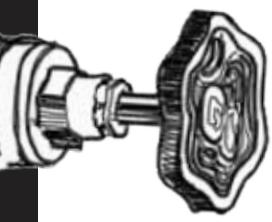
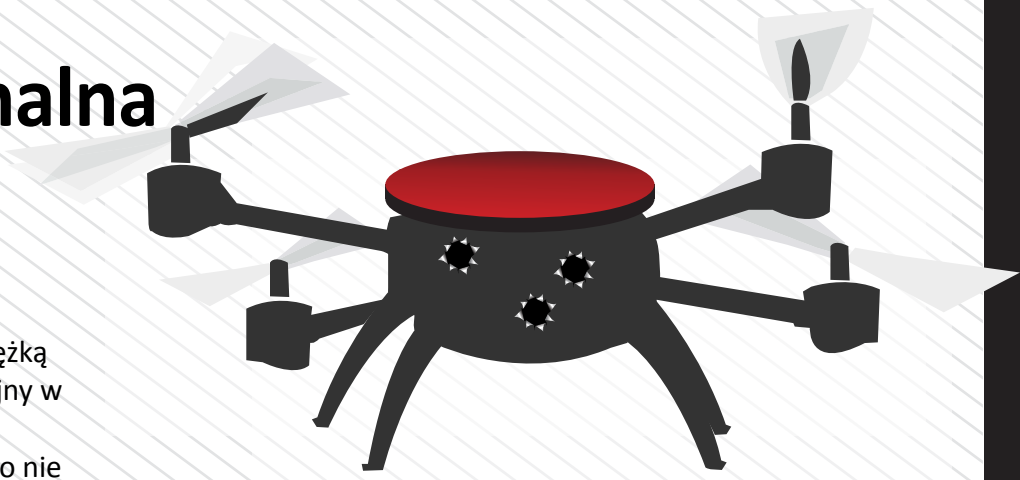
19/2015

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 19/2015

Nieproporcjonalna reakcja?

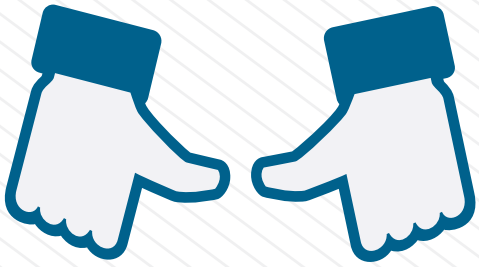


Cierpliwość pewnego Amerykanina z Kentucky została wystawiona na ciężką próbę, gdy - jak twierdzi - po raz kolejny w ciągu ostatnich miesięcy nad jego podwórkiem zaczął krążyć dron. Długo nie zastanawiając się, chwycił za broń i trzema strzałami zaatakował maszynę.
William Merideth zapewnia, że nigdy nie wystrzeliłby do drona, gdyby ten „tylko przelatywał". Jednak dron z przyczepioną kamerką krążył nad jego terytorium i najwyraźniej coś filmował, zakłócając spokój i prywatność jego rodziny. Po paru minutach od zdarzenia na miejscu pojawił się samochód z czterema mężczyznami „szukającymi zaczepki", z których jeden był właścicielem drona. Merideth zagroził, że „zaraz będzie następna strzelanina". Mężczyźni widząc, że jest uzbrojony wycofali się i wezwali policję. Okazało się, że maszyna warta była 1800 dolarów.
Strzelca aresztowano na parę godzin. Choć podobno policja przyznała mu rację, postawiono mu zarzuty m.in. narażenia zdrowia i życia, za co grozi od 1 do 5 lat więzienia. „Ludzie, którzy posiadają drony i ludzie, którzy nienawidzą broni są jedynymi, którzy się nie zgadzają z tym, co zrobiłem". „Jako Amerykanie mamy prawo do obrony naszych prac i własności".
Co dalej w tej sprawie? „Mam prawnika i wyznaczoną datę na przesłuchanie w sądzie". Merideth jest przekonany o tym, że zarzuty zostaną oddalone.
Co chciałby powiedzieć właścicielowi drona? „Chciałbym po prostu, aby podszkolił się odnośnie zabawki i nauczył szanować prawa innych ludzi".
Nie wiemy czy dron został „zabity" czy tylko ranny. My w każdym razie mamy radę, aby przed atakiem na drona zawsze upewnić się, że nikt z rodziny nie zamawiał niczego na Amazonie. [1]

Jak rasowy Fejsbookowicz

Znany z internetowych eksperymentów Joe Veix - w ramach kolejnego ćwiczenia - założył niedawno na Facebooku ogólnodostępne konto pod nazwą PublikFacebook™. Do korzystania z niego wysłał publiczne zaproszenie na Twitterze, podając nazwę użytkownika oraz hasło. Hasło, które w zasadzie marnie mogło spełniać rolę prawdziwego hasła: password1234.
Veix nie chciał, aby ktokolwiek czuł się wykluczony. Był ciekawy co się zdarzy: „Jeśli profil w mediach

społecznościowych ma odzwierciedlać naszą osobowość, jak będzie wyglądać konto, z którego może korzystać każdy?" - pytał. Rezultat okazał się odbiciem kolektywnej osobowości mediów społecznościowych, z całą głupotą, przechwalaniem się i brakiem rozwagi.
Pierwsza rzecz, do której doszło była do przewidzenia: ktoś w Berkeley w Kalifornii zmienił hasło, blokując konto. Potem zdarzyło się to jeszcze kilkakrotnie. Wkrótce ktoś zmienił nazwę konta z John Smith na Maximilien Manning. Jak w kalejdoskopie zmieniały się zdjęcia profilowe i te w tle. Na profilu Maxa ktoś wpisał jako miejsce pracy serwis obsługi klienta w restauracji Taco Bell. Cztery dni od rozpoczęcia eksperymentu konto miało 135 logowań od 100 różnych użytkowników, z „tak egzotycznych lokalizacji jak Paryż, Szwecja, Kolumbia, Zjednoczone Emiraty Arabskie i New Jersey".
Jedni „lajkowali" wszystko „jak leci", inni masowo wysyłali zaproszenia do wszystkich swoich znajomych. Przez weekend „Max" zdążył być w Ouagadougou, Nowym Meksyku, Brooklynie, Bali, Boca Raton i Nebrasce. Ktoś przyznał 5 gwiazdek kontu ISIS, więc skądkolwiek się logował jest teraz pewnie na czarnych listach rządowych. Max polubił 322 rzeczy, w tym 50 krematoriów dla zwierząt, liczne strony o charakterze komunistycznym, na temat planowania ślubów oraz z memami.
Podobny eksperyment Veix przeprowadził na Instagramie i Twitterze. Konto na Instagramie szybko musiał zlikwidować - po 74 postach ktoś zaczął nękać nastolatkę. Twitter z kolei sam zamknął konto ze względu na podejrzaną działalność, zanim autor zdążył skopiować tweety. Autor eksperymentu zastanawia się dlaczego konto na Facebooku nie zostało zamknięte za spam? Agresywna aktywność Maxa była jak wirus, a algorytmy Facebooka przez długi czas jej nie wychwyciły.



Joe Veix przypuszcza, że prawdopodobnie „użytkownik" zachowywał się jak „prawdziwy" Fejsbookowicz, stąd nie budził podejrzeń. Można powiedzieć „ręce opadają" [2]

Pomocne selfie

Konkurencja wśród kandydatów do nagrody na najgłupsze selfie robi się coraz większa. W środowisku przestępczym moda na „słitfocie" trzyma się wyjątkowo mocno. A im głupszy złodziej, tym policja ma łatwiejsze zadanie.
Tym razem policja z Los Angeles zwróciła się z prośbą o pomoc w zidentyfikowaniu mężczyzny podejrzewanego o włamanie do domu w dzielnicy Venice. W dniu 11 lipca br. około godziny 7 rano podejrzany wszedł do rezydencji na Paloma Avenue korzystając z otwartych bocznych drzwi. W środku znalazł iPhone'a właścicieli, w którym przypadkowo aktywował aplikację wideo. Bardzo wyraźnie nagrała ona jak czarnoskóry mężczyzna w czarnej czapce stoi w pokoju właścicieli domu. Następnie ukradł on smartfona i uciekł.
Co ciekawe, wszystko działo się gdy trzy mieszkanki: dorosła kobieta i dwie 15-latki spały w sypialniach obok. Włamywacz nawet się nie zorientował. A może wstąpił do rezydencji, zwabiony selfie z wakacyjnego wyjazdu którejś z nich? [3]

Czarownica zaklina komputery

Czy zdarza się, że twój komputer lub smartfon odmawia współpracy? Zawiesza się lub wyłącza bez powodu? Problem może być poważniejszy niż ci się wydaje - to może być nawiedzenie przez

złe duchy, a w takich przypadkach trzeba sięgnąć po metody niestandardowe. Firmy z Krzemowej Doliny współpracują z czarownicą, która chroni komputery przed wirusami i biura przed złymi duchami. Reverend Joey Talley praktykuje Wicca, neopogańską religię stworzoną w latach 40. XX wieku w Anglii, i twierdzi, że ma nadprzyrodzony dar do techniki. Legitymuje się trzema tytułami magistra i ma ponad 40 lat doświadczenia. Choć problemy z komputerami nie są jedynymi, którymi mistyczka zajmuje się, od dawna jest wzywana na ratunek, gdy technologia zawodzi. Przybywa wtedy ze swoją energią i zaklina złe duchy. W zależności od problemu stosuje różne metody czarowania. „Większość osób chce chronić swoje komputery przed wirusami i atakami hakerskimi" - powiedziała Talley gazecie SF Weekly. „Więc zaklinam je. Lubię używać roślin". Gdy chodzi o problemy ze sprzętem biurowym, Talley posługuje się czarnym kamieniem, który służy do blokowania energii. W skrajnych wypadkach rzuca „czary ochronne" na całą firmę. Wśród jej klientów wymieniani są Facebook, Salesforce i Apple. Czarownica przywołuje historię start-up'u, w którego biurze wył przez cały dzień alarm i nikt nie mógł sobie z nim poradzić, nawet elektrycy. Wezwana do akcji Talley szybko „wykurzyła złego ducha".
Na swojej stronie ogłasza, że zajmuje się sprawami niezwykłymi i niebezpiecznymi. Jest otwarta na każde wyzwanie, nawet starcie z niesprawną drukarką. Zanim jednak sięgniesz po telefon, miej świadomość, że usługi Talley nie są tanie. Bierze 200 dolarów za godzinę, konsultacja telefoniczna jest bezpłatna. Czy takie eksperymenty opłacają się, zwłaszcza, że często godzinne czary nie wystarczą? Może taniej po prostu kupić nową drukarkę? [4]

Los, który zmienił los

O tej sprawie już informowaliśmy. Amerykanin Eddie Raymond Tipton, szef działu bezpieczeństwa Międzystanowego Stowarzyszenia Loteryjnego (MUSL), chciał oszukać system instalując na komputerze samokasującego się rootkita, który pozwoliłby mu wytypować odpowiednie numery i wygrać na własnej loterii 14,3mln dolarów. Dodatkowo zmienił ustawienia kamery w pomieszczeniu, przez co na nagraniu nie widać jak wprowadza USB ze złośliwym oprogramowaniem. Niestety ostatecznie wpadł, a teraz oficjalnie uznano go winnym oszustwa.
Od czasu tej historii MUSL wprowadził dużo zmian, aby poprawić bezpieczeństwo w firmie. Jej CEO Terry Rich uznając, że ostatecznie cała sprawa wyszła grom loteryjnym na dobre, napisał w oświadczeniu, że MUSL „chce być o krok przed tymi, których kusiłoby do oszustw".
Choć na komputerze nie pozostało ani śladu, a nagrania z kamery też nie mogą być twardym dowodem, to jednak wszystkie ślady prowadzą do Tiptona i po sześciu godzinach obrad ława przysięgłych uznała go za winnego.
Wyrok zapadł 9 września. Oszust został skazany na 10 lat więzienia w zawieszeniu. Taki los zagwarantował mu „wygrany los"... [5]

Selfie oka zamiast tokenów?

W temacie narzędzi weryfikacji co tydzień coś nowego. Było już o odblokowywaniu telefonu uchem, czas na oko. Firma Solus, zajmująca się biometrycznymi

systemami bezpieczeństwa, opracowała 2-stopniową technologię weryfikacji Eyeprints, polegającą na identyfikacji użytkownika przy pomocy oka. Podczas gdy inne metody weryfikacji wymagają często tokenów i kluczy, które łatwo zgubić, technologia Eyeprint opisywana jest jako niskokosztowa i „bez hardware'u".
Jednak tak naprawdę bazuje ona na „sprzęcie", który już masz, czyli smartfonie i oczach. Potrzebujesz tylko wiedzieć jak zrobić selfie i zapamiętać numer PIN.
Eyeprint działa przez zrobienie zdjęcia naczyń krwionośnych oka użytkownika. Technologia jest w stanie rozpoznać do 400 unikalnych punktów w oku. Firma Solus twierdzi, że „naczynia lub żyłki nie zmieniają się z wiekiem i mogą być skutecznym loginem, wykorzystywanym we wszystkich warunkach oświetlenia oraz nawet przez okulary i szkła kontaktowe." Technologia Eyeprint ma działać zarówno na urządzeniach z Androidem, jak i z systemem iOS - o ile są one wyposażone w kamerę HD.
Co w przypadku zwyrodnienia plamki żółtej, której towarzyszą nieregularne dodatkowe krwinki w obrębie siatkówki? Eyeprint polega na zdjęciu białka oka, nie skanuje siatkówki, ani tęczówki.
Tym technologia Eyeprint różni się od skanu - twierdzi CEO Solus Matthew Ainscow.
Andy Kemshall, współzałożyciel i dyrektor techniczny firmy SecurEnvoy ostrzega, że taka forma technologii biometrycznej „nie jest dojrzała, ani sprawdzona" i może być narażona na błędy.
Ciekawe czy tę technologię da się oszukać podstawiając do telefonu najwyższej jakości zdjęcie oka? [6]

Relacja z konferencji SECURITY CASE STUDY

[1] http://tinyurl.com/qbjakbx
[2] http://tinyurl.com/p4tced8
[3] http://tinyurl.com/q77roew
[4] http://tinyurl.com/pob9gln
[5] http://tinyurl.com/olarmcl
[6] http://tinyurl.com/qx2jny2

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

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo