Akademia Górniczo-Hutnicza im. Stanisława Staszica
w Krakowie

Analiza Malware

Wstęp

Laboratorium ma na celu zaprezentowanie statycznej analizy malware przy wykorzystaniu utworzonego na pierwszych zajęciach środowiska wirtualnego, odseparowanego od stacji roboczej (hosta). W trakcie zajęć student pozna narzędzia oraz metody identyfikacji typu pliku, co przekładać się będzie na określenie celu OS, architektury oraz formatu (np. dll i exe). Ponadto przedstawione zostaną metody identyfikacji złośliwego oprogramowania poprzez generowanie hash-a z unikalnym identyfikatorem. Identyfikator posłuży do określenia, czy badany złośliwy plik został już kiedyś zdekonspirowany. Sprawdzimy wszystkie elementy czytelne, mogące pomóc w określeniu sposobu działania naszego analizowanego programu dzięki m.in. analizie informacji z nagłówków PE.

Przedstawione zadania zostały opracowane na podstawie książki "Practical Malware Analysis" autorstwa Michael Sikorski i Andrew Honig.

Wykorzystane narzędzie:

1. **PEview**
2. **PEiD**
3. **PPEE**
4. **PE-bear**
5. **Resource Haker**

Do analizy posłuży spakowany plik o nazwie „binaries" (Lab 2 - UPEL). Hasło do pliku to „malware".

UWAGA pobrany plik jest szkodliwy i nie należy pod żadnym pozorem uruchamiać go na własnym komputerze, bez przygotowania odpowiedniego środowiska testowego.

Laboratorium 1.1

W tym laboratorium wykorzystaj pliki Lab02-01.exe i Lab02-01.dll. Skorzystaj z narzędzi przeznaczonych do statycznej analizy i odpowiedz na poniższe pytania.

1. Wyciągnij hasha (np. md5 lub sha-1) z plików i sprawdź na stronie *www.VirusTotal.com*, czy pliki o tych samych sumach kontrolnych zostały wcześniej analizowane pod kątem szkodliwego oprogramowania?
2. Wykorzystując narzędzie PEview odszukaj informacje o dacie skompilowania programu.
3. Często bywa tak, że złośliwe oprogramowanie znajduje się w formie spakowanej lub zaciemnionej utrudniając analizę. Wykorzystaj narzędzie PEiD lub PPEE do

sprawdzenia, czy analizowane pliki znajdują się w formie umożliwiającej pełną analizę. Opisz uzyskany rezultat.

4. W celu statycznego sprawdzenia jak działa złośliwe oprogramowanie, możemy przeanalizować importy do bibliotek wykonywane przez analizowane pliki. Do tego możemy wykorzystać program PE-bear (program posiada funkcjonalność jednoczesnego analizowania dwóch plików). Przeanalizuj wykorzystywane importy do określenia sposobu działania pliku exe oraz dll (Lab02-01.exe i Lab02-01.dll). Opisz wybrane przez ciebie najciekawsze importy (za co odpowiadają?).
5. Za co odpowiedzialna jest biblioteka WS2_32.dll (Lab02-01.dll)?
6. Wyświetl informacje strings z programu PPEE dla pliku Lab02-01.exe. Zwróć uwagę na ścieżki dostępowe do biblioteki C:\Windows\System32\Kernel32.dll i jego odpowiednika. O czym mogą świadczyć dwa osobne podobne rekordy?
7. Przeanalizuj tym samym sposobem plik Lab02-01.dll i odpowiedz, czy posiada on jakieś informacje mogące świadczyć o komunikacji internetowej?
8. Posiadając aktualne informacje, czy jesteś w stanie określić w jaki sposób działają analizowane pliki oraz opisać zależność miedzy plikami (exe i dll)?

Laboratorium 1.2

Wykonaj analizę pliku Lab02-02.exe i odpowiedz na pytania.

1. Czy sygnatura analizowanego pliku była już wcześniej analizowana w VirusTotal? Jeśli tak, to podaj wynik skanowania.
2. Sprawdź, czy coś świadczy o tym, że plik jest spakowany lub zaciemniony? Spróbuj go rozpakować.
3. Wykorzystuj poznane narzędzia do porównania importów pliku spakowanego z rozpakowanym. Podaj jakie są różnice pomiędzy nimi oraz wymień najciekawsze importy z rozpakowanego pliku.
4. Odszukaj w strings informacje świadczące o połączeniach programu z siecią Internet.

Laboratorium 1.3

Przeprowadź analizę pliku Lab02-03.exe

1. Czy sygnatura analizowanego pliku była już wcześniej analizowana w VirusTotal? Jeśli tak, to podaj wynik skanowania.
2. Sprawdź, czy coś świadczy o tym, że plik jest spakowany lub zaciemniony? Czy będziesz w stanie rozpakować go przy pomocy UPX? Jeśli nie, to dlaczego?
3. Czy jesteś w stanie sprawdzić datę kompilacji pliku (Time Data Stamp)?
4. Wykorzystuj poznane narzędzia do porównania importów pliku, odpowiedz, czy jesteś w stanie sprawdzić funkcjonalność badanego pliku, w taki sam sposób jak w Laboratorium 1.1?
5. Odszukaj w strings informacje świadczące o połączeniach programu z siecią Internet.

Laboratorium 1.4

Przeprowadź analizę pliku Lab02-04.exe

1. Czy sygnatura analizowanego pliku była już wcześniej analizowana w VirusTotal? Jeśli tak, to podaj wynik skanowania.
2. Sprawdź, czy coś świadczy o tym, że plik jest spakowany lub zaciemniony?
3. Kiedy ten plik został skompilowany?
4. Wykorzystuj poznane narzędzia do porównania importów pliku, odpowiedz, czy jesteś w stanie sprawdzić funkcjonalność badanego pliku, w taki sam sposób jak w Laboratorium 1.1?

5. Odszukaj w strings informacje świadczące o połączeniach programu z siecią Internet.
6. Czy analizowany plik posiada importy świadczące o dostępie do funkcji sieciowych?
7. Badany plik zawiera jeden zasób w sekcji zasobów. Użyj programu Resource Haker, aby zbadać ten zasób, a następnie użyj go do jego wyodrębnienia. Wczytaj plik w programie a następnie użyj funkcji „Action->Save Resource to Bin File" Czego możesz się dowiedzieć analizując ten wyeksportowany zasób?