**Naukowcy wykorzystują anomalie poboru mocy do wykrywania złośliwego oprogramowania w urządzeniach IoT**

**Uniwersytet Stanowy Karoliny Północnej oraz Uniwersytet Teksasu w Austin opublikowały razem dowód słuszności koncepcji (PoC) wykorzystania fluktuacji pobieranej mocy jako podstawy mechanizmu wykrywania szkodliwego oprogramowania w systemach wbudowanych.**

Według współautora dokumentu, Aydina Aysu, ataki złośliwym oprogramowaniem, zaprojektowanym specjalnie pod kątem architektury narażonego systemu, umożliwiają przejęcie kontroli nad systemem wbudowanym, łącznie z dostępem do jego danych.

„Systemy wbudowane to – w zasadzie – wszystkie komputery, które nie mają fizycznej klawiatury, od smartfonów po urządzenia internetu rzeczy” – mówi Aysu. „Systemy wbudowane stosowane są we wszystkich, aktywowanych głosem, asystentach wirtualnych obecnych w naszych domach, jak również w przemysłowych systemach sterowania, takich jakie pracują w elektrowniach. A atakujące te systemy złośliwe oprogramowanie może zostać wykorzystane do przejęcia nad nimi kontroli lub do kradzieży danych”.

Te wymierzone w mikrosystemy ataki są trudne do zauważenia, jednak autorzy PoC sądzą, że znaleźli na to sposób. Anomalie w poborze mocy pozwolą na ich wykrywanie i lokalizację z dużą dokładnością. Aysu wyjaśnia:

„Dobrze wiemy, jak wygląda zużycie energii, gdy systemy wbudowane działają normalnie. Znajdując anomalie w poborze mocy, możemy stwierdzić, że w systemie działa złośliwe oprogramowanie – nawet jeżeli nie możemy zidentyfikować tego złośliwego oprogramowania bezpośrednio”.

Na razie jest to tylko PoC, a zaproponowane rozwiązanie ma swoje ograniczenia. Po pierwsze, wymaga wprowadzenia nowej technologii w „inteligentnych” źródłach zasilania, współpracujących z systemami wbudowanymi. Innymi słowy, wymaga nowego standardu branżowego, którego wdrożenie zajmuje zwykle lata. Po drugie, nowa technika detekcji opiera się na monitorowaniu pobieranej przez systemy wbudowane mocy, co wymaga w większości przypadków zaplecza laboratoryjnego. Po trzecie, autorzy jako pierwsi przyznają, że „działające na zasadzie monitorowania poboru mocy urządzenie wykrywające może zostać oszukane, jeśli złośliwe oprogramowanie będzie modyfikować swoją aktywność tak, by odpowiadała wzorcom «normalnego» zużycia energii”.

„Ustaliliśmy, że koszt obliczeniowy wymagany do naśladowania normalnego zużycia energii i unikania detekcji zmusi złośliwe oprogramowanie do spowolnienia transferu danych w granicach 86-97%. Krótko mówiąc, zaproponowane przez nas podejście może znacznie ograniczyć skuteczność złośliwego oprogramowania, nawet w tych nielicznych przypadkach, gdy nie zostanie ono wykryte” – mówi Aysu.

- *Przedstawiona koncepcja to z pewnością interesujące nowe podejście do problemów związanych z bezpieczeństwem systemów wbudowanych, ale jej ograniczenia zdają się poddawać w wątpliwość praktyczność takiego rozwiązania. Na razie najlepszym sposobem zabezpieczenia, podłączonych do internetu systemów wbudowanych, pozostaje stosowanie tych dopracowanych już rozwiązań, których skuteczność została wcześniej udokumentowana* - **wyjaśnia Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken Systemy Antywirusowe** (www.bitdefender.pl).