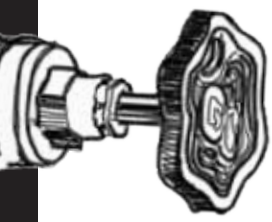
17/2015

FUNDACJA bezpieczna cyberprzestrzeń



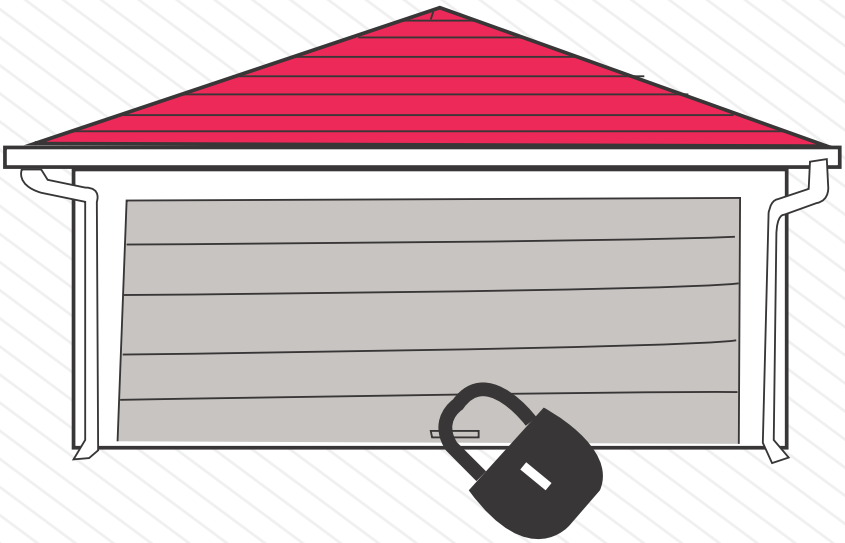
zawór bezpieczeństwa 17/2015

Parkometry nie lubią mera?

Automaty parkingowe we francuskim mieście Meaux, 40 km od Paryża, zaatakowały klientów biletami z obraźliwymi epitetami wymierzonymi w mera miasta, Jean-François Copé. Jak donosi „Le Parisien" w maju rozdystrybuowanych zostało ponad 500 takich paragonów.
W 2012 roku Jean-François Copé został wybrany na przewodniczącego Unii na rzecz Ruchu Ludowego. Z poparciem 50,3% głosujących pokonał byłego premiera François Fillona, który jednak również ogłosił zwycięstwo.
W 2014 po słabych wynikach swojej partii w wyborach europejskich oraz nieprawidłowościach finansowych ujawnionych przez media, Copé został zmuszony do rezygnacji z funkcji przewodniczącego. „Le Point" oskarżył go m.in. o zatrudnianie firmy znajomego do organizowania imprez partii. Do merostwa wpłynęło wiele skarg od oburzonych zachowaniem parkometrów mieszkańców Meaux. Podczas gdy sprawę ciągle bada policja, „Le Parisien" donosi, że stoi za nią najprawdopodobniej były pracownik firmy parkingowej Q Park. Dostęp do komputera, przy pomocy którego wpisano obraźliwe teksty, wymagał bowiem podania nazwy użytkownika i hasła. Lise Botrel, dyrektor ds. komunikacji firmy Q Park France, winy szuka na zewnątrz: „Być może padliśmy ofiarą hakera".
A może to francuskie wydanie „Buntu Maszyn". Parkometry nie lubią mera i mamy do czynienia z małą rewolucją francuską, tym razem w wydaniu maszyn, które zaraz zaczną wypisywać „Vive La Parcmètre!". [1]

Cyber Alibaba

Ostatnio głośno było o nowej szpiegolalce Barbie. Teraz okazuje się, że niezwykłe właściwości mają również te bardziej „przedpotopowe" zabawki.



Samy Kamkar, znany ekspert od bezpieczeństwa, tym razem w swoich eksperymentach sięgnął po zabawkę firmy Mattel IN-ME, rodzaj „pre-smartfona"

do czatowania dla dzieci. Ten kieszonkowy komputerek, mimo że już niedostępny na rynku, od czasu do czasu pojawia się na eBayu w cenie około 12$. Kamkar znalazł sposób na zhakowanie zabawki, dodał do niej antenę i kawałek harware'u i tym sposobem zrobił z niej... „klucze do garażu". Swoją konstrukcję nazwał OpenSesame.
Aż dziw, że sam nie przyjął nicku Cyber Alibaba.
„Każdy może otworzyć drzwi w ciągu paru sekund" - mówi Kamkar. OpenSesame umożliwia otwarcie drzwi garaży, które posługują się tzw. systemem „fixed code". Chodzi o system do bezprzewodowej komunikacji z pilotem, w którym kod do odblokowania drzwi jest stały przy każdym naciśnięciu przycisku na pilocie. Dla takiego systemu istnieje 4096 kombinacji cyfr. Złamanie kodu zajęłoby hakerowi 29 minut. Z czasem jednak Kamkar udoskonalił swoją metodę i udało mu się zredukować czas ataku z 1771 sekund do 8. Bezpieczniejszym rozwiązaniem jest tzw. „rolling code", który zmienia się po każdym naciśnięciu przycisku na pilocie. Kamkar przygotował filmik wideo - ostrzeżenie, w którym wyjaśnia jak rozpoznać czy nasze drzwi do garażu mogą być narażone na atak.
Nie wiadomo tak naprawdę ile garaży posługuje się systemem ze stałym kodem. A może czas wrócić do garaży zamykanych na kłódkę? Czas ataku dłuższy, a w szczególności trudno o atak zdalny. [2]

Nadstaw ucho, a powiem Ci kim jesteś

To coś dla leniwych, którym już nawet palcem nie chce się kiwnąć. Biometryczne technologie autoryzacji dostępu do urządzeń idą do przodu: już nie tylko odcisk palca pozwoli nam na odblokowanie smartfona. Amazon opatentował

właśnie system pozwalający na zalogowanie się do komórki... uchem.
Podobnie jak odciski palców, ludzkie ucho uznawane jest za unikalny identyfikator człowieka. Technologia opracowana przez Amazon bazuje na rozpoznaniu kształtu ucha i pozwala na odblokowanie telefonu bez konieczności wpisywania hasła - aby odebrać rozmowę przychodzącą wystarczy przyłożyć telefon do ucha i blokada zostanie zdjęta. Oprócz weryfikacji użytkownika technologia ta pozwoli również na regulację głośności dzięki oszacowaniu odległości między aparatem a uchem użytkownika. Według tej koncepcji możemy mieć pewność, że telefon będzie działał tylko z naszym uchem.
Na pewno Van Gogh uznałby, że to rozwiązanie mało praktyczne. My tymczasem czekamy, żeby zobaczyć która część ciała jest następna w kolejce. Być może na rynku pojawią się też zimowe czapki z otwieranym okienkiem do ucha. [3]

FUNDACJA bezpieczna cyberprzestrzeń

Szczyt facebookowej głupoty

Oto historia naszego kandydata do nagrody w kategorii najgłupsze posty na Facebooku. W marcu czterech uzbrojonych w atrapę pistoletu rabusiów napadło na buchmachera Ladbrokes na Portobello High Street w Edynburgu.
Po napadzie jeden z nich, 21-letni bezrobotny Gary Pacitti, napisał na swoim profilu na Facebooku: „Kocham pieniądze, to jest mój problem". Post okrasił „zawstydzoną" emotikoną. Gdy zaintrygowana siostra dopytała o szczegóły Gary dopisał: „Ladbrokes Portobello". Dzień przed napadem Pacitti pisał na Facebooku „Pięć lat za parę kawałków - nie dziękuję". Napastnicy zrabowali cenny zegarek i 4100 funtów. W czasie ucieczki jeden ze złodziei wskazując drogę krzyknął do Pacitti: „Gary, tędy". Dodatkowo DNA Pacitti znaleziono na pozostawionej masce, którą rabuś miał na sobie w trakcie napadu oraz na porzuconym samochodzie Audi, który służył grupie do ucieczki.
Policja dostała więc wystarczająco dużo wskazówek. Gdy namierzono rabusia, był zbyt pijany, aby mógł zostać przesłuchany. Aresztowany 9 marca Pacitti skomentował „Patrząc na ładne 7 lat... trochę wygrywasz, trochę przegrywasz", a odkąd trafił do aresztu pisał, że „kocha życie w Costa Del Saughton". Pacitti przyznał się do uczestnictwa w napadzie. Żadne skradzione przedmioty nie zostały odzyskane. Póki co aktywny Facebookowicz czeka na rozprawę, która odbędzie się w sądzie w Glasgow w lipcu. Trzej pozostali członkowie gangu pozostają na wolności.
Policja zapewne żałuje, że Pacitti nie zameldował się na Facebooku w trakcie napadu i nie oznaczył swoich kompanów, ale nic straconego – sąd mógłby mu nakazać korzystać z Facebooka w areszcie. [4]

DDoS-ami w szkoły

Siedemnastoletni uczeń szkoły średniej Eagle High School, który dokonał ataku DDoS na sieć komputerową dystryktu szkolnego w stanie Idaho, może zostać oskarżony o przestępstwo. Cyberataki nękały szkolne sieci przez półtora tygodnia.
W dystrykcie są 52 szkoły i ponad 36 tysięcy uczniów. Nastolatek najprawdopodobniej „wynajął" kogoś do przeprowadzenia ataków z różnych komputerów. Działanie młodego cyberprzestępcy miało dotkliwe dla całej społeczności szkolnej skutki. Uczniowie przygotowujący sie do testów stracili całą swoją pracę. Przez prawie cały tydzień nie były dostępne podręczniki oraz materiały online. Ucierpiały także dokumenty administracyjne, łącznie z listą płac. Dostęp do sieci przywrócono, ale to nie koniec historii. Uczeń został zawieszony i grozi mu wyrzucenie ze szkoły. Śledczy pracują nad sprawą i jeśli potwierdzi się, że to on stoi za atakami, najprawdopodobniej zostanie mu postawiony zarzut przestępstwa komputerowego, za który grozi do 180 dni w ośrodku dla trudnej młodzieży. Na jego rodziców może zostać nałożona kara finansowa jako rekompensata za straty poniesione przez szkołę.
Tymczasem dyrekcja, obawiając się, że uczniów z podobnymi umiejętnościami i ambicjami może być więcej, wysłała do wszystkich rodziców prośbę o rozmowę z dziećmi o cyberatakach i ich konsekwencjach. Pewnie rodzice powinni się skupić na konsekwencjach karnych, bo te związane z niefunkcjonowaniem szkoły mogą okazać się dla wielu uczniów zbyt atrakcyjne. [5]

Swój grafik lepiej zapisz na kartce

HotSchedules to oprogramowanie służące głównie restauracjom i małym firmom do zarządzania grafikami pracowników. Ci z kolei przy jego pomocy

mogą np. zamieniać się dyżurami z kolegami. Z HotSchedules korzystają sieci McDonald's, Chili i Bufallo Wild Wings. Narzędzie dostępne jest tylko online i akurat pechowo stało się ostatnio celem ataku DDoS, który przestawił je w tryb offline. Na Facebooku i Twitterze administratorzy poinformował użytkowników, że firma ma problemy techniczne, nad rozwiązaniem których pracuje. Obsługa klienta wysyłała harmonogramy pracy do każdego klienta, który zadzwonił albo wysłał maila, a nawet tych, którzy nie zgłosili się. Około 9-tej wieczorem w dzień ataku HotSchedules powiadomiło klientów, że oprogramowanie ciągle odnotowuje przestoje, ale jest już online. „Nasi inżynierowie pracują nad usprawnieniami, które uodpornią system na przyszłe możliwe ataki. Przepraszamy za niedogodności i doceniamy waszą cierpliwość. Będziemy wysyłać aktualizacje". Podczas gdy HotSchedules walczył z atakami, pracownicy masowo nie pojawiali się w pracy, powodując paraliż w niejednej firmie. Mimo, że obsługa klienta dobrze radziła sobie z reklamacjami, to okres przestoju niebezpiecznie przedłużał się, a komentarze na temat całego zdarzenia w mediach społecznościowych były bezlitosne. Ciekawe ilu pracowników pofatygowało się, by sprawdzić swój grafik bezpośrednio u źródła oraz ilu pracodawców potraktowało tę sytuację awaryjną jako test na lojalność? Na szczęście nie ma doniesień o DDoS-ie na Big Maca i skrzydełek Buffalo. [6]

[1] http://tinyurl.com/onjggyu
[2] http://tinyurl.com/otg8uqs
[3] http://tinyurl.com/odf5mmp
[4] http://tinyurl.com/nafrqj9
[5] http://tinyurl.com/no82xfm
[6] http://tinyurl.com/oml88mo

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

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo