Jakub Kwaśnik[1]

Charakterystyka subkultury *hackerów* jako kluczowego elementu cyberprzestępczości

Geneza subkultury i ogólna charakterystyka środowiska

Początki sieci internetowej nie wróżyły tak dynamicznego jak obecnie rozwoju: tego typu łącznością zainteresowały się pierwotnie jedynie znaczące korporacje i instytucje międzynarodowe. Przodkiem dzisiejszej sieci internetowej był ARPANET (***A****dvanced* ***R****esearch* ***P****rojects* ***A****gency* ***Net****work)*, który powstał jako eksperyment techniki umożliwiający połączenia. Projekt zainicjował Pentagon, zwołując w roku 1967 konferencję na temat możliwości łączności na wypadek wojny nuklearnej. Z początkiem lat 70. powołano specjalny sztab ludzi, w skład którego wchodzili pracownicy naukowi i studenci amerykańskich uniwersytetów. Zespół ten stworzył podstawę struktury Internetu – model TCP/IP[2]. Imiennie zasługę stworzenia Internetu można by przypisać Vintonowi Gray'owi Cerfowi[3], który odegrał kluczową rolę w tworzeniu tego modelu, oraz doktorowi Josephowi Carlowi Robnettowi Lickliderowi, który był odpowiedzialny w ARPANECIE za początki budowy cyberprzestrzeni, kierując projektem rozwoju technologii komputerowych; jednakże należy pamiętać, że sieć internetowa miała wielu pionierów, gdyż powstawała przez wiele lat, zanim osiągnęła obecny kształt. Internet szybko stał się magnesem dla osób ambitnych: spora część młodych ludzi od razu dostrzegła ogromny potencjał związany z nowym wynalazkiem i zainteresowała się metodami tworzenia witryn, zabezpieczeniami, grafiką komputerową oraz mechanizmami działania całości systemu oraz łączy.

Dynamiczny rozwój technologii oraz komunikacji komputerowej przyniósł gwałtowny wzrost usług świadczonych za pomocą Internetu. Skutkiem rosnącego poziomu wydajności i jakości łączy przesyłu danych stał się widoczny wzrost liczby użytkowników sieci, w tym szerokiej grupy przedsiębiorców, którzy w coraz większym stopniu upatrują tu istotne pole działań w zakresie funkcjonowania rynku sprzedaży, a także reklamy. Taki

[1] Autor jest studentem III roku Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego i członkiem Sekcji Kryminalistyki Towarzystwa Biblioteki Słuchaczów Prawa.

[2] D. Littlejohn Shinder, E. Tittel, *Cyberprzestępczość*, Gliwice 2004, s. 75

[3] Informacje pochodzą ze strony internetowej http://www.ibiblio.org/pioneers/cerf.html.

kierunek rozwoju wiąże się nieuchronnie z zainteresowaniem przestępczego światka, który postrzega Internet jako rynek złożony z dwóch półkul. Na jednej z nich funkcjonuje handel zabronionymi przez prawo dobrami, na drugiej zaś znajduje się rynek dóbr legalnych. Ta druga półkula jest z kolei dla cyberprzestępców zbiorem potencjalnych celów, których zaatakowanie i ewentualne przejęcie może przynieść określone korzyści. Warto w tym miejscu przytoczyć definicję cyberprzestępstwa według wykładni ONZ, która wydaje się najbardziej odpowiednia, by zrozumieć zakres zjawiska. Jeśli chodzi o wąskie znaczenie, jest to „wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych i procesowanych przez te systemy danych". Szerokie ujęcie definiuje cyberprzestępstwo jako „wszelkie nielegalne działanie popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[1]". Na potrzeby tego opracowania wyłączyć trzeba przestępstwa klasyczne, które mogą być popełniane bez użycia komputera, a w których sieć odgrywa jedynie rolę sposobu komunikacji przestępców lub pełni funkcję miejsca handlu zakazanymi dobrami. Skoncentruję się jedynie na analizie typowych przestępstw komputerowych popełnianych przez ludzi o określonych umiejętnościach informatycznych, czyli *hackerów*, których środowisko do dnia dzisiejszego stanowi istotny element funkcjonowania sieci. Chcąc efektywnie zapobiegać negatywnemu oddziaływaniu zjawiska *hackingu*, trzeba spojrzeć przekrojowo na tę subkulturę, dostrzec niepokojące elementy i umiejętnie je rozpracować, co ułatwi dokładna analiza grup cyberprzestępczych oraz motywów i metodyki działalności włamywaczy.

Nazwa *hacker* wywodzi się od słowa *hack*, którego powszechnie używa się w znaczeniu „rąbać", ale które występuje także w żargonie studentów Uniwersytetu w Massachusetts i oznacza tyle, co „poprawiać"[2]. Opinia publiczna przeważnie utożsamia *hackerów* z pierwszym znaczeniem wyrazu, bowiem odnosi je do działań grupy, która przełamuje zabezpieczenia i włamuje się na konta bądź serwery chronione, tymczasem w pewnym stopniu właściwa jest także druga opcja, która oddaje istotę jasnej strony działalności tego specyficznego środowiska użytkowników. Włamywacze komputerowi są jednym z dobrych przykładów zamkniętej grupy ludzi, która wedle swoich zadań i celów, kierując się odmiennymi wartościami, wyróżnia się spośród pozostałej części społeczeństwa. Według klasyfikacji Franka Hagana określiłbym całość tej grupy jako częściowo zorganizowany syndykat przestępczy[3]. Nie możemy bowiem wyróżnić ścisłej hierarchii wewnętrznej, zauważyć można natomiast skoordynowane i spójne działania grup składowych środowiska, które mają jasno sprecyzowane cele. Schemat organizacyjny odpowiada w zasadzie również strukturze siatkowej zorganizowanej grupy przestępczej, którą obok układu gwiaździstego i liniowego wyróżnia Andrzej Gaberle[4]. Wyjątek stanowi podgrupa *hackerów* zajmujących się *phishingiem*. Działalność subkultury *hackingu* może mieć zarówno charakter intelektualnej

[1] D. Littlejohn Shinder, E. Tittel *Cyberprzestępczość*, Gliwice 2004, , s. 35
[2] Zob. http://helionica.pl/index.php/Haker.
[3] A. Michalska-Warias, *Przestępczość zorganizowana i prawnokarne formy jej przeciwdziałania*, Lublin 2006, s. 36.
[4] T. Hanausek, *Kryminalistyka – zarys wykładu*, Kraków 2005, s. 286.

zabawy, swoiście pojmowanego sportu nastawionego na wynajdywanie luk komputerowych w systemach zabezpieczeń, może też mieć znamiona aktywności przestępczej w formie bezpośredniej, jak ataki na określone cele, bądź pośredniej, jako umożliwianie popełnienia innych przestępstw – głównie piractwa. To, co łączy wszystkich *hackerów*, to przekonanie o tym, że nie ma takich informacji na świecie, których nie mogliby oni zdobyć. Wiąże się to z celebrowaniem wolności jako wartości gwarantującej nieograniczoną i niekomercyjną swobodę pozyskiwania dóbr (w tym informacji)[5]. Poprzez działalność w cyberprzestrzeni próbują manifestować swoje poglądy. *Hackerzy* są najczęściej osobami wykształconymi i niezwykle ambitnymi, o czym świadczy doskonała znajomość zarówno teoretycznej, jak i praktycznej wiedzy informatycznej. *Hacker* jest jednak nie tylko ekspertem komputerowym, ale także doskonałym socjotechnikiem i człowiekiem o rozległej wiedzy z zakresu psychologii i innych dziedzin pokrewnych socjologii. Jak przyznają ludzie z tego środowiska, wielką rolę odgrywa odpowiednia rozmowa z ofiarami, bowiem często to one same podają istotne wskazówki i ważne dla *hackerów* informacje. Sztuczki psychologiczne w połączeniu z odpowiednimi trickami pozwalają bez użycia komputera wydobyć najbardziej strzeżone hasła oraz dane.

Podział ze względu na kryterium etyczne[6]

Wśród *hackerów* możemy dokonywać różnych podziałów, z których najważniejsze dotyczą etyki, motywów i metod działania. Przejdźmy więc do pierwszego, najpopularniejszego podziału. Możemy wyróżnić tutaj trzy grupy. Pierwszą stanowią tzw. *white hats*[7], czyli „białe kapelusze", *hackerzy*, którzy zajmują się testowaniem zabezpieczeń i legalną pracą dla różnego rodzaju firm, organizacji i instytucji. Zawsze działają na rzecz poprawy bezpieczeństwa i rozwoju podmiotów. Pracują przeważnie w gigantycznych firmach o rozbudowanym dziale komputerowym i z działalnością internetową, pełnią rolę specjalistów od zabezpieczeń, pracują nad udoskonaleniem systemów i poprawą wydajnościi efektywności działania. *White hats* angażują się także w działania organów ścigania i wywiadu państwowego. Odgrywają istotną rolę w poszukiwaniu możliwości dostępu do najbardziej strzeżonych i niedostępnych informacji w Internecie. Kolejną grupą są tzw. *grey hats*, co tłumaczymy jako „szare kapelusze". *Hackerzy* przynależący do tej grupy zajmują się poszukiwaniem i pozyskiwaniem danych. Próbują udowodnić społeczeństwu, że są w stanie znaleźć w Internecie bądź na żywo każdą informację. Są przekonani o tym, że dzięki własnym umiejętnościom, ogromnej wiedzy i znajomości socjotechniki mogą kontrolować dosłownie wszystko. Wykorzystują działania zarówno legalne, jak też zabronione przez prawo, z tego względu należy ich umieścić pośrodku. Ostatnią z grup są „czarne kapelusze", czyli *black hats*. Powszechna opinia określa ich jako „tych złych". Celem, który sobie stawiają, jest ukraść dane, zniszczyć wroga oraz zdewastować zawartość komputera danej osoby.

[5] Informacje pochodzą z wywiadu środowiskowego przeprowadzonego przez autora wśród czterech hackerów krakowskiej grupy Phoenix; rozmówcy chcieli pozostać anonimowi.

[6] Jak wyżej.

[7] Podział ze względu na kolor kapeluszy wywodzi się ze starych westernów, w których bohaterowie pozytywni nosili jasne kapelusze, natomiast czarne charaktery ubierały ciemne.

Podział ze względu na motywy działań

Podział przy uwzględnieniu kryterium motywu działań jest nieco bardziej rozbudowany i zdarza się, że poszczególne jego gałęzie nachodzą na siebie, przez co nie jest on rozłączny, jak ma to miejsce w przypadku poprzedniego podziału. Na płaszczyźnie motywów możemy wyróżnić *hackerów* ciekawskich, chciwych, żądnych sławy, złośliwych, pomocnych (co nie zawsze oznacza działania zgodne z prawem, o czym szerzej w dalszej części rozdziału) oraz legalnych. Zdecydowałem się na wyodrębnienie tych kategorii, gdyż to one wyczerpują uniwersum. Przejdę teraz do krótkiej charakterystyki kolejnych kategorii.

Hackerzy ciekawscy to osoby ambitne, ceniące sobie umiejętność zdobycia każdej informacji. Nie lubią, gdy informacje na stronach są owiane tajemnicą, zamaskowane czy też dobrze zabezpieczone. Z tego też powodu celem ich ataków stają się często portale społecznościowe obfitujące w ogrom informacji o osobach prywatnych, a także strony internetowe firm, instytucji rządowych, organów politycznych i wojskowych. *Hackerzy* z tej grupy włamują się do miejsc uznawanych za niedostępne i przeważnie ograniczają się do pozyskania danych informacji, nie wyrządzając przy tym szkód administratorom. Tak postąpił na przykład Ehud Tenenbaum[8], izraelski *hacker* o pseudonimie *Analyzer*, który uzyskał dostęp do ponad 1000 serwerów wojskowych, w tym do sieci Pentagonu, nie niszcząc przy okazji danych, co więcej, nawet ich nie wykorzystywał. *Hackerzy* ciekawscy pragną pogłębiać wiedzę o zabezpieczeniach i choć czynią to w sposób często niezgodny z prawem, to jednak ich działalność nie jest nastawiona na destrukcję, można więc zaliczyć ich do *grey hats*. W pewien sposób przyczyniają się do rozwoju zabezpieczeń, gdyż zazwyczaj zostawiają informację o dziurze w zabezpieczeniach, która pozwoliła im na włamanie.

Grupa *hackerów* chciwych jest najbardziej elitarną w środowisku włamywaczy komputerowych, a równocześnie jedną z najniebezpieczniejszych. Jej działalność koncentruje się wokół pozyskiwania korzyści, najczęściej majątkowych, i przybiera różne formy. Część *hackerów* chciwych zainteresowana jest wykradaniem drogiego oprogramowania i rozpowszechnianiem go przed oficjalną premierą na rynku, zarabiając przy tym ogromne sumy. Inni *hackerzy* skupiają się na manipulacjach w różnych konkursach z nagrodami, gdzie włamując się do systemu losowania i przydzielania nagród, próbują oszukać go, nakierowując na swoje konto i zwiększając swoje szanse na wygraną nawet do stu procent. Ilustrację stanowi przykład Kevina Paulsena, który dwa razy wygrał samochód Porsche 944 w konkursie radiowym dla słuchaczy stacji KIIS-FM w Los Angeles. Zwycięstwo w konkursie było możliwe dzięki zablokowaniu centrali telefonicznej w ten sposób, ze tylko Paulsen mógł się dodzwonić do radia[9]. *Hackerzy* telekomunikacyjni z kolei oszukują firmy bądź użytkowników, prowadząc na ich koszt rozmowy i korzystając za darmo z usług oferowanych przez operatorów, co powoduje znaczne straty. Obiektem zainteresowania *hackerów* zachłannych stają się również numery kart kredytowych i wirtualne sklepy internetowe, które przeważnie nie sprawdzają danych na karcie kupującego.

[8] http://www.i-slownik.pl/1,1442,tenenbaum,ehud.html.

[9] Ł. Gawrych, *Hierarchia wartości w środowisku hackerów*, praca licencjacka, Warszawa 2008, s. 17.

O metodach wyłudzania danych do kart i kont w kolejnym rozdziale. Zagrożeniem niosącym największe straty ze strony chciwych *hackerów* są włamania do kont bankowych i bankomatów. Choć ich liczba jest niewielka ze względu na skuteczne zabezpieczenia, nadal zdarzają się spektakularne kradzieże dużych kwot. Na początku wspomniałem, że grupa włamywaczy nastawiona na czerpanie korzyści majątkowych jest najbardziej elitarna w środowisku. Ma to związek ze stopniem trudności wosiągnięciu celu. *Hackerzy* bankowi muszą być bardzo przebiegli i pomysłowi oraz obdarzeni wielką inteligencją, by oszukać czujne systemy i ostrożnych administratorów.

Hackerzy żądni sławy stanowią z kolei grupę najszerszą, o czym świadczy dominujący udział popularnych stron internetowych w zbiorze celów ataków. Są to ludzie, którzy często chcą zabłysnąć umiejętnościami, zostać docenieni w środowisku, uzyskać prestiż jako osoby utalentowane informatycznie, chcą też zwrócić uwagę potencjalnych pracodawców, bowiem często zdarza się, że różne instytucje i firmy są zainteresowane pozyskaniem speców od zabezpieczeń. Warto wymienić tutaj przykład Kevina Mitnicka[10] znanego w sieci jako Kondor, *hackera*-wynalazcy, który po odbyciu wyroku założył Mitnick Security Consulting – jedną z najbardziej uznanych firm w zakresie ochrony różnych korporacji i agencji przed włamywaczami oraz intruzami.

Przedstawiciele *hackerów* złośliwych stosują najczęściej metody czarnych kapeluszy i nie zwracają uwagi na jakiekolwiek założenia etyki. Kierując się chęcią dominacji, skłonności do destrukcji oraz zemstą i złością wynikającą z prywatnych konfliktów z różnymi osobami, włamują się do cudzych komputerów, aby niszczyć dane, przejmować kontrolę nad komputerem ofiary, modyfikować i kopiować istniejące pliki. Przeważnie pozostawiają ostrzeżenia dla właścicieli komputerów zawierające często groźby i obraźliwe lub wulgarne teksty. Przykład może stanowić działająca w Polsce pod koniec lat 90. ubiegłego wieku grupa Gumisie[11], która dokonywała włamań na strony popularnych firm z różnych dziedzin.

Hackerów pomocnych charakteryzuje działalność, która w ich przekonaniu ma ułatwić użytkownikom dostęp do informacji i dóbr zgromadzonych w Internecie. Z reguły jednak podjęte przez nich działania naruszają interes innych jednostek czy też instytucji. Przykładem jest włamywanie się na strony zawierające materiały płatne w celu udostępnienia zawartości innym użytkownikom za darmo lub wykradanie filmów, gier, muzyki i programów oraz łamanie ich haseł i wrzucanie na serwery sieci wymiany plików P2P[12], serwisy torrentowe[13] czy serwery gromadzenia zbiorów. Uzasadnieniem takiego postępowania jest

[10] Kevin Mitnick (ur. 1963, Kalifornia) – najbardziej rozpoznawalny hacker na świecie. Autor *Sztuki podstępu* oraz *Sztuki infiltracji*. Socjotechnik. Obecnie związany z działalnością na rzecz poprawy bezpieczeństwa komputerowego (za: http://pl.wikipedia.org/wiki/Kevin_Mitnick).

[11] Grupa Gumisie była szczególnie aktywna pod koniec lat 90. ubiegłego wieku i specjalizowała się w atakach na strony i serwery TP SA, podmieniając strony oryginalne na własne, zawierające wulgarne lub żartobliwe protesty przeciw polityce cenowej firmy. Przywódcami grupy byli hackerzy sygnujący się jako Toudi i Księciunio (nazwy zaczerpnięte z telewizyjnej bajki *Gumisie*).

[12] Peer-to-peer = sieć wymiany plików między użytkownikami, bardzo popularna do przesyłania plików muzycznych i filmowych pochodzących z nielegalnych źródeł lub przy naruszeniu praw autorskich.

[13] Sieć wymiany plików między użytkownikami, którzy pobierają i udostępniają nawzajem pliki.

wysoka pozycja wolności w hierarchii wartości tego środowiska. Do tej grupy zalicza się tzw. *crackerów*, którzy bywają także *hackerami* złośliwymi. Stawiają sobie oni za zadanie takie obejście zabezpieczeń konkretnych programów, by działały one prawidłowo, potem zaś wystawiają je na czarnym rynku, udostępniając przy okazji kody i klucze pozwalające na swobodne i darmowe korzystanie z programów.

Ostatnią z wyróżnionych grup *hackerów* jest marginalizowana nieco przez resztę, jednak darzona szacunkiem, grupa *hackerów* legalnych wywodząca się z *white hats*, której działania są w pełni zgodne z prawem i mają na celu poprawę bezpieczeństwa w sieci oraz pracę nad rozwojem sieci internetowej, pod względem zarówno technicznym, jak też funkcjonalności. Ludzie z tej grupy dobrze znają mechanizmy sieci i mają duże umiejętności. Głównie są wynalazcami i programistami. Nierzadko pracują z policją i w działach informatycznych wielu firm; są dobrze opłacani za to, że testują zabezpieczenia i tworzą nowe bariery dla intruzów. Część *hackerów* legalnych jest tzw. nawróconymi, co oznacza, że dawniej mieli do czynienia z ciemną stroną *hackingu*, jednakże porzucili ją na rzecz legalnych działań. Wśród tej grupy istnieje sporo *hackerów*, którzy są też obrońcami moralności i zajmują się oczyszczaniem sieci z treści amoralnych i antyspołecznych.

Wymienione przeze mnie grupy tworzą spójne wypełnienie uniwersum, jednakże należy pamiętać, że podział ze względu na motywy nie jest rozłączny. Poszczególne jego elementy często zazębiają się i nachodzą na siebie, dodatkowo korelując z wcześniejszym podziałem ze względu na stopień etyczności działań co prowadzi do licznych kombinacji różnych typów *hackerów*.

