

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Definitions and History	1
1.2	Motivation	4
<b>2</b>	<b>Getting There</b>	<b>9</b>
2.1	Installation	9
2.1.1	Explicit, Voluntary Installation	9
2.1.2	Drive-by Downloads, User Involvement	10
2.1.3	Drive-by Downloads, No User Involvement	16
2.1.4	Installation via Malware	19
2.2	Startup	20
2.2.1	Application-Specific Startup	20
2.2.2	GUI Startup	21
2.2.3	System Startup	22
2.2.4	Kernel Startup	22
2.2.5	Defenses	23
<b>3</b>	<b>Staying There</b>	<b>29</b>
3.1	Avoiding Detection	29
3.1.1	Basic Detection Avoidance	29
3.1.2	Anti-Spyware	32
3.1.3	Advanced Detection Avoidance: Rootkits	33
3.2	Avoiding Uninstall	37
3.2.1	Passive Avoidance	37
3.2.2	Active Avoidance	38
<b>4</b>	<b>Keylogging</b>	<b>45</b>
4.1	User Space Keylogging	47
4.1.1	Polling	47
4.1.2	Event Copying	48
4.1.3	Event Monitoring	48

4.2	User Space Keylogging Defenses .....	49
4.3	Authentication .....	53
<b>5</b>	<b>Phoning Home .....</b>	<b>59</b>
5.1	Push vs. Pull .....	59
5.2	Finding Home .....	61
5.3	Steganography .....	63
5.4	Information Leaking Defenses .....	66
<b>6</b>	<b>Advertising .....</b>	<b>71</b>
6.1	Types of Advertisement .....	71
6.1.1	Banner Advertisement .....	74
6.1.2	Banner Advertisement with Pull-down Menu .....	75
6.1.3	Expandable Banner Advertisement .....	76
6.1.4	Pushdown Banner Advertisement .....	77
6.1.5	Pop-up Advertisement .....	77
6.1.6	Pop-under Advertisement .....	78
6.1.7	Floating Advertisement .....	79
6.1.8	Tear-back Advertisement .....	79
6.1.9	In-text Advertisement .....	80
6.1.10	Transition Advertisement .....	81
6.1.11	Video Advertisements .....	82
6.2	Intent and Content .....	83
<b>7</b>	<b>Advertisement Implementation .....</b>	<b>91</b>
7.1	Implementation Location .....	92
7.1.1	Implementation on the User Machine .....	92
7.1.2	Implementation in the Network .....	96
7.1.3	Implementation near the User Machine .....	97
7.1.4	Implementation on the Server .....	98
7.2	Choosing Keywords .....	99
7.3	Blocking Advertisements .....	101
7.3.1	Pop-up Blocking .....	101
7.3.2	General Advertisement Blocking .....	102
7.3.3	Blocker Evasion and Blocker Blocking .....	103
<b>8</b>	<b>Tracking Users .....</b>	<b>111</b>
8.1	Cookies .....	111
8.1.1	Defenses .....	116
8.1.2	Other Browser-Related Tracking Methods .....	117
8.2	User Profiling .....	118
8.2.1	Cognitive Styles, Mood, and Personality .....	119
8.2.2	Future Actions .....	119
8.2.3	Demographic Information .....	120
8.2.4	Social Networks .....	120
8.2.5	Real World Activities .....	121

8.2.6	Physical Location .....	121
8.2.7	Search Terms and Keywords .....	122
8.2.8	Disinterests .....	122
<b>9</b>	<b>Conclusion .....</b>	<b>127</b>
	<b>References .....</b>	<b>129</b>
	<b>Index .....</b>	<b>143</b>



<http://www.springer.com/978-0-387-77740-5>

Spyware and Adware

Aycock, J.

2011, XIV, 146 p., Hardcover

ISBN: 978-0-387-77740-5