Google's Software is Malware

Other examples of proprietary malware

Malware means software designed to function in ways that mistreat or harm the user. (This does not include accidental errors.) This page explains how Google's software is malware.

Malware and nonfree software are two different issues. The difference between free software and nonfree software is in whether the users have control of the program or vice versa. It's not directly a question of what the program *does* when it runs. However, in practice nonfree software is often malware, because the developer's awareness that the users would be powerless to fix any malicious functionalities tempts the developer to impose some.

If you know of an example that ought to be in this page but isn't here, please write to <webmasters@gnu.org> to inform us. Please include the URL of a trustworthy reference or two to serve as specific substantiation.

Type of malware

- Back doors
- Censorship
- Digital restrictions management or "DRM"—functionalities designed to restrict what users can do with the data in their computers.
- Insecurity
- Interference
- Sabotage
- Surveillance
- Tyrants—systems that reject any operating system not "authorized" by the manufacturer.

Google Back Doors

- Android has a back door for remotely changing "user" settings.

  The article suggests it might be a universal back door, but this isn't clear.

- ChromeOS has a universal back door. At least, Google says it does—in section 4 of the EULA.

- In Android, Google has a back door to remotely delete apps. (It was in a program called GTalkService, which seems since then to have been merged into Google Play.)

  Google can also forcibly and remotely install apps through GTalkService. This is not equivalent to a universal back door, but permits various dirty tricks.

  Although Google's *exercise* of this power has not been malicious so far, the point is that nobody should have such power, which could also be used maliciously. You might well decide to let a security service remotely *deactivate* programs that it considers malicious. But there is no excuse for allowing it to *delete* the programs, and you should have the right to decide who (if anyone) to trust in this way.

Google Censorship

- Google offers censorship software, ostensibly for parents to put into their children's computers.

- On Windows and MacOS, Chrome disables extensions that are not hosted in the Chrome Web Store.

  For example, an extension was banned from the Chrome Web Store, and permanently disabled on more than 40,000 computers.

- Google censored installation of Samsung's ad-blocker on Android phones, saying that blocking ads is "interference" with the sites that advertise (and surveil users through ads).

  The ad-blocker is proprietary software, just like the program (Google Play) that Google used to deny access to install it. Using a nonfree program gives the owner power over you, and Google has exercised that power.

  Google's censorship, unlike that of Apple, is not total: Android allows users to install apps in other ways. You can install free programs from f-droid.org.

Google DRM

- Google now allows Android apps to detect whether a device has been rooted, and refuse to install if so. The Netflix app uses this ability to enforce DRM by refusing to install on rooted Android devices.

  Update: Google *intentionally* changed Android so that apps can detect rooted devices and refuse to run on them. The Netflix app is proprietary malware, and one shouldn't use it. However, that does not make what Google has done any less wrong.

- Chrome implements DRM. So does Chromium, through nonfree software that is effectively part of it.

  More information.

- Android contains facilities specifically to support DRM.

Google Insecurity

These bugs are/were not intentional, so unlike the rest of the file they do not count as malware. We mention them to refute the supposition that prestigious proprietary software doesn't have grave bugs.

- Many Android apps can track users' movements even when the user says not to allow them access to locations.

  This involves an apparently unintentional weakness in Android, exploited intentionally by malicious apps.

- The NSA can tap data in smart phones, including iPhones, Android, and BlackBerry. While there is not much detail here, it seems that this does not operate via the universal back door that we know nearly all portable phones have. It may involve exploiting various bugs. There are lots of bugs in the phones' radio software.

Google Interference

This section gives examples of Google software harassing or annoying the user, or causing trouble for the user. These actions are like sabotage but the word "sabotage" is too strong for them.

- Google is modifying Chromium so that extensions won't be able to alter or block whatever the page contains. Users could conceivably reverse the change in a fork of Chromium, but surely Chrome (nonfree) will have the same change, and users can't fix it there.

Google Sabotage

The wrongs in this section are not precisely malware, since they do not involve making the program that runs in a way that hurts the user. But they are a lot like malware, since they are technical Google actions that harm the users of specific Google software.

- Revolv is an IoT device which managed "smart home" operations: switching the lights, operate motion sensors, regulating temperature, etc. On May 15th, 2016, Google said it would shut down the service linked to the device, making it unusable.

  Although you may own the device, its functioning depended on the server that never belonged to you. So you never really had control of it. This unjust design is called Service as a Software Substitute (SaaSS). That is what gave the company the power to convert it into a $300 out-of-warranty brick, for your "dumb home".

- Google/Alphabet intentionally broke Revolv home automatic control products that depended on a server to function, by shutting down the server. The lesson is, reject all such products. Insist on self-contained computers that run free software!

- Google has long had a back door to remotely unlock an Android device, unless its disk is encrypted (possible since Android 5.0 Lollipop, but still not quite the default).

Google Surveillance

- Google "Assistant" records users' conversations even when it is not supposed to listen. Thus, when one of Google's subcontractors discloses a thousand confidential voice recordings, users were easily identified from these recordings.

  Since Google "Assistant" uses proprietary software, there is no way to see or control what it records or sends.

  Rather than trying to better control the use of recordings, Google should not record or listen to the person's voice. It should only get commands that the user wants to send to some Google service.

- Google Chrome is an instrument of surveillance. It lets thousands of trackers invade users' computers and report the sites they visit to advertising and data companies, first of all to Google. Moreover, if users have a Gmail account, Chrome automatically logs them in to the browser for more convenient profiling. On Android, Chrome also reports their location to Google.

  The best way to escape surveillance is to switch to IceCat, a modified version of Firefox with several changes to protect users' privacy.

- Google tracks the movements of Android phones and iPhones running Goggle apps, and sometimes saves the data for years.

  Nonfree software in the phone has to be responsible for sending the location data to Google.

- Google invites people to let Google monitor their phone use, and all internet use in their homes, for an extravagant payment of $20.

  This is not a malicious functionality of a program with some other purpose; this is the software's sole purpose, and Google says so. But Google says it in a way that encourages most people to ignore the details. That, we believe, makes it fitting to list here.

- An Android phone was observed to track location even while in airplane mode. It didn't send the location data while in airplane mode. Instead, it saved up the data, and sent them all later.

- Some Google apps on Android record the user's location even when users disable "location tracking".

There are other ways to turn off the other kinds of location tracking, but most users will be tricked by the misleading control.

- Android tracks location for Google even when “location services” are turned off, even when the phone has no SIM card.
- Low-priced Chromebooks for schools are collecting far more data on students than is necessary, and store it indefinitely. Parents and students complain about the lack of transparency on the part of both the educational services and the schools, the difficulty of opting out of these services, and the lack of proper privacy policies, among other things.

  But complaining is not sufficient. Parents, students and teachers should realize that the software Google uses to spy on students is nonfree, so they can't verify what it really does. The only remedy is to persuade school officials to exclusively use free software for both education and school administration. If the school is run locally, parents and teachers can mandate their representatives at the School Board to refuse the budget unless the school initiates a switch to free software. If education is run nation-wide, they need to persuade legislators (e.g., through free software organizations, political parties, etc.) to migrate the public schools to free software.
- Google's new voice messaging app logs all conversations.
- Google Play (a component of Android) tracks the users' movements without their permission.

  Even if you disable Google Maps and location tracking, you must disable Google Play itself to completely stop the tracking. This is yet another example of nonfree software pretending to obey the user, when it's actually doing something else. Such a thing would be almost unthinkable with free software.
- Google Chrome makes it easy for an extension to do total snooping on the user's browsing, and many of them do so.
- Google Chrome includes a module that activates microphones and transmits audio to its servers.
- Nest thermometers send a lot of data about the user.
- Google Chrome spies on browser history, affiliations, and other installed software.
- Spyware in Android phones (and Windows? laptops): The Wall Street Journal (in an article blocked from us by a paywall) reports that the FBI can remotely activate the GPS and microphone in Android phones and laptops. (I suspect this means Windows laptops.) Here is more info.
- Spyware is present in some Android devices when they are sold. Some Motorola phones, made when this company was owned by Google, use a modified version of Android that sends personal data to Motorola.
- A Motorola phone listens for voice all the time.
- Google Play intentionally sends app developers the personal details of users that install the app.

  Merely asking the “consent” of users is not enough to legitimize actions like this. At this point, most users have stopped reading the “Terms and Conditions” that spell out what they are “consenting” to. Google should clearly and honestly identify the information it collects on users, instead of hiding it in an obscurely worded EULA.

  However, to truly protect people's privacy, we must prevent Google and other companies from getting this personal information in the first place!
- Many web sites report all their visitors to Google by using the Google Analytics service, which tells Google the IP address and the page that was visited.
- Google Chrome contains a key logger that sends Google every URL typed in, one key at a time.

Google Tyrants

- Motorola, then owned by Google, made Android phones that are tyrants (though someone found a way to crack the restriction). Fortunately, most Android devices are not tyrants.

TOP ▲
