How private is your browser's privacy mode?

18 February 2016, by David Bradley

Credit: Wikipedia

A forensic analysis of the so-called "private" browsing modes of the most popular web browsers, Microsoft's Internet Explorer, Google Chrome, Mozilla Firefox, and Opera, reveals that the Microsoft product tested in this research leaves traces on the user system that could betray browsing details; the other browsers maintain much better privacy, according to a report published in the *International Journal of Electronic Security and Digital Forensics*.

Cassandra Flowers, a Specialised Systems Support and Development Manager at the Babraham Research Campus, in Cambridge, and colleagues Ali Mansour and Haider Al-Khateeb of the Department of Computer Science and Technology, University of Bedfordshire, Luton, England, explain how private or "incognito" modes in web browsers prevent a barrier to forensic investigation of a user's web browsing habits. All the popular web browsers offer such a mode that automatically deletes the browser cache, cookies, downloaded files list, and browser history when the user exits the program. However, whether or not all data is deleted beyond forensic recovery is a moot point.

Now, the team has demonstrated that forensic analysis can still retrieve traces of data from an "InPrivate" browser session for one of the most commonly used applications, Microsoft's Internet Explorer. " We analyse volatile memory and demonstrate how physical memory by means of dump files, hibernate and page files are the key areas where evidence from all browsers will still be recoverable despite their mode or location they run from," the team reports.

During an InPrivate browser session using Internet Explorer version 11 the program added .dat files to the Recovery directory as it would during a normal session, which allows recovery after a computer or software crash. It also heavily utilised the LowContent.IE5 directory to cache files during InPrivate browsing, the team explains. They add that existing .log files in the WebCache folder were removed and new logs created in the same directory for the current session, the browser also used the "CryptnetUrlCacheContent" directory to store certificates. On closing the browser some cleanup was carried out but not all log files were deleted until a new instance of the browser was opened.

By contrast, Firefox and Opera undertook very little hard drive activity during private browsing, most of the constant hard drive activity in Chrome was down to plugin actions. All the browsers left some file modifications that might be extracted through detailed analysis of the computer hard drive or USB stick. However in "portable" private mode none of these browsers left artefacts and all files were cleaned from the USB stick from which the browser was being run. Even in this mode it was possible to retrieve cached Internet Explorer files that closing the InPrivate session that left behind.

"Web browser claims that browsing history will not be recoverable in private modes may prevent an average computer user from finding evidence, but using forensic techniques plenty of evidence was recoverable which may prove to be crucial to a forensic investigation," the team reports, which suggests the unwary criminal might be caught through this evidential trail. Conversely, third parties spying on an everyday user could retrieve information about that user even from private modes. In addition, the team adds that, "It is also crucial for internet users to learn that browsers security does not make them anonymous when their network is monitored by an internet service provider or a network administrator at the workplace."

More information: Flowers, C., Mansour, A. and Al-Khateeb, H.M. (2016) 'Web browser artefacts in private and portable modes: a forensic investigation', *Int. J. Electronic Security and Digital Forensics*, Vol. 8, No. 2, pp.99–117.

Provided by Inderscience Publishers

APA citation: How private is your browser's privacy mode? (2016, February 18) retrieved 18 November 2019 from https://phys.org/news/2016-02-private-browser-privacy-mode.html