.org/CSTB/CSTB_056215#questions

- [3] Jacobellis v. Ohio, 378 U.S. 184 (1964).

- [4] "Critical Infrastructure and Key Assets: Definition and Identification," CRS Report for Congress RL32631, October 1st, 2004. http://www.fas.org/sgp/crs/RL32631.pdf

- [5] Theodore Gyle Lewis, "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation," Wiley-Interscience, 2006, ISBN-13 978-0471786283 at pages 3 and 30-31.

- [6] "National Infrastructure Protection Plan: Information Technology Sector," Department of Homeland Security. Undated. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_informationtechnology.pdf (linked from http://www.dhs.gov/files/programs/gc_1188479464996.shtm)

References (cont.)

- [7] "E-Mail Outage Forces White House to Operate the Oldfangled Way," Washington Post, January 27th, 2009. www.washingtonpost.com/wp-dyn/content/article/2009/01/26/AR2009012602087.html

- [8] About Spamhaus. http://www.spamhaus.org/organization/index.lasso

- [9] While Spamhaus doesn't generally publicly enumerate the sites that use its block lists, in October 2006, Steve Linford, Spamhaus CEO, disclosed that the Whitehouse, the U.S. Army, and the European Parliament were (and presumably still are) among the sites protected by its block lists. (see http://www.foxnews.com/wires/2006Oct09/0,4670,AntiSpamLawsuit,00.html)

  ISPs which have publicly disclosed that they use Spamhaus data for spam filtering include some of the largest and most professionally run ISPs in the world, including AOL (see http://postmaster.aol.com/Postmaster.Errors.html), Comcast (see www.comcast.com/About/PressRelease/PressReleaseDetail.ashx?PRID =926), Road Runner (see http://security.rr.com/mail_blocks.htm) and Yahoo (http://help.yahoo.com/l/us/yahoo/mail/postmaster/errors/550-bl23.html)

- [10] The Spamhaus Block List. http://www.spamhaus.org/sbl/.

- [11] The Spamhaus Exploits Block List. http://www.spamhaus.org/xbl/

References (cont.)

- [12] Spamhaus Policy Block List. http://www.spamhaus.org/pbl/
- [13] Spamhaus Domain Block Listhttp://www.spamhaus.org/dbl/
- [14] Spamhaus White List http://www.spamhauswhitelist.com/en/about.htm
- [15] http://www.dkim.org
- [16] Spamhaus Register of Known Spam Operations. http://www.spamhaus.org/rokso/
- [17] Spamhaus Don't Route or Peer List. http://www.spamhaus.org/drop/
- [18] Comcat Business Class Acceptable Use Policy. http://business.comcast.com/acceptable-use-policy/index.aspx
- [19] Hostgator Terms of Service. http://www.hostgator.com/tos/tos.php

References (cont.)

- [20] Hurricane Electric Acceptable Use Policy (AUP). http://he.net/aup.html
- [21] Level 3 Acceptable Use Policy. http://www.level3.com/index.cfm?pageID=321
- [22] Limestone Networks Acceptable Use Policy for Dedicated Servers. http://www.limestonenetworks.com/service_info/aup.html
- [23] Rackspace Acceptable Use Policy http://www.rackspace.com/apps/aup/
- [24] The Planet Acceptable Usage Policy. http://www.theplanet.com/content/Documents/legal/Planet-AUP.pdf
- [25] Spamhaus XBL Frequently Asked Questions. http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20XBL See also the CBL FAQ. http://cbl.abuseat.org/faq.html
- [26] Internet Message Format. April 2001. www.ietf.org/rfc/rfc2822.txt
- [27] Simple Mail Transfer Protocol. April 2001. www.ietf.org/rfc/rfc2821.txt

References (cont.)

- [28] While that handoff host IP is non-spoofable, we must also recognize that it may still be subject to BGP hijacking via route injection. See, for example, "Route Injection and the Backtrackability of Cyber Misbehavior," Dec 5, 2006. http://www.uoregon.edu/~joe/fall2006mm/fall2006mm.pdf

- [29] Whois data is accessible over the Internet from ARIN, RIPE, APNIC, LACNIC, AFRINIC, etc. Most Unix hosts support the whois command at the command prompt. For example:

```
% whois -h whois.ripe.net 62.178.14.11
```