

Random Cookie Names

As forensic examiners will be aware, Microsoft Internet Explorer stores cached data within randomly assigned folders. This behaviour was designed to prevent Internet data being stored in predictable locations on the local system in order to foil a number of attack types. Prior to the release of Internet Explorer v9.0.2, cookies were an exception to this behaviour and their location was insufficiently random in many cases.

Cookie Files

Generally, for Vista and Windows 7, cookie files are stored in the location shown below:

Microsoft Windows Internet Explorer Cookie Location
<code>\AppData\Roaming\Microsoft\Windows\Cookies\</code>

The cookie filename format was the user's login name, the @ symbol and then a partial Hostname for the domain of the cookie.

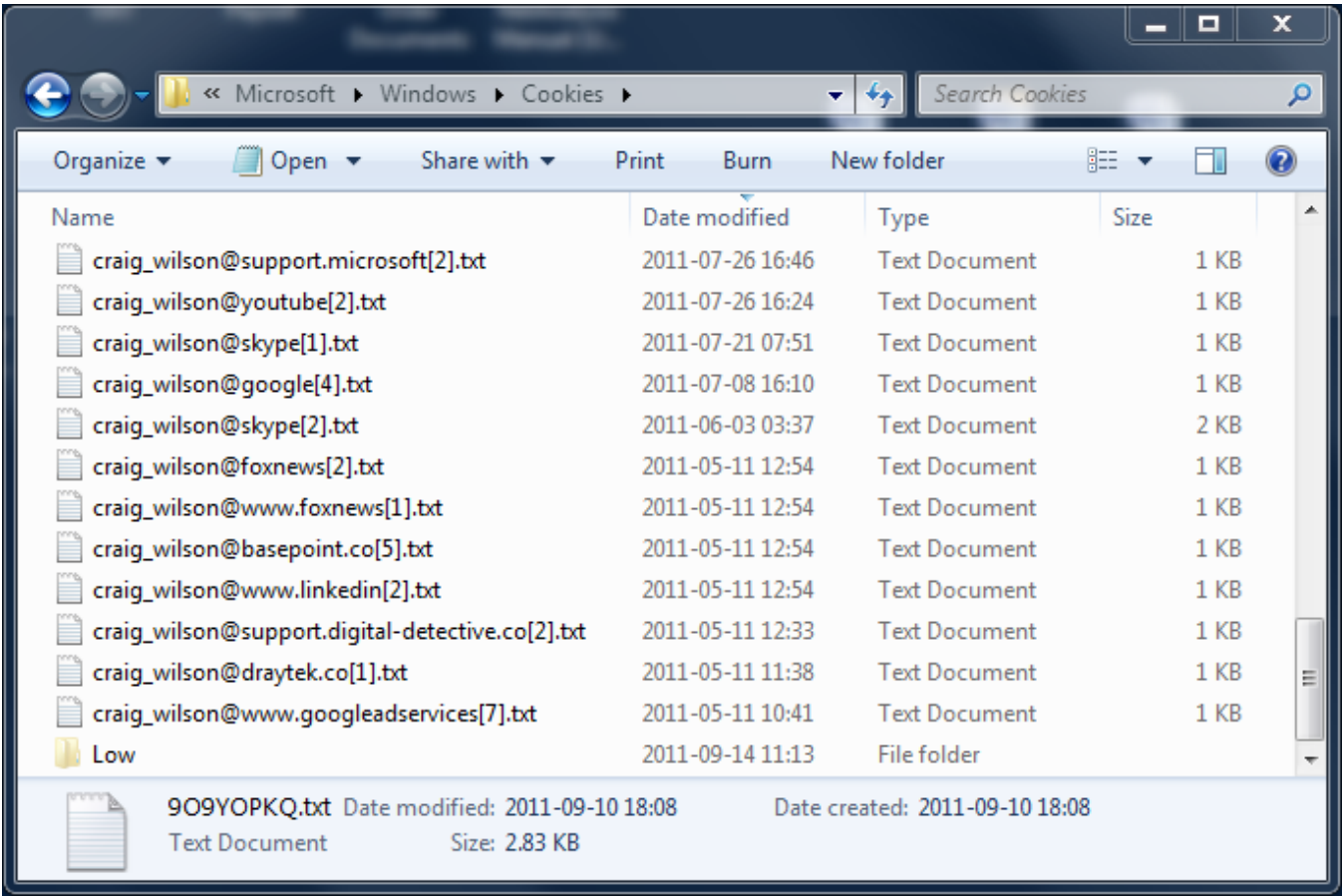


Figure 1