System wartości w środowisku hackerów[14]

Tak jak w każdej grupie społecznej, tak i w środowisku *hackerów* komputerowych odnaleźć można wspólny dla grupy system wartości, który jest wyznawany przez wszystkich niezależnie od stopnia etyki podejmowanych działań. Środowisko *hackerów* jest środowiskiem wtórnym, bowiem pochodzą oni z różnych grup społecznych, wyznają różne poglądy i wiarę, są zróżnicowani pod względem etnicznym oraz kulturowym. Wielu *hackerów* prowadzi dwa style życia, z których jeden podporządkowany jest grupom społecznym pierwotnym, drugi zaś jest życiem w sieci internetowej. Stosunkowo niewielka część podporządkowała swoje życie *hackingowi*, lekceważąc rzeczywistość i prawdziwe życie. Skrzętnie jednak ukrywają oni swoje zainteresowania, unikają chwalenia się swymi umiejętnościami. *Hacker* nie ma przypisanego określonego stylu ubioru, zachowania czy światopoglądu. Ludzie mają różne wyobrażenia o typowych *hackerach*, jednakże z reguły nie mają one odbicia w rzeczywistości. Stereotypowe wyobrażenie *hackera* jawi się w osobie drobnego, zamkniętego w sobie okularnika, studenta prestiżowej uczelni technicznej, który całe dnie spędza przed komputerem, zapominając o życiu religijnym i społecznym. Tymczasem *hackerzy* są osobami w różnym wieku, niekoniecznie płci męskiej, raczej mocno angażują się i spełniają

[14] Informacje pochodzące z wywiadu środowiskowego wśród grupy czterech hackerów krakowskiej grupy Phoenix chcących pozostać anonimowymi i obserwacji grup hackerów w Internecie (fora internetowe, zamieszczane przez hackerów manifesty na przejętych stronach itd.).

na różnych płaszczyznach życiowych, ich wykształcenie niekoniecznie jest techniczne, gdyż część *hackerów* indywidualnie rozwija wiedzę informatyczną a dla oderwania wybrali kierunek studiów humanistyczny bądź związany z przedmiotami przyrodniczymi (albo też zainteresowanie komputerami pojawiło się później), są ludźmi rodzinnymi, nierzadko też wyznają jakąś wiarę[15].

Najbardziej cenionym aksjomatem wśród włamywaczy komputerowych jest wolność. Przejawia się ona w trzech wymiarach, o czym wspomina badacz *hackingu* Manuel Castells[16]. Jest to wolność tworzenia, wolność w dostępie do wiedzy oraz wolność form dzielenia się wiedzą. *Hackerzy* interpretują pojęcie wolności w sposób bardzo szeroki, dając tym samym uzasadnienie dla swoich ataków. Usprawiedliwienie dotyczy swobody uzyskania każdej informacji i dostępu do każdego miejsca w sieci. Piractwo komputerowe wynika także ze specyficznego pojmowania wolności jako bezpłatnego korzystania z wszelkich dóbr, które można uzyskać w Internecie. Część „białych kapeluszy" zaangażowała się w ruchy *free software* i *open source*, które propagują wolne oprogramowanie. Przedstawicielem tego poglądu jest Linus Torvalds[17], twórca jądra Linux, bezpłatnego systemu operacyjnego. Według założeń wolnego oprogramowania (FLOSS) system ten użytkownicy mogą dowolnie wykorzystywać, modyfikować i rozpowszechniać. *Hackerzy* pragną walczyć o prawo jednostki do nieograniczonego dostępu do danych, dążą do tego, by uznano dobra dostępne w Internecie za własność ogółu. Sprzeciwiają się też inwigilacji społeczeństwa w sieci, chcą rozszerzenia prawa do prywatności, którego według nich nie przestrzegają i nie szanują różne korporacje i instytucje.

Włamywacze komputerowi poza wolnością bardzo cenią prestiż i uznanie w środowisku, do czego dążą, wybierając coraz trudniejsze cele ataków bądź też tworząc coraz doskonalsze techniki włamań i narzędzia służące atakom. Spektakularna akcja wraz z zatarciem możliwie wszystkich śladów pozwala na wzrost pozycji w grupie *hackerów*, co dalej prowadzi do objęcia przywództwa w kolejnych atakach. Prestiż w środowisku *hackerskim* oznacza nie tylko szacunek kolegów, ale też możliwość znalezienia dobrej pracy w przyszłości, bowiem rynkowi giganci w każdej dziedzinie poszukują i rekrutują specjalistów w działach informatycznych często po odpowiednim rozpoznaniu w świecie internetowych podbojów.

Hackerzy cenią umiejętności i samodzielność. *Hacker* powinien być pomysłowy, bo umiejętności informatyczne nie zawsze gwarantują uzyskanie interesujących danych. Gdy jakaś osoba dokonuje włamania przy pomocy własnoręcznie napisanych programów, zasługuje na wyższy szacunek. Środowisko nie lubi zjawiska tzw. *script-kiddies*, czyli niedoświadczonych początkujących osób, które by uzyskać dostęp do różnych miejsc czy też pozyskać interesujące informacje, używają jedynie aplikacji napisanych przez innych, nie rozumiejąc przy tym podstawowych zasad i założeń danego programu. Ważną rolę w profesji

[15] Obserwacja polskiej sceny *hackingu*, grup Phoenix, Desperados, Fiery Eye, United Brothers (nazwy podane przez członków) oraz innych grup, których nazwy pozostają do wiadomości autora, ze względu na wolę anonimowości członków oraz ich obawy dotyczące utraty zaufania w środowisku i możliwości odpowiedzialności prawnej.

[16] M. Castells, *Information Age Trilogy: The Rise of the Network Society*,Oxford 1996 oraz informacje z: http://pl.wikipedia.org/wiki/Haker_(slang_komputerowy).

[17] http://pl.wikipedia.org/wiki/Linus_Torvalds.

hackera odgrywa socjotechnika i *social engineering*[18]. Jak Kevin Mitnick wspominał w swojej książce *Sztuka infiltracji*, większość haseł jest pozyskiwana przez *hackerów* dzięki umiejętnej i sprytnej rozmowie, w trakcie której ofiara dobrowolnie podaje interesującą informację bądź wskazówkę do jej uzyskania. *Hackerzy* według Mitnicka częściej łamią nie hasła, a ludzi, którzy udostępniają informacje i różne dane.[19]

W sieci internetowej łatwo można znaleźć żartobliwą twórczość ludzi utożsamiających się ze środowiskiem *hackerów*, która w znacznej części odzwierciedla jednak zasady grupy i podejście do *hackingu*. Przykład stanowi tzw. dekalog *hackera*[20]:

Dekalog hackera

Zasada podstawowa: Dobry *hacker* może wszystko.

1. Każde zabezpieczenie można złamać.
2. Włam się tam, gdzie jeszcze nikt się nie włamał.
3. Informacja chce być wolna.
4. Wina jest zawsze po stronie admina.
5. W sieci wszyscy są równi.
6. Jeśli nie możesz złamać hasła – po prostu o nie zapytaj.
7. Bądź nieprzewidywalny.
8. Hacker nie potrzebuje spać.
9. Hackera może złapać tylko inny hacker.
10. Kto ma władzę nad komputerem, ten ma władzę nad wszystkim (nad ludźmi, informacjami i światem).

Analizując poszczególne przykazania *hackerów*, możemy dostrzec specyfikę tego środowiska: każda z zasad ma sens, pomimo że niektóre wydają się wręcz absurdalne. Jakie informacje chcą nam przekazać o sobie twórcy dekalogu?

Pierwsze przykazanie wraz z zasadą podstawową stanowią potwierdzenie wiary w nieograniczone możliwości ludzi posiadających odpowiednie umiejętności i wiedzę oraz przekonanie, że nie istnieje tzw. zabezpieczenie idealne, które sprostałoby wszystkim możliwym zagrożeniom.

