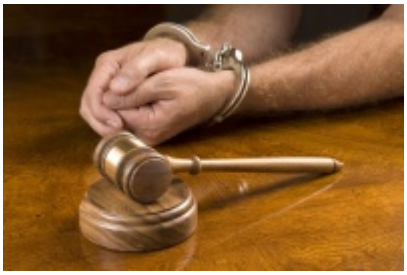
Cyberprzestępcy nie są bezkarni



Eksperci z Kaspersky Lab przygotowali zestawienie najciekawszych przypadków skutecznego ukrócenia działalności międzynarodowych cyberprzestępców przez organy ścigania w lutym 2014 r.

3 lata za atak DDoS

Na samym początku lutego Christopher Sudlik został skazany na 36 miesięcy więzienia w zawieszeniu, 60 godzin prac społecznych oraz otrzymał karę pieniężną w wysokości 111 000 dolarów w ramach rekompensaty za popełnione przestępstwa.
22-latek już wcześniej przyznał się, że był członkiem internetowej grupy hakerskiej Anonymous, która dopuściła się m.in. ataku typu DDoS na stronę firmy Angel Soft w lutym i marcu 2011 roku. Angel Soft jest filią przedsiębiorstwa Koch Industries, które było celem ataku. Christopher wraz z grupą hakerów użyli oprogramowania LOIC (Low Orbit Ion Cannon), którego zadaniem było wytworzenie masowego ruchu w celu bezpośredniego ataku na wybraną stronę internetową. Na przestrzeni trzech dni w wyniku nieustannych ataków na różne serwery sieciowe Koch Industries stracił sto tysięcy dolarów.

Kolejny "anonimowy" poległ

Po skazaniu tych dwóch osób za ataki DDoS agenci z FBI kontynuowali swoją działalność i ścigali każdego, kto brał na cel Koch Industries. Dzień 12 lutego nie był szczęśliwy dla trzeciego aktywisty grupy Anonymous, Jacoba Allena Wilkensa z Postville, w stanie Iowa, który został skazany na 24 miesiące w zawieszeniu i musiał zapłacić 111 dolarów zadośćuczynienia. Młody cyberprzestępca również wykorzystywał oprogramowanie Low Orbit Ion Cannon przeznaczone do zalewania serwerów ruchem, co miało zakłócić działanie strony. Niestety, LOIC przechowywał adresy IP atakujących, dzięki czemu agenci federalni odnaleźli Wilkensa.

Skazany za zarabianie na atakach DDoS

Wyrok można otrzymać za sam udział w ataku DDoS, a tym bardziej za zarabianie na nim pieniędzy. Pewien rosyjski 26-latek przyznał się do zorganizowania ataku na kilka dużych firm finansowych. Za każdy dzień przestoju firmy młody cyberprzestępca otrzymywał niecałe 100 dolarów.
Młody mężczyzna został złapany na gorącym uczynku przez policję, która wyciągnęła z niego wszystkie informacje, łącznie ze szczegółami jego aktywności na forach cyberprzestępczych i dowodami, że to on organizował ataki. Ostatecznie został skazany na dwa lata w zawieszeniu.

2,5 roku za oszustwo z użyciem papierów wartościowych

W lutym skazano jeszcze jednego Rosjanina - tym razem nie w zawieszeniu. Zamieszkały w Nowym Jorku Petr Murmiliuk wziął udział w kradzieży z kont do handlu online należących do takich domów maklerskich jak Scottrade, E*Trade, Fidelity, Schwab i innych. Członkowie spisku najpierw uzyskali nieautoryzowany dostęp do internetowych kont klientów domów maklerskich, następnie wykorzystali skradzione dane do otworzenia dodatkowych kont w innych domach maklerskich. Później użyli kont ofiar do przeprowadzenia transakcji papierami wartościowymi, które były korzystne tylko dla członków spisku. Akcja ta spowodowała łączne straty ofiar na około 1 milion dolarów.

Do pudła za lepsze oceny

Roy Sun, były amerykański student, został skazany na 18 miesięcy w zawieszeniu i 200 godzin prac społecznych za... zmianę swoich ocen po włamaniu do uczelnianego systemu komputerowego.
Wszystko wydarzyło się między 2008 a 2010 rokiem w Purdue University, w stanie Indiana. Roy z dwoma przyjaciółmi włamali się do pokoju profesora, zainstalowali na komputerach keyloggery, po czym zebrali informacje dotyczące logowania. Dane uwierzytelniające zostały później użyte do zmiany stopni na szóstki. Roy ukończył Purdue University w 2010 r., a incydent wyszedł na światło dzienne w 2013 roku, gdy jeden z profesorów zwrócił się do działu IT z informacją, że jego hasło zostało zmienione. W drodze śledztwa wyszły na jaw poprawki ocen.
Jeden z przyjaciół oszusta, Sujay Sharma, który także zdecydował się na zmianę swoich ocen, również został skazany i otrzymał karę 18 miesięcy w zawieszeniu i 200 godzin prac społecznych.

Źródło: Kaspersky Lab

Zdjęcie: Joe Belanger / Photogenica