

2004 WEB SERVER INTRUSION STATISTICS

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 maintains the largest archive of information about attacks against Internet web servers. The database contains information related to nearly one million server intrusions over a span of several years. Every day the Zone-H volunteers receive an average of 2.500 notifications related to web server intrusions. Each instance is then verified and catalogued.

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

Why does Zone-H take the duty to catalogue the attacks?

There are several reasons; the most important can be briefly summarized as:

There is no security without concern, there is no concern without the disclosure of correct information.

In a world where the Internet is taking over most of the processes that are allowing our society to exist, a weak Internet would cause much greater problems than the webserver defacements. The fact that webserver defacements are the most visible, tangible and monitorable form of the criminal phenomenon. Zone-H collects and uses this information as the way to check the pulse of the Internet insecurity. From this our motto *"the Internet thermometer"*

Moreover, defacement is just a choice of the attacker; in most circumstances the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage.

The Collection of this information provides for the evolution of trends and definition of techniques. The disclosure of the techniques, allows system administrators the opportunity to test their own servers and close the security holes that are used. The information provides Zone-H a crystal-clear view of what is going on the Net.

This document contains aggregated information related to the Zone-H webserver intrusion database and is copyright 2000-2005 Zone-H. This document is probably the only unbiased and reliable source of information related to server side cyber intrusions. Zone-H information might differ from that provided by other vendors or large commercial institutes; the reason is that Zone-H is basing its data on concrete facts. This report was created from the largest known database of its kind. It was not created from what is commonly used; rumors, commercial hysteria or unverifiable facts.

This data can be reproduced partially or totally with permission and credit to Zone-H.org. The title as provided

Independent observation of web server cybercrimes
Statistics provided by www.zone-h.org
Copyright 2002-2005 Zone-H

as well as respecting the Creative Common License attached at the end of the document.

INDEX

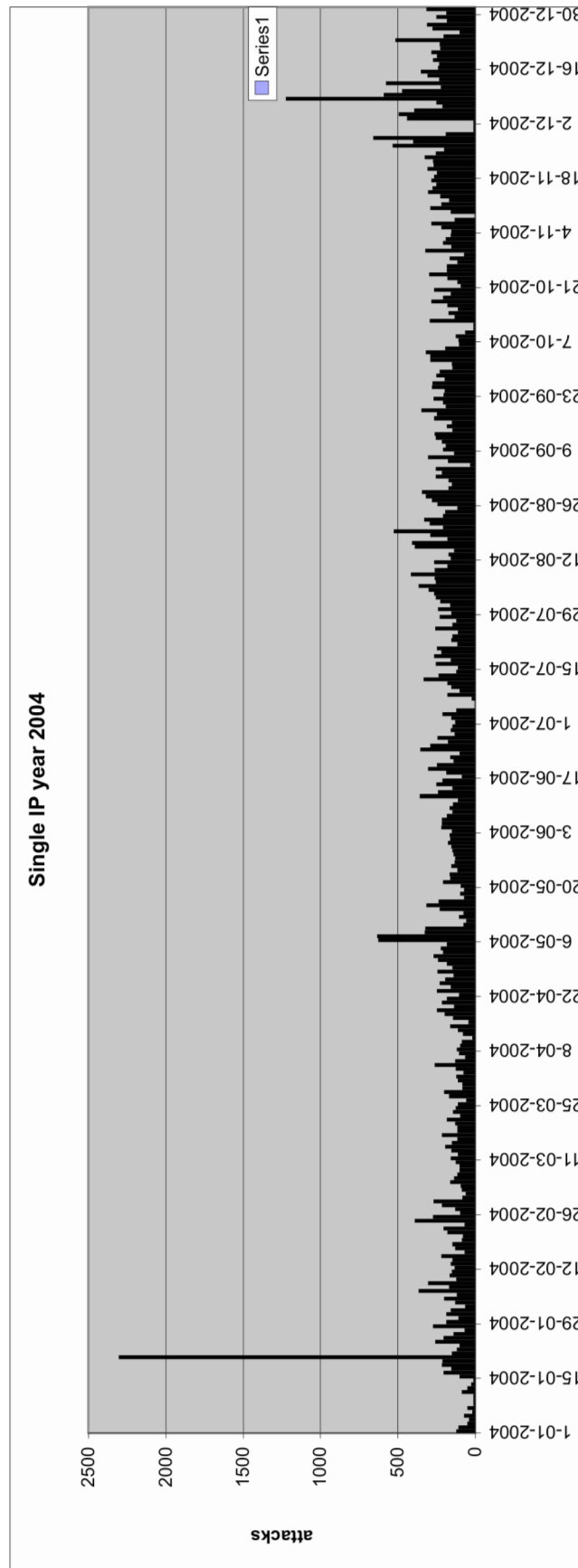
- 1 – 2 Disclaimer
- 4 Single IP – daily statistics for the year 2004
- 5 Mass defacements – daily statistics for the year 2004
- 6 Single and mass defacements by months for the year 2004
- 7 Mass defacements for the years 2000 – 2004 (by months)
- 8 Single IP for the years 2000 – 2004 (by months)
- 9 OS families, single IP for the years 2000 – 2004 (by months)
- 10 OS families mass defacements for the years 2000 – 2004 (by months)
- 11 Webserver families single IP and mass for years 2003 – 2004 (by months)
- 12 Attacker's motivations for years 2002 – 2004 (by months)
- 13 Attack technical details for years 2002 – 2004 (by months)
- 14 Creative Commons Licensing scheme

