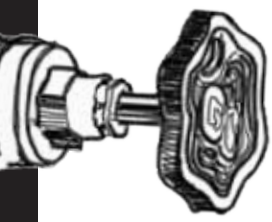
15/2015

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 15/2015

Hiszpanie zhackowali przepisy hologramami

Hiszpanie pokazali, że rząd tak łatwo ich nie uciszy. Wprowadzone ostatnio restrykcyjne „Ley Mordaza” czyli „prawo knebla” zakłada surowe kary m.in. za publiczne protesty i zgromadzenia, fotografowanie i filmowanie policji oraz okupowanie banków w czasie protestów. Aby obejść te obostrzenia hiszpańscy aktywiści sięgnęli po bardzo nietypową, acz wymowną w swojej symbolice formę protestu: zorganizowali marsz hologramów. Do marszu „Hologramas para la Libertad” czyli „Hologramy dla wolności” mógł włączyć się każdy umieszczając na stronie akcji swoje nagranie lub protest. Wszystkie materiały były w czasie strajku wyświetlane jako hologram. Ostatecznie pod budynkiem parlamentu przeszło kilkanaście tysięcy hologramowych postaci, które domagały się zmiany przepisów.
To pierwszy tego typu strajk na świecie. Policja nie podjęła konfrontacji z protestującymi wirtualnymi postaciami. Czyżby obawiała się, że nałożone grzywny zostaną opłacane w postaci bnknotów-hologramów? [1]

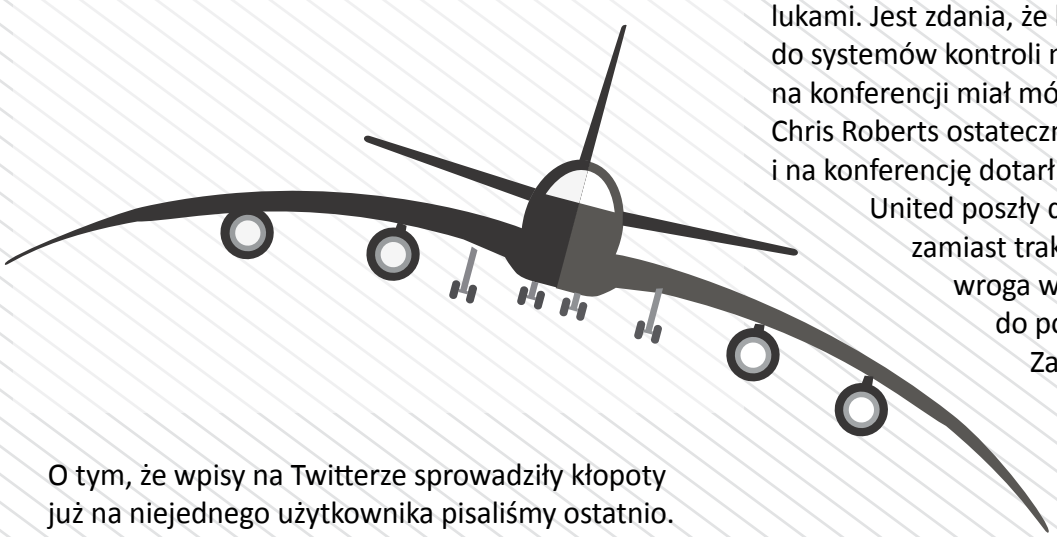
Kulka w komputer

Komputery potrafią wyprowadzić człowieka z równowagi. Dla niektórych urządzeń źle się to niestety kończy. Za swoją niesubordynację wysoką cenę zapłacił sprzęt pewnego Amerykanina: właściciel nie mogąc dogadać się z maszyną... sięgnął po broń.
38-letni Lucas Hinch z Kolorado miał dość ciągłych Microsoft Windows Blue Screen of Death czyli „niebieskich ekranów śmierci”. Na Craigslist kupił pistolet i z zimną krwią wystrzelił w komputer 8 pocisków kalibru 9mm.

Wezwanej do zdarzenia policji dumny z egzekucji Hinch tłumaczył, że miał dość „wielomiesięcznej walki z komputerem”. Wcześniej był wielokrotnie notowany za używanie broni w terenie zabudowanym. Za swój ostatni występek ma wkrótce stanąć przed sądem. Co ciekawe, Hinch prowadzi sklep z produktami homeopatycznymi. Szkoda, że wcześniej nie znalazł tam niczego dla siebie na ukojenie skołatanych nerwów. Chociaż przeciwnicy homeopatii zapewne powiedzą, że to co zrobił to dowód na to, że jednak znalazł. [2]

FUNDACJA bezpieczna cyberprzestrzeń

Linie lotnicze nie mają poczucia humoru



O tym, że wpisy na Twitterze sprowadziły kłopoty już na niejednego użytkownika pisaliśmy ostatnio. Tym razem ofiarą swoich żartów padł Chris Roberts, specjalista ds. bezpieczeństwa i założyciel One World Labs z Denver. Robertsa niespodzianka spotkała gdy wybierał się na dużą konferencję branżową do San Francisco.

Wcześniej podczas lotu z Denver do Syracuse, podłączony do pokładowego wifi, zastanawiał się na Twitterze czy byłby w stanie „pobawić się" EICAS (systemem dostarczającym załodze informacji o parametrach lotu) i uruchomić maski tlenowe. Żart najwyraźniej nie przypadł do gustu FBI, którego przedstawiciele czekali na Robertsa po wylądowaniu i przesłuchiwali go kilka godzin, konfiskując przy okazji cały sprzęt: iPada, MacBooka Pro, dyski twarde i pamięci USB.

Po tym incydencie na zimne postanowiły dmuchać United Airlines, które kilka dni później odmówiły Robertsowi wpuszczenia na pokład. Rzecznik United decyzję linii tłumaczył jego wcześniejszymi wpisami na Twitterze: „komentarze, jakich dopuścił się Roberts, są pogwałceniem polityki linii". Wspomniał też o złym wpływie na nastroje pozostałych pasażerów i członków załogi.

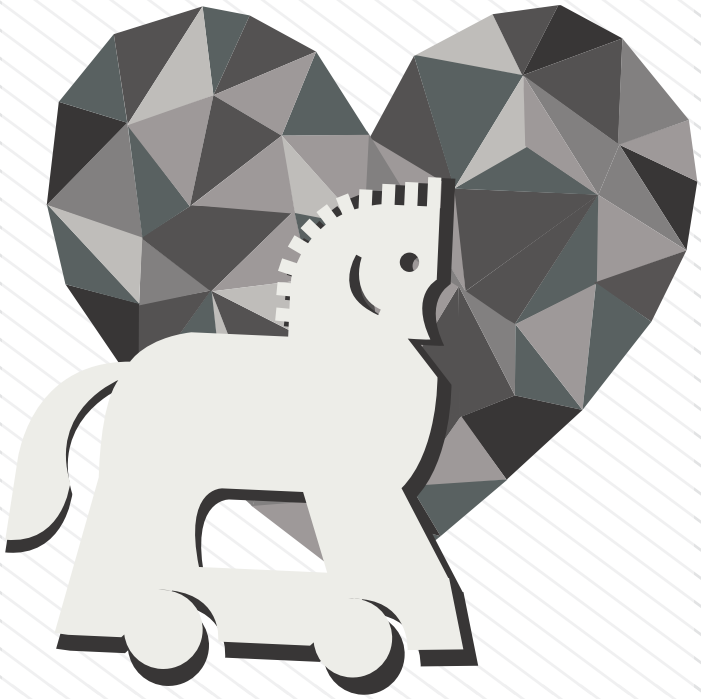
Linia lotnicza twierdzi, ze pechowego pasażera powiadomiono o decyzji parę godzin wcześniej. Organizacja Electronic Frontier Foundation określiła postępowanie United Airlines jako rozczarowujące i dezorientujące. Roberts znany jest z tego, że już od dłuższego czasu próbuje zainteresować linie lotnicze problemem bezpieczeństwa pokładowych systemów komputerowych i występującymi w nich lukami. Jest zdania, że każdy haker może włamać się do systemów kontroli nad samolotem. Jak na ironię na konferencji miał mówić właśnie na ten temat. Chris Roberts ostatecznie dostał się na inny lot i na konferencję dotarł. Wydaje się jednak, że linie United poszły dość niefortunną drogą: może zamiast traktować go jako pokładowego wroga warto było posłuchać co ma do powiedzenia w temacie? Zaś opuszczenie masek z tlenem w kabinie pasażerskiej nie zepsułoby raczej „atmosfery". [3]

Wszczep sobie czipa

PayPal stracił wiarę w ludzką pamięć do haseł i zabrał się za szukanie bardziej niezawodnych metod weryfikacji użytkowników. Dodatkowo - jak twierdzą przedstawiciele firmy - hasła i tak łatwo złamać, bo mało kto korzysta z różnych do każdego serwisu, większość użytkowników polega na jednym ub dwóch łatwych do zapamiętania.

Jonathan LeBlanc z firmy PayPal objechał ostatnio Stany Zjednoczone i Europę ze swoją prezentacją „Kill all passwords", w której argumentuje, że „przyszła identyfikacja nie będzie już polegać na hasłach", ale czymś bezpieczniejszym i łatwiejszym w użyciu. O co chodzi? Wcale nie o nowoczesne techniki bazujące na skanowaniu linii papilarnych czy rozpoznawaniu głosu. PayPal chce iść

o krok dalej i snuje wizje na temat technologii zintegrowanej z ludzkim ciałem.
Jednym z pomysłów są mikroczipy wszczepiane w ludzką skórę lub do mózgu. Mogłyby one być połączone z miniaturowym urządzeniem EKG, które rejestrowałoby aktywność serca i bezprzewodowo przesyłało dane do urządzeń. W ten sposób odblokowywany byłby dostęp do serwisów czy usług.
Te futurystyczne wizje pewnie nie ziszczą się jutro, ale PayPal chce być liderem badań



w dziedzinie weryfikacji i identyfikacji użytkowników. Oby się nie skończyło, że z taką weryfikacją tożsamości nie nie można się na przykład zapisać na wizytę do kardiologa, bo ten odmówi jej twierdząc, że hasło wskazuje na to, że pacjent jest zdrowy. A o konsekwencjach zawirusowania wszczepionego czipa nawet lepiej nie spekulować. Koń trojański na rozrusznik to wizja zbyt przerażająca. [4]

