

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

List: [bleeding-signs](#)
 Subject: [\[Bleeding-signs\] Bleeding Snort Daily Signature Changes](#)
 From: [bleeding \(\) bleedingsnort ! com](#)
 Date: [2006-07-06 1:00:11](#)
 Message-ID: [20060706010011.2EFC55502A3 \(\) gort ! offsitefilter ! com](#)
[\[Download RAW message or body\]](#)

[***] Results from Oinkmaster started Wed Jul 5 21:00:11 2006 [***]

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

2002682 - BLEEDING-EDGE CURRENT EVENTS Microsoft Internet Explorer Window() Possible \ Code Execution (bleeding-exploit.rules) 2003001 - BLEEDING-EDGE TROJAN Unknown \ Trojan Communication (bleeding.rules) 2003002 - BLEEDING-EDGE TROJAN TLS/SSL Client \ Hello on High Port TLS (bleeding-policy.rules) 2003003 - BLEEDING-EDGE TROJAN \ TLS/SSL Client Hello on High Port SSLv3 (bleeding-policy.rules) 2003004 - \ BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port Case 2 (bleeding-policy.rules) \ 2003005 - BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port SSLv3 \ (bleeding-policy.rules) 2003006 - BLEEDING-EDGE TROJAN TLS/SSL Client Key Exchange \ on High Port (bleeding-policy.rules) 2003007 - BLEEDING-EDGE TROJAN TLS/SSL Client \ Key Exchange on High Port SSLv3 (bleeding-policy.rules) 2003008 - BLEEDING-EDGE \ TROJAN TLS/SSL Client Cipher Set on High Port (bleeding-policy.rules) 2003009 - \ BLEEDING-EDGE TROJAN TLS/SSL Client Cipher Set on High Port SSLv3 \ (bleeding-policy.rules) 2003010 - BLEEDING-EDGE TROJAN TLS/SSL Server Hello on High \ Port (bleeding-policy.rules) 2003011 - BLEEDING-EDGE TROJAN TLS/SSL Server Hello on \ High Port SSLv3 (bleeding-policy.rules) 2003012 - BLEEDING-EDGE TROJAN TLS/SSL \ Server Certificate Exchange on High Port (bleeding-policy.rules) 2003013 - \ BLEEDING-EDGE TROJAN TLS/SSL Server Certificate Exchange on High Port SSLv3 \ (bleeding-policy.rules) 2003014 - BLEEDING-EDGE TROJAN TLS/SSL Server Key Exchange \ on High Port (bleeding-policy.rules) 2003015 - BLEEDING-EDGE TROJAN TLS/SSL Server \ Key Exchange on High Port SSLv3 (bleeding-policy.rules) 2003016 - BLEEDING-EDGE \ TROJAN TLS/SSL Server Hello Done on High Port (bleeding-policy.rules) 2003017 - \ BLEEDING-EDGE TROJAN TLS/SSL Server Hello Done on High Port SSLv3 \ (bleeding-policy.rules) 2003018 - BLEEDING-EDGE TROJAN TLS/SSL Server Cipher Set on \ High Port (bleeding-policy.rules) 2003019 - BLEEDING-EDGE TROJAN TLS/SSL Server \ Cipher Set on High Port SSLv3 (bleeding-policy.rules) 2003020 - BLEEDING-EDGE TROJAN \ TLS/SSL Encrypted Application Data on High Port (bleeding-policy.rules) 2003021 - \ BLEEDING-EDGE TROJAN TLS/SSL Encrypted Application Data on High Port SSLv3 \ (bleeding-policy.rules)

[///] Modified active 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) 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)

[---] Removed rules: [---]

```

2002189 - BLEEDING-EDGE Current Events OSA4.GIF Detected Possible Trojan.Tooso \
Infection (bleeding.rules) 2002378 - BLEEDING-EDGE CURRENT Hostile Javascript \
s_ta_ts.js Requested (bleeding.rules) 2002682 - BLEEDING-EDGE CURRENT EVENTS \
Microsoft Internet Explorer Window() Possible Code Execution (bleeding.rules) \
2002747 - BLEEDING-EDGE CURRENT Possible Phishing URL Retrieved (bleeding.rules) \
2002884 - BLEEDING-EDGE CURRENT Possible W32.Nugache P2P Botnet Communication INBOUND \
(bleeding.rules) 2002885 - BLEEDING-EDGE CURRENT Possible W32.Nugache P2P Botnet \
Communication OUTBOUND (bleeding.rules) 2002890 - BLEEDING-EDGE CURRENT Possible \
W32.Nugache P2P Botnet Communication OUTBOUND Initial Packet (bleeding.rules) \
2002891 - BLEEDING-EDGE CURRENT Possible W32.Nugache P2P Botnet Communication INBOUND \
Initial Packet (bleeding.rules)

```

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

-> Added to bleeding-policy.rules (10):

```

#by matt Jonkman
#TLS/SSL State Machine for 8081 and up
#if you have sessions that do NOT trip this please let me know.
#I only know this will work for sslv2, sslv3, and most TLS.
#Client Hello
#Client Key exch and setup
#Server Hello
#Server cert and key exchange
#Server Cipher set
#Application data stream

```

-> Added to bleeding-sid-msg.map (21):

```

2003001 || BLEEDING-EDGE TROJAN Unknown Trojan Communication
2003002 || BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port TLS
2003003 || BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port SSLv3
2003004 || BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port Case 2
2003005 || BLEEDING-EDGE TROJAN TLS/SSL Client Hello on High Port SSLv3
2003006 || BLEEDING-EDGE TROJAN TLS/SSL Client Key Exchange on High Port
2003007 || BLEEDING-EDGE TROJAN TLS/SSL Client Key Exchange on High Port \
SSLv3
2003008 || BLEEDING-EDGE TROJAN TLS/SSL Client Cipher Set on High Port
2003009 || BLEEDING-EDGE TROJAN TLS/SSL Client Cipher Set on High Port SSLv3
2003010 || BLEEDING-EDGE TROJAN TLS/SSL Server Hello on High Port
2003011 || BLEEDING-EDGE TROJAN TLS/SSL Server Hello on High Port SSLv3
2003012 || BLEEDING-EDGE TROJAN TLS/SSL Server Certificate Exchange on High \
Port
2003013 || BLEEDING-EDGE TROJAN TLS/SSL Server Certificate Exchange on High \
Port SSLv3
2003014 || BLEEDING-EDGE TROJAN TLS/SSL Server Key Exchange on High Port
2003015 || BLEEDING-EDGE TROJAN TLS/SSL Server Key Exchange on High Port \
SSLv3
2003016 || BLEEDING-EDGE TROJAN TLS/SSL Server Hello Done on High Port
2003017 || BLEEDING-EDGE TROJAN TLS/SSL Server Hello Done on High Port SSLv3
2003018 || BLEEDING-EDGE TROJAN TLS/SSL Server Cipher Set on High Port
2003019 || BLEEDING-EDGE TROJAN TLS/SSL Server Cipher Set on High Port SSLv3
2003020 || BLEEDING-EDGE TROJAN TLS/SSL Encrypted Application Data on High \
Port
2003021 || BLEEDING-EDGE TROJAN TLS/SSL Encrypted Application Data on High \
Port SSLv3

```

-> Added to bleeding.rules (4):

```

#Matt JOnkman
# This is a snlge packet sent out by a bot binary that was submitted
# If you get a hit on this check out the source system, and let us know \
please

```

We have yet to figure out what this is. It doesn't get a reply but appears \ important

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

-> Removed from bleeding-sid-msg.map (7):

```
2002189 || BLEEDING-EDGE Current Events OSA4.GIF Detected Possible \
Trojan.Tooso Infection
2002378 || BLEEDING-EDGE CURRENT Hostile Javascript s_ta_ts.js Requested || \
url,isc.sans.org/diary.php?date=2005-09-21
2002747 || BLEEDING-EDGE CURRENT Possible Phishing URL Retrieved || \
url,www.millersmiles.co.uk/report/1838 2002884 || BLEEDING-EDGE CURRENT Possible \
W32.Nugache P2P Botnet Communication INBOUND || \
url,isc.sans.org/diary.php?date=2006-04-30 || \
url,www.sarc.com/avcenter/venc/data/w32.nugache.a@mm.html 2002885 || BLEEDING-EDGE \
CURRENT Possible W32.Nugache P2P Botnet Communication OUTBOUND || \
url,isc.sans.org/diary.php?date=2006-04-30 || \
url,www.sarc.com/avcenter/venc/data/w32.nugache.a@mm.html 2002890 || BLEEDING-EDGE \
CURRENT Possible W32.Nugache P2P Botnet Communication OUTBOUND Initial Packet || \
url,isc.sans.org/diary.php?date=2006-04-30 || \
url,www.sarc.com/avcenter/venc/data/w32.nugache.a@mm.html 2002891 || BLEEDING-EDGE \
CURRENT Possible W32.Nugache P2P Botnet Communication INBOUND Initial Packet || \
url,isc.sans.org/diary.php?date=2006-04-30 || \
url,www.sarc.com/avcenter/venc/data/w32.nugache.a@mm.html
```

-> Removed from bleeding.rules (8):

```
#By david Glosser. This is an experiment. There are a large number of \
phishing scams
# using this login url. We want to see if this is a useful thing to alert on.
#by Blake Hartstein
#Matt Jonkman
# From the ISC post, and shadowserver.org research. New Bot nets using \
ecrypted P2p traffic # These sigs will greatly change as we learn more
#matt Jonkman from ISC diary entry of 9/21/05
# From forum post by merphie. We should remove this around 8/25 or so \
assuming the threat has passed
```

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](#)