NASK
akademia

oferta szkoleń specjalistycznych

Nasze szkolenie pt.:

Przydomowe laboratorium analizy malware'u

Cena: 980 zł netto

(udział w szkoleniu i lunch dla 1 osoby)

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. Najsłabszym 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".

Prowadzący

Kamil Frankowicz

Łowca niepożądanego oprogramowania (bug & malware) w CERT Polska. Zawodowo "rozbraja" malware oraz wyszukuje podatności bezpieczeństwa w wielu projektach open-source. Fan automatyzacji wejścia/wyjścia. Prelegent i trener na konferencjach związanych z bezpieczeństwem IT: Warszawskie Dni Informatyki 2017, SECURE 2016, Security BSides 2015 & 2016. Współautor polskiego corocznego raportu CERT (sekcje: ransomware, polski malware oraz najważniejsze podatności).

Jarosław Jedynak

Analityk malware i specjalista od bezpieczeństwa IT w CERT Polska. W pracy zajmuje się głównie analizą malware ze szczególnym uwzględnieniem botnetów spamowych oraz P2P oraz ransomware. Dodatkowo aktywnie śledzi działalność przestępców i ich kampanie. Zdobytą wiedzą dzieli się na konferencjach (ostatnio na Warszawskich Dniach Informatyki 2016 i Security BSides Warsaw 2016), oraz prowadzi warsztaty (ostatnio na SECURE 2016). W wolnym czasie jest zapalonym graczem w konkursach z dziedziny bezpieczeństwa IT (tzw. CTFy). Współzałożyciel zespołu p4 (który zyskał piąte miejsce na świecie w 2016 roku), który także organizuje zawody CTF.

Adresaci szkolenia

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

Zakres minimalnych wymagań dla uczestników szkolenia

- 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.
- 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.

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.

Wymiar godzinowy i forma zajęć

8 godzin zajęć (warsztaty)