Szczęście źle zaprogramowane, czyli loteria z rootkitem w tle

Niektórzy rodzą się szczęściarzami, inni uznają, że szczęściu trzeba trochę pomóc. Amerykanin Eddie Raymond Tipton, szef działu bezpieczeństwa MUSL – – Międzystanowego Stowarzyszenia Loteryjnego, z oczywistych względów nie mógł brać udziału w loteriach. Perspektywa wygrania 14 mln dolarów była jednak na tyle kusząca, że opracował inny pomysł na wygraną. Potrzebował tylko kogoś do odbioru nagrody. Początkowo wszystko szło zgodnie z planem. Po prawie roku, krótko przed upłynięciem czasu, kiedy pieniądze powinny zostać odebrane, tajemnicza firma zarejestrowana w Belize zgłosiła się po nie za pośrednictwem adwokata z Nowego Jorku.
To gwarantowałoby posiadaczowi szczęśliwego losu anonimowość. Pech w tym, że prawo stanu Iowa wymagało danych zwycięzcy, stąd wydania nagrody odmówiono.
Sprawa szybko wzbudziła zainteresowanie odpowiednich władz. Tiptona zdemaskowano, gdyż na nagraniu z kamer współpracownicy zidentyfikowali go jako osobę kupującą los. Wkrótce też okazało się, że to on, pod pretekstem zmiany czasu na komputerze, dostał się do zamkniętego pokoju, w którym znajdował się sprzęt generujący zwycięskie numery i wgrał oprogramowanie, pozwalające mu na kontrolę wygrywających liczb. Dodatkowo najprawdopodobniej zmienił ustawienia kamery w pomieszczeniu, gdyż akurat w ten dzień rejestrowała ona tylko jedną klatkę na minutę zamiast standardowo ciągły obraz. W ten sposób na nagraniu nie widać jak wprowadza USB ze złośliwym oprogramowaniem.
Współpracownicy określili Tiptona jako mającego „obsesję" na punkcie samokasujących się rootkitów zdolnych do dokonywania zmian w komputerach. Wprawdzie po złośliwym oprogramowaniu nie

pozostało ani śladu, ale jak często bywa w takich historiach zawiódł czynnik ludzki. No cóż – los chciał, że się nie udało. Proces Tiptona rusza w lipcu. Wydaje się, że jego jedyna szansa to próba„zaprogramowania" ławy przysięgłych i cela posiadająca zamek z portem USB. [5]

Nauczycielu, miej się na baczności!

Tymczasem na Florydzie czternastolatek został oskarżony o cyberatak. Uczeń ze szkoły Paul Smith Middle School w Holiday przy użyciu hasła administratora zalogował się do komputera nauczyciela, którego nie lubił i zmienił tło pulpitu na zdjęcie dwóch całujących się mężczyzn. Właściciela laptopa nie było wtedy w szkole, ale nauczyciel na zastępstwie odkrył sprawę i zgłosił ją władzom szkoły. Chłopaka-żartownisia zawieszono na 3 tygodnie. To jednak nie koniec tej historii. Wkrótce potem kwalifikację występku zmieniono i chłopaka oskarżono o cyberatak, który jest przestępstwem. Jak wyjaśnia szeryf Chris Nocco uczeń korzystając z hasła administratora zalogował się do kilku sieci, w tym do komputera z testami egzaminacyjnymi i mógł zapoznać się z pytaniami.
Jak na ironię, chłopak tłumaczy, że po prostu skorzystał z hasła, które podczas lekcji... pokazał sam nauczyciel, na oczach wszystkich logując się... swoim nazwiskiem. Dodatkowo broni się, że nie był jedynym, któremu zdarzyło się użyć tego jakże wymyślnego hasła.
Nastolatek został już zwolniony z aresztu i oddany pod opiekę matki. Wydaje się, że komuś przy tej sprawie zabrakło zdrowego rozsądku. A nauczycielowi elementarnej wiedzy na temat obsługi komputera.
My czekamy na informację, czy udało się przywrócić tło pulpitu i jak ono teraz wygląda. [6]

[1] http://tinyurl.com/puqc8re
[2] http://tinyurl.com/q5h289b
[3] http://tinyurl.com/oy2ggns
[4] http://tinyurl.com/mcefgq5
[5] http://tinyurl.com/nwh8wty
[6] http://tinyurl.com/q2hnm9b

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

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo