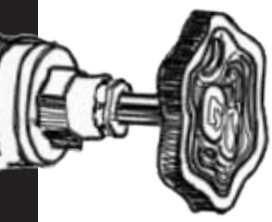
13/2015

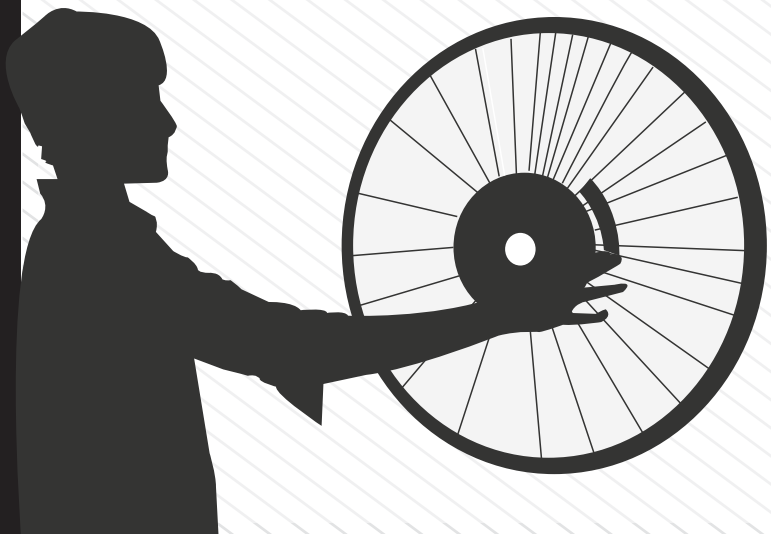
FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 13/2015

Roboty mają głos

W lutym tego roku Europol przeprowadził operację zdjęcia jednego z botnetów, czyli sieci komputerów kontrolowanych przez cyberprzestępców. Microsoft, współpracując z Europolem przy tej operacji (oprócz technicznej strony operacji, zajmował się również prawnymi aspektami przejęcia serwerów w czterech krajach), wykorzystał urządzenie do monitorowania armii robotów i analizy dźwięków przez nie wydawanych. Okazało się, że ciche armie robotów zombie „mają głos". I dosłownie i w przenośni można powiedzieć, że są to dźwięki, które przekazują skalę problemu cyberprzestępczości.
Takie legiony komputerów zombie (może i Twój) zainfekowanych złośliwym oprogramowaniem wydają „upiorne dźwięki". Przypomnijmy - złośliwe oprogramowanie zamienia urządzenia bez wiedzy właścicieli w urządzenia do np. kradzieży bankowych danych uwierzytelniających, rozprzestrzeniania wirusów, rozsyłania spamu itp., najprawdopodobniej ty i ja przeszliśmy dzisiaj obok pół tuzina takich niewolników.
Uwięzione w botnetach komputery są tak zaprogramowane, aby być w stałym kontakcie z ich komputerami sterującymi i stale proszą o zlecenia. Oczywiście takie prośby nie brzmią: „Które konta bankowe mam okraść?". Takie zapytanie jest rytmicznym dźwiękiem. Projekt pozwala naukowcom sortować dźwięki z zainfekowanych komputerów z całego świata. System przedstawia również dane dźwiękowe w postaci wizualnej.
Niestety botnety są mocno eksploatowanym narzędziem w rękach przestępców w sieci. Można ironicznie powiedzieć, że zagrożenia płynące z cyberprzestrzeni do tej pory był to cichy problemem, w tej chwili możemy go usłyszeć. Może naukowcom udałoby się skonstruować moduł, dzięki któremu po rozpoznaniu infekcji nasz komputer zacząłby płakać, coraz głośniej z każdym dniem bez łatania. [1]



NIEsławni Hakerzy

Ciekawy film o przypuszczalnie 10 najbardziej niesławnych hakerach – ever. Film klasyfikuje od dziesiątego miejsca do pierwszego uwzględniając w sumie wielkość szkód jakie zostały poczynione przez dane osoby pod względem finansowym,

