PREFIX IPv4 BROKER

Cleaning up after the Nr 3 SPAM botnet and the worst prefix

By Erik Bais – RIPE75

October, 2017

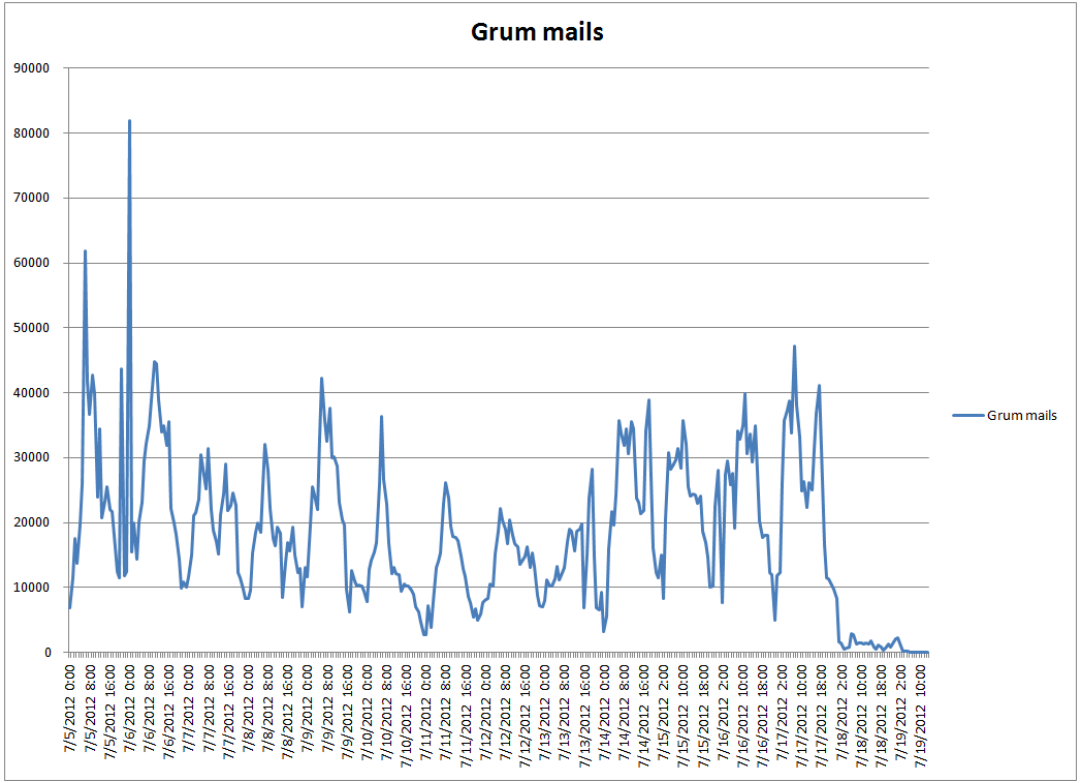
A bit of background

Taking down of the largest GRUM bot network

- A nice read about this whole story : https://krebsonsecurity.com/2012/07/top-spam-botnet-grum-unplugged/

- Once a botnet is down, you can see the effects of that botnet (when it has the size of GRUM) in the global spam effects..

Stats of Grum during July – 2012 till shutdown



Source: Symantec Message Labs

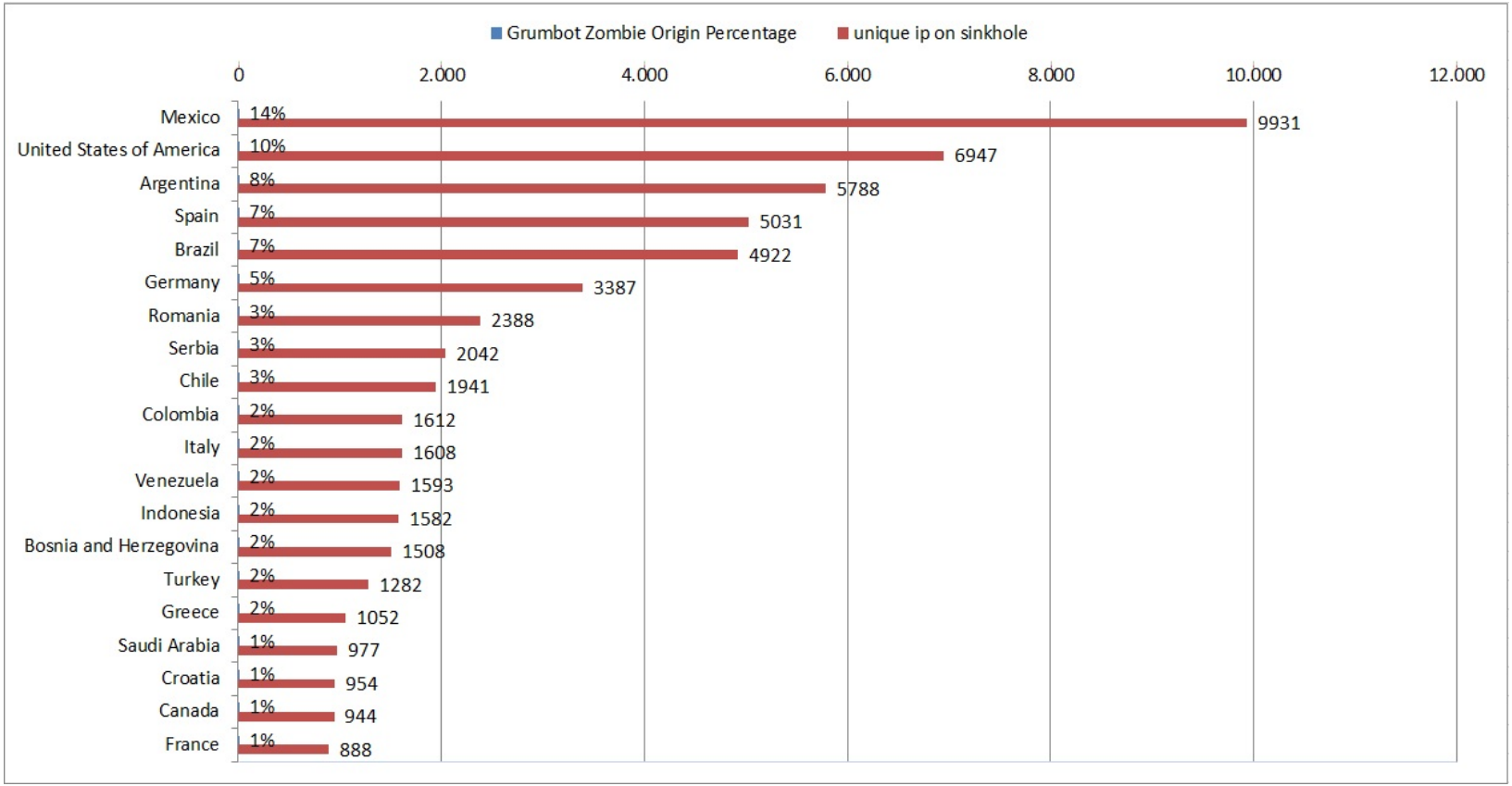
Taking over the IP's of a C&C …

- When all the C&C's where down, we got access to the 'GRUM' IP's.
- And even better .. The actual server was shutdown, but not wiped. ;-)
- We wipe the server (after a backup) and setup a secure sinkhole for the zombie's …

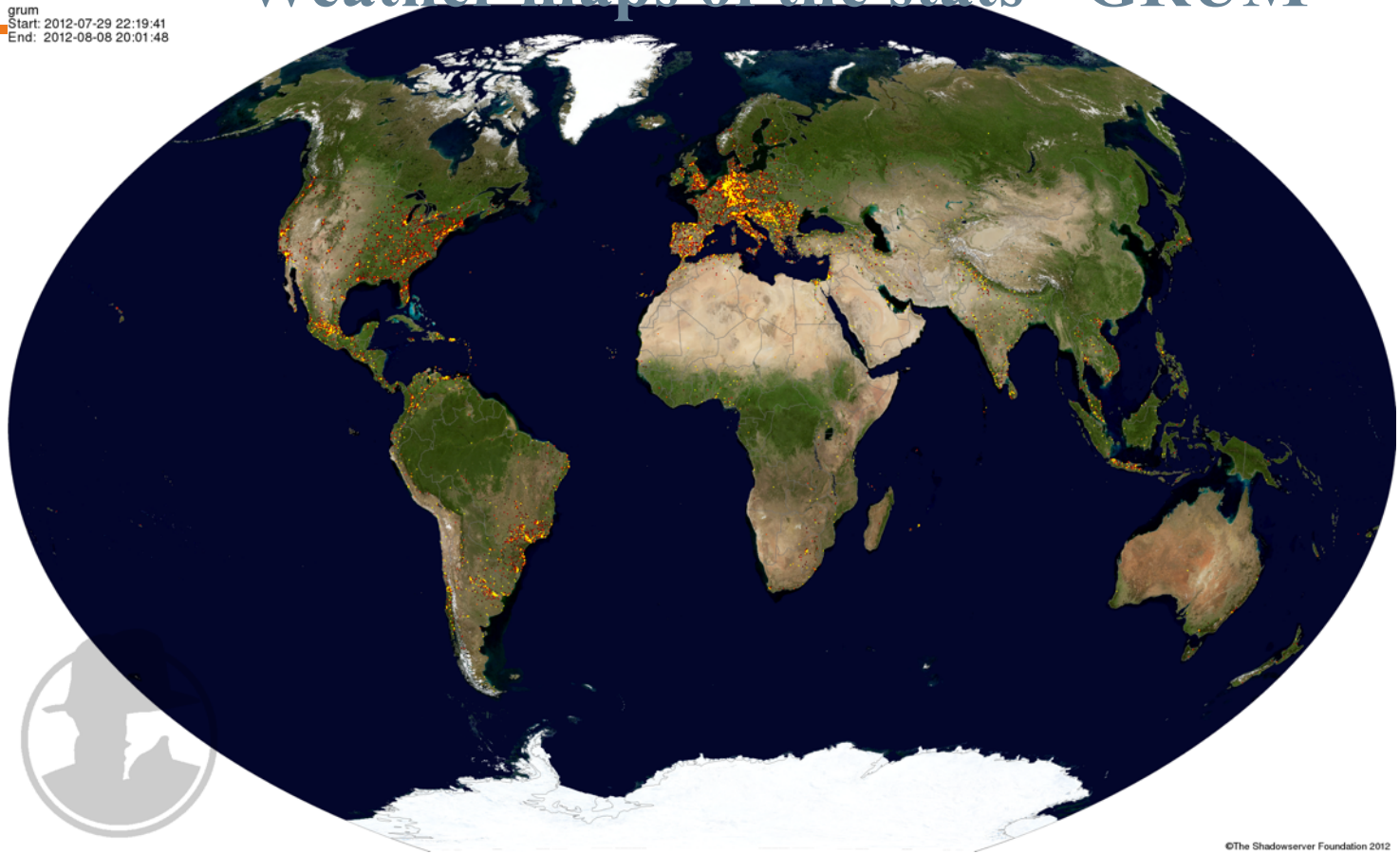
Target : Cleaning the zombie's

- Taking down the C&C's and the botnet will leave a lot of infected PC's (zombies) … dormant ..
- How do you clean those zombies ?
- We opted for reporting to the ISP's per unique connection to the C&C IP's with a signature.. Once per day .. And later per hour ..
- Not all malware has a reliable 'kill / un-install switch' and you don't want to be held responsible for that ..

Initial stats by Country and Unique IP's (Grum)



Weather maps of the stats - GRUM



So how did we do this ?

- Once we had access to the C&C IP's, we worked together with ISC SANS and Shadowserver for building the right infra for a new feed.

- No need to build your own Abuse reporting infra .. Shadowserver already has this infrastructure in place !!

- And a lot of ISP's already parse their messages …

Running the feeds

- Running the feeds means you would expect some clean-up in the numbers …
- Not exactly … ok.. Some improvements .. But not a lot ..

The down-side of opt-in reporting

- Shadowserver only reports to ISP's that wanted to receive their messages..
- Yes, those reports are : opt-in ..
- So we discussed the approach with Abusix and they suggested the following :
  - Report each hour on each unique IP connection.. Instead of each day..
  - Use abuse mailbox info in the IRR DB's and send each hour in x-arf.

