Packages - Privacy Issue #2646

Win.Trojan.Maljava-2 FOUND

2020-03-03 02:37 PM - libreuser

Status:	not-a-bug	**% Done:**	0%
Priority:	bug		
Assignee:			
Category:			

Description

Clamscan reports:

```
/var/cache/pkgfile/community.files: Win.Trojan.Maljava-2 FOUND
```

Hint: Already removed and reloaded by

```
rm -r /var/cache/pkgfile/*
pkgfile -u
```

History

#1 - 2020-03-03 03:09 PM - freemor

Most likely a transient false positive. Can not reproduce.
Are you on i686 or arm? I haven't tried to reproduce on those yet.

As it is just a large ASCII cpio archive a false positive is more than possible.

#2 - 2020-03-03 03:29 PM - GNUtoo

I've tried on i686.

It's could also have fixed between the time you last updated your local malware database and the time I did the same.

I've done:

```
sudo freshclam
pkgfile -u
clamscan /var/cache/pkgfile/community.files
```

And I've the following result:

```
/var/cache/pkgfile/community.files: OK

----------- SCAN SUMMARY -----------
Known viruses: 6759120
Engine version: 0.101.2
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 146.79 MB (ratio 0.00:1)
Time: 161.971 sec (2 m 41 s)
```

Could you try after re-updating the malware database with freshclam?

By the way do you know if there is an easy way to update that database without giving root access to freshclam?

PS: Most of the time I don't agree network terms of services for things like WiFi when they prevent you from sending or transmitting viruses as there are legitimate cases where for instance you might want to send a virus sample to clamav, which is free software.

PPS: It would be an interesting project to use sandboxing for clamscan as in general programs like antivirus are parsing a lot of untrusted files. It has been done by the tracker project which is a project to parse and index files.

Denis.

#3 - 2020-03-03 03:38 PM - freemor

clamscan can be easily sandboxed with firejail
it even comes with a pre-defined clamscan profile.

I'll take a look at updating clamscan as I can build for all archs

#4 - 2020-03-03 03:50 PM - libreuser

https://www.virustotal.com/gui/file/f54b012dd91f6cbdde351a5d334ef7518017d630e5c0a3f6f8f1f95ddd8f682f/detection

#5 - 2020-03-03 03:57 PM - libreuser

CPU: x86_64

#6 - 2020-03-03 06:05 PM - freemor

Well thats what I'm on and I am getting the same non-result as GNUtoo

#7 - 2020-03-03 06:33 PM - freemor

from your Virustotal link it is definitely looking like a false positive,

#8 - 2020-03-04 06:40 PM - libreuser

I think most virus scanners don't scan huge files like this. :/

#9 - 2020-03-04 09:28 PM - freemor

The chances of this being an acutal virus are very low.

- Win.Trojan.Maljava-2 - Would indicate a Windows malware
- The file is a just a huge ASCII file. so not executeable
- The file is a fairly trivial format (cpio archive) so it's doubtful that there a flaw in the extractor
- The file merely contains a bunch of text file named for packages which list the files/directories in thos packages
- Java has nothing to do with this file in the normal rource of things (cause it's not a jar, cause it's not exectuable)

The Chance of a false positive is high.

- All that is needed for a false positive is for there to be a string that matches what the IOC sting for that malware
- with 170 MB of strings to look at it wouldn't take much

if you still have the "Infected" file there are ways you could track down where the false positive is matching but that is a longer discussion.

#10 - 2020-03-04 09:39 PM - freemor

Although if malware did by some fluke get injected in that cpio archive it'd be a very interesting find :)

#11 - 2020-03-04 09:55 PM - freemor

And it looks like it has false positived in the past too.

https://github.com/falconindy/pkgfile/issues/46

An it looks like there is a history of Clamav Falsing on this particular detection:

http://www.edison-newworld.com/2017/04/clamav-false-positive-on-java-malware.html

#12 - 2020-03-04 10:04 PM - freemor

- Status changed from unconfirmed to not-a-bug

#13 - 2020-04-30 12:44 AM - bill-auger

the proper thing to do of course, is to notify the maintainers of the virus scan program of this recurring false positive, and sending them an example pkgfile list which triggered it

#14 - 2020-04-30 01:28 AM - libreuser

I already did. I mean I reported it on the clamav website https://www.clamav.net/reports/fp

Probably; twice. :)

#15 - 2020-04-30 03:06 AM - bill-auger

for most bug reports, the arch and init information is usually not important - it gave me an idea though, to add that information to an optional post

signature, definable in the user profile https://labs.parabola.nu/issues/2715