2.Sytuacja prawna.

Legalność wytwarzania oprogramowania typu keylogger pozostaje kwestią sporną. Z jednej strony ustawodawca dość precyzyjnie stwierdza w Art. 269b Kodeksu Karnego (Ust. Z dn. 6.06.1997 r.,Tekst jednolity ):

W Rozdziale XXXIII pt. Przestępstwa przeciwko ochronie informacji):

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.

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.

Zostawia jednak pewną lukę:

§ 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

Wygląda na to, że, jak to często bywa, najwazniejsza jest interpretacja. Kiedy można nazwać wyprodukowane oprogramowanie złośliwym wirusem, a kiedy narzędziem diagnostycznym, służącym poprawie bezpieczeństwa? To pytanie należy pozostawić prawnikom (szczególnie tym zajmującym się ochroną sytuacji prawnej firm takich jak Google czy Microsoft ☺).

Trudno stwierdzić, kiedy kończy się tylko działalność w celu poprawienia bezpieczeństwa, a zaczyna szpiegostwo i inwigilacja. Interesującym przykładem mogą być produkty znalezionej naprędce w wyszukiwarce Google jednej z firm:

<zdjecie1>

Która oferując kompleksowe rozwiązanie w zakresie *dyskretnego monitoringu komputera i telefonu* (co jest moim zdaniem bardzo uprzejmą nazwą szpiegostwa komputerowego), sprzedaje programy zawierające jako elementy składowe keyloggery:

Na przykład, jednym z produktów oferowanej firmy jest Ninjalogger STD, który oferuje kompleksowy *monitoring* wybranego komputera pod względem wprowadzanego tekstu, przeglądanych stron www. , rozmów za pomocą komunikatorów typu Skype, czy nawet

odtwarzanych multimediów.
Sposób instalacji takiego oprogramowania jest bardzo prosty: należy umieścić wyglądem przypominający pendrive nośnik w komputerze, który chcemy *monitorować*, zainstalować oprogramowanie, a następnie odmontować nośnik i zabrać go ze sobą. Co ciekawe, widoczność pracy programu jest bardzo utrudniona oraz zapisuje on dane w postaci zaszyfrowanej, można więc przypuścić, że przeciętny użytkownik komputera (niepodejrzewający, że ktos go szpieguje) nie zauważy działania tego typu oprogramowania.
Następnie program przesyła na wskazany adres email logi zawierające kompletne informacje, w których przechwycone dane z klawiatury są jedynie jej elementem składowym.

Firma reklamuje swoje usługi do celów:

- Chcesz wiedzieć czy Partner/Partnerka Cię zdradza
- Chcesz wiedzieć co Twoje dziecko robi przy komputerze
- Wydajność Twoich pracowników nie jest zadowalająca
- Chcesz chronić swoje dzieci przed zagrożeniami czyhającymi w sieci takimi jak np. pedofilia czy narkotyki
- Podejrzewasz kogoś o kradzież Twoich danych prywatnych lub firmowych

Zasadniczym problemem jest to, iż tego typu oprogramowanie można wykorzystać w sposób dowolny. Już sam fakt, że po zainstalowaniu pracuje oraz przechwytuje dane w sposób dyskretny, bez świadomości szpiegowanej osoby, powoduje, że możemy mówić o wielu sytuacjach, w których doszło do złamania prawa. Zatem jeśli firma sprzedaje oprogramowanie, które umożliwia użytkownikowi szpiegowanie cudzych komputerów, można mówić o naruszeniu Art. 269b.

Firma istnieje na rynku już 5 lat (jeśli wierzyć informacjom podanym na stronie producenta). Nie ulega wątpliwości, iż sprzedaż oprogramowania do *dyskretnego monitoringu komputera i telefonu*, będącym w istocie oprogramowaniem szpiegowskim, jest na granicy poszanowania prawa.

3. Sposób działania
Mechanizm pracy keyloggera jest bardzo prosty: urządzenie bądz program, zainstalowane w danym komputerze, przechwytuje strumienie znaków wejściowych wprowadzanych przez użytkownika z klawiatury podczas jego użycia, oraz zapisuje je w pamięci własnej lub w pamięci komputera.

