Cyberbezpieczeństwo

Projekt

Mikołaj Jonkis, Filip Krzemień, Andrzej Manderla, Mikołaj Mrózek

Wydział Matematyki Stosowanej
Politechnika Śląska

10 stycznia 2025

Spis treści

Definicja

Keylogger to rodzaj oprogramowania lub urządzenia, którego celem jest rejestrowanie i zapisywanie naciśnięć klawiszy na klawiaturze komputera lub innego urządzenia. Zbierane dane mogą obejmować wprowadzane hasła, numery kart kredytowych, wiadomości, e-maile, czy inne wrażliwe informacje. Keyloggery mogą działać w tle, bez wiedzy użytkownika, i przesyłać zebrane dane do cyberprzestępców lub innych nieautoryzowanych osób.

Rodzaje

- **Programowe:** Aplikacje, które działają na komputerze, przechwytując dane z klawiatury i zapisując je w pliku lub przesyłając w sieć.
- **Sprzętowe:** Urządzenia, które fizycznie łączą się z komputerem (np. jako adapter USB lub urządzenie między klawiaturą a komputerem), przechwytując naciśnięcia klawiszy.

Program

Aplikacja keyloggera została zaimplementowana w języku Python. Działa w tle, przechwytując naciśnięcia klawiszy i zapisując je do pliku tekstowego. W regularnych odstępach czasu plik z zapisanymi klawiszami jest przesyłany na konto Dropbox.

Sprzęt

Sprzętowy keylogger wykorzystuje Arduino Nano i pamięć EEPROM do przechowywania naciśnięć klawiszy przesyłanych przez port szeregowy. Po odebraniu znaku zapisywany jest on w pamięci EEPROM. Na żądanie (np. poprzez wysłanie znaku #) zawartość pamięci jest wyświetlana na monitorze szeregowym.

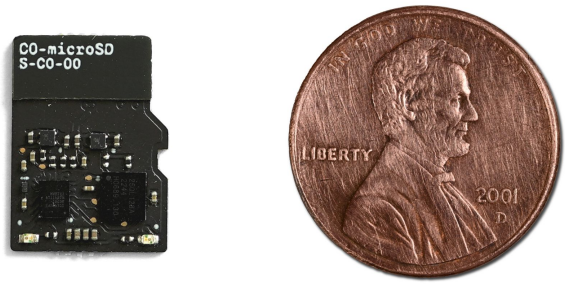
Inne przykłady

Keyloggery nie ograniczają się jedynie do prostych aplikacji i urządzeń. W praktyce ich implementacja może być znacznie bardziej zaawansowana:

- Wstrzykiwanie fragmentów kodu do popularnych aplikacji codziennego użytku.
- Wysyłanie skryptów instalujących keyloggera na urządzenia docelowe.
- Wykorzystanie mikrokontrolery wielkości kart microSD, które działają jako urządzenia HID, rejestrując i przesyłając dane na inne urządzenia w sieci.

Rozwój technologii sprawia, że keyloggery stają się coraz trudniejsze do wykrycia, co podkreśla potrzebę edukacji i odpowiednich narzędzi ochrony.

Signaloid C0 microsd



Rysunek: [Signaloid-C0-microsd]

USB Rubber Ducky

Rysunek: [USB Rubber Duck]

Czego dowiedzieliśmy się z projektu

Czego dowiedzieliśmy się z projektu

- Łatwość tworzenia keyloggerów
- Zróżnicowanie metod ataków
- Zwiększające się zagrożenia

Jak chronić się przed keyloggerami

- Oprogramowanie antywirusowe: Używanie zaufanych programów antywirusowych, które skanują komputer w poszukiwaniu podejrzanych aplikacji
- Regularne aktualizowanie systemów operacyjnych i aplikacji: Wiele keyloggerów wykorzystuje luki w systemach operacyjnych i oprogramowaniu.
- Używanie silnych haseł oraz dwuskładnikowej autoryzacji
- Sprzętowe tokeny bezpieczeństwa: Używanie urządzeń takich jak tokeny USB czy czytniki linii papilarnych, które weryfikują użytkownika na poziomie sprzętowym, może chronić przed keyloggerami sprzętowymi.
- Monitorowanie aktywności systemu
- Edukacja i świadomość użytkowników: Edukowanie użytkowników na temat zagrożeń związanych z keyloggerami i zachęcanie do zachowania ostrożności podczas otwierania nieznanych plików, klikaniu w linki lub pobieraniu oprogramowania z nieznanych źródeł.

Źródła

Signaloid-C0-microsd

`https://www.crowdsupply.com/signaloid/signaloid-c0-microsd`

USB Rubber Duck

`https://payload.pl/usb-rubber-ducky/`

The End