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	
\AppData\Roaming\Microsoft\Windows\Cookies\	

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

			_		x			
🕞 💭 🚽 🐇 « Microsoft 🕨 Windows 🕨 Cookies 🕨 🛛 👻 🤟 Search Cookies								
Organize 👻 🦳 Open 👻 Share with 👻	Print Burn M	New folder			?			
Name	Date modified	Туре	Size					
craig_wilson@support.microsoft[2].txt	2011-07-26 16:46	Text Document		1 KB				
craig_wilson@youtube[2].txt	2011-07-26 16:24	Text Document		1 KB				
craig_wilson@skype[1].txt	2011-07-21 07:51	Text Document		1 KB				
📄 craig_wilson@google[4].txt	2011-07-08 16:10	Text Document		1 KB				
craig_wilson@skype[2].txt	2011-06-03 03:37	Text Document		2 KB				
craig_wilson@foxnews[2].txt	2011-05-11 12:54	Text Document		1 KB				
craig_wilson@www.foxnews[1].txt	2011-05-11 12:54	Text Document		1 KB				
craig_wilson@basepoint.co[5].txt	2011-05-11 12:54	Text Document		1 KB				
craig_wilson@www.linkedin[2].txt	2011-05-11 12:54	Text Document		1 KB				
craig_wilson@support.digital-detective.co[2].txt	2011-05-11 12:33	Text Document		1 KB	1			
📄 craig_wilson@draytek.co[1].txt	2011-05-11 11:38	Text Document		1 KB				
craig_wilson@www.googleadservices[7].txt	2011-05-11 10:41	Text Document		1 KB				
low	2011-09-14 11:13	File folder						
909YOPKQ.txt Date modified: 2011-09-10 Text Document Size: 2.83 KB) 18:08 Date c	reated: 2011-09-10 18:	08					

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.

🖌 🖉 🎍 « Microsoft 🕨 Windows 🕨	COUNES P	Search Cook	153	-	3
Organize 🔻 🥘 Open 👻 Share wit	h 🔻 Print Burn	New folder	. ≡		0
Name	Date modified	Туре	Size		
M0AJ1JKR.txt	2011-08-29 16:50	Text Document		1 KB	
NV29HXIC.bt	2011-08-22 16:02	Text Document		1 KB	
VDD750XS.txt	2011-08-19 16:57	Text Document		1 KB	
B418E6EJ.bt	2011-08-17 10:04	Text Document		1 KB	
ILLTARNX.txt	2011-08-13 16:28	Text Document		1 KB	
R2P8FWNO.txt	2011-08-13 16:28	Text Document		1 KB	
TPAUJBJ9.6d	2011-08-12 18:49	Text Document		1 KB	a
A1JWUGTU.txt	2011-08-12 17:02	Text Document		1 KB	
ZP223BTF.txt	2011-08-12 17:00	Text Document		1 KB	
AVKF8NL2.bt	2011-08-12 17:00	Text Document		1 KB	
RNC6GNA4.txt	2011-08-12 17:00	Text Document		1 KB	
7JTHTH2P.bt	2011-08-12 16:33	Text Document		1 KB	
W8M6JORJ.txt	2011-08-12 16:07	Text Document		1 KB	

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.

🗰 🖬 🖡		i 🕰 📊 🙀 🕅 🐂 🗌	🗐 🖗 🖹 🕼 🛠 🕐								GMT Standard Time [UTC +00
Key		Value			Host	Secure	Last Mo	dified Date [UT(] Last Modi	fied Date [Local]	Expiration Date [UTC]
SITESER	VER	ID=6221688df0434ecdb1505	b6ecc5fd29a		dell.com/	False		8-12 08: 16:43 F		12 09: 16: 43 Fri	2016-08-12 08:16:44 Fri
Туре		Last Visited [UTC]	Last Visited [Local]	Hits	Cache File		L	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	4	2021-08-12 11:36:34 Thu
🏐 cookie		2011-09-06 14:41:17 Tue	2011-09-06 15:41:17 Tue	4	5HMCSOEQ.txt			.txt	103	4	2016-08-12 08:16:44 Fri
🍪 cookie	M	2011-09-12 13:43:11 Mon	2011-09-12 14:43:11 Mon	1225	7JTHTH2P.txt			.txt	315	4	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	4	2011-08-31 06:43:16 Wed
🍪 cookie	V	2011-09-10 17:18:10 Sat	2011-09-10 18:18:10 Sat	16	7YYV1Z0J.txt			.txt	609	4	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	4	2031-09-02 08:04:08 Tue
🎲 cookie		2011-09-14 06:51:19 Wed	2011-09-14 07:51:19 Wed	339	9O9YOPKQ.txt			.txt	2898	4	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	4	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	4	2012-08-11 16:02:12 Sat
🍪 cookie		2011-08-28 09:52:03 Sun	2011-08-28 10:52:03 Sun	254	AVKF8NL2.txt			.txt	685	4	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	4	2035-01-01 00:00:00 Mon
🍪 cookie		2011-09-05 13:31:28 Mon	2011-09-05 14:31:28 Mon	19	EIZS4C3Q.txt			.txt	176	4	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	4	2016-08-10 13:47:24 Wed
🔋 cookie		2011-09-14 06:49:33 Wed	2011-09-14 07:49:33 Wed	58	HC4JQWEQ.txt			.txt	109	4	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	4	2013-08-29 14:06:10 Thu
🎲 cookie	V	2010-09-05 01:05:59 Sun	2010-09-05 02:05:59 Sun	7	IFNYT5QM.txt			.txt	270	4	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	4	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	4	2011-08-13 08:58:10 Sat
🎲 cookie	M	2011-08-12 13:55:36 Fri	2011-08-12 14:55:36 Fri	59	JPYEBNCM.txt			.txt	182	4	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	4	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	4	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	4	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	4	2011-09-11 13:48:56 Sun

Figure 3

Figure 3 shows NetAnalysis displaying the new format cookies.