SPIS TREŚCI

Słowo wstępne. Jeszcze możemy odzyskać kontrolę (*Katarzyna Szymielewicz*) 5

Podziękowania 19

Wprowadzenie 23

Część I TERMINOLOGIA ZACIEMNIANIA

1. Podstawowe przypadki 35
   - 1.1 Zasłona: jak pokonać wojskowy radar 35
   - 1.2 Bot w Twitterze: zapełnianie kanału szumem 37
   - 1.3 CacheCloak: usługi lokalizacyjne bez śledzenia lokalizacji 44
   - 1.4 TrackMeNot: wymieszanie autentycznych i fikcyjnych wyszukań 46
   - 1.5 Przesyłanie informacji na strony z przeciekami: zakopywanie ważnych plików 49
   - 1.6 Fałszywe telle: tworzenie wzorów w celu oszukania wyszkolonego obserwatora 51

1.7 Tożsamość grupowa: wiele osób pod tym samym nazwiskiem. 52
1.8 Identyczność: wiele osób w identycznym stroju. 53
1.9 Nadprodukcja dokumentacji: utrudnianie analizy 56
1.10 Przetasowywanie kart SIM: wprowadzenie elementu niepewności do namierzania celów za pomocą danych mobilnych 57
1.11 Przekierowania przez Tor: żądania w imieniu innych, które pozwalają na ukrycie własnej aktywności. 60
1.12 Taśmy z bełkotem: chowanie mowy w mowie 63
1.13 Operacja Vula: zaciemnianie w walce z apartheidem 64

2. Inne przykłady 73
2.1 Pająki: zaciemniające zwierzęta 73
2.2 Fikcyjne zamówienia: zaciemnianie w walce z konkurencją w biznesie 74
2.3 Fikcyjne stanowiska radarowe: francuska wojna z antyradarami 75
2.4 AdNauseam: klikanie we wszystkie reklamy 77
2.5 *Quote stuffing*: zaburzanie strategii algorytmów giełdowych 78

2.6 Wymiana kart lojalnościowych w celu zaburzenia analizy zachowań konsumenckich. 80
2.7 BitTorrent Hydra: fałszywe żądania w celu utrudnienia gromadzenia adresów. 83
2.8 Celowo nieprecyzyjny język: zaciemniający styl. 85
2.9 Zaciemnianie anonimowego tekstu: zapobieganie analizie stylometrycznej. 86
2.10 Zaciemnianie kodu: zbijanie z tropu ludzi, ale nie maszyn. 91
2.11 Indywidualna dezinformacja: strategie jednostkowego znikania. 94
2.12 Patent Apple'a na „usługę klonowania": zanieczyszczyć profilowanie elektroniczne 96
2.13 Vortex: zaciemnianie ciasteczek jako gra i rynek. 99
2.14 „Bayesowska powódź" i uczynienie internetowej tożsamości „niesprzedawalną" 102
2.15 FaceCloak: ukrywać proces ukrywania 104
2.16 Zaciemnione farmy lajków: ukrywanie oznak manipulacji. 105
2.17 Inwigilacja URME: „protezy tożsamości" jako wyraz protestu. 106
2.18 Produkowanie sprzecznych dowodów: gmatwanie śledztwa 107

Część II ZROZUMIEĆ ZACIEMNIANIE

3. Dlaczego zaciemnianie jest konieczne? 113
3.1 Zaciemnianie pokrótce. 113
3.2 Zrozumienie asymetrii informacyjnej: wiedza i władza. 121
3.3 Iluzja życia poza systemem 132
3.4 Narzędzia walki słabych: w czym może pomóc zaciemnianie? 136
3.5 Jak odróżnić zaciemnianie od mocnych systemów ochrony prywatności? 143
3.5.1 A może to na prywatnych firmach powinien spoczywać obowiązek stosowania praktyk najkorzystniejszych dla ich klientów? 146
3.5.2 A może powinniśmy oczekiwać od władz, że uchwalą lepsze przepisy i wymuszą ich stosowanie? 149
3.5.3 A może sytuację naprawią bardziej zaawansowane technologie? 151

4. Czy zaciemnianie jest usprawiedliwione? 155
4.1 Etyka zaciemniania. 157
4.1.1 Nieuczciwość 157
4.1.2 Marnotrawstwo 159
4.1.3 Życie na cudzy koszt 163
4.1.4 Zanieczyszczanie danych, działalność wywrotowa i niszczenie systemu 168

4.2 Od etyki do polityki 171
4.2.1 Cele i środki 171
4.2.2 Sprawiedliwość i uczciwość 180
4.2.3 Sprawiedliwość informacyjna oraz asymetrie władzy i wiedzy 188
4.2.4 Dla dobra innych 193
4.2.5 Ryzyko i dane 196
4.2.6 Podsumowanie 197

5. Czy zaciemnianie będzie skuteczne? 199

5.1 Zaciemnianie dotyczy celów 201
5.2 Chciałbym wykorzystać zaciemnianie do... 206
5.2.1 ...gry na zwłokę 208
5.2.2 ...uzyskania osłony 209
5.2.3 ...odmowy ponoszenia odpowiedzialności 210
5.2.4 ...uniknięcia zdemaskowania 210
5.2.5 ...zaburzania profilowania 211
5.2.6 ...wyrażania protestu. 212
5.3 Czy moje zaciemnianie jest projektem… . . . 213
5.3.1 ...indywidualnym czy kolektywnym? 213
5.3.2 ...jawnym czy niejawnym? 215
5.3.3 ...jednostkowym czy ogólnym? 217
5.3.4 ...krótko- czy długoterminowym? 220

Epilog. 225

Bibliografia 229