

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

List: [bleeding-sigs](#)
 Subject: [\[Bleeding-sigs\] Bleeding Snort Daily Signature Changes](#)
 From: [bleeding \(\) bleedingsnort ! com](#)
 Date: [2006-07-10 1:00:08](#)
 Message-ID: [20060710010008.5207755026A \(\) gort ! offsitefilter ! com](#)
[\[Download RAW message or body\]](#)

[***] Results from Oinkmaster started Sun Jul 9 21:00:08 2006 [***]

[+++] Added rules: [+++]

2003026 - BLEEDING-EDGE POLICY Known SSL traffic on port 443 being excluded from SSL \ Alerts (bleeding-policy.rules) 2003027 - BLEEDING-EDGE POLICY Known SSL traffic on \ port 8000 being excluded from SSL Alerts (bleeding-policy.rules) 2003028 - \ BLEEDING-EDGE POLICY Known SSL traffic on port 8080 being excluded from SSL Alerts \ (bleeding-policy.rules) 2003029 - BLEEDING-EDGE POLICY Known SSL traffic on port \ 8200 being excluded from SSL Alerts (bleeding-policy.rules) 2003030 - BLEEDING-EDGE \ POLICY Known SSL traffic on port 8443 being excluded from SSL Alerts \ (bleeding-policy.rules) 2003031 - BLEEDING-EDGE POLICY Known SSL traffic on port \ 5222 (Jabber) being excluded from SSL Alerts (bleeding-policy.rules) 2003032 - \ BLEEDING-EDGE POLICY Known SSL traffic on port 5223 (Jabber) being excluded from SSL \ Alerts (bleeding-policy.rules)

[////] Modified active rules: [////]

2003002 - BLEEDING-EDGE POLICY TLS/SSL Client Hello on Unusual Port TLS \ (bleeding-policy.rules) 2003003 - BLEEDING-EDGE POLICY TLS/SSL Client Hello on \ Unusual Port SSLv3 (bleeding-policy.rules) 2003004 - BLEEDING-EDGE POLICY TLS/SSL \ Client Hello on Unusual Port Case 2 (bleeding-policy.rules) 2003005 - BLEEDING-EDGE \ POLICY TLS/SSL Client Hello on Unusual Port SSLv3 (bleeding-policy.rules) 2003006 - \ BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange on Unusual Port \ (bleeding-policy.rules) 2003007 - BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange \ on Unusual Port SSLv3 (bleeding-policy.rules) 2003008 - BLEEDING-EDGE POLICY TLS/SSL \ Client Cipher Set on Unusual Port (bleeding-policy.rules) 2003009 - BLEEDING-EDGE \ POLICY TLS/SSL Client Cipher Set on Unusual Port SSLv3 (bleeding-policy.rules) \ 2003010 - BLEEDING-EDGE POLICY TLS/SSL Server Hello on Unusual Port \ (bleeding-policy.rules) 2003011 - BLEEDING-EDGE POLICY TLS/SSL Server Hello on \ Unusual Port SSLv3 (bleeding-policy.rules) 2003012 - BLEEDING-EDGE POLICY TLS/SSL \ Server Certificate Exchange on Unusual Port (bleeding-policy.rules) 2003013 - \ BLEEDING-EDGE POLICY TLS/SSL Server Certificate Exchange on Unusual Port SSLv3 \ (bleeding-policy.rules) 2003014 - BLEEDING-EDGE POLICY TLS/SSL Server Key Exchange \ on Unusual Port (bleeding-policy.rules) 2003015 - BLEEDING-EDGE POLICY TLS/SSL \ Server Key Exchange on Unusual Port SSLv3 (bleeding-policy.rules) 2003016 - \ BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on Unusual Port \ (bleeding-policy.rules) 2003017 - BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on \ Unusual Port SSLv3 (bleeding-policy.rules) 2003018 - BLEEDING-EDGE POLICY TLS/SSL \ Server Cipher Set on Unusual Port (bleeding-policy.rules) 2003019 - BLEEDING-EDGE \ POLICY TLS/SSL Server Cipher Set on Unusual Port SSLv3 (bleeding-policy.rules) \ 2003020 - BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual Port \ (bleeding-policy.rules) 2003021 - BLEEDING-EDGE POLICY TLS/SSL Encrypted Application \ Data on Unusual Port SSLv3 (bleeding-policy.rules) 2400000 - BLEEDING-EDGE DROP \ Spamhaus DROP Listed Traffic Inbound (bleeding-drop.rules) 2400001 - BLEEDING-EDGE \ DROP Spamhaus DROP Listed Traffic Inbound (bleeding-drop.rules) 2400002 - \ BLEEDING-EDGE DROP Spamhaus DROP Listed Traffic Inbound (bleeding-drop.rules) \ 2400003 - BLEEDING-EDGE DROP Spamhaus DROP Listed Traffic Inbound \ (bleeding-drop.rules) 2400004 - BLEEDING-EDGE DROP Spamhaus DROP Listed Traffic \

```
Inbound (bleeding-drop.rules) 2401000 - BLEEDING-EDGE DROP Spamhaus DROP Listed \
Traffic Inbound - BLOCKING SOURCE (bleeding-drop-BLOCK.rules) 2401001 - \
BLEEDING-EDGE DROP Spamhaus DROP Listed Traffic Inbound - BLOCKING SOURCE \
(bleeding-drop-BLOCK.rules) 2401002 - BLEEDING-EDGE DROP Spamhaus DROP Listed \
Traffic Inbound - BLOCKING SOURCE (bleeding-drop-BLOCK.rules) 2401003 - \
BLEEDING-EDGE DROP Spamhaus DROP Listed Traffic Inbound - BLOCKING SOURCE \
(bleeding-drop-BLOCK.rules) 2401004 - BLEEDING-EDGE DROP Spamhaus DROP Listed \
Traffic Inbound - BLOCKING SOURCE (bleeding-drop-BLOCK.rules)
```

[+++] Added non-rule lines: [+++]

-> Added to bleeding-policy.rules (3):

```
#Adding these sigs to prevent known ssl ports from being included. You may \
need to duplicate some of these # to exclude known ssl traffic in your environment.
# You can also avoid falses by suppressing sigs 2003002-5 for the hosts that \
you expect unusual port SSL to/from
```

-> Added to bleeding-sid-msg.map (27):

```
2003002 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on Unusual Port TLS
2003003 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on Unusual Port SSLv3
2003004 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on Unusual Port Case 2
2003005 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on Unusual Port SSLv3
2003006 || BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange on Unusual Port
2003007 || BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange on Unusual Port \
SSLv3
2003008 || BLEEDING-EDGE POLICY TLS/SSL Client Cipher Set on Unusual Port
2003009 || BLEEDING-EDGE POLICY TLS/SSL Client Cipher Set on Unusual Port \
SSLv3
2003010 || BLEEDING-EDGE POLICY TLS/SSL Server Hello on Unusual Port
2003011 || BLEEDING-EDGE POLICY TLS/SSL Server Hello on Unusual Port SSLv3
2003012 || BLEEDING-EDGE POLICY TLS/SSL Server Certificate Exchange on \
Unusual Port
2003013 || BLEEDING-EDGE POLICY TLS/SSL Server Certificate Exchange on \
Unusual Port SSLv3
2003014 || BLEEDING-EDGE POLICY TLS/SSL Server Key Exchange on Unusual Port
2003015 || BLEEDING-EDGE POLICY TLS/SSL Server Key Exchange on Unusual Port \
SSLv3
2003016 || BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on Unusual Port
2003017 || BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on Unusual Port \
SSLv3
2003018 || BLEEDING-EDGE POLICY TLS/SSL Server Cipher Set on Unusual Port
2003019 || BLEEDING-EDGE POLICY TLS/SSL Server Cipher Set on Unusual Port \
SSLv3
2003020 || BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual \
Port
2003021 || BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on Unusual \
Port SSLv3
2003026 || BLEEDING-EDGE POLICY Known SSL traffic on port 443 being excluded \
from SSL Alerts
2003027 || BLEEDING-EDGE POLICY Known SSL traffic on port 8000 being excluded \
from SSL Alerts
2003028 || BLEEDING-EDGE POLICY Known SSL traffic on port 8080 being excluded \
from SSL Alerts
2003029 || BLEEDING-EDGE POLICY Known SSL traffic on port 8200 being excluded \
from SSL Alerts
2003030 || BLEEDING-EDGE POLICY Known SSL traffic on port 8443 being excluded \
from SSL Alerts
2003031 || BLEEDING-EDGE POLICY Known SSL traffic on port 5222 (Jabber) being \
excluded from SSL Alerts
2003032 || BLEEDING-EDGE POLICY Known SSL traffic on port 5223 (Jabber) being \
excluded from SSL Alerts
```

[---] Removed non-rule lines: [---]

-> Removed from bleeding-sid-msg.map (20):

```

2003002 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on High Port TLS
2003003 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on High Port SSLv3
2003004 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on High Port Case 2
2003005 || BLEEDING-EDGE POLICY TLS/SSL Client Hello on High Port SSLv3
2003006 || BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange on High Port
2003007 || BLEEDING-EDGE POLICY TLS/SSL Client Key Exchange on High Port \
        SSLv3
2003008 || BLEEDING-EDGE POLICY TLS/SSL Client Cipher Set on High Port
2003009 || BLEEDING-EDGE POLICY TLS/SSL Client Cipher Set on High Port SSLv3
2003010 || BLEEDING-EDGE POLICY TLS/SSL Server Hello on High Port
2003011 || BLEEDING-EDGE POLICY TLS/SSL Server Hello on High Port SSLv3
2003012 || BLEEDING-EDGE POLICY TLS/SSL Server Certificate Exchange on High \
        Port
2003013 || BLEEDING-EDGE POLICY TLS/SSL Server Certificate Exchange on High \
        Port SSLv3
2003014 || BLEEDING-EDGE POLICY TLS/SSL Server Key Exchange on High Port
2003015 || BLEEDING-EDGE POLICY TLS/SSL Server Key Exchange on High Port \
        SSLv3
2003016 || BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on High Port
2003017 || BLEEDING-EDGE POLICY TLS/SSL Server Hello Done on High Port SSLv3
2003018 || BLEEDING-EDGE POLICY TLS/SSL Server Cipher Set on High Port
2003019 || BLEEDING-EDGE POLICY TLS/SSL Server Cipher Set on High Port SSLv3
2003020 || BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on High \
        Port
2003021 || BLEEDING-EDGE POLICY TLS/SSL Encrypted Application Data on High \
Port SSLv3

```

Bleeding-signs mailing list

Bleeding-signs@bleedingsnort.com

<http://lists.bleedingsnort.com/mailman/listinfo/bleeding-signs>

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

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