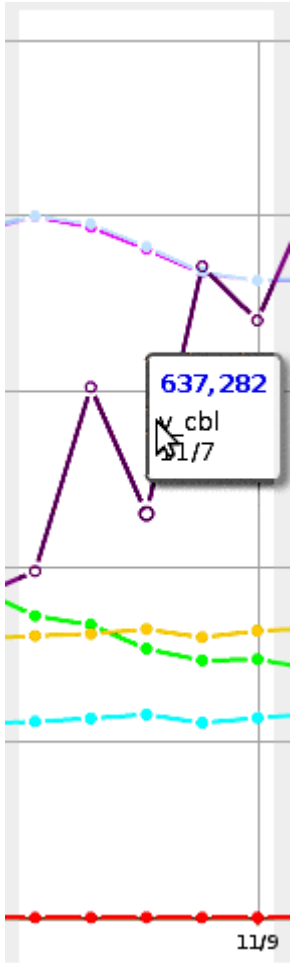
FireEye's Ozdok Botnet Takedown

In Spam Blocklists and Volume



Observed by
IIAR Project, CREC, UT Austin

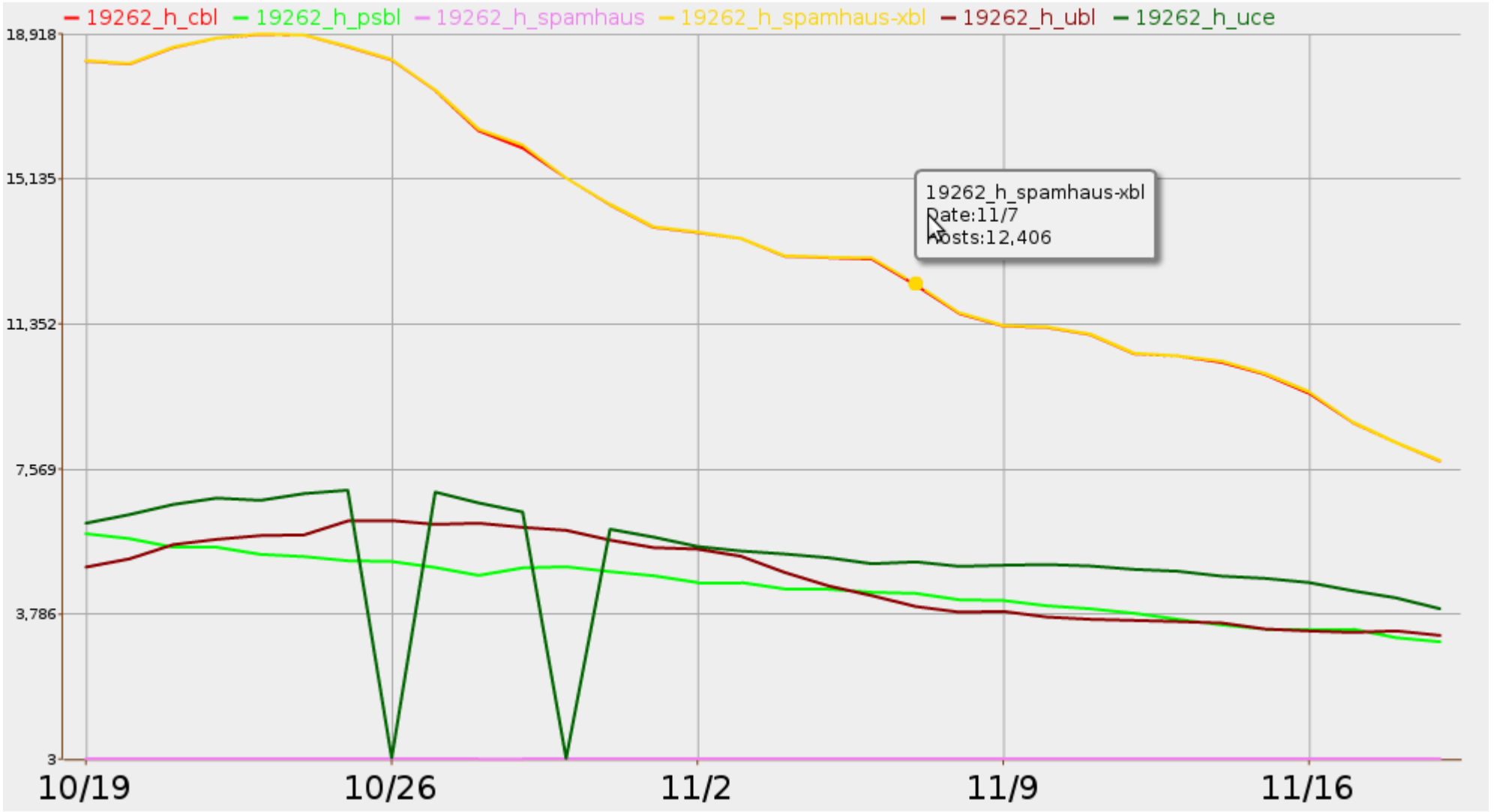
John S. Quarterman
Quarterman Creations
antispam@quarterman.com

