Rubber Ducky

Jakub Chuchla, Olaf Sujata, Łukasz Czerwiec, Małgorzata Andrasz

May 2023

1 Wstęp

Projekt Rubber Ducky ma na celu poznanie sposobu komunikacji z urządzeniami peryferyjnymi. Przygotowaliśmy urządzenie z oprogramowaniem emulującym wciśnięcia klawiszy klawiatury po podłaczeniu do komputera przez USB. Zasada działania jest analogiczna do urządzenia Rubber Ducky.

Rubber to z pozoru przypominające pendrive urządzenie zaliczane jest do kategorii tzw. bad USB, czyli narzędzi, które są nam w stanie wyrządzić jakąś szkodę po podłączeniu do portu USB komputera

2 Opis działania

Rubber Ducky, chociaż wygląda jak pamięć flash, w rzeczywistości jest wykrywany przez system operacyjny jako urządzenie HID (Human Interface Device), a konkretnie klawiatura. Po podłączeniu do komputera zaczyna wysyłać zaprogramowane wcześniej ciągi znaków, poleceń i skrótów klawiaturowych. Efekt jest zatem taki, jakby osoba, która podłącza urządzenie do swojego komputera pozwoliła intruzowi skorzystać z własnej klawiatury.

3 Zagrożenia

Rubber Ducky niesie ze sobą wiele różnych zagrożeń, tutaj wymienimy kilka z nich:

- pozwala stworzyć fałszywe okno logowania do Windowsa wykradając w ten sposób dane logowania lub przesłać wszystkie hasła przeglądarki Chrome na serwer hackera.
- dzisiejsze Rubber Ducky pozwalają nawet na sprawdzenie do jakiego komputera został podłączony hakerski pendrive (PC czy Mac) i dopiero wtedy wykonanie dostosowanych do danego sprzętu poleceń, ponadto USB Rubber Ducky może teraz kodować dane w formacie binarnym i przesyłać je wykorzystując sygnały zapalające na klawiaturze lampkę od caps locka

- Kradzież danych logowania: Rubber Ducky może skopiować lub przechwycić wprowadzane dane logowania, takie jak nazwy użytkowników i hasła, które następnie mogą być wykorzystane przez atakującego do uzyskania nieautoryzowanego dostępu do kont i systemów.
- Wstrzykiwanie złośliwego kodu: Atakujący może użyć Rubber Ducky do wstrzykiwania złośliwego kodu lub skryptów na zainfekowanym komputerze. Może to prowadzić do instalacji szkodliwego oprogramowania, takiego jak wirusy, trojany czy keyloggery, które mogą kontrolować system lub kraść dane.
- Wykonanie zautomatyzowanych działań: Rubber Ducky może wykorzystać skrypty do wykonywania automatycznych działań, takich jak uruchamianie szkodliwego oprogramowania, przechwytywanie obrazów ekranu, zmiana ustawień systemowych lub przeglądarki, co może prowadzić do utraty prywatności, naruszenia bezpieczeństwa lub poważnych szkód dla użytkownika.
- Przejęcie sesji lub zdalne sterowanie: Atakujący może wykorzystać Rubber Ducky do przejęcia sesji użytkownika lub zdalnego sterowania komputerem, co pozwala im na monitorowanie działań, kradzież danych lub kontrolę nad systemem.
- Wprowadzanie zmian w systemie: Rubber Ducky może zmieniać ustawienia systemowe, takie jak firewall, antywirusy czy aktualizacje, aby umożliwić łatwiejsze wdrożenie złośliwego oprogramowania lub uniknąć wykrycia przez zabezpieczenia.
- Atak fizyczny na infrastrukturę: Rubber Ducky może być wykorzystany do przeprowadzenia ataków fizycznych na infrastrukturę, takie jak wstrzykiwanie złośliwego kodu w systemy sterowania przemysłowego, bankomaty lub urządzenia IoT.

4 Działania prewencyjne

Jak możemy bronić nasz komputer przed takim atakiem:

- świadomość i edukacja: dowiedz się więcej o atakach "Rubber Ducky". Wiedza na temat zagrożeń i podstawowych zasad bezpieczeństwa cyfrowego pomoże Ci lepiej rozpoznawać potencjalne zagrożenia i unikać ich.
- przede wszystkim nie możemy pozwolić na podłączenie pendriva nieznanego pochodzenia do naszego urządzenia, nie zostawiaj nigdy swojego komputera bez opieki w publicznym miejscu
- zaktualizowane oprogramowanie: Regularnie aktualizuj oprogramowanie na swoim komputerze, w tym system operacyjny, przeglądarkę internetową i inne aplikacje. Aktualizacje często zawierają łatki bezpieczeństwa, które chronią przed znanymi lukami w zabezpieczeniach,

- Programy antywirusowe i antymalware: Zainstaluj i regularnie aktualizuj programy antywirusowe i antymalware na swoim komputerze. Skanuj system w poszukiwaniu potencjalnych zagrożeń, a także uważaj na ostrzeżenia i blokady, które mogą wskazywać na potencjalne złośliwe oprogramowanie.
- Firewall: Włącz firewall (zaporę sieciową) na swoim komputerze, aby kontrolować ruch sieciowy i blokować podejrzane połączenia.
- Wyłączanie automatycznego uruchamiania: Zablokuj automatyczne uruchamianie skryptów lub programów z urządzeń zewnętrznych, takich jak pendrive'y. Możesz to zrobić, dostosowując ustawienia urządzenia lub oprogramowania do zarządzania urządzeniami pamięci masowej.
- Monitorowanie aktywności USB: Jeśli jesteś zaniepokojony możliwością ataku "Rubber Ducky", możesz skorzystać z narzędzi monitorujących aktywność na porcie USB, takich jak USBGuard, aby wykryć i zablokować podejrzane działania.

Trzeba pamiętać, że żadna metoda nie jest w pełni skuteczna i niezawodna. Dlatego warto stosować kombinację różnych środków ostrożności i zasad bezpieczeństwa cyfrowego, aby jak najlepiej chronić się przed różnymi rodzajami ataków, w tym atakiem "Rubber Ducky".

5 Cel projektu

Zdecydowaliśmy się na wybranie tego tematu projektu, żeby móc lepiej zrozumieć działanie i możliwości tego niebezpiecznego, ale bardzo ciekawego narzędzia. Przede wszystkim pomogło nam to zwiększyć świadomość dotyczącą bezpieczeństwa. Mamy nadzieję, że wiedza o działaniu Rubber Ducky może nam w przyszłości pomóc w ochronie przed tego typu atakami. Kolejnym powodem naszego wyboru tego tematu jest fakt, że przy projektowaniu Rubber Ducky pracujemy z mikrokontrolerem. Dodatkowa wiedza z tym związana jest dla nas bardzo przydatna, ponieważ na naszych studiach pracujemy z mikrokontrolerami również na innych zajęciach, więc szlifowanie umiejętności z tego zakresu jest dla nas niezwykle przydatne.

Literatura

[1] https://opensecurity.pl/arsenal-ethical-hackera-rubber-ducky/

[2] https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/falszywy-hakerski-pendrive-stal-sie-jeszcze-grozniejszy-jest-jeden-sposob-zeby-sie/7l4v3re

[3] https://chat.openai.com/