From: Jonathan Lee jonathanlee571@gmail.com
Subject: Re: [clamav-users] Antivirus Bases showing outdated main.cvd with a version dated year 2021
Date: August 30, 2023 at 1:53 PM
To: Andrew C Aitchison andrew@aitchison.me.uk, Jonathan Lee via clamav-users clamav-users@lists.clamav.net

Thank you for your email.

I was confused as the following statement from Clam AV's website doesn't reflect new date ranges within main.cvd correctly. This confusion stems from the following statement about main.cvd containing and I quote "signatures previously in daily.cvd." Therefore, the signature migration into main.cvd I assumed would constitute a new file or create a new date and version number for the main.cvd after several new daily.cvd updates.

I was under that assumption.

Thanks for the information.

"main.cvd contains signatures previously in daily.cvd that have shown to have a low false-positive risk."

Get Outlook for Android

From: Andrew C Aitchison <andrew@aitchison.me.uk>
Sent: Wednesday, August 30, 2023 12:14:33 PM
To: Jonathan Lee via clamav-users <clamav-users@lists.clamav.net>
Cc: Jonathan Lee <jonathanlee571@gmail.com>
Subject: Re: [clamav-users] Antivirus Bases showing outdated main.cvd with a version dated year 2021

On Wed, 30 Aug 2023, Jonathan Lee via clamav-users wrote:

> Hello fellow ClamAV members,
>
>
> Can you please help?
>
>
> Per ClamAV's website:
> "ClamAV signatures come in a variety of formats, one for each of the distinct detection methods that the ClamAV file scanning engine supports. ClamAV also uses the ClamAV Virus Database (CVD) file format, which serves as a container for the compressed and digitally-signed official signature sets that power ClamAV — daily.cvd, main.cvd, and bytecode.cvd. Each signature set serves a different purpose:
>
> bytecode.cvd contains all compiled bytecode signatures evaluated by the bytecode interpreter engine
> daily.cvd contains signatures for the latest threats (updated daily)
> main.cvd contains signatures previously in daily.cvd that have shown to have a low false-positive risk."
>
>
> The main.cvd is not replacing itself with an updated version.
>
> Squid ClamAV is not updating the main.cvd and is listing 2021 version

You have the latest version.
ClamAV have not made a new version of main.cvd for nearly two years

ClamAV have not made a new version of mainforce for nearly two years. It is a very big file and stores the definitions that do not change very often.

daily.cld (or daily.cvd depending how it reaches your machine) contains the latest updates.

> Squid Version 5.7
> Antivirus Scanner ClamAV 0.105.1_1,1 C-ICAP 0.5.10,2 + SquidClamav 7.2
> Antivirus Bases
> Database Date Version Builder
> daily.cld 2023.03.14 26841 raynman
> bytecode.cvd 2023.02.22 334 anvilleg
> main.cvd 2021.09.16 62 sigmgr
> Last Update Tue Mar 14 00:22:56 2023
> Statistics Found 124 virus(es) total.
>
> Please see attached ClamAV is functional again main is not updating with prior daily.cvd
>
>
> It shows from 2021 still
>
>
>
> Ref:
> https://redmine.pfsense.org/issues/14108
> https://bugs.squid-cache.org/show_bug.cgi?id=5297
>
> Per developer investigation this is the newest file available for main.cvd
>
>

--
Andrew C. Aitchison   Kendal, UK
          andrew@aitchison.me.uk