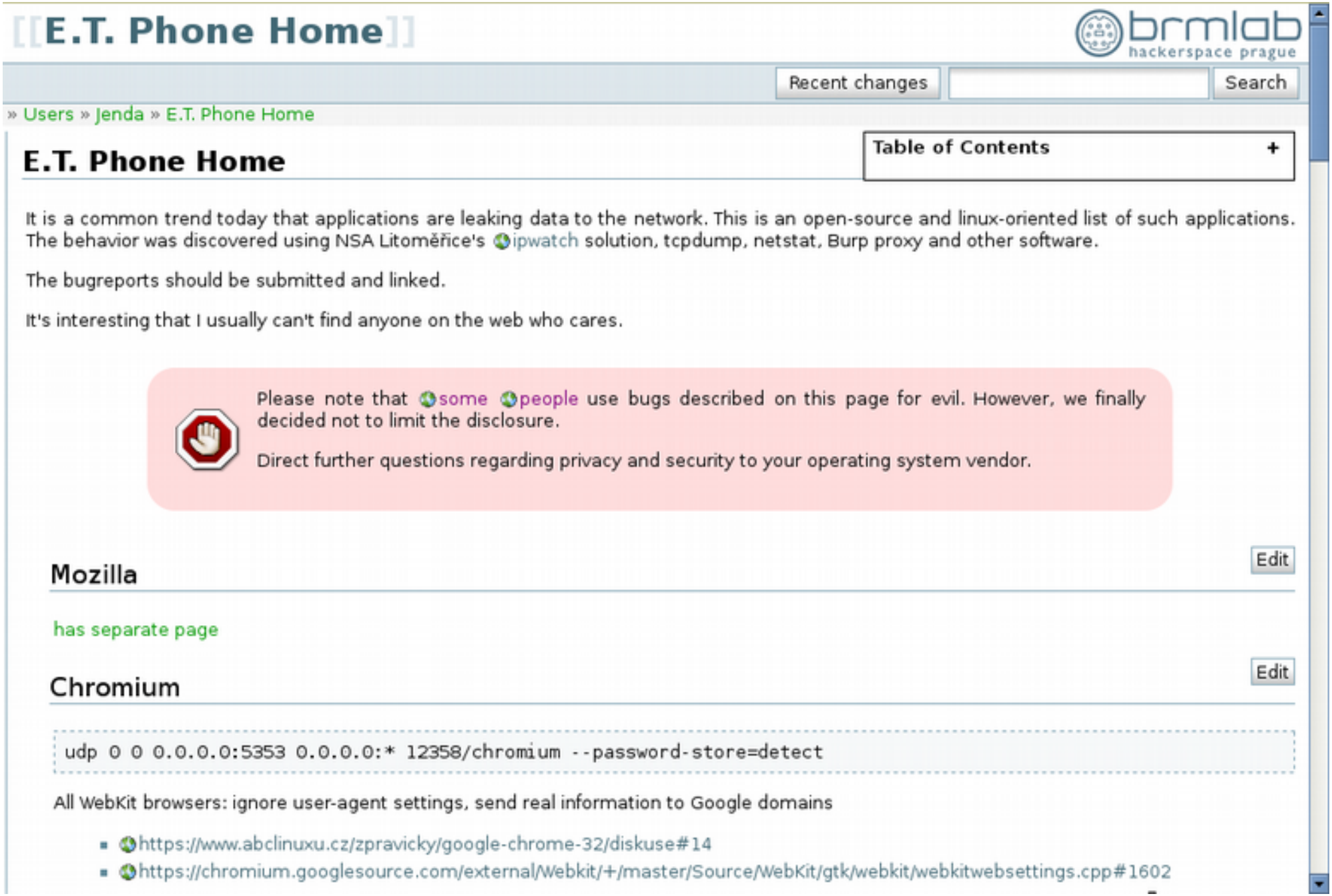

[[E.T. Phone Home]]

brmlab hackerspace prague

Recent changes | Search

» Users » Jenda » E.T. Phone Home

E.T. Phone Home

Table of Contents +

It is a common trend today that applications are leaking data to the network. This is an open-source and linux-oriented list of such applications. The behavior was discovered using NSA Litoměřice's ipwatch solution, tcpdump, netstat, Burp proxy and other software.

The bugreports should be submitted and linked.

It's interesting that I usually can't find anyone on the web who cares.

Please note that some people use bugs described on this page for evil. However, we finally decided not to limit the disclosure.

Direct further questions regarding privacy and security to your operating system vendor.

Mozilla

Edit

has separate page

Chromium

Edit

```
udp 0 0 0.0.0.0:5353 0.0.0.0:* 12358/chromium --password-store=detect
```

All WebKit browsers: ignore user-agent settings, send real information to Google domains

- https://www.abclinuxu.cz/zpravicky/google-chrome-32/diskuse#14
- https://chromium.googlesource.com/external/Webkit/+/master/Source/WebKit/gtk/webkit/webkitwebsettings.cpp#1602

- No application firewall in Linux (out-of-tree-patches)
- ipwatch (iptables match UID), warn_services, ...
- Update checks...

Stardict

Edit

As of 12/2015, the default configuration of Stardict in Debian Sid uses dict.cn as the default dictionary. Additionally, as clipboard scanning is enabled by default, this means that as you start Stardict, your clipboard contents gets sent in the following HTTP request:

```
GET HTTP://dict.cn/ws.php?utf8=true&q=HESLO HTTP/1.1\r\n
```

It has been confirmed that if you use KeePassX, which by default uses "copy password to clipboard", this password is immediately sent by Stardict.

Bug:

- https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=806960

Related, but not the same:

- https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=613236
- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2260

GNOME

- gitg leaks e-mail addresses from commit messages to gravatar
- gnome-contacts leaks physical address of your contact to proxy.gnome.org, Akamai and OSM Nominatim

https://bugzilla.gnome.org/show_bug.cgi?id=744159, https://bugzilla.gnome.org/show_bug.cgi?id=750192

Debian (systemd/resolved)

Uses 8.8.8.8 DNS server if no other is available: https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=761658

GQRX

Sends broadcasts upon startup, so others can sniff while you sniff.

Spyzilla

Table of Contents +

Mozilla products by default send some information to NSA. This guide will show you how to change these settings to other secret service of your choice or how to turn them off completely.

See also list of other applications that do not respect privacy.

Client certificates

Edit

Check *Advanced → Certificates → Ask me every time*, we really don't want to authenticate to the remote server automatically! Exploited in the wild!

Firefox

Edit

- Run with parameter -P. Select "Start offline"
- Visit Preferences. In "Security", turn off "Block reported attack sites" and "Block reported web forgeries"
- Uncheck Advanced → Updates
- Uncheck Advanced → Certificates → Validation → OCSP (of course this disables fetching certificate revocation info - be sure you know what are you doing)
- Visit about:config. Set extensions.blocklist.enabled = false.
- Search for "http". Change all URLs to nsalitomerice.cz, localhost or other secret service of your choice.
- Unfortunately, Firefox will still download favicons from Google, Yahoo and Mibbit (incl. cookies) when browsing Preferences in a certain way. Bugreport pending.
- Since FF 32, on Windows, hashes of certain downloaded files are sent to Google. This can be disabled by the aforementioned settings. 1, 2
- If you want to test this with an intercepting proxy, make sure you have security.cert_pinning.enforcement_level 0 or 1
- Disable automatic resolving of local names and URL-like patters: set browser.fixup.alternate.enabled and keyword.enabled to false. PT
- media.peerconnection.enabled: false (enumhosts, mirror)
- Since version 33, some plugins seem to be downloaded automatically. Set media.gmp-gmpopenh264.autoupdate = false.
  - Since version 38, it is not possible to turn this feature off. Additionally, the downloaded binary contained a buffer overflow.
    - media.gmp-gmpopenh264.enabled does not help and media.gmp-gmpopenh264.autoupdate does note exist anymore. Try setting media.gmp-manager.lastCheck to the future and media.gmp-manager.url to some non-existent URL.
- Since version 38 (on Windows), a DRM backdoor from Adobe is downloaded automatically: The CDM will be downloaded from Adobe shortly after you upgrade or install Firefox and will be activated when you first interact with a site that uses Adobe CDM.