

Przydomowe laboratorium analizy malware'u

Omówienie

Infekcje systemów operacyjnych, w szczególności z rodziny Microsoft Windows, powodują co roku straty liczone w miliardach dolarów i już dawno stały się jednym z najpoważniejszych zagrożeń, nie tylko użytkowników domowych ale także dla korporacji i często także funkcjonowania państw. Komputery, które coraz częściej otaczają nas w każdym miejscu i czasie i za pośrednictwem których wykonujemy coraz więcej codziennych czynności, stają się narażone na nowatorskie i trudne do wykrycia ataki. Najstabszym ogniwem pozostają użytkownicy domowi, których komputery są z reguły niewystarczająco zabezpieczone i co za tym idzie najtrudniejsze do obrony.

Warsztaty mają na celu przybliżyć uczestnikom przede wszystkim zasady działania najpopularniejszych typów złośliwego oprogramowania (boty, ransomware) oraz metody ich analizy. W tym celu zaprezentowane zostaną narzędzia oraz serwisy internetowe, które z powodzeniem mogą być używane w "Przydomowym laboratorium analizy malware'u".

Adresaci szkolenia

Administratorzy systemów i sieci, zaawansowani użytkownicy i pasjonaci bezpieczeństwa komputerowego, osoby chcące rozpocząć przygodę z analizą złośliwego oprogramowania.

Zakres tematyczny

- Podstawy konfiguracji środowiska laboratoryjnego,
- Omówienie narzędzi używanych w podstawowej analizie złośliwego oprogramowania,
- Analiza ruchu sieciowego generowanego przez malware,
- Odnajdywanie źródeł infekcji,
- Statyczna analiza próbek i pamięci systemu operacyjnego.

Wymagania:

- Średnio-zaawansowana znajomość obsługi i konfiguracji środowiska wirtualizacji VirtualBox,
- Znajomość obsługi narzędzia do analizy ruchu sieciowego – Wireshark,
- Podstawowa znajomość protokołów sieciowych,
- Podstawowa umiejętność pracy w systemie Linux i Windows.

Wymagania techniczne:

- Własny komputer, który:
- posiada kartę ethernet lub WiFi,
- posiada minimum 2 GB pamięci RAM,
- posiada minimum 2-rdzeniowy procesor,
- posiada przynajmniej 10GB miejsca na dysku.
- zainstalowany system wirtualizacji oparty na VirtualBox,
- zainstalowane narzędzie Wireshark.

Prowadzący

Specjaliści z Zespołu CERT Polska