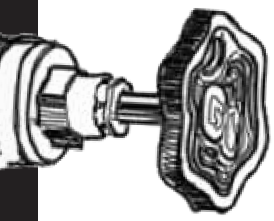
FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 18/2015

Dni otwarte w Land Roverze

Land Rover poszukuje ponad 65 tysięcy właścicieli samochodów, w których wystąpił błąd w oprogramowaniu sterującym zamykaniem drzwi. Może on powodować samoczynne odblokowanie i otwarcie drzwi, nawet w trakcie jazdy, a kierowcy nie otrzymają wcześniej żadnego sygnału. Firma zapewnia, że dotychczas nie doszło do żadnego groźnego incydentu.

Chodzi o samochody Range Rover i Range Rover Sport sprzedawane od 2013 roku. Właściciele wszystkich modeli z tego okresu zostali wezwani do serwisów, gdzie wadliwy sterownik zostanie naprawiony i przeprogramowany.

Coraz częściej branża samochodowa pada ofiarą błędów w oprogramowaniu. W parze z latami doświadczeń w projektowaniu silników, karoserii i dizajnerskich wnętrz nie idzie niestety doświadczenie w kwestiach software'owych.

W zeszłym roku dochodziło do wielu kradzieży luksusowych aut Range Rovers i BMW X5s, które złodzieje otwierali przy pomocy tajemniczej „czarnej skrzynki”. W związku z tym niektóre firmy ubezpieczeniowe niechętnie sprzedawały ubezpieczenia na te modele lub np. wymagały od właścicieli parkowania wyłącznie na strzeżonych parkingach.

Póki co przestępcy zacierają ręce. Dni otwartych drzwi w Land Roverze cały czas trwają. [1]

Co jeszcze spadnie z nieba?

Nowy Jork uhonorował niedawno paradą zwycięstwa piłkarki, które wygrały FIFA Women's World Cup, zdobywając tytuł mistrzyń świata. Z tej szczególnej okazji władze miasta udzieliły zgody na wykorzystanie konfetti. Na ulice, na których świętowały tłumy, spadł deszcz pociętych pasków i wstążek. I nie byłoby w tym niczego dziwnego, gdyby nie to, że znalazły się wśród

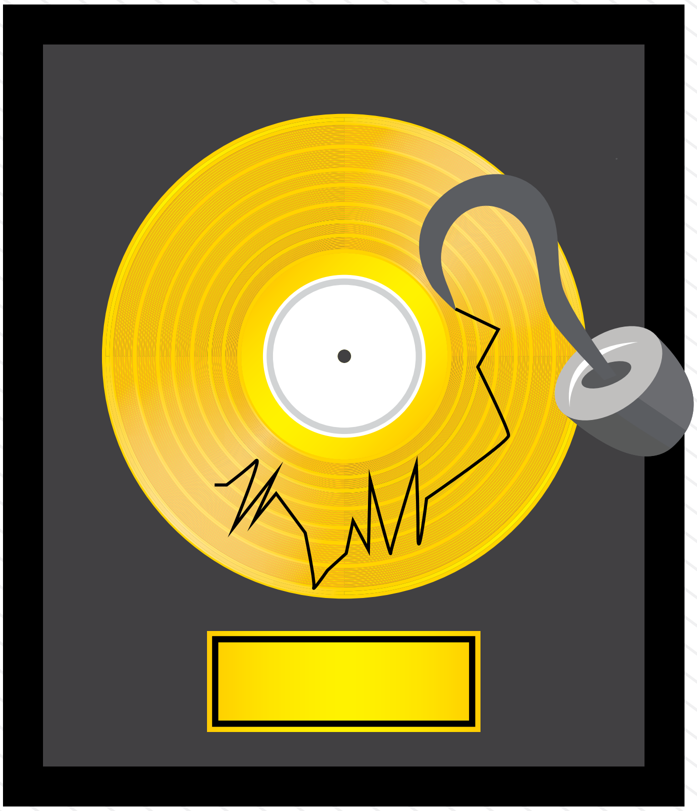
nich zmielone w niszczarce kawałki recepty lekarskiej. Pocięte tak grubo, że z kawałków można było ułożyć całą receptę, jak donieśli dziennikarze na Twitterze. Podobna akcja miała już miejsce w 2012 roku. Podczas parady New York Giants Super Bowl z budynku biurowego spadło konfetti z numerami social security. W tym samym roku na paradzie z okazji Thanksgiving Day unosiły się pocięte policyjne dokumenty.
Jak to możliwe, że w konfetti fruwają prywatne informacje? Specjalnie wyprodukowane konfetti na imprezę w Nowym Jorku dostarczyła firma Atlas Packaging Company - dwie tony czystych pociętych pasków. Tymczasem ekipy sprzątające zebrały z ulic... 34 tony. Czyżby to starcie konfetti „oficjalnego" z biurowym?
Konfetti z poufnymi danymi to naszym zdaniem kiepski pomysł na puzzle. Niektórzy już czekają na kolejną paradę, licząc na to, że z nieba w końcu zaczną spadać odpowiednio grubo zmielone banknoty. [2]

Hakerska pita

Grupa badaczy zajmujących się bezpieczeństwem sieci z Uniwersytetu w Tel Aviwie: Daniel Genkin, Lev Pachmanov, Itamar Pipman i Eran Tromer znalazła nowy sprytny sposób na włamanie się do komputera. Wystarczy odbiornik radiowy i kawałek chlebka pita.
Wykorzystanie sygnału radiowego w celu wykradania danych z komputerów nie jest niczym nowym, ale dotychczas wymagało drogiego sprzętu laboratoryjnego. Ekspertom z Izraela wystarczyły tanie komponenty.
Jak to działa? Atakujący wysyła maila z zaszyfrowanym tekstem w celu zainfekowania komputera, gdy komputer zaczyna go odszyfrowywać podsłuchiwane są fale radiowe, co pozwala na wyciągnięcie klucza kryptograficznego do danych.
A do czego w tym wszystkim chlebek pita? Skuteczna akcja hakerska to przede wszystkim dobre zachowanie pozorów. W tym właśnie pita ma pomóc - aby całe przedsięwzięcie wydawało się naturalne, nie wzbudzało żadnych podejrzeń, ani nie przyciągało uwagi. Odbiornik do przechwytywania fal radiowych z komputera jest tak mały, że mieści się właśnie w picie. PITA to także akronim Portable Instrument for Trace Acquisition - przenośnego urządzenia do szpiegowania. Metoda działa w odległości do 50 cm. Dalej robi się bezpiecznie.
Czy to początek hakerskich popisów kulinarnych? My tymczasem czekamy na coś z kuchni polskiej. Może być z tego niezły bigos. [3]

Falstart Madonny

Wyjątkowego pecha miała Madonna, pracująca od miesięcy nad nowym albumem. Do komputerów osób pracujących z gwiazdą włamał się haker, który wykradł wersje demo nowych utworów i upublicznił je w Internecie. Trzynaście piosenek sprzedał.



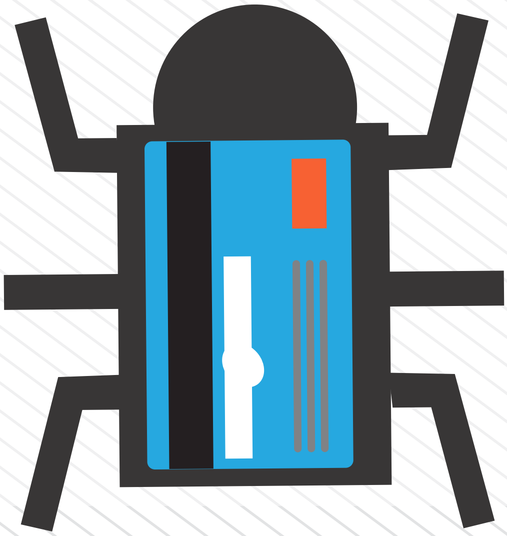
Utwory z najnowszego albumu „Rebel Heart” wyciekły do Internetu pod koniec zeszłego roku. Sama piosenkarka prosiła fanów na Instagramie, aby nie słuchali kradzionych singli. „Zostały pogwałcone moje prawa jako człowieka i artystki”. Później w ramach wczesnego prezentu gwiazdkowego dla fanów artystka wypuściła sześć piosenek.
Madonna od dawna darzyła Izrael szczególną sympatią i twierdziła, że jest „centrum światowej energii”. Wielokrotnie koncertowała w tym kraju, od lat praktykuje kabałę, formę mistycyzmu żydowskiego.
Haker, który przysporzył gwieździe kłopotów to 39-letni Adi Lederman, aspirujący piosenkarz, który brał udział w telewizyjnym konkursie TOP Izrael i castingu do izraelskiego reality show „A Star is Born in 2012”.
Lederman został aresztowany na początku tego roku i przyznał się do zarzucanych mu czynów.
Śledztwo w jego sprawie prowadzono przy współpracy z FBI. Sąd w Tel Awiwie skazał go na 14 miesięcy więzienia oraz grzywnę w wysokości 15 tysięcy szekli (ok. 3900 dolarów). W uzasadnieniu wyroku zaznaczono, że kara ma odstraszać innych z podobnymi zamiarami. Zapytany przez sędziego jak dotychczas zarabiał na życie Lederman odpowiedział: „Wydaje się, że głównie marnując życie, bo jak mi powiedziano - powinienem być na scenie”. I zaśpiewał piosenkę Stevie Wondera „Niczym się nie martw.”
Złośliwi twierdzą, że powinni go skazać na słuchanie całego albumu Madonny, dzień w dzień, przez 14 miesięcy. To dopiero byłaby dotkliwa kara. [4]

Na nic chowanie głowy w piasek

Przed czujnym okiem Facebooka już się nie ukryjesz. Naukowcy z działu sztucznej inteligencji portalu ogłosili na niedawnej konferencji w Bostonie powstanie nowego eksperymentalnego algorytmu, który jest w stanie rozpoznać na zdjęciach ludzi, nawet jeśli ich twarz nie jest widoczna. W takim przypadku algorytm w zamian poszukuje innych unikatowych cech charakterystycznych, takich jak fryzura, ubranie, sylwetka czy przybierana poza.
„Ludzie mają charakterystyczne cechy, nawet jak się patrzy na nich z tyłu” - mówi LeCun, szef sztucznej inteligencji w portalu. „Na przykłada Marka Zuckerberga można bardzo łatwo rozpoznać, bo zawsze nosi T-shirty koloru szarego”.
Ta zapowiedź oczywiście wystarczyła do tego, aby obrońcy prywatności wpadli w popłoch.
Zespół badaczy z Facebooka przeanalizował 40 tysięcy zdjęć z serwisu Flickr: na niektórych twarze ludzi były wyraźne, na innych ludzie byli odwróceni.
Ostatecznie skuteczność identyfikacji wyniosła aż 83 procent. Teraz wszyscy użytkownicy Facebooka drżą, aby znaleźć się w puli szczęśliwych 17 procent.
Czekamy na kolejne sukcesy badaczy z FB i może na przykład rozpoznawanie osób na podstawie zdjęć ich psów i kotów. [5]

Wydojeni w zoo

Service Systems Associates, firma obsługująca sklepy z pamiątkami i restauracje przy ogrodach zoologicznych i ośrodkach kultury w całych Stanach Zjednoczonych, przyznała, że w ich punktach doszło do naruszenia bezpieczeństwa przy płatnościach dokonywanych kartami kredytowymi i debetowymi.
Wszystko przez złośliwy malware zainstalowany na terminalach płatniczych.



W oficjalnym oświadczeniu Service System Associates napisano, że doszło do włamania i „jeśli gość korzystał z karty kredytowej lub debetowej płacąc w sklepie z pamiątkami pomiędzy 23 marca a 25 czerwca 2015 to dane z jego karty mogły zostać odczytane.” Jednocześnie firma zadeklarowała, że współpracuje w tej sprawie z organami ścigania i specjalistami ds. kryminalistyki. Zapewniła też, że malware został zidentyfikowany i usunięty, oraz że „wszyscy odwiedzający mogą już czuć się pewnie korzystając z karty kredytowej czy debetowej w punktach SSA”. Firma odmówiła podania dokładnych lokalizacji, w których doszło do naruszenia bezpieczeństwa, ale lista prawdopodobnych adresów i tak wyciekła do Internetu.

W ciągu ostatnich dwóch lat większość nadużyć dotyczących kart była wynikiem właśnie złośliwego oprogramowania zainstalowanego na terminalu płatniczym, dzięki któremu przestępcy wykradali numery kart i piny. Przechwycone w ten sposób dane mogą zostać sprzedane oszustom, którzy zrobią z nich pożytek np. w sklepach z drogim sprzętem takich jak Target czy Best Buy. Rozwiązaniem bezpieczniejszym niż karty magnetyczne są karty z chipem, których sfałszowanie jest bardzo trudne. Od października tego roku w Stanach Zjednoczonych to po stronie sprzedawców, którzy jeszcze nie zainstalowali czytników do takich kart, spoczywać będzie odpowiedzialność za nadużycia związane z płatnościami.

Mimo to, niektóre punkty sprzedaży przechodzą na czytniki do kart chipowych w żółwim tempie. Jeśli więc cyberprzestępcy chcą z kogoś zrobić jelenia czy wystrychnąć na dudka to mają jeszcze trochę czasu. I zoo okazało się dobrym miejscem na wydojenie karcianej krowy. [6]

[1] http://tinyurl.com/nlqwqlc
[2] http://tinyurl.com/o2x43ww
[3] http://tinyurl.com/q6ndu7l
[4] http://tinyurl.com/pysucr6
[5] http://tinyurl.com/psqbmju
[6] http://tinyurl.com/oc3mqtd

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