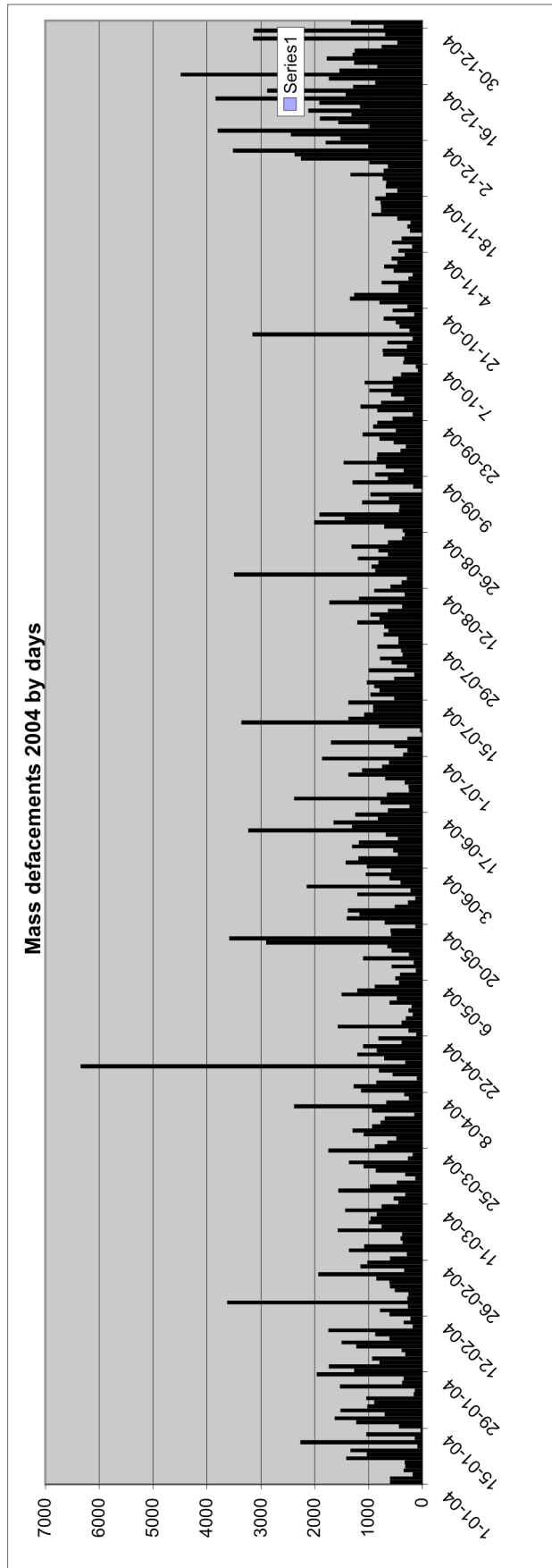
Notes:

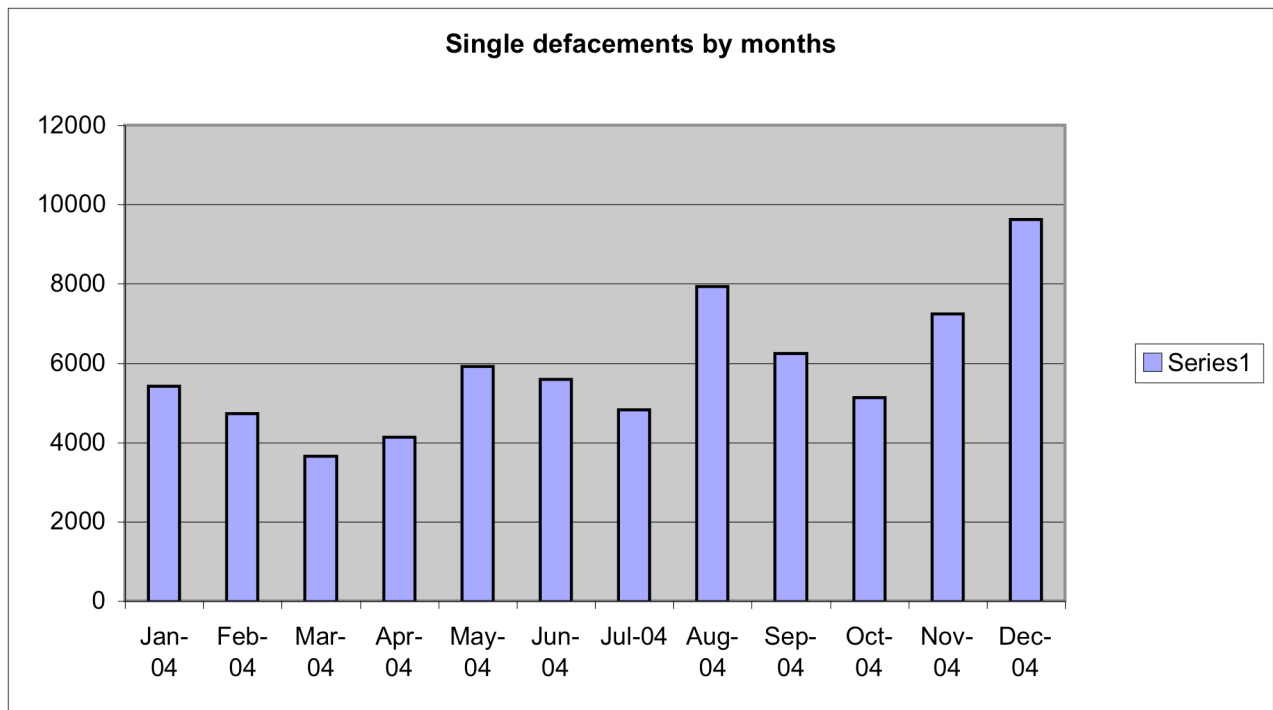
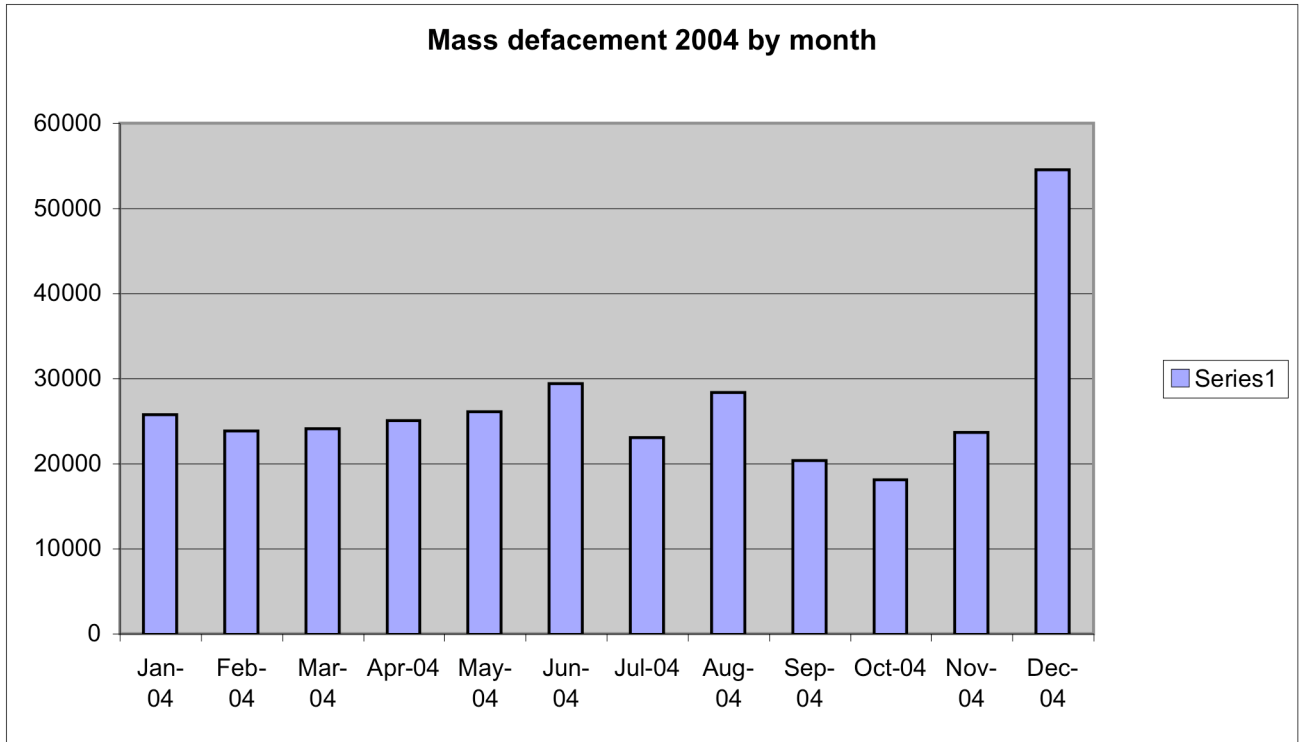
1: Time periods before July 2002 contains partial/incomplete data

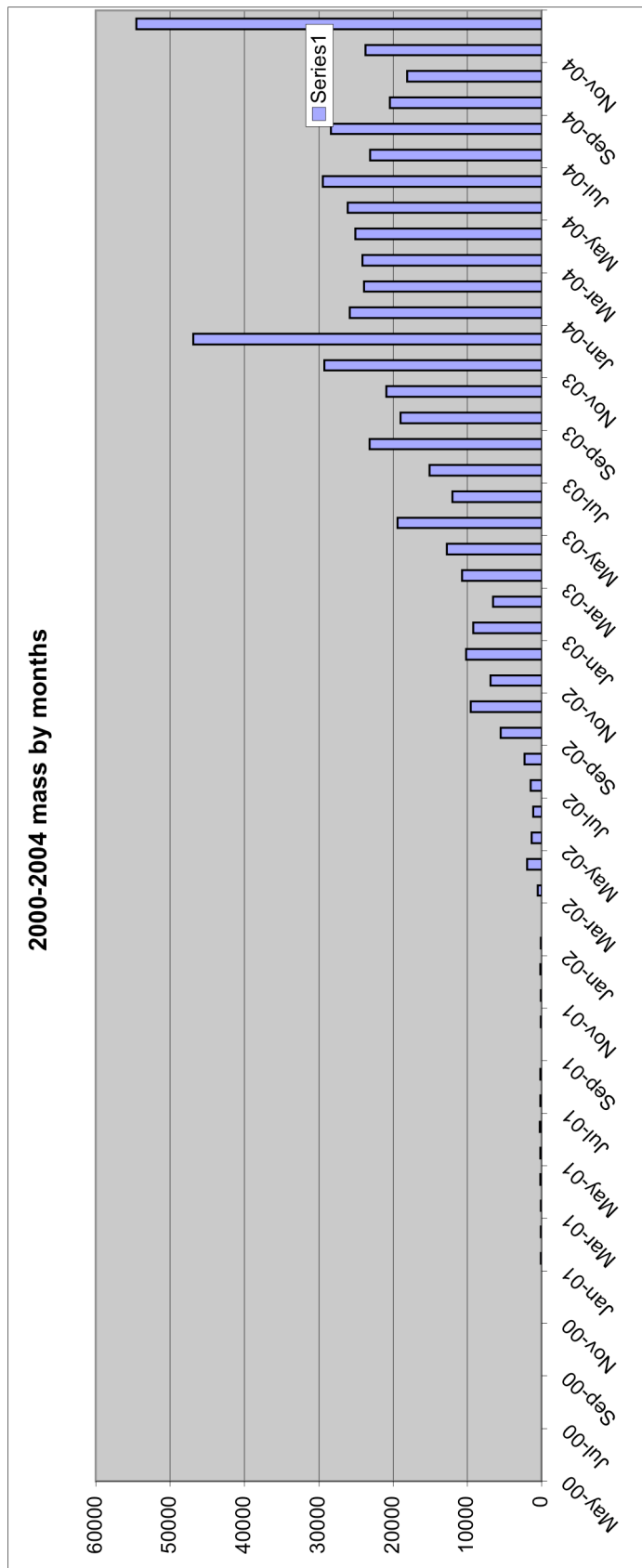
2: in-depth technical details related to exploitation level will be available for 2005 statistics

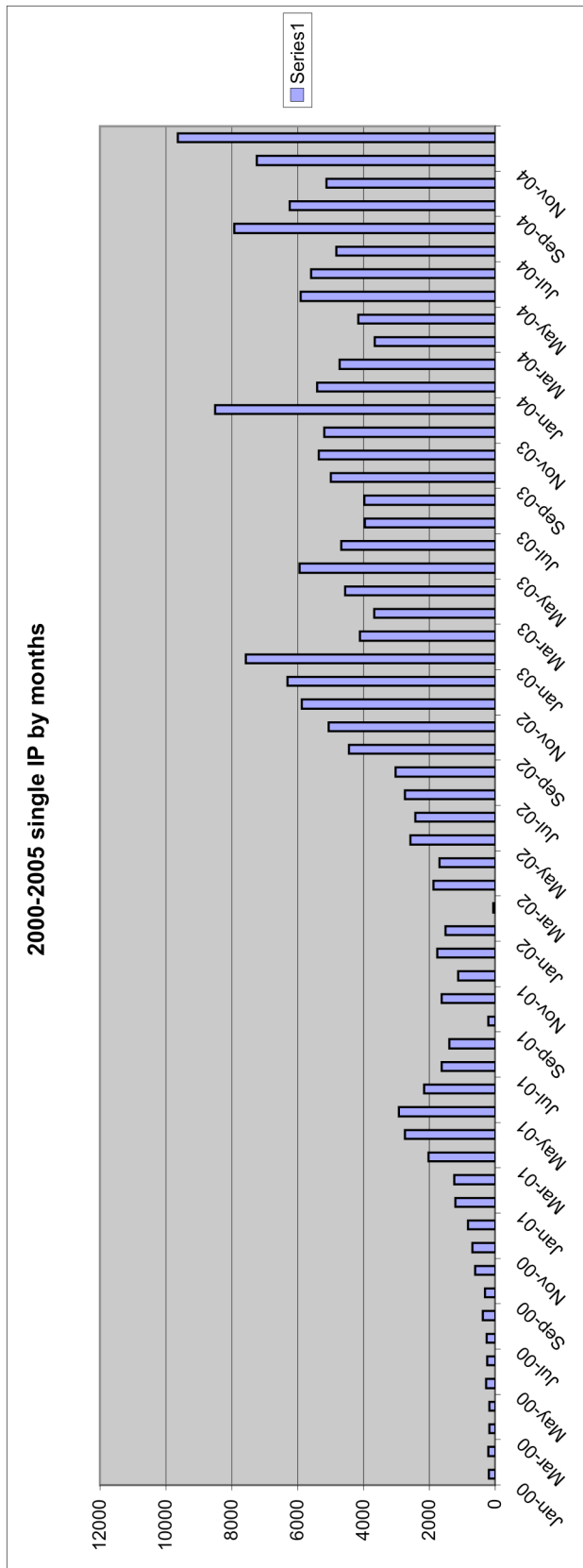
3: Single IP, is a web server that operates as a standalone server and was defaced. A mass defacement occurs when a web server (single IP) normally residing at a hosting company becomes compromised, this provides access to multiple web sites that are then defaced. For example a hosting company server becomes compromised and 1200 websites are housed on the server, which are then defaced. The Zone-H database accounts for both types the single IP and mass defacements filing 1 single IP and 1999 mass defacements