Prof. Andrew Whinston, PI
CREC, UT Austin

The Event

- FireEye coordinated a takedown,
  - of botnet Ozdok or Mega-D,
  - on 5-6 Nov 2009,
  - with cooperation by many ISPs and DNS registrars.
- Good show!
- What effects did it have on spam?
- Not just spam from this botnet; spam in general.

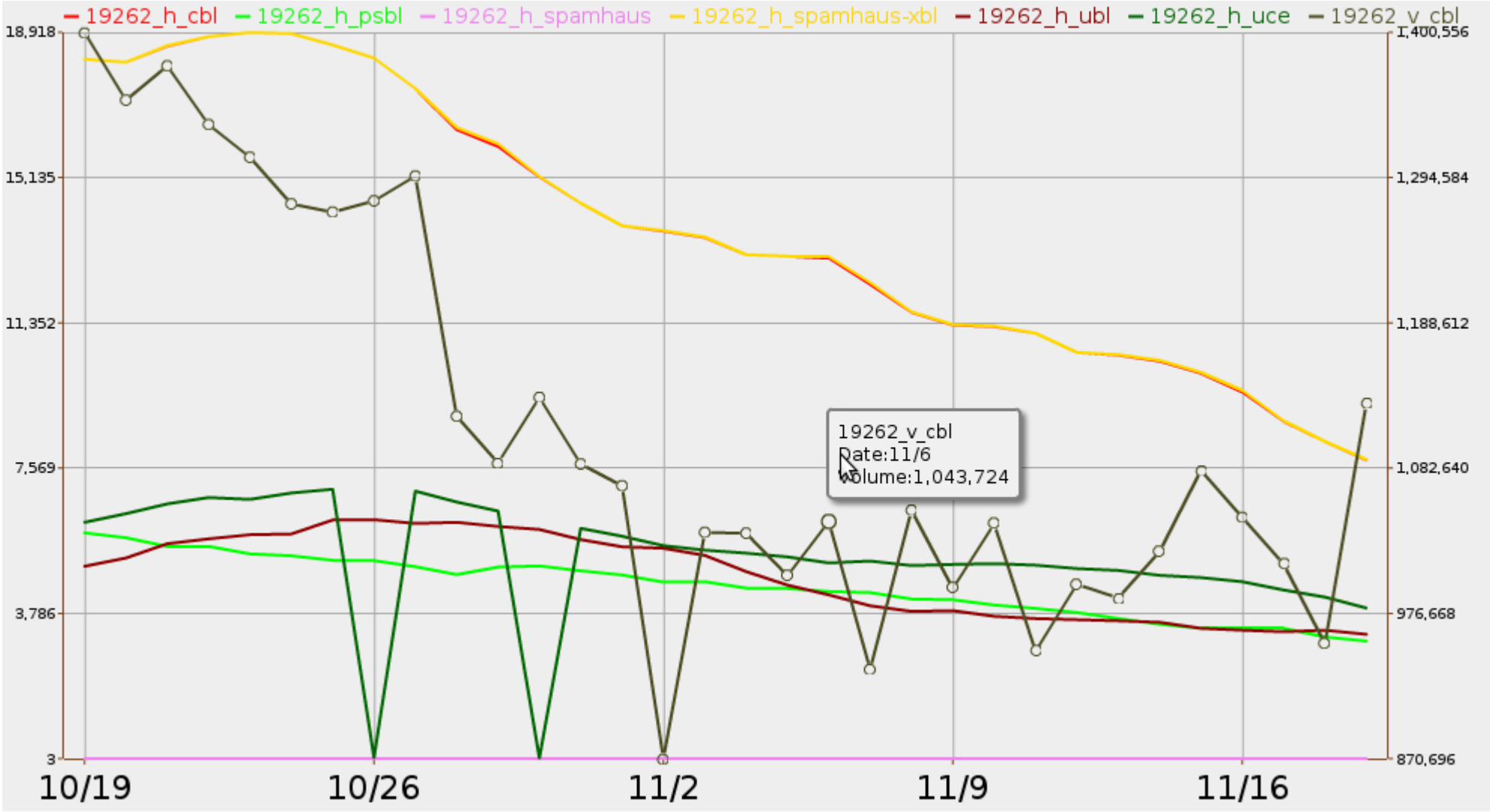
AS 19262 CBL and XBL



AS 19262 CBL and XBL Notes

- Slight decrease 7 Nov 2009 in number of IP addresses (left Y axis) in all netblocks listed on CBL and Spamhaus XBL
- Trend on those two blocklists was down anyway
- XBL is mostly composed of CBL, so their curves are very similar

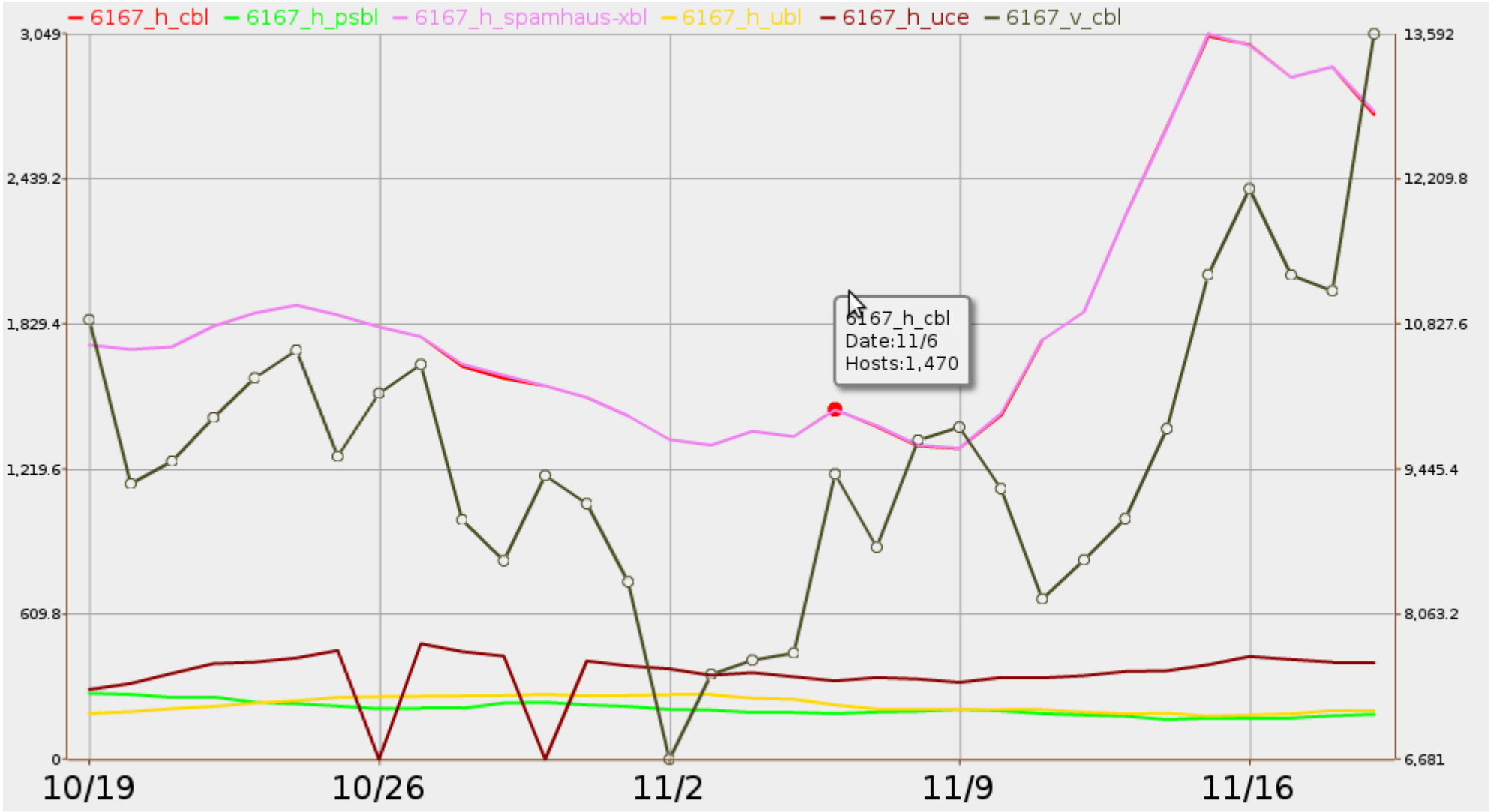
AS 19262 CBL Volume



AS 19262 and CBL Volume Notes

- v_cbl shows number of spam messages as recorded by selected CBL spam traps (right Y axis)
- Spam volume decrease that one day only
- Hard to tell from noise
- Thanks to CBL Team for the CBL volume data