More stats – September 2012

timestamp	source	tag	connections	unique_ips	unique_asns	unique_geos
2012-09-16 00:00:00	drones	grum	1518703	87654	2161	175
2012-09-15 00:00:00	drones	grum	1685809	93043	2231	178
2012-09-14 00:00:00	drones	grum	1819142	102839	2539	185
2012-09-13 00:00:00	drones	grum	1785254	105531	2603	186
2012-09-12 00:00:00	drones	grum	1809333	106376	2626	183
2012-09-11 00:00:00	drones	grum	1874680	107011	2646	185
2012-09-10 00:00:00	drones	grum	1804284	106289	2635	184
2012-09-09 00:00:00	drones	grum	1708316	94092	2249	182
2012-09-08 00:00:00	drones	grum	1720786	98288	2277	177
2012-09-07 00:00:00	drones	grum	1710694	106210	2534	186

Results in November 2012 !!

timestamp	source	tag	connections	unique_ips	unique_asns	unique_geos
2012-11-13 00:00:00	drones	grum	1200093	69840	1929	173
2012-11-12 00:00:00	drones	grum	1245087	69446	1916	171
2012-11-11 00:00:00	drones	grum	1191635	64081	1680	167
2012-11-10 00:00:00	drones	grum	1159224	66043	1724	173
2012-11-09 00:00:00	drones	grum	1160222	71957	1946	173
2012-11-08 00:00:00	drones	grum	1242629	72832	1985	168
2012-11-07 00:00:00	drones	grum	1261095	74043	1995	172

The Level3 abuse desk ‘issue’

- The sinkhole hoster almost got shutdown by their upstream because they didn’t matched the reports correctly to their ‘offending’ customers
- They thought the sinkhole was the source of the issue ..
- This took a couple days to understand the issue and to fix the reporting.
  - Lesson learned : don’t include the sinkhole IP in the abuse reports.

A huge shout out to :

Next challenge : the ‘dirtiest’ prefix …

- After the experience with the GRUM botnet … we had the opportunity to buy the LIR with IP space from a Dutch bulletproof hoster …
- The person running the hoster, was just released by the Dutch Police … and was planning to sell his IP space.
- It looked like a proper challenge to get that IP space usable again …

How bad was it ?

- The IP space was blacklisted listed for several years .. Due to known abuse ..
- On SBL .. (over 75 times .. For the actual /19 and many /32 and /24's)
- On DROP .. (Is anyone actually using this ??)
- and that was just on Spamhaus .. But also on many other RBL's and lists.

Approach

- Get full ownership of the LIR.
- Change all references from the previous holder to the new holder.
- Build a new sinkhole.
- Start routing the IP’s to the sinkhole …
- See what we find … we might get lucky …

Hoping for the jackpot

The logs revealed … 12 C&C's

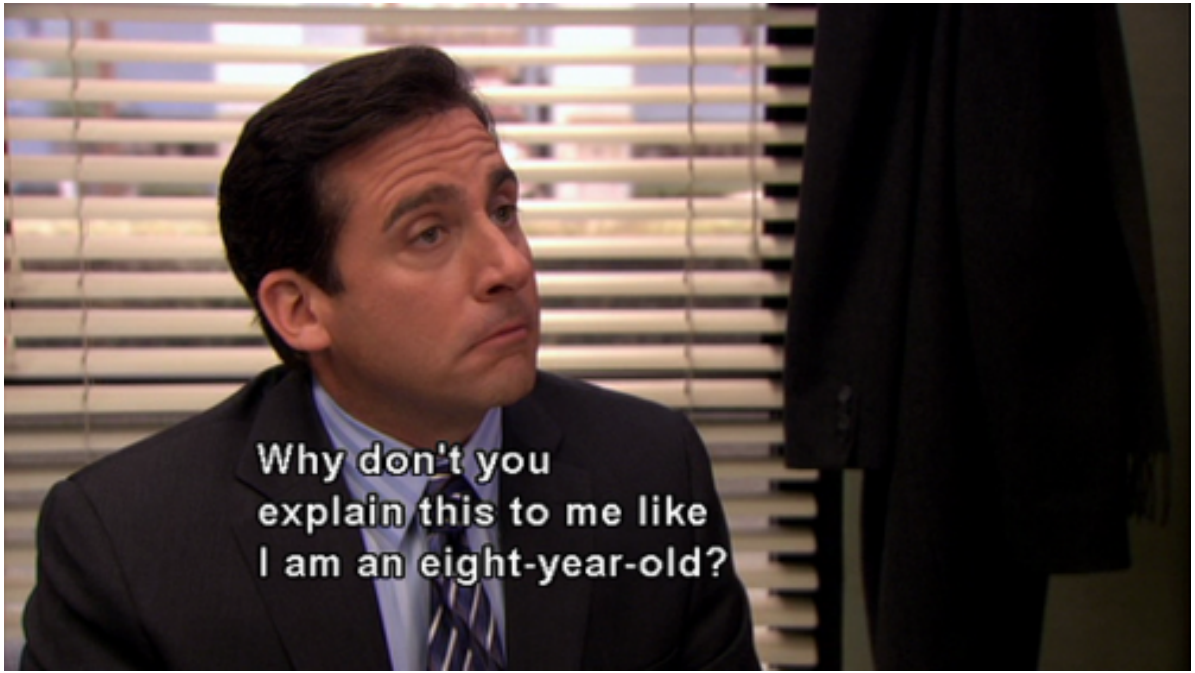
- GRUM bot zombies .. (I wonder how we found these.. ☺)
- Citadel zombies
- Alina zombies
- Black Energy
- Fake AV

Happy happy joy joy

Now what ?

- See if anyone is actually null-routing traffic to the specific prefix ..?
- RIPE Atlas was a great help in finding any routing issues like SH DROP filtering for instance.
- Contacting the RBL owners to de-list the prefix ..

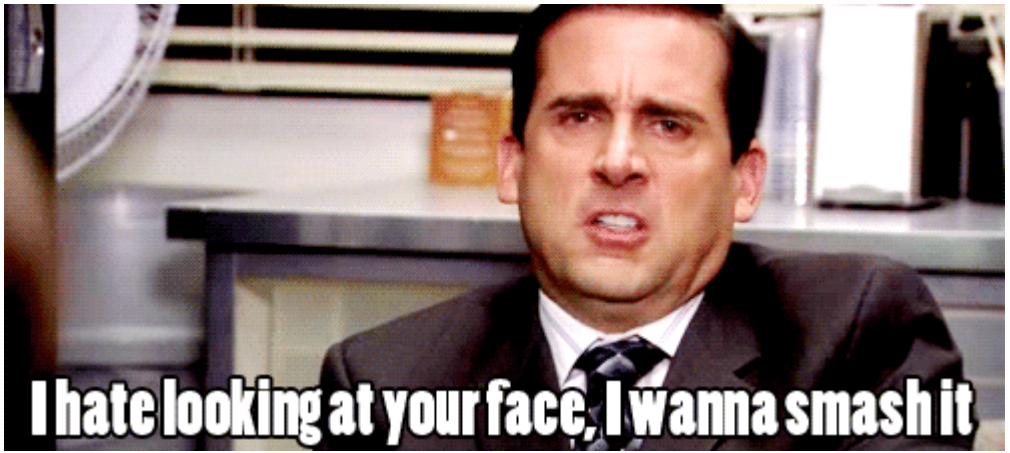
Initial replies from the RBL's



Explain it again with more logic …

- Show them what we are doing ..
- Show initial results of the sinkhole ..
- Kindly explain that we can´t (and won't) be held hostage or accountable from someone elses actions or lack of that..

- Receive kind replies :



Selling the IP Space

- The new owner knew which IP space he was buying and the reputation of the original owner … Transparency is key ..
- They knew upfront about our efforts to clean up the space and the sinkhole.
- The sinkhole was provided along with the feeds to Shadowserver and Abusix after the IP transfer.
- The buyer wanted to purchase the IP space ‘over time’ …

Lessons learned :

Almost all IP ranges can be cleaned .. But some historic issues, take a HUGE amount of time/effort to clean.
And some people would be more than happy to help you..

You might be able to get a good deal as long as you don’t mind null-routing some of the old C&C IP’s in a /19 or so.

PREFIX IPv4 BROKER

Any questions ? ??

THANK YOU

ADDRESS
De Hoefsmid 13
1851PZ Heiloo
The Netherlands

EMAIL
sales@prefixbroker.net

PHONE
+31 85 902 0417

Feel free to contact us if you have any questions