Rodzaje zagrożeń w Internecie

1. **Wirusy –** klasyczne pojęcie wirusów komputerowych obejmuje oprogramowanie, które potrafi dołączyć się do innych aplikacji zmieniając ich sposób działania. Celem infekcji wirusowej są najczęściej działania niepożądane z punktu widzenia właściciela komputera, nierzadko celem jest przejęcie kontroli nad systemem lub zniszczenie danych na komputerze.
2. **Robaki** – są oprogramowaniem, które do rozprzestrzenia się wykorzystują sieci komputerowe. Zarażają komputery z poziomu innego komputera. Na przykład potrafią pobrać adresy odbiorców z książki adresowej klienta pocztowego i przesłać im swoje „robakowe" kopie. Mogą też przesyłać się do innych komputerów w sieci na podstawie ustalonych adresów sieciowych komputerów w danej sieci. Robaki, przeciwnie niż wirusy, do klonowania się na ogół nie potrzebują zasobów dyskowych, wystarczy pamięć operacyjna komputerów (RAM).
3. **Trojany** – to „podstępne" programy, które wykonują szkodliwe działania takie jak kradzież poufnych informacji, niszczenie plików na dyskach, niestabilne działanie systemu operacyjnego itp. Trojany różnią się tym od wirusów, że na ogół same nie potrafią się „dokleić" do innego kodu wykonywalnego, często są „przemycane" przez hackerów pod postacią użytecznego oprogramowania, które użytkownik sam instaluje w komputerze.

   Uwaga! Niektóre szkodliwe programy łączą w sobie dwie lub nawet trzy z tych klas (robaki, wirusy, trojany).

---

4. **Phishing** – polega na kradzieży w celach zarobkowych danych typu hasło do konta bankowego lub numer karty kredytowej; przestępca zazwyczaj tworzy stronę www, która wygląda jak strona banku lub sklepu internetowego i której adres w niewielkim stopniu różni się od podrabianej strony. Nieuważny klient wchodząc na taką stronę i logując się podaje swoje wrażliwe dane, które zostają przechwycone przez autora podrobionych stron. Bardzo często przestępcy wykorzystują również emaile w treści których na ogół są hiperłącza do fałszywych stron. W email'u zawarta jest prośba o sprawdzenie lub aktualizację swoich danych, a po ich podaniu następuje przesłanie ich do złodziei.
5. **Malware** – to różnego rodzaju oprogramowanie, którego głównym celem jest wyrządzenie szkody w komputerze ofiary (stąd określenie „złośliwe oprogramowanie"). Mogą to być wirusy, które niszczą część danych zapisanych na dyskach lub szyfrują jakiś rodzaj plików np. wszystkie pliki graficzne. Często przestępcy proponują w email'u przesłanie klucza odszyfrowującego zaszyfrowane dane po przelaniu określonej kwoty pieniędzy na ich konto. Do malware należą również trojany, które pozwalają przestępcy na dostęp do naszych danych poprzez sieć lub programy typu spyware. Korzystanie z firewall'a (zapory ogniowej) pozwala na pewną kontrolę przesyłu danych w sieci.
6. **Spyware** – to programy „szpiegujące" danego użytkownika zainfekowanego komputera. Szpiegowanie to najczęściej polega na zbieraniu wrażliwych informacji typu hasła, loginy, piny, numery kart kredytowych itp. Spyware przesyła te dane do przestępcy bez wiedzy użytkownika. Szczególnym rodzajem programów szpiegujących są tzw. keylogery, które po zainstalowaniu na maszynie ofiary zapamiętują w plikach wszystko to, co ofiara pisze na klawiaturze, w tym szczególnie cenne dla złodzieja np. loginy i hasła.
7. **Ransomware** (**oprogramowanie szantażujące)** przeważnie jest trojanem, wprowadzanym do systemu poprzez np. pobrany plik lub w wyniku luki w usłudze sieciowej; szyfruje pliki ofiary, uniemożliwiając ich normalny odczyt i żąda okupu w zamian za deszyfrację. W prawidłowo przeprowadzonym ataku przywrócenie danych bez posiadania klucza deszyfrującego jest praktycznie niemożliwe.
8. **Phreaking** – nielegalne podłączenie się do sieci komputerowej w taki sposób, że koszty ponosi inna osoba; wcześniej było to łamanie zabezpieczeń sieci telefonicznych, celem uzyskania połączenia darmowego lub tańszego niż tradycyjne

9. **Instalowanie nielegalnych programów** – wielu użytkowników komputerów chcąc uniknąć opłat związanych z wykupem licencji bardzo często instaluje dany program legalizując go poprzez stosowanie różnego rodzaju „cracków" tzn. narzędzi, które umożliwiają uzyskanie pełnej funkcjonalności „pirackiego" oprogramowania. Nierozważny użytkownik wchodząc na stronę i ściągając takie oprogramowanie naraża się na niebezpieczeństwo zainstalowania na swoim komputerze programu ze złośliwym kodem, który może okazać się np. malware'm. Firma badawcza IDC ocenia, że samo wchodzenie na taką stronę zwiększa ryzyko zainfekowania komputera o 25%.
10. **Riskware –** to oprogramowanie, które zasadniczo nie zawiera szkodliwych funkcji, ale przez to, że może zawierać niezabezpieczone fragmenty kodu tzw. luki („dziury") zdarza się, że hakerzy używają tego oprogramowania do wklejenia złośliwego kodu. Do grupy riskware należą aplikacje, które pozwalają na pracę zdalną, na ukrywanie lub zatrzymywanie procesów, na podłączanie się do przeglądarki internetowej i przekierunkowanie ruchu danych w sieci.
11. **Adware** – to fragment kodu, który jest umieszczany w innym oprogramowaniu, zazwyczaj typu darmowego (tzw. freeware) w celach reklamowych. Taki kod może być wykorzystywany do zbierania informacji o użytkowniku aplikacji i przesyłaniu ich poprzez sieć do osób zainteresowanych zbieraniem danych. Często zdarza się, że adware potrafią zmienić poziom zabezpieczeń lub podmienić stronę startową w przeglądarce internetowej. Czasami dochodzi do obciążenia połączenia internetowego lub bezpośrednich strat finansowych.
12. **Botnety –** to grupy komputerów, które poprzez różnego rodzaju działania powodują szkody. Komputer nieświadomego użytkownika może stać się częścią takiej grupy po zainfekowaniu go złośliwym kodem. Botnety są odpowiedzialne za ataki kradzieży informacji (np. danych uwierzytelniających), za spam (ocenia się, że spam stanowi ok. 90% wiadomości poczty elekronicznej) i za ataki złośliwego oprogramowania.

Sprawdź https://zaufanatrzeciastrona.pl/