AS 6167 Down then Up



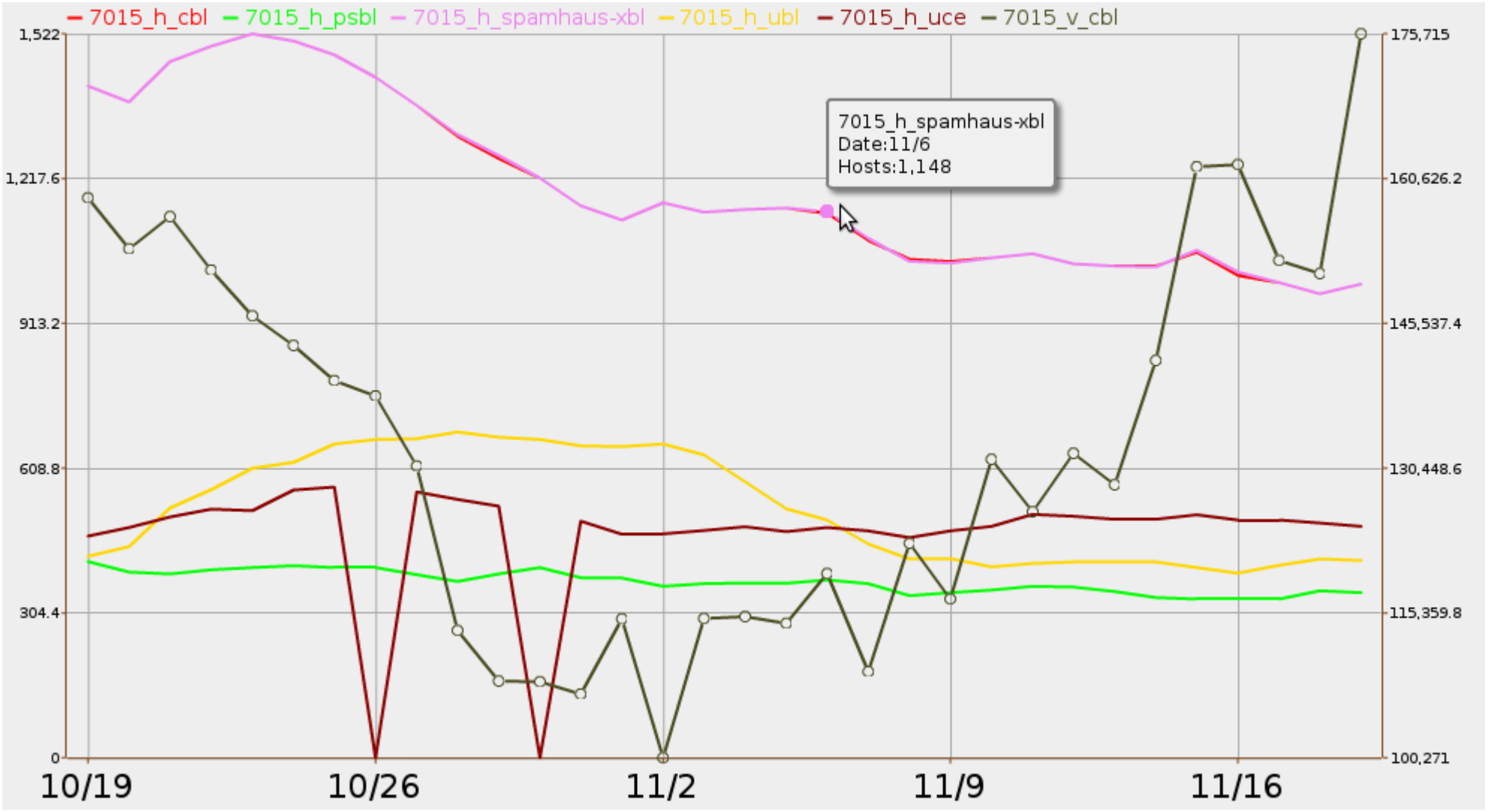
AS 6167 Cellco Notes

- CBL, XBL down 7 Nov
  - And trend down for a few days
  - But then head back up above where they started
- CBL volume spikes down 7 Nov
  - But heads right back up

Trend Search

- So far shown: all ASNs that had many CBL listings.
