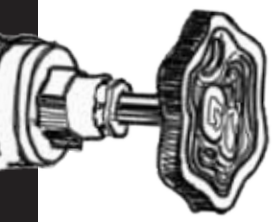
14/2015

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 14/2015

Szalony bot

Gdy na Twitterze z konta @jeffrybooks wysłany został zawierający groźby wpis „I seriously want to kill people" (*ang. na serio, chcę zabijać ludzi*), odnoszący się do jednej z imprez w Amsterdamie, policja długo nie zwlekała z wizytą u właściciela. Jednak podczas przesłuchania 28-letniego Holendra, szybko wyszło na jaw, że sprawa nie jest tak oczywista jak się początkowo wydawało: Jeffry van der Goot nie był autorem tych gróźb. Okazało się, że do prowadzenia konwersacji na Twitterze i publikowania wpisów korzystał z bota, który brał losowe słowa z archiwum wcześniejszych wpisów i układał z nich zdania. Złożywszy wyjaśnienia policji, van der Goot musiał zamknąć konto, na którym szalał bot. Czuł się jednak zagubiony w kwestii odpowiedzialności prawnej za niefortunną kompilację na Twitterze: przyznał się do uruchomienia bota, ale zdecydowanie zdystansował od tezy, jakoby produkcja robota miała wyrażać jego osobiste opinie.
Nie po raz pierwszy szaleństwa bota sprowadzają na właściciela kłopoty. Jak będzie z odpowiedzialnością prawną w takich przypadkach? Przyszłość pokaże, czy wolność słowa uchroni właścicieli przed procesem. Zagadką pozostaje w jaki sposób policja dowiedziała się o tym potencjalnie groźnym wpisie - podobno nie ze zgłoszenia osób trzecich. Czyżby więc śledzenie w sieci miało sens? A może policja ma swojego podobnego bota, który losowo trafia na podejrzanych? No i udało się. [1]

Szkoła w szachu ransomware

Ransomware, czyli programy przygotowane przez przestępców w celu wyłudzenia haraczu, atakują coraz odważniej. Na ataki narażeni są nie tylko użytkownicy prywatni. Złośliwe oprogramowanie nie oszczędza też firm, ani instytucji. Oszukańczy program czasami przybiera postać fałszywego antywirusa. To wyjątkowo uciążliwy malware, gdyż szyfruje wszystkie dane znajdujące się na dysku. Ich odzyskanie możliwe jest po uiszczeniu haraczu - użytkownik ma wtedy otrzymać klucz do odszyfrowania.
Ostatnimi czasy celem ataku ransomware stał się jeden z okręgów szkolnych w południowo-zachodnim New Jersey. Dziennik The South Jersey Times donosi, że na skutek działania ransomware padł cały system od zarządzania obiadami w szkolnej stołówce po serwery mailowe. W zaatakowanym zespole szkolnym uczy się około 1700 uczniów na czterech

poziomach szkoły podstawowej. Dostęp do swoich plików stracili i oni i grono pedagogiczne: zaatakowane zostały głównie dokumenty Word, Excell i pliki pdf. „Jak w 1981 roku" - mówił zaskoczony dyrektor Terry Van Zoeren, jednocześnie zapewniając, że zaszyfrowane pliki zostały odzyskane z backupu, a dostęp do maili zostanie szybko przywrócony. Pochodzący najprawdopodobniej z mailowego załącznika ransomware szybko dokonał spustoszenia w całej szkolnej sieci, a za odkodowanie danych szantażysta domagał się 500 bitcoinów . Cyberprzestępcy nie wybrali najbogatszego celu ataku, ale mimo że na opłacenie haraczu decyduje się zaledwie 2 procent właścicieli zaatakowanych urządzeń, to przy masowej liczbie ataków zysk jest zapewniony. Póki co sprawą zajmuje się policja i FBI, a dzieciaki... cieszą się, bo w szkole przełożono planowane testy i liczą na to, że na stołówce poradzą sobie z problemem. [2]

Pod czujnym okiem

Chcesz wiedzieć czy ktoś śledzi twoją korespondencję? Jeśli korzystasz z Gmaila i przeglądarki Chrome, teraz jest to proste: przed śledzącymi mailami ostrzega nowa wtyczka UglyEmail.
Wiele firm, jak dla przykładu Yeswear, Bananatag oraz Streak, sprawuje czujną pieczę nad twoją aktywnością mailową. Wiedzą o niej prawie wszystko: kiedy otworzyłeś maila jednego z ich klientów, gdzie się aktualnie znajdujesz, z jakiego urządzenia się logujesz, na jaki link klikasz. Oczywiście wszystko bez twojej zgody.
Podglądanie korespondencji użytkowników jest bardzo popularną praktyką wykorzystywaną przez firmy. Aby śledzić maile firmy dokładają w treści wiadomości malutki, zwykle przezroczysty, obrazek o wymiarach 1x1 pikseli. To tak zwany piksel zliczający lub trakujący, który rejestruje aktywność użytkownika.
Działanie UglyEmail jest bardzo proste - ze strony http://uglyemail.com/ wystarczy pobrać i zainstalować

wtyczkę, która identyfikuje niechciane maile - obok takich wiadomości będzie wyświetlać się mała ikonka oka. To ostrzeżenie, że jeśli nie chcemy przekazywać naszych informacji reklamodawcom, lepiej takiego maila nie otwierać.
Autorem wtyczki jest Sonny Tulyaganov, który zapewnia, że "UglyEmail nie przechowuje, nie zapisuje, ani nie przekazuje żadnych danych użytkownika z jego skrzynki Gmail, ani z komputera". Póki co narzędzie to ma jednak parę ograniczeń: pod czujnym okiem UglyEmail pracować mogą tylko użytkownicy Gmaila, wtyczka nie współpracuje z popularnym Outlookiem. A dodatkowo działa jedynie na przeglądarce Chrome, choć Tulyaganov zapewnia, iż wersje na Firefoxa i Safari to tylko kwestia czasu. Autor zapowiada również, że w niedalekiej przyszłości właściwości programu mają być rozszerzone na umiejętność rozpoznawania pikseli śledzących także innych firm. „Brzydki email" wydaje się dość atrakcyjny dla fanów prywatności. [3]

Alerty męczą mózg

Czy kiedykolwiek czułeś, że szklą ci się oczy i siada koncentracja, gdy na monitorze pojawia się kolejny alert bezpieczeństwa? Spokojnie, nie ma powodu do zmartwień – reakcja Twojego organizmu jest zgodna z biologią.

Przy użyciu rezonansu magnetycznego naukowcy zbadali jak reaguje ludzki mózg na wielokrotne ostrzeżenia wyskakujące w krótkim czasie na ekranie monitora. Eksperyment wykazał, że już po jednym alercie bezpieczeństwa następowało gwałtowne obniżenie aktywności mózgu przy przetwarzaniu bodźców wizualnych. Po trzynastym ostrzeżeniu zauważono ogólnie bardzo duży spadek. Takie osłabienie koncentracji jest wynikiem zjawiska habituacji, czyli procesu polegającego na stopniowym zanikaniu reakcji na powtarzający sie bodziec, jak w tym przypadku wyskakujące okienko z alertem.

Już wcześniej wiele badań potwierdziło, że im więcej razy komputer czy smartphone pokazuje ostrzeżenie, tym trudniej o reakcję użytkownika i jego bezpieczną decyzję. Ludzie niejako przyzwyczajają się do alertów i często odkładają działanie na później, co zwykle przypisywane jest beztrosce lub nieuwadze. Jest to tymczasem proces neurologiczny, zachodzący nieświadomie, związany z tym jak mózg przetwarza bodźce wizualne. Naukowcy doszli więc do wniosku, że jedynym sposobem na lepsze przyciągnięcie uwagi użytkownika byłoby zaprojektowanie interfejsów mniej podatnych na proces habituacji. Jak wykazał przeprowadzony na 25 osobach eksperyment jednym z takich skutecznych rozwiązań mogłaby być gama alertów o różnych kształtach, kolorach i innych właściwościach. Taki arsenał zmiennych ostrzeżeń dynamizowałaby uwagę odbiorcy, aktywizując szczególnie te części mózgu, które przestawały nadążać przy powtarzających się takich samych okienkach.

To wnioski pomocne dla producentów hardware'u i software'u, którzy na co dzień pracują nad ulepszeniami w interfejsach użytkownika. Pozostaje liczyć na to, że wymyślą oni atrakcyjne alerty, które będą pobudzać a nie zamęczać i wszyscy będą z utęsknieniem czekać na kolejną paczkę patchy. [4]

Gorące dane

Pojęcie "air gap" (dosłownie "szczelina powietrzna") w świecie IT oznacza fizyczne odłączenie komputera od sieci. Taka praktyka jest wykorzystywana przy pracy z poufnymi danymi lub w miejscach, gdzie prowadzone są różne krytyczne procesy (np. banki, elektrownie) i dąży się do wyeliminowania wszelkiego ryzyka ataków sieciowych.

Wydawać by się mogło, że komputerowi odłączonemu od Internetu nic poważnego nie grozi i faktycznie rozwiązania typu "air gap" uznawane były dotychczas za bezpieczne. Jednak tylko do czasu, cyberprzestępcy zabrali się również za nie, stosując do wykradania danych „malware air gap".

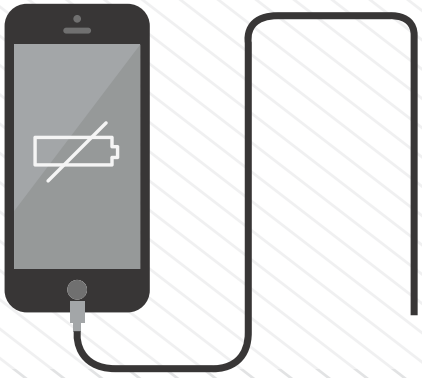
W zeszłym roku donoszono o metodzie wykorzystywania fal dźwiękowych do ataków na niepodłączone do sieci, pozostające w bezpośredniej bliskości komputery, z tym że dane mogły być odczytane z odległości maksymalnie 7 metrów.

Najnowsza metoda wykradania danych, opisana przez naukowców z Uniwersytetu Ben Gurion, nazywa się BitWhisper i polega na wykorzystywaniu wymiany ciepła pomiędzy dwoma komputerami. Skuteczny atak wymaga zainstalowania na urządzeniach wysyłającym i przyjmującym złośliwego oprogramowania, które umożliwi wymianę informacji. Trzeba dodać, że metoda nie jest zbyt wydajna - szybkość transferu danych to 8 bitów na godzinę. To zapewne jednak wystarczy, żeby wykraść np. hasła. Szybkość przesyłu to nie jedyny mankament. Kolejny to na przykład to, że komputery nie mogą być oddalone od siebie więcej

niż 40cm. Nas zastanawia czy pod wpływem ciepła pakiety nielegalnie przejęta informacja nie ulega „odkształceniu”? [5]

Ładowarki do lamusa?

Powraca temat bezprzewodowego ładowania. Po Starbucksie i McDonald’s, które już wcześniej zdecydowały się na ofertę stacji dokujących, z duchem czasu chce iść IKEA. Jeszcze w kwietniu ma wprowadzić do sprzedaży serię mebli wykorzystującą nowy standard ładowania bezprzewodowego.
Rozwiązanie to zaprezentowano na Mobile World Congress w Barcelonie. Bezprzewodowe ładowarki pozwolą na wyeliminowanie wijących się po podłodze kabli, które często zaburzają estetykę wnętrza. W nowej ofercie znajdą się m.in. lampy stołowe i podłogowe oraz stoliki nocne. Bezprzewodowe meble mają kosztować około 20 euro więcej. Dla tych, którzy przemeblowania robić nie planują, a chcieliby korzystać z nowego standardu, IKEA wypuści specjalne podstawki ładujące, w cenie 30 euro, możliwe do zainstalowania na już posiadanych sprzętach. Aby naładować telefon wystarczy położyć go na ładowarce indukcyjnej zintegrowanej z danym meblem. Jest jednak pewne ograniczenie, a mianowicie kwestia kompatybilności urządzenia. Komórka musi pracować w standardzie ładowania Qi, a takie aparaty - mimo że jest ich coraz więcej - nie są jeszcze powszechne. Standard Qi pozwala na indukcyjne przekazywanie energii elektrycznej z odległości do 4cm. Same ładowarki będą podłączone do prądu przy pomocy klasycznego kabla. Złośliwi pytają na co to komu, komentując że w istocie chodzi o zamianę kabla w jednym miejscu na kabel w innym miejscu. Pozostaje liczyć na to, że ktoś wymyśli bezprzewodowe kable. [6]



[1] http://tinyurl.com/o9bcz93
[2] http://tinyurl.com/p3xwcc2
[3] http://tinyurl.com/pq9gl4h
[4] http://tinyurl.com/pfqzume
[5] http://tinyurl.com/qbr6dle
[6] http://tinyurl.com/p9fh228

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