Wzrost popularności urządzeń Internetu rzeczy otwiera przestępcom kolejną furtkę do Twoich wrażliwych danych

Urządzenia internetu rzeczy (IoT) coraz śmielej wkraczają w nasze codzienne życie. Wg raportu firmy analityczno-konsultingowej Ovum, w 2021 roku średnia liczba urządzeń IoT przypadająca na gospodarstwo domowe osiągnie wartość 8,7.

Analitycy ds. bezpieczeństwa sieciowego ostrzegają przed atakami sieciowymi typu przechwycenie sesji (hijacking attacks) z wykorzystaniem urządzeń IoT znajdujących się w obrębie tej samej sieci domowej. Ten rodzaj ataku polega na nielegalnym dostępie do sesji użytkownika i przejęciu nad nią kontroli. Po wpisaniu poświadczeń i zainicjowaniu sesji przez logującą się do serwera ofiarę , atakujący ma możliwość podania się za którąkolwiek ze stron i wysyłania dowolnych informacji. Dzięki temu haker zyskuje możliwość wykonania na serwerze poleceń z uprawnieniami zalogowanego klienta.

Aby przechwycić sesję atakujący musi znajdować się na drodze pomiędzy klientem i serwerem. W tym celu wykorzystywane są znajdujące się w obrębie tej samej sieci LAN (w jednej domenie kolizyjnej) słabo zabezpieczone urządzenia IoT. Po przejęciu kontroli nad IoT, atakujący widzi wszystkie pakiety wysyłane przez serwer i użytkownika.

Przechwycone pakiety, zawierające poświadczenia (najczęściej w formie zaszyfrowanej) są następnie łamane lub sprzedawane posiadającym niezbędną wiedzę i narzędzia deszyfrujące podmiotom trzecim. W ten sposób loginy i hasła dostają się w ręce przestępców.

Zdobyte tą drogą poświadczenia zestawia się w listy zawierające często miliony rekordów. Następnie, specjalnie spreparowane w tym celu skrypty, automatycznie skanują tysiące usług online sprawdzając, czy można się do nich zalogować na podstawie wykradzionych haseł. Według statystyk, skuteczność pozyskania nieautoryzowanego dostępu do usług z wykorzystaniem przedstawionej techniki wynosi 5%.

Proces automatycznego testowania milionów haseł, w setkach tysięcy usług, wymaga gigantycznych zasobów. W tym celu ponownie wykorzystywane są słabo zabezpieczone urządzenia IoT (w przeciwieństwie do tradycyjnych komputerów dostępne 24 godziny na dobę przez 7 dni w tygodniu), z których tworzone są botnety, czyli sieci będących pod kontrolą przestępców urządzeń zombie, realizujących zlecone przez nich zadania.

Specjaliści z Bitdefender zalecają, by przestrzegać stosowania unikalnego hasła dostępu do każdej usługi. Hasła powinny zawierać możliwie dużą liczbę znaków. Im krótsze hasło, tym łatwiej je złamać z wykorzystaniem przechwyconych techniką Hijacking pakietów. Zaleca się również uwierzytelnianie dwuetapowe, które skutecznie chroni przez większością ataków.