RODZAJE ZŁOŚLIWEGO OPROGRAMOWANIA

Złośliwe oprogramowanie (ang. malicious software) to programy, które muszą zostać wprowadzone do komputera użytkownika. Mogą one uszkodzić system, zniszczyć dane, a także uniemożliwić dostęp do sieci, systemów lub usług. Mogą one też wykraść dane lub informacje osobiste ze stacji użytkownika i przesłać je samoczynnie do przestępców. W większości przypadków mogą same się replikować i rozprzestrzeniać na inne hosty dołączone do sieci. Czasem techniki te są używane w połączeniu z socjotechniką, aby oszukać nieostrożnego użytkownika, by ten nieświadomie uruchomił taki atak. Przykładami złośliwego oprogramowania są wirusy, robaki oraz konie trojańskie.

Wirus jest programem, który działa i rozprzestrzenia się przez modyfikowanie innych programów lub plików. Wirus nie może uruchomić się sam, musi zostać uaktywniony. Po uaktywnieniu, wirus może nie robić nic poza replikacją i rozprzestrzenianiem się. Nawet prosty typ wirusa jest niebezpieczny, gdyż może szybko zużyć całą dostępną pamięć komputera i doprowadzić system do zatrzymania. Groźniejszy wirus, przed rozprzestrzenieniem się, może usunąć lub uszkodzić pliki. Wirusy mogą być przenoszone przez załączniki poczty elektronicznej, pobierane pliki, komunikatory, płyty CD/DVD lub urządzenia USB

Rodzaje wirusów komputerowych:

1. Pasożytnicze – wykorzystują swoje ofiary do transportu;
2. Polimorficzne – mogą zmieniać swój kod;
3. Wirusy plików wsadowych – wykorzystują do transportu pliki z rozszerzeniem .bat.

Robak (ang. worm) jest podobny do wirusa, lecz w odróżnieniu od niego nie musi dołączać się do istniejącego programu. Robak używa sieci do rozsyłania swych kopii do podłączonych hostów. Robaki mogą działać samodzielnie i szybko się rozprzestrzeniać. Nie wymagają aktywacji czy ludzkiej interwencji. Samorozprzestrzeniające się robaki sieciowe są o wiele groźniejsze niż pojedynczy wirus, gdyż mogą szybko zainfekować duże obszary Internetu. Najbardziej znane robaki to: I Love You, Melissa, My Doom, Netsky.

Sasser

https://www.youtube.com/watch?v=AR0zY945QLU

Koń trojański (ang. trojan horse), zwany również trojanem, jest programem, który nie replikuje się samodzielnie. Wygląda jak zwykły program, lecz w rzeczywistości jest narzędziem ataku. Idea działania konia trojańskiego polega na zmyleniu użytkownika, by ten uruchomił jego kod myśląc, że uruchamia bezpieczny program. Koń trojański jest zwykle mało szkodliwy, ale może zupełnie zniszczyć zawartość twardego dysku. Trojany często tworzą furtkę dla hakerów – pełny dostęp do zasobów komputera. Najbardziej znane trojany to: Connect4, Flatley Trojan, Poison Ivy.
S.O.V.A.
https://www.dobreprogramy.pl/sova-atakuje-androida-i-kradnie-pieniadze-to-trojan-bankowy-ale-nie-tylko,6682734122040288a

https://www.threatmark.com/about-s-o-v-a-malware-family/

Bomba logiczna (ang. logical bomb), w odróżnieniu od konia trojańskiego, nie uruchamia ukrytego złośliwego oprogramowania od razu tylko w odpowiednim czasie (np. po zajściu określonego zdarzenia lub po kilkukrotnym uruchomieniu wybranej aplikacji).
Exploit jest programem wykorzystującym błędy programistyczne i przejmującym kontrolę nad działaniem procesu
błędy zero-day
https://kapitanhack.pl/2022/03/11/nieskategoryzowane/microsoft-naprawia-3-zero-daye-oraz-inne-krytyczne-bledy/

Keylogger jest oprogramowaniem, mającym na celu wykradanie haseł poprzez przejęcie kontroli nad obsługą klawiatury.

Ransomware (ang. ransom – okup) jest aplikacją wnikającą do atakowanego komputera a następnie szyfrującą dane jego właściciela. Perfidia tego złośliwego oprogramowania polega na zostawieniu odpowiedniej notatki z instrukcją, co musi zrobić właściciel zainfekowanego komputera, aby odzyskać

Rootkit jest programem ułatwiającym włamanie do systemu komputerowego poprzez ukrycie niebezpiecznych plików i procesów mających kontrolę nad systemem. Wykrycie takiego programu w zainfekowanym komputerze jest bardzo trudne, gdyż jest on w stanie kontrolować pracę specjalistycznych narzędzi do jego wykrywania. Najbardziej znane to: Hacker Defender, CD Sony

Spyware jest złośliwym oprogramowaniem mającym na celu szpiegowanie działań użytkownika komputera. Zadaniem spyware jest gromadzenie informacji o użytkowniku (adresy stron internetowych odwiedzanych przez użytkownika, dane osobowe, numery kart kredytowych i płatniczych, hasła, adresy e-mail). Najbardziej znane spyware to: Gator, Cydoor, Save Now

Stealware jest oprogramowaniem mającym na celu okradanie nieświadomego użytkownika poprzez śledzenie jego działań. Instalacja takiego programu odbywa się bez wiedzy i zgody użytkownika za pomocą odpowiednio spreparowanych wirusów komputerowych, robaków lub stron WWW wykorzystujących błędy i luki w przeglądarkach internetowych. Stealware w przypadku stwierdzenia próby płatności przez Internet podmienia numer konta, na które zostaną wpłacone pieniądze