Apple na celowniku CIA

24 marca 2017
Serwis „Wikileaks” ujawnił kolejne tajemnice CIA. Tym razem dowiadujemy się, że Agencja przygotowała oprogramowanie atakujące nowo wyprodukowane iPhone’y oraz że co najmniej od 2008 roku infekuje łańcuch dostaw telefonów Apple’a.

Z ujawnionych dokumentów dowiadujemy się, że pracująca w ramach CIA komórka o nazwie Embedded Development Branch przygotowała wiele rodzajów kodu atakującego UEFI komputerów Mac. Jest wśród nich projekt o nazwie „Sonic Screwdriver” w ramach którego opracowano „mechanizm wykonywania kodu na urządzeniach peryferyjnych podczas startu komputera Mac”. Pozwalał on na wystartowanie szkodliwego kodu np. z klipsu USB. Mechanizm infekujący urządzenia peryferyjne znajdował się w zmodyfikowanym przez CIA firmware’u przejściówki pomiędzy złączami Thunderbolt i Ethernet.

Z kolei „DarkSeaSkies” to kod rezydujący w EFI MacBooka Air. Składa się on z modułów „DarkMatter”, „SeaPea” oraz „NightSkies” działających, odpowiednio, na poziomie EFI, jądra i użytkownika. Wykradziona CIA dokumentacja mówi również o wielu innych projektach, w ramach których powstał kod atakujący urządzenia Apple’a.

Dowiadujemy się również, że o ile czasem na zlecenie CIA dokonywane są bezpośrednie ataki na urządzenia, które są w posiadaniu interesujących Agencję osób, to częściej zdarzają się ataki w łańcuchu dostaw. Urządzenia takie są infekowane przez osoby, które mają do nich wówczas dostęp.

Autorstwo: Mariusz Błoński
Na podstawie: DV Hardware
Źródło: KopalniaWiedzy.pl