



2006 Internet Attack Statistics for Belgium

Hillar Leoste
Zone-H.org

**OWASP
BeLux
Chapter**

Copyright © 2007 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms
of the Creative Commons Attribution-ShareAlike 2.5 License. To view this license, visit
<http://creativecommons.org/licenses/by-sa/2.5/>

The OWASP Foundation
<http://www.owasp.org>

Agenda

- About Zone-H and defacements
- Statistics

What is Zone-h.org

- News, advisories and opinions, provided from recognized IT security news sites, trusted product vendors and pro-active members of **zone-h** international community
- Statistics of most recent digital attacks, surveys and detailed analyses, presented in our regular reports
- Worth-to-read articles, describing new developments in the IT security world
- Interviews with leading IT Security industry experts, accompanied by an opportunity to discuss different topics in specialized forums and IRC chatrooms
- Ongoing evaluations of current digital threats and short-time prognosis
- Case and motivation studies of digital incidents.
- Daily newsletters
- Free Security services: daily “early warning” bulletin + InfoSec pager

What is Zone-h.org

Disclaimer:

Zone-h neither: condones, promotes, and/or participates in attacks that are recorded within our database. It is however in a unique position that such attacks are freely reported to our organization.

Zone-h catalogues several useful pieces of information for each intrusion including the timestamp of the attack, software version of the webserver, the operating system, motivation of the attacker, and reported technical details of the intrusion methodology.

Defacement

Defacement is an attack against webpage, replacing the main (usually) page with attackers page.

Reasons:

Political (hacktivism) – Mohammed cartoons, G8, war in Iran, conflict between Israel and Palestine, etc

Best defacer

Fun

Challenge

Statistics for .be

	<u>2005</u>	<u>2006</u>		<u>2005</u>	<u>2006</u>
Jan	401	159	Jul	274	1832
Feb	320	415	Aug	268	1040
Mar	160	168	Sep	85	1347
Apr	297	341	Oct	137	359
May	354	205	Nov	205	299
Jun	189	443	Dec	199	415

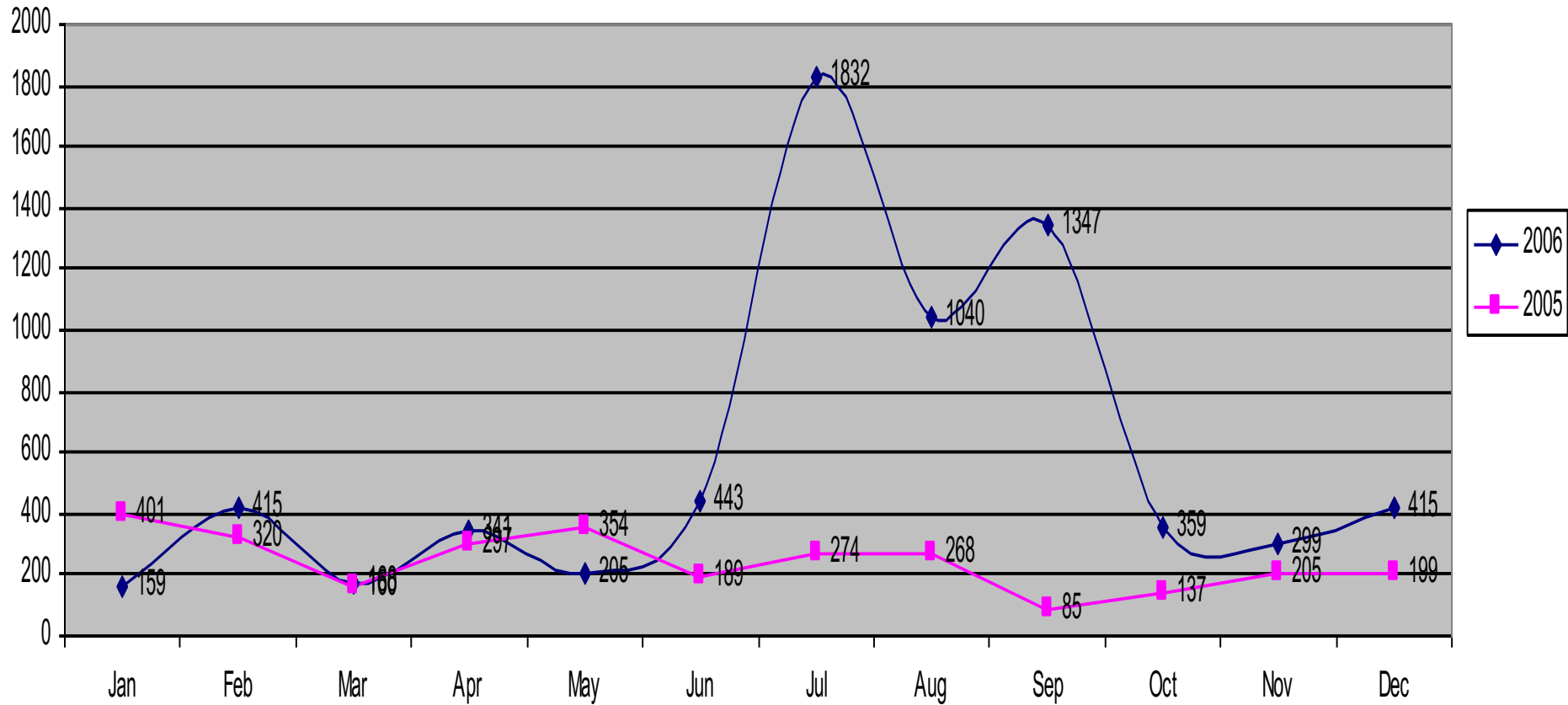
Total:

2005 – 2889

2006 - 7023

Statistics for .be

Defacements 2005 & 2006



Statistics for .be

By OS:

2005

Linux	1824	63 %
Windows	919	32 %
BSD	53	1 %
Mac	46	1 %
Solaris	20	1 %
Tru64	17	1 %
Unknown	10	1 %

2006

Linux	4883	70 %
Windows	1916	27 %
BSD	156	2 %
Mac	45	0.6 %
Solaris	12	0.2 %
Unknown	10	0.15 %
OS2	1	0.05 %

Statistics for .be

By webserver:

2005

Apache	1918	66 %
IIS	913	31 %
Roxen	38	1 %
Unkown	17	0.5 %
Lotus-Domino	1	0.5 %
WebSTAR	1	0.5 %
Zeus	1	0.5 %

2006

Apache	5046	72%
IIS	1905	27%
Unknown	48	0.7%
Nginx	17	0.2%
NOYB	4	0.05%
SonataServer	2	0.03%
Lighttpd	1	0.02%

Statistics 2005 for .be

By attack type:

File inclusion	1090	Radmin panel attacks	52
Attacks against user	327	DNS attacks	52
Other web app bug	303	URL poisoning	19
SQL Injection	276	Known vuln.	19
Not available	225	SSH server intrusion	16
FTP server intrusion	127	Mail server intrusion	15
Web server intrusion	122	Telnet server intrusion	14
MITM	86	Shares	8
Other server intrusion	57	Firewall/router attacks	8
Web server ext. module	57	0day	6
		RPC server intrusion	5
		Brute force	3
		Misconfig	2

Statistics 2006 for .be

By attack type:

Attacks against user	1696	Firewall/router attacks	185
File inclusion	904	MITM	177
SQL injection	638	Shares	170
Not available	569	RPC server intrusion	169
Other web app bug	437	DNS attacks	109
Other server intrusion	414	Remote service attacks	108
FTP server intrusion	326	Web server intrusion	101
Web server ext. module	319	Telnet server intrusion	99
SSH server intrusion	300	URL poisoning	81
Radmin panel attacks	194	Mail server intrusions	27

Statistics 2005 for .be

By apps:

forum	222
guestbook/gastenboek/gastje	95
foto/photo	13
blog	12
bb2	10
nuke	3
gallery	3

Statistics 2006 for .be

By apps:

forum	347
foto/photo/album	75
phpbb	39
gallery	27
guestbook/gastenboek/gastje	25
cms	20
joomla	12
blog	11
mambo	10
board	8
nuke	7

Statistics 2006 for .be

Bits and pieces

police.be/forum

Some sites from

kuleuven.ac.be

and

ulg.ac.be

140 double defacements

21 big (more that 30 sites per IP) attacked

Statistics for .be

?