

# [NEWS] The Slammer Worm Effect: Why Linux OS is More Attackable than Windows OS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0012.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 06/09/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 9 Jun 2003 18:34:06 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>, or call 617-399-6980

-----

The Slammer Worm Effect: Why Linux OS is More Attackable than Windows OS

---

## SUMMARY

A very interesting analysis of the amount of attacked hosts (Linux vs. Windows) has been created by Zone-H. It shows that taking into account such worms as Slammer, reveals that Linux is currently the most attacked host on the Internet.

## DETAILS

The news appeared during the last days in which London based MI2G.com stated that Linux OS is now more attacked then Windows has been reported by media and immediately criticized by the IT Security world.

MI2G is basing part of their research job relying on Zone-H.org databases therefore they based their last press release using the data Zone-H is sending to all its mail subscribers regarding the daily attacks.

## Securiteam: [NEWS] The Slammer Worm Effect: Why Linux OS is More Attackable than Windows OS

Using such data MI2G was calculating that the amount of Linux attacks has stably overcome the Windows attacks.

The direct result of Zone-H data organized in a chart graphically supporting MI2G statement is in fact showing that today Linux attacks are as 5 times higher than the Windows ones.

The IT Security world has immediately attacked MI2G statement saying that when counting the attacks MI2G accounted all the mass-defacement (an attack that while hitting a single IP or host, generates multiple defacements like it usually happens to big hosting companies) as single hits.

The Itsec purists argued that the mass-defacements should be accounted instead as 1 single hit therefore MI2G statement was either premature or inaccurate.

The only organization that has enough authority to solve the dilemma is Zone-H as today is holding the most complete database having access to direct statistics.

Therefore, today Zone-H staff started to dig in the archives filtering out all attacks by SINGLE IP divided into the different OSs.

The results that came out is clear: Linux is in effect the most attacked Operative System, and this already since middle March 2003 as you can check by this graph:

The graph is showing the attacks trend during the last 16 months.

The graph shows clearly that one of the most hit OS over the time was Windows (red line). The interesting fact is that since middle-January 2003 Windows became for some unknown reasons less attacked (and less attackable) than Linux.

Zone-H identified the reason of this strange phenomenon in what Zone-H calls the "Slammerworm effect".

In fact, the Slammer worm has produced since December 2002 a spike in the Windows 2000 statistics. Since then, the Slammer worm threat has been so much covered by the media that companies started to patch at a speed never seen before. The result of this process is that Windows OS has instantly become less attractive for crackers.

If we also consider that the number of the worldwide Windows installations is presumably higher than the Linux installation it means that a properly weighted analysis would reveal that the Linux "hacker attractiveness" would be even clearer.

The graph generated from Zone-H databases is also showing other interesting aspects: the web cracking phenomenon is transforming more and

Securiteam: [NEWS] The Slammer Worm Effect: Why Linux OS is More Attackable than Windows OS

more into a social problem very much related to political issues.

The September 11th anniversary and the Iraq war have been the reason why the overall number of attacks has increased 500%, hitting this year an amount of targets never seen before.

If anybody before was under evaluating the web-cracking events, these graphs and numbers should be the reason of paying more attention to these facts as they are more and more configuring a sociologic problem.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.zone-h.org/winvslinux>> <http://www.zone-h.org/winvslinux>

The information has been provided by SyS64738 of <<http://www.zone-h.org/>>  
<http://www.zone-h.org/>.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====  
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.