- Now: look for ASNs trending down 4 - 8 Nov.
- Many examples with low numbers, such as Rice, Harvard, Columbia, Purdue, UCB, Rutgers, Upenn, etc., but those vary all the time.
- Also AS 19262 Verizon (already examined)

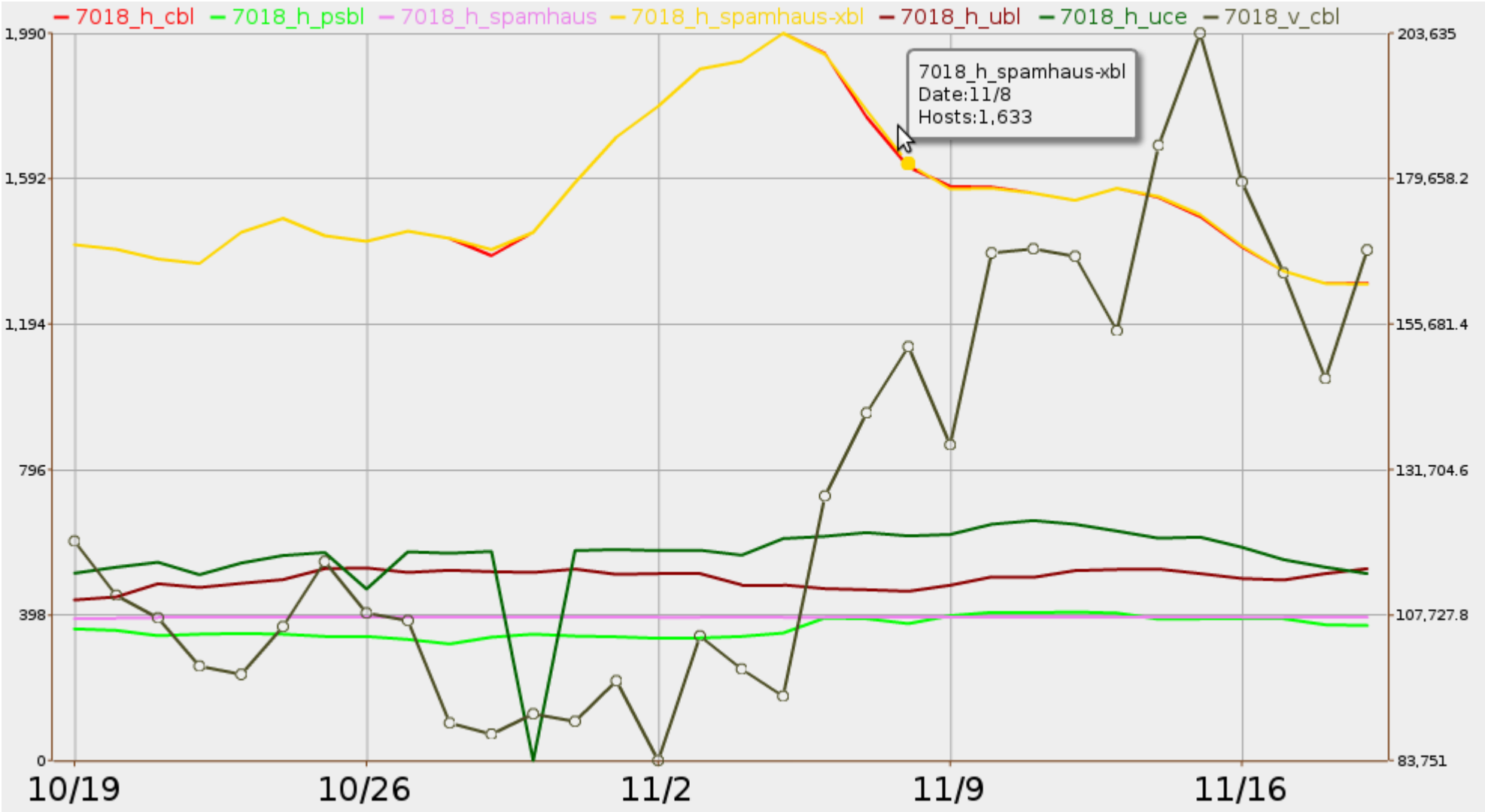
AS 7015 Pyrrhic Victory?



