



The Aggregation Point for Snort Signatures and Research

Search

[Contribute](#) | [Web Resources](#) | [Advanced Search](#) | [Account Information](#) | [Feeds](#) | [Signature Maker](#) | [Signatures](#) | [Sponsors](#) | [Forum](#) | [My Downloads](#) |

Welcome to the Bleeding Edge of Snort

Wednesday, December 29 2004 @ 09:39 PM EST

Topics

Home
[General News](#)
[About Bleeding Snort](#)
[New Rules](#)
[Documentation](#)

Internet Storm Center

- [ISC Poll Results, Port 1433 scans](#)
- [Infocon: green](#)
- [Top Port: microsofts 445](#)
- [Fastest Rising: 1433 ms-sql-s](#)

User Functions

Username:

Password:

Don't have an account yet? Sign up as a [New User](#)

US-CERT

- [SB04-364: Summary of Security Items from December 22 through December 28, 2004](#)
- [SB04-357: Summary of Security Items from December 15 through December 21, 2004](#)
- [TA04-356A: Exploitation of phpBB highlight parameter vulnerability](#)
- [SB04-350: Summary of Security Items from December](#)

Bleeding Snort Signatures

Current Bleeding Snort Rulesets

All in one file: [Bleeding CVS Web Interface](#)
[bleeding-all.rules](#) [SPADE CVS Web Interface](#)
[bleeding.rules.tar.gz](#) [Daily Change Summary](#)
[bleeding-sid-msg-map.txt](#) [Bleeding for the Impatient](#)
Individual Rulesets [How to Submit a Signature or Idea](#)

Latest Forum Posts

Forum	Topic	Last Post
New Signatures	squ1rt Apache DoS sig	➡ 12/29/04 15:06
New Signatures	PHP outbound connection detect..	➡ 12/29/04 00:10
New Ideas	bogons	➡ 12/28/04 22:51
New Signatures	Winhelp32 Trojan Sigs	➡ 12/28/04 10:26
New Signatures	Santy Worm Sigs	➡ 12/25/04 15:31
General	Merry Christmas / Feliz Navida..	➡ 12/25/04 12:51
Tweaks to Existing Signatures	[Q] Joseph Gama's nmap -f -sN ..	➡ 12/23/04 17:50

Today's Featured Article Ruleset Rearranging

Wednesday, December 29 2004 @ 04:06 PM EST
 Contributed by: [jonkman](#)
 Views: 38

We've made some organizational moves to the rulesets. The Scan, DOS, EXPLOIT, ATTACK RESPONSE, and WEB rules are now in their own rulesets. There were enough of each to justify it for roganizational reasons.



What this means to you:

What's New

STORIES

[1 story in last 24 hours](#)

COMMENTS last 48 hrs

- [Ruleset Rearranging](#) [+2]

LINKS last 2 wks

- [TLD's by Country](#)

Forumposts

Order By: [New](#) [Views](#) [Posts](#)
 Latest 5 Forum Posts

- [squ1rt Apache DoS ..](#)
 By: [nnachefski](#)
 On: 12/29/04 15:06 PM
 Views 36 Replies 2
- [PHP outbound conne..](#)
 By: [cooljay](#)
 On: 12/29/04 00:10 AM
 Views 151 Replies 8
- [bogons](#)
 By: [emf](#)
 On: 12/28/04 22:49 PM
 Views 238 Replies 7
- [Winhelp32 Trojan S..](#)
 By: [jonkman](#)
 On: 12/28/04 10:26 AM
 Views 185 Replies 2
- [Santy Worm Sigs](#)
 By: [jonkman](#)
 On: 12/25/04 15:30 PM
 Views 423 Replies 4

BOFH

- [BOFH gets into the Xmas spirit](#)
- [BOFH and the serial killer](#)
- [BOFH: Et tu, PFY-us?](#)
- [Introducing the big, bad BOFH polo shirt](#)
- [BOFH: The hostage's guide to lift imprisonment](#)
- [BOFH: A little Ray of sunshine](#)