With sufficient information about a user's environment, an attacker might have been able to establish the location of any given cookie and use this information in an attack. To mitigate the threat, Internet Explorer 9.0.2 now names the cookie files using a randomly-generated alphanumeric string. Older cookies are not renamed during the upgrade, but are instead renamed as soon as any update to the cookie data occurs. Figure 2 shows an updated cookie folder containing the new files.

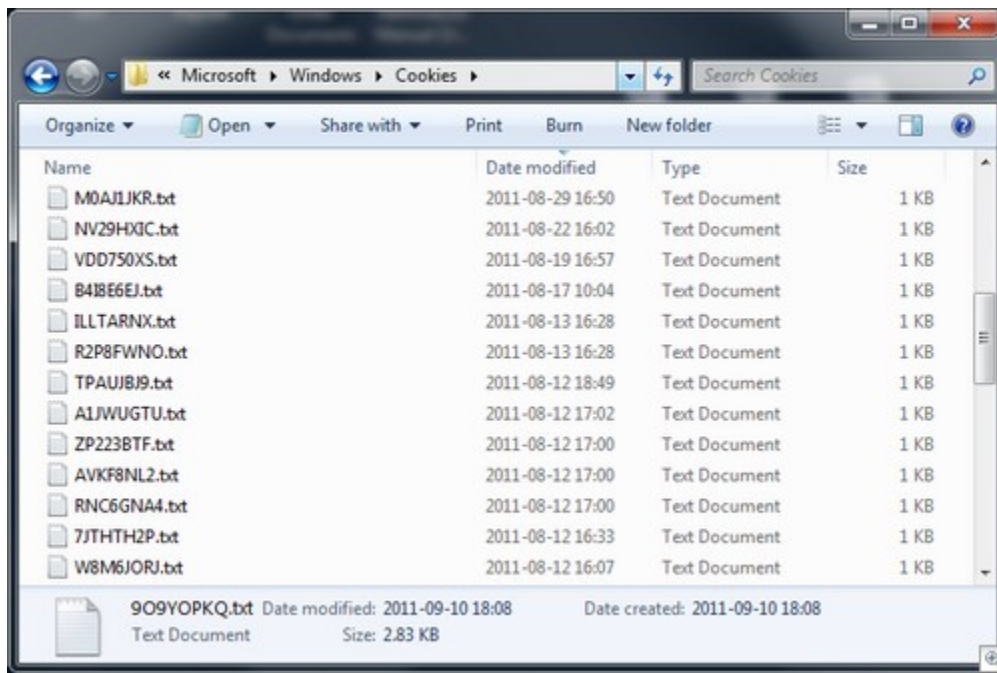


Figure 2

This change will have no impact on dealing with the examination of cookie data. It will obviously no longer be possible to identify which domain a cookie belongs to from just the file name.

NetAnalysis v1.53 - Forensic Internet History Analysis

File Filter Searching Tools Bookmarks Reports Audit View Column Help

GMT Standard Time [UTC +0000]

Key	Value	Host	Secure	Last Modified Date [UTC]	Last Modified Date [Local]	Expiration Date [UTC]
✓ SITESERVER	ID=6221688df0434ecdb1505b6ecc5fd29a	dell.com/	False	2011-08-12 08:16:43 Fri	2011-08-12 09:16:43 Fri	2016-08-12 08:16:44 Fri

Type	Last Visited [UTC]	Last Visited [Local]	Hits	Cache File	Extension	Length	Exists	Date Expiration [UTC]
cookie	2011-09-10 17:18:10 Sat	2011-09-10 18:18:10 Sat	5	2ISSQICR.txt	.txt	223	✓	2021-08-12 11:36:34 Thu
cookie	2011-09-06 14:41:17 Tue	2011-09-06 15:41:17 Tue	4	SHMCSOEQ.txt	.txt	103	✓	2016-08-12 08:16:44 Fri
cookie	2011-09-12 13:43:11 Mon	2011-09-12 14:43:11 Mon	1225	7JTHTH2P.txt	.txt	315	✓	2013-08-11 15:02:52 Sun
cookie	2011-08-31 06:38:11 Wed	2011-08-31 07:38:11 Wed	1	7RZJHMB8.txt	.txt	114	✓	2011-08-31 06:43:16 Wed
cookie	2011-09-10 17:18:10 Sat	2011-09-10 18:18:10 Sat	16	7YV1Z0J.txt	.txt	609	✓	2021-09-02 17:25:48 Thu
cookie	2011-09-07 08:04:04 Wed	2011-09-07 09:04:04 Wed	2	90X4T0VH.txt	.txt	93	✓	2031-09-02 08:04:08 Tue
cookie	2011-09-14 06:51:19 Wed	2011-09-14 07:51:19 Wed	339	909YOPKQ.txt	.txt	2898	✓	2041-05-10 09:30:40 Fri
cookie	2011-08-12 13:48:53 Fri	2011-08-12 14:48:53 Fri	38	9V6AWCGX.txt	.txt	990	✓	2012-02-08 13:48:56 Wed
cookie	2011-08-12 16:02:09 Fri	2011-08-12 17:02:09 Fri	15	A1JWUGTU.txt	.txt	96	✓	2012-08-11 16:02:12 Sat
cookie	2011-08-28 09:52:03 Sun	2011-08-28 10:52:03 Sun	254	AWKF8NL2.txt	.txt	685	✓	2013-08-12 16:00:00 Mon
cookie	2011-08-17 09:04:09 Wed	2011-08-17 10:04:09 Wed	2	B4I8E6EJ.txt	.txt	105	✓	2035-01-01 00:00:00 Mon
cookie	2011-09-05 13:31:28 Mon	2011-09-05 14:31:28 Mon	19	EI2S4C3Q.txt	.txt	176	✓	2012-09-04 13:31:28 Tue
cookie	2011-08-12 15:59:54 Fri	2011-08-12 16:59:54 Fri	4	H23DPRZR.txt	.txt	114	✓	2016-08-10 13:47:24 Wed
cookie	2011-09-14 06:49:33 Wed	2011-09-14 07:49:33 Wed	58	HC4JQWIEQ.txt	.txt	109	✓	2016-08-10 14:02:30 Wed
cookie	2011-08-30 14:06:41 Tue	2011-08-30 15:06:41 Tue	5	I27C2T8K.txt	.txt	353	✓	2013-08-29 14:06:10 Thu
cookie	2010-09-05 01:05:59 Sun	2010-09-05 02:05:59 Sun	7	IFNYT5QM.txt	.txt	270	✓	2013-09-03 13:46:42 Tue
cookie	2011-08-13 15:28:12 Sat	2011-08-13 16:28:12 Sat	2	ILLTARNX.txt	.txt	196	✓	2021-08-10 15:28:16 Tue
cookie	2011-08-12 08:58:08 Fri	2011-08-12 09:58:08 Fri	2	J78AROMD.txt	.txt	106	✓	2011-08-13 08:58:10 Sat
cookie	2011-08-12 13:55:36 Fri	2011-08-12 14:55:36 Fri	59	JPYEBNOM.txt	.txt	182	✓	2011-09-11 13:48:56 Sun
cookie	2011-08-30 16:35:07 Tue	2011-08-30 17:35:07 Tue	17	JX8DLUNQ.txt	.txt	90	✓	2012-08-12 14:02:34 Sun
cookie	2011-09-02 13:54:32 Fri	2011-09-02 14:54:32 Fri	7	M0AJ1JKR.txt	.txt	111	✓	2011-10-28 15:50:20 Fri
cookie	2011-09-07 14:33:07 Wed	2011-09-07 15:33:07 Wed	6	N2IPM5ZD.txt	.txt	101	✓	2011-09-07 22:36:58 Wed
cookie	2011-08-12 13:48:53 Fri	2011-08-12 14:48:53 Fri	51	NP5J20Y4.txt	.txt	110	✓	2011-09-11 13:48:56 Sun

www.digital-detective.co.uk TAG Filter Cookie C:\Users\Craig Wilson\Desktop\Cookies\index.dat FO: 30720 URL Records: 40

Figure 3

Figure 3 shows NetAnalysis displaying the new format cookies.