HOST exploit

Top 50 Bad Hosts & Networks 2011 Q1

WORLDWIDE CYBERCRIME SERIES

Main findings of this quarter's report

#1 Bad Host 2011 Q1

Webalta
Russia
www.wahome.ru
AS41947: ~15,000 IPs

For hosting Zeus servers, exploit servers, spam, C&Cs and others.

The "winner" of this quarter's Top Bad Host is the Russian-based host Webalta. The situation on Webalta's servers has steadily worsened over the last few months, and it has come in at #1 overall without being ranked #1 in any of the specific badness categories. This is a result of being highly-ranked in a broad array of sectors, which suggests extremely slack abuse procedures.

This quarter we discuss many of the pertinent industry topics such as the LizaMoon SQL injection attacks, the Rustock takedown, Advanced Persistent Threats, mobile malware and 32-bit ASNs.

We also continue our regular themes on crime servers, biggest movers, good hosts and country analysis.

Download the full report here.

Worst hosts by category...

Spam	AS45899 - VNPT	Vietnam
Botnets	AS36408 - Panther Express	United States
Zeus Botnet	AS49469 - Sa Nova Telecom	Romania
Phishing	AS10297 - ENET-2 - eNET Inc.	United States
Exploit Servers	AS21607 - DeployLinux	United States
Badware	AS33626 - Oversee.net	United States
Infected Sites	AS6851 - BKCNET "SIA" IZZI	Latvia
Current Events	AS16138 - Interia.pl	Poland

AT A GLANCE

37,271 ASes TESTED

An increase of 900 since the 2011 Q4 report.

WHAT'S NEW

» Top 10 New Hosts
» Rustock Analysis

REPEAT OFFENDERS

» AS29073 Ecatel
» AS45899 VNPT
» AS16138 Interia.pl

MOST PREVALENT COUNTRIES

» United States
» Russia
» China
» Germany

ONE TO WATCH

AS50693 Konsing group: up from #28,462 to #26.

a CyberDefcon service

CONGRATULATIONS TO OUR BEST HOST

AS2688 AT&T LA - #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 AVAILABLE UPON APPLICATION

http://hostexploit.com

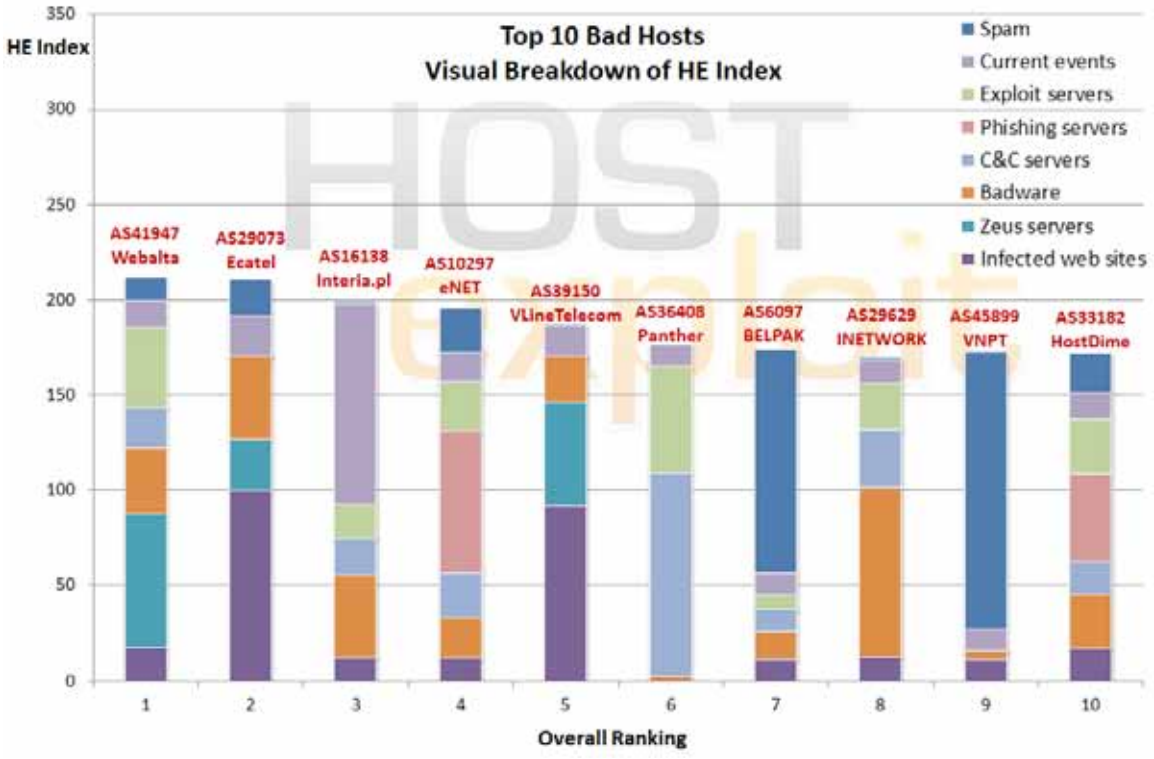
http://sitevet.com

Part of CyberDefcon

http://cyberdefcon.com

Contact:

admin@cyberdefcon.com



REPORT HIGHLIGHTS

- Breakdown of the worst hosts by categories of malicious activity
- Analysis of the Rustock takedown and the impact on spam levels
- Dealing with new threats - mobile malware and Advanced Persistent Threats (APT)
- 32-bit ASNs - what is their effect on cybercriminal activity?
- The most improved and most deteriorated hosts as well as crime servers and good hosts

SERVICES AVAILABLE

- Host remediation
- Malware and exploit analysis
- Reverse engineering
- Threat analysis
- Early warning advice
- Individual assessment by application

a CyberDefcon service