[8 through December 14, 2004](#)

- [ST04-024: Understanding ISPs](#)
- [SB04-343: Summary of Security Items from December 1 through December 7, 2004](#)
- [SA04-336A: Update for Microsoft Internet Explorer](#)
- [TA04-336A: Update for Microsoft Internet Explorer HTML Elements Vulnerability](#)
- [SB04-336: Summary of Security Items from November 24 through November 30, 2004](#)
- [ST04-023: Understanding Your Computer: Email Clients](#)

If you're not just using the bleeding-all ruleset you need to add the following to your snort.conf...

[read more](#) (42 words) [2 comments](#)  
Most Recent Post: 12/29 06:37PM by jonkman

Thanks to Incidents.org

Monday, December 27 2004 @ 05:04 PM EST

Contributed by: [jonkman](#)

Views: 39

Incidents.org mentioned the Bleeding Snort community as being a great contributor to their investigations this year in today's diary entry: <http://isc.sans.org/diary.php?date=2004-12-26>



We'd like to thank the ISC for their efforts. A lot of the signatures we have are due to their work. If you have the opportunity we encourage you to support that organization through their excellent training programs and the like.

More...

[read more](#) (280 words) [0 comments](#)  
[Post a comment](#)

Trojan Active that Exploits Unpatched XPSP2 Vulnerabilities

Monday, December 27 2004 @ 01:47 PM EST

Contributed by: [jonkman](#)

Views: 192

A worm has been identified in the wild that exploits the previously mentioned vulnerabilities in Internet Explorer/XP SP2. There is no patch, these vulnerabilities have been known for a long time and remain unpatched. Your only protection is to not use IE. More...



[read more](#) (95 words) [0 comments](#)  
[Post a comment](#)

Santy.B On the Loose Using AOL/Yahoo Search

Saturday, December 25 2004 @ 12:40 PM EST

Contributed by: [jonkman](#)

Views: 86

One of a couple variants of Santy (the PhpBB worm) is using AOL and Yahoo to search. Another as mentioned at Incidents.org is setting up a command connection to an IRC channel.



[read more](#) (39 words) [1 comments](#)  
Most Recent Post: 12/25 03:20PM by jonkman

Working SPADE/Snort 2.3.0RC2 Tarball Available.

Tuesday, December 21 2004 @ 01:15 AM EST

Contributed by: [jonkman](#)

Views: 147

Steve Donegan has sent us a compilable tarball with spade integrated into snort 2.3.0RC2. This represents a good deal of work on Steve's part, many thanks.



[read more](#) (91 words) [0 comments](#)  
[Post a comment](#)

- [BOFH: When sorry seems to be the hardest word](#)
- [BOFH: How to survive a Boring Geek Alert](#)
- [The BOFH mobile comms quiz](#)
- [BOFH: Seek, locate and destroy](#)
- [BOFH: A ringside seat at the Boss-baiting pit](#)
- [BOFH tests the law of redundant supply](#)
- [BOFH 2004: The whole shooting match](#)
- [BOFH: What to do when the Boss gets touchy-feely](#)
- [PFY proves self abuse cures male-pattern baldness](#)

Security Tracker

- [QNX crtttrap '-c' Lets Local Users Read or Write Arbitrary Files](#)
- [Moodle 'file.php' Discloses Session ID Files and 'view.php' Permits Cross-Site Scripting Attacks](#)
- [Owl Intranet Engine Has Unspecified Input Validation Holes That Permit SQL Injection and Cross-Site Scripting Attacks](#)
- [PHProjekt 'authform.inc.php' Include File Flaw Lets Remote Users Execute Arbitrary Command](#)
- [WHM AutoPilot 'server.inc' Include File Flaw Lets Remote Users Execute Arbitrary Commands](#)

Sophos Virus Alerts

- [29 Dec W32/Leebad-B](#)
- [29 Dec W32/Dedler-H](#)
- [28 Dec W32/Forbot-DH](#)
- [27 Dec Perl/Santy-Fam](#)
- [24 Dec Troj/Agent-ZC](#)
- [24 Dec Troj/Bancos-AS](#)
- [23 Dec Troj/Multidr-BG](#)
- [23 Dec W32/Rembot-A](#)
- [23 Dec W32/Rbot-SD](#)
- [22 Dec W32/Agobot-OR](#)
- [Source: Sophos](#)

WindowsSecurity.com

- [Happy Holidays from WindowSecurity.com!](#)
- [Quick Check: Is Internet Explorer Safe?](#)

CVS Updates Available via RSS**Sunday, December 19 2004 @ 11:50 AM EST****Contributed by: jonkman****Views: 86**

By request we've made the CVS changes available via RSS Feed. The rss feed will be updated with each push made into the new rulesets.



We think this will solve the issue of getting timely updates of rule changes without making a mailing list that'd be just too much traffic.

We've also as a side note added a text Changelog for review.

[read more](#) (42 words) [0 comments](#)
[Post a comment](#)

- [Enforcing GPO Security Settings](#)
- [Web Server Security Issues and Front Page Server Extensions](#)
- [Is it Time to Start Encrypting Your E-mail?](#)
- [Windows Server 2003 Hardening List \(Part 1\)](#)
- [Social Engineering meets the Bot \(Part 3\) - All is Revealed](#)
- [Windows Update Services Review](#)

Honeynet Security Console 1.2 Released**Thursday, December 16 2004 @ 10:48 AM EST****Contributed by: Jeff Dell****Views: 147**

Honeynet Security Console is a free analysis tool to view events on your personal network or honeynet. It gives you the power to view events from Snort, TCPDump, Firewall, Syslog and Sebek logs. It also allows you to correlate events between each of these data types to have a full view of the attackers' actions.



[read more](#) (8 words) [0 comments](#)
[Post a comment](#)

ISC Needs Your Help!!**Saturday, December 11 2004 @ 12:16 AM EST****Contributed by: jonkman****Views: 310**

The intrepid Incident Handlers at <http://isc.sans.org> are on the trail of the recent UDP strangeness noted in the last couple days Diary Entries.



<http://isc.sans.org/diary.php?date=2004-12-10>

Erik Fichtner put great effort into writing signatures to detect this very complex traffic they're investigating. They've asked that we distribute these rules and ask that you report the details of any hits.

[read more](#) (61 words) [1 comments](#)
Most Recent Post: 12/14 09:22AM by jonkman

Vulnerability in All Major Browsers**Wednesday, December 08 2004 @ 10:59 PM EST****Contributed by: jonkman****Views: 215**

Yes, "All" includes the free browsers as well. The vulnerability is a popup window injection issue. These have never been considered that much of a threat by the security community because the attacker has to know something about where you're going to be browsing, and have their page open at the same time or get you to follow link on their page.



This is a very interesting set of issues for other reasons. Those reasons and a link to a demonstration:

[read more](#) (252 words) [0 comments](#)  
[Post a comment](#)

Snort Installation Guide with BASE and MySQL

Wednesday, December 08 2004 @ 08:38 PM EST

Contributed by: [jonkman](#)

Views: 281

Ghaith Nasrawi has just posted a very detailed and useful installation guide to get you going with BASE and snort on Mysql. Very useful if you're trying to get into the IDS arena and need a little push.



[read more](#) (48 words) [0 comments](#)  
[Post a comment](#)

[First](#) | [Previous](#) | [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) | [Next](#) | [Last](#)

Copyright © 2004 the Bleeding Edge of Snort
All trademarks and copyrights on this page are owned by their respective owners.

Thanks to [infotex!](#) for providing the material resources to maintain this project. <http://www.infotex.com>

All content released under the [BSD License](#)
Created this page in 0.25 seconds