

RE: NAI VirusScan [was: probable virus]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-10/6302.html>

From: Mike Tanca (mike@sentex.net)

Date: 10/30/01

Date: Tue, 30 Oct 2001 14:47:55 -0500

To: "Brandon Harper" <lists-inet@booms.net>, <freebsd-security@FreeBSD.ORG>

From: Mike Tanca <mike@sentex.net>

The .tar files on the ftp site are updated usually once per week. You can get more up to date files from their web site at

<http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/virus-4d.asp>

http://download.nai.com/products/mcafee-avert/daily_dats/DAILYDAT.ZIP

As the files names are all UPPERCASE, I just did

In clean.dat CLEAN.DAT

In scan.dat SCAN.DAT

In names.dat NAMES.DAT in the

so that when I unzipped the file I would not have to worry about renaming things. They seem to work OK so far. As well as the ones posted to the list, I did get a copy of

http://vil.nai.com/vil/virusSummary.asp?virus_k=99237

sent to my network by other means so I wanted to have a method to stop this particular virus without having to wait another day for the next scheduled weekly release.

The disclaimer however says that these _daily_ dat files are considered beta.

---Mike

At 12:39 PM 10/30/01 -0700, Brandon Harper wrote:

> >

> >

> > *Just to followup, the daily dat file seems to be working fine.*

> > *Anyone out*

> > *there using it on a regular basis, I would be interested in hearing your experiences.*

> >

> > ---Mike

> >

>

>

>Mike--

>

RE: NAI VirusScan [was: probable virus]

FreeBSD-Security: RE: NAI VirusScan [was: probable virus]

>I'm also using UVScan and know that my definition files are getting updated
>daily via cron, and it hasn't been catching these latest virii either. I
>also had someone privately e-mail me who said it wasn't working for them
>either yesterday. I'm using version 4.x, and have the latest dat file:
>
>bash-2.04# ls -la dat*.*
>-rw-r--r-- 1 root wheel 2222080 Oct 23 21:15 dat-4167.tar
>
>bash-2.04# ls -la scan.dat
>-rwxr--r-- 1 root wheel 1543967 Oct 23 22:15 scan.dat
>
>It did however catch a W95.Hybris.gen message yesterday (the
>haha@sexyfun.net worm), so the problem seems to be related to the
>definitions for UVScan itself.
>
>- Brandon
>
><!-- <http://www.booms.net> -->
>
>
>To Unsubscribe: send mail to majordomo@FreeBSD.org
>with "unsubscribe freebsd-security" in the body of the message

To Unsubscribe: send mail to majordomo@FreeBSD.org
with "unsubscribe freebsd-security" in the body of the message