The Grum botnet cleanup

November 2012

DENOG4

Taking down Grum

- July 9th 2012 – FireEye posted a blog stating that only 4 C&C's were left online for the GRUM botnet.
- Grum was at that moment still the 3rd largest SPAM sending botnet globally.
- After a quick communication with the ISP hosting the Dutch C&C servers, FireEye was updated on the progress.
  - FireEye worked with other security researchers to knock down the last 2 C&C servers.
- July 17th 2012 – Only 2 more C&C's still online ..
- July 18th 2012 – Last 2 C&C knocked down.

Taking down Grum

- After a few days, there was a short period that the Botnet herder was regaining controll of 1 C&C server.. But that was not enough to point the malware to a new location.

- Grum malware only used hardcoded IP address. No domain name was used.

Getting in control

- After the initial takedown, the Dutch hoster was asked to provide the IP's to redirect them to a sinkhole...
- He did even better ...
- As the original server was still online, we received the server to be cleaned up...

Getting in control

- Instead of cleaning up the server ...
- 2 secure disk copies were made using a CAINE LIVE CD. (using DC3DD) to a USB HDD
  - 1 copy worked like a charm and the second copy didn't, we found out..
- After the copy the server was re-ïnstalled with a fresh OS and implemented as a sinkhole for the zombies.
  - After that, the null-routes were removed and the fun could get started ...

Digging through it ...

- The original GRUM C&C server had 350 Gb of uncompressed data on online ....
- It took about 3 evenings to process the majority of the data ...
- That effort was done together with Brian Krebs from http://www.krebsonsecurity.com
  - The SPAM panel was setup again on another server ...
  - The MD5 passwd was cracked using a fancy online rainbow decrypter.
  - We found encrypted and de-crypted malware samples.
  - And lots of HUGE spamlists.. About 300 Gb of un-compressed maillists.
  - Including spam templates and data about online pharmacy orders ...
  - http://krebsonsecurity.com/2012/08/inside-the-grum-botnet/ Blogpost about it all
- And .. We found very strong effidence on the drive about who ran the server ...

Inside the Grum Botnet

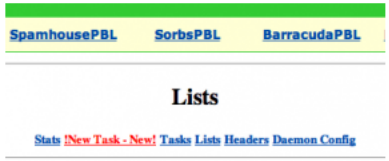
KrebsOnSecurity has obtained an exclusive look inside the back-end operations of the recently-destroyed **Grum** spam botnet. It appears that this crime machine was larger and more complex than many experts had imagined. It also looks like my previous research into the identity of the Grum botmaster was right on target.

A source in the ISP community who asked to remain anonymous shared a copy of a Web server installation that was used as a controller for the Grum botnet. That controller contained several years' worth of data on the botnet's operations, as well as detailed stats on the spam machine's size just prior to its takedown.

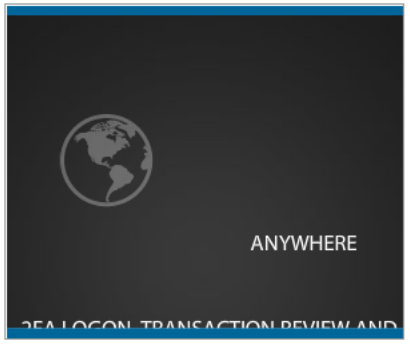
The "Stats" page from a Grum botnet control panel show more than 193,000 systems were infected with the malware.

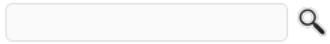
At the time of Grum's demise in mid-July 2012, it was responsible for sending roughly one in every six spams delivered worldwide, and capable of blasting 18 billion spam emails per day. Anti-spam activists at Spamhaus.org estimated that there were about 136,000 Internet addresses seen sending spam for Grum.

But according to the database maintained on this Grum control server prior to its disconnection in mid-July, more than 193,000 systems were infected with one of three versions of the Grum code, malware that turned host systems into spam-spewing zombies. The system seems to have kept track of infected machines not by Internet address but with a unique identifier for each PC, although it's not immediately clear how the Grum botnet system derived or verified those identifying fingerprints.



The Web interface used to control the botnet was called "Zagruska Systems," ("zagruska" is a transliteration of the Russian word "загрузка," which means "download"). The HTML code on the server includes the message "Spam Service Coded by -= (





Recent Posts

Infamous Hacker Heading Chinese Antivirus Firm?
Microsoft Patches 19 Security Holes
Malware Spy Network Targeted Israelis, Palestinians
Experts Warn of Zero-Day Exploit for Adobe Reader
Adobe Ships Election Day Security Update for Flash

Subscribe by email

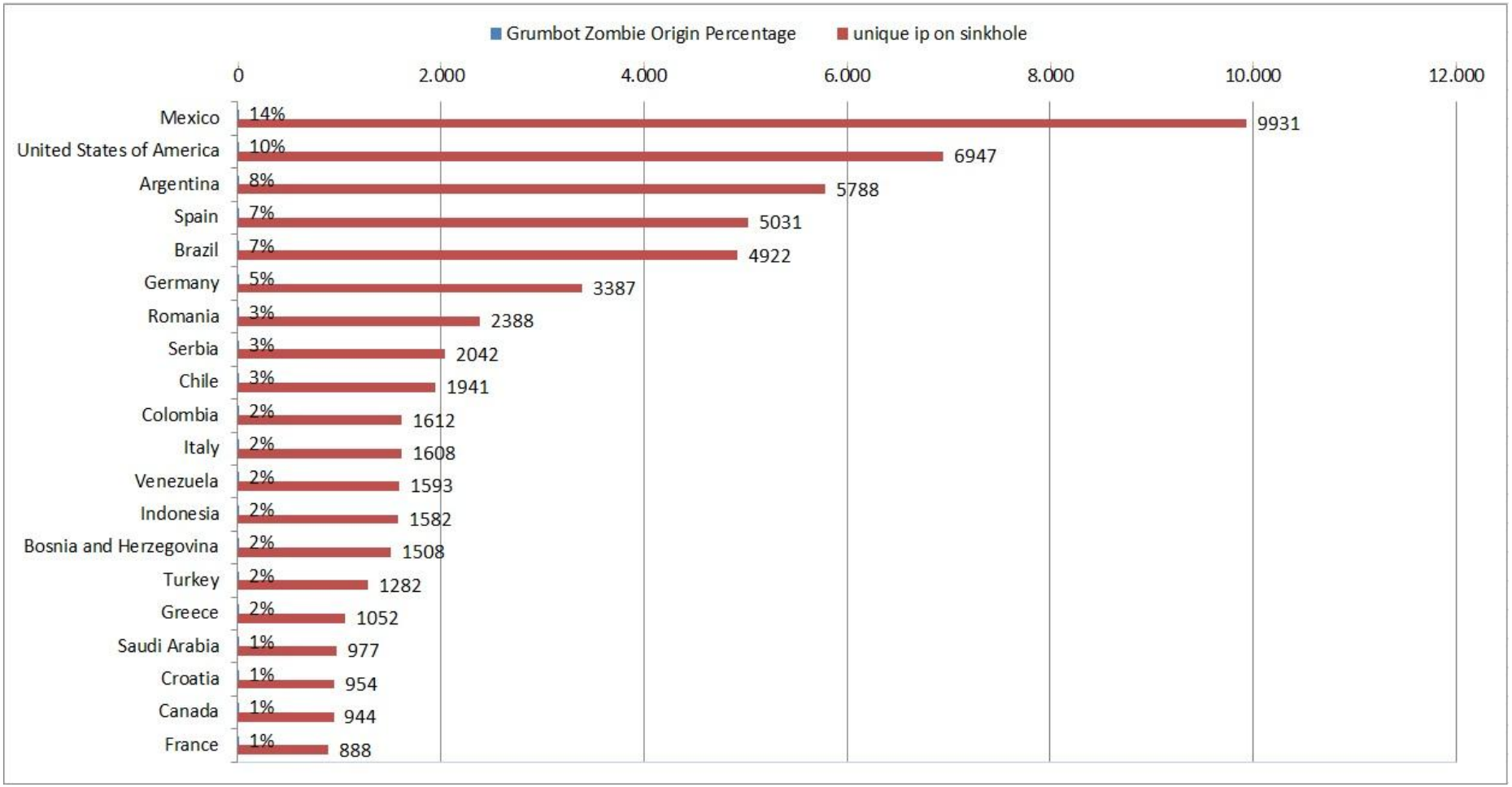
Your email:

Enter email address...

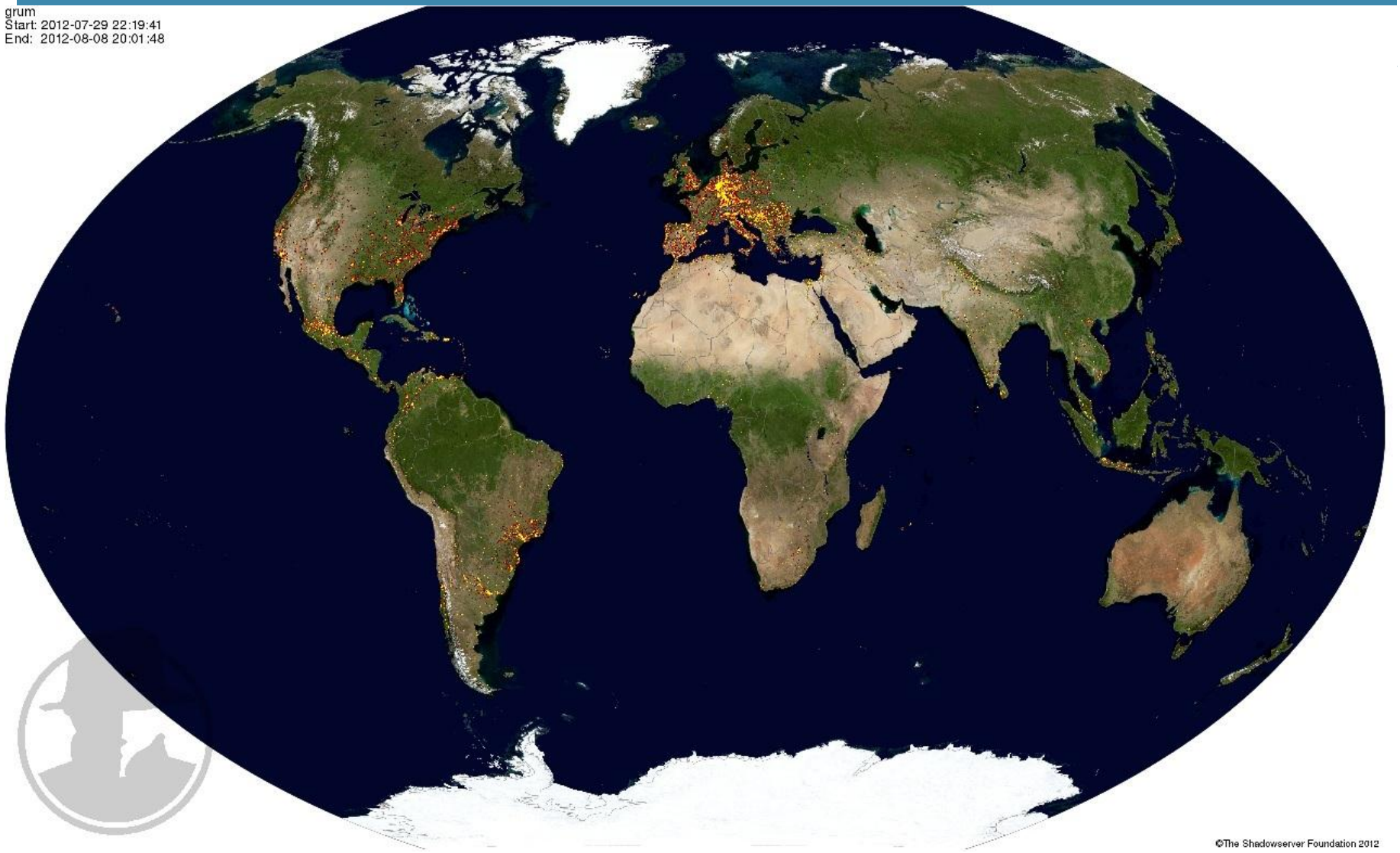
Running a sinkhole

- So running a sinkhole is one ... But what to do with all the data ?
- Shadowserver.org to help ...
  - Shadowserver.org is a non-profit foundation
  - Provides a free daily update on infections in your network.
- Got a sinkhole ? Check with shadowserver.org if they can use the feed / logs for processing.
- The goal of the Grum sinkhole is getting the zombie's logged and the logs processed, to reduce the infections.

