Foto: pexels.com

Sprucie hasła „1234” trwało coś około doby. Jeśli mam być szczery, mocno mnie to zaskoczyło. Musiałem wykonać kilka prób, aby przekonać się, że program o wdzięcznej nazwie John the Ripper faktycznie działa.

Miałem powody do zdziwienia. Komputer z procesorem 3,5 GHz, łamanie w tzw. trybie słownikowym, które w teorii powinno dać wynik natychmiast. Podpiąłem słownik – drobne 15 GB. To „1234” należy podobno do jednych z najczęściej stosowanych głupich haseł. A jednak…

Sprawdziłem. Naprawdę szybko program znajduje hasła, które są tworzone na bazie danych do logowania. Konto „jasio” – hasło „jasio” pada natychmiast, co prawda wymaga to uruchomienia programu w odpowiednim trybie, ale hackarz to umie. Na to trzeba naprawdę uważać, przy tworzeniu konta system (diabli wiedzą po co) wymaga wpisania szeregu danych, które potem figurują w plikach odpowiedzialnych za logowanie. Jeśli jako hasła użyjemy którejkolwiek z tych danych, choćby zmodyfikowanej (np. „jAcio”), to leżymy.

Aliści spokojnie. Kiedy w ogóle hackarz „pruje” hasła? Gdy na skutek różnych tajemnych knowań uzyska dostęp do całego dysku, także obszaru systemu. To się zdarza na wielkich serwisach, dla komputera domowego taki przypadek stanowi kuriozum. Dlaczego hasła trzeba „pruć” i co w ogóle robi ów John the Ripper? Hasła są zapisywane w pamięci komputera w postaci tzw. „haszy”. Logowanie przebiega tak, że po wklepaniu naszego tajnego zaklęcia otwierającego system jest ono przekształcane przez tzw. funkcję jednokierunkową. To operacja, dla której nie znamy odwrotnej. Dostajemy długi, chaotyczny ciąg znaków. Nie ma sposobu, by z niego odtworzyć hasło. Jeśli jest on identyczny z tym, który komputer ma zapisany w pamięci, zostajemy wpuszczeni do systemu. Oczywiście to, z czym przekształcone hasło jest porównywane, co komputer trzyma jako wzorzec, także zostało „zahashowane”, przepuszczone przez tę samą funkcję jednokierunkową.

Jeśli włamywacz przeniknie do komputera, to dostanie jedynie owe zupełnie nieczytelne, długaśne ciągi znaków. Aby mógł się zalogować na konto, musi wiedzieć, z czego powstały, bo to trzeba wpisać jako hasło. John the Ripper zna chyba wszystkie algorytmy produkujące „hasze” i próbuje znaleźć metodą prób i błędów właściwe zaklęcie. Metoda słownikowa (słynna?) jest inteligentniejsza, sprawdzamy realnie stosowane hasła, słowa i ich przekształcenia. Gdy program ma (dobry?) słownik, zaczyna od tych najpopularniejszych. Wedle opisów – „1234” powinno zostać znalezione w ciągu jakiś minut.

W końcu doczytałem się. Problem idiotycznych haseł był ćwiczony już ponoć w gdzieś w 70. latach XX wieku. Wówczas powstał jeden z pierwszych skutecznych pomysłów. Tak zwane „solenie”, haseł metoda Morrisa oraz Thompsona, rok 1979.

Są przynajmniej dwa powody, przez które łamanie haseł z dobrym słownikiem dramatycznie (może nawet dziesiątki tysięcy razy) przyspiesza pracę. Komputer wymija

kombinacje znaków, których człowiek nigdy nie użyje. Oczywiście jest ich pewnie 99,9 procenta ze wszystkich jakie można wygenerować. Powód drugi: w słowniku mamy pary hasło-hasz. Komputer nie musi wyliczać owego hasza, przez co czasami wyjątkowo skraca czas przeszukiwania.

Jeśli dodamy do hasła „sól" losowy ciąg znaków, który może być nawet znany włamywaczowi, to słownik leży. Funkcję haszującą konstruuje się tak, żeby zmiana jednego bitu danych wejściowych powodowała zmianę co najmniej ponad połowy bitów na wyjściu – jest „bardzo wrażliwa". Dodawana sól jest długa, to kilkadziesiąt znaków. Dlatego że hasze są zupełnie inne od zapisanych w słowniku. Wyłoży się także bardziej cwana wersja słownika, tzw. tęczowe tablice, które prócz haseł mają załączone reguły ich przekształcania. „Sole" są w komputerze zapisywane w jawnej postaci, ale nie zmienia to ich skuteczności.

Już ładnych parę lat temu kryptolodzy spotkali się z poważnym problemem w postaci ogromnej mocy obliczeniowej kart graficznych. Zawierają one dziś np. 2048 prostych procesorów. Można na nich prowadzić obliczenia równolegle. Czyli np. pobrać 2048 haszy, haseł z ukradzionej bazy, i każde nich osobno próbować złamać. Albo dla jednego hasza wypróbowywać 2048 kombinacji jednocześnie.

Oczywiście oznacza to ogromny przyrost prędkości procesu krakowania. Co prawda nie jest on wprost proporcjonalny do liczby procesorów na karcie, ale pojawił się taki problem, że moc obliczeniowa porównywalna z wielkimi komputerami znalazła się w dyspozycji tzw. zwykłego użytkownik. Powiedzmy od razu, że nie tak zwykłego, trzeba się jednak dość wysilić i wydać trochę kasy na taki klaster obliczeniowy. Mimo to trzeba było jednak coś przedsięwziąć.

W tej chwili w wielu systemach stosowany jest jest algorytm opracowany w USA przez National Security Agency z serii algorytmów nazywanych sha2 o nazwie SHA512, w którym ustawia się parametr „rounds" oznaczający liczbę przebiegów haszowania. Bierzemy hasło, wykonujemy z niego hasz, następnie z tego hasza kolejny. Tak mnóstwo razy. Cel jest prosty: zwiększyć czas wyliczania hasza na tyle, aby skompensował przyrost mocy obliczeniowej systemów zbudowanych na GPU, czyli nowoczesnych kartach graficznych. Jak wyczytałem, dla sha512 typowa wartość parametru rounds wynosi 5000 i to już załatwia problem.

Warto zauważyć, że gdyby nie solenie haseł, to ta operacja byłaby psu na budę. Słownik bowiem będzie zawierał pary hasz–hasło. Nie trzeba uruchamiać programu wyliczającego ów hasz, przeszukiwanie idzie piorunem.

Ale gdy mamy i solenie, i wielokrotne haszowanie, to znalezienie hasła „1234" trwa naprawdę dziesiątki godzin na normalnym komputerze. Połamania bazy wykradzionych haseł liczącej dziesiątki tysięcy sztuk nie może dokonać ktokolwiek.

Krótko mówiąc, eksperymentalnie się przekonałem, że i w specjalistycznych publikacjach, i w tych popularnych, pisze się bajki: nawet bardzo durne hasło w dzisiejszych czasach nie jest łatwe do przełamania.

Media nam wmawiają, że zagrożenia cybernetyczne rosną. Tyle że jeśli przyjrzeć się technicznym bebechom, to widać coś innego.

Tak, pojawiają się nowe narzędzia crakerów, jak komputery z kartami graficznymi. Lecz znajdujemy się w sytuacji, że posiadają je tylko niektórzy ludzie. To już nie może być kilkunastoletni wandal komputerowy, jak bywało jeszcze kilkanaście lat temu. Ktoś musi wyłożyć kasę, musi mieć w tym jakiś cel. A broniący się może podkręcić mocniej owo „rounds", np, razy 10, może ustawić minimalną długość hasła w systemie na kilkanaście znaków, może zmienić funkcję haszującą na nowszą. Na przykład bcrypt. Algorytm lub

program przeznaczony specjalnie do tego, by spowolnić proces haszowania. Można w nim ustawiać złożoność aż do takich wartości, że na normalnym komputerze operacja będzie trwała gdzieś około 1,5 roku. Jest tak zaprojektowany, że procesu nie da się rozbić na wiele równoległych, nie da się więc złamać algorytmu za pomocą superkomputerów NSA czy NASA albo chińskich gigantów, ponieważ i tak poszczególne procesory pracują z prędkościami bliskimi tych w domowych maszynach. Ten program może stawić czoła wszystkim komputerom na świecie połączonym w jeden klaster. Nawet jeśli ustawimy sobie głupie hasło – i tak możemy ustawić komplikację haszowania na takim poziomie, że jego łamanie będzie trwać za długo dla każdego.

Wynik mojego eksperymentu był dla człowieka znającego współczesne systemy operacyjne oczywisty. To znaczy… powinien być oczywisty. Jednak nigdzie nie przeczytałem, że to będzie tak wyglądać. Dodam, że dla eksperymentu gdzieś od półtora miesiąca próbuję złamać inne hasła, które zdawały mi się słabe. Cóż… chyba się jeszcze przydadzą.

Mogę stwierdzić, że nieprawdziwa jest często powtarzana informacja, że ze wzrostem mocy obliczeniowej musimy wprowadzać coraz bardziej skomplikowane hasła. Nie, inżynierowie znaleźli na to sposoby. Owszem, nie są do końca skuteczne, inna sprawa, ale dość skuteczne, że gdy mamy hasło trochę lepsze od „1234”, i jeśli nie nazywamy Julian Assange, prawdopodobnie możemy spokojnie spać.

Trochę zaskakujący wynik prucia hasła skłonił mnie do pokopania w sieci. Jak to jest dziś z bezpieczeństwem komputerowym? Konkluzja jest taka, że może być bezpiecznie. Może. A to, czy jest, zależy od użytkownika. Konkluzja jednak inna od oficjalnego biadolenia. Możesz zapewnić bezpieczeństwo, o ile nie popełniasz jakiś bardzo durnych błędów, jak instalowanie sobie trojanów.

W sytuacji, gdy systemy operacyjne zostały wyczyszczone z grubych błędów umożliwiających włamania, tak naprawdę jedynym problemem staje się głupota użytkownika. Kiedyś zasadniczym problemem był faktyczny brak zabezpieczeń w takich systemach jak Windows, w systemach uniksowych ciągle znajdowały się „dziury”, zazwyczaj procesy uruchamiane przez użytkownika, które pozwalały na uzyskanie praw administratora.

Dziś nie ma systemów operacyjnych niedostosowanych do pracy w sieci, a włamywacze zazwyczaj zatrzymują się na sprzętowych routerach, przez które przebić się nie daje. One także już stały się praktycznie zupełnie „szczelne”, choć kiedyś bywały podatne na ataki. Częste kiedyś wypadki „wejścia na maszynę” dziś są praktycznie nieznane. Czy zauważyliśmy, że tak naprawdę bezpieczeństwo w sieci mocno się poprawiło? Płacimy dość bezpiecznie za pomocą internetu, kupujemy bilety, załatwiamy sprawy w urzędach. To możliwe np. dzięki temu, że usługę z zamierzchłych czasów zwaną „telnet” zastąpił protokół ssh, czyli Secure Shell, protokół http szyfrowany https. I tak dalej. W sieciach Wi-Fi WEP zastąpił WAP2 obecnie WAP3, któremu podobno można ufać.

Niestety „nie wolno” tak tych spraw opisywać. To znaczy jeśli ktoś napisze, że w gruncie rzeczy problemem nie jest nawet znajomość narzędzi, ale głupota, to straci czytelnika. Tekst nie może się zaczynać od informacji, że „jest bezpiecznie”.

I to jest konkluzja, ku której zmierzam. Bo… no właśnie, nie warto pisać, gdy wszystko jest dobrze. Szczegółowe zagadnienie bezpieczeństwa komputerowego znakomicie ilustruje ogólny problem. Gdy nakaz straszenia rzuca się na kształtowanie opinii publicznej, to mamy problem.

Teraz panuje moda, aby widzieć w technice zagrożenie. Nie dostrzegamy faktów, że udało się zlikwidować problemy. Można odjechać daleko od komputerów i zauważymy

to samo: jedynie biadanie się sprzedaje.

Nie wolno pisać, że to technologia załatwiła bardzo poważny problem zanieczyszczenia powietrza. Kiedyś w powietrze waliły ogromne ilości tlenków siarki, całkiem niedawno w miastach śmierdziało spalinami. Dziś, idąc ulicą obok korka samochodowego, czuję zapach rosnących obok krzaków jaśminu. Bo samochody mają sprawniejsze silniki i – co pewnie najważniejsze – katalizatory.

Z trudem do publiczności przebija się oczywista prawda, że praktycznie jedynym źródłem tak zwanego smogu w miastach są domowe piece, a nie silniki spalinowe. Ale jeszcze nie przyszedł czas na to, by ludzie zauważyli, że samochody elektryczne raczej zwiększą problem smogu, a nie zmniejszą go, bo kolejnym źródłem pyłów zawieszonych są opony, które same się ścierają i mielą na drobniutki pył nawierzchnię. A elektryki muszą by dużo cięższe od benzyniaków.

Technika za dobrze poradziła sobie z emisją pyłów. Spalanie już ich nie generuje, jest ich tak mało, że widać wpływ źródeł, które wcześniej nie miały znaczenia. Tak, czasami dociera do nas pył z Sahary. Z nim także trzeba wojować?

Z tego, że nie wypada dobrze pisać o tym, co wyszło laboratoriów, co wynika z nauki i techniki, mamy problem z antyszczepionkowcami. Że medycyna chroni nas przed takimi chorobami jak odra, nie wypada pisać, na medycynę wypada narzekać. Modnie jest straszyć koncernami farmaceutycznymi, eksperymentami w stylu doktora Wiktora Frankensteina, których nigdy nie przeprowadzano poza filmami SF. A ludzie już sami dojdą do tego, że może ich uratować jedynie tak zwana medycyna naturalna.

Mamy pasztet z GMO. Trzeba ponosić gigantyczne koszty na badania, tylko z tego powodu, że publiczność została przestraszona i nie rozumie, o co chodzi. A tak naprawdę rzecz w tym, że glikofosat stosowany do zwalczania chwastów może być stosowany w znacznie mniejszych dawkach od innych środków. Przez to uprawa jest nie tylko tańsza, ale potencjalnie bezpieczniejsza dla środowiska. Jest tylko ten problem, że załatwi on także rośliny uprawne. Wyhodowanie na drodze modyfikacji genetycznych kukurydzy odpornej na ten związek chemiczny rozpoczęło awanturę.

Dowcip w tym, że nie GMO jest potencjalnie niebezpieczne, ale ów glikofosat. Tymczasem publiczność wojuje z całych sił z GMO. Skutkuje to potencjalnie niewyobrażalnymi stratami w rolnictwie. GMO może być skutecznym sposobem na przykład na zanieczyszczenie środowiska metalami ciężkimi, na głód na świecie, ale o GMO wolno pisać tylko jako o straszaku.

Zagrożeniem są smartfony, zagrożenie stanowiła całkiem niedawno głośna muzyka, czyli technika Hi-Fi, o grach komputerowych wolno pisać jedynie źle, chyba że w pismach fanowskich. Plastik to dramat. Ostatnio modny stał się mikroplastik. Przy czym nie wiadomo jeszcze, czym grozi. Ale grozi.

Eksperyment z pruciem tego „1234” pokazał mi, jak daleko ten popularny obraz świata jest od rzeczywistości. Karmi się nas bajkami – po prostu. Nie kilka minut, ale kilkadziesiąt godzin. Tak, lepsze nawet tak głupie hasło, niż żadne, bo „oni i tak wszystko kontrolują”. Jeden ze skutków napuszonych tekstów o bezpieczeństwie jest właśnie taki, że zwykły użytkownik dochodzi do wniosku, że zabezpieczenie się jest tak trudne, że przekracza jego możliwości, i nie robi nic.

Obraz cyber(nie)bezpieczeństwa, jaki wyłania się z mediów, jest mniej więcej taki, że wiedzą o nas wszystko i wielkie rządowe organizacje, i wielkie korporacje. Banki śledzą wszystkie transakcje, strony internetowe rejestrują każde wejście, a nawet ruchy myszki (to akurat prawda), a ciemne, czające się w mitycznym DarkNecie gangi handlują danymi

do naszych kart bankowych, numerami dowodów i bogi wiedzą, czym jeszcze. Jeśli podawane są rady, jak się chronić, to zwykle są one tak zawiłe i niezrozumiałe, jak ów wymóg używania znaków specjalnych w hasłach. I tak zwany zwykły user dochodzi do wniosku, że lepiej zaryzykować, a jak dojdzie do katastrofy, to będzie się martwił. Bo i tak nie rozumie, jakie to hasło ma być.

Zabawa we wzajemne straszenie się doprowadziła do tego, że w krytycznych sprawach, jak choćby czy ospa wietrzna jest groźną chorobą, albo jakie dane można umieścić na Facebooku, żeby nie zaprosić do mieszkania złodzieja, panuje głupota. Nie niewiedza, ale głupota, przekonanie, że jest się mądrym, a w rzeczywistości robimy krzywdę sobie i innym.

Nasze pojęcie o świecie kształtowane wedle treści popularnych mediów niewiele się różni w swej trafności od tego, co wpajano w światlejsze głowy w wiekach średnich. Pocieszające jest to, że gdy do Europy w XIV wieku dotarła dżuma, nie dała rady zniszczyć cywilizacji, choć nie było w tym żadnej zasługi ludzkiej mądrości.

Adam Cebula