



... mad about email, sane about security ...

WARNING

Please use the provided download scripts where possible... and **make sure that you double-check the cron job scheduling, as neither myself or the mirrors will appreciate signatures being downloaded, every second.**

The mirrors reserve the right to block your IP address, if you are downloading too many times per hour or are abusing their servers/bandwidth in any way.

If the download service is abused, the public rsync mirrors will be moved to a password only service, **with only people that have donated receiving the password to let them access the mirrors.**

Main Changes

- wget/curl etc. will no longer be used to download the signatures, we're moved to rsync. So please disable all old downloads urls and scripts for the signatures, as they won't be coming back using the old urls.
- Signatures are now signed using GnuPG, ensuring integrity of the signatures. The public key for these signature will be available from [here](#).

For example, here's a good verify:

```
gpg --verify junk.ndb.sig
gpg: Signature made 01/09/09 09:55:48 using DSA key ID 31EA4D9E
gpg: Good signature from "Saneseecurity (Saneseecurity Signatures)"
```

Here's a bad verify:

```
gpg --verify junk.ndb.sig
gpg: Signature made 01/09/09 09:55:48 using DSA key ID 31EA4D9E
gpg: BAD signature from "Saneseecurity (Saneseecurity Signatures)"
```

- A round-robin dns system, to help spread the load over multiple rsync servers. This has been setup using editdn.net dns service, in order to manage the multiple A records. As this is currently a free account, the TTL (time to live) for each server is set to 300 (5 minutes). If I receive enough donations, I'll update the account.
- **Four new signature databases** added: spear.ndb, spamimg.hdb, lott.ndb and spam.ldb (see details section below)
- A donation page, using PayPal will now also accept credit cards and hopefully we will be able to provide an invoice for people who want one. **Anyone who donates will be given a non-public download url, using only the fastest mirrors and in addition, be notified of any important changes.**

- A Mailing list is now available, **which is recommended that signature users subscribe to**, so that any future problems can be reported directly to you. Signup to the Sanesecurity mailing list, by sending a subject of subscribe to: sanesecurity-request@freelists.org
- There is an archive, so you can read previous messages here: <http://www.freelists.org/archive/sanesecurity>
- A Wikki, for user contributed information: <http://sanesecurity.wikidot.com/>
- new domains; sanesecurity.net and sanesecurity.org

Details

Current signature names

phish.ndb: phishing, malware, ecards

scam.ndb: spam, 419s, lottery, job, stocks

junk.ndb: phishing, malware, ecards, spam, 419s, lottery, job, stocks

spear.ndb: email spears/phishing, converted from <http://code.google.com/p/anti-phishing-email-reply/>

rogue.hdb: fake anti-virus software, other malware

spamimg.hdb: spam images

lott.ndb: simple lottery scams

spam.ldb: spam (using logical signatures)

Other files

phish.ndb.sig: gpg signed file for phish.ndb

scam.ndb.sig: gpg signed file for scam.ndb

junk.ndb.sig: gpg signed file for junk.ndb

spear.ndb.sig: gpg signed file for spear.ndb

rogue.hdb.sig: gpg signed file for rogue.hdb

spamimg.hdb.sig: gpg signed file for spamimg.hdb

lott.ndb: gpg signed file for lott.ndb

spam.ldb: gpg signed file for spam.ldb

Donations

SaneSecurity signatures are a culmination of hard work and commitment to providing Third-Party signatures to the web community that are of professional quality. We are not a company... and producing the signatures and support for the signatures, are carried out in my spare time.

If you feel that you would like to give a donation for your use of these signatures, or just because you want to support us, please consider making a donation via this page (we ask that you at least donate \$5 to cover PayPal processing fee's):

<http://www.sanesecurity.co.uk/donate.htm>

Rsync Mirrors

If you wish to mirror the Sanesecurity signature files and be added to the dns round-robin system, please contact me (steveb_clamav AT sanesecurity.com)

The mirror needs are basic...I need rsync access to a directory and also you'll need to setup IPTables to block IP's which may try to hammer the server.. more details will be given later.

Thanks

Malcolm Scott at Retrosnub Internet Services (www.retrosnub.co.uk) for providing a mirror, download script and for his knowledge in helping to setup the new download system.

Malcolm Scott at Retrosnub, Doc Schneider at FSL (<http://fsl.com>), Steve Freegard at FSL (<http://fsl.com>), Steve Swaney at FSL (<http://fsl.com>), Laurent CARON, Joerg.Traeger, Panagiotis Christias, Roland Pelzer, Patrick Ben Koetter and Matt at mxuptime for their invaluable help in mirroring the signatures and providing assistance.

False Positives

Please go to this page and report any false positives you find.

While you wait for the faulty signature to be fixed, the following two examples show you how to create a **local.ign** file, to skip signatures, which are causing you a problem.

Example 1:

If you have a false positive for **Sanesecurity.Phishing.Rdi.5.UNOFFICIAL** (which is in the **phish.ndb** database), all you have to do it create a **local.ign** file containing a line like this:

```
phish.ndb:5:Sanesecurity.Phishing.Rdi.5
```

And that signature will then be ignored.

<p>Note: make sure you leave off the .UNOFFICIAL from the signature name in the .ign file, otherwise it won't work.</p>
--

Example 2:

If you have a false positive for **Sanesecurity.Stk.3440.UNOFFICIAL** (which is in the **scam.ndb** database), all you have to do it create a **local.ign** file containing a line like this:

```
scam.ndb:3440:Sanesecurity.Stk.3440
```

And that signature will then be ignored.

<p>Note: make sure you leave off the .UNOFFICIAL from the signature name in the .ign file, otherwise it won't work.</p>
--

Commercial use: You can use the Sanesecurity signatures in commercial products. However, it would be appreciated if you make a donation and send an email, with information about the name of company and what product the signatures are being used in.

If you are using the signatures for a anti-spam/virus product and wish to **mirror the signatures for your own users to download directly** then please contact me, (steveb_clamav AT sanesecurity.com).

Disclaimer

Whilst every effort has been made by Sanesecurity to ensure that the signatures don't lead to false positives, we make no warranty that the signatures will meet your requirements, be uninterrupted, complete, timely, secure or error free

Trademarks

Signatures © sanesecurity.org.uk. All Rights Reserved.
ClamAV is a registered trademark of Sourcefire, Inc.

```
00101000011000110010100100100000010100110111010001100101011101100
11001010010000001000010011000010111001101100110011011110111001001
100100
```