

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

List: [bleeding-sigs](#)
 Subject: [Re: \[Bleeding-sigs\] BLEEDING-EDGE POLICY TLS/SSL Encrypted Application](#)
 From: [Matt Jonkman <jonkman \(\) bleedingthreats ! net>](#)
 Date: [2007-05-28 21:28:41](#)
 Message-ID: [465B4989.9060502 \(\) bleedingthreats ! net](#)
 [Download RAW [message](#) or [body](#)]

Good point, thanks for bringing it up.

I've added an exclusion rule for that:

```
alert tcp any any -> any 1521 (msg:"BLEEDING-EDGE POLICY Known SSL
traffic on port 1521 (Oracle) being excluded from SSL Alerts";
flow:established,to_server; flowbits:noalert;
flowbits:set,BS.SSL.Known.Port; classtype:not-suspicious; sid:2003934;
rev:1;)
```

Matt

Michael Scheidell wrote:

```
>
> 05/28-10:24:52 TCP 10.200.40.222:49996
> <https://success-ae.hackertrap.net/base/base\_stat\_ipaddr.php?ip=10.200.40.222>
> --> 10.200.199.21:1521
> <https://success-ae.hackertrap.net/base/base\_stat\_ipaddr.php?ip=10.200.199.21>
>
> [1:2003021:5] <http://www.snort.org/pub-bin/sigs.cgi?sid=2003021>
> BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual Port
> SSLv3
> [Classification: A client was using an unusual port] [Priority: 2]
>
> port 1521 is not really unusual for ssl. it is the encrypted version
> for oracle.
>
>
> This email has been scanned and certified safe by SpammerTrap(tm). For
> Information please see http://www.spammertrap.com
>
>
> Bleeding-sigs mailing list
> Bleeding-sigs@bleedingthreats.net
> http://lists.bleedingthreats.net/cgi-bin/mailman/listinfo/bleeding-sigs
```

--

 Matthew Jonkman
 Bleeding Edge Threats
 765-429-0398
<http://www.bleedingthreats.net>

PGP: <http://www.bleedingthreats.com/mattjonkman.asc>

 Bleeding-sigs mailing list
 Bleeding-sigs@bleedingthreats.net
<http://lists.bleedingthreats.net/cgi-bin/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](#)