Purism

THREATS THE LIBREM NOTEBOOK COMPUTERS COULD PREVENT

The following examples of data theft and security breaches from the past year illustrate potential security threats Librem computers can prevent:

Corporate data exploitation: "Superfish" pre-installed man-in-the-middle malware, where all secure communications were intercepted, including user's bank login credentials.

Social media data theft: Over 2 million Facebook, Gmail, and Twitter accounts were intercepted from keylogger malware.

Spying and stalking: There have been numerous reports of stalkers remotely activating user's microphone, webcam, or recording VoIP services, such as Skype calls.

Backdoors: "Backdoors" (or proprietary code for which no security experts can verify the source code) are built into competitor's software and operating systems.

Data-mining: Third-party trackers and ad trackers gather personal information about users' browsing habits, often selling the information.

Ransomware: Malware such as CryptoLocker and CryptoWall encrypt the users' drives, forcing them to pay for a decryption key to retrieve their data.

Antivirus applications do not prevent these threats. While these examples are recent, there may be more threats in the future that could be prevented using a Librem private computer.

PRESS CONTACT:

Giselle Bisson
PR Director, Purism
https://puri.sm
(415)655-1050
giselle.bisson@puri.sm