**Międzynarodowe sukcesy w walce z cyberprzestępczością w sierpniu 2013 r.**

**Jakie cechy posiada cyberprzestępca? Jeżeli pominiemy aspekty techniczne, dokładnie takie same jak tradycyjny przestępca. Osoby takie łamią prawo i – przy odpowiednich staraniach organów ścigania – trafiają za kratki.**

Cyberprzestępcy często nie wiedzą jednak o tym, że społeczność ekspertów IT pomaga policji na całym świecie tropić internetowe szumowiny. To dlatego aresztowania są dla nich zazwyczaj ogromnym zaskoczeniem – wydaje im się, że nie można ich złapać. Eksperci z Kaspersky Lab przygotowali zestawienie sierpniowych sukcesów w walce z cyberprzestępczością.

**Orient Express**

Przynajmniej 17 osób było zaangażowanych w cyberprzestępczą grupę „Western Express”, która specjalizowała się w kradzieży numerów kart kredytowych. Nazwę „Western Express” wymyślili policjanci ze względu na to, że przestępcy wykorzystywali do swoich transakcji międzynarodową sieć American Western Express. Członkowie grupy weszli w posiadanie i sprzedali łącznie 95 tysięcy numerów kart kredytowych. Szkody wyrządzone przez cyberprzestępców są szacowane na 5 milionów dolarów. Na dzień dzisiejszy skazanych zostało 11 członków szajki.

Grupa „Western Express” składała się z obywateli wielu krajów, m.in. Rosji, Ukrainy i Mołdawii. Najbardziej dotkliwy wyrok – do 40 lat pozbawienia wolności – usłyszał ukraiński haker Jegor Szewielow, znany jako Eskslubur lub Esk, który został oskarżony o sprzedaż 75 000 skradzionych numerów kart kredytowych. Służby specjalne aresztowały także administratora forum DumpsMarket, które pośredniczyło w tej nielegalnej sprzedaży. Jednocześnie, podobne wyroki przedstawiono twórcom systemu e-płatności WEI – Wadimowi Wasiljence i jego żonie Elenie Barysziewej, którzy byli zaangażowani w pranie brudnych pieniędzy w ramach tej samej grupy przestępców. Oskarżeni przyznali się do wszystkiego.

**Winny czy niewinny?**

Nie każdy przestępca chce jednak wyznać swoje grzechy. Pewien obywatel Rosji – niejaki Dmitrij Smilaniec – mimo solidnych dowodów przeciwko niemu do dzisiaj nie przyznaje się do udziału w sprawie, która praktycznie została już zamknięta. Do dowodów tych należy około 160 milionów zdefraudowanych kart kredytowych i straty szacowane na 300 milionów dolarów. Dmitrij jednak nie chce puścić pary z ust - oświadczył jedynie, że jest właścicielem klubu cybersportowego Moscow Fife, a nie jakimś tam złodziejem. Mimo to organy ścigania mają solidne podstawy, by sądzić inaczej –udowodniono już winę kilku partnerom Dmitrija. Na ostateczne zakończenie tej sprawy musimy jednak jeszcze zaczekać.

**Ściśle tajne**

Reynaldo Rivera został oskarżony o ujawnienie danych osobowych w Stanach Zjednoczonych w ramach ataku na sieć Sony Pictures Entertainment. W 2011 r. Rivera był członkiem grupy Lulzsec, która spenetrowała serwery Sony i weszła w posiadanie danych osobowych i rejestracyjnych setek tysięcy użytkowników usługi tego giganta, po czym udostępniła publicznie wszystkie informacje zgromadzone w trakcie ataku. Mimo że atak nie pociągnął za sobą strat finansowych, ujawnianie takich informacji jest zabronione przez prawo. Poza rokiem pozbawienia wolności Rivera został ukarany grzywną w wysokości 605 tysięcy dolarów.

**E-płatności pod ostrzałem**

Sąd w Moskwie skazał na 2,5 roku więzienia Pawła Wróblewskiego – udziałowca w systemie e-płatności Chronopay. Zgodnie z informacjami ujawnionymi w ramach śledztwa, w 2010 r. Wróblewski zamówił atak DDoS na konkurencyjną firmę Assist. Celem ataku było storpedowanie i w efekcie wymuszenie zerwania kontraktu między rosyjskimi liniami lotniczymi Aeroflot a firmą Assist. Sprawa ta jest szczególnie istotna, ponieważ po raz pierwszy w historii rosyjskiego prawodawstwa postawiono zarzuty zarówno osobom, które zamówiły atak, jak i jego wykonawcom.

**To nie ja!**

Denis Czalowski, obywatel Litwy, znalazł się w dość niekomfortowej sytuacji – jego dalszy los rozstrzygnie się podczas przesłuchań prowadzonych przez europejskie i amerykańskie organy ścigania. Amerykanie sądzą, że Denis jest przestępcą – według ich danych, Czalowski, Rosjanin Nikita Kuzmin i obywatel Rumunii Mikhai Paunesku stworzyli oraz rozprzestrzenili wirusa Gozi, który zainfekował ponad milion komputerów na całym świecie. Szkodnik ten został użyty do zhakowania dziesiątek tysięcy kont bankowych i wygenerował straty na poziomie kilkudziesięciu milionów dolarów. Do ofiar wirusa Gozi należy 160 komputerów NASA. Łącznie, Czalowski może zostać skazany na 67 lat pozbawienia wolności.

Jest jednak druga strona tej opowieści. Sam Denis nie przyznaje się do niczego i ma świadka, który zeznał, że Czalowski nie byłby w stanie stworzyć jakiegokolwiek szkodliwego programu, ponieważ zna się wyłącznie na naprawianiu komputerów i nie jest programistą. Sprawę komplikuje jeszcze bardziej ekstradycja Denisa do Stanów Zjednoczonych, która miała miejsce, mimo że nie istnieją przeciwko niemu jednoznaczne dowody. W związku z tym, europejskie organizacje praw człowieka bronią Czalowskiego przed zarzutami Amerykanów. Sytuacja jest zagmatwana i sprawa zapewne nie zostanie szybko rozwiązana.

**INTERPOL: Szanghaj na linii**

Po raz pierwszy w historii oddział policji w Szanghaju odpowiedzialny za przestępstwa online współpracował z INTERPOLem w celu ujęcia lidera grupy odpowiedzialnej za kradzież blisko 30 milionów Yuanów (około 5 milionów dolarów) od obywateli Chin. Ponad dwa tysiące Chińczyków padło ofiarą grupy pięciu hakerów ukrywających się na Tajlandii. Schwytani zostali wszyscy z nich z wyjątkiem niejakiego pana Vana, który – jak się okazuje – jest liderem grupy i ciągle się ukrywa. Co ciekawe, Van odbył już raz karę 14 miesięcy pozbawienia wolności, nałożoną na niego za zaangażowanie w nielegalne zamknięcie aukcji online w 2009 r. Jak widać, pobyt w więzieniu niewiele zmienił w nawykach tego przestępcy. Z raportów organów ścigania wynika, że Van nie zatarł za sobą wszystkich śladów, więc schwytanie go jest tylko kwestią czasu.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.