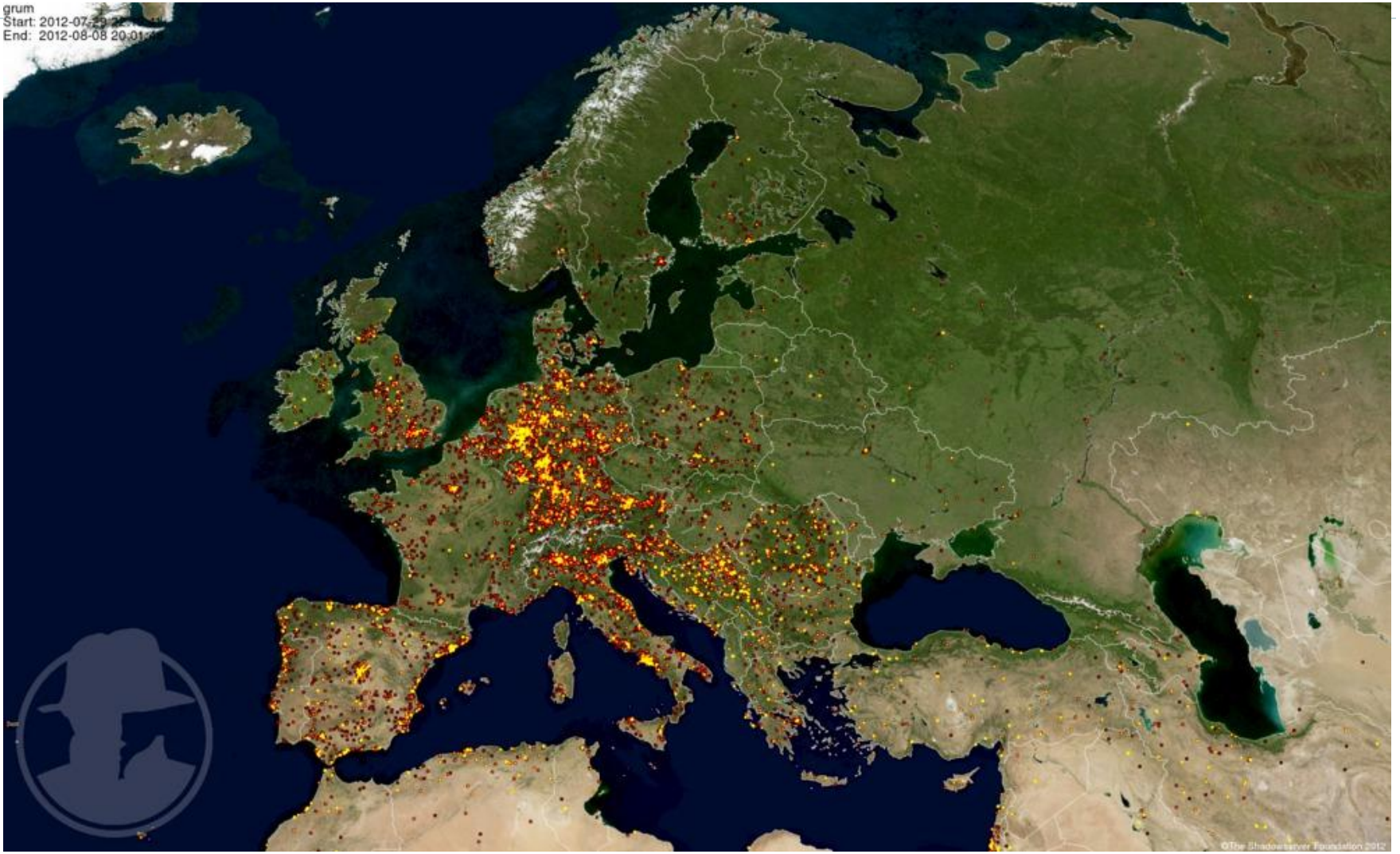
Geo origin ....


Grumbot Zombie Origin Percentage
unique ip on sinkhole
0
2.000
4.000
6.000
8.000
10.000
12.000
Mexico 14% 9931
United States of America 10% 6947
Argentina 8% 5788
Spain 7% 5031
Brazil 7% 4922
Germany 5% 3387
Romania 3% 2388
Serbia 3% 2042
Chile 3% 1941
Colombia 2% 1612
Italy 2% 1608
Venezuela 2% 1593
Indonesia 2% 1582
Bosnia and Herzegovina 2% 1508
Turkey 2% 1282
Greece 2% 1052
Saudi Arabia 1% 977
Croatia 1% 954
Canada 1% 944
France 1% 888

Global Weathermap



Weathermap – Grum infections Europe



Infections for Germany
Rank #6 globally

timestamp	source	tag	geo	connections	unique_ips	country
2012-11-13 00:00:00	drones	grum	DE	71543	4447	Germany
2012-11-12 00:00:00	drones	grum	DE	71152	4490	Germany
2012-11-11 00:00:00	drones	grum	DE	74644	4314	Germany
2012-11-10 00:00:00	drones	grum	DE	67116	4118	Germany
2012-11-09 00:00:00	drones	grum	DE	65086	4412	Germany
2012-11-08 00:00:00	drones	grum	DE	72520	4655	Germany
2012-11-07 00:00:00	drones	grum	DE	71210	4731	Germany
2012-11-06 00:00:00	drones	grum	DE	65897	4572	Germany
2012-11-05 00:00:00	drones	grum	DE	64454	4446	Germany

What can you do ...

- Make sure your abuse info is up to date in the RIPE DB

- Subscribe to the Shadowserver.org
  - http://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork
  - Email the required info to : **request_report *<at>* shadowserver.org**
  - Only for prefixes you control directly and/or your ASN.
- Process the X-ARF messages send out by ABUSIX.org (http://www.abusix.org)

Who has the first question ?