Packages - Bug #3269

[telegram-desktop] possible DRM, security, privacy, and anonymity issues

2022-05-05 02:25 PM - GNUtoo

Status:	unconfirmed	**% Done:**	0%
Priority:	freedom issue		
Assignee:	oaken-source		
Category:			

Description

Hi,

Someone described on the gnu-linux-libre mailing list a Telegram anti-feature that looks like DRM to me[1]: that anti-feature "forbids the user to copy/paste or forward text (and also forbids saving images or other media included in the messages) from certain groups where the admin has enabled the restriction".

[1] https://lists.nongnu.org/archive/html/gnu-linux-libre/2022-05/msg00002.html

History

#1 - 2022-05-05 03:23 PM - bill-auger

i have not read the email; but by that description, that feature is not DRM - DRM is non-free code, running on the client - telegram is, and always was, non-free code running on a server; but the client in parabola is presumed to be libre

if the code responsible for the restrictions are running on the server, then there is nothing for us to do - if people do not like that, they should stop using that service (which has been my advice ever since this client entered parabola)

AFAIAC, this is no different than the original accusations about this software when it entered parabola - people suggested that it's fundamental operation involved constantly downloading ephemeral javascript from the server, and executing it blindly - of course iceweasel does that too; but not necessarily - the suggestion was that this software would be useless without those remote javascript instructions, invisible to the user

i asked RMS about it, because i wanted a reason to audit it, due to those accusations - in short, he told me we could keep it - i believe that was the wrong decision; but i did not care to argue about it - i would rather remove any software like this, rather than spend time auditing and rescuing it

unfortunately, he answered as if i had only asked the common "is it SaaSS?" question, without responding directly to the subtlety of the ephemeral javascript running blindly on the client, which was the only reason i bothered him - i already knew that he would say it is not SaaSS

in any case, i dont see any difference with that original accusation, and this alleged DRM feature, or real DRM blobs in web browsers for that matter - it is not important what the non-free code does - it only matters which machine it is running on - in fact, DRM in web browsers, is much less significant than the original accusation; because it is not *the* fundamental necessary feature of the web browser - you could use a web browser indefinitely, without ever encountering an offer for a DRM blob - yet we spend several hours each month patching mozilla, for really only that reason

again, i do not know if telegram client actually does that; because RMS dissuaded me from scrutinizing it - but to be consistent with the "GNU message", if the FSDG prohibits web browsers which accept remote DRM loads, then it should prohibit clients that necessarily execute ephemeral javascript from one, and only one remote service, for which no libre replacement server code exists, or is ever likely to exist - i see no difference in those two examples, other than the buzzword "DRM", and the format of the code (minified JS vs machine code - thats not important)

the libre argument is that it could be used with another server, in theory; but in reality, that is never going to happen - this is disposable, frivolous vanity software, for a very special use case: namely, as an accessory to one proprietary service - there is no compelling libre argument for it - it is the bic lighter of software - if (when) the corporate telegram service shut down, no one would use the telegram client with any other server, even if another server existed; and we all know that

that was maybe long winded; but i did not agree with the decision to keep this program in parabola when it first arrived, and i dont care to fuss over it now - if it has any problems at all, lets just scrap it, and move on - IMHO, it is not worth rescuing - IIRC it was oaken-source who wanted to keep it - so i am assigning this ticket to him

#2 - 2022-05-05 03:42 PM - bill-auger

- Assignee set to oaken-source

#3 - 2022-05-05 05:20 PM - gap

Freedom issues with Telegram aside, it's also horrifically insecure (IIRC messages are encrypted in-transit and then decrypted on the server, which essentially means the server, of which nobody can self-host because it is unreleased proprietary software, is a permanent MITM), horrifically un-private (IIRC it requires a SIM/phone number), and obsolete because numerous other libre messenger protocols are more secure and private, not to mention decentralised, eg. Tox.

Unless there is a special reason to keep Telegram around, IMHO it should be purged from the repos.
If the decision is made to keep it around for whatever reason, then adding anything Telegram-related to the your-privacy blacklist is a no-brainer.

See also: #3010.

#4 - 2022-05-05 05:40 PM - bill-auger

- Assignee deleted (oaken-source)

FWIW, there is nothing to be learned from #3010, other than it was closed as 'not-a-bug', just like the original complaint #1882 was, despite the fact the freemor and i basically agreed with the OP, and shared the same opinion on telegram's value to parabola,, which i re-stated again today

i doubt that there is anything new or interesting to discuss about telegram which is not already known - people just dont like "corporate stuff"; and complaints like this are common - i have not read the new discordapp ticket; but off-hand, i suspect that it is in exactly the same category as telegram - totally libre, so parabola can keep it; but totally a corporate vanity tool, which offers no unique value to parabola

IMHO, if people are so passionate about rejecting "corporate stuff"; then those people should be *much* more worried about the corporate influence on linux, chromium, and other programs, which are much more popular and difficult to audit, than any chat client - the energy behind these complaints is very mis-directed IMHO - people complain about these things precisely because they are not important - these programs can easily be discarded or simply ignored

freemor wrote:

> As long as the client has the 4 freedoms I see no reason for it not to remain. While I'd never recommend anyone use it.
>
> Now if it's lacking the 4 freedoms then chuck it in the dust bin.

#5 - 2022-05-05 05:54 PM - bill-auger

- Assignee set to oaken-source

#6 - 2022-05-05 06:27 PM - gap

For the record, I'm not against Telegram, or any other free program for that matter, because it is "corporate", I'm against it because it has horrific security, privacy, and anonymity issues.
Whether there is a causal link between corporate contributions and such issues is a different question.

#7 - 2022-05-05 08:01 PM - bill-auger

- Subject changed from [telegram-desktop] possible DRM to [telegram-desktop] possible DRM, security, privacy, and anonymity issues

> For the record, I'm not against ... "corporate", I'm against it because it has horrific security, privacy, and anonymity issues.

you can not possibly know that - no one can - it is a presumption; and i am certain that is only because those are operated by corporations - no one ever accuses a small business or independent service of these evil-doings - it is always the corporate ones

i will add this here just to save time - it would be the general response to all of those privacy bug reports you opened today

none of those programs are privacy-invading - very few, or maybe nothing in [nonprism] is there because it is privacy-invading - the remote servers that they are *able* to connect with, may be considered to be privacy-invading; but there is no reason for those clients connect to their servers automatically - if they do, the FSDG would require that behavior to be removed; but only the automatic or hidden behavior

for things like pidgin and kaccounts which allow connecting to many different kinds of services, that is not likely at all - the user must explicitly enter credentials for each server, before they will connect to any

but most importantly, anyone who uses those programs, obviously wants to connect to the remote service - which means that the user *wants* that server to "invade their privacy" - which is actually nonsense - if the act was voluntary, then no "invasion" happened - to connect your computer to anyone else's computer, is necessarily to forfeit privacy to the owner of that computer,

always, in every case

it makes no difference if people believe that the server decodes the transmission, or if they believe otherwise - no one, other than the operator of the server, knows if that happens, or if it does not - so the wise assumption, if one is concerned about that sort of thing, is to assume that it always happens

the only alternative is to avoid using those programs - in that case, it makes no difference which repo they are available in, or if there is a blacklist package to prevent installing something that you dont want to use anyways - why would anyone install something named: 'telegram-client', unless they knew what the telegram server is, and wanted to connect to it ? - in most cases, it is not even possible to register for the service using the libre program - they usually require a web browser to register first on the website

#8 - 2022-05-06 12:07 AM - gap

The security, privacy, and anonymity implications of messenger software are not merely a presumption; any centralised server no matter whether it is corporate or run by a single person, has great power over the network and messages sent via it, so there is no way of trusting it and knowing it is secure, private, and anonymous, without blind faith, or running it yourself.
That is why decentralisation is so important; because in that paradigm no single central controller exists, let alone needs to be trusted.
In the case of Telegram, IIRC, we know for certain it is neither secure, nor private, nor anonymous, for the reasons I mentioned earlier.

Your argument that the packages in question are only installed by people who accept the violation of privacy is flawed, because it mirrors the argument that people only install proprietary packages if they are willing to give up freedom.
In either case, people might not know their freedom/privacy is a stake, and might not even know the program is being installed at all, as it may be a dependency.
That is why the respective blacklists and your-* package conflicts are so important; they prevent accidental installation of known troublesome software, and choosing to make the override is a conscious decision on the part of the user.

The sole purpose of these programs is not to be a general-purpose tool like a web browser, but to connect to specific online dis-services which are known to violate privacy.

Moreover, I thought we already agreed the solution to the issues with Telegram is that it is obsolete and shouldn't be used.
In this way, is Parabola sending the wrong message by keeping packages known to endanger privacy in its repos at all and failing to protect its users by default?
Our approach to privacy-disrespecting packages is similar to the approach of other distros with regards to proprietary software, ie. keep it, but keep it demarcated.
Hyperbola chose to remove such packages entirely.

As I mentioned previously, the argument that people choose to give up their privacy mirrors the argument that people choose to give up freedom; in both cases shouldn't we make nonfree and un-private packages not part of Parabola, and unsupported?

Should we have a poll to see how many users have your-privacy installed?