Wirus może manipulować wynikami tomografii i rezonansu

9 kwietnia 2019

Izraelscy specjaliści zwracają uwagę na słabe zabezpieczenia sprzętu medycznego i sieci. Stworzony przez nich wirus tak manipulował obrazami wykonanymi za pomocą tomografii komputerowej i rezonansu magnetycznego, że pojawiały się na nich fałszywe guzy nowotworowe. Złośliwe oprogramowanie było też zdolne do usuwania z obrazów rzeczywiście istniejących guzów i nieprawidłowości. W obu przypadkach tego typu atak może mieć poważne konsekwencje dla pacjenta.

Yisroel Mirsky, Yuval Elovici i dwóch innych specjalistów z Centrum Badań nad Bezpieczeństwem Cyfrowym na Uniwersytecie Ben-Guriona mówią, że np. taki atak można np. przeprowadzić na polityka, by skłonić go do wycofania się z wyborów.

Izraelczycy dowiedli, że to, co mówią, to nie tylko teoria. Podczas testów wykorzystali swoje oprogramowanie do zmanipulowania zdjęć płuc wykonanych za pomocą tomografu. Zdjęcia dano do przeanalizowania trzem doświadczonym

radiologom. Okazało się, że diagnoza niemal zawsze była nieprawidłowa. Tam, gdzie złośliwe oprogramowanie dodało fałszywe guzy nowotworowe, radiolodzy w 99% przypadków zdiagnozowali chorobę. Tam, gdzie prawdziwe guzy nowotworowe zostały usunięte przez wirusa, radiolodzy w 94% przypadków orzekli, że pacjent jest zdrowy. Nawet wówczas, gdy radiologom powiedziano, że będą mieli do czynienia ze zmanipulowanymi obrazami i dano im do przeanalizowali kolejny zestaw zdjęć, to w przypadku tych fotografii, na których wirus dodał fałszywego guza radiolodzy w 60% zdiagnozowali chorobę, a tam, gdzie złośliwy kod guza usunął, radiolodzy w 87% przypadków stwierdzili, że pacjent jest zdrowy. Jeszcze gorzej niż ludzie poradziło sobie oprogramowanie, które jest często wykorzystywane przez radiologów do potwierdzenia diagnozy. Ono w 100% dało się oszukać fałszywym guzom.

„Byłam zaszokowana" – przyznaje Nancy Boniel, radiolog z Kanady, która brała udział w badaniach. „Poczułam się tak, jakby ktoś usunął mi grunt spod stóp. Zostałam bez narzędzia diagnostycznego."

Mirsky, Elovici i inni przeprowadzili eksperymenty ze zdjęciami płuc, jednak są pewni, że ich atak będzie też działał w przypadku guzów mózgu, chorób serca, zatorów żylnych, uszkodzeń rdzenia kręgowego, złamań kości, uszkodzeń więzadeł oraz artretyzmu.

Złośliwe oprogramowanie może losowo dodawać fałszywe guzy do wszystkich obrazów, powodując w szpitalu chaos oraz spadek zaufania personelu do sprzętu medycznego, może też wyszukiwać konkretnych pacjentów po ich nazwisku czy numerze identyfikacyjnym i dodawać fałszywe informacje tylko do ich diagnoz. To zaś oznacza, że osoba poważne chora może nie otrzymać pomocy, a osoby zdrowe zostaną poddane niepotrzebnym, ryzykownym i szkodliwym zabiegom leczniczym. Co więcej, program może też śledzić kolejne badania konkretnego pacjenta i dodawać do nich guzy, fałszywie informując o rozprzestrzenianiu się choroby, lub też pokazywać, że guzy się

zmniejszają, sugerując, iż leczenie działa. Jest ono też zdolne do manipulowania wynikami badań klinicznych, przekazując fałszywe dane na temat testowanych leków czy technik leczniczych.

Mirsky mówi, że atak jest możliwy do przeprowadzenia, gdyż szpitale nie podpisują cyfrowo skanów. Obrazy wykonane przez tomograf i rezonans są przesyłane do stacji roboczych oraz baz danych. Gdyby obrazy cyfrowo podpisywano, a transmisję szyfrowano, niezauważona zmiana obrazu byłaby niemożliwa. Jako, że nie jest to robione, osoba z dostępem do sieci szpitala może zainfekować ją szkodliwym kodem.

„Szpitale przywiązują bardzo dużą uwagę do prywatności. Ale tylko tam, gdzie dane są dzielone z innymi szpitalami czy jednostkami zewnętrznymi. Tutaj istnieją bardzo ścisłe przepisy dotyczące ochrony danych osobowych i medycznych. Jednak to, co dzieje się wewnątrz szpitala to inna historia" – stwierdza Mirsky. To, jak się okazuje, problem nie tylko Izraela. Fotios Chantzis, główny inżynier odpowiedzialny za bezpieczeństwo w amerykańskiej Mayo Clinic potwierdza, że sytuacja taka jest możliwa i że wewnętrzne sieci szpitali zwykle nie są zabezpieczone. Wiele szpitali uważa bowiem, że ich sieci są niedostępne z zewnątrz. Nawet tam, gdzie sieci wewnętrzne umożliwiają szyfrowanie, to nie jest ono używane np. ze względów na obawy o kompatybilność ze starszym, wciąż wykorzystywanym, oprogramowaniem.

Podczas przygotowywania swojego szkodliwego kodu naukowcy z Uniwersytetu Ben Guriona wykorzystali techniki maszynowego uczenia się, za pomocą których wytrenowali wirusa tak, by szybko przedostawał się do obrazów przesyłanych przez sieć szpitalną oraz by dopasowywał umieszczane przez siebie na zdjęciu fałszywe informacje do anatomii pacjenta. Dzięki temu fałszywe guzy wyglądały bardziej realistycznie. Wirus może działać w trybie całkowicie automatycznym, zatem wystarczy wpuścić go do sieci, a wykona swoją pracę bez nadzoru i oczekiwania na polecenia od napastnika.

Infekcji można dokonać albo mając dostęp do szpitalnych urządzeń i podłączając się do nich za pomocą kabla lub też wykorzystując internet. Izraelczycy odkryli bowiem, że wiele sieci szpitalnych jest albo wprost podłączonych do internetu, albo też w szpitalu istnieje urządzenie, które ma dostęp jednocześnie i do internetu i do sieci wewnętrznej szpitala.

Izraelczycy przeprowadzili nawet atak na szpital w swoim kraju. Mirsky dostał się, po godzinach pracy, na oddział radiologii i podłączył urządzenie ze złośliwym kodem do wewnętrznej sieci. Cała operacja zajęła mu zaledwie 30 sekund. Nikt go nie niepokoił, nie pytał, co tam robi. Dyrekcja szpitala wydała pozwolenie na przeprowadzenie testu, ale personel nie był o niczym poinformowany.

Mirsky mówi, że najlepszym sposobem na uniknięcie tego typu ataków byłoby szyfrowanie komunikacji wewnątrzszpitalnej i cyfrowe podpisywanie wszystkich danych, komputery powinny być tak skonfigurowane, by wszczynać alarm, gdy tylko których z obrazów nie jest odpowiednio podpisany. Jednak, jak zauważają specjaliści, nie jest to takie proste. Wielu szpitali nie stać na takie rozwiązania lub też używają starych, często 20-letnich, technologii, które nie wspierają szyfrowania i cyfrowych podpisów. „To zmiany, które wychodzą daleko poza same urządzenia i dotyczą całej infrastruktury sieci, zauważa Suzanne Schwartz z amerykańskiej FDA.”

Autorstwo: Mariusz Błoński
Na podstawie: Cyber.bgu.ac.il
Zdjęcie: jarmoluk (CC0)
Źródło: KopalniaWiedzy.pl