

[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

List: [bleeding-sigs](#)
Subject: [Bleeding-sigs] New SSL/TLS State Machine
From: [Matt Jonkman <matt \(\) infotex ! com>](#)
Date: [2006-07-05 14:54:25](#)
Message-ID: [1152111265.5260.17.camel \(\) bob ! infotex ! com](#)
[Download RAW [message](#) or [body](#)]

Have a working string of sigs to identify a good ssl or tls session. They're targeted now at high ports, over 8081. The impetus to create this was a new bot that's using standard ssl for a command and control session on a high port. This catches that.

If you're running ssl apps on high ports a suppress statement for the first sigs in the chain, or the data sigs at the end will quiet it down for you.

See the sigs here:

http://www.bleedingsnort.com/cgi-bin/viewcvs.cgi/sigs/POLICY/POLICY_SSL_TLS_on_High_Port?view=markup

Please let me know if you can run sessions without these tripping. It's set to get sslv2, sslv3, and most tls implementations. I'm sure there's more than that to catch.

Matt

--

Matthew Jonkman, CISSP
Senior Security Engineer / CTO
Infotex
765-429-0398 Direct Anytime
866-679-5177 24x7 NOC
my.infotex.com
[www.offsitefilter.com](#)
[www.bleedingsnort.com](#)

Bleeding-sigs mailing list
Bleeding-sigs@bleedingsnort.com
<http://lists.bleedingsnort.com/mailman/listinfo/bleeding-sigs>
[\[prev in list\]](#) [\[next in list\]](#) [\[prev in thread\]](#) [\[next in thread\]](#)

[Configure](#) | [About](#) | [News](#) | [Add a list](#) | Sponsored by [KoreLogic](#)