AS 7015 Comcast Notes

- Another Comcast ASN
- CBL and XBL down for 7 Nov and a few days
- CBL volume down 7 Nov then up
  - And then rapidly up
- Doing away with one botnet may have let an even spammier one take over.

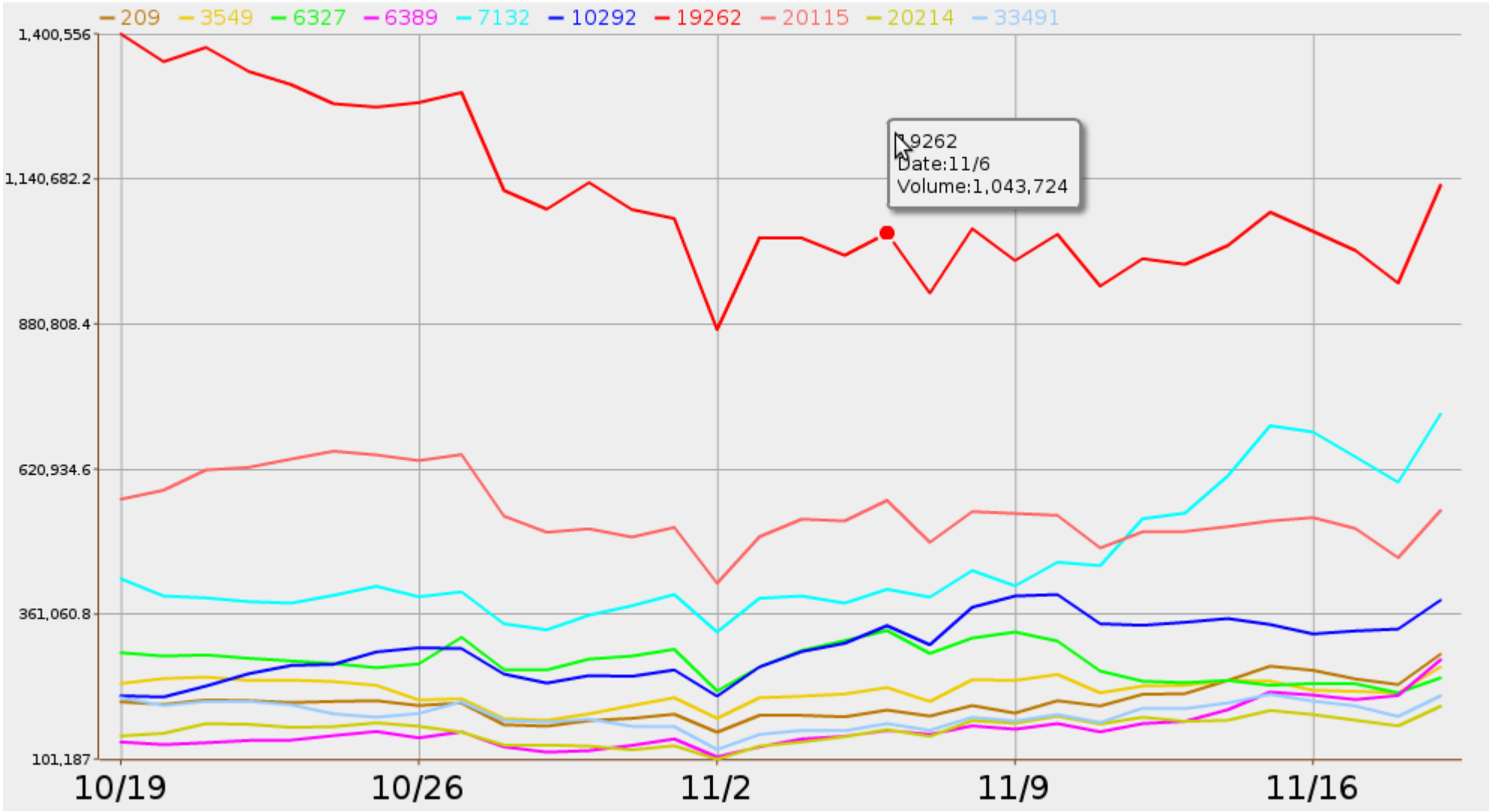
AS 7018 Good and Bad



AS 7018 AT&T Worldnet

- CBL and XBL down starting 6 Nov
- And continue down for 2 weeks
- But CBL volume shows no clear trend

