Przegląd narzędzi użytych do Analizy Malware

1. Lista narzędzi użytych umożliwiających przeprowadzenie analizy statycznej:

PEiD

PEiD to narzędzie służące do identyfikacji packerów, kompresorów i kryptorów stosowanych w plikach wykonywalnych Windows PE. Jest szczególnie przydatne w analizie plików binarnych, pozwalając na szybkie rozpoznanie użytych technik ukrywania kodu.

PE-bear

PE-bear to narzędzie do analizy i edycji plików PE (Portable Executable), które oferuje funkcje takie jak przeglądanie struktury pliku, modyfikowanie sekcji i eksploracja nagłówków. Jest cenione za intuicyjny interfejs i możliwości głębokiej inspekcji plików binarnych.

PEStudio

PEStudio to narzędzie do wstępnej analizy plików PE, które pozwala na ocenę potencjalnych zagrożeń bez ich uruchamiania. Umożliwia przeglądanie zależności, analizę importowanych i eksportowanych funkcji, a także wykrywanie wskaźników kompromitacji.

Detect It Easy

Detect It Easy (DIE) to zaawansowane narzędzie do analizy plików wykonywalnych, które identyfikuje użyte packery, kryptory i kompresory. Umożliwia także dekompresję plików oraz dostarcza szczegółowe informacje o strukturze plików PE.

IDA Pro

IDA Pro to interaktywne narzędzie do dekompilacji i analizy binarnej, które umożliwia inżynierię wsteczną złośliwego oprogramowania. Pozwala na statyczną i dynamiczną analizę kodu, oferując rozbudowane funkcje dekompilacji i wizualizacji.

VirusTotal.com

VirusTotal to internetowa usługa umożliwiająca skanowanie plików i adresów URL przy użyciu wielu silników antywirusowych i narzędzi do wykrywania zagrożeń. Pozwala na szybkie zidentyfikowanie potencjalnie złośliwego oprogramowania i uzyskanie szczegółowych raportów na temat analizowanych próbek.

2. Lista narzędzi umożliwiających przeprowadzenie analizy dynamicznej:

RegShot

RegShot to narzędzie do monitorowania zmian w rejestrze Windows. Umożliwia tworzenie zrzutów stanu rejestru przed i po wykonaniu podejrzanego pliku, co pozwala na identyfikację modyfikacji wprowadzonych przez malware.

Process Monitor

Process Monitor to narzędzie do monitorowania aktywności systemu plików, rejestru i procesów w czasie rzeczywistym. Jest używane do śledzenia działań złośliwego oprogramowania i analizy jego wpływu na system operacyjny.

Process Explorer

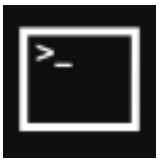
Process Explorer to zaawansowany menedżer procesów, który oferuje

szczegółowe informacje o uruchomionych procesach i otwartych przez nie zasobach. Jest przydatny do identyfikacji podejrzanych procesów i ich powiązań.

x64_dbg

x64_dbg to darmowy debugger dla systemów Windows, obsługujący zarówno aplikacje 32-bitowe, jak i 64-bitowe. Umożliwia dynamiczną analizę kodu i debugowanie złośliwego oprogramowania.

VMPDump



VMPDump to narzędzie służące do dekompilacji plików zabezpieczonych za pomocą VMProtect. Umożliwia ekstrakcję oryginalnego kodu, co ułatwia dalszą analizę złośliwego oprogramowania.

Hybrid-Analysis.com sandbox

Hybrid Analysis to internetowa platforma do dynamicznej analizy złośliwego oprogramowania w środowisku sandbox. Zapewnia szczegółowe raporty na temat działania próbki, w tym jej zachowania sieciowego, zmian systemowych i innych wskaźników kompromitacji.

3. Lista narzędzi umożliwiających przeprowadzenie analizy sieciowej:

FakeNet-NG

FakeNet-NG to narzędzie do symulacji środowiska sieciowego, które pozwala na przechwytywanie i analizę ruchu sieciowego generowanego przez złośliwe oprogramowanie. Pomaga w badaniu zachowań sieciowych malware bez ryzyka dla rzeczywistej infrastruktury.

Wireshark

Wireshark to popularny analizator protokołów sieciowych, który umożliwia przechwytywanie i szczegółową analizę ruchu sieciowego. Jest używany do badania komunikacji sieciowej złośliwego oprogramowania i identyfikacji podejrzanych aktywności.