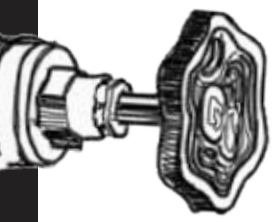
16/2015

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 16/2015

Roboty w służbie chirurgii - czy bezpieczne?

Ostatnie doniesienia kładą się cieniem na bezpieczeństwie operacji chirurgicznych wykonywanych przy udziale robotów. Naukowcy z Uniwersytetu Waszyngtona dowiedli, że podczas tego typu operacji istnieje ryzyko ataku hakerskiego. Przeprowadzili oni eksperyment na robocie medycznym Raven II, którego w kontrolowany sposób zhakowali. Odkryli tym samym, że istnieje możliwość nie tylko monitorowania i zakłócania zdalnie trwającej operacji, ale także całkowitego przejęcia kontroli nad robotem i przebiegiem procesu.
Naukowcom udało się również uruchomić mechanizmy powodujące automatyczne zatrzymanie pracy robota i przerwanie operacji.
Komunikacja między lekarzem a robotem odbywa się przy wykorzystaniu specjalnie stworzonego protokołu ITC (Interoperable Telesurgery Protocol), który okazał się być całkowicie otwarty i dostępny publicznie.
Obraz operacji przeprowadzanych przy udziale Ravena II był transmitowany przez Internet bez szyfrowania - operację mógł więc podglądać każdy.
Najłatwiejszym sposobem na zabezpieczenie się przed tego typu atakiem jest przepuszczenie ruchu między chirurgiem i robotem przez szyfrowane połączenie VPN.
Wprawdzie powyższe zdarzenie było tylko kontrolowanym eksperymentem, ale strach pomyśleć jakie konsekwencje miałby prawdziwy atak hakerski podczas operacji. Oby luki w systemie zostały szybko załatane, bo nikt nie chciałby zostać na stole operacyjnym np. z otwartym brzuchem czy też mieć do czynienia z innymI skutkami, których opisy nadają się do kategorii czarnego humoru. [1]

Aplikacja Pizzy Hut uratowała życie

Do niecodziennej sytuacji doszło w miasteczku Avon Park na Florydzie: 4 maja o godzinie 3:40 nad ranem za pośrednictwem aplikacji mobilnej do lokalnej Pizzy Hut wpłynęło zamówienie, zawierające w polu komentarza prośbę o wezwanie pomocy pod numerem 911. Pracownicy Pizza Hut rozpoznali, że kontakt pochodzi od stałej klientki, Cheryl Treadway, zrozumieli zgłoszenie chęci pomocy i prośbę potraktowali poważnie.

Wezwani przez nich policjanci z Highlands County Sheriff's Office udali się pod wskazany adres, gdzie zastali kobietę z małym dzieckiem na rękach, przetrzymywaną przez swojego partnera.
W domu przebywała też dwójka starszych dzieci. Uzbrojony w nóż Ethan Nickerson więził partnerkę przez cały dzień. Powodem miała być wcześniejsza kłótnia pary. Dopiero po całym dniu kobiecie udało się przekonać napastnika, aby mogła skorzystać z telefonu i pozwolił jej zamówić pizzę.
Mieszkaniec Florydy, 26-letni Ethan Earl Nickerson został aresztowany pod zarzutami m.in. napadu z bronią, pobicia i porwania. Kobiecie należy pogratulować pomysłu na wezwanie pomocy.
Nie wiemy jednak czy do przetrzymywanej wraz z policyjną odsieczą dotarła też pizza, która jest jedną z najbardziej popularnych potraw w cyberbezpieczeństwie, choć do tej pory głównie znana przy okazji pizza DDoS attack, czyli zamówieniu na czyjś adres ilości pizzy przekraczającej możliwości zjedzenia. [2]

Pokazowa egzekucja w Guild Wars 2

Twórcy wielu gier typu MMO czyli rozgrywanych przez wielu graczy w sieci nagminnie borykają się z oszustwami ze strony użytkowników. W takich przypadkach gra dla oszusta najczęściej kończy się po „zbanowaniu" przez administratorów, choć niektórych i taka kara nie odstrasza.
Gracza Guild Wars 2 pod pseudonimem DarkSide spotkało coś więcej. Twórcy gry ArenaNet postanowili pokazać, że stosowanie nieuczciwych metod w grze nie będzie tolerowane i rozprawili się z oszustem w niecodzienny sposób. Przejęli jego konto, rozebrali postać do naga i zmusili ją do popełnienie samobójstwa poprzez skok z mostu.
Całość nagrano na filmiku. Skasowano również wszystkie postacie należące do DarkSide'a i zamknięto jego konto. ArenaNet nie ujawniła jakiego typu nadużyć dopuścił się użytkownik DarkSide. Publiczne upokorzenie i egzekucja ma przestrzec innych przed nieuczciwością, choć pewnie znajdą się i tacy, którzy będą testować cierpliwość i pomysłowość twórców, powinni jednak oni pamiętać, że pomysłowość w upokarzaniu też może być duża. [3]

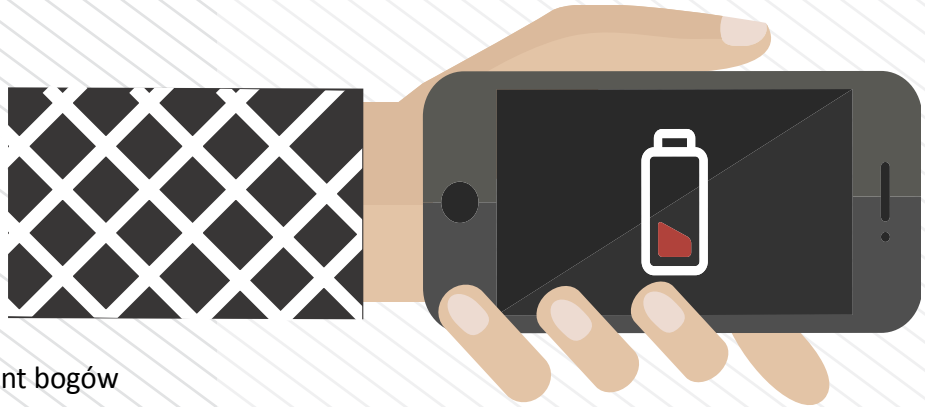
Do paki za ściąganie

Podczas gdy w Polsce na ściąganie i podpowiadanie wśród studentów jest ciągle duże przyzwolenie społeczne, to w krajach zachodnich uchodzi za haniebny występek. W Wielkiej Brytanii zapadł właśnie pierwszy wyrok za tego typu oszustwo, a media piszą ostatnio o fali takich praktyk na uczelniach wyższych.
Imran Uddin, 25-letni student ostatniego roku

Uniwersytetu Birmingham, został skazany na cztery miesiące więzienia za włamanie do uniwersyteckiego systemu komputerowego. Uddin kupił na eBayu urządzenia śledzące klawiaturę, które rejestrują uderzenia w klawisze (tzw. keylogery) i podłączył je do kilku komputerów na uczelni. W ten sposób udało mu się wykraść hasła pracowników. Po zalogowaniu do uniwersyteckiego systemu ocen „poprawił" sobie wyniki pięciu egzaminów, w tym jednego z 57% na 73%.

Sprawa wyszła na jaw w zeszłym roku w październiku, kiedy dwójka pracowników przeprowadzając rutynowy przegląd i aktualizację komputerów, odkryła podłączone z tyłu urządzenia. Sprawdzono wtedy wszystkie uniwersyteckie komputery - dodatkowo znaleziono trzy inne urządzenia. Sędzia prowadzący sprawę był bezlitosny wobec występku studenta i uznał, że cała akcja była dobrze zaplanowana. Zdecydował, że nie może wydać wyroku w zawieszeniu, gdyż chciał, aby orzeczona kara odstraszała, bo „tego rodzaju czyny podburzają lub mogą podburzyć publiczne zaufanie do systemu ocen, ustanowionego przez uniwersytet".
Na nic zdały się argumenty obrońcy, że oskarżony był jedyną osobą z rodziny, której udało się rozpocząć studia uniwersyteckie. Rzecznik Uniwersytetu Birmingham zaznaczył, że uczelnia nie komentuje indywidualnych przypadków, ale w każdym współpracuje z policją, traktując tego typu występki bardzo poważnie.
Uddin będzie miał więc przez najbliższe miesiące wystarczająco dużo czasu, aby tak przygotować się, by przy następnych egzaminach osiągnąć wyniki na poziomie 100%. Chyba, że zainstaluje kolejnego keylogera na elektronicznym zamku celi więziennej. [4]

W metrze wyłącz komórkę



Smartfony od dawna uznaje się za prezent bogów dla szpiegów. Nie bez powodów: właśnie okazało się, że posiadając komórkę przed hakerami nie da się schronić nawet pod ziemią. Najnowsze badania przeprowadzone przez naukowców z Nanjing University w Chinach pokazały, że hakerzy mogą śledzić ruch milionów pasażerów korzystających z metra na całym świecie poprzez ich telefony komórkowe. I to nawet przy braku zasięgu sieci. Wszystko dzięki danym zebranym z akcelerometru wbudowanego w urządzenie mobilne, które pozwalają na ustalenie położenia osoby. Akcelerometr to czujnik badający ruch i przyspieszenie danego obiektu. Nie jest on tak dobrze zabezpieczony jak nadajnik GPS czy modem odpowiedzialny za połączenia telefoniczne, więc ryzyko i skuteczność ataku są dużo większe. Do akceleratora można włamać się i odczytać dane bez wiedzy użytkownika. W eksperymencie przeprowadzonym z udziałem ochotników wykazano, że tego typu atak pozwala śledzić podróżnych nawet z 92% dokładnością.
To poważne zagrożenie bezpieczeństwa dla milionów ludzi korzystających codziennie z transportu publicznego. Szacuje się, że np. w Nowym Jorku z metra korzysta ponad 5,5 mln pasażerów dziennie, a ponad połowa z nich ma urządzenia mobilne. "Śledząc użytkownika smartfona przez kilka dni, atakujący może poznać jego tryb życia i rejony, w których mieszka i pracuje, a tym samym poważnie zagrozić jego bezpieczeństwu fizycznemu" - napisali badacze Jingyu Hua, Zhenyu Shen i Sheng Zhong. Jaka można chronić się przed tego typy atakami?

Paradoksalnie w bardzo prosty sposób: kluczem jest obserwacja baterii w telefonie. Śledzenie kogoś wymaga ciągłego dostępu do akcelerometra w komórce, a to powoduje wyjątkowo szybkie zużycie baterii, które powinno wzbudzić nasze podejrzenie. Neutralizacja pomiaru przyśpieszenia poprzez szybki bieg w kierunku przeciwnym do biegu pociągu raczej nie pomoże. [5]

FUNDACJA bezpieczna cyberprzestrzeń

Komputerowe szczury w ataku na kamerki

W Kanadzie policja aresztowała 27-letnią kobietę, która specjalizowała się w zdalnym przejmowaniu komputerów i szpiegowaniu ofiar przy pomocy kamerki internetowej. Jest także podejrzewana o wrzucanie na YouTube filmików instruktażowych na temat infekowania komputerów.
Policja zarekwirowała jej sprzęt w domu Saint-Alphonse-Rodriguez w prowincji Quebec. Kobieta była podobno administratorem forum dla hakerów, liczącego sobie 35 tysięcy członków z całego świata. Według policji posługiwała się malware'em, aby infekować komputery i potem przejmować kontrolę nad kamerkami. Aresztowana zarządzała serwerem command&control botnetu, czyli sieci zarażonych komputerów. Sprzęt infekowano przy pomocy narzędzia typu RAT (Remote Administration Tool), co pozwalało hakerom na przejmowanie zdalnej kontroli nad komputerami.

Następnie ofiary, w tym dzieci, były nękane, podsłuchiwano ich prywatne rozmowy, z ich komputerów logowano na strony z pornografią. Poszkodowani pochodzili z Kanady i zagranicy. Praktyka przejmowania kamerek jest coraz częstsza wśród hakerów. Narzędzie do tego typu ataków na czarnym rynku można dostać już za 100 dolarów. Tysiące internautów mogą nie wiedzieć, że ich największym wrogiem są możliwości ich własnego sprzętu. Koniec więc z naśmiewaniem się z zaklejających kamerki plastrem, bo może się skończyć znanym powiedzeniem – ten się śmieje kto się śmieje ostatni. [6]

[1] http://tinyurl.com/oy2da57
[2] http://tinyurl.com/op6b4ea
[3] http://tinyurl.com/npxxp3z
[4] http://tinyurl.com/k54jfrk
[5] http://tinyurl.com/mrbpp7p
[6] http://tinyurl.com/oaz7mja

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