ROZDZIAŁ

3

KTO CHCE NAM ZAGROZIĆ?



3 Kto chce nam zagrozić?

3.1 Hacker, Cracker i ugrupowania

Internet jest miejscem, które zdecydowanie zawładnęło ludzkim światem. Zakupy, oszczędności, prywatne dane, kontakty – wszystko to skupia się w Internecie. Jednak wśród ogromu ludzi korzystających z dostępu do sieci są też tacy, którzy nie zawsze mają dobre i uczciwe zamiary. Próbują oni wykorzystać swoją wiedzę o budowie i strukturach Internetu by wykradać dane lub pieniądze z kont innych użytkowników sieci. Osoby takie nazywamy hackerami.

Hacker to osoba, która wyszukuje i wykorzystuje dziury w oprogramowaniu, by następnie je wykorzystać na swoją korzyść. Hackera możemy porównać do włamywacza, który sforsuje zamek i dostanie się do środka chronionego obiektu.

Rysunek 3.1 Symboliczny obraz Hackera (*Źródło: https://mashable.com)*

W przypadku sieci, dostanie się do chronionego systemu informatycznego przeglądając i wykradając poufne dane w celu ich sprzedaży lub szantażu. Hackerzy stosują różnego rodzaju metody socjotechniczne, spam i fałszywe witryny w swoich działaniach.

Osoby zajmujące się przestępczością internetową mają różne zainteresowania i cele. Oni sami lubią się też od siebie odróżniać.

I tak **Cracker** to ktoś, kto łamie zabezpieczenia wszelkiego rodzaju oprogramowania lub serwerów wykorzystując znajomość języków programowania oraz kodu binarnego. Głównym celem Crackera jest napisanie kodu, który udostępni nielegalnie oprogramowanie lub pozwoli na nieautoryzowany dostęp do serwera. Dla Crackera pojęcie Hacker to inaczej przestępca internetowy, który często wykorzystuje narzędzia Crackera do swoich celów.

Anonymous to najbardziej rozpoznawane ugrupowanie skupiające ludzi sprzeciwiających się cenzurze, korupcji czy wpływowi kościoła katolickiego. Mają wiedzę i umiejętności pozwalające im nazywać się Hackerami, jednak mają bardziej ugruntowany cel społeczno – polityczny.

Rysunek 3.2 Logo Anonymous *(Źródło: http://www.forbiddensymbols.com/anonymous/)*

Dążą oni do uzyskania ogólnoświatowego równouprawnienia, sprawiedliwości i wolności słowa. Anonymous są bardzo zaangażowani w sytuację polityczną na całym świecie i aktywnie działają w sprawach wyższej wagi. Działacze Anonymous są poszukiwani na prawie całym świecie, a jedną z najaktywniej ścigających tych działaczy organizacji jest FBI.

Są też inne ugrupowania Hackerów i Crackerów występujące pod różnymi nazwami i kierujące się różnymi celami. Niestety są też tacy, którzy są bardzo zradykalizowani w swoich poglądach i działaniach. Ich działania są często bardzo dotkliwe, możemy nazwać je nawet cyberterroryzmem zagrażającym bezpośrednio gospodarce i przede wszystkim życiu ludzi.

Jak można łatwo zauważyć cała ta sfera owiana jest tajemnicą i lekkim bałaganem pojęć. Co innego mówią specjaliści, co innego władze, a co innego sami Hackerzy czy Crackerzy. Jednak na pewno możemy powiedzieć, że Hackerzy i Crackerzy to ludzie, którzy:

- Posiadają dużą wiedzę na temat działania podstawowych struktur aplikacji i samej sieci.
- Muszą znać języki programowania.
- Posiadają umiejętności psychologiczne i socjologiczne, muszą orientować się w sposobie działania użytkownika systemu i sieci.
- Często posiadają wykształcenie informatyczne lub mają takie hobby.

Ze względu na cele jakie przyświecają tej grupie ludzi możemy powiedzieć, że mamy grupę przysłowiowo „złych" i „dobrych" hackerów. Do grupy „złych" zaliczamy tych, których cele związane są z przestępczością lub złośliwym działaniem w celu osiągniecia chorej satysfakcji.

„Dobrymi" hackerami możemy nazwać tych ludzi, którzy mają wiedzę i umiejętności hackerów, ale nie chcą się nimi identyfikować, ponieważ nie chcą popełniać przestępstw sieciowych. Sprzeciwiają się oni cyberprzestępczości i cyberterroryzmowi, działają wprawdzie często na granicy prawa, ale dla ogólnego dobra. Chcą poznać działanie systemów dla ogólnej świadomości społeczeństwa i w celu likwidacji zagrożeń.

Osoby posiadające takie cele często są aktywistami lub pracują jako specjaliści od zabezpieczeń. Tworzą wolne oprogramowanie i ujawniają zasady działania urządzeń w celu przeciwdziałania błędom w oprogramowaniu, zmuszając producentów do usuwania wad w ich urządzaniach i programach.

3.2 Firma szukająca lub oferująca tanią i nieuczciwą reklamę

Na nasze skrzynki poczty elektronicznej przychodzi dużo różnych reklam, ogłoszeń czy ankiet, tzw. **spamu**. Część z tej korespondencji jest przez nas nie zamówiona, ponieważ nigdy świadomie nie zgadzaliśmy się na jej otrzymywanie. Ktoś, kto ją wysłał odgadł lub automatycznie wygenerował nasz adres, albo zdobył go nieuczciwymi metodami.

Korespondencja taka przeważnie nie jest dla nas niczym niebezpiecznym, jednak może zawierać złośliwy kod, ponieważ nie wszystkie firmy zadawalają się tylko wysłaniem treści reklamowej.

Zdarzają się sytuacje, gdzie firmy zatrudniają Hackerów w celu pozyskania informacji bardziej szczegółowej na nasz temat. Takie firmy również handlują naszymi preferencjami produktowymi, zwyczajami, a nawet tajemnicami pokazującymi nasze słabe strony. Oczywiście działają pod przykrywką legalnych działań, ukrywając dodatkowe źródła dochodów przed władzami i konsumentami ich produktów.

Hackerzy znając się na metodach socjotechnicznych, przygotowują na zlecenie takich firm scenariusze działań i złośliwe oprogramowanie do podsłuchiwania aktywności w sieci. Oczywiście takie oprogramowanie musi trafić do wielu użytkowników, więc podczepia się je za pomocą włamań do serwisów internetowych, wysyła w spamie.

Częstym działaniem jest podszywanie się pod znane i cenione firmy, witryny, organizując ankiety lub konkursy z atrakcyjnymi nagrodami, gdzie pytania są proste, oczywiście nagroda jest cenna i gwarantowana. Niestety, ale w taki sposób po prostu sami udostępniamy swoje dane

adresowe i osobowe, a żadnej nagrody nie otrzymamy. Metoda taka to tak zwany **scam**.

Rysunek 3.3 Fałszywy konkurs (Źródło: https://interaktywnie.com)

3.3 Złodziej, czyli fałszywy profil w Internecie

Weryfikacja tożsamości, czy też wiarygodność zamieszczanych danych w sieci jest bardzo trudna do wykonania. Skutkiem tego jest możliwość stworzenia fikcyjnego adresu e-mail, konta na portalu społecznościowym i nie tylko. Kłopoty zaczynają się jednak wtedy, gdy stworzony profil wykorzystuje dane prawdziwej, realnej osoby. Pamiętajmy, że jest to karalne.

Skradzione dane mogą zostać wykorzystane do uwiarygodnienia przestępstwa, podrabiania dokumentów, czy też zrobienia zakupów na rachunek ofiary. Nieświadomość użytkowników jest tu kluczową przyczyną stania się ofiarą.

Miejsce zamieszkania, aktualna lokalizacja, numer telefonu, czy też nasz adres e-mail. Te wszystkie informacje, które zamieszczamy na naszych profilach portali społecznościowych mogą być tzw. wabikiem na cyberprzestępców.

Innym powodem tworzenia fałszywych kont przez złodziei internetowych jest wyłudzenie pieniędzy, od znajomych ofiary kradzieży tożsamości. Tylko ostrożność pomoże nam rozpoznać fałszywy profil, dzięki kilku charakterystycznym cechom, chociaż przestępcy często zmieniają scenariusze działań.

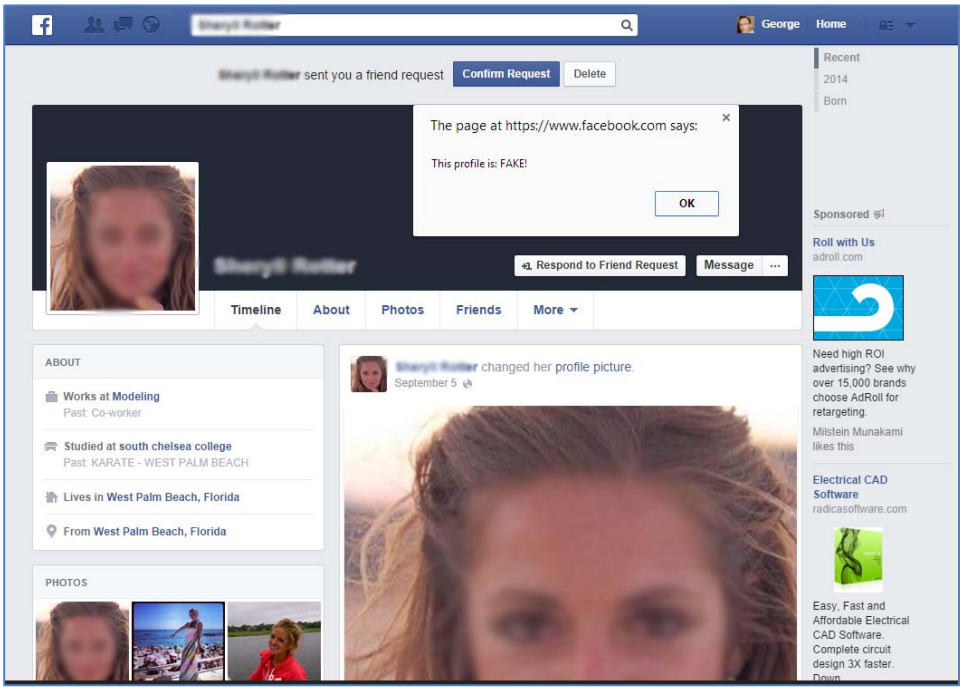
Zazwyczaj fałszywe profile nie są zbyt długo aktywne, mają sztampowe wpisy, wiele przeklejonych informacji z innych profili, a zamieszczanie postów jest bardzo rzadkie. Takie konta mają bardzo dużo znajomych, ponieważ właściciele fałszywych kont zapraszają wszystkich po kolei. Natomiast zdjęcia na profilu, jeśli w ogóle są, to mogą nie mieć zbyt wielu polubień. Jest to podejrzane, jeśli ma się sporą listę znajomych, a aktywność jest szczątkowa. Aby utrudnić życie takim oszustom, możemy wyłączyć opcję podglądu kto należy do grona naszych znajomych, ukrywać swoje dane przed podglądem publicznym, a także ostrożnie akceptować zaproszenia, zawsze dokładnie weryfikując zapraszającego.

Musimy jednak cały czas pamiętać, że fałszerz będzie zmieniał techniki tak, aby utrudnić swoje rozpoznanie i uwiarygodnić sobie profil. Być może już teraz powstała całkiem nowa metoda przygotowania kradzieży. Niestety w świecie realnym i wirtualnym przestępca zawsze jest krok przed nami.

3.4 Ataki ukierunkowane

Ataki ukierunkowane są coraz częstszym zagrożeniem dla firm, organizacji i nawet całych rządów. Ataki takie mogą być zamówione dla korzyści materialnych lub kierowane światopoglądem, albo innym przekonaniem.

Cyberterroryści stosując różne metody wykradają ważne informacje, niszczą wizerunek lub blokują. Przed atakiem napastnicy zbierają informacje o sposobie działania ofiary na wielu płaszczyznach. Następnie gromadzą zasoby i obmyślają strategię ataku.

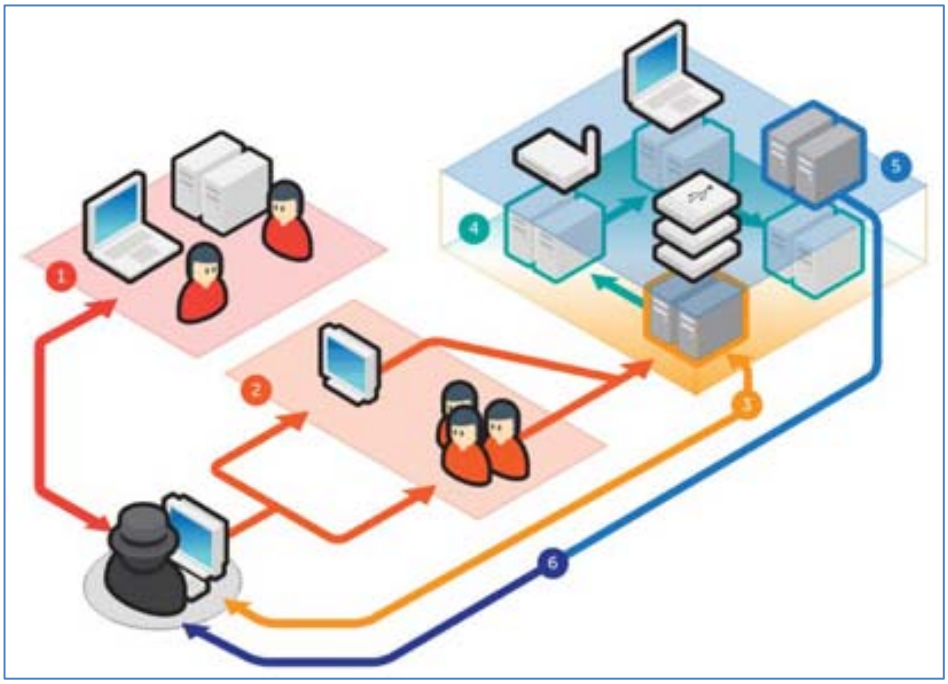


Rysunek 3.4 Fałszywy profil w sieci (Źródło: https://greece.greekreporter.com)

Wywołują przeciążenia serwerów poprzez wysyłanie ogromnej liczby żądań łączności DDOS, socjotechnikę, spam i fałszywe wiadomości (**fake news**). Wykorzystując błędy pracowników lub zabezpieczeń systemów firmy napastnicy osiągają swój cel. Może mieć to katastrofalne skutki.

Pomimo coraz większego zagrożenia atakami ukierunkowanymi to wciąż są organizacje, firmy lub instytucje bagatelizujące zagrożenie lub nie inwestujące odpowiednich środków w metody przeciwdziałania i zabezpieczania danych i sprzętu.

Za spektakularne i szeroko znane ataki ukierunkowane była odpowiedzialna organizacja **Anonymous**, o której już wspominaliśmy.



Rysunek 3.5 Atak ukierunkowany (Źródło: https://blog.trendmicro.pl)