

# zawór bezpieczeństwa 20/2015

## Wścibskiemu dronowi dostało się słusznie

Ciąg dalszy sprawy ze wścibskim dronem, o której informowaliśmy ostatnio. Podczas trwającej prawie 2 godziny rozprawy amerykański sąd uznał, że William Merideth z Kentucky, który w lipcu br. zestrzelił drona, miał do tego prawo. Przypomnijmy: opalające się w ogrodzie córki Merideth przybiegły poinformować ojca o krążącym nad ich głowami latającym obiekcie. Ten bez chwili wahania chwycił za broń. Aresztowany przez policję twierdził, że sąsiad David Boggs, operator drona, łamał jego prywatność i szpiegował rodzinę. Sam Boggs zaprzeczył jakoby celowo krążył nad posiadłością sąsiadów. Merideth chce, aby wyrok w jego sprawie był precedensem dla podobnych historii tego typu, choć jednocześnie zastrzega, że nie jest zwolennikiem tego, aby na widok drona każdy od razu łapał za broń. Boggs ma zamiar odwoływać się od wyroku. Kwestią sporną okazały się niuanse o charakterze telemetrycznym: przed zestrzeleniem obiekt latał w powietrzu 200 stóp nad ziemią przez około 2 minuty. Na nagraniu wideo widać jak dron zwalnia i krąży - nie nad samą posiadłością Meridetha, ale tuż obok - przez około 26 sekund. Sędzia uznała jednak, że skoro

co najmniej dwóch świadków widziało drona poniżej linii drzew, to można uznać zdarzenie za naruszenie prywatności. A to oznacza, że Merideth miał prawo drona zestrzelić.

Gdyby satelity, z których korzysta Google i inni, były w zasięgu broni osobistej to zapewne niejedna skończyłaby jak dron Boggsa. **[1]** 

## Ktoś patrzy Ci na ręce?

Grasz w pokera online? Tego zapewne się nie spodziewałeś: ktoś może patrzeć ci na ręce! Eksperti z firmy ESET wytropili nietypowego trojana o nazwie Win32/Spy. Odlanor, który atakuje graczy w pokera online. Złośliwe oprogramowanie w szczególności upodobało sobie strony PokerStars i Full Tilt Poker. Jak działa Odlanor? W łatwy sposób: na zainfekowanym



komputerze trojan podgląda karty gracza i robi rzuty ekranu. Te są następnie przesyłane na komputery oszustów. Na screenach widać nie tylko wirtualne karty oponenta, ale także jego ID. Obie wspomniane wyżej strony pozwalają na wyszukiwanie użytkowników za pomocą ich ID, więc atakujący może z łatwością dołączyć do konkretnego stołu, przy którym gra ofiara. I oczywiście w ten sposób uzyskać przewagę w grze. Podobnie jak w przypadku innego złośliwego oprogramowania, Odlanora można złapać ściągaając aplikacje z nieznanym źródłem. Często towarzyszy on także różnym programom związanym z pokerem, jak np. Tournament Shark, Poker Calculator Pro, Smart Buddy czy Poker Office.

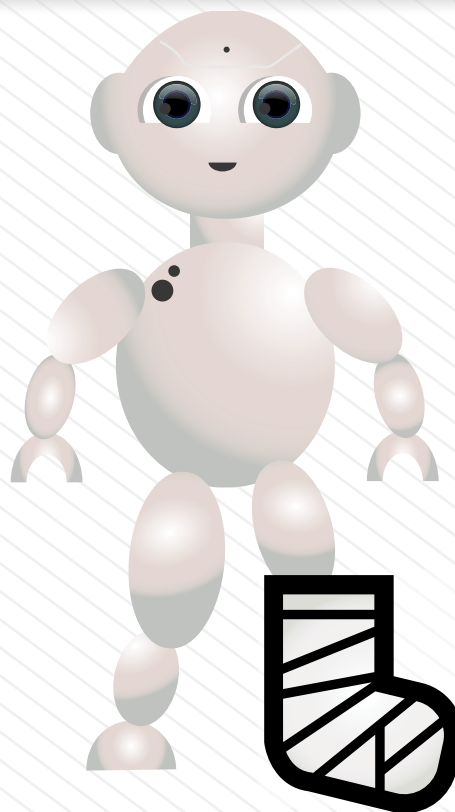
Pierwsze doniesienia o tym trojanie pojawiły się w marcu br. Do największej liczby infekcji dochodzi w krajach Europy Wschodniej, gł. w Rosji (36%) i na Ukrainie (35%). Wiele ofiar było również wśród graczy w Czechach, Polsce i na Węgrzech.

Cóż, pokerowi od zawsze towarzyszyła aura przestępczego półświatka. Na wieść o trojanie zapewne ucieszyliby się kowboje z amerykańskich westernów. Ta metoda gry, choć nieczna, może niejednego uchroniłaby od porachunków z rewolwerem. [2]

## Pijacki atak

Maszyny nierzadko padają ofiarami ludzkich frustracji. Wyjątkowego pecha miał humanoid Pepper - biały plastikowy robot z wbudowanym tabletem, których tysiące pracują w Japonii w punktach obsługi klienta jednego z operatorów komórkowych. Ten niezwykle przyjazny robocik z reguły wywołuje uśmiech na twarzach klientów: sam się porusza, rozmawia z klientami i przyjmuje od nich opinie. Pepper ma zdolność uczenia się: poprzez analizę mowy, wyraz twarzy i język ciała, robot potrafi odczytywać ludzkie emocje i odpowiednio na nie reagować: np. śpiewać lub opowiadać kawały.

Sześćdziesięcioletni klient, Kiichi Ishikawa, był wyjątkowo sfrustrowany jakością obsługi w jednym z punktów i postanowił wyżyć się na niewinnym robocie. Do tego delikwent okazał się pijany, więc



biedny Pepper nie miał w starciu większych szans. Mężczyzna kopnął robota, w efekcie czego Pepper porusza się teraz wolniej i prawdopodobnie ma uszkodzony wewnętrzny system komputerowy. Robot kosztuje 1460 euro plus miesięczny abonament. Sprawcę ataku zatrzymano za spowodowanie uszczerbku na zdrowiu robota. Przyznał się do winy, tłumacząc, że nie podobało mu się zachowanie obsługi sklepu. Faktycznie pracownika nie wypada kopnąć, Pepper napatoczył się jako łatwy cel. Najwyraźniej sympatyczny robocik nie był zaprogramowany do odpowiadania na pijackie ataki. Chyba w ramach aktualizacji oprogramowania Peppera trzeba będzie wgrać mu alokomat. [3]

## Jak syn wtopił ojca

Joaquin „El Chapo” Guzman to najbardziej poszukiwany na świecie baron narkotykowy, szef słynnego kartelu z Sinaloa. W lipcu br. dokonał

spektakularnej ucieczki z meksykańskiego więzienia Altiplano o zastrzonym rygorze, ośmieszając meksykańskie władze. I to zresztą nie po raz pierwszy - już raz udało mu się zbiec w 2001 roku. I za każdym razem odgraża się, że jeśli go złapią, ucieknie ponownie.

Podczas ostatniej ucieczki przedostał się przez kratkę prysznicową do wydrążonego tunelu, w którym czekał na niego motor na szynach. Przypuszcza się, że wcześniej mógł przekupić służby więzienne.

Czy El Chapo ukrywa się teraz w Kostaryce?

Wszystko na to wskazuje. Na ten trop naprowadził syn barona Jesus Alfredo Guzman Salazar, aktywny użytkownik mediów społecznościowych, który wrzucił na Twittera swoje zdjęcie z restauracji, okraszając je komentarzem „Wiecie z kim jem”. Na zdjęciu widać jeszcze dwóch innych mężczyzn - jeden z nich, mimo zakrytej emotikonką twarzy, po wąsach i budowie ciała zdradza niepodważalne podobieństwa do samego „El Chapo”.

Pech w tym, że młody Guzman zapomniał wyłączyć w telefonie lokalizację, która automatycznie wyświetliła się przy zdjęciu prowadząc do Kostaryki. Niefortunną fotkę mogło zobaczyć nawet 149 tysięcy śledzących go na Twitterze osób.

Podczas gdy policja kostarykańska sprawdza czy szef kartelu faktycznie przebywa na jej terytorium, za pomoc w złapaniu gangstera meksykańskie władze przeznaczyły nagrodę w wysokości 3.8 milionów dolarów. Stany Zjednoczone dorzuciły jeszcze 5 milionów i otworzyły specjalny hotline dla osób, które mogą pomóc.

Póki co wszystkie wysiłki pozostają bezskuteczne.

Połowę roboty wykonał już Twitter, może teraz pozostaje czekać aż o dokładnym miejscu przebywania „El Chapo” zaćwierkają ptaki. Przecież Kostaryka jest ich prawdziwym królestwem. [4]

## Hasło ze zdjęcia

Wszystko wskazuje na to, że w temacie biometrycznych metod identyfikacji użytkowników nie powiedziano jeszcze ostatniego słowa. Słynny haker Starbug stwierdził niedawno, że weryfikacja za pomocą linii

papilarnych już wcale nie jest taka bezpieczna.

Niemiecki badacz Jan Krissler z Uniwersytetu Technicznego w Berlinie, znany jako Starbug, ogłosił, że złamał słynne „hasło idealne” czyli Apple Touch ID i że hasło papilarne jest w stanie zdobyć ze zdjęcia palców użytkownika. Swoje dokonania zaprezentował na konferencji Biometrics 2015 w Londynie.

Jak to działa? Wystarczy zrobić wysokiej rozdzielczości zdjęcie palca z liniami papilarnymi, wydrukować je i wykonać lateksowy model, który po wyschnięciu przykładamy do czytnika, aby odblokować telefon. Starbug utrzymuje, że w ten sposób udało mu się odtworzyć odcisk palca niemieckiej minister ds. obrony narodowej, Ursuli von der Leyer.

Jego zespołowi udało się również odtworzyć tęczówkę kanclerz Angeli Merkel, wykorzystując wysokiej rozdzielczości zdjęcie zrobione podczas konferencji prasowej. Uzyskany obraz można nadrukować na soczewkę kontaktową i tym sposobem włamać się do jakiegokolwiek urządzenia, bazującego na tej metodzie identyfikacji.

Wszystkie dane można wykraść - twierdzi Starbur. Jednocześnie zaznacza, że biometria jest nadal przyszłością weryfikacji użytkowników, acz różne metody wymagają udoskonalenia. A póki co na wszelki wypadek zakładamy do zdjęć rękawiczki zabezpieczające i ciemne okulary. [5]



## Bezpieczeństwo za 2 dolce

Ile kosztuje hasło nie do złamania? Dwa dolary. Tyle życzy sobie 11-latek ze Stanów Zjednoczonych, która otworzyła niedawno manufakturę super bezpiecznych haseł. Swoją ofertę przedstawia



na stronie [www.dicewarepasswords.com](http://www.dicewarepasswords.com). Mira Modi tworzy hasła na zamówienie metodą Diceware. O co dokładnie chodzi? Diceware to metoda znana w kryptografii od dawna. Dziewczynka rzuca tradycyjną kostką do gry i otrzymane wyniki paruje ze słowami z listy

losowych wyrazów. W ten sposób tworzy sześciowyrazowe kombinacje niemożliwe do złamania. Skąd taki pomysł na biznes u 11-latki? Nieprzypadkowo. Mira jest córką Julii Angwin, dziennikarki zajmującej się tematami prywatności i autorki książki "Dragnet Nation". W ramach badań do książki zaangażowała ona córkę do tworzenia haseł metodą Diceware. Dziewczynka towarzyszyła matce wielokrotnie przy spotkaniach autorskich, a nawet sprzedawała podczas nich swoje hasła. Za każdym razem gdy przychodzi zamówienie Modi wyciąga kostkę. Odręcznie przygotowuje ciąg słów i efekty swojej pracy wysyła tradycyjną pocztą. Gdyby miała się tym zajmować na cały etat, wyciągnęłaby nawet 12 dolarów za godzinę - to więcej niż minimalna stawka godzinowa w Nowym Jorku. Dotychczas sprzedała około 30 haseł. Gdy nie zajmuje się produkcją haseł, uprawia gimnastykę i tańczy. Swoją przyszłość wiąże jednak z kryptografią i bezpieczeństwem. Przedsiębiorczość godna podziwu, acz złośliwi pytają po co komuś płacić za hasło, które i tak zna już ktoś inny? [6]

[1] <http://tinyurl.com/pl2gn2w>

[2] <http://tinyurl.com/pn2bdwv>

[3] <http://tinyurl.com/neplyzj>



[4] <http://tinyurl.com/nd7cyts>

[5] <http://tinyurl.com/ndo9h2h>

[6] <http://tinyurl.com/q76vndv>

Kolejne numery można śledzić również na serwisie społecznościowym **LinkedIn** 

Biuletyn „Zawór bezpieczeństwa” jest własnością Fundacji Bezpieczna Cyberprzestrzeń. Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści jak i samego biuletynu.

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