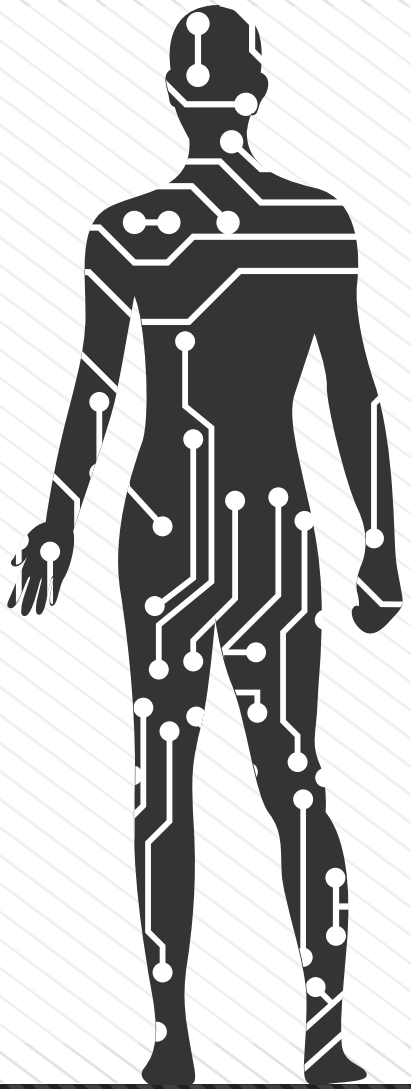
politycznym czy wizerunkowym.
Skoro już znalazła się taka klasyfikacja przybliżymy trochę historie jej „bohaterów".
Miejsce **10-te** zajął
Gary McKinnon – włamał się do NASA, oskarżany o popełnienie „największego włamania do wojskowych systemów komputerowych wszechczasów".
McKinnon twierdzi, że widział na serwerach NASA oryginalne zdjęcia z satelitów tejże instytucji zawierające obiekty UFO.
Miejsce **9-te Grupa hakerska LulzSec** grupa, która przyznała się do ataków na Sony Pictures w 2011 roku, a także do ataków na CIA, FBI & Scotland Yard.
Miejsce **8-me Adrian Lamo** – znany z licznych włamań do systemów komputerowych takich instytucji i firm jak: Yahoo!, AOL Time Warner, MCI, WorldCom, Microsoft, National Security Agency, New York Times. Postrzegany jako jeden z najlepszych specjalistów od wykrywania zależności między pozornie niezwiązanymi z sobą zdarzeniami w złożonych sieciach komputerowych. Nazywany "bezdomnym hakerem", ze względu na cygański styl życia.
Mathew Bevan & Richard Pryce zajęli miejsce **7-me.** Włamali się do wojskowych komputerów USA i używali ich do infiltracji zagranicznych systemów i o mało co nie wywołali międzynarodowego incydentu między USA i Koreą Północną.
Jonathan Joseph James na miejscu 6-tym – zmusił NASA do zamknięcia strony na 3 tygodnie. Po tym jak skradł oprogramowanie, które kontrolowało środowisko życia na międzynarodowej stacji kosmicznej. W sieci działał pod pseudonimem c0mrade, zdobywając dostęp do serwerów dzięki backdoorom.
Miejsce **5-te dla Kevina Poulsena** osadzonego w więzieniu po włamaniu do komputerów Pentagonu, FBI i uzyskaniu informacji nt. sił powietrznych USA. Skazany na 51 miesięcy więzienia w 1995 roku po tym jak w celu wygrania w konkursie radiowym Porsche 944 włamał się do komputerów radia KISS-FM. Sprawa włamania została przedstawiona w programie Unsolved Mysteries (ang. Nierozwiązane

