Uczmy się od rosyjskich szpiegów!

4 lipca 2010

W ciągu ostatnich kilku dni agenci FBI aresztowali 11 rosyjskich szpiegów działających na terenie USA. Siatka zdemaskowanych agentów obcego wywiadu była ponoć świetnie wyszkolona i przygotowana do pełnienia typowych szpiegowskich zadań. Jako że, jak na typowych szpiegów przystało, w grę wchodziły najnowsze technologie, cała sprawa jest świetną okazją do przyjrzenia się narzędziom informatycznym stosowanym przez rosyjskich agentów. Okazuje się, że agenci popełnili szereg błędów i nie zadbali wystarczająco o zabezpieczenie własnej komunikacji oraz gromadzonych danych.

Z obszernych informacji publikowanych na temat całej sprawy przez różne anglojęzyczne media, dowiadujemy się między innymi wielu szczegółów na temat działalności 28-letniej Anny Chapman, jednej z zatrzymanych rosyjskich agentek.

Okazuje się, że Anna przekazywała zbierane przez siebie informacje przedstawicielom rosyjskich władz w trakcie dyskretnych spotkań w księgarniach oraz kawiarniach na nowojorskim Manhattanie. Co ciekawe, nie dochodziło jednak do typowego spotkania. Cała komunikacja odbywała się na odległość poprzez zestawiane na tę okazję połączenie typu ad hoc Wi-Fi. Dzięki temu, agenci FBI byli prawdopodobnie w stanie przechwytywać komunikację, śledząc zawsze te same adresy MAC poszczególnych urządzeń. Ostatecznie jednemu z agentów FBI udającemu przedstawiciela władz rosyjskich udało się przechwycić przenośny komputer należący do Chapman.

Rosyjscy szpiedzy zostali wyposażeni przez Służbę Wywiadu Zagranicznego Rosji w specjalnie przygotowane, niedostępne na rynku oprogramowanie steganograficzne. Szpiedzy pobierali ze specjalnie do tego celu przygotowanych witryn pliki graficzne,

zawierające ukryty przekaz. Agentom FBI udało się przechwycić ponad sto tego typu plików, z niektórych udało się wydobyć ukryte w nich pliki tekstowe. Co najciekawsze, amerykańskim służbom śledczym udało się odczytać zawartość przechwyconych dysków twardych pochodzących z komputerów rosyjskich szpiegów. Wszystkie dyski były zaszyfrowane, jednak agenci FBI poradzili sobie i z tym problemem, o czym za chwilę.

Zgodnie z ustaleniami FBI, w taki oto sposób rosyjscy szpiedzy przez wiele lat zbierali i przekazywali do Moskwy informacje na temat amerykańskiej broni jądrowej, ekonomii oraz wielu innych aspektów życia publicznego.

Jak się więc okazuje, od rosyjskich szpiegów możemy się nauczyć tego w jaki sposób nie należy zabezpieczać swej komunikacji oraz danych.

Przede wszystkim wątpliwości budzi zastosowanie połączenia typu ad hoc Wi-Fi. Tego typu rozwiązanie pozwala jedynie na zastosowanie szyfrowania WEP, co jest zabezpieczeniem niewystarczającym. Pewnym rozwiązaniem tego problemu mogłoby się okazać wykorzystanie oprogramowania komunikacyjnego dodatkowo szyfrującego przesyłane dane. Wygląda również na to, że niezmienność stosowanych przez szpiegów adresów MAC (które przecież w prosty sposób można zazwyczaj zmieniać) ułatwiła amerykańskim agentom śledzenie nawiązywanych połączeń.

Uzyskanie dostępu do danych zgromadzonych na zaszyfrowanych silnymi algorytmami szyfrującymi dysków twardych wymagało podania 27-znakowego hasła. Jednak i z tym agenci FBI sobie poradzili! W trakcie potajemnego przeszukania domu jednego ze szpiegów, odkryto kartkę papieru z zapisanym na niej długim ciągiem rozmaitych znaków. Ostatecznie okazało się, że było to właśnie hasło do zaszyfrowanych dysków. Widzimy więc po raz kolejny, że stosowanie zbyt skomplikowanych haseł prowadzi jedynie do ich… zapisania na kartce papieru. Jeśli już więc mamy problemy z zapamiętaniem skomplikowanych haseł, zapiszmy je na żółtej karteczce w taki sposób, by jej przechwycenie nie

pozwoliło na odczytanie klucza. Warto również zauważyć, że przeszukania pod nieobecność podejrzanych są jednak przez niektóre służby śledcze praktykowane.

Stosowana przez rosyjskich szpiegów steganografia w formie ukrywania plików tekstowych wewnątrz plików graficznych może być świetnym sposobem na ukrycie pewnych treści w publicznie dostępnych zbiorach. Jak jednak uczy nas przykład zdemaskowanych rosyjskich agentów, tego rodzaju zabezpieczenia nie powstrzymają jednak poważnych służb śledczych przed odnalezieniem drugiego dna w naszych plikach.

W całej spawie zaskakuj jeszcze jedno. Czy w dobie satelitów szpiegowskich, bezzałogowych samolotów, Internetu oraz ataków hakerskich zdolnych do zinfiltrowania najlepiej strzeżonych systemów komputerowych, potrzebni są jeszcze w ogóle typowi szpiedzy? Okazuje się jednak, że służby wywiadowcze nadal cenią sobie bardziej dane wywiadowcze gromadzone w sposób klasyczny.

Co również jest dość interesujące, Anna Chapman prowadziła dość bujne życie online. Na koniec spójrzmy więc na materiał video oraz kilka zdjęć pochodzących z jej Facebooka. Czy odgadlibyście, że ta sympatyczna pani, to prawdziwy rosyjski szpieg?

Autor: \m/ojtek
Na podstawie: newyork.fbi.gov
Źródło: Hard Core Security Lab