# 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.

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 "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 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 64-bitowy system operacyjny (sugerowany Windows lub Ubuntu Linux),
    - posiada kartę Ethernet lub WiFi,
    - posiada minimum 4 GB (sugerowane 8GB) pamięci RAM,
    - posiada minimum 2-rdzeniowy procesor,
    - posiada przynajmniej 20GB wolnego miejsca na dysku.
    - zainstalowane oprogramowanie VirtualBox,
    - zainstalowane narzędzie Wireshark,
    - konto administratora w systemie operacyjnym,
    - brak oprogramowania antywirusowego lub możliwość jego wyłączenia.

Akademia NASK
ul. Kolska 12, 01-045 Warszawa
tel: +48 22 380 82 00, 380 85 49
szkolenia@nask.pl, www.akademia.nask.pl

Uczestnik warsztatów musi posiadać maszynę wirtualną z zainstalowanym systemem operacyjnym Windows 7 (x64, dowolna edycja). O poprawność licencji zadbać musi uczestnik szkolenia. NASK nie dostarcza licencji, ani obrazów instalacyjnych Microsoft Windows.

## Zakres tematyczny

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

## Czas trwania i forma zajęć

8 godzin zajęć (warsztaty)

## Prowadzący

**Kamil Frankowicz**

Bug & malware hunter w CERT Polska. Zawodowo "rozbraja" malware oraz wyszukuje podatności bezpieczeństwa w różnych projektach open-source. Prelegent i trener na konferencjach związanych z bezpieczeństwem IT: Warszawskie Dni Informatyki 2017, SECURE 2016, Security BSides 2015 & 2016.

**Jarosław Jedynak**

Analityk malware i specjalista w zakresie bezpieczeństwa IT w CERT Polska. W pracy zajmuje się głównie analizą malware, szczególnie botnetami P2P oraz spamowymi, a także ransomware. Dodatkowo aktywnie śledzi działania 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 nałogowym graczem w konkursach z dziedziny bezpieczeństwa IT (tzw. CTFy). Współzałożyciel zespołu p4, który zyskał piąte miejsce na świecie w 2016 roku.