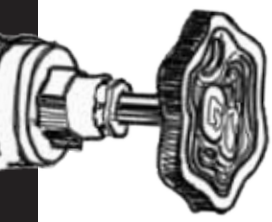
4/2014

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 4/2014

Piękny zachód słońca a w nim ...Wirus

Steganografia to metoda ukrywania jednej treści w drugiej. Widzimy obrazek z Pałacem Kultury, a w środku na przykład wiadomość: „Akcję zaczynamy o godzinie 20:00”. To metoda znana od tysięcy lat. Wszyscy wiemy czym jest atrament sympatyczny. W starożytności posłańcowi tajnej wiadomości zapisywano ją na łysej głowie, czekano by włosy odrosły i wówczas wysyłano w drogę. Dziś steganografią posługują się na przykład terroryści. Przesyłają sobie niewinne zdjęcia, a w środku znajdują się inne istotne zdjęcia, albo tajne treści. Niestety problem dosięgnął też użytkowników e-bankingu. Badacze odnaleźli co najmniej dwa zdjęcia - jedno zachodzącego słońca a drugie kota, które zawierały w sobie pliki konfiguracyjne bankowego wirusa. Nawet znalezienie takich „wirusów” nie wzbudza dużych obaw - „Ot, kotek i tyle.” [1]

ДДОС?

Powtórka z języka rosyjskiego niestety potrzebna

Wraz z napięciem za naszą wschodnią granicą warto przypomnieć sobie trochę rosyjskich słów, a raczej się ich nauczyć. Chodzi o słowa będące połączeniem rosyjskiego i komputerowego slangu. I tak: ИМХО to znane angielskie IMHO (In My Humble Opinion), „zaliv” (залив) to metoda kradzieży danych, „mylo” („мыло”) czyli mydło oznacza co ciekawe email - ze względu

na odobieństwo fonetyczne, „Offtopnu” (оффтопну) to oczywiście „off-topic” a „Traf” („Траф”) to nie polski „przypadek” tylko angielski „traffic”. Nie życzymy nikomu ДДоСа i innych przekrości. A o nie nie trudno bo ceny w podziemiu очень доступные. [2]

Włamanie do samochodu ...Wirusem?

„Panie władzo ktoś się włamał do mojego samochodu!” Już niedługo po takim zgłoszeniu możemy usłyszeć pytanie: „A czy był zapaczowany?”. Tak jak telefony stały się komputerami, tak powoli stają się nimi też samochody. Wyniki badań naukowych nad możliwościami „zaatakowania” samochodów są lekko przerażające. W ich trakcie przejęto kontrolę

nad układem kierowniczym i hamulcowym (sic!). Na razie wzięto „na warsztat” Forda Escape i Toyotę Prius. Przy okazji badania samochodowych programów okazało się, że używane są w nich „secret keys”. Brzmi dobrze, tyle, że „tajnymi kluczami” były łatwo odczytywalne wartości ASCII, np: JAMES, MAZDA, PANDA, COLIN i ... „Jesus”. Przed ostatnim wystarczy dodać „Oh” i mamy podsumowanie. [3]

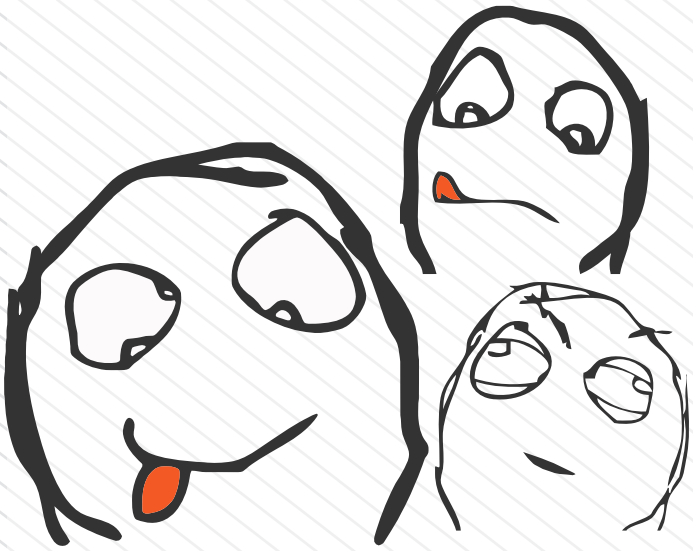
FC BARCELONA - - Syrian Electronic Army 0:1

FC Barcelona (FCB) „straciła gola” na własnym boisku. Syryjscy haktywiści z grupy SEA włamali się na konto twitterowe hiszpańskiego klubu i umieścili tam apel do zarządu klubu aby zrezygnował z katarskich funduszy, które „ociekają krwią”. Dość długo trwało zanim administratorzy konta usunęli wpis zamieszczony przez SEA. Ich działania zdecydowanie przyśpieszyły po tym jak na profilu FCB pojawił się drugi komunikat: „Special Hi to @RealMadrid!”. A tak w ogóle to trochę nas niepokoi bliskość skrótów FCB i FBC ;). [4]

O czym rozmyślają trolle?

Naukowcy zza oceanu, tym razem kanadyjscy, przeprowadzili szerokie badania tego jak zachowują się internauci komentujący różne sieciowe

wiadomości. Przebadano 1215 osób. Okazało się, że osoby zachowujące się tak jak sieciowe trolle (dla przypomnienia: generalnie uprzykrzający życie innym swoimi komentarzami) mają skłonności sadystyczne, makiawelistyczne, psychopatyczne i narcystyczne. Ciekawe co oznacza fakt, że Kanadyjczycy przekazali do wypełnienia swoją ankietę tylko sąsiadom z południa. Och, było to troszkę znęcaniem się na sąsiadami. Takiego ruchu nie powstydziłby się chyba sam Machiavelli. [5]



Włamanie
z zamkniętymi oczami

„Hakerzy" z grupy Anon Ghost dokonali dość precedensowego ataku. Otóż włamali się oni na stronę Yorkshare Banku. Problem polegał na tym, że dokonali udanego przejęcia strony z phishingiem na klientów YB przygotowanej przez innych „hakerów". „We are watching you: Don't close your eyes". Tym samym pojawiła się poważna konkurencja dla najbardziej „spektakularnego włamania". Zagrożony jest przypadek włamania islamiskich haktywistów na stronę „Belvoir Castle" miejsca wypoczynku brytyjskich rodzin, zamiast na stronę „Belvoir Fortress" - fortecy chrześcijańskich krzyżowców. Apel „don't close your eyes" nabiera dość specjalnego znaczenia w tym przypadku. [6]

[1] http://tinyurl.com/cybsecurity-zawor-4-1
[2] http://tinyurl.com/cybsecurity-zawor-4-2
[3] http://tinyurl.com/cybsecurity-zawor-4-3
[4] http://tinyurl.com/cybsecurity-zawor-4-4
[5] http://tinyurl.com/cybsecurity-zawor-4-05
[6] http://tinyurl.com/cybsecurity-zawor-4-06

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