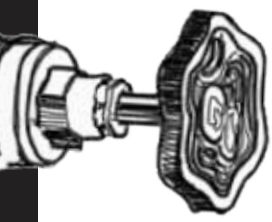
6/2014

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 6/2014

ZeuS w kawie

Cyberprzestępcy nie ustają w próbach wymyślania nowych ataków typu social engineering. Tym razem rozsyłają informację do potencjalnych klientów sieci kawiarni Starbucks z „darmowym" prezentem. Tytuł maila: „Starbucks Coffee Company gift from your friend". Czytając dowiadujemy się, że nasz znajomy dopiero co kupił kawę w Starbucksie i wskazał nas jako beneficjenta darmowego prezentu. Do informacji załączony jest plik, który rzekomo zawiera menu do wyboru oraz miejsce i czas odbioru prezentu. Śpieszymy poinformować, że „prezent" odbiera się natychmiast po otwarciu załącznika. Jest nim jedna z odmian wirusa ZeuS. Dodatkowy bonus może się pojawić przy wejściu na konto bankowe. Wiadomo jaki bonus. [1]

Cyberprzestępcy zainteresowani operacjami plastycznymi?

Cyberprzestępcy najprawdopodobniej włamali się do kliniki wykonującej operacje plastyczne i wykradli z niej dane blisko pół miliona pacjentów. Przejęto imiona, nazwiska, e-maile, nr telefonów i daty urodzenia. Na szczęście (tak twierdzą poszkodowani) nienaruszone pozostały dane finansowe i kliniczne. Teraz informacje o korzystaniu z usług zmniejszania nosa, powiększania piersi, zaokrąglania ust i usuwania zmarszczek mogą stać się publiczne i nieprzyjemnie zaskoczyć właścicieli „przeróbek". Brytyjski „The Sun" twierdzi, że za włamaniem stoją przestępcy z Rosji. Ciekawe czy założą grupę hakerską „B0T0X"? [2]

Himalaje phishingu

Jak przystało na „najwyższe" państwo świata - Nepal odnotował najwyższy wskaźnik stron phishingowych na 10 000 zarejestrowanych domen. Na to wskazują statystyki podane przez znaną organizację APWG (Anty Phishing Working Group), do której zresztą nasza fundacja należy :). O miano

lidera w tej niechlubnej klasyfikacji Nepal stoczył zażartą walkę z inną „potęgą" - Palau. Fanów gór uspakajamy - wysokość n.p.m ma się nijak do zjawiska phishingu. Najwyższy szczyt Palau ma 242 m. Może ciekawszy w kontekście phishingu jest fakt, że na liście gatunków fauny Palau 1 400 pozycji to ryby. W opisie fauny Nepalu słowo „ryba" nie występuje.[3]

Szpiedzy na ścianie - Banksy?

Znany, choć owiany lekką tajemnicą, brytyjski artysta - Banksy, który specjalizuje się w ulicznym graffiti, tym razem wziął na warsztat brytyjskich szpiegów. W każdym bądź razie wszystko na to wskazuje, że to Banksy. Na ścianie jednego z budynków w miejscowości Cheltenham pojawiło się graffiti otaczające budkę telefoniczną. Graffiti przedstawia trzech brytyjskich szpiegów z urządzeniami do podsłuchu, którzy skoncentrowani są na podsłuchiwaniu osoby, która właśnie znajduje się budce telefonicznej. Jak widać afery dotyczące szpiegowania obywateli, powiązane chociażby z PRISM i rewelacjami Snowdena, stały się już zjawiskiem społecznym. Zaangażowany od lat w artystyczne akcje nawiązujące wydarzeń politycznych i społecznych - Banksy, systematycznie wymyka się mediom i pozostaje postacią na pół tajemniczą. Wielbicielom jego talentu, którym zależy na poznaniu jego personaliów, pozostaje nadzieja, że teraz ustalą je dokładnie ludzie z GCHQ (brytyjskiego centrum szpiegowania), w szczególności jeśli niektórzy z nich rozpoznają swoje twarze na rysunku.[4]

Putin uspokaja - nie szpiegujemy was. Odpowiadając użył „zawodowego języka".

Wszyscy odetchnęliśmy z ulgą po tym jak rosyjski przywódca - Władimir Władimirowicz Putin uspokoił nas, że Rosja nie stosuje systemów masowego podsłuchu obywateli z wykorzystaniem najnowszych zdobyczy techniki. W każdym bądź razie taka była odpowiedź na pytanie jakie zadał Putinowi Edward Snowden w czasie corocznej sesji zadawania pytań przywódcy przez obywateli - „Nie mamy takiego systemu i zgodnie z prawem nie może on istnieć". Oprócz ciekawego faktu, że Snowden wystąpił w charakterze obywatela Federacji Rosyjskiej, niewielu też zwróciło uwagę na wstęp jaki uczynił Putin przed zasadniczą odpowiedzą. A brzmiał on następująco: „Panie Snowden - pan jest byłym agentem, ja też

miałem związek z wywiadem, także możemy sobie porozmawiać używając zawodowego języka". Jeśli ktoś chciałby dowiedzieć się, co w zawodowym języku znaczyła odpowiedź Władimira Władimirowicza polecamy lekturę na temat

rosyjskiego systemu SORM (Система Оперативно-Розыскных Мероприятий), ostatnio uaktualnionego przy okazji olimpiady w Soczi.[5]

Jak szybko zmienić hasła do systemów na lotnisku?

Takie pytanie zadają sobie zapewne całe grupy zadaniowe specjalnie powołanych do takiego zadania specjalistów. Obradują czasami całymi tygodniami po czym zastanawiają się czy będzie trzeba przy tej okazji zamknąć lotnisko czy jakoś sobie poradzimy. A sytuacja jest znacznie prostsza. Hasła mogą być zmienione bardzo szybko i nie potrzeba do tego żadnych specjalnych przygotowań. Udowodnili to pracownicy z japońskiego lotniska w Hanedzie. Jeden z członków „zespołu projektowego" zgubił w hali odlotów... kartkę z poufnymi kodami dostępu do systemów. Reszta „zespołu projektowego" bardzo szybko zmieniła wszystkie te kody w systemach, tak aby pozostawały one bezpieczne. Trzeba jednak przyznać, że do tak sprawnego działania mieli oni specjalnych motywatorów z zewnątrz. Byli nimi minister transportu Japonii, który nakazał zmianę kodów, prezydent Obama, który miał lądować na lotnisku następnego dnia i 16 000 japońskich policjantów zmobilizowanych na tę okazję.[6]

[1] http://tinyurl.com/prwcwq2
[2] http://tinyurl.com/m5xoplr
[3] http://tinyurl.com/lsw78fj
[4] http://tinyurl.com/mehjg5v
[5] http://tinyurl.com/y9n5ckq
[6] http://tinyurl.com/kldtspq

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

www: http://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen