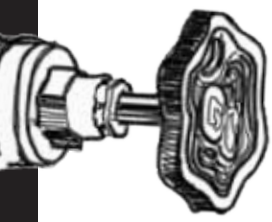
12/2015

FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 12/2015

„На ваш сайт ведется DDoS – атака”

Dziś w dobie wszechpanującego Internetu każde istotne działanie ma niemalże natychmiastowo swój odzew w sieciach społecznościowych. Weźmy na przykład użytkowników Twittera – praktycznie nic nie umknie uwadze jego użytkownikom. Oczywiście włączając w to temat bezpieczeństwa w Internecie. W związku z tym, że początek roku charakteryzuje różnego rodzaju podsumowanie tego, który właśnie minął, firma Kaspersky przedstawiła subiektywny Top 10 tweetów na temat bezpieczeństwa IT w 2014 r. Poniżej niektóre z nich.

I tak w dziesiątce znalazł się np „kulturalny“ komunikat od atakującego, który poinformował właściciela, za pośrednictwem publicznie dostępnego kanału, że jego firma będzie nękana atakami DDoS jeśli ten nie zapłaci okupu 1000 $.

„На ваш сайт ведется DDoS – атака”. *(Na Twojej stronie przeprowadzany jest atak DDoS).*

Także za pośrednictwem Twittera Premier Rosji Dmitrij Medvedev „poinformował“ cały świat, że rezygnuje z funkcji jaką pełni, wstydzi się działań rządu i jest mu bardzo przykro.

„Ухожу в отставку. Стыдно за действя правительства. Простите.“ *(Rezygnuję. Wstyd mi za działania rządzących. Przepraszam)*

Jak się okazało nie były to osobiste przemyślenia polityka nad wydarzeniami za naszą wschodnią granicą, o których niestety słyszymy każdego dnia. Oczywiście tweet ten był wynikiem włamania na konto Premiera Rosji i wszystkie wiadomości pisane przez atakujących zostały szybko usunięte. Co się stało z winowajcami i czy zostali złapani – do tej pory nie jest to wiadome.

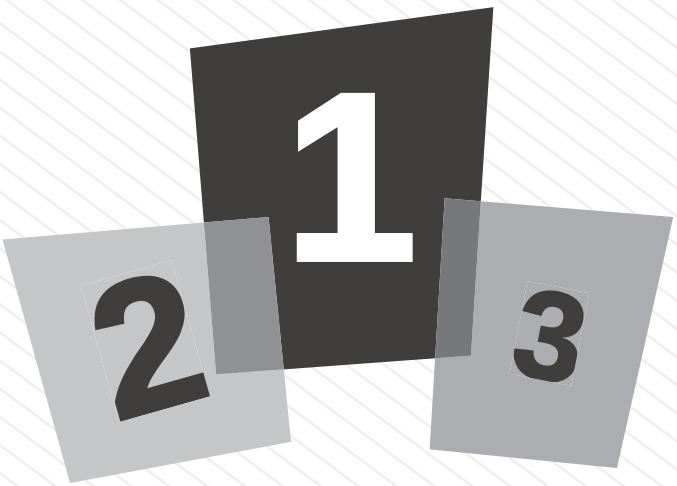
Dużą sympatię wzbudził wpis, który został stworzony przez ludzi z - uwaga! - CIA (*Centralnej Agencji Wywiadowczej – amerykańska agencja rządowa*). Twardziele z poczuciem humoru.

„We can neither confirm nor deny that this is our first tweet.“ (*Nie potwierdzamy i nie zaprzeczamy, że to nasz pierwszy tweet*).

Od razu dodajemy, że to był pierwszy tweet CIA, bo właśnie dopiero w zeszłym roku agencja utworzyła swój profil na Twitterze. Swoją drogą spójrzcie poniżej - trzeba przyznać, że to niezły wynik. Pierwszy tweet i od razu podany dalej 300 tysięcy razy i 190 tysięcy dodało tweeta do „ulubionych”. [1]

Czyje logo najpiękniejsze?

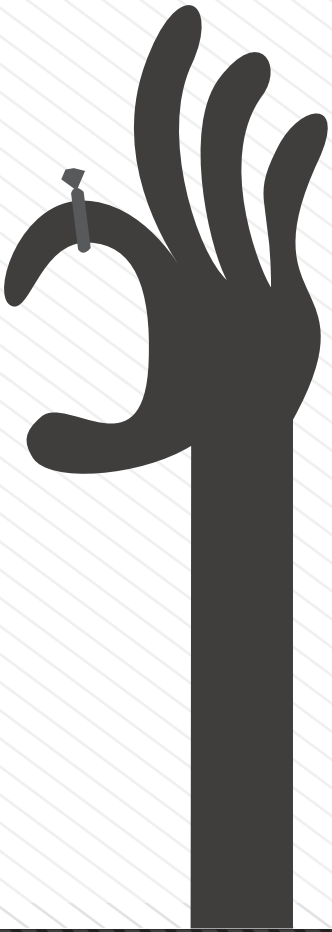
Wbrew pozorom odpowiedzi na pytanie zadane w tytule nie znajdziemy na stronach designerskiego magazynu czy też konferencji poświęconej projektowaniu graficznemu. Pytanie takie postawili internautom autorzy pewnego bloga z dziedziny bezpieczeństwa IT i dotyczyło ono... logotypów grup hakerskich. Na co dzień specjaliści od spraw



bezpieczeństwa w Internecie zajmują się różnymi działaniami tych grup, ale w dzisiejszych czasach ważny jest wizerunek i również takie poczucie mieli twórcy grup, bo jak się okazuje wszystkie posiadają identyfikację wizualną „firmy".
Na podium znaleźli się kolejno zaczynając od zwycięzcy: Anonymous, LulzSec, UGNazi. [2]

Drużyna pierścienia

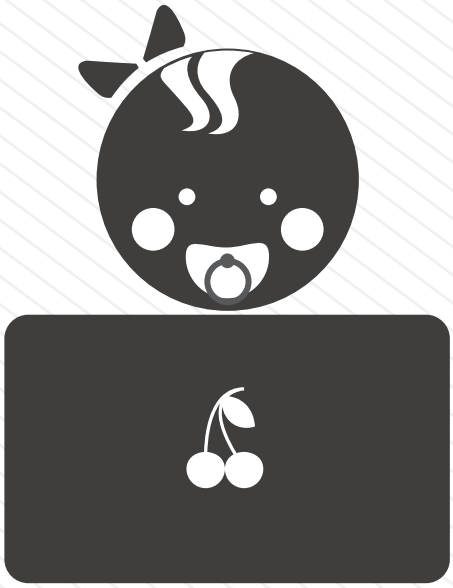
Coraz częściej możemy usłyszeć o urządzeniach typu „wearable" (takich, które można nosić na sobie). Nieubłagana technika goni nas i dopada z każdej strony. Przykładem takiego urządzenia może być inteligentny pierścień, którym można zdalnie sterować smartfonem za pośrednictwem połączenia Bluetooth. Urządzenie jest tak zaprojektowane, że aby szczęśliwy posiadacz mógł skorzystać z jego funkcji musi wygiąć palec w odpowiedni sposób. I tak, np. do uzyskania dostępu do kamery wbudowanej w smartfonie, właściciel musi wygiąć palce tak, aby przybrał kształt litery „C", jeśli „narysuje" w powietrzu kształt trójkąta urządzenie odtworzy muzykę. Na razie zasięg działania takiej biżuterii to 5 metrów.



Nam spodobały się skarpety dla prowadzących aktywny tryb życia. Skarpety zaopatrzone są w czujniki badające np. jaki styl biegania preferuje właściciel. Dane ze skarpetkowych czujników wysyłane są do smartfona, który informuje posiadacza skarpet o błędach w ćwiczeniach, co powinien zmienić, aby trening był bardziej efektywny i powiedzmy mniej kontuzyjny. Pewnie by się przydał również moduł, dzięki któremu skarpeta informuje właściciela, że czas ją zmienić.
Oczywiście jeśli mówimy o ubiorach nie może zabraknąć czegoś dla pań – Enter Belty – mowa o inteligentnym pasku. Jak przystało na tego typu sprawy i modę zaprojektowany przez francuską firmę pasek skonstruowany w ten sposób, że dopasowuje się automatycznie do kształtu ciała. Zmienia swoją długość zależnie od tego, co robimy w danym momencie, gdy siadamy pasek zwiększa swoją długość, tak aby nas nie uwierał i odpowiednio wraca do formy gdy wstaniemy z powrotem. Pasek może również monitorować zdrowie swojego właściciela. Mierzy np. obwód talii (badając czy tyjemy lub chudniemy), ponadto pasek może poinformować właściciela, że np. znajduje się on w grupie osób podwyższonego ryzyka, np. takich, które mogą zachorować na cukrzycę.
Czytając o urządzeniach „wearable" można mieć wrażenie, że to historie rodem z lektur a ich twórcą jest słynny Q, twórca gadżetów dla agenta Jamesa Bonda. [3]

O tym, jak siedmiolatka zhackowała sieć Wi-Fi

Korzystanie z publicznych sieci Wi-Fi nie jest rozważne! Piszemy i informujemy o tym, bardzo często na stronach Fundacji Bezpieczna Cyberprzestrzeń. Jeśli jednak jest jeszcze ktoś kto nie jest do końca o tym przekonany to może historia 7-letniej Betsy Davies będzie bardziej przekonywująca od nas. Betsy włamała się do publicznej sieci Wi-Fi a na dodatek w mniej niż 11 min.
Dziewczynka uczestniczyła w eksperymencie przeprowadzonym w ramach nowej kampanii na rzecz bezpieczeństwa publicznego, przeprowadzanego przez jednego z dostawców sieci VPN. Kampania miała na celu uświadomić ludziom jak proste jest włamanie do darmowych publicznych hotspotów sieci Wi-Fi i co za tym idzie, jak niebezpieczne skutki niesie to dla nieostrożnych użytkowników.
Sam eksperyment polegał na tym, że zbudowano dla Betsy odpowiednie środowisko pracy, w tym specjalnie wykonaną otwartą sieć Wi-Fi, podobną do dowolnej publicznej sieci tego typu. Betsy miała do pracy przygotowany komputer, wyszukiwarkę Google i instrukcję hackingu (których jak wiadomo nie brakuje w Internecie).
Wyniki eksperymentu zadziwiły samych inicjatorów. Dziewczynka dokonała samodzielnie ataku „man in the middle" (MiTM), który umożliwił jej podsłuchanie komunikatów ofiary (uczestnika eksperymentu) to jedno ale zadziwiający jest fakt, że zajęło jej to zaledwie 10 minut i 54 sekundy. Miejmy nadzieję, że eksperyment nie stanie się fragmentem programu szkolnego dla sześciolatków. [4]



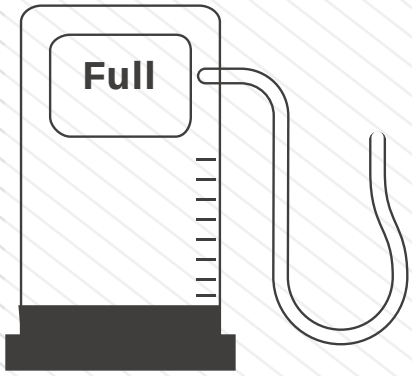
W spadku po dziadku

Jeśli któregoś dnia dostaniesz wiadomość, że od dziś jesteś szczęśliwym posiadaczem spadku, to niech Cię nie zdziwi gdy owym spadkiem okaże się ni mniej ni więcej tylko profil na Facebooku.
Portal wprowadził funkcję wirtualnego spadkobiercy. W ustawieniach, włączając opcję „Legacy Contact" użytkownik będzie mógł wskazać osobę, której chciałby po śmierci oddać zarządzanie profilem. Opcja ta dostępna jest z poziomu ustawień konta użytkownika. Dotychczas było tak, że o odejściu osoby administratorów mogła powiadomić rodzina i wówczas Facebook „zamrażał" zgłoszone konto. W tej chwili „spadkobierca" otrzymuje: dostęp do konta osoby, która „zapisała" mu swój profil, możliwość pisania postów oraz zmiany zdjęcia profilowego, będzie mógł odpowiadać na zaproszenia znajomych, a także pobierać zawartość zdjęć i postów. „Spadkobiercy" nie będzie natomiast wolno: usunąć zdjęć i konta, nie będzie miał dostępu do wiadomości prywatnych, a także nie będzie mógł wyznaczyć kolejnego „spadkobiercy", czyli tylko raz możemy wybrać osobę, która przejmie profil – kolejne zmiany

nie będą możliwe. Funkcja dostępna jest już w Stanach Zjednoczonych, w ciągu kilku tygodni będzie dostępna dla wszystkich użytkowników. Więc jeśli ktoś uważa swój profil za niezwykle cenną rzecz i chciałby nim kogoś obdarzyć już za kilka tygodni będzie miał taką możliwość. Tym bardziej proszę uważać na „fejsbukowe" wirusy, aby nie przekazywać ich w razie czego w spadku.[5]

Kontrolka paliwa

Amerykański inżynier Jack Chadowitz zidentyfikował słabość w urządzeniach służących do monitorowania poziomu paliwa, automatycznego miernika zbiornika (ATG), na stacjach benzynowych. Około 115 tysięcy stacji benzynowych w Stanach Zjednoczonych korzysta z takich urządzeń - jak wykazało badanie podatnych na atak było około 5 tysięcy. Podatność mierników wykorzystywanych do monitorowania zbiorników paliwa jest kolejnym przykładem problemów zabezpieczeń dotyczących urządzeń kontroli procesów przemysłowych, które coraz częściej są podłączone do Internetu. Bardzo podobna sytuacja jest z urządzeniami typu IoT (*Internet of Things*) czyli Internetem Rzeczy.



Słabość zidentyfikowana przez Chadowitza teoretycznie może mieć wpływ na zmianę kalibracji i co za tym idzie fałszywe raporty na temat stanu paliwa w zbiornikach np. wpisane dane nie wykażą tego, że zbiorniki są puste i należałoby zamówić dostawę – albo dokładnie odwrotnie. Podatność ta pozwala również napastnikowi na zmianę danych w taki sposób, że miernik zgłasza wyciek, co automatycznie powoduje wyłączanie pomp i przestój w pracy stacji benzynowej. Właściciel takiej stacji nie byłby szczęśliwy z takiego obrotu sprawy ale konkurencja ..., a i kierowcy samochodów nie obrazili by się gdyby się okazało, że przy okazji ktoś „obniżył" cenę paliwa.[6]

[1] http://tinyurl.com/qakyzqh
[2] http://tinyurl.com/narcpwl
[3] http://tinyurl.com/qzrwt2g
[4] http://tinyurl.com/pa6mulk
[5] http://tinyurl.com/pvkzx8g
[6] http://tinyurl.com/nsq45xg

Kolejne nr można śledzić również na serwisie społecznościowym LinkedIn

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