**Wrześniowa kronika cyberkryminalna: jesienne aresztowania**

**Wrzesień już się skończył i najwyższy czas, by sprawdzić, jakie postępy w łapaniu cyberprzestępców poczyniły organy ścigania przy współudziale ekspertów ds. bezpieczeństwa IT na całym świecie. Eksperci z Kaspersky Lab przygotowali zestawienie wrześniowych sukcesów w walce z międzynarodową cyberprzestępczością.**

**Szaman i twórca wirusów w jednym**

Na rozległych terenach Rosji nierzadko dzieją się dziwne rzeczy. Całkiem niedawno mieszkaniec Wołgogradu został złapany i skazany za kilka przestępstw związanych z praktykami okultystycznymi i rozprzestrzenianiem szkodliwych programów. W małym rodzinnym biznesie niejaki Azamat Werbicki pełnił rolę szamana i przy okazji wyłudzał pieniądze od niczego nie podejrzewających ofiar. Najwyraźniej jednak szamańskie rytuały nie przynosiły mu wystarczających zysków, ponieważ zajął się dodatkowo pisaniem i rozprzestrzenianiem trojanów bankowych. Okazało się, że lepiej byłoby dla niego, gdyby pozostał przy swoim pierwotnym zajęciu – jego nowa cyberprzestępcza osobowość bardzo szybko przyciągnęła uwagę policji, a aktywną rolę w schwytaniu tego przestępcy odegrali analitycy z Kaspersky Lab. W ciągu najbliższych siedmiu lat pozbawienia wolności Azamat będzie musiał zaprzestać swojej działalności szamańskiej i programistycznej.

**Stary miś... nowe sztuczki**

Mogłoby się wydawać, że typowy cyberprzestępca to młody, zbuntowany człowiek. Dlatego właśnie 62-letni Michael Musachchino wyróżnia się z tłumu. Ten były pracownik firmy Exel Transportation Services z Teksasu chciał dorobić sobie do emerytury rozpoczynając własną działalność gospodarczą. Problemem okazało się jednak stworzenie bazy usługobiorców i Michael postanowił zainteresować się klientami swojego byłego pracodawcy. Musachchino włamał się do sieci firmowej i przeprowadził szpiegostwo przemysłowe, co - ku jego niezadowoleniu - nie umknęło służbom bezpieczeństwa firmy. Sędzia prowadzący rozprawę najwyraźniej wykazał się poczuciem humoru – wiedząc, że Musachchino ma 62 lata, skazał go na 63 miesiące więzienia.

**Z wesela do więzienia**

John Anthony Borell III – haker z Toledo (Ohio, USA) - nie tylko włamywał się do serwerów, ale także ożenił się tuż przed tym, jak został schwytany. Sędzia oznajmił, że zapoznawał się z aktami sprawy „z zainteresowaniem oraz smutkiem” i nałożył na Johna na stosunkowo łagodną karę – trzy lata pozbawienia wolności w więzieniu, które znajdowało się niedaleko od domu Borella. Niestety, sędzia dorzucił to tego także grzywnę w wysokości 227 000 dolarów, którą Borell musi zapłacić właścicielom zhakowanych stron. A biorąc pod uwagę to, że więzienie znajduje się blisko domu hakera, jego żona z pewnością będzie codziennie przypominała mu o długach, w jakie ich wpędził. A przy okazji – niektórzy eksperci uważają, że John Anthony Borell III ma powiązania z grupą haktywistów Anonymus.

**2,1 mln dolarów do podziału na ośmiu**

Grupa ośmiu złodziei została niedawno schwytana w Wielkiej Brytanii po włamaniu do banku Barclays. Przestępcy wykonali napad, którego nie powstydziłby się autor scenariusza do hollywoodzkiej produkcji – podszyli się pod pracowników banku, uzyskali fizyczny dostęp do sieci korporacyjnej i zainstalowali specjalne urządzenie, które pozwoliło im ukraść 2,1 mln dolarów. Wszystko miało miejsce w kwietniu 2013. Natychmiast po wykryciu niekontrolowanego wypływu pieniędzy system alarmowy banku powiadomił ochronę, jednak do aresztowania cyberprzestępców doszło dopiero w połowie września. Ręka sprawiedliwości nie była może w tym przypadku szybka, jednak z pewnością długa i skuteczna.

**Rumuńska miłość do pieniędzy**

Dwóch przedsiębiorczych i zaawansowanych technicznie obywateli Rumunii zostało aresztowanych w Stanach Zjednoczonych za liczne cyberprzestępstwa. W latach 2009 – 2012 zhakowali oni kilkaset terminali POS (wykorzystywanych w sklepach do realizowania płatności kartą) i zainstalowali szkodliwe oprogramowanie, które umożliwiło im przechwytywanie danych związanych z transakcjami i kartami płatniczymi klientów. Oficjalnie zakomunikowano, że cyberprzestępcom udało się tego dokonać przy użyciu luk w 250 terminalach. W ramach cyberataku poszkodowanych zostało około 100 000 osób, a łączne straty oszacowano na 17,5 mln dolarów. Skala cyberataku i wywołane przez niego straty były tak duże, że wyrok musiał być odpowiedni: „mózg operacji” - Adrian-Tiberiu Oprea - trafił do więzienia na 15, a jego wspólnik - Lulian Dolan – na siedem lat.

**Game over...**

...dla hakera Dmitrija Szaszkina z Moskwy, który kradł hasła do płatnych gier online. Może nie mamy tu do czynienia z milionami dolarów wyprowadzonymi z banku, jednak tego typu działalność przestępcza także przynosi zyski i – jakby nie patrzeć – jest to kradzież. 28-letni haker został skazany na osiem miesięcy pozbawienia wolności.

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>.