Druga zasada promuje oryginalność w środowisku, stawiając przed adeptami sztuki *hackerskiej* ambitne i trudne, a przede wszystkim nowe cele ataków. Ma za zadanie motywować członków środowiska do rozwijania umiejętności.

Trzecie przykazanie stanowi odzwierciedlenie pojmowania w środowisku istoty wolności (*vide* wolność w dostępie do wiedzy wyróżniona przez prof. Castellsa). *Hackerzy* powinni dbać o to, by ogół użytkowników sieci miał dostęp do informacji jako własności ogółu.

Czwarta reguła stanowi usprawiedliwienie działań *hackerów*. Środowisko próbuje tłumaczyć, że to niekompetentni administratorzy sieci i niewłaściwie postawione zabezpieczenia

[18] Inżynieria społeczna – termin powiązany z socjotechniką i społeczno-psychologicznym oddziaływaniem na ludzi w celu wpłynięcia na ich zachowanie.

[19] K.D. Mitnick, W.L. Simon, *Sztuka infiltracji*, Warszawa 2006, s. 260–285.

[20] Dekalog *hackera* można znaleźć np. na: http://forum.pclab.pl/index.php?showtopic=136181. Popularna jest też wersja audio w formie utworu anonimowego wykonawcy.

winni są atakom, gdyż z jednej strony stanowią ich potencjalny cel, z drugiej zaś pozwalają na włamanie, bo gdyby były kompletne i rzetelnie skonstruowane, to być może zdołałyby uchronić przed danym *hackerem* zabezpieczane dobro.

Piąta zasada wyraża pogląd *hackerów* o funkcjonowaniu sieci internetowej. Według nich, wszyscy użytkownicy są równi, każdy, kto ma dostęp do Internetu, ma takie same możliwości i taki sam dostęp do dóbr jak inni. Niezależnie, czy mamy do czynienia z gigantycznym przedsiębiorstwem, czy też z prywatnym internautą – mają oni takie same prawa do egzystencji w sieci oraz korzystania z informacji i dóbr.

Szósta wytyczna podkreśla istotną rolę socjotechniki w działaniach *hackerów*. Atak socjotechniczny, według magazynu „*hacking*.pl", to „kierowanie rozmową przy wykorzystaniu uczuć, wiedzy i aspiracji interlokutora przeciwko niemu samemu, co w efekcie prowadzi do jego skrzywdzenia, naruszenia prywatności lub zaszkodzenia organizacji, w której pracuje". Dzięki odpowiedniej rozmowie często można uzyskać interesujące informacje albo chociaż wskazówki, które w jakiś sposób naprowadzają na osiągnięcie celu. Potwierdzają to badania socjologów i administratorów sieci na temat haseł używanych w Internecie, gdzie znaczna część użytkowników tworzy hasło dostępu złożone z imion bliskich osób, dat ważnych chwil w życiu, przezwisk, ulubionych liczb bądź skojarzeń. Takie informacje bardzo łatwo pozyskać może każdy z nas, a co dopiero wprawiony w socjotechnicznej sztuce włamywacz komputerowy[21].

Siódme przykazanie to wskazówka doświadczonych *hackerów*. Informują oni, że warto szukać trudniejszej drogi dostępu, mniej przewidywalnej, bo przyniesie ona lepsze efekty. Początkowi cyberprzestępcy idą po linii najmniejszego oporu – szukają najprostszej, najpopularniejszej drogi, co bywa zgubne, bo wpadają w pułapki policji lub nie realizują celu, gdyż zostawiają ślady włamania, przez co mogą zostać odkryci przez administratorów. Wybierając zaś zaawansowaną technikę włamania, zmniejszają szanse na wykrycie i równocześnie zwiększają prawdopodobieństwo powodzenia.

Ósma zasada jest żartobliwym ujęciem kwestii pory ataku. Najlepiej bowiem dokonywać ataków w nocy, kiedy sieć i miejsce włamania nie są tak strzeżone, monitorowane na bieżąco przez administratorów jak za dnia. W nocy pozostaje więcej czasu na sprawne działania i dokładne zatarcie śladów. Przestępstwo zostaje wykryte później, gdy pracownicy działu informatycznego przychodzą do biura, a do tego czasu *hacker* jest już daleko. Taką sytuację można porównać do działań pająków w przyrodzie, które zastawiają sieci wieczorem, nocą łapią w nie swoje ofiary, ale rano sieć zostaje naprawiona i czysta wyczekuje na następną ofiarę, która nie domyśli się nawet, że przez noc działo się coś niepokojącego.

Dziewiąta reguła stanowi z jednej strony usprawiedliwienie w razie niepowodzenia dla *hackera* środowiska, a z drugiej to hołd dla ludzi, którzy wykrywają i przyłapują *hackerów*. Włamywacz komputerowy nie może pozwolić sobie na to, by jego działania zostały wykryte przez laika. Uważa, że tylko wybitne osoby obdarzone równie wysokimi umiejętnościami jak on, mogą przyłapać go na włamaniu, inaczej utraciłby reputację w oczach kolegów ze środowiska. Zostałby uznany za lamera, amatora, który nie zasługuje na tytuł *hackera*.

[21] R. Podsiadły, *Ataki socjotechniczne*, „Haking.pl" 2008, nr 12, s. 28–33.

Ostatnia, dziesiąta wytyczna, jest kwintesencją ogółu poglądów cyberprzestępców. Ten, kto zdoła pojąć całą magię komputera, różne sztuczki, języki programowania, programy, zasady funkcjonowania sieci i wszystkie te elementy, które składają się na wiedzę komputerową, ten ma nieograniczone możliwości ich wykorzystania.

Dekalog ten jest w pewnym sensie pomnikiem kultury. Przez swoją popularność i trwałość zawsze będzie stanowił cenne źródło wiedzy o tym środowisku oraz o profesji *hackerów*.

Metody i techniki włamań

Cyberprzestępcy, będąc grupą ambitną i pomysłową, wypracowali do tej pory wiele różnorodnych technik włamań, które sukcesywnie dopracowują i ulepszają. Programy wykorzystywane przez włamywaczy potrafią między innymi zmylić innych użytkowników, zapewnić kontrolę nad komputerem ofiary, podsłuchać lub przechwycić istotne informacje, powodować straty i zniszczenia. Środowisko *hackerów* musimy połączyć ze względu na podobne metody działań razem z innymi zjawiskami, jak *cracking*, *phreaking* i *sniffing*, chociaż nie jest to do końca poprawne powiązanie, gdyż część działań nie jest uznawana przez włamywaczy komputerowych za typowe i właściwe *hackerom*.

Zanim *hacking* uzyskał aktualną postać, którą charakteryzują włamania do sieci komputerowej, przeszedł długi proces formowania, podczas którego zmieniały się zarówno metody działań, jak i cele. Najwcześniej, bo już na początku lat 70. XX wieku, wykształciła się dziedzina *phreakingu*. Termin ten oznacza łamanie zabezpieczeń sieci telefonicznych i kojarzy się z praprzodkiem *hackerów* Johnem Draperem, o finezyjnym pseudonimie Captain Crunch. Człowiek ten użył znalezionego w paczce chipsów gwizdka, który emitował dźwięki o częstotliwości 2600 Hz, do wykonywania darmowych rozmów telefonicznych[22]. Grupy *phreakerów* zajmują się obecnie nie tylko wykonywaniem darmowych połączeń. Szerokie znaczenie ujmuje całokształt włamań telekomunikacyjnych, w tym także działalność zmierzającą do podsłuchu rozmów.

