

Emil Sierżęga
MIMUW

Quo vadis hakerze,

czyli o tym kto i w jakim celu okradnie Cię za kilka lat.*

Haker¹ (ang. hacker) – osoba o bardzo dużych, praktycznych umiejętnościach informatycznych (lub elektronicznych) która identyfikuje się ze społecznością hakerską. Hakerzy odznaczają się bardzo dobrą orientacją w Internecie, znajomością wielu języków programowania, a także świetną znajomością systemów operacyjnych, w tym zwłaszcza z rodziny Unix (GNU/Linux, BSD itp.)

Cracker² (z ang., dosłownie łamacz) – osoba zajmująca się łamaniem zabezpieczeń komputerowych (crackingiem). Wyróżnia się dwie główne kategorie działań crackerów:

- łamanie zabezpieczeń zamkniętego oprogramowania (zobacz: crack, cracking, CrackMe, patch),
- łamanie zabezpieczeń serwerów (zobacz: exploit, gry crackerskie).

Jak było jeszcze niedawno?

10 lat temu słowo 'haker' brzmiało naprawdę groźnie. Wydaje się, że właśnie w tym czasie media wypaczyły jego znaczenie, celowo tworząc hakera synonimem crackera. *New York Times* i *Newsweek* codziennie donosiły o działaniach policji mających na celu schwytać „demonicznego” Kevina Mitnicka³. Od momentu zagoszczenia jego twarzy na okładce *Timesa* oraz obwieszczenia go osobą będącą „zagrożeniem dla ogólnoswiatowej rewolucji w telefonii komórkowej” oraz „zagrożeniem dla całego internetu” w ogóle⁴ świat pojął, że osoba świetnie poruszająca się w przestrzeni komputerów może być niezwykle groźna. Ten okres, mojej młodości, to okres najwspanialszej hakerskiej twórczości. Fascynacja informatyzacyjną globalizacją powodowała nagły wzrost dziedzin życia, w które wkraczał komputer, a tym samym stwarzał kolejne potencjalne luki w zabezpieczeniach. Jednak hakerom/crackerom w większości przyświecała, szczytna idea: poszerzania własnych horyzontów, zdobywania wiedzy i doświadczenia, działań mającym najczęściej na celu prześciganie samych siebie i dociera tam gdzie nie dotarł nikt inny (np. włamanie na serwery pewnej firmy przez klienta sieciowego starej drukarki Hewlett-Packard, której niepostrzeżenie nikt jeszcze nie wyrzucił na śmietnik⁵). Odsetek świadka hakerskiego, który czerpał korzyści ze swojej działalności był marginalny, ale przecież to on stanowi najlepszą pożywkę dla mediów...

1 [http://pl.wikipedia.org/wiki/Haker_\(slang_komputerowy\)](http://pl.wikipedia.org/wiki/Haker_(slang_komputerowy)) (dostęp 9.V.2011)

2 <http://pl.wikipedia.org/wiki/Cracker> (dostęp 9.V.2011)

3 „Kevin David Mitnick, znany też pod pseudonimem Condor (ur. 6 sierpnia 1963 roku w Van Nuys, Kalifornia) – jeden z najbardziej znanych komputerowych włamywaczy. Za swoje przestępstwa został skazany na wieloletnie pozbawienie wolności. 15 lutego 1995 roku FBI przy pomocy dziennikarza komputerowego Johna Markoffa i Tsutomu Shimomury aresztowało go. Został oskarżony o włamanie na terenie USA do kilku ważnych systemów komputerowych. Nigdy jednak nie zarzucono mu czerpania korzyści materialnych z crackingu” - Wikipedia.org (dostęp 9.V.2011)

4 Okładka „New York Times”. Wydanie z dnia 4.VII.1994. Proszę zwrócić także uwagę na wymowę daty. Czwarty lipca jest Dniem Niepodległości Stanów Zjednoczonych.

5 „Hakerzy atakują. Jak przejąć kontrolę nad siecią”. Helion, wyd. I, 2004, rozdział 4

Jak jest teraz?

Dzisiaj żaden cracker nie „dostanie” pierwszej strony w *New York Times*. Za to gdzieś pośrodku tygodników czy gazet, w małych artykułach możemy przeczytać o kradzieży danych z kont około 70 mln. użytkowników usługi *PlayStation Network* firmy Sony⁶, ataku na firmę *Epsilon* rozsyłającą rocznie ok. 40 mld reklamowych e-maili czy przejęciu danych firmy *Heartland Payment Systems* w wyniku, której crackery przejęli informacje o 45 mln kart kredytowych⁷. I to wszystko drobnym druczkiem, gdzieś z boku. Przecież inaczej mogłaby się rozpętać medialna burza (znowu!), a ludzie zaczęliby zastanawiać się nad udostępnianiem przez siebie danych lub co gorsza patrzyli bardziej podejrzliwym okiem na zabezpieczenia niektórych banków (np. popularnego w Polsce mBanku).

Jednak prawdy nie da się zatuszować i odsunąć na bok. Dzisiaj hakerem nazwać można większość naprawdę dobrych programistów⁸. Dla poszerzenia własnych horyzontów włamią się czasem niepostrzeżenie na konta jakiejś większej spółki albo zablokują dostęp do stron kilku działaczy Samoobrony. Jednak prawdziwym zagrożeniem jest cracker (zwracam uwagę na właściwy dobór słów!) przejmujący miliony bajtów danych niczego nieświadomych ludzi.

Codziennie po cichu, przez nikogo nie zauważeni kradną olbrzymie ilości wartości NAJWAŻNIEJSZEJ w ówczesnym świecie – informacji. Cracker/Haker to nie osoba, która wysyła koledze „trojana” żeby trochę pobawić się jego kosztem. To człowiek, który w coraz to lepiej wyposażonym mieszkaniu przejmuje dane sklepów internetowych, serwisów aukcyjnych, serwisów płatniczych czy, najważniejsze, banków. Takie dane są dobrą pożywką np. dla spamerów (o prawdziwych bandytach nie wspomnę). 70 mln maili graczy konsoli PlayStation jest olbrzymim potencjałem dla osób, które 'udostępnią gry na PlayStation po niezłodziejskiej cenie', 10 mln adresów e-mail odwiedzających, czynnie, serwisy pornograficzne jest wspaniałym potencjałem dla osób sprzedających akcesoria erotyczne⁹. Właśnie z takich 'niegroźnych' danych jesteśmy okradani codziennie. Ale co z tego? Przecież około 70% użytkowników facebook.com, twitter.com czy nk.pl udostępnia swoje profile jako publiczne.

Z kim będą walczyć Twoje dzieci?

Jeśli teraz informacja jest najbardziej pożądaną wartością na kuli ziemskiej to, za 15-20 lat będzie to wartość ultra-pożądana. Życie każdego z nas w dużej mierze ulegnie przełożeniu na ciągi bitów. Ogólnoświatowe systemy śledzące, stopniowa monopolizacja i globalizacja usług bankowych, możliwość załatwienia każdej rzeczy przez Internet, zdalnie sterowane samochody¹⁰, ewolucja telewizora, radia (kto jeszcze słucha radia ze stacjonarnego odbiornika?), lodówki czy zwykłego naściennego zegara w komputer potrafiący odtworzyć dowolny film czy pokazać treść dzisiejszej Gazety Wyborczej (niechaj się nikt nie martwi, książka w wydaniu analogowym, mimo wszystko będzie miała się dobrze). To wszystko spowoduje, że

6 http://wyborcza.pl/1,76842,9505425,Wielki_wlam_na_konsoli.html (dostęp 8.V.2011)

7 http://wyborcza.biz/biznes/1,100896,9511936,Cyberapetyt_na_dane_Na_celowniku_banki_sklepy_popularne.html (dostęp 8.V.2011)

8 Czyli np. absolwentów wydziału MIM Uniwersytetu Warszawskiego :-)

9 Przyjmuje się, że sukcesem bazy danych jest ratio (procent odpowiedzi na spam) w okolicach 1-2%, zwykle ratio waha się w granicach 0,01-0,1%

10 Już teraz istnieją bardzo dobrze działające systemy zapewniające taką funkcjonalność, jednak do tego by poruszać się zdalnie sterowanymi pojazdami po ulicach miasta potrzeba nie 10-ciu a 50-ciu lat. Nie ze względu na technikę, a mentalność ludzką – wszak takie diabelstwo zabroni Polakowi pędzić 140 km/h o godzinie 14, na obszarze zabudowanym mając we krwi 1,4‰ alkoholu.

informacja stanie się jeszcze cenniejsza, a zdolności hakerskie jeszcze bardziej upragnione.

Na 24. piętrze biurowca świetnie wyposażona grupa programistów, do 16:00 pracujących nad system usprawniającym działanie lokalnego urzędu pracy, po przerwie na kawę, od 16:30 zajmą się przejmowaniem danych z serwera, przynoszącej olbrzymie zyski, firmy X, działając na zlecenie firmy Y (która chce przerzucić się na rynek firmy X). Znajomi naszych biurowych znajomych, już na innym kontynencie postarają się przejąć dane nt. broni jądrowej kraju Z, na zlecenie kraju, w którym mieszkają¹¹. Grupa pasjonatów z Los Angeles spróbuje przejąć (ukraść) jeden ze zdalnie sterowanych samolotów amerykańskiej armii, nowa grupa FailOverflow¹² II znowu zajrzy na serwery Activision w poszukiwaniu kodów źródłowych jeszcze nie wypuszczonej oficjalnie gry najnowszej generacji (kosztującej firmę ponad 100 mln. dolarów). A gdzie w tej wyliczance zwykły szary człowiek? Spokojnie, jego dane, aktualne położenie oraz numer rachunku z wczorajszej kolacji w lokalnej restauracji są już w około 50-ciu różnych bazach danych.

Konkluzja? Im więcej danych zostawisz w Sieci tym więcej z nich możesz stracić, im więcej informacji uznasz za nieistotne, tym więcej z nich stanie się informacją publiczną, im bardziej odporny staniesz się na przepływ informacji, tym większy przepływ informacji stworzysz, im szybciej zapiszesz numer PIN swojej karty kredytowej jako notatkę w swoim iPhone...

Strzeż się! Swoją nierozwagą dziś przyzwolisz na wirtualny atak jutro.

* - a Ty nawet tego nie zauważysz

11 Jestem święcie przekonany, że np. rząd USA takie działania już prowadzi. Na dodatek w pełni legalnie.

12 <http://gry-info.re.pl/artykul/22233.html> (dostęp 9.V.2011). Grupa crackerska, która jako pierwsza dokonała włamania na serwery Sony kradnąc dane około 10 mln kont użytkowników PlatStation.