171 milionów dolarów straty i utrata reputacji w oczach milionów klientów – to wszystko przez złośliwy skrypt, którego napisanie zabrało młodemu hakerowi jedynie 10 godzin.

Procesy hakerów oskarżonych o kradzież poufnych danych z systemu amerykańskiej korporacji TJX właśnie dobiegły końca. Jeszcze w maju skazani mają zameldować się w więzieniach. Sprawa ciągnęła się od 17 stycznia 2007, kiedy firma po raz pierwszy ujawniła informacje dotyczące kradzieży numerów kart bankowych swoich klientów. Był to wówczas największy zanotowany w historii wyciek danych – w ręce cyberprzestępców dostało się 45 milionów numerów kart kredytowych, o łącznym rozmiarze 80 GB. Na chwilę obecną usuwanie strat kosztowało firmę 171 milionów dolarów.

Zdaniem ekspertów od bezpieczeństwa z firmy **G Data Software**: „Z posiadanych przez nas danych wynika, że w samym 2009 roku ponad dwie trzecie badanych firm i instytucji miało problemy spowodowane złośliwym oprogramowaniem. Mimo lekcji odebranych przez niektóre przedsiębiorstwa, takie rzeczy będą zdarzać się również w przyszłości. W imię oszczędności wiele firm myśli krótkoterminowo, przykładając należytą wagę do zabezpieczeń dopiero po tym, jak doświadczą ataku na własnej skórze. Szybko okazuje się jednak, że poniesione straty przekraczają wielokrotnie zakładane korzyści. Firma jest tak słaba jak jej najsłabsze ogniwo, a w przypadku TJX tym ogniwem były dane przetrzymywane bez należytego zabezpieczenia."

Zarabiali miliony, on nie dostał niczego
Mózgiem całej operacji był Albert Gonzales, szef międzynarodowej grupy cyberprzestępczej o nazwie ShadowCrew. Gonzales spędzi najbliższe 20 lat w więzieniu. Wśród znajomych znany był z tego, że często przebywał w luksusowych hotelach, a na jedno ze swoich przyjęć urodzinowych wydał 75,000 dolarów. Pewnego dnia podobno narzekał na to, że musi ręcznie liczyć 360 tysięcy dolarów jakie zarobił na internetowych przekrętach, ponieważ zepsuł mu się automat do liczenia pieniędzy. Jak się okazało w trakcie śledztwa, był on również inicjatorem jeszcze bardziej spektakularnego ataku na amerykańską instytucję finansową Heartland. W chwili aresztowania policja znalazła w domu Gonzalesa w Miami ponad milion dolarów gotówką.

W sprawie TJX skazanych zostało w sumie 11 osób z różnych krajów. Prawdopodobnie największe kontrowersje wywołuje wyrok nałożony na Stephena Watta: dwa lata więzienia oraz pokrycie strat firmy i kosztów sądowych na sumę 171 milionów dolarów. Ten 26-latek miał jeszcze do niedawna obiecującą karierę na Wall Street, z zarobkami sięgającymi 130 tysięcy dolarów rocznie. Wszystko to zmieniła chwila, kiedy na prośbę Gonzalesa zgodził się napisać złośliwy skrypt do wyciągnięcia informacji z systemu informatycznego TJX. Napisanie i przetestowanie programu zajęło mu zaledwie 10 godzin. Adwokat Watta argumentował, że była to jedynie przysługa i z dokonanych ataków Watt nie otrzymał od Gonzalesa nawet centa, ani też nie wiedział gdzie dokładnie oprogramowanie zostanie wykorzystane. Jego zdania nie podzieliła ława przysięgłych.

Wirtualny atak, realne straty
Chociaż od daty ujawnienia przestępstwa minęło 14 miesięcy, TJX wciąż liczy straty. Eksperci z TJX szacują, że w wyniku ataku firma utraciła 171 milionów dolarów. Złożyły się na to koszty związane z usuwaniem strat ataku, odszkodowania dla klientów, koszty procesów. W wyniku trwających nadal postępowań o odszkodowania suma ta może wzrosnąć w ciągu następnych lat do 1 miliarda. Firma postanowiła załatać system bezpieczeństwa angażując do pracy specjalistów z General Dynamics, IBM i Deloitte.

Stephen Watt, zapytany przez reportera Wired.com o odczucia na temat całej tej sprawy, odpowiedział: „Z moralnego punktu widzenia zupełnie nie żałuję tego co zrobiłem. Nie jest to coś, co by mi specjalnie spędzało sen z powiek. Martwią mnie tylko szkody, jakie może to potencjalnie wyrządzić mojej matce oraz żonie."

Someday Interactive