Rdzeń najprostszego keyloggera może wyglądać następująco (implementacja w C++):
<prntscrren3>
Obecnie istnieje cała gama różnych keyloggerów, od czysto sprzętowych, podłączanych do komputera za pośrednictwem usb bez instalacji jakiegokolwiek oprogramowania, po dyskretne, trudno wykrywalne programy z kategorii *spyware*. Istnieją również wyspecjalizowane, bardzo zaawansowane keyloggery, które potrafią przeniknąć do firmware'u sterowników urządzeń, przez co są bardzo trudne do wykrycia.
Zasadniczą ideę działania keyloggera można opisać za pomocą recepty „przechwyć strumień wejściowy klawiatury i prześlij dane do właściciela tak, aby nikt tego nie zauważył". Jak widać na podstawie powyższego kilkunastolinijkowego kodu, sam proces przechwytywania jest najprostszą sprawą (choć profesjonalne keyloggery implementują rozwiązanie na poziomie dużo niższym niż z wykorzystaniem gotowej funkcji GetAsyncKey() z języka C++ czy innej podobnej), dużo trudniejsze jest zaszycie takiego programu w taki sposób, aby udało mu się przeniknąć do docelowego systemu. Nie wspominając o tym, że stworzenie keyloggera odpornego na współczesne programy antywirusowe znacząco komplikuje wydawałoby się prosty z idei problem.
Jednym z takich profesjonalnych, komercyjnych keyloggerów jest Secretlogger. Jest to wirus stworzony do przechwytywania haseł oraz odzyskiwania utraconych kont internetowych. Twórcy gwarantują odporność na wszystkie programy antywirusowe, pełną anonimowość i zapewniają pełne wsparcie techniczne. Co ciekawe, na stronie można znaleźć zachwalające produkt treści typu:
<printstreen4

Jak widać, wspomniany już Art. 269b nie cieszy się popularnością i nie ma większego zastosowania w praktyce.

5. Jak się przed nimi chronić?
W momencie, gdy posiadamy już pewną wiedzę na temat szkodliwego oprogramowania, wystarczy stosować elementarne środki bezpieczeństwa, aby zmniejszyć ryzyko infekcji do minimum. Trzeba mieć świadomość, że to właśnie na etapie ochrony przed infekcją możemy najwięcej zdziałać – jeśli skutecznie będziemy zapobiegać przedostawaniu się niepożądanego oprogramowania. Należy stosować podstawowe zasady higieny codziennego korzystania z komputera, przy czym nie należy wykonywać 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

Dobrze jest również, pomimo posiadania oprogramowania antywirusowego, korzystać dodatkowo z oprogramowania antymalware, jak np. AdwCleaner.
Zalecana jest również ostrożność w korzystaniu z przeglądarki, w tym rezygnacja z przeglądania podejrzanych stron www. Należy pamiętać, że nawet najlepsze programy antywirusowe nie dają nam stuprocentowej zapory, szczególnie jeśli niefortunnie natrafimy w sieci na chętne do penetracji naszego komputera profesjonalne spyware typu Secretlogger. Ich producenci zapewniają przecież o niewidzialności przez nasze programy antywirusowe i dokładają starań, aby produkt pozostawał jak najwyższej jakości i był należycie aktualizowany w stosunku do pojawiających się innowacji w dziedzinie oprogramowania antywirusowego.
Jeśli z jakichś przyczyn czujemy, że możemy nie być wystarczająco chronieni, bardzo dobrym zabezpieczeniem przed keyloggerami jest wpisywanie haseł bez użycia klawiatury, za pomocą menedżera hasła. Możemy stosować również weryfikację dwuetapową, co w połączeniu z odpowiedni silnym hasłem, menedżerem haseł stanowi jedną z najsilniejszych metod obronnych przeciwko keyloggerom.
Inną metodą jest korzystanie z programów, które szyfrują wszystko to, co wprowadzimy z klawiatury, przesyłają w miejsce przeznaczenia, i tam odszyfrowują. Przykładem może być KeyScrambler Personal lub Zemana AntiLogger.

Podsumowanie

Keyloggery, choć bardzo proste w budowie, potrafią wyrządzić ogromne szkody materialne i niematerialne, kradnąc najbardziej wrażliwe dane, takie jak loginy i hasła do internetowych kont bankowych, portali społecznościowych czy poczty elektronicznej. Możemy się przed nimi chronić stosując elementarne zasady bezpieczeństwa i ograniczonego zaufania podczas poruszania się w sieci, a także poprzez stosowanie menedżera hasła, który umożliwia wprowadzenie hasła bez użycia klawiatury i zapewnia bezpieczeństwo przesyłu za pomocą zaszyfrowania wprowadzonych danych. Inną, choć nie zawsze skuteczną metodą, jest korzystanie z klawiatury ekranowej.

1. Bibliografia

https://pl.wikipedia.org/wiki/Keylogger
http://forum.haker.edu.pl/viewtopic.php?t=7#p7

Wersję rastrową wykonał użytkownik polskiego projektu wikipedii: Andrew313, Zwektoryzował: Krzysztof Zajączkowski - Wersja rastrowa:http://pl.wikipedia.org/wiki/Plik:Malwaregraph.png 1. July 2007, 18:49 Andrew313 uploaded "Plik:Malwaregraph.png" (Praca Własna. Podstawowe grupy złośliwego oprogramowania i wzajemne ich powiązania.)