Policyjni włamywacze

4 lutego 2009
Chciałem poruszyć sprawę policyjnych włamywaczy. Choć nie do końca policyjnych, ale w jakimś stopniu z policją związanych.

A więc do rzeczy. Niecałe dwa miesiące temu podczas rozmów jakie przeprowadziłem wspólnie z moimi znajomymi, ze znawcami tematu, uzyskałem… – a dodam że chodzi o specjalistów z dziedziny tak zwanego hakowania i hakingu, czyli po prostu komputerowych zabezpieczeń – ni mniej ni więcej tylko następujących informacji:

1. Znaczna liczba „infekcji" komputerowych, wraz ze słynnymi „Koniami Trojanami" rodzi się w zaciszach laboratoriów służb specjalnych, i to nie tylko rosyjskich i chińskich. Na zlecenie tajnych służb, albo nawet ludzie pracujący bezpośrednio dla nich, programiści i informatycy pracują nad szkodliwym oprogramowaniem, dzięki którym następnie mogą dostać się do wnętrza naszego komputera by go przeszukać pod kątem cennych dla siebie informacji.

W samym „środowisku" znawcy tematu uważają że nawet połowa szkodliwych wirusów i trojanów jest pochodzenia „służbowego". Mało tego niektórzy z nich uważają że służby współpracują często z organizacjami przestępczymi dokonując wspólnych działań, lub wymieniając informację.

Drugą sprawą o jakiej mówią specjaliści z dziedziny hakingu i zabezpieczeń jest TOR. Znowóż wielu z nich uważa, że jak to nazywają: „znaczna część węzłów TORa jest kontrolowana przez „służby", a w przypadku Niemiec, nawet osiemdziesiąt, lub dziewięćdziesiąt procent węzłów TORa jest kontrolowanych przez tajne służby".

W przypadku Niemiec to chyba nie dziwi, większość ugrupowań politycznych uważanych za wrogie jest kontrolowana, a jak uważają złośliwi kreowana przez tajne służby (niemiecka tajna

policja NPD kontynuuje tradycje pruskie i nie ma się czemu dziwić).

Dlatego mała prośba:

NIE PRZESYŁAJCIE TOREM CENNYCH DLA SIEBIE INFORMACJI!!!

Tor jest dobry dla ukrycia swojej tożsamości np. na forach internetowych, i do tego można go używać. Znacznie bezpieczniejszy wydaje się być FreeNet.

A teraz do czego dążę? Dążę do tego żeby pokazać iż działalność ustawodawców i policji może zepsuć podwodne serfowanie służb w sieci, ponieważ chcą za pomocą swoich łodzi motorowych całkowicie zburzyć spokojne lustro wody i wywołać prawdziwy zamęt. Może władza ustawodawcza i administracja zazdrosna jest o wiedzę służb, a może obawia się jej znaczenia, dość że chce sama przejąć to co kiedyś było „działką służbową".

CHCĄ NIE TYLKO PRZESZUKIWAĆ TWÓJ KOMPUTER, ale także zmusić właścicieli lub producentów zabezpieczeń-programów szyfrujących do przekazania „kopi" kluczy. Nie oddasz państwu odcisku klucza do swojego domu i numeru konta w banku? Nie ma problemu – pójdziesz siedzieć.

To nic nowego, zapytajcie tylko producentów programów szyfrujących, a oni powiedzą wam. W czym problem? Problem jest w tym, że każdy praktycznie twórca programów szyfrujących tworzy tak zwane dziury, albo zapadki („luki"), dzięki którym można łatwo dostać się do systemu. Na przykład wtedy, gdy użytkownik zapomniał hasła, co zdarza się niestety bardzo często. Kiedy zapytacie znajomego pracującego nad programami szyfrującymi o te zapadki założę się, że zrobi wtedy tajemniczą minę, lub przynajmniej się uśmiechnie…

Teraz jednak zamiast subtelnych i wyrafinowanych nierzadko wytrychów, które należy porzucić w opinii ustawodawców zachodnioeuropejskich, przyszedł czas łomów do wyważania drzwi

i siekier do ich rąbania, jeśli nie dadzą się wyważyć i okażą zbyt mocne i dobrze zabezpieczone.

Pisze o tym ZDNet.co.uk (patrz artykuł w języku angielskim **tutaj**) oraz VaGla.pl (pełna treść **tutaj**): „W Unii Europejskiej, a szczególnie w Niemczech i Wielkiej Brytanii, prawodawcy starają się wyposażyć organy ścigania w narzędzia prawne pozwalające na zdalną kontrolę komputerów obywateli. Skoro część obywateli będzie szyfrować dane, w Wielkiej Brytanii prawodawca poszedł jeszcze dalej (Szyfrujesz? Ujawnij klucz, albo więzienie!). Do publicznej dyskusji włączyły się przedsiębiorstwa, które oferują rozwiązania w dziedzinie bezpieczeństwa, w szczególności oprogramowanie antywirusowe, i ogłosiły, że dostarczane przez nich rozwiązania będą blokowały wszelkie próby zdalnego dostępu do komputerów użytkowników takiego oprogramowania, które będą podejmowane przez Policję. Przypuszczam, że może być to chwyt marketingowy, bo łatwo wyobrazić sobie zobligowanie takich przedsiębiorstw do pozostawiania w ich oprogramowaniu backdoorów, albo zakazanie im blokowania prób policyjnych włamań.”

Autor: cenntrolew
Materiał nadesłany do „Wolnych Mediów”