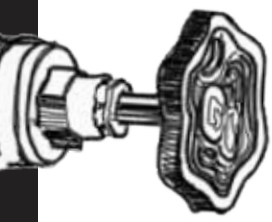
5/2014

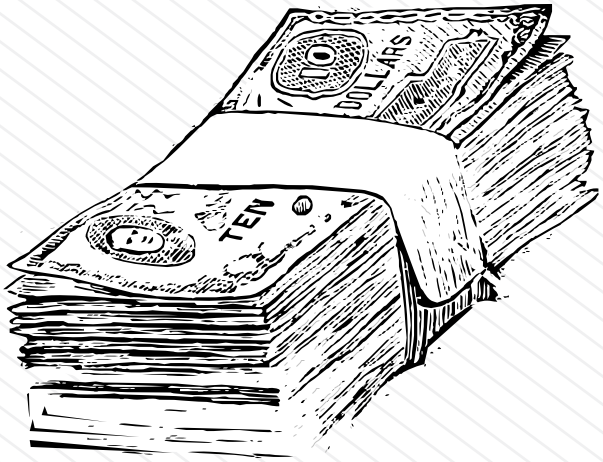
FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 5/2014

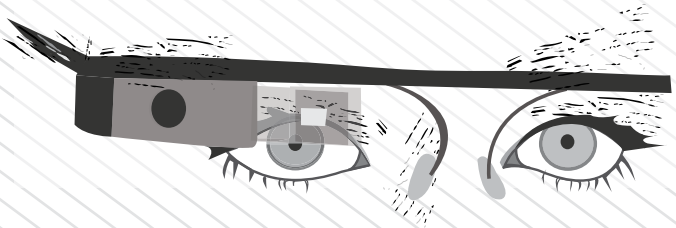
Sms-em wypłacisz gotówkę z bankomatu

Wypłata z bankomatu przez przesłanie do niego SMS-a to nie jest niestety nowy produkt bankowców tylko kolejny sposób na kradzież pieniędzy z bankomatów. Przestępcy opracowali metodę, która polega na uruchamianiu złośliwego oprogramowania w bankomacie, który jak wiadomo jest komputerem. Przesyłają do bankomatu SMS-a. Jak? Wcześniej, włamując się fizycznie do bankomatu, podłączają



do niego swój telefon komórkowy. Następnie łączą go poprzez port USB (nie trzeba ładować baterii w telefonie!). Przesłane SMS'y są odczytywane jako komendy uruchamiające malware (w tym wypadku "Ploutus"). Z bankomatu wypływa gotówka. Jak dostaniesz SMS-a o treści: "1000000101000031" to znaczy, że ktoś cię pomylił z bankomatem.[1]

Zdjęcia twojego życia



Dwójka naukowców z California Polytechnic San Luis Obispo stworzyła złośliwe oprogramowanie, które po zainstalowaniu na okularach Google'a (Google Glass) może bez wiedzy ich właściciela wykonywać zdjęcia co 10 sekund i przesyłać je do intruza. Wszystko na co spojrzy właściciel okularów zostanie udokumentowane i niestety może być wykorzystane przez przestępców, np: jeśli gdzieś spojrzy na swoje hasła, nie wspominając już o wszystkich sytuacjach prywatnych. Zwykle, gdy okulary robią zdjęcia w okularach zapala się lampka. W opisywanej sytuacji wykonanie zdjęcia jest zupełnie niewidoczne. Zdaje się, że to dopiero początek problemów z Google Glass. Aż strach pomyśleć co się będzie działo przy powszechnym ich używaniu. Chyba czas pomyśleć o ochronie przed zainfekowanymi okularami - w sytuacji wykrycia Google Glass w swoich okolicach. [2]

Sprytni chłopcy z helpdesku

"Sprytni chłopcy z helpdesku" (Smart Support Guys) to nowatorski, choć nie polecany, sposób na zarabianie pieniędzy. 34-letni Mohammed Khalid

Jamil wyłudzał pieniądze od klientów w Wielkiej Brytanii, którzy oczekiwali jego wsparcia przy rozwiązywaniu kłopotów z komputerem. Mohommed zapewniał, że jego firma pracuje dla Microsoft a on jest certyfikowanym inżynierem. Ofiarami firmy zatrudniającej specjalistów z hinduskim akcentem, tak popularnym wśród pracowników infolinii, były głównie osoby starsze. „Sprytni chłopcy" pomagali w usuwaniu problemów z bezpieczeństwem, po czym jak się łatwo domyślić właściciele mieli tych problemów jeszcze więcej. Kosz usługi od 42 do 180 EURO. Mahommed to recydywista - przed tym jak został „sprytnym chłopcem" był "PC Masterem". Na wymyślenie następnej ciekawej nazwy będzie miał sporo czasu. Wyrok sądu - 4 miesiące, 6 000 Euro kary, prawie 7 000 Euro rekompensaty dla 41 ofiar i prawie 17 000 Euro. No i wyszło na to, że najwięcej na tym zarobił sąd. [3]

Latający dron zaatakował triatlonistkę

Raija Ogden dzielnie walczyła na trasie triatlonu w zachodniej Australii kiedy nagle... coś jej spadło na głowę. Tym czymś okazał się dron, który służył do filmowania zawodów. Dron przez pewien czas spokojnie unosił się nad głowami zawodników, po czym nagle lotem nurkowym, z wysokości 10 m, wylądował na głowie dzielnej zawodniczki. Nie obyło się bez interwencji lekarskiej. Wstępne dochodzenie ustaliło, że przyczyną mogło być przejęcie dronu przez intruza, który „wbił" się w komunikację pomiędzy jego właścicielem a dronem i przejął kontrolę nad dronem. Oczywiście trudno jest ustalić źródło tego hackingu - wszystko odbyło się drogą radiową. Jeśli ktoś się nie weźmie za bezpieczeństwo tych urządzeń to w następnych zawodach triatloniści zmieniając rower na buty biegowe nie powinni zdejmować kasków rowerowych. [4]

Złośliwy twórca antywirusa na komórki

Na początku kwietnia numerem jeden sprzedaży wśród nowych aplikacji w Google Play było oprogramowanie "Virus Shield". Wszystkich specjalistów od bezpieczeństwa cieszy fakt, że użytkownicy Androida - najbardziej podatnego na ataki systemu operacyjnego dla urządzeń mobilnych - tak ochoczo wzięli się za instalowanie oprogramowania antywirusowego. Radość potęguje fakt, że zdecydowali się nawet zapłacić za nie 3,99$. Zaś wszystkich, którzy zainstalowali oprogramowanie cieszył fakt, że ich system jest wreszcie bezpieczny. Uruchomione skanowanie wskazywało wynik - zero

odnalezionych wirusów. Jednak ten fakt nie cieszył już wszystkich specjalistów od bezpieczeństwa - dlaczego? Wynik potwierdzał w 100% funkcjonalność programu, który... w czasie skanowania nie robił nic! Absolutnie nic! Natomiast wynik skanowania konta bankowego twórcy programu wykazał przychody następujące: 10 000 pobrań razy 3,99$ równa się 39 900$. Twórcy oprogramowania w jednej kategorii należą się podziękowania - program nie instalował żadnego złośliwego oprogramowania - złośliwy był tylko on sam. Jest obawa, że następnym razem i twórca i program mogą być złośliwi. [5]

Bezpieczne hasło powinno zawierać literę z serialu „Zdrówko”

Fali informacji dotyczącej nieszczęsnej dziurze w protokole OpenSSL towarzyszą oczywiście porady dotyczące tego co teraz robić aby być bezpiecznym. Niektóre z nich nadają się bardziej do kabaretu

F3kFk3

(zresztą przygotowywane z takim zamysłem). Serwis FunnyOrDie prezentuje zestaw dość idiotycznych porad, np:
– przystaw usta do komputera i wyssij z niego truciznę,
– korzystaj z komputera swojego kolegi jeśli nie jesteś pewien swojego,
– ściśnij dłoń swojemu komputerowi aby był pewien, że jesteście w jak najlepszych stosunkach.
Jednak nam najbardziej do gustu przypadła porada dotycząca zmiany haseł:
– zmień swoje hasła na nowe - powinny zawierać jedną wielką literę, jedną cyfrę i jedną literkę z serialu „Zdrówko”, gdyż badania pokazują, że hakerzy go nie oglądają.
Pewnie przekładając to na nasze rodzime poletko
– zmień swoje hasła na nowe - powinny zawierać jedną wielką literę, jedną cyfrę i jedną literkę z serialu „Klan”. [6]

[1] http://tinyurl.com/qa67re2
[2] http://tinyurl.com/ohbdzre
[3] http://tinyurl.com/pxus4y4

[4] http://tinyurl.com/qa694cp
[5] http://tinyurl.com/nj88acc
[6] http://tinyurl.com/nnpmuo9

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