

## Wzburzona cyberprzestrzeń

Autor tekstu: **Monika Sadlok**

**S**tyczeń 1997 roku odwiedzający stronę [www.plannedparenthood.com](http://www.plannedparenthood.com) zostali przywitani hasłem „Witamy na stronie domowej Planned Parenthood” z linkiem do książki dotyczącej aborcji „koszt aborcji”. Strona ta nie była jednak oficjalną, wymienioną organizacją na rzecz wolności macierzyństwa, a atakiem aktywisty antyaborcyjnego Richarda Bucci.

Styczeń 2006 r. raport firmy F-Secure zwraca uwagę na rosnącą ilość ataków hakerskich na firmy, w tym na banki.

Kwiecień 2009 — włamanie do najdroższego i najbardziej zaawansowanego programu zbrojeniowego realizowanego przez Pentagon (myśliwce F-35).

Luty 2010 — ataki hakerskie na formę Google.

Marzec 2010 — chińscy hakerzy zaatakowali konta pocztowe na Yahoo.

Styczeń 2011 — główny udziałowiec Facebooka Mark Zuckerberg, musiał zmienić adres strony z profilem, po włamaniu hakerskim.

Luty 2011 — prasa poinformowała o działaniach chińskich hakerów infiltrujących kompanie naftowe i gazowe.

Czerwiec 2011 - hakerzy zaatakowali system MFW.

To tylko kilka, z wielu opisywanych i ujawnionych, przykładów skutecznych ataków przeprowadzonych przez hakerów, cyberprzestępców. Tego typu działalność użytkowników internetu została podzielona na kilka podstawowych grup:

1. cyberprzestępczość, czyli wyłudzenie informacji od osób prywatnych, dotyczących numerów kart kredytowych, haseł dostępu do konta itp.,
2. dostawcy spamu, czyli zarabianie pieniędzy dzięki nielegalnej reklamie,
3. zorganizowane i dysponujące dużymi pieniędzmi organizacje, zajmujące się kradzieżą własności intelektualnej,
4. bardzo podobną grupą są szpiegzy gospodarczy, z tym, że wyróżniają je mniej zorganizowane struktury,
5. cyberwojownik, czyli haker specjalizujący się w znajomości narzędzi informatycznych, mogących skutecznie pozbawić jakieś państwo obrony militarnej, urażony/zwolniony pracownik, który kieruje się impulsywną chęcią zemsty,
6. i jedna z najciekawiej rozwijających się aktywności hakytywizm.

Korzystając na co dzień z komputera, często nie zdajemy sobie sprawy z liczby niebezpieczeństw, na które jesteśmy narażeni, używając tak powszechnych narzędzi jak przeglądarka internetowa, wyszukiwarka. Alfred Huger, specjalista i wiceprezydent firmy zajmującej się bezpieczeństwem sieciowym, wymienia kilka najbardziej popularnych sposobów ataków hakerskich: przeglądarka Google — łatwo można otworzyć stronę zawierającą szkodliwe, szpiegowskie oprogramowanie, z uwagi na jej ponadprzeciętną popularność, tracimy czujność, ufamy otwieranym stronom; przeglądarka internetowa Mozilla, mająca stanowić alternatywę dla dziurawego Explorera, także nie uniknęła wpadek; media społecznościowe stanowią doskonałe narzędzie nie tylko atakowania profilu, ale także wydobycia cennych informacji. Ataki na osoby prywatne, mimo, że niezwykle dokuczliwe w mikroskali, nie stanowią jednak tak poważnego zagrożenia jak ataki na infrastrukturę państwową, energetyczną, jądrową itp. O możliwości realizacji tego scenariusza, przekonuje działalność cyber gangu „Coreflood”, który z dużą łatwością przejął kontrolę na systemami komputerowymi dużych korporacji, szpitali, uniwersytetów, a nawet agend rządowych.

Państwa Unii Europejskiej oraz NATO, o problemie cyberprzestępczości, a przede wszystkim jej przeciwdziałania dyskutują od wielu lat i jak podkreśla Maeve Dion, dyrektor programowy Ośrodka ds. Ochrony Infrastruktury w George Mason School of Law "w jednym kraju cyberobrona może polegać przede wszystkim na wysiłkach militarnych zmierzających do ochrony przed cyberatakami i reagowania na nie; w innym — cyberobrona może obejmować prewencję i reagowanie zmierzające do ograniczenia szkód w sieciach cyfrowych, spowodowanych przez katastrofy naturalne i wypadki".

Jednak fala zagrożenia ciągle rośnie, a możliwości hakerów są praktycznie nieograniczone.

Zjawiskiem, które nie do końca można zakwalifikować jako typowy przykład cyberprzestępczości to działania wynikające z pobudek politycznych.

Czym jest to zjawisko?

Posługując się szeroką definicją, przestępstwa internetowe, za którymi stoją cele i motywacje polityczne dzielą się na dwie kategorie: inspirowane międzynarodowymi problemami/zagadnieniami, czyli wspomniany hakytywizm (zakwalifikowany przez A.Samuęla, jako kolejne pojęcie zasługujące na miejsce w leksykonie politologicznym) oraz cybernetyczne nieposłuszeństwo obywatelskie.

Różnice są oczywiście niewielkie i bardzo rozmyte, metody w obu przypadkach mogą być takie same, różnica widoczna więc będzie jedynie na poziomie motywacji. Generalizując można wymienić trzy powody wzrostu liczby tego typu aktywności cyberaktywistów. Po pierwsze wzrost możliwości szybkiej komunikacji, praktycznie z każdym zakątkiem świata. Wynika z niego powód drugi, oburzenie wobec wszelkich przypadków łamania praw społecznych, może nabrać natychmiast realnego kształtu, jednocześnie nie zmuszając do ujawnienia prawdziwej tożsamości. W raporcie Symantec Internet Security wyraźnie widać wzrost liczby tego typu aktów obywatelskich, w przypadku Zjednoczonych Emiratów Arabskich o 344%, w Jordanii o 250%, na Kubie o 188%, gdzie Internet jest postrzegany jako medium dające możliwość wykrzyczenia swoich prawd nawet najmniejszym grupom sprzeciwu.

Drugą formą przestępstw komputerowych inicjowanych pobudkami politycznych, jest popierany przez anarchistów i aktywistów ruch protestu online - hakytywizm, czyli symbioza hakingu i protestów, gdzie motywacja jest bardzo różna, dotycząca wielu materii: sprzeciw wobec globalizacji, walka o prawa zwierząt, ruch związkowy, ruch przeciwko modyfikacji żywności, ruch antywojenny. Tego typu działania, poza swoją formą elektroniczną, mają bardzo często także wsparcie lub powiązania z realnie odbywającymi się protestami, manifestacjami.

Działalność hakerska opierająca się na motywacjach politycznych, w przeciwieństwie do tradycyjnej, nie może pozostać w ukryciu. Cele, w imię których podejmowane są przecież wymanione działania, są zbyt ważne społecznie, dlatego ich organizatorzy, bardzo szybko dostrzegli potrzebę współpracy z dobrymi PR - owcami, docierając do nich poprzez specjalistyczne strony internetowe. Jedną z najbardziej znanych i efektywnych jest Indymedi, która sens swojej działalności określa jako „szerzenie w ponad 20 językach, w 35 państwach, za pomocą nowoczesnych technik informatycznych, wszelkich przypadków nadużyć”

Pomimo niewątpliwie, szybkiego i gwałtownego wzrostu zarówno samych aktów aktywizmu, jak i zainteresowania ze strony tradycyjnych mediów, to historia przestępstw online, z nutą politycznej motywacji jest znacznie starsza i sięga początków działalności niemieckiej grupy Chaos Computer Club. W latach 80' jej członkowie w obecności polityków Partii Zielonych i The Grune Alternative Liste, dyskutowali o możliwości wyrażenia wsparcia dla działań CCC. W 1989 roku pięciu członków tej organizacji zostało aresztowanych za przeprowadzenie ataków na systemy wówczas jeszcze Związku Radzieckiego. W 1995 roku, CCC zakłóciła w proteście przeciwko przeprowadzaniu prób z bronią nuklearną, działalność francuskiej sieci telekomunikacyjnej. Również duńscy aktywiści przeprowadzili szeroko nagłośnioną akcję, włamania do systemu komputerowego Ministerstwa Obrony Stanów Zjednoczonych przed rozpoczęciem działań zbrojnych w Zatoce Perskiej. W 1989 roku Australijczyk napisał złośliwe oprogramowanie o nazwie WANK (Worm Against Nuclear Killers — robak przeciwko nuklearnym zabójcom). Szkodnik atakował komputery pracujące pod kontrolą systemu VMS i wyświetlał w nich komunikat krytykujący nuklearny wyścig zbrojeń. W żaden sposób nie szkodził systemowi, jego podstawowym zadaniem było przekazanie komunikatu politycznego

Hakytywizm wzbogacony więc zostaje o jeszcze jedną formę aktywności, związana z dystrybucją właściwego przekazu medialnego. Oczywiście wynika to także z faktu coraz szerszego ich zasięgu, łatwości przekazywania informacji. Dzięki Hilary Clinton, która zainicjowała ofensywę Internet Freedom, - Twitter, Youtube, Facbook, naznaczony został piętnem polityki, a hakywiści uzyskali nowe narzędzi szybkiej i masowej komunikacji.

Ta nowa forma sprzeciwu obywatelskiego jest elementem debat wielu teoretyków, którzy dostrzegają w Internecie możliwość odtworzenia greckiej agory. Hakytywizm pokazał, że kształt tej e — demokracji nie koniecznie musi przybierać formę grzecznej wymiany zdań. Thornton twierdzi, iż właśnie internet pozwoli „obywatelom swobodnie dyskutować o sprawach państwa i osiągać konsensus. Ponadto przyczyni się do zmodyfikowania dotychczas obowiązującego systemu i zasad funkcjonowania państw". Państwo, w swojej tradycyjnej formie pozostanie jeszcze długo najważniejszym aktorem. Cyberprzestrzeń daje jednak możliwość większej efektywności, tym niemniej perspektywa powstania cyberwładzy wydaje się jeszcze dosyć odległą.

**Monika Sadlok**

Politolożka, obecnie kończy doktorat z zakresu nauk o polityce. Poza pracą naukową, działa również społecznie w "Fundacji Rozwoju Demokracji Lokalnej", w "Stowarzyszeniu Meritum", oraz w "Fundacji Młodzi Twórcy im. prof. P. Dobrowolskiego". W marcu 2011 dołączyła do grona celebrantów humanistycznych.

[Pokaż inne teksty autora](#)

(Publikacja: 13-08-2011)

[Oryginał.](http://www.racjonalista.pl/kk.php/s,2128) (<http://www.racjonalista.pl/kk.php/s,2128>)

Contents Copyright © 2000-2011 Mariusz Agnosiewicz

Programming Copyright © 2001-2011 Michał Przech

Autorem portalu Racjonalista.pl jest Michał Przech, zwany niżej Autorem.  
Właścicielami portalu są Mariusz Agnosiewicz oraz Autor.

Żadna część niniejszych opracowań nie może być wykorzystywana w celach komercyjnych, bez uprzedniej pisemnej zgody Właściciela, który zastrzega sobie niniejszym wszelkie prawa, przewidziane w przepisach szczególnych, oraz zgodnie z prawem cywilnym i handlowym, w szczególności z tytułu praw autorskich, wynalazczych, znaków towarowych do tego portalu i jakiegokolwiek jego części.

Wszystkie strony tego portalu, wliczając w to strukturę katalogów, skrypty oraz inne programy komputerowe, zostały wytworzone i są administrowane przez Autora. Stanowią one wyłączną własność Właściciela. Właściciel zastrzega sobie prawo do okresowych modyfikacji zawartości tego portalu oraz opisu niniejszych Praw Autorskich bez uprzedniego powiadomienia. Jeżeli nie akceptujesz tej polityki możesz nie odwiedzać tego portalu i nie korzystać z jego zasobów.

Informacje zawarte na tym portalu przeznaczone są do użytku prywatnego osób odwiedzających te strony. Można je pobierać, drukować i przeglądać jedynie w celach informacyjnych, bez czerpania z tego tytułu korzyści finansowych lub pobierania wynagrodzenia w dowolnej formie. Modyfikacja zawartości stron oraz skryptów jest zabroniona. Niniejszym udziela się zgody na swobodne kopiowanie dokumentów portalu Racjonalista.pl tak w formie elektronicznej, jak i drukowanej, w celach innych niż handlowe, z zachowaniem tej informacji.

Plik PDF, który czytasz, może być rozpowszechniany jedynie w formie oryginalnej, w jakiej występuje na portalu. **Plik ten nie może być traktowany jako oficjalna lub oryginalna wersja tekstu, jaki prezentuje.**

Treść tego zapisu stosuje się do wersji zarówno polsko jak i angielskojęzycznych portalu pod domenami Racjonalista.pl, TheRationalist.eu.org oraz Neutrum.eu.org.

Wszelkie pytania prosimy kierować do [redakcja@racjonalista.pl](mailto:redakcja@racjonalista.pl)