

Złośliwe oprogramowanie sieci BADBOX

Zakup taniego **urządzenia z Androidem** może być kosztownym błędem, zwłaszcza jeżeli jest zainfekowane wirusami już w momencie wyjęcia nowego urządzenia z pudełka. Analitycy cyberbezpieczeństwa uważają, że co najmniej 74 tys. urządzeń z Androidem tj. telefonów komórkowych, tabletów, urządzeń Connected TV itp. mogło zostać zainfekowanych preinstalowanym złośliwym oprogramowaniem, jako część sieci BADBOX, **które zostało załadowane na etapie produkcji**. Mamy w tym przypadku do czynienia ze skompromitowanym łańcuchem dostaw sprzętu.

Takie właśnie produkty zawierające złośliwy backdoor zostały znalezione w sieciach szkół publicznych w całych Stanach Zjednoczonych. **Zespół analityków z Human Security zidentyfikował łańcuch dostaw chińskiego producenta, który został naruszony w celu włamania się do oprogramowania kilku produktów dostarczanych do sprzedawców, fizycznych sklepów detalicznych i magazynów ecommerce.**

Backdoor oprogramowania układowego był oparty na złośliwym oprogramowaniu Triada, które było znajdowane na przestrzeni lat w tanich smartfonach z Androidem.

„Niestety, urządzenia zainfekowane BADBOX są nie do naprawienia przez przeciętnego użytkownika. Ponieważ złośliwe oprogramowanie znajduje się na partycji tylko do odczytu (ROM) oprogramowania układowego urządzenia, przeciętny użytkownik nie będzie w stanie usunąć BADBOX ze swojego produktu.”

Nie tylko tanie urządzenia mogą być źródłem problemów. **Podatności i błędy w systemie wykrywane są również regularnie w sprzęcie dużych dostawców takich jak Samsung, czy Apple.**

Rekomendacje!!!

- Użytkownicy powinni pamiętać o regularnych aktualizacjach sprzętu. Zawierają one ważne poprawki błędów i zapobiegają wykorzystaniu znanych podatności w systemach.
- Przy zakupie sprzętu wybieraj marki, które istnieją od dłuższego czasu i są aktywnie sprzedawane w wielu krajach.
- Jeśli masz okazję zobaczyć urządzenie w sklepie, zrób to. Tam przejdź do ustawień i sprawdź, czy istnieje opcja instalacji aktualizacji. Sprawdź też jaką wersję systemu ma zainstalowany telefon.
- Wszystko poniżej wersji 12 w przypadku Androida można uznać za przestarzałe.
- Przeczytaj opinie kupujących na specjalistycznych forach - nie na platformach handlowych lub stronach internetowych sklepów.
- Natychmiast po zakupie urządzenia zapoznaj się z jego ustawieniami, zaktualizuj oprogramowanie do najnowszej wersji, a następnie odinstaluj lub wyłącz za pomocą ustawień wszystkie aplikacje, które wydają się zbędne.

Źródło: Biuletyn informacyjny „Zagrożenia w cyberprzestrzeni 10/2023”, który został opracowany przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji