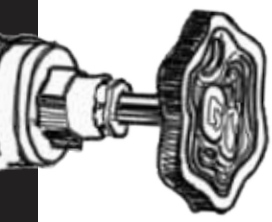
6/2016

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 6/2016

10-latek zgarnął od FB 10 tysięcy dolarów

Za młody, by zgodnie z regulaminem mieć na Facebooku konto, ale właśnie odebrał 10 tysięcy dolarów za odkrycie luki w Instagramie – aplikacji do zdjęć, którą Facebook kupił w 2012 roku. Dziesięcioletni Jani z Finlandii jest najmłodszym zdobywcą bonusa w programie „bug bounty", w ramach którego Facebook przyznaje nagrody za znalezienie i zgłoszenie błędu. Luka, którą chłopak odkrył, pozwalała na kasowanie dowolnych komentarzy innych użytkowników na Instagramie. Lokalnej gazecie zdradził, że eksperymentował nawet przy kontach gwiazd, w tym Justina Biebera. Swój raport udowodnił poprzez skasowanie komentarza, który firma zamieściła na koncie testowym. Wcześniej aplikacja nie sprawdzała dokładnie czy osoba usuwająca komentarz była tą samą, która go napisała. Dotychczas Facebook rozdał około 4.3 miliona dolarów ponad 800 zgłaszającym z całego świata. Najwięcej pochodziło z Indii, poprzedni najmłodszy odkrywca luki miał 13 lat. Jani zdradził mediom, że sztuczek hakowania uczył się z filmików na YouTube. Chłopakowi gratulujemy, ale dla Facebooka to chyba marny powód do dumy, skoro nawet 10-latek jest w stanie odkryć u niego „niedoróbki". [1]

Bezpieczeństwo dronów pod lupą

Sprzedaż dronów bije ostatnio rekordy. Przewiduje się, że w samych Stanach Zjednoczonych w 2016 roku sprzeda się około 2,5 miliona dronów hobbistycznych i komercyjnych.
Badacze z amerykańskiego Uniwersytetu Johna Hopkinsa postanowili sprawdzić jak łatwo hakerzy mogą zmusić te bezzałogowe pojazdy do zignorowania swoich ludzkich kontrolerów. Podczas przeprowadzonych eksperymentów odkryli i opisali trzy luki w popularnych dronach hobbistycznych. Znaleźli trzy różne sposoby na wysłanie z laptopa fałszywych poleceń i w ten sposób udało im się zmusić drony do m.in. „niekontrolowanego lądowania" i lądowania awaryjnego.
Producent drona nie odpowiedział na ich raport, więc eksperci zabrali się za droższe modele.
Choć drony tanieją, to te wykorzystywane do zabawy, fotografowania, wideofilmowania oraz zaawansowanych misji komercyjnych to wciąż drogie gadżety. Jak się okazuje największą ceną może być w ich przypadku bezpieczeństwo. Nikt nie chciałby, aby jego przesyłka z Amazonu wylądowała w czyimś ogrodzie i bezpowrotnie trafiła w niepowołane ręce. [2]

FUNDACJA bezpieczna cyberprzestrzeń

Nie kupisz kota w worku

„Action Fraud", czyli centrum zgłoszeń oszustw w Wielkiej Brytanii, ostrzega przed kupowaniem zwierząt domowych za pośrednictwem internetu. Okazało się, że na popularnych portalach aukcyjnych wystawianych jest coraz więcej fałszywych ogłoszeń o ich sprzedaży, zwłaszcza kociąt i szczeniaków. Oszuści wykorzystują kradzione zdjęcia. Gdy zgłosi się zainteresowany kupnem zwierzaka, twierdzą, że przebywają obecnie za granicą. Gdy mimo wszystko uda im się uzgodnić sprzedaż, do płatności dochodzi zwykle przelewem albo poprzez tzw. money transfer. Zwierzak jednak się nie pojawia. Czasami oszuści proszą jeszcze o dalsze pieniądze na pokrycie przesyłki, kuriera lub też weterynarza.
Zakochany w pupilu ze zdjęcia przyszły właściciel zwierzaka nigdy nie ujrzy, gdyż ten po prostu nie istnieje! Niby oczywiste, ale niektórzy nadal się nabierają. „Action Fraud" ostrzega, żeby przy tego typu aukcjach postarać się osobiście zobaczyć zwierzaka, nie wpłacać wcześniej żadnych pieniędzy, zwłaszcza gdy sprzedawca nagle zmienia metodę płatności. A najlepiej na poszukiwania pupila udać się do hodowcy, ośrodka adopcyjnego albo schroniska. Bo w przypadku takich aukcji nawet na kota w worku nie ma co liczyć. [3]

Czekoladowe hasło

Co ma wspólnego czekolada z bezpieczeństwem internetowych haseł? Badacze z Uniwersytetu w Luksemburgu udowodnili, że poczęstowani np. czekoladą, są bardziej skłonni do wyjawienia swoich haseł osobom trzecim.
Często najłatwiej wydobyć wrażliwe dane po prostu ładnie o nie prosząc. Autorzy badania podkreślają, że oszuści polegając na różnych metodach inżynierii społecznej wykorzystują poczucie obowiązku i potrzebę oddania przysługi, które pojawiają się u wielu osób po otrzymaniu małego prezentu. A dzielenie się hasłami okazało się wcale nie należeć do wyjątków. Badania przeprowadzone na 1208 osobach wykazały, że już niewielki podarek, jak np. czekolada, znacznie ułatwiała oszustom zdobycie hasła.
Gdy była oferowana przed rozmową, aż 43,5% osób decydowało się ujawnić swoje hasło prowadzającemu wywiad, zaproponowana po rozmowie dawała wynik na poziomie 29,8%.
Nie wiadomo jednak ile z przekazanych haseł było prawdziwych. Ciekawe czy przekąski słone również dają podobny efekt? [4]

Selfie z celi

Internet podbiło ostatnio zdjęcie z celi, które zrobiła sobie grupa więźniów z amerykańskiego stanu Wirginia Zachodnia. Pamiątkowym selfie pochwalili się na Facebooku, więc fotka bardzo szybko obiegła świat, docierając też do władz więzienia. Te zachodzą w głowę w jaki sposób skazani weszli w posiadanie telefonu komórkowego.
Na zdjęciu widać uśmiechniętych więźniów, a pod fotką widnieje komentarz: „Jest ciężko przez cały dzień". Inicjatorem selfie był Shane Holbrook. Ciążą na nim m.in. zarzuty zastrzelenia mężczyzny podczas napadu z bronią. Zapytany w jaki sposób zrobił zdjęcie, odpowiada: „Myślę, że mogło chodzić o telefon komórkowy. Tyle mogę powiedzieć". Odmawia też odpowiedzi na pytanie w jaki sposób wszedł w posiadanie urządzenia. „Powiedzmy, że je znalazłem". „Pioruny czasami trafiają w drzewa, komety czasami spadają na

ziemię, a facet w więzieniu czasami zdobywa telefon''. „W tamtym czasie nie myślałem o konsekwencjach" tłumaczy Holbrook. Przyznaje, iż wiedział, że to co robi jest wbrew zasadom więziennym, ale chciał dać swojej rodzinie znać, że ma się dobrze. No i dał. Teraz grozi mu zaostrzenie wyroku, więc przekazać, że trochę się pogorszyło, może już nie mieć jak. [5]

Robot „zwinna łapka"

Wśród wielu testowanych ostatnio sposobów weryfikacji użytkowników jest metoda analizy gestów. W skrócie chodzi o obserwację ruchów użytkownika na urządzeniu z ekranem dotykowym i stworzenie dla niego indywidualnego profilu, będącego podstawą przyszłej weryfikacji na tymże urządzeniu. Czy to bezpieczne? Czy hakerowi nie wystarczy po prostu uważne poobserwowanie i potem naśladowanie gestów danej osoby? Otóż nie chodzi jedynie o gesty, ten system weryfikacji pod uwagę bierze również profil ręki użytkownika, jego nadgarstka, etc. Jeden z ostatnich raportów przyjmując perspektywę bardziej wyrafinowanego hakera opisuje dwa ataki z udziałem robotów LEGO. Roboty z wyprofilowanymi palcami przeszkolono wcześniej w obsłudze urządzeń dotykowych. Pierwszy atak opierał się na statystykach dotyczących gestów zbieranych przez dłuższy czas od grupy 41 osób. Drugi bazował na danych skradzionych bezpośrednio od użytkownika, które zostały przez robota wykorzystane do odtworzenia odcisków palców. Oba ataki okazały się skuteczne. A skoro tak, jeśli korzystasz drogi Czytelniku z urządzeń dotykowych, kolejnym razem lepiej nie podawaj na powitanie ręki robotowi. [6]

[1] http://tinyurl.com/gw6hxpt
[2] http://tinyurl.com/glxemj7
[3] http://tinyurl.com/j4y723p
[4] http://tinyurl.com/jb8f9e7
[5] http://tinyurl.com/zgtsrq3
[6] http://tinyurl.com/hhnw77s

Kolejne numery biuletynu można śledzić na serwisie społecznościowym LinkedIn

Zapraszamy do uczestnictwa w Konferencji!

14-15 września 2016 roku w Warszawie i 4 warsztatach 13-16 września 2016 (prowadzenie: CIRCL.LU, SHODAN.IO, ComCERT i SEKURAK.PL). Podczas koferencji czołowe firmy z branży IT SECURITY będą prezentowały swoje usługi i produkty na stoiskach w przestrzeni wystawowej. Ta część oraz niektóre prelekcje, w tym keynote - Mikko Hypponena będą udostępnione dla wszystkich zainteresowanych bezpłatnie po wcześniejszej rejestracji na stronie: https://www.securitycasestudy.pl/rejestracja/

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

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo