Spam Reputation as Output Measure of Infosec

John S. Quarterman
Serpil Sayin
Manoj Parameswaran
Jouni Reinikainen
Andrew B. Whinston, PI
IIAR Project, U. Texas at Austin

Spam Volume per Country

Symantec Apr 2010	Sophos Jan-Apr 2010	Project Honeypot 21 Apr–21 May 2010	IIAR Q3 2009	IIAR Q4 2009	IIAR Q1 2010
US	US	IN	BR	BR	BR
IN	IN	BR	KR	VN	IN
NL	BR	VN	US	KR	US
BR	KR	DE	VN	IN	KR
DE	VN	US	IN	CN	RU
UK	DE	RO	CN	US	VN
FR	UK	RU	RU	RU	CO
PL	RU	UK	PL	CO	UA
VN	IT	IT	CO	PL	AR
IT	FR	PO	AR	AR	DE

Spamming Countries

Left 3 table columns are a few well-known country rankings (there are many more)
No 2 agree on rankings

Right 3 table columns are 3 quarters by IIAR

Each ranking uses different data and methods
Most don't even use the same time periods
BR, IN, US in all 6 rankings
VN in IIAR and 2 others, etc.

IIAR Country Rankings Plausible

Which helps validate IIAR data.

Raw data comes from CBL blocklist,
With custom volume field per blocked address
collected from 2 CBL spam traps
(CBL uses more spam traps for their blocklist)

Top 10 ASNs, Q1 2010

ASN	Owner	Type	CC	%Vol	
7738	T da Bahia	State T	Brazil	4%	
7643	VNPT	Nat. T	Vietnam	3%	
9829	BSNL	Nat. Backbone	India	2%	
8167	T da Santa Catarina	State T	Brazil	2%	
27699	T da Sao Paulo	State T	Brazil	2%	
4766	Korea T	Nat. T	Korea	2%	
24560	Bharti Airtel	Intl T	India	2%	
28573	NET Servicos de Com.	Nat. Cable	Brazil	2%	
17974	PT. T Indonesia	Nat. T	Indonesia	1%	
9050	Romtelecom	Nat. T	Romania	1%	

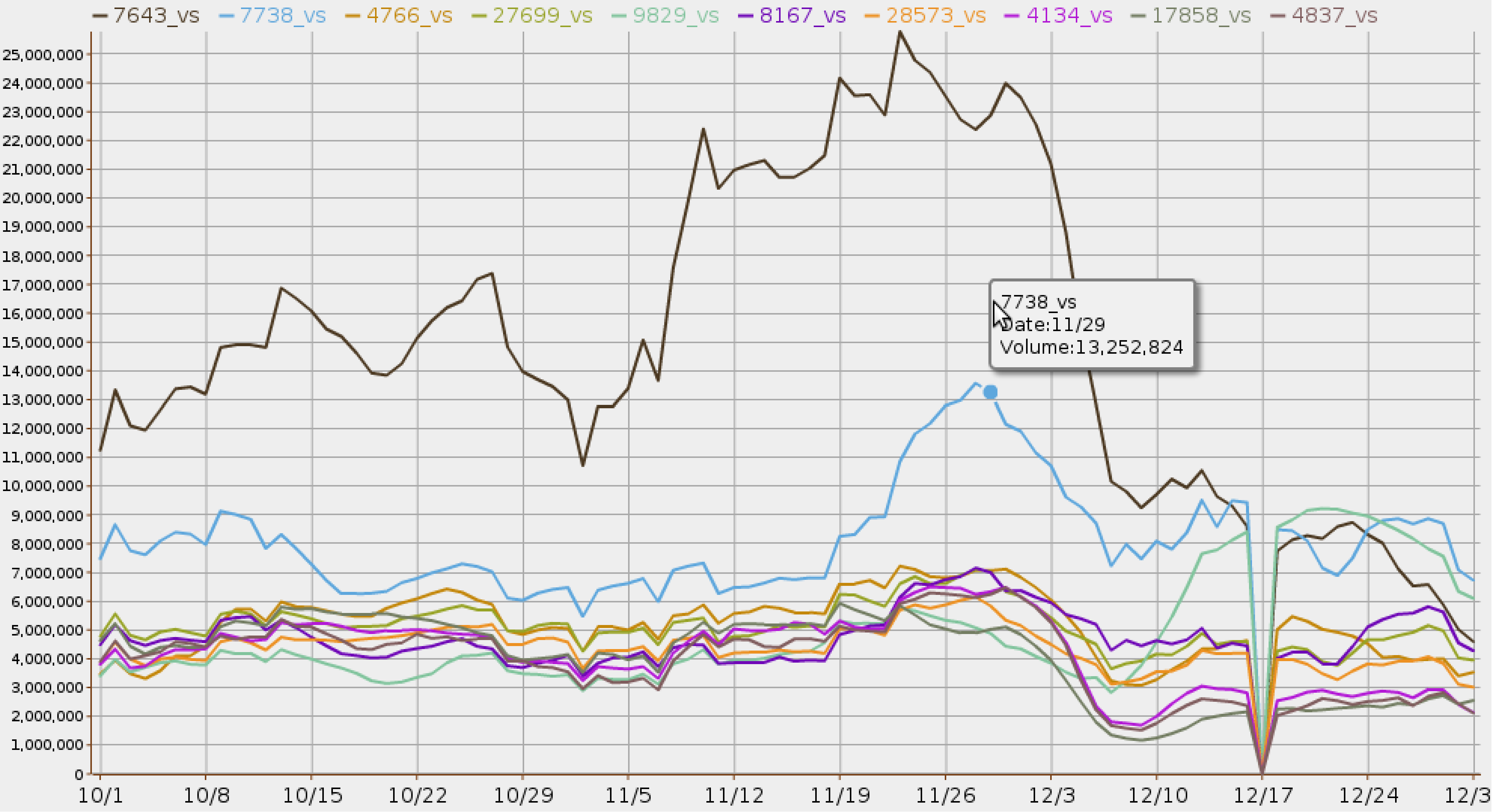
National Telecom Considered Spammy

4 of top 10 ASNs are national telecoms.
Another 3 are telecoms for Brazilian states, delegated by national telecom.
Another is a national broadband network.

Gov-controlled telecoms are spammy?

What other patterns can be found?

Top 10 ASNs, Q4 2009



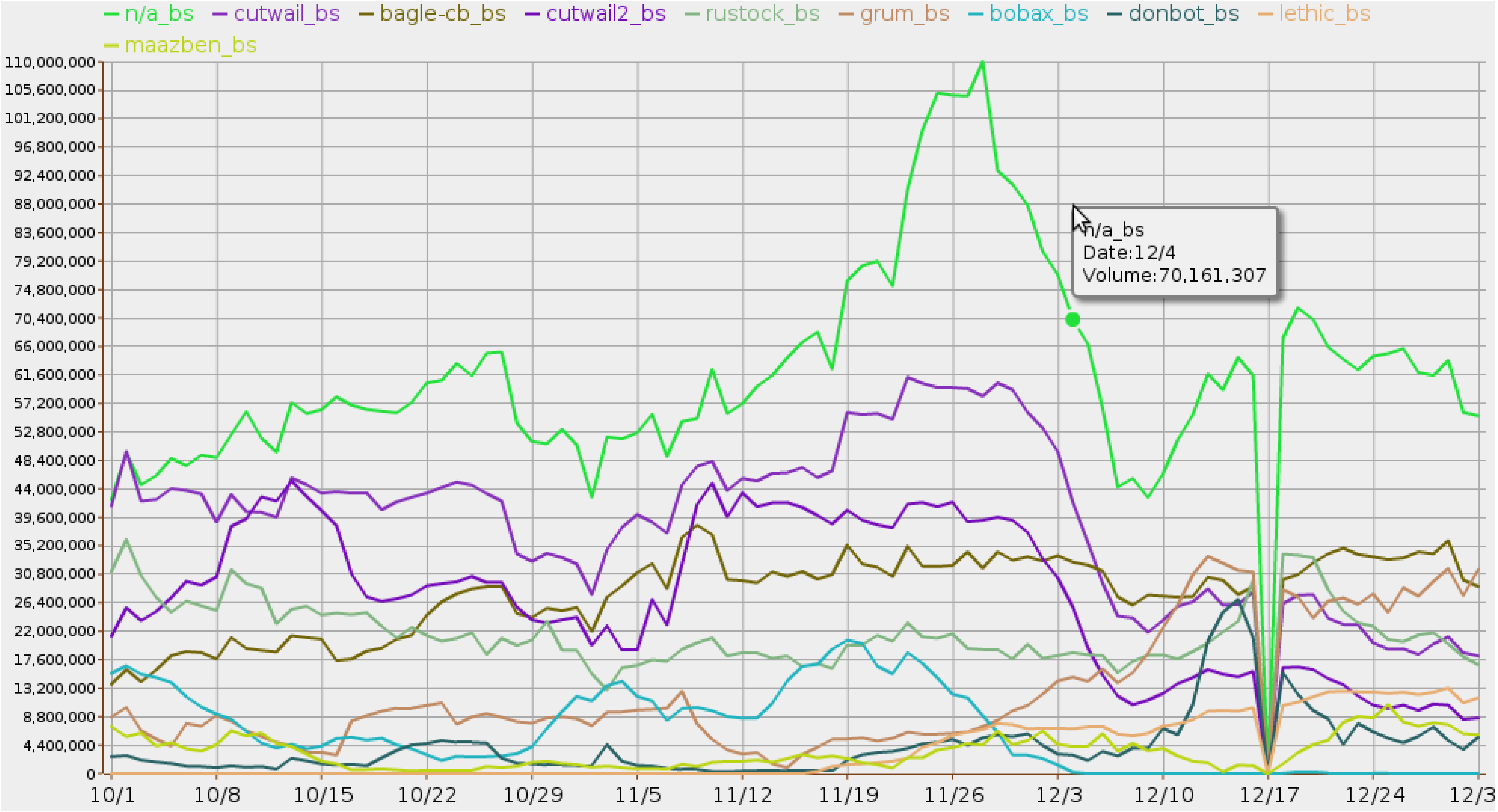
About Top 10 ASNs Q4 2009

Top ASN for this quarter was AS 7643, VNPT
Did they do something right end of November?

Second was AS 7738, T. da Bahia.
Pretty impressive: a state ISP
comes in second worldwide!

(Data loss on 17 Dec 2009.)

Top 10 Botnets Q4 2009

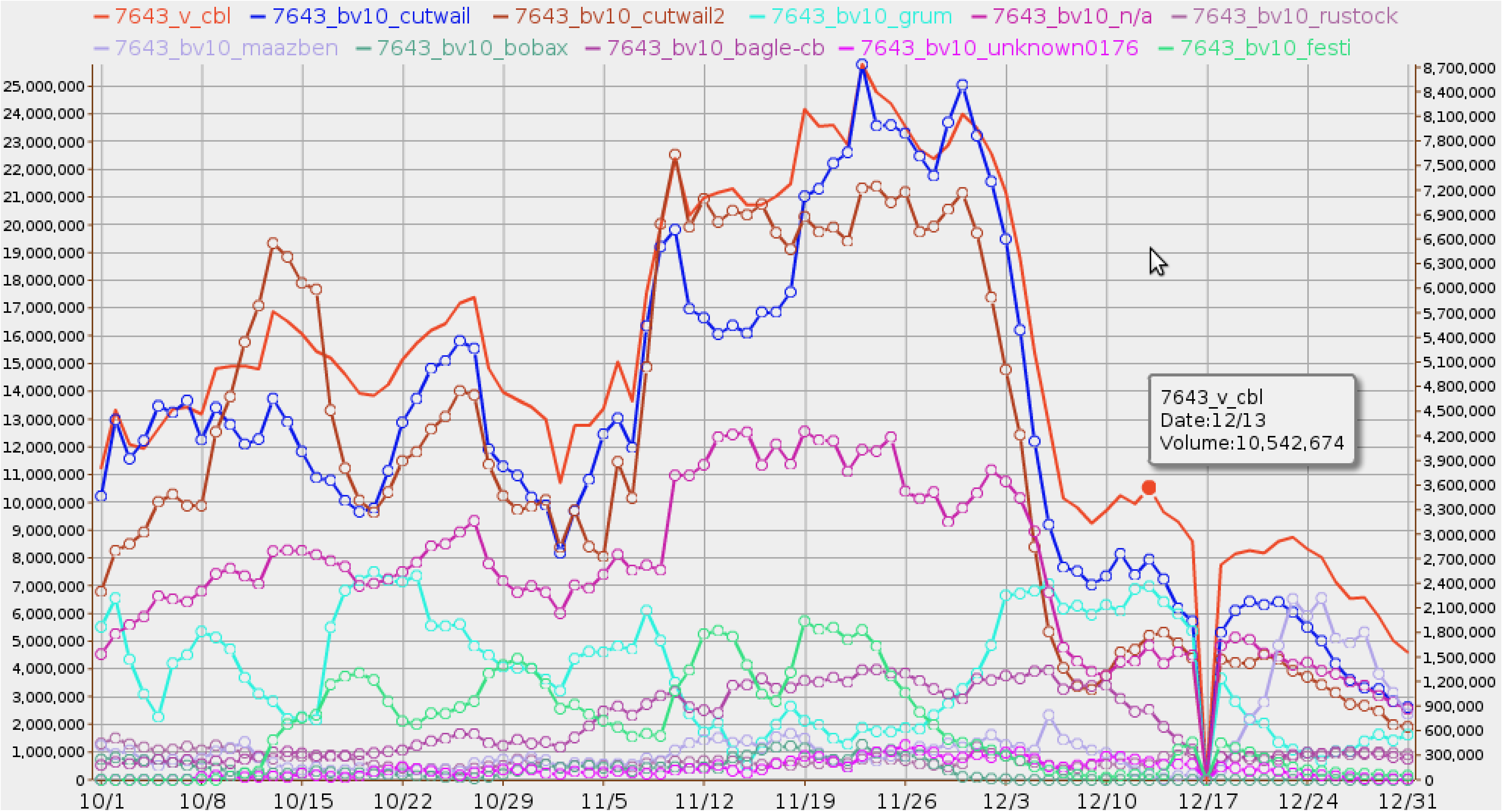


About Top 10 Botnets Q4 2009

Maybe VNPT didn't do anything good end Nov;
Maybe cutwail and cutwail2
finished a spam campaign.

(The highest curve is for n/a
because CBL rejects a lot of spam by rules
that don't require checking which botnet.
Others: bagle_cb, rustock, bobax, grum, lethic,
maazben, donbot)

Botnets per AS 7643 Q4 2009



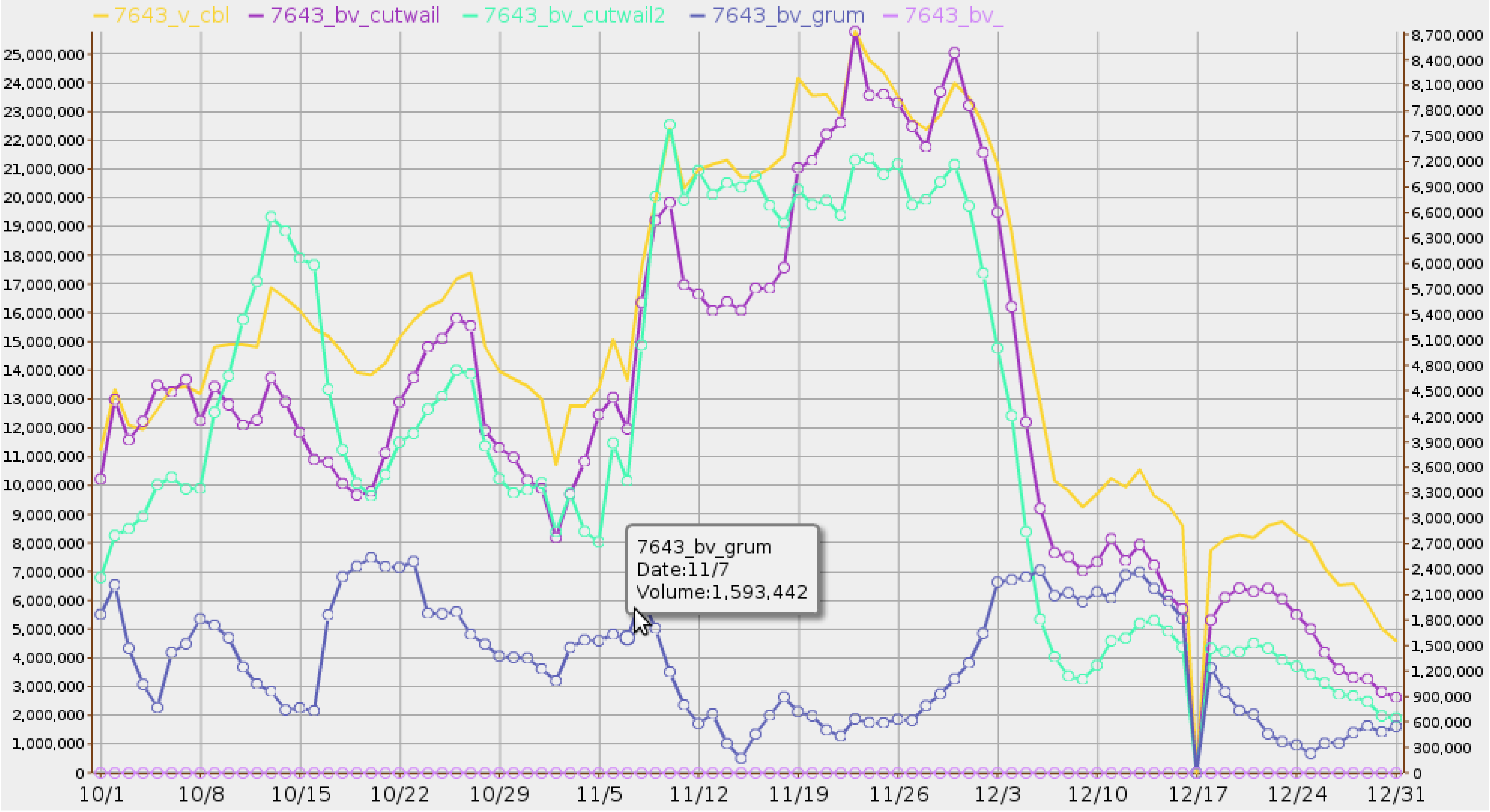
About Botnets per AS 7643

AS 7643, VNPT, Vietnamese National T

Left axis: spam volume this ASN (red line)

Right axis: volume top 10 botnets from AS 7643

Top 3 botnets per AS 7643



About Top 3 Botnets per AS 7643

For VNPT, total volume tracks
Cutwail + Cutwail2 pretty closely.
Although on 17 Oct 2009 they decrease
While grum increases keeping total volume up.

We can drill down farther, into specific IP
addresses, but you get the idea:
Compare at very high levels, such as countries
or ASNs or botnets, then mix and drill down
to find clusters and correlations.

Proposed Reputation System

Could publish this kind of material as a
Reputation system (RS)
providing **market signals**
about security-conscious email providers:
Economic incentive for more effective infosec.

A mechanism to **turn the economic externalities**
Of spam and botnets **into internal incentives**.

(Or for national telecoms, policy incentives.)

The IIAR Method

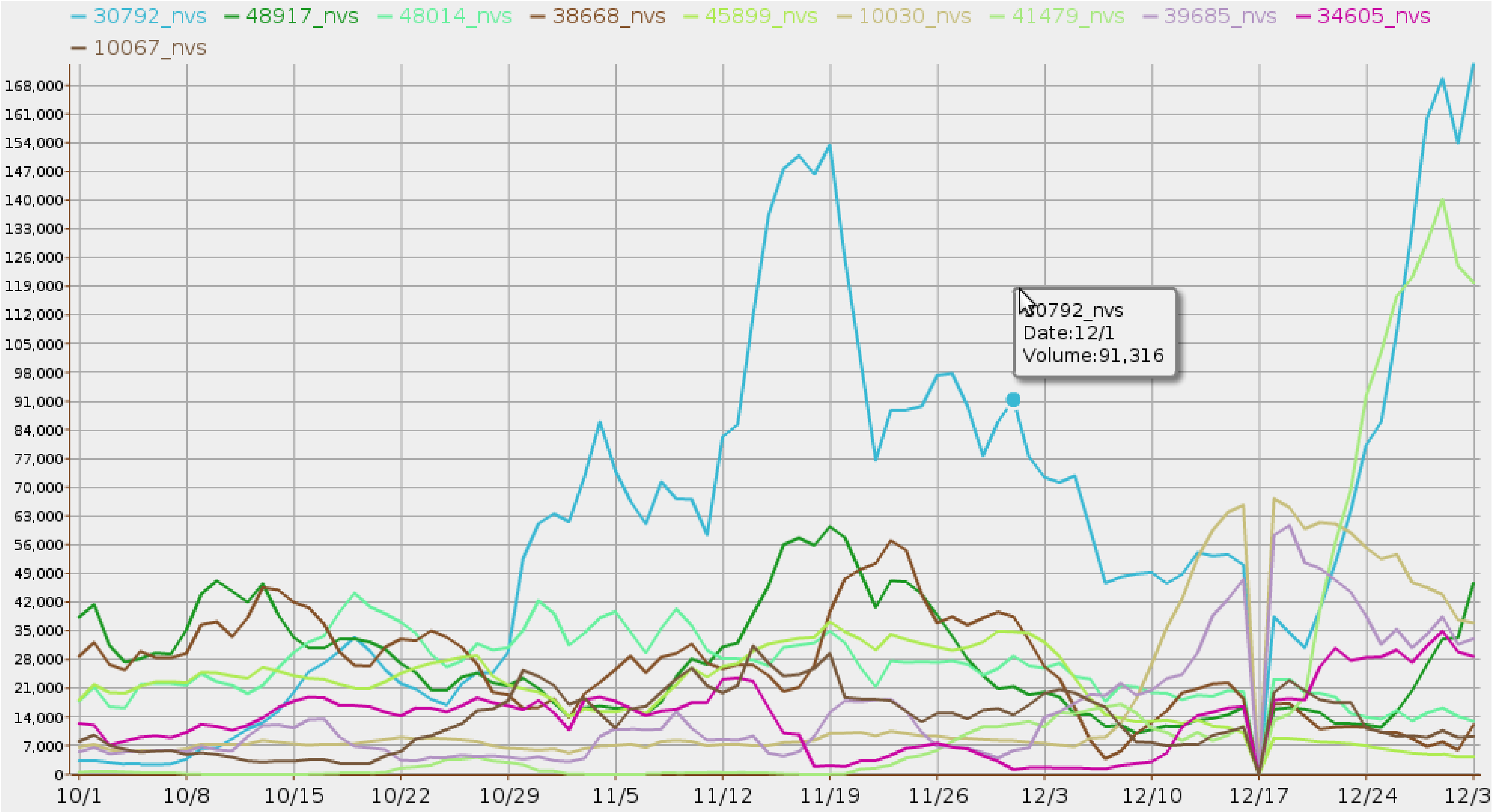
Scope: the whole Internet
(all spam volume and addresses found by CBL and half a dozen other blocklists, compared to the entire Internet address space and all ASNs)

Consistency: daily, with permanent archives

Variety: vol/size, %addr, etc. + summary

Applicability: can correlate with other information about networks and organizations

Top 10 ASNs / size Q4 2009



Table, Top 10 ASNs / size Q4 2009

ASN	Country	Description
30792	Ukraine	Luganet Lukansk
48917	Bulgaria	Optinet Ltd
48014	Russia	Interanet Ltd (Voronezh)
38668	Korea	Konkuk University Hospital
45899	Vietnam	VNPT
10030	Malaysia	Celcom ISP
41479	Ukraine	Technoclub, Ltd.
39685	Czechia	Firm Radio Ltd.
34605	Ukraine	Linet Home Network
10067	Korea	LGNET-China-AS-KR

About Top 10 ASNs / size Q4 2009

VNPT manages to be in this top 10, too,
Although it's a different ASN this time.
All the other ASNs are different,
There's more variety of types,
And more variety of countries.

Not Just ISPs

Botnets try to infest every kind of organization that sends email.

Ranking hosting centers for customer choice: providing **economic incentive** for better hosting infosec.

Banks, retailers, NGOs, etc.: **nobody wants a reputation for bad security.**

Each type of organization can be ranked with its peers.

Outbound Measures Show Results

Traditional application and certification of information security (infosec) techniques, procedures, and policies,
usually about inbound measures,
is great, but doesn't say what works.

A reputation system using external measures of outbound spam
Can show which ASNs are actually doing better.

Infosec per ASN?

What if we also knew which infosec techniques, procedures, and policies each ASN uses?

Possible sources: OSSTMM (Open Source Security Testing Methodology Manual), Verizon Business or ICSA Labs (see "Necessary Measures," Baker, et al., CACM Oct 2007) Delft U. or MSU or Trend Micro (see "The Role of Internet Service Providers in Botnet Mitigation", van Eeten et al., WEIS 2010)

Which Specific Infosec Works?

If we know which infosec ASNs are using,

And we see different levels of spam volume that correlate with specific infosec,

That's a clue as to **which** specific technique, policy, or procedure **works**.

Exploits per Botnet?

Spam source addresses are proxies for bots.

Which exploits does each botnet use?
Are some exploits used by several botnets?
Many other organizations collect this.

Reputation system may be able to show **which** infosec **works against which exploits**.

Current, Frequent, Adaptable

A reputation system is like a cross-sectional study (rankings compare ASNs), but also basically different: ongoing.

What works right now!
Try something and watch rankings change.
No need to construct an event chain:
Change infosec and watch rankings.

Potential Infosec ROI

Given how much a measure costs,

How long it lasts,

And how much effect it has
(according to reputation system)

Could compute ROI for that measure.

Ack, Merci, Contact

Thanks to CBL for the volume data.
Thanks to Team Cymru for mappings of different data types.

This material is based upon work supported by the National Science Foundation under Grant No. 0831338. Any opinions, findings, and conclusions or recommendatioons expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Contact: antispam@quarterman.com
iiar@utlists.utexas.edu