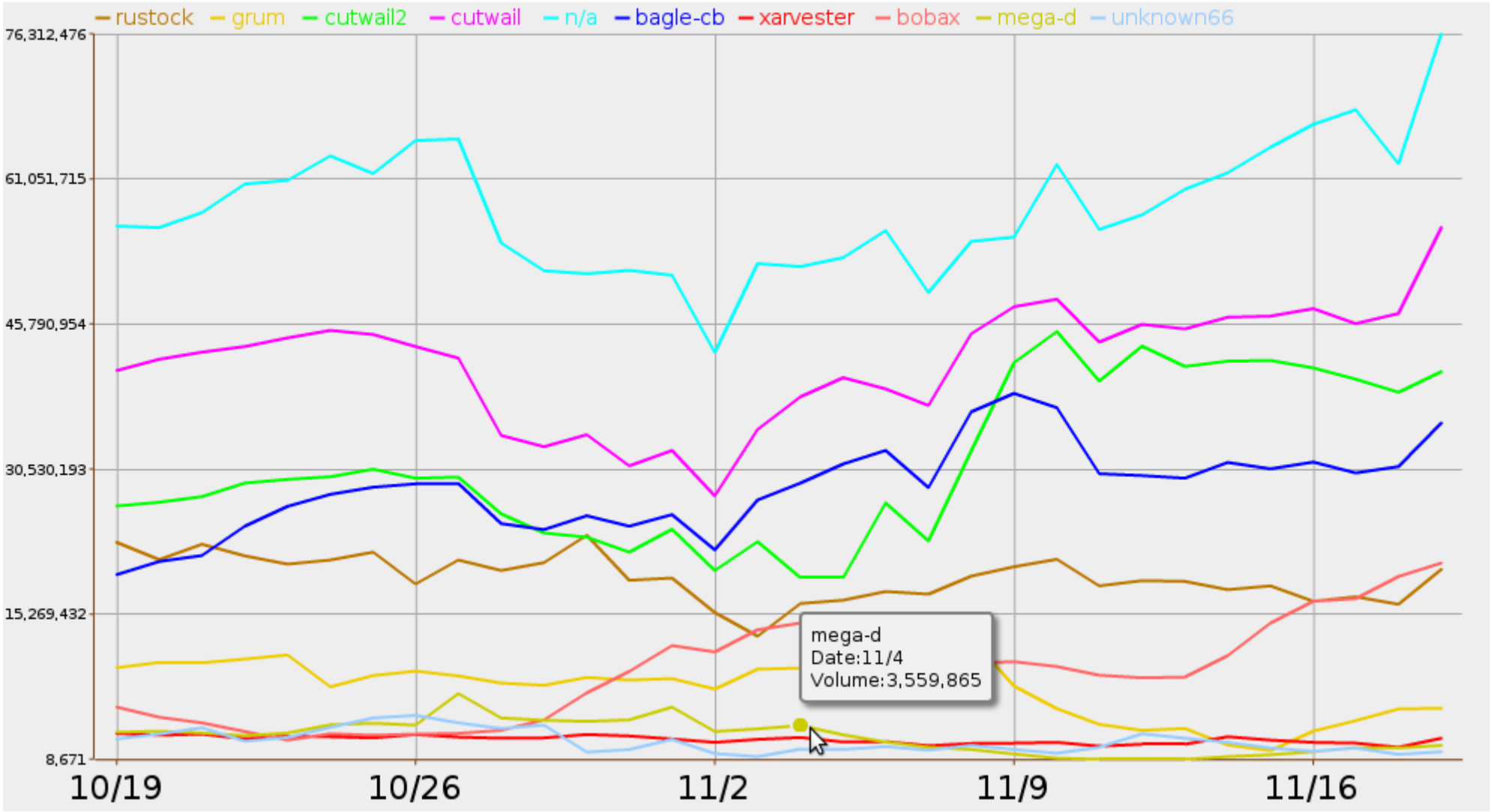
Highest ASes: 7 and 2 Nov



Top 10 ASNs, Volume Notes

- Geographical range limited to ARIN
  - (U.S., Canada, Caribbean)
- We've already seen AS 19262 Verizon
- The rest show the same pattern:
  - A slight dip on 7 Nov that doesn't last
  - And a bigger dip on 2 Nov
- Did somebody do a takedown on 1 Nov?
- Or 28 Oct?

Top 10 Botnets by Volume



Top 10 Botnets by Volume Notes

- N/a, cutwail, cutwail2, bagel-cb, rustock, bobax, grum, mega-d, xarvester, unknown66
- FireEye's target, Mega-D, produced relatively little spam, but even that decreased around takedown time, from 3.5M to 8.6K.
- Mega-d curve similar to M86 Security Labs' Spambot Activity Over Time:
  - www.m86security.com/labs/spam_statistics.asp
  - Order of bots is different (different spamtraps)

Comment from FireEye

- '”Pulling the plug” on a command and control infrastructure is fairly straightforward and can cause an immediate dent while the criminals respond, but without folks like Shadowserver to quickly take the sinkhole data for remediation, you'd see these bots pop back up very quickly (date-based dns c&c generation). That they haven't is a testment to those guys' work.'
- --Alex Lanstein, FireEye

Summary

- Further documentation of something you already knew:
  - Takedowns are great.
  - Congratulations again to FireEye and all the ISPs and registrars who took down this botnet.
- But it's going to take a lot more takedowns a lot more frequently to make a real dent in spam or botnets.

Acknowledgements and Disclaimers

- This material is based upon work supported by the National Science Foundation under Grant No. 0831338 (Insurance, Incentives, and Audited Reputation: An Economic Approach to Controlling Spam).
  - Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.
- Thanks to the blocklist providers, especially to CBL for the volume data, to the RIRs for registration data, and to Team Cymru for consistent global ASN and netblock registration and routing announcement data.
  - They're not responsible for anything in this presentation, either.