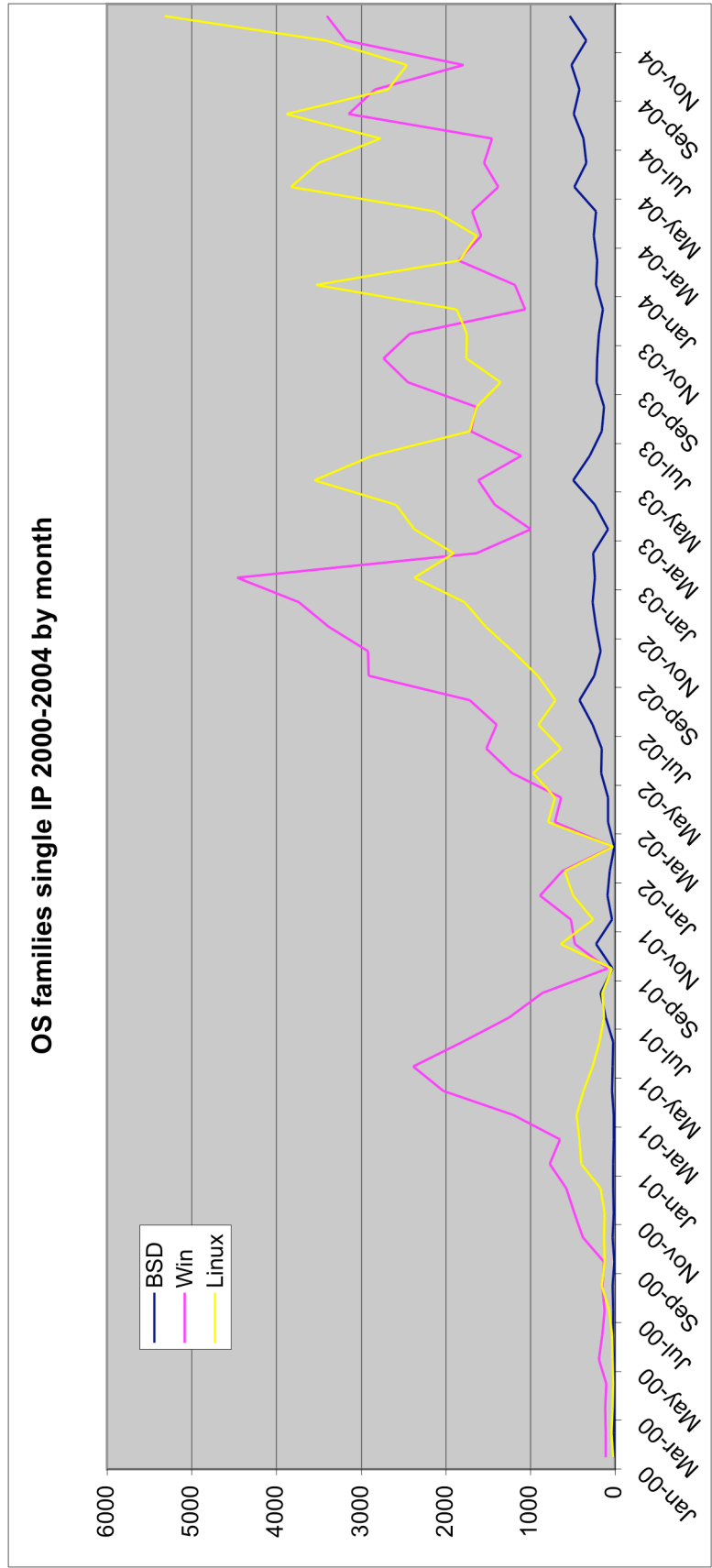


