Rootkit w notebookach Lenovo

14 sierpnia 2015

Jeden z użytkowników notebooka Lenovo odkrył, że jego producent zainstalował w nim rootkita. Zadaniem ukrytego kodu jest upewnienie się, że na notebooku zawsze będzie zainstalowane dodatkowe oprogramowanie Lenovo. Nawet jeśli wyczyścimy komputer i przeinstalujemy Windows, rootkit pobierze i zainstaluje oprogramowanie Lenovo.

Lenovo wyjaśnia, że program Lenovo Service Engine pobiera program o nazwie OneKey Optimizer, który jest „potężnym narzędziem przyszłej generacji optymalizującym system". Jego zadaniem jest aktualizacja firmware'u, sterowników oraz preinstalowanych aplikacji. OneKey Optimizer kontaktuje się z serwerami Lenovo, ale, jak zapewnia firma, nie wysyła żadnych danych pozwalających na zidentyfikowanie użytkownika.

Lenovo mogło zainstalować rootkita, gdyż Microsoft pozwala producentom komputerów na załadowanie do BIOS-u pliku EXE podczas startu systemu. Odpowiada za to technologia o nazwie Windows Platform Binary Table (WPBT), która uruchamia taki plik przed zalogowaniem się użytkownika do systemu. WPBT nie można wyłączyć. Głównym celem WPBT jest automatyczna instalacja oprogramowania zabezpieczającego przed kradzieżą. Może ono np. kontaktować się co jakiś czas z odpowiednim serwerem i sprawdzać, czy zgłoszono kradzież komputera. Jeśli tak, zostanie on trwale unieruchomiony. Lenovo korzysta z tej technologii w komputerach z Windows 8. W maszynach z Windows 7 firma nadpisuje plik autochk.exe i w ten sposób pobiera aktualizacje.

Jakby tego było mało, okazało się, że Lenovo Service Engine zawierało dziurę pozwalającą cyberprzestępcom na zainstalowanie szkodliwego kodu na komputerze ofiary. Lenovo opublikowało poprawkę, jednak trzeba zainstalować ją ręcznie, co oznacza, że prawdopodobnie większość użytkowników jest

nadal narażonych na atak.

Użytkownicy mogą sprawdzić, czy w ich notebooku znajduje się rootkit Lenovo. W przypadku maszyn z systemami Windows 8/8.1/10 należy w logowaniu zdarzeń sprawdzić wpis dla „Microsoft-Windows-Subsys-SMSS” i jeśli znajduje się tam wpis: „A platform binary was successfully executed”, mamy rootkita. Alternatywnie możemy zajrzeć do katalogu c:windowssystem32. Jeśli w maszynie zainstalowano rootkita, w katalogu będzie plik wpbbin.exe. Użytkownicy Windows 7 mogą zaś zalogować się jako administrator z sesją konsoli i w linii poleceń wpisać sfc /VERIFYFILE=c:windowssystem32autochk.exe. Jeśli wystąpi błąd i/lub data nie zgadza się z datą instalacji systemu, rootkit jest obecny. Alternatywnie można użyć komendy /sfc /VERIFYONLY i dalej postępować według instrukcji.

Autorstwo: Mariusz Błoński
Na podstawie: myce.com
Źródło: KopalniaWiedzy.pl