**Kronika cyberkryminalna – maj 2014 r.**

**W maju wokół hakerów i cyberprzestępców pojawiło się wiele ciekawych informacji, a powstrzymanie haktywistów, zlikwidowanie sieci dystrybucji nielegalnych leków i aresztowanie stu przestępców na raz to tylko niektóre z nich. Eksperci z Kaspersky Lab przygotowali zestawienie majowych sukcesów organów ścigania w walce z ogólnoświatową cyberprzestępczością.**

**Lider LulzSec skazany na siedem miesięcy**

Informator grupy LulzSec o pseudonimie Sabu nie zdołał po raz kolejny uniknąć więzienia i został skazany za udział w przeprowadzeniu kilku ataków na znane cele. Kolejny haktywista z LulzSec, Hector Monsegur, wyszedł z sądu w Nowym Jorku jako wolny człowiek dzięki współpracy z FBI w identyfikowaniu i śledzeniu wielu innych członków grupy oraz pomocy w udaremnieniu kolejnych ataków. Monsegur był ważnym członkiem grupy LulzSec, a władze oskarżyły go o branie udziału w wielu jej działaniach, łącznie z atakiem na PayPal i inne firmy. Gdy w 2011 r. został aresztowany przez FBI, Monsegur zaczął współpracować i dostarczał agencji informacje na temat działań innych haktywistów. Prokuratorzy zwrócili się do sędziego o łagodny wyrok, w związku z czym Monsegur wyszedł na wolność, jednak przez rok pozostanie pod nadzorem sądowym.

**Stu hakerów na raz**

W maju jedną z największych akcji była sprawa 97 hakerów, którzy zostali oskarżeni o używanie trojana zdalnego dostępu Blackshades. Szkodliwe oprogramowanie można było kupić na forach cyberprzestępczych za 40 dolarów i dawało ono przestępcom możliwość zdalnego przekształcania komputerów ofiar w urządzenia do inwigilacji. Według FBI to narzędzie zdalnej administracji zostało rozesłane do tysięcy maszyn w ponad 100 firmach i jest odpowiedzialne za ponad 500 000 infekcji. Blackshades posiadał także zdolność samodzielnego rozprzestrzeniania się na inne komputery i posługiwał się w tym celu oszukańczymi szkodliwymi odnośnikami do kontaktów w sieciach społecznościowych i innych platformach komunikacji. W całej akcji udział wzięły organy ścigania z 19 krajów oraz ponad 300 badaczy. Nie wiadomo, jakie grzywny i wyroki odsiadki dostaną przestępcy, ale twórcy Blackshades (prawdopodobnie Szwed Alex Yucel, lat 24, i Amerykanin Michael Hogue, lat 23) mogą spędzić nawet 20 lat za kratkami.

**20 lat za sprzedawanie fałszywych kart**

David Ray Camez, lat 22, znany także jako „Bad Man” i „doctorsex”, został skazany przez amerykański Sąd Okręgowy w połowie maja. Camez został zatrzymany pod koniec 2013 r. – usłyszał zarzut udziału w organizacji zajmującej się przestępczością zorganizowaną oraz korupcją, a także spiskowania w ramach innej organizacji tego samego rodzaju. Młody mężczyzna dołączył do Carder.su sześć lat temu, gdzie przez dwa lata kupował i sprzedawał fałszywe dowody tożsamości oraz karty kredytowe. W akcie oskarżenia ogłoszonym w styczniu 2012 r. Camez był jednym z 39 skazanych. Siedmiu innych przyznało się do winy, rozprawa dwóch odbędzie się w czerwcu, a reszta to uciekinierzy. Szesnastu innych oskarżonych również zostało skazanych w trzech oddzielnych aktach oskarżenia, a 14 przyznało się do winy. Poza karą więzienia w wysokości 20 lat Camez został również skazany na trzy lata wolności pod nadzorem, jak również ma zapłacić 20 milionów dolarów odszkodowania.

**Współzałożyciel The Pirate Bay aresztowany**

Ostatniego dnia maja Peter Sunde, jeden z założycieli i były rzecznik torrentowego serwisu The Pirate Bay, został aresztowany w Szwecji przez INTERPOL. Prokuratorzy poszukiwali Sunde’a przez ponad dwa lata, a jego wyrok został ostatecznie ogłoszony w 2012 r. przez Sąd Najwyższy Szwecji, który w sprawie przeciwko założycielom The Pirate Bay postanowił do odwołania nie wypuszczać tego długo ukrywającego się przestępcy. Wtedy Sunde zwrócił się ze swoim przypadkiem do Europejskiego Trybunału Praw Człowieka i do Szwedzkiego Sądu Najwyższego, jednak nigdzie nie uzyskał poparcia. Teraz dostanie wyrok w wysokości około 8 miesięcy pozbawienia wolności. Kolejnych dwóch aktywistów opuściło więzienie, a jeden kolega przestępcy wciąż próbuje uniknąć sprawiedliwości, ukrywając się gdzieś w Azji.

**Największa w historii operacja związana z fałszywymi lekami**

Około 200 organów ścigania z ponad stu państw wzięło udział w Operacji Pangea 7, która miała na celu sieć przestępców sprzedających fałszywe leki w nielegalnych aptekach internetowych. Operacja zakończyła się ponad 230 aresztowaniami na całym świecie i konfiskatą potencjalnie niebezpiecznych leków o wartości blisko 36 milionów dolarów. W trakcie tych działań wszczęto 1 235 śledztw, usunięto blisko 20 000 reklam nielegalnych leków z platform społecznościowych, zamknięto ponad 10 000 stron WWW, a także skonfiskowano 9,4 miliona fałszywych i nielegalnych leków. Ta międzynarodowa operacja było koordynowana przez INTERPOL, a z pomocą przyszło wiele organizacji, łącznie ze Światową Organizacją Celną, centrum odpowiedzialnym za bezpieczeństwo aptek internetowych (CSIP) i firmami takimi jak Microsoft, PayPal, MasterCard czy Visa.

**Spamer tekstowy dostaje ogromną grzywnę**

Phil Flora, znany także jako Phil P., został oskarżony o spamowanie przy użyciu wiadomości tekstowych, za co musi zapłacić ponad 148 000 dolarów. Człowiek ten wysłał do użytkowników ponad 29 milionów wiadomości tekstowych, obiecując „darmowe” karty podarunkowe. Oszustwo było dość proste: po kliknięciu przez ofiarę odnośnika pojawiał się formularz, który należało wypełnić w celu uzyskania rzekomej darmowej karty podarunkowej do sieci Walmart, o wartości 1 000 dolarów. Jeśli użytkownik wprowadził wymagane informacje, musiał jeszcze kliknąć kilka odnośników. Podane przez użytkowników dane zostały wykorzystane do wysyłania niechcianych wiadomości. Oszustwo stało się problemem dla niektórych sprzedawców. W deklaracji procesu sądowego, wypełnionej dla Federalnej Komisji Handlu, dyrektor działu prywatności w Walmart Stores powiedział, że sklep otrzymał przynajmniej 14 000 reklamacji. Czas i wysiłek włożony w wyśledzenie źródła spamu oraz kwestie łagodzenia niezadowolonych klientów kosztowały firmę ponad 100 000 dolarów.

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>.

Więcej bieżących informacji o atakach cyberprzestępczych i metodach ochrony znajduje się na oficjalnym blogu Kaspersky Lab: Kaspersky Daily – <http://plblog.kaspersky.com>.