HOST exploit

Top 50 Bad Hosts & Networks 2010 Q4

WORLDWIDE CYBERCRIME SERIES

Main findings of this quarter's report

#1 Bad Host 2010 Q4

VolgaHost
Russia
Private Registration
AS29106 - 256 IPs

For hosting Zeus servers, malicious web sites, badware, C&C and exploit servers.

In the #1 slot this quarter is **VolgaHost AS29106.** This is no shock horror story as this small Russian network with only 256 IPs is known for hosting malware, trojans and all manner of nefarious cybercrime friendly activities. In some quarters it has been called an 'evil network'.[1]

More disappointing than surprising is the return of **eNom AS21740**, the registrar arm of Demand Media, to the #3 position after what seemed to be a geniune effort to clean up its networks. A more determined attempt to rid its servers of outlets that deliver badware is required before the pending IPO can be taken seriously.

More vigilance on keeping networks clean is the theme of this quarter's report. Token efforts may produce good publicity for a short while but that will only be short-lived if not maintained. The quarterly ***HostExploit 'Top 50 Bad Hosts and Networks Report',*** an analysis based on the ***HE Index***, will continue in its mission to reveal the best and the worst hosts.

1 http://blog.dynamoo.com/2010/07/evil-network-as29106-91213174024.html

[Download the full report here.]

Worst hosts by category...

Spam	AS31133 - MegaFon	Russia
Botnets	AS36408 - CDNetworks	United States
Zeus Botnet	AS20564 - Informex	Ukraine
Phishing	AS10297 - eNET	United States
Exploit Servers	AS13100 - Data Electronics Group	Ireland
Badware	AS21740 - eNom / DemandMedia	United States
Infected Sites	AS6851 - BKCNET	Latvia
Current Events	AS16138 - Interia.PL	Poland

AT A GLANCE

36,371 ASes TESTED
An increase of 858 since the 2010 Q3 report.

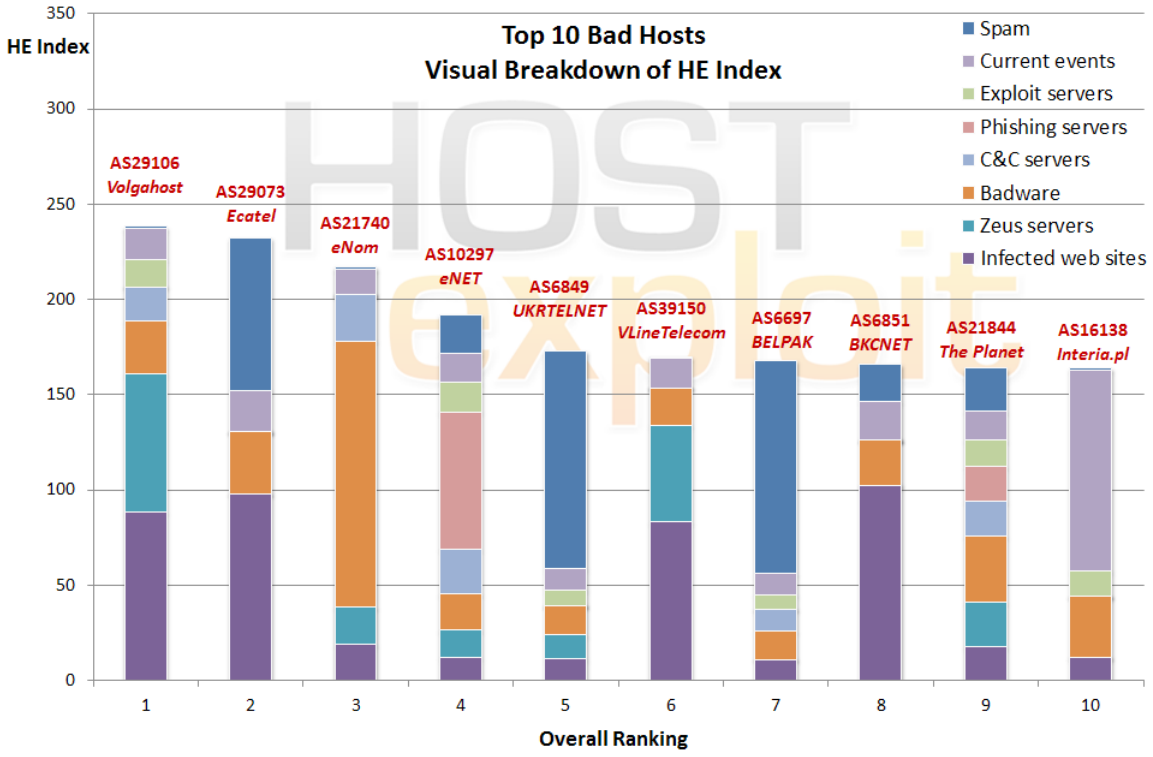
WHAT'S NEW
Worst Hosts by Sector Comparison Chart - a ready reckoner.

REPEAT OFFENDERS
Volgahost, Ecatel, eNom: Not much surprise to us that familiar names appear yet again in the top positions.

WORST COUNTRY OR BEST COUNTRY?
United States: 21 Bad Hosts in Top 50 but also 3 Good Hosts in Top 10

MOST DISAPPOINTING
Back up to #3 for eNom

a CyberDefcon service



CONGRATULATIONS TO OUR BEST HOST

Symbio Networks (AU) AS38333 #1 Good Host for low levels of badness.

ARE CLEAN NETWORKS ACHIEVEABLE:

Yes, with a combination of vigilance, advice from specialist security analysts, working with law enforcement and local CERTS. See the *Top 10 Good Hosts* in the full report.

INDEPTH ANALYSIS

Read the full *'Top 50 Bad Hosts and Networks Report'* for an indepth analysis and breakdown of these results. Available for download here.

Individual assessments are available upon application.

http://hostexploit.com

http://sitevet.com

Part of the CyberDefcon Group

http://cyberdefcon.com

Contact:

admin@cyberdefcon.com

REPORT HIGHLIGHTS

- #1 Bad Host **Volgahost AS29106** appears in the Top 10 listings for infected web sites, and botnet hosting.
- At #2 **Ecatel AS29073** hosts operations with high levels of infected web sites, current events, badware and spam.
- #3 Bad Host **eNom AS21740** is in pole position for high levels of badware.
- Congratulations to Good Hosts: **#1 Symbio Networks**, **#2 Open Access** and **#3 CyberTrails**,
- A reputation for clean hosting is achievable and worthwhile. Don't let turning a blind eye to cybercriminal activity ruin your reputation as a host.

SERVICES AVAILABLE

Host remediation

Malware and exploit analysis

Reverse engineering

Threat analysis

Early warning advice

Individual assessment by application

a CyberDefcon service