

SQL Slammer (Sapphire Worm) Frequency?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-04/msg00068.html>

- *From:* "Shawn A. Corrello" <shawnc@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 7 Apr 2008 11:40:33 -0400 (EDT)
-

My company normally sees 7-10 SQL Slammer infection attempts on a daily basis.

This morning, starting at ~6:30 AM EST (it's now 11:30 AM EST), I've logged nearly a thousand. While some of the attempts are from repeating IP addresses, most are unique.

I'm not very concerned with these infection attempts causing me problems as our servers are patched and my IDP drops them anyway. However, I'm curious as to the drastic increase in volume. Anyone else seeing this today?

Could this be controlled servers gearing up for a big DDoS (unlikely given my understanding of Slammer as a "dumb" DoS worm), or a new version of Sapphire?

-SAC