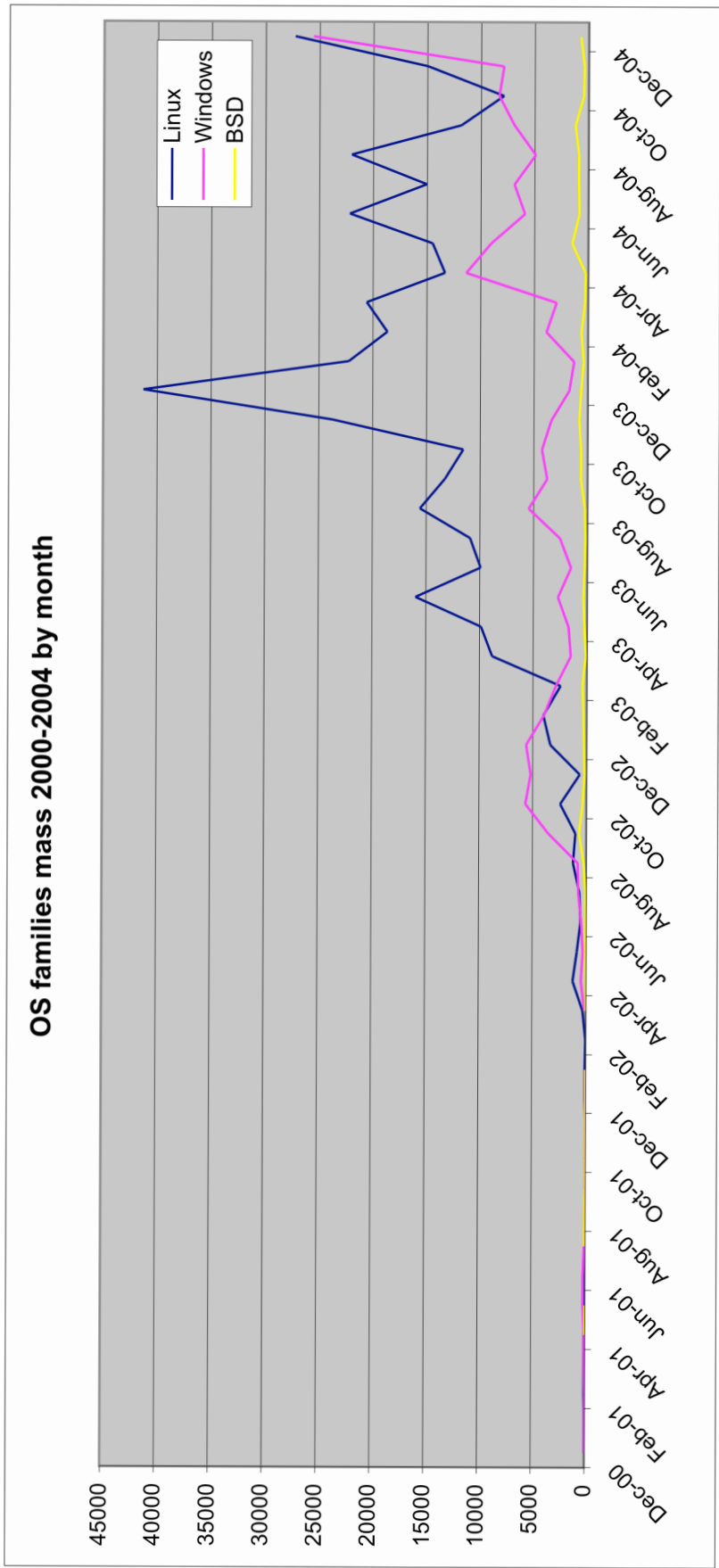


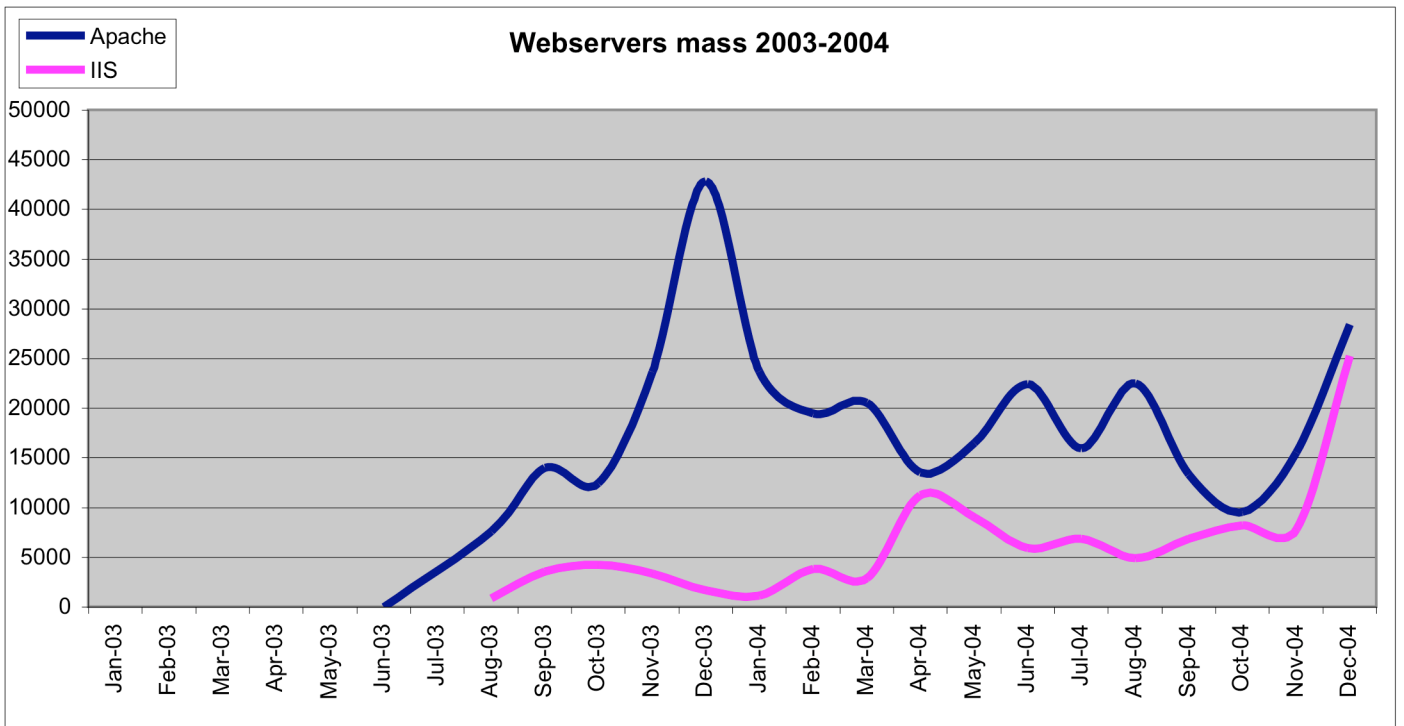
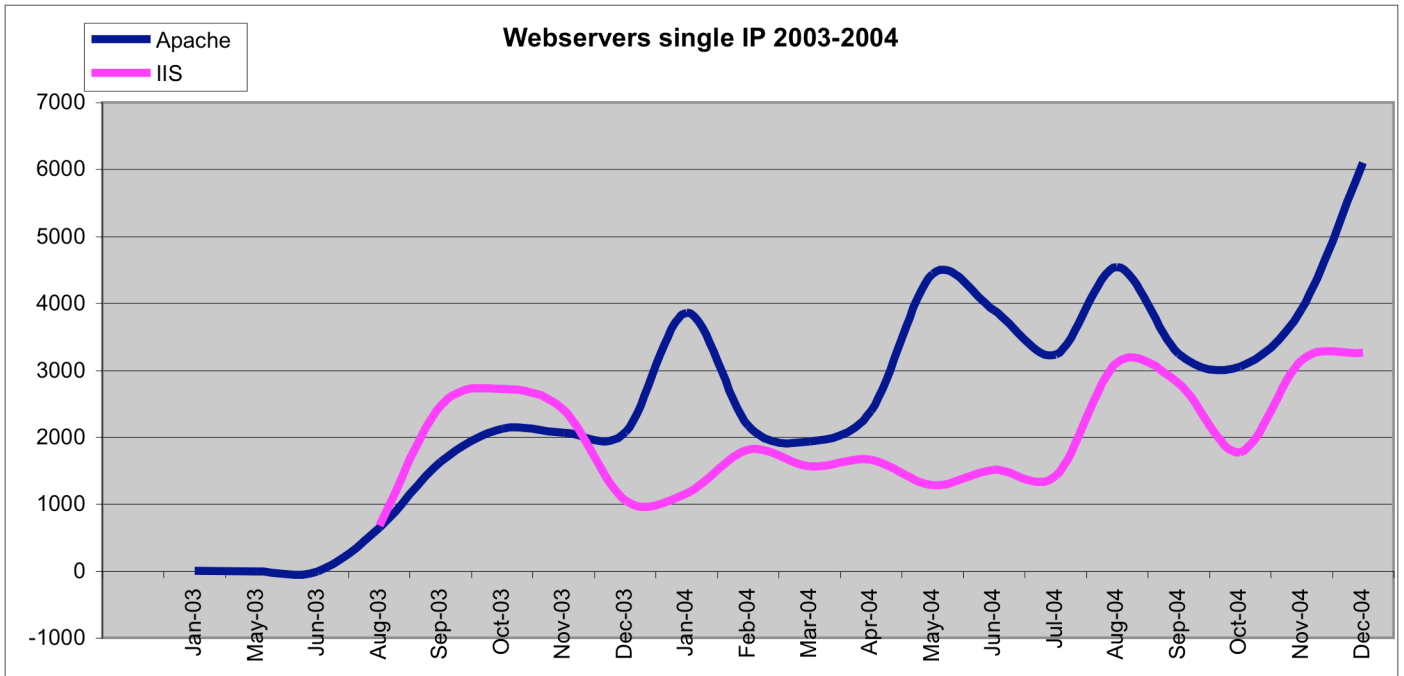


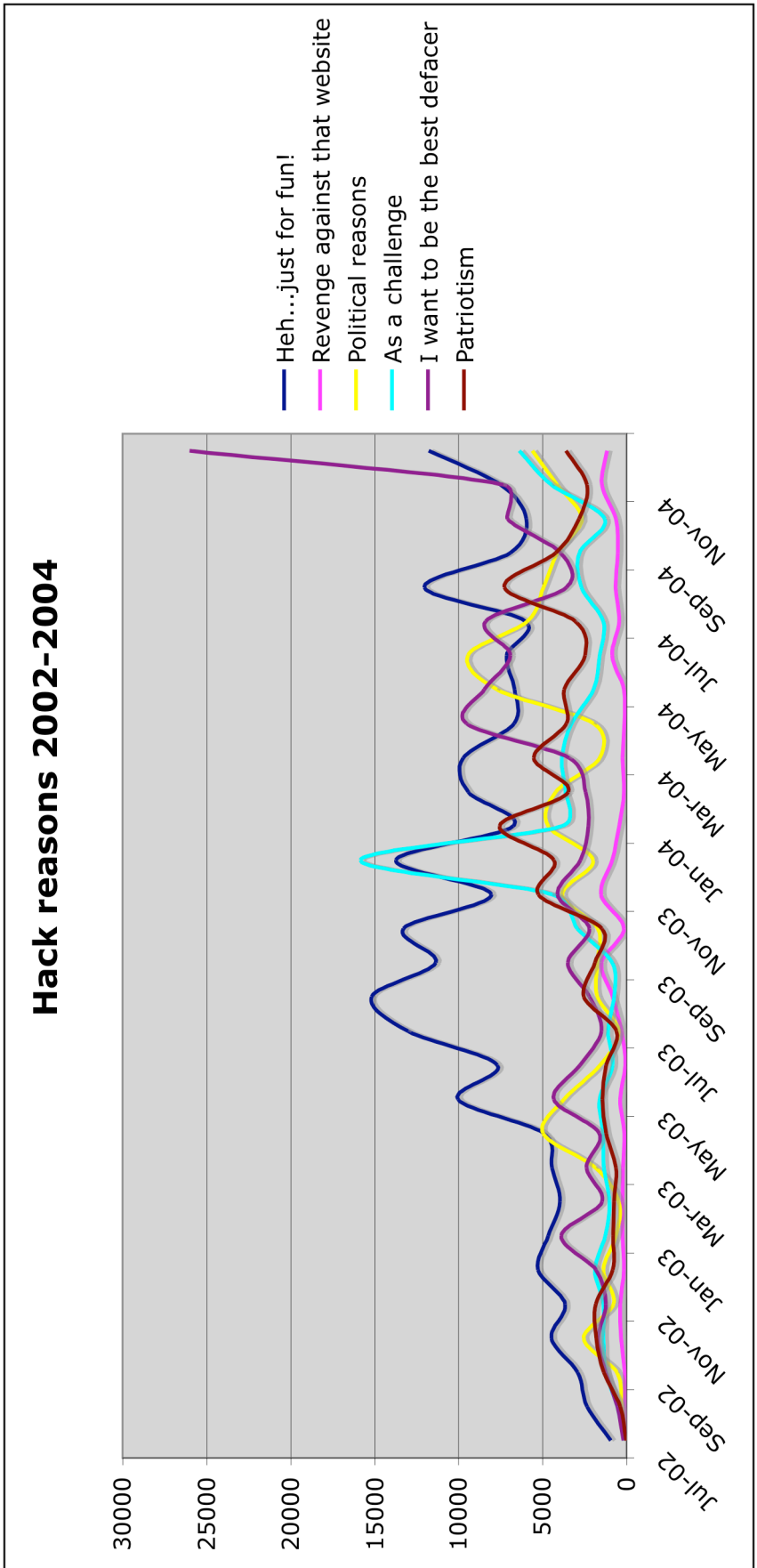


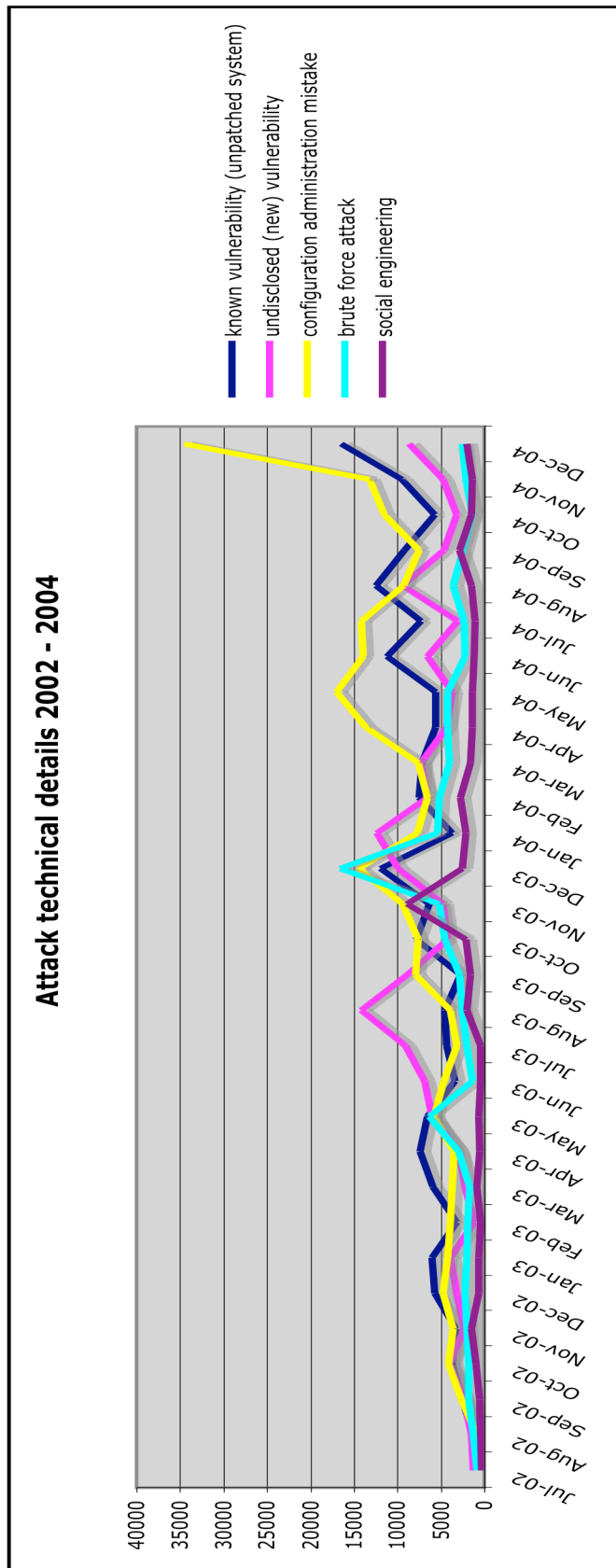














Attribution-NonCommercial-NoDerivs 2.0

You are free:

- to copy, distribute, display, and perform the work

Under the following conditions:



Attribution. You must give the original author credit.



Noncommercial. You may not use this work for commercial purposes.



No Derivative Works. You may not alter, transform, or build upon this work.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

Your fair use and other rights are in no way affected by the above.

This is a human-readable summary of the [Legal Code \(the full license\)](#).

[Disclaimer](#) 