Jak odzyskać (złamać) hasło do woluminu TrueCrypta?

14 lutego 2011

Szyfrowanie naszych danych z wykorzystaniem programów takich jak popularny TrueCrypt, może stanowić dla naszych sekretów bardzo skuteczną ochronę. Zastosowanie silnego szyfrowania wraz z odpowiednio silnym hasłem, może być nie lada wyzwanie dla organów ścigania poszukujących cyfrowych dowodów. Oczywiści w razie zapomnienia hasła, TrueCrypt powstrzyma przed dostępem do danych również uprawnionego właściciela informacji. Jak się jednak okazuje, odzyskanie (złamanie) hasła broniącego dostępu do zaszyfrowanego woluminu czasem jest jednak jak najbardziej wykonalne, a potrzebne do tego narzędzia są ogólnie dostępne. Spójrzmy na mały praktyczny przykład.

Załóżmy, że chcielibyśmy odzyskać (złamać) hasło broniące dostępu do pewnego testowego woluminu (TC_test) utworzonego za pomocą domyślnych ustawień TrueCrypta. Hasło dostępowe stanowi następująca względnie silna fraza:

45m0d3u52@!

W celu przeprowadzenia naszego eksperymentu skorzystamy z mało znanego programu TCBrute 2.5, który to znajduje się nadal w bardzo wczesnej fazie rozwojowej, jednak już pozwala na wykonania powyższego przykładowego zadania. TCbrute wbrew swej nazwie nie pozwala na przeprowadzania automatycznych ataków siłowych, a jedynie wspiera ataki słownikowe. Musimy więc przygotować sobie słownik potencjalnych haseł.

Dla uproszczenia, słownik wygenerowałem za pomocą programu Common User Passwords Profiler, z zachowaniem tych samych zasad co we wpisie Oto program, który jest w stanie odgadnąć twoje hasła! Założyłem więc, że dysponujemy pewną wiedzą o właścicielu hasła i na tej podstawie z pomocą programu CUPP

powstał słownik zawierający 23892 hasła (słownik można pobrać TUTAJ). Teraz pozostaje nam już tylko skonfigurować TCBrute'a (wskazujemy plik z woluminem oraz słownik z hasłami):

Już po kilku minutach właściwe hasło zostało odnalezione:

Prędkość TCBrute'a nie zachwyca. Udało mi się osiągnąć góra kilkadziesiąt prób na sekundę. W praktyce wyklucza to więc poważne ataki polegające na sprawdzaniu wszystkich możliwych kombinacji dłuższych haseł. Z drugiej jednak strony, taka prędkość spokojnie pozwala na sprawdzenie słownika zawierającego kilkadziesiąt lub nawet kilkaset tysięcy haseł w całkiem rozsądnym czasie. W obecnej wersji program jest już w stanie rozłożyć obliczenia na wiele w pełni niezależnych wątków, dzięki czemu wielordzeniowe procesory/systemy powinny nam pozwolić na spore przyspieszenie całego procesu.

Jaki z tego wszystkiego płynie wniosek? TCbrute i podobne rozwiązania nie mogą oczywiście zagrozić bardzo silnym i z niczym nie kojarzącym się hasłom. Jeśli jednak nasze hasło stanowi fraza znane ze słowników haseł typowych, jest podobne do innych naszych haseł wykorzystywanych w różnych systemach informatycznych lub też kojarzy się z jakimiś informacjami ogólnie dostępnymi na nasze temat, to TCbrute z pewnością może posłużyć intruzowi do przeprowadzenia całkiem skutecznego ataku. Pamiętajmy również zawsze, że typowe ataki słownikowe to nie jedyne metody odzyskiwania haseł do zaszyfrowanych danych. Inne całkiem proste ataki mogą się okazać zabójczo skuteczne.

Oczywiście TCbrute może się również okazać przydatny osobom, które zapomniały hasła do własnego woluminu. Na podstawie dostępnych wspomnień hasła oraz znajomości własnych nawyków związanych z tworzeniem haseł, będziemy mogli w takim przypadku przygotować sobie słownik, który przy odrobinie szczęścia pozwoli nam na odzyskanie utraconego dostępu do własnych danych. W jednym i drugim przypadku warto jednak

przede wszystkim zdawać sobie sprawę, że narzędzia pozwalające na słownikowe ataki na TrueCrypta istnieją i są ogólnie dostępne.

Autor: \m/ojtek
Źródło: Hard Core Security Lab