KeepassXC Browser plugin

Calling Home

Onkobu Tanaake

2021-05-10T10:00:00

As I raked through open connections I found suspicious IPs with lasting connections and very low traffic. Looking them up their origin is KeepassXC Browser addon. A simple invocation of `lsof -i tcp` is sufficient.

- 216.58.213.202 - Google
- 44.241.164.82 - Amateur Radio Digital Communications
- 143.204.93.8 - Software Editing Corporation, SEC.com, registered in the 90s[1]

The target port was always 443, regular TLS connection. Quote from page[2]:

> KeePassXC needs network access for downloading […] favicons for password entries and for providing KeePassHTTP-compatible browser extensions with access to your database.

And also written there this can be disabled completely even as compiler switch. Such a switch is called USE variable on Gentoo. In this case I'd emerge with USE=-network. I removed the browser plugin completely. In addition I disabled any egress from KeepassXC. Connections gone.

Warning

I didn't inspect the traffic more detailed. Also the possibility of outgoing connections is stated clearly in the manual. Those connections can easily be disabled from within KeepassXC. In addition I never authorized the plugin on Gentoo to access the keystore – the application explicitely notifies about this. It is very unlikely that my passwords were exfiltrated. But lesser connections mean smaller attack surface.

Update 2021-06-07T21:00:00

Correct date of publication, was not in 2018.