Zagadki), amerykańskiego odpowiednika polskiego programu 997. Został złapany właśnie dzięki widzowi programu.
Obecnie Poulsen jest jednym z redaktorów serwisu Wired. Współpracuje z policją, w 2006 roku pomógł policji złapać pedofila, który na kontach na MySpace zamieszczał pornografię dziecięcą.
Miejsce **4-te dla Kevina Mitnicka**. Włamał się do Pentagonu, Motoroli i Nokii. Złapany przez FBI odsiedział 5 lat więzienia i miał 3 letni zakaz korzystania z Internetu. Inżynieria społeczna była dla Mitnicka główną metodą uzyskiwania informacji, w tym także haseł dostępu.
Na corocznej konwencji hakerów DEFCON w Las Vegas w 2014 roku Mitnick ogłosił, że ukradnie tożsamość dowolnego uczestnika w 3 minuty, czego dowiódł odnajdując numer ubezpieczenia społecznego jednego z ochotników wybranego spośród słuchaczy.
Na niechlubnym podium znaleźli się na **3-cim miejscu Anonymous** – globalna grupa aktywistów internetowych. Niektóre z ich celów: Rząd Chin, Watykan, FBI, CIA.
Miejsce **2-gie** należy do **greckiego matematyka ASTRY** (nieznana prawdziwa tożsamość), który ukradł i sprzedał dane dot. technologii broni. Spowodowanie szkody szacowane są na ponad 360 mln USD.
Zwycięzcą został Albert "seqvec" Gonzalez, oskarżony o kierowanie grupą przestępczą, która dokonała łącznie kradzieży i ich późniejszej odsprzedaży ponad 170 milionów numerów kart kredytowych oraz danych ich posiadaczy – szacuje się, że koszt

szkód przekracza 400 milionów USD i jest to największe takie oszustwo w historii. Tego typu rankingi można podsumować tylko tak: im lepiej tym gorzej! Wreszcie możemy być dumni z faktu, że w rankingu nie ma Polaków. [2]

Co w skórze piszczy

Społeczność biohakerska to społeczność, dla której genom i komórki naszych organizmów to kawałek kodu jak program komputerowy, który można zmieniać, ulepszać i też hakować. Biologia to po prostu technologia - twierdzi dr Rob Carlson, biotechnolog i autor książki „Biology is Technology". Biohakerzy zajmują się ingerencją w ciało człowieka min. wszczepianiem implantów i czipów.
Wszczepianie „ciał obcych" to nie nowość, jednak kojarzy się raczej z urządzeniami, wszczepianymi w ludzkie ciała z powodów medycznych – implanty, rozruszniki serca, pompy insulinowe – takie części zamienne dla człowieka. W obszarze zainteresowań szwedzkiej firmy skupiającej biohakerów BioNyfiken jest również wszczepianie technologii człowiekowi ale po to by stworzyć ludzi doskonalszych, lub poprawiać wygodę życia. Tak, tak, to już nie fikcja, to się już dzieje.
Jak przekonują Szwedzi, osób, które eksperymentują z implantami umożliwiającymi wykonanie codziennych zadań jest coraz więcej. Ta społeczność rośnie i możliwość wykonywania takich czynności jak: odblokowanie urządzeń osobistych bez kodu PIN, uzyskiwanie dostępu do systemów komputerowych i przechowywanych danych, robienie e-zakupów, a także prostszych jak kontrola zamków w drzwiach – zastosowanie w biznesie przyszłości – jak to ma już miejsce w budynku Epicenter w Sztokholmie kusi człowieka przyszłości.
Temat tzw. „udoskonalonych" ludzi budzi wiele kontrowersji jednak trend rozwija się błyskawicznie, jest wielu jego entuzjastów, którzy twierdzą, że nie unikniemy wzrostu społeczności, która eksperymentując, z pełną świadomością ryzyka będzie testować na sobie różnorakie technologie i ulepszenia. Dobrze więc byłoby w zgodzie z duchem czasu mieć na względzie również kwestie regulacji i bezpieczeństwa.



Jeśli pozwolimy, aby nasze ciało zawierało dane osobiste, to stwierdzenie: „Ktoś się do mnie włamał" już wkrótce może nabrać nowego znaczenia. [3] [4]

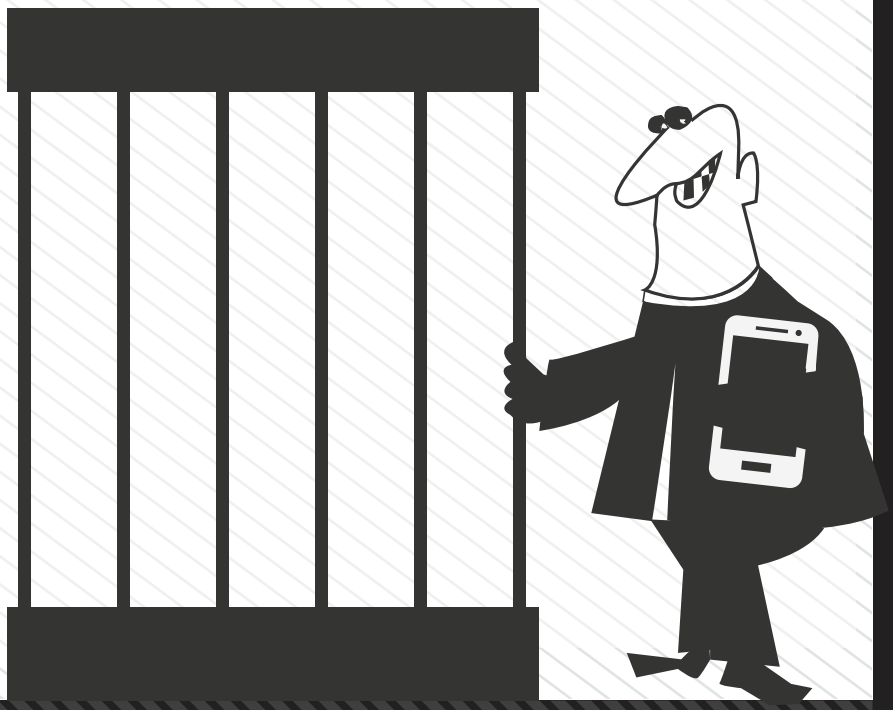
Wystarczy, że spojrzysz na smartfona i sam się odblokuje?

W tym roku na „Mobile World Congress" przedstawione zostały ciekawe produkty, które wykorzystują kamery smartfonów. Oprócz ciekawostek, jak nakładka na kamerę smartfona, która „zmienia" telefon w kamerę termowizyjną oraz urządzenia SCiO, które przy pomocy Bluetooth LE łączy się z telefonem i ma umiejętność identyfikacji wskazanego produktu wraz ze szczegółowymi informacjami

na jego temat (np.: informacje o zawartości tłuszczu, węglowodanów, cukrów oraz liczbie kalorii w badanym produkcie), znaleźliśmy także coś „bezpiecznego".
Owe „bezpieczne" rozwiązania, mogą zainteresować tych, którzy mają już dość zapamiętywania coraz to nowych i trudniejszych haseł. Otóż podczas marcowego „Mobile World Congress" zaprezentowano dwa urządzenia, które przy użyciu zwykłego aparatu smartphone i odpowiedniej aplikacji mogą być wykorzystywane dla identyfikacji biometrycznej, są to: skaner linii papilarnych i skaner oczu. Za ich pomocą można zrobić sobie scan swojego odcisku palca lub scan wzoru naczyń krwionośnych w białkach oczu, które są unikatowe dla każdej osoby, podobnie jak wzory linii papilarnych i używać ich później do np.: blokowania i odblokowania swojego telefonu.
Z pewnością mamy coraz większy wybór urządzeń i aplikacji dla naszych smartfonów, aparaty mogą służyć do bardziej kreatywnych rzeczy niż robienie selfies i zdjęć kotów. Można będzie robić więcej rzeczy „z przymrużeniem oka". [5]

14-letni haker samochodu

Podczas CyberAuto Challenge, organizowanym przez Battelle – organizację non-profit, 14-letni chłopak z powodzeniem włamał się do komputera samochodu (organizatorzy nie ujawniają ani marki samochodu ani danych czternastolatka). Hackathon który jest wyzwaniem dla uczniów, organizowany jest od trzech lat i skupia oprócz uczestników, także producentów i technologów samochodów. W najnowszych modelach samochodów, większość działa za pomocą układów elektronicznych. Właśnie ogromna liczba informacji wymienianych między dziesiątkami urządzeń w nowoczesnym aucie wymusiła zastosowanie magistrali danych, np. CAN (Controller Area Network). Nastolatek choć nie znał się na technologii użytej w samochodzie miał pojęcie o czymś takim jak magistrala CAN.
Do skonstruowania przyrządu do bezprzewodowej kontroli niektórych funkcji w samochodzie użył bardzo prostych części: nadajnika i płytki obwodu drukowanego. Co prawda pozwoliło mu to na uzyskanie dostępu do niewielu funkcji, jednak i tak to już coś. Był w stanie uruchomić bezprzewodowo ze swojego telefonu komórkowego wycieraczki, szyby czy światła. Czternastolatkowi do włamania wystarczyły części zakupione za niecałe 15 USD.
Nadchodzą czasy, w których pokolenie „digital natives" dochodzi do głosu, już niedługo możemy zastanawiać się nad tym czy większe zagrożenie stanowią młodzi kierowcy z ich brawurową jazdą czy młodzi hackerzy samochodów. Poproszenie nastolatka z prawem jazdy o wstawienie samochodu do garażu, z nadzieją oderwania go od komputera, też może okazać się słabym pomysłem. [6]



FUNDACJA bezpieczna cyberprzestrzeń

Dali się złowić

Do ciekawego zdarzenia doszło ostatnio w więzieniu Wandsworth w południowo-zachodnim Londynie. Uwięziony w nim oszust Neil Moore wysłał do funkcjonariuszy więziennych fałszywy e-mail zawierający przygotowany przez niego dokument zezwalający na jego wyjście z więzienia za kaucją. E-mail musiał wyglądać bardzo wiarygodnie, ponieważ urzędnicy dali się „złowić" i 28 letni Neil Moore został zwolniony z więzienia.
Do utworzenia fałszywego konta pocztowego Moore wykorzystał, nielegalnie zdobyty telefon komórkowy, z którego wysłał do personelu więziennego e-mail rzekomo od starszego referenta sądu z zaleceniem wypuszczenia jego samego za kaucją. Ponadto Moore utworzył fałszywą domenę internetową, która tylko nieznacznie różniła od oficjalnej domeny Trybunału, zarejestrowaną z wykorzystaniem danych jednego z przedstawicieli organów ścigania. Więzień został zwolniony w dniu 10 marca. Co ciekawe podstęp Moore'a został odkryty dopiero, gdy przyszedł do niego adwokat.
Moore wrócił ze swojego zwolnienia po trzech dniach. Jak się można domyślić oszustwa komputerowe to nie nowość dla pana Moore'a. Już przed swoją spektakularną ucieczką z więzienia udając pracowników banków: Barclays, Lloyds Bank, Santander udało mu się oszukać kilka organizacji, w sumie na kwotę 1 819 000 £. Moore przyznał się do ośmiu zarzutów.
Zadziwiający w tej całej historii jest również fakt, że sędzia opisał pana Moore'a mianem „genialnego" przestępcy, który wykazał się pomysłowością, przebiegłością i kreatywnością. Przecież każdego dnia słyszymy o oszustwach internetowych, fałszywych e-mailach i stronach internetowych, słyszymy o różnego rodzaju phishingu, gdzie przestępcy podszywający się pod strony banków i instytucji kradną wiele pieniędzy, każdy chyba na „własnej skrzynce" przekonał się o problemie wszechpanującego spamu. Szczęśliwy pan sędzia, który nie dostaje spamu z phishingiem. [7]

[1]http://tinyurl.com/ow5vusw
[2] http://tinyurl.com/qdtou6m
[3] http://tinyurl.com/pqeysh7 [4] http://tinyurl.com/ncf6ky9
[5] http://tinyurl.com/p4fq9mh
[6] http://tinyurl.com/mb33f2u
[7] http://tinyurl.com/q4vyh7w

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