CIA podejrzy cię z telewizora i wyłączy smartfon

26 marca 2018

7 marca „WikiLeaks” zadała kolejny cios amerykańskim agencjom wywiadowczym i amerykańskim firmom zajmującym się zaawansowanymi technologiami, publikując bezprecedensowy duży zbiór tajnych materiałów CIA, które opisują zaawansowane technologicznie operacje szpiegowskie wywiadu USA.

Oto najbardziej skandaliczne fakty z dokumentów opublikowanych przez WikiLeaks:

1. CIA posiada duży zestaw gotowych narzędzi do hakowania urządzeń Apple i Android, a także komputerów działających w systemach Windows, macOS, a nawet Linux. Teraz użytkownicy i administratorzy nawet najegzotyczniejszych systemów operacyjnych powinni wiedzieć, że CIA od dawna ma klucze do ich systemów. Amerykańscy hakerzy mają łatwy dostęp do wszystkich danych, w tym geolokacji urządzeń, zawartości ich pamięci i informacji przekazywanych przez system audio i mikrofon.

Wisienka na torcie – CIA może zdalnie wyłączyć dowolne urządzenie lub komputer pracujący na niezabezpieczonych systemach, co skutecznie może zakłócić działanie dowolnej struktury, której działanie zależy od systemów elektronicznych. Trudno nawet sobie wyobrazić, co może się stać w newralgicznych zakładach produkcyjnych lub w dowolnym systemie energetycznym, jeśli wszystkie komputery w centrach nagle przestaną działać.

2. CIA może używać tak zwanych „inteligentnych telewizorów” (Smart TV) do podsłuchiwania i podglądania użytkowników. Wiele współczesnych telewizorów ma zarówno mikrofon, jak i małą kamerę wideo, co otwiera ogromne możliwości szpiegowskie, a także do zbierania kompromitujących materiałów audio i wideo z

drogich hoteli, a także sypialni prywatnych mieszkań. Z niewiadomych powodów panom z CIA i ich brytyjskim kolegom z MI- 5 szczególnie spodobały się telewizory Samsung. Nawiasem mówiąc, wyłączenie takiego telewizora nie ma sensu – jego mikrofon podsłuchowy i tak działa.

3. Narzędzia do hakowania różnych systemów informatycznych swobodnie krążą w amerykańskiej społeczności wywiadowczej, a nawet przekazywane są pewnym podwykonawcom, czyli najprawdopodobniej prywatnym firmom, które wykonują konkretne zamówienia dla CIA. W jednej z takich prywatnych firm obsługującej NSA, pracował Edward Snowden.

Oznacza to, że szanse na wyciek tej bardzo niebezpiecznej cyber-broni są bardzo wysokie. Strach pomyśleć, co z takim arsenałem mogłaby zrobić jakaś organizacja terrorystyczna, która włamałaby się do systemów komputerowych jakiejś elektrowni jądrowej.

Dokumenty opisujące narzędzia CIA do włamań, wyciekły do WikiLeaks właśnie taką drogą, od nieznanego pracownika z prywatnej firmy, który z nimi współpracował. Oznacza to, że dokładnie taka sama broń cybernetyczna może trafić do każdego. Jest to realne zagrożenie dla wszystkich krajów świata, które nawet odrobinę ustąpią pod groźbami takimi jak rozprzestrzenianie broni jądrowej lub biologicznej.

4. Szczególny niepokój budzi program CIA do hakowania systemów wbudowanych w nowoczesne samochody i sprzęt medyczny. Mając dostęp do zautomatyzowanych systemów kontroli nowoczesnego samochodu lub elektronicznego systemu podtrzymywania życia w szpitalu, CIA może dokonywać zabójstw politycznych, których nie będzie można odróżnić od wypadku.

5. Ukochane dodatki polityków, urzędników i dziennikarzy, takie jak Telegram i Whatsapp, które do tej pory posiadały reputację bezpiecznych w dziedzinie prywatności i szyfrowania, okazały się całkowicie bezbronne z amerykańskimi szpiegami. To

proste – po co włamywać się do samej aplikacji lub zaszyfrowanej wiadomości, jeżeli można włamać się do systemu operacyjnego, na którym pracuje Telegram lub Whatsapp? Z dużym prawdopodobieństwem można stwierdzić, że wiadomość jest przechwytywana zanim aplikacja ma czas aby ją zaszyfrować, czyli wszystkie środki bezpieczeństwa podjęte przez twórców tych aplikacji nie mają sensu.

Najbardziej logiczny wniosek, który powinni wyciągnąć wszyscy użytkownicy podobnych aplikacji jest taki, że nie mają oni żadnej prywatności..

6. CIA walczy z firmami antywirusowymi, które uniemożliwiają im pracę. Nie ma jeszcze szczegółów tego działania, ale możemy się spodziewać, że zostaną one ujawnione w przyszłości.

7. CIA często stara się pozostawić w miejscu włamania fałszywe ślady, które wskazują, że włamania dokonali… uwaga… rosyjscy hakerzy. Tak, ci sami legendarni hakerzy z Rosji, na których zwalono porażkę Hillary Clinton w wyborach.

WikiLeaks obiecuje kontynuację publikowania tajnych dokumentów i podkreśla, że to nie wszystko. Ale pierwsze polityczne następstwa tych publikacji już są.

Chiny wyraziły zaniepokojenie działaniami CIA, zwłaszcza że amerykańscy politycy często oskarżają chińską stronę o rozpętanie cyberwojny przeciwko USA. Teraz Pekin może spokojnie odpowiedzieć na wszystkie twierdzenia, że □□to amerykańskie służby specjalnie maczały w tym palce. Na razie nie jest jasne jak będą się tłumaczyli amerykańscy dyplomaci.

Według WikiLeaks niemiecka prokuratura zainteresowała się wykorzystaniem co najmniej jednego amerykańskiego przedstawicielstwa dyplomatycznego w Niemczech jako twierdzy amerykańskich hakerów, którzy szpiegowali niemieckich obywateli. Skandal może stać się bardziej znany i rozkręcić wraz z niemiecką kampanią wyborczą, która może wpłynąć na wyniki wyborów.

Reuters donosi, że amerykańscy specjaliści od cyberbezpieczeństwa byli w stanie zidentyfikować jeden z wirusów opisanych w materiale WikiLeaks. Przed skandaliczną publikacją wierzono, że wirus ten został uruchomiony przez rosyjskich lub chińskich hakerów, ale okazuje się, że jest to wirus CIA.

Nasuwa się pytanie: jak powinniśmy zareagować na to wszystko, jak powinno państwo i społeczeństwo zareagować?

Musimy rozwijać własną branżę IT tak aktywnie jak to tylko możliwe, i nie słuchać rozmów o nieuchronnym technologicznym zacofaniu Rosji. Nie trzeba też pisać dowcipów o specjalnej rosyjskiej drodze i marnowaniu pieniędzy na rozwój rosyjskich aplikacji, systemów operacyjnych czy sprzętu. Musimy maksymalnie skomplikować zadanie dla naszych geopolitycznych przeciwników. Czemu nie opracować swoich technologii.

Nawiasem mówiąc, WikiLeaks opublikował te dokumenty w samą porę. Donald Trump potrzebuje argumentów do odparcia oskarżeń o mitycznych rosyjskich hakerów, którzy pomogli mu wygrać wybory. Teraz ma bardzo mocne argumenty, które trudno będzie odrzucić.

I na koniec. Pomimo, że news dosłownie wysadził amerykańskie infopole, kanał CNN ignorował go tak uparcie, że w sieciach społecznościowych nawet zaczęto żartować na ten temat. Jak pokazuje praktyka, we współczesnym świecie to już nie działa, Internet jeszcze nie pokonał telewizji, ale nigdy już nie będzie można go zignorować.

Autorstwo: Rusłan Ostaszko
Na podstawie: WikiLeaks.org
Źródło oryginalne: LiveJournal.com
Źródło polskie: Treborok.wordpress.com