Kod szkolenia: **MALWARE/ANA**

Tytuł szkolenia: **Malware analysis - analiza oraz zabezpieczanie przed szkodliwym kodem w praktyce**

Dni: 2

Opis:

Adresaci szkolenia

Szkolenie kierowane jest do administratorów, sieciowców oraz ludzi zajmujących się obsługą incydentów bezpieczeństwa.

Cel szkolenia

Przedstawienie narzędzi i podejścia przy analizie szkodliwego oprogramowania oraz technik zabezpieczania sieci komputerowej przed malware. Wykorzystywane są Remnux (dystrybucja Linux) oraz FLARE VM (Windows) - dystrybucje narzędzi dedykowane do analizy malware.

Wymagania

biegłe posługiwanie się systemem Windows i Linux, podstawowa znajomośc asemblera i umiejętność czytania kodu programów w języku C.

Parametry szkolenia

2 *8 godzin (2 *7 godzin netto) wykładów i warsztatów (z wyraźną przewagą warsztatów).

Program szkolenia:

1. Rodzaje szkodliwego oprogramowania: backdoory, keyloggery, trojany bankowe, ransomware
2. Sposoby infekcji systemu
    - Phishing, wodopój, supply chain attacks, 0-daye, grupy APT
3. Analiza stron WWW
    - Analiza skryptów Javascript
4. Analiza plików PDF
5. Analiza plików Office
    - Analiza i deobfuskacja Makr
6. Analiza złośliwych skryptów Powershell
    - Techniki ataku z użyciem WMI
    - Zaawansowana obfuskacja kodu

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel.+48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl

7. Analiza plików wykonywalnych
    - Podstawy formatu plików wykonywalnych (PE, PE64)
    - Analiza plików natywnych, Delphi, .NET, AutoIt, Java
    - Rozpoznanie
        - API Virustotal
        - Wykrywanie zmian w systemie: rejestr, autostart, pliki systemowe, mechanizm Prefetch
    - Analiza statyczna
        - Magiczne stałe i ciągi
        - Sygnatury (Yara rules)
        - dezasemblacja i dekompilacja, analiza kodu assemblerowego
        - przykłady kodu asemblerowego
    - Analiza dynamiczna
        - Monitorowanie aktywności w systemie: Regmonitor, Filemonitor, Api monitor
        - Analiza z użyciem Debuggera
        - Monitorowanie komunikacji w fałszywej sieci
    - Zabezpieczenia malware przed analizą
        - Wykrywanie maszyn wirtualnych typu VMWare
        - Obfuskacja kodu
        - Pakery i protektory, ręczne i automatyczne rozpakowywanie plików
        - Implementacja z użyciem maszyny wirtualnej
8. Wykrywanie szkodliwego oprogramowania w systemie (rootkity):
    - Metody ukrywania w systemach Windows i Linux
    - Metody wykrywania modyfikacji w systemie
        - struktury systemowe
    - ukrywanie procesów
9. Zautomatyzowana analiza malware za pomocą Cuckoo Sandbox
10. Metody zabezpieczania
    - Antywirusy - dobre czy złe?
    - Whitelisting
11. Pułapki dla szkodliwego oprogramowania
    - Honeypots i Honeytraps

Sages sp. z o.o., ul. Nowogrodzka 62c, 02-002 Warszawa
tel. +48 22 203 56 00 fax: +48 22 203 56 01
e-mail: biuro@sages.com.pl web: www.sages.com.pl