**Najbardziej spektakularne aresztowania cyberprzestępców w VI 2013**

**Eksperci z Kaspersky Lab przyjrzeli się, jak organy ścigania na całym świecie radzą sobie z walką z cyberprzestępcami. W czerwcu 2013 r. pojawiło się kilka sukcesów na tym polu - od drobnych aresztowań osób, które zhakowały konta na Facebooku, po incydent z praniem 6 miliardów dolarów. Główną "gwiazdą" czerwcowego zestawienia jest jednak aresztowanie przez policję gangu, który zajmował się nie tylko cyberprzestępczością, ale i handlem narkotykami.**

Tak jak w Hollywood

Akcja, która z powodzeniem nadawałaby się na scenariusz hollywoodzkiej superprodukcji, miała miejsce na terenie Holandii oraz Belgii. Policja aresztowała siedmiu duńskich przemytników i dwóch zatrudnionych przez nich belgijskich hakerów. Holenderska szajka narkotykowa postanowiła przejąć zmierzający do Rotterdamu transport niemal dwóch ton kokainy i heroiny. Zadaniem hakerów było włamanie się do systemu firmy przewozowej i dokonanie zmiany adresu dostawy wspomnianego ładunku na Antwerpię w Belgii. Hakerzy wykonali swoją robotę, jednak ich działalność została zauważona przez dział bezpieczeństwa, który natychmiast poinformował policję. Gdy przemytnicy narkotyków zjawili się, by odebrać ładunek, zostali przywitani przez stróżów prawa.

**Jak ukraść milion**

Amerykańsko-ukraiński gang cyberprzestępczy skradł 15 milionów dolarów od piętnastu firm z sektora finansowego. Wśród ofiar znalazły się między innymi takie organizacje jak Citibank, JP Morgan Chase oraz PayPal. Przestępcy włamali się do serwerów banków, skąd zdobyli informacje o ich klientach i przelali pieniądze z legalnych kont na przedpłacone karty debetowe. Skradzione pieniądze zostały wypłacone z bankomatów w Stanach Zjednoczonych oraz poprzez dokonanie serii fałszywych zakupów. Zarzuty postawiono ośmiu członkom gangu, jednak dwóch liderów ciągle pozostaje na wolności – prawdopodobnie ukrywają się oni na Ukrainie.

**Edukacja w domu warta 63 tysiące dolarów**

W Moskwie ujęto wyrzuconego ze szkoły średniej młodego człowieka, który nie dysponował żadnym wykształceniem technicznym. 19-latek kształcił się sam w domu, korzystając z doświadczenia cyberprzestępców udzielających się na podziemnych forach online. Zdobyta wiedza umożliwiła mu stworzenie i rozesłanie szkodliwego programu, z użyciem którego młody przestępca skradł wiele danych logowania do systemów płatności online. Informacje te posłużyły mu do przywłaszczenia sobie niemal 63 tysięcy dolarów. 19-latek z pewnością nie spodziewał się, że za swoje działania otrzyma wyrok pięciu lat pozbawienia wolności.

**Wolność słowa i areszt domowy**

W czerwcu aresztowano kanadyjskiego hakera, który przeprowadził cyberatak na stronę rządową Quebecu. Okazało się, że do ataku włamywacz posłużył się informacjami z wewnątrz rządowej infrastruktury IT, a pomogło mu w tym to, że jest on byłym pracownikiem lokalnej Izby Gmin. Sędzia orzekł, że atak nie miał na celu okazania protestu politycznego, ani też nie został przeprowadzony w celu uzyskania korzyści majątkowych. Wszystko wskazuje na to, że cyberprzestępca chciał po prostu pokazać światu swoje poglądy. Cel został osiągnięty, jednak za cenę ośmiu miesięcy aresztu domowego.

**Cybernękanie nie popłaca**

34-letni haker z Morgan City zhakował facebookowe konto pewnej kobiety, po czym zmienił hasło i zaczął publikować groźby oraz uwłaczające komentarze na jej profilu. Policja zareagowała błyskawicznie - podejrzany znalazł się w areszcie po upłynięciu zaledwie dwóch dni od zgłoszenia sprawy przez ofiarę cybernękania do obsługi portalu społecznościowego.

**Międzynarodowy handel kartami kredytowymi**

Przy udziale stróżów prawa ze Stanów Zjednoczonych, Wielkiej Brytanii oraz Wietnamu udało się zamknąć jedno z najstarszych forów specjalizujących się w handlu skradzionymi kartami kredytowymi. FBI poinformowało, że za pośrednictwem forum sprzedano dane dotyczące ponad miliona kart kredytowych, a związany z nimi cyberprzestępczy zysk przekroczył 220 milionów dolarów. Klientów forum ujęto w Wielkiej Brytanii, a założyciel „biznesu” - Van Tien Tu - został aresztowany w Wietnamie.

**Pralnia dzisiaj nieczynna**

Władze Stanów Zjednoczonych przejęły domeny powiązane z systemem płatności Liberty Reserve, którego właściciele zostali oskarżeni o pranie brudnych pieniędzy i nielegalny obrót gotówką. Serwis Liberty Reserve stał się ulubionym narzędziem cyberprzestępców, ponieważ oferował całkowitą anonimowość. Operatorzy systemu w żaden sposób nie weryfikowali klientów i udostępniali narzędzia dodatkowe, takie jak możliwość ukrywania danych nadawcy oraz wypłacania pieniędzy przy użyciu usług zewnętrznych. Oskarżyciele zarzucają firmie, że pomogła wyprać ponad 6 miliardów dolarów.

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