**Domowe żarówki źródłem potencjalnych podsłuchów i ataków na nasze komputery**

**Inteligentne żarówki w lampach naszych domów mogą mieć nieszczelne sterowniki, pozwalające hakerom na włamanie się do naszych sieci domowych – dowodzą analitycy firmy Check Point Research. Luki w oprogramowaniu smart żarówek Philips Hue, pozwalają na dostęp do sieci przy użyciu zdalnego kodu typu exploit.**

Podczas konferencji CPX w Wiedniu badacze firmy Check Point pokazali, jak osoby atakujące mogłyby wykorzystać sieć IoT do zainicjowania ataków na konwencjonalne sieci komputerowe w domach i firmach, a nawet w inteligentnych miastach. Wykorzystując podatności najpopularniejszych na rynku żarówek uzyskali dostęp do sieci przy użyciu kodu exploit w protokole transmisji danych w sieciach bezprzewodowych [ZigBee](https://en.wikipedia.org/wiki/ZigBee). Protokół ten charakteryzuje się małym poborem energii i jest używany do sterowania różnymi urządzeniami w domu - IoT**.**

W opublikowanej już jakiś czas temu [analizie](https://eyalro.net/publication/rosw17.html) zabezpieczeń inteligentnych żarówek sterowanych przy użyciu protokołu ZigBee badacze poinformowali, że udało im się przejąć kontrolę nad żarówką Hue w sieci, zainstalować w niej złośliwe oprogramowanie układowe i rozsyłać je do sąsiednich sieci żarówek.

Korzystając z zachowanej luki, badacze postanowili pójść o krok dalej: użyli żarówki Hue jako platformy służącej do przejęcia kontroli nad mostkiem sterującym żarówek, a ostatecznie do zaatakowania docelowej sieci komputerowej, np. za pomocą oprogramowania wymuszającego okup lub szpiegujące ofiarę. Należy zauważyć, że nowsze generacje układów stosowanych w żarówkach Hue nie mają omawianej luki.

*- Wielu z nas ma świadomość, że urządzenia IoT mogą wywołać ryzyko naruszenia bezpieczeństwa. To badanie pokazuje jednak, w jaki sposób nawet tak zwyczajne, pozornie „nieme” urządzenia jak żarówki mogą zostać wykorzystane przez hakerów do przejęcia kontroli nad sieciami lub rozsyłania złośliwego oprogramowania* – powiedział Yaniv Balmas, dyrektor ds. badań w dziedzinie bezpieczeństwa cybernetycznego w firmie Check Point Research.

*- Bardzo ważne jest, aby organizacje i osoby indywidualne zabezpieczyły się przed tego rodzaju atakami, aktualizując posiadane urządzenia w oparciu o najnowsze poprawki oraz oddzielając te urządzenia od innych komputerów w sieciach w celu ograniczenia ewentualnego rozprzestrzeniania się złośliwego oprogramowania. Wobec złożoności współczesnych ataków piątej generacji nie stać nas na zaniedbanie zabezpieczeń jakichkolwiek elementów połączonych z naszymi sieciami.*

Badanie przeprowadzone przy udziale organizacji [Check Point Institute for Information Security (CPIIS)](http://cpiis.cs.tau.ac.il/) we współpracy z Uniwersytetem w Tel Awiwie ujawniono już wcześniej, w listopadzie 2019 roku, firmom Philips i Signify (właścicielom marki Philips Hue). Firmy potwierdziły istnienie luki w swoim produkcie i opublikowała poprawioną wersję oprogramowania układowego (Firmware 1935144040), dostępną obecnie w ramach automatycznej aktualizacji. Zalecamy użytkownikom dopilnowanie, aby posiadany produkt otrzymał automatyczną aktualizację tej wersji oprogramowania układowego.

*- Czujemy się zobowiązani do ochrony prywatności naszych użytkowników oraz podjęcia wszelkich działań, dzięki którym nasze produkty będą bezpieczne. Jesteśmy wdzięczni za odpowiedzialne ujawnienie informacji i współpracę ze strony firmy Check Point. Umożliwiło nam to opracowanie i wdrożenie koniecznych poprawek mających zapobiec narażeniu konsumentów na ryzyko* – powiedział George Yianni, dyrektor ds. technologii marki Philips Hue.

**Jak wygląda scenariusz potencjalnego ataku?**

1. Haker steruje barwą i jasnością żarówki w taki sposób, aby użytkownicy sądzili, że uległa ona usterce. W aplikacji sterującej użytkowników żarówka ma status „Niedostępna”, więc będą próbowali ją zresetować.

2. Jedynym sposobem zresetowania żarówki jest usunięcie jej z aplikacji, a następnie wydanie polecenia dla mostku sterującego, aby ten ponownie ją wykrył.

3. Mostek wykrywa feralną żarówkę, a użytkownik ponownie dodaje ją do swojej sieci.

4. Wtedy kontrolowana przez hakera żarówka ze zaktualizowanym oprogramowaniem układowym wykorzystuje luki w protokole ZigBee, aby zainicjować oparte na stosie przepełnienie bufora w mostku sterującym. W tym celu wysyła ona do mostka dużą ilość danych. Dzięki tym danym haker może również zainstalować złośliwe oprogramowanie w mostku, który z kolei połączony jest z docelową siecią firmową lub domową.

5. Złośliwe oprogramowanie łączy się z hakerem, a ten przy użyciu znanego kodu typu exploit (np. [EternalBlue](https://en.wikipedia.org/wiki/EternalBlue)) może uzyskać dostęp do docelowej sieci IP z poziomu mostka i rozsyłać oprogramowanie wymuszające okup lub szpiegujące.

Oto [film demonstrujący](https://youtu.be/4CWU0DA__bY) sposób przeprowadzenia ataku. Pełny techniczny opis badania zostanie opublikowany w późniejszym terminie, co ma zapewnić użytkownikom czas na skuteczne wprowadzenie poprawek w posiadanych wrażliwych urządzeniach.