Phreaking pośrednio można więc łączyć ze *sniffingiem*, czyli działaniami nastawionymi na przechwytywanie i analizę danych przesyłanych za pośrednictwem sieci. *Snifferzy* pozyskują w ten sposób poszukiwane dane o celu bądź ofierze, a także prowadzą wywiad środowiskowy dotyczący interesujących informacji. Metoda *sniffingu* bywa wykorzystywana przez FBI jako sposób kontroli podejrzanych osób i grup przestępczych.

Do grupy podsłuchów *sensu largo* zaliczyć można także popularne *keyloggery* oraz oprogramowanie szpiegujące (*spyware*). *Keyloggery* są aplikacjami, które rejestrują każdy użyty na komputerze ofiary znak i zapisują go do oddzielnego pliku, który zostaje przesłany do *hackera*. W ten sposób włamywacze pozyskują najczęściej hasła i dane poufne. *Keyloggery* bywają oddzielnymi programami, ale mogą funkcjonować też jako element konia trojańskiego, który jest najpopularniejszym środkiem używanym zarówno przez początkujących włamywaczy, jak też przez zawodowców. Różnica polega jedynie na tym, że profesjonaliści zazwyczaj korzystają z własnoręcznie stworzonych trojanów, natomiast amatorzy (zwani w środowisku *noobami* bądź *script-kiddies*) używają programów stworzonych wcześniej

[22] Ł. Gawrych, *Hierarchia wartości w środowisku hackerów*, *op. cit.*, s. 15.

przez kogoś innego. Obecne trojany są bardzo rozbudowane i pozwalają *hackerowi* na szeroką ingerencję w komputer ofiary, włączając w to możliwość całkowitej kontroli i monitorowania działań. Konie trojańskie są tworzone przy różnych aplikacjach jako zbindowany (dołączony) element i wprowadzane do komputerów za pomocą luki w programie (*bugu*) zwanej też tylnym wejściem (*backdoorem*). Nazwa wywodzi się od analogicznie działającego konia trojańskiego z mitologii greckiej.

Hackerzy wykorzystują oprogramowanie szpiegowskie, by zdobyć informacje dotyczące numerów kont, haseł i rozmaitych cennych informacji o użytkowniku. Metody używane przez nich nie ograniczają się jednak tylko do prostych programów. Zaawansowani włamywacze układają całą strategię, która pozwala im przejąć informacje. Efektywny plan polega nie tylko na właściwym wykonaniu, ale przede wszystkim na odpowiednim przygotowaniu. *Hacker*, o czym wcześniej wspomniałem, najpierw próbuje zgromadzić jak najwięcej wskazówek, co czyni za pomocą socjotechnicznych sztuczek. Ingerencja za pomocą programów zostaje ograniczona tym samym do minimum, co ma wpływ na zmniejszenie ilości pozostawionych śladów bądź całkowite ich zatarcie.

Hackerzy, których zajęciem jest łamanie haseł i zabezpieczeń, są nazywani *crackerami*. Ten odłam zapoczątkował także kontrowersje związane z używaniem pojęcia *hacker*, bowiem media używają tych dwóch terminów zamiennie, co jest błędem. Należy podkreślić, że *crackerzy* należą do *black hats*, a ta grupa z kolei jest jedynie częścią środowiska. *Cracker* posługuje się metodami, które z reguły są niezgodne z prawem. Proces zdobycia hasła w zależności od przyjętej metody jest mniej lub bardziej czasochłonny. Jeżeli włamywacz ograniczy się jedynie do użycia programów wyciągających hasła z aplikacji i łamiących je, trwa to zazwyczaj dość krótko, bowiem zdecydowana większość prywatnych użytkowników i małych przedsiębiorstw nie posiada odpowiednich zabezpieczeń. Ilustrację zagadnienia na poziomie lokalnym może stanowić problem niezabezpieczonych sieci w Krakowie. Programiści z całej Polski, którzy 7 marca 2009 roku zebrali się na konferencji „4 Developers", wykazali poważne braki odpowiedniej ochrony w krakowskich *hot-spotach*, czyli miejscach udostępniania bezprzewodowego Internetu. Na cztery tysiące przebadanych punktów ponad dwa i pół tysiąca nie spełniło wymogów bezpieczeństwa[23]. Rodzi to poważny problem: jeżeli osoba korzystająca z takiej sieci dokona oszustwa na przykład na aukcji internetowej, odpowiedzialność spadnie na właściciela sieci.

Bardziej czasochłonną metodą na zdobycie hasła jest stworzenie odpowiedniego programu. Potrzebna jest tu nie tylko umiejętność programowania, ale także znajomość kryptografii i spora wiedza informatyczna. *Cracker* potrafi także pozyskać dane w bardziej wymyślny sposób. Może przykładowo przeprowadzić najpierw wywiad środowiskowy, poznając otoczenie ofiary i ją samą. W ten sposób uzyskuje wskazówki. Włamywacz może także próbować zdobyć kompromitujące materiały lub inne cenne dla osób dane i użyć ich do wymuszenia hasła bądź do szantaży oraz gróźb. Dobrzy socjotechnicy, którym zależy na cenniejszym łupie, potrafią doskonale maskować się i podszywać pod osoby/instytucje obdarzone zaufaniem (wiele osób bardzo chętnie poda wszystkie informacje osobie podającej się za pracownika działu informatycznego, osobę wydelegowaną przez szefa do

[23] P. Tymczak, *Hakerzy z całego świata przyjadą do naszego miasta*, „Dziennik Polski" z 9 marca 2009 roku.

sprawdzenia zabezpieczeń itd.). Takie podszywanie się pod innych użytkowników wiąże się z terminem *phishing* (także *spoofing*). Ten rodzaj ataku polega na wyłudzaniu poufnych danych przy wykorzystaniu kamuflażu. Celem stają się konta bankowe, konkurencyjne firmy na rynku bądź aukcje internetowe. *Hackerzy* posługujący się *phishingiem* starannie przygotowują odpowiednie warunki do uzyskania informacji, tworząc np. łudząco podobne do oryginalnych strony internetowe, używając takiego samego *designu* strony bądź znaków firmowych instytucji, co osłabia czujność niedoświadczonych użytkowników. Wspomniałem wcześniej, że grupa *hackerów* zajmująca się *phishingiem* posiada odmienną strukturę niż ogół środowiska. Według mnie, odłam ten jako jedyny spełnia wszystkie przesłanki wymienione przez Tadeusza Hanauska[24] definiującego zorganizowaną przestępczość grupową, która:

- dotyczy wspólnych i skoordynowanych działań grupy (częsta współpraca przy atakach)
- opiera się na kooperacji pozytywnej i pewnych zasadach hierarchizacji (można wyróżnić podział ról oraz przywódców ataku, którzy kierują działaniami)
- posiada zmienne zakresy kompetencji członków (roszady pomiędzy osobami czynnie uczestniczącymi w bezpośrednich atakach oraz socjotechnikami)
- określa cele i kierunki działań, przygotowując ich algorytmy (ścisła analiza potencjalnych celów i opracowany szczegółowo plan)
- opracowuje działania ochronne (zacieranie śladów i wycofywanie w razie niepowodzenia)
- jest nastawiona na przynoszenie korzyści (stanowi to *sui generis* cel *phishingu*).

Black hats uprawiają jeszcze jedną bardzo niebezpieczną działalność w sieci – tworzą wirusy, czyli aplikacje mające uszkodzić system operacyjny bądź pliki komputerowe. Niszczenie danych jest najbardziej dotkliwym przejawem cyberprzestępczości, zwłaszcza, że często ofiarami padają przypadkowi użytkownicy. Tworzenie wirusów wynika z chęci dominacji i jest motywowane pragnieniem władzy. Jest charakterystyczną metodą działania *hackerów* złośliwych.

Cyberprzestępczość w Polsce – stan faktyczny i prognozy

Kryminalne działania *hackerów* należą do grupy przestępstw, których ujawnienie i wykrycie stanowi jeszcze spory problem dla polskiej informatyki śledczej (*computer forensics*). Wynika to z zaawansowanego stopnia umiejętności *hackerów* oraz stosunkowo niskiej liczby wykwalifikowanych specjalistów zwalczających przestępczość komputerową. Statystyki policyjne charakteryzują jedynie ogólne tendencje cyberprzestępczości, zwracając uwagę na najbardziej popularne wśród *hackerów* formy przestępstw, jednakże nie odzwierciedlają one rzeczywistej przestępczości. Uwzględniając nasilające się zjawisko ataków internetowych na prywatne osoby oraz małe przedsiębiorstwa, które rzadko przekazują sprawę policji, oraz gigantyczny obszar piractwa komputerowego, bezsprzecznie możemy stwierdzić, że ujawniona przestępczość komputerowa stanowi niewielki procent faktycznych rozmiarów *hackingu*. Nie jesteśmy w stanie poznać dokładnych danych dotyczących przestępczości

[24] T. Hanausek, *Kryminalistyka..., op. cit.*, s. 286.

nieujawnionej z oczywistych względów, skoncentruję się więc na podsumowaniu ogólnych trendów *hackingu* w oparciu o dane Komendy Głównej Policji.

Statystyki policyjne przedstawiają zjawisko cyberprzestępczości następująco[25]

	Oszustwo komputerowe art. 287 par. 1–2	Uzyskanie informacji art. 267 par. 1–3	Zniszczenie lub zmiana istotnej informacji art. 268 par. 1–3 i 268a	Zniszczenie lub zmiana informacji art. 269 par. 1–2	Sabotaż komputerowy art. 269a	Wytwarzanie programu komputerowego do popełnienia przestępstwa art. 269b
2008	404	505	249	2	13	12
2007	492	384	168	0	11	4
2006	444	370	136	4	19	9
2005	568	260	98	3	1	6
2004	390	248	89	0	–	–
2003	168	232	138	2	–	–
2002	368	215	167	12	–	–
2001	279	175	118	5	–	–
2000	323	240	48	5	–	–
1999	217	113	49	1	–	–

Dominującym kierunkiem komputerowej działalności przestępczej jest uzyskanie nieuprawnionego dostępu do informacji, który to czyn jest penalizowany przez art. 267 kodeksu karnego. Jest to zjawisko typowe dla grupy „szarych kapeluszy", której przedstawiciele pogłębiają swą wiedzę i umiejętności, włamując się do miejsc kuszących niedostępnością i wyszukując interesujące ich dane. Na podstawie powyższych statystyk możemy stwierdzić, iż przestępstwo to charakteryzuje w ostatnich latach niewątpliwie tendencja wzrostowa, gdyż liczba ujawnionych przestępstw sukcesywnie rośnie od roku 2001 i w roku 2008 osiągnęła najwyższą wartość. Dość duży przeskok pomiędzy dwoma ostatnimi latami nasuwa istotne pytanie: czy zjawisko uzyskiwania nieuprawnionego dostępu wzrosło rzeczywiście w ostatnim roku, czy też utrzymuje się na podobnym poziomie, a wzrosły jedynie umiejętności policyjnych ekspertów do spraw walki z cyberprzestępczością? Biorąc pod uwagę intensywny rozwój sieci internetowych, które pociągają za sobą wzrost zjawiska *hackingu*, przychyliłbym się do uznania, że to pierwszy czynnik (wzrost grupy *hackerów gray hats*) przyczynił się do pogłębienia liczby tego rodzaju przestępstw. Jest to związane także ze zmieniającym się stanem gospodarki na przełomie lat 2007/2008, który wtedy jeszcze charakteryzował się napływem przedsiębiorców zagranicznych do naszego kraju, *ergo* wzrosło zainteresowanie zagranicznych *hackerów* rynkiem krajowym (mnogość nowych firm z dobrymi zabezpieczeniami i potencjalną renomą, które kuszą informacjami).

[25] http://www.policja.pl/portal/pol/4/321/Przestepczosc_komputerowa.html.

Znaczną część osób złapanych przez policję stanowią osoby młode i niedoświadczone, które kierując się osobistymi pobudkami, wynikającymi z działań podjętych w złości czy zemście, włamywały się do komputerów koleżanek i kolegów. Pomimo iż wydają się to czyny o niskiej szkodliwości społecznej, niosą duże zagrożenie dla prywatności, dlatego są szczególnie ścigane przez policję.

Nieco mniej popularnym zjawiskiem jest oszustwo komputerowe (art. 287), czyli już faktyczna ingerencja ze strony *hackerów* w dane znajdujące się na serwerach i dyskach zarówno osób prywatnych, jak i korporacji, prowadząca często do uzyskania korzyści. Do tej grupy przestępstw zaliczamy także *phishing*. Struktura oszustw wygląda bardzo nierównomiernie, co jakiś czas odnotowuje się gwałtowny wzrost bądź znaczny spadek ich liczby. Jedną z prób wytłumaczenia takiego układu jest rozwój technologii zabezpieczeń. *Phishing* dotyczy głównie kont bankowych i aukcji internetowych, które zdając sobie sprawę z zagrożenia, ciągle udoskonalają linię obrony, niwelując stopień włamań. *Hackerom* dopiero po jakimś czasie udaje się przełamać zabezpieczenia i wtedy wzrasta liczba oszustw. Powtarza się to w sposób cykliczny, powodując skoki liczby tego rodzaju przestępstw.

Trzecim zjawiskiem, które znajduje się w trójce przestępstw popularnych, jest zniszczenie lub zmiana istotnej informacji (art. 268 i 268a). Statystyka pokazuje dwa okresy, w których ten rodzaj przestępczości stopniowo się nasila. Są to lata 1999–2002 oraz 2004–2008. W roku 2008 zjawisko przybrało największe rozmiary z tych odnotowanych w statystykach i fakt ten ponownie nasuwa alternatywę: wzrosła skuteczność policji czy też nasiliło się samo zjawisko? W tym przypadku obie odpowiedzi będą właściwe. Ofiarami tych przestępstw są duże korporacje, w tym banki oraz operatorzy telefonii komórkowej, którym bardzo zależy na budowaniu swojego wizerunku jako instytucji godnej zaufania, bezpiecznej i rzetelnej. Z tego też powodu firmy te usilnie starają się eliminować wszelkie działania ze strony *hackerów* i zgłaszają je organom ścigania[26]. Artykuły 268 i 268a są przepisami, które *de facto* są zarzutami najczęściej stawianymi prawdziwej elicie *hackerów*, bowiem osoby, które przymierzają się na ataki banków, telekomunikacji czy największych korporacji, muszą posiadać dość duże doświadczenie i umiejętności. Odpowiadają oni z tego artykułu, gdyż można go najłatwiej udowodnić. Podmieniając oryginalną stronę, *hackerzy* niszczą przecież lub zmieniają informacje na niej zawarte, a to z reguły zostaje udokumentowane później przez firmy w postaci chociażby zrzutu ekranu. Oszustwo lub nieuprawniony dostęp wymaga dokładniejszej analizy i potrzeba wykwalifikowanych informatyków śledczych, którzy będą w stanie odzyskać i zinterpretować np. skasowane dane, pliki tymczasowe, logi, rejestry, pocztę elektroniczną, powiązania z innymi sieciami, partycje dysków lub pliki wymiany. Lata 2002–2003 wiążą się ze spadkiem odnotowanych przestępstw zniszczenia lub zmiany informacji. Jedna z prób wyjaśnienia spadku mówi że było to spowodowane niepokojem środowiska. W roku 2001 dokonano wielu spektakularnych włamań na strony oddziałów Telekomunikacji Polskiej, które były zorganizowaną akcją wymierzoną przeciw operatorowi. *Hackerzy* przejęli strony oddziałów w Gorzowie, Krośnie, Łomży i Lublinie (podczas jednego weekendu – 27 maja 2001 roku), a także w Koszalinie, Psarach, Zielonej Górze, Szczecinie, Słupsku i Kielcach. Ataki przypisuje się

[26] Informacje pochodzące z wywiadu środowiskowego wśród członków grup Phoenix oraz Fire Eye.

grupie Gumisie. 1 czerwca włamywacze komputerowi z grupy Red Wave postawili sobie za cel przejęcie 10 stron, a kolejnym krytycznym dniem był 10 czerwca, kiedy *hackerzy* przeprowadzili 7 udanych ataków (przejęto serwery Biblioteki Głównej Akademii Medycznej w Poznaniu, Wydziału Rolniczego AR w Szczecinie, TP SA w Słupsku, Phi Beta Kappa Society, Ars Info, Informafu oraz strony zagranicznej bstc.cc.al.us). Tymi dwoma seriami ataków zainteresowała się policja i przez dwa lata mocno infiltrowała środowisko *hackerów*, przez co wtedy ich aktywność spadła[27].

Przestępstwa karane z artykułu 269 oraz 269a i 269b stanowią mały odsetek notowanych przejawów cyberprzestępczości, co wynika rzeczywiście z rzadkiego ich występowania oraz trudności w wykryciu sprawcy i udowodnieniu mu czynów. Oczywiście zdarzały się pojedyncze przypadki ataków na instytucje rządowe (serwery Urzędu Rady Ministrów i Ministerstwa Obrony Narodowej), jednakże nie są one tak popularne, gdyż środowisko jest świadome konieczności ścigania przestępstw zagrażających instytucjom państwowym i obronności kraju i nie chce się niepotrzebnie narażać.

Pośrednim owocem działań *hackerów* są przestępstwa umożliwiane przez *crackerów*, czyli łamanie kodów zabezpieczających programy komputerowe i wprowadzanie ich na czarny rynek jako udostępnianych za nielegalną opłatą bądź nawet za darmo. Piractwo komputerowe jest coraz powszechniejsze i w porównaniu z innymi typami przestępstw stanowi największy element cyberprzestępczości. Rozwija się bardzo dynamicznie i według prognoz stwarza największe zagrożenie dla rynku. W ciągu zaledwie 9 lat liczba odnotowanych kradzieży programów wzrosła prawie 15-krotnie[28].

Kradzież programu komputerowego art. 278 § 2	
2008	15.093
2007	14.426
2006	10.635
2005	10.538
2004	8.914
2003	9.734
2002	5.722
2001	6.220
2000	6.461
1999	1.197

Przewidywania dotyczące cyberprzestępczości na rok 2009 były niepokojące ze względu na pogłębiający się kryzys ekonomiczny. Eksperci Trend Micro ocenili, że to przestępstwo *phishingu* stanie się dominującym problemem, co znajduje potwierdzenie w rzeczywistości nawet teraz, w 2010 roku. Paul Ferguson, specjalista do spraw badanych zagrożeń, przewidział, że użytkownicy podczas kryzysu będą bardziej podatni na klikanie

[27] Informacje pochodzą ze strony http://www.artur.pl/muzeum2.html, obserwacji własnych i wywiadu środowiskowego.

[28] http://www.policja.pl/portal/pol/34/591/Kradziez_art_278.html.

w niewłaściwe linki związane na przykład ze spamem wysyłanym na skrzynki pocztowe, gdyż *hackerzy* mogą próbować wysyłać fałszywe ostrzeżenia dotyczące rzekomych fuzji banków, zajęcia obciążonych nieruchomości itd. Już w 2008 roku *phishing* zebrał spore żniwo (ataki gangu Rock Phish w kwietniu na klientów Bank of America oraz ataki wrześniowe na Wachovia Bank i bank Merrill Lynch). Teraz *hackerzy* mogą dodatkowo kusić fałszywymi promocjami oraz szantażować różne przedsiębiorstwa, wymuszając okup za zaniechanie ataków bądź przywrócenie stanu przed włamaniem[29].

Hacking jest bardzo niebezpiecznym zjawiskiem, które przyczynia się do wzrostu cyberprzestępczości zarówno w sposób bezpośredni (ataki, zniszczenia), jak i pośredni (łamanie kodów, umożliwianie piractwa). Biorąc pod uwagę postępujący rozwój techniki i popularność Internetu, zjawisko to będzie się pogłębiać w najbliższych latach, powodując stopniowe zwiększenie udziału przestępczości komputerowej w ogólnej strukturze przestępstw. Z tego też powodu niezwykle potrzebne wydają się inwestycje i rozwój informatyki śledczej, zwłaszcza w kwestii podnoszenia kwalifikacji pracowników tego pionu, by móc efektywnie przeciwdziałać *hackerom* i zapobiegać niebezpieczeństwu *phishingu*, które w najbardziej dotkliwy sposób narusza prywatność, poufność, integralność i dostępność danych.

[40] http://www.egospodarka.pl/38232,Kryzys-ozywia-cyberprzestepczosc,1,12,1.html.