Laboratorium analizy malware'u

Zespół Edukacji i Szkoleń Akademii NASK

www.akademia.nask.pl
szkolenia@nask.pl

NASK

NASK akademia

Oferta szkoleń specjalistycznych

Naukowa i Akademicka Sieć Komputerowa
jest państwowym instytutem badawczym prowadzącym działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność i bezpieczeństwo sieci teleinformatycznych. Jako operator telekomunikacyjny NASK oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki.

Akademia NASK realizuje działalność edukacyjną i popularyzatorską Instytutu. Prowadzi m. in. unikatowe szkolenia z tematyki cyberbezpieczeństwa ICT oraz zagrożeń dzieci i młodzieży w internecie.

Zespół Edukacji i Szkoleń Akademii NASK jest działem Akademii NASK, który zajmuje się edukacją i szkoleniem w zakresie bezpieczeństwa w sieci, wykorzystywaniem nowoczesnych technologii i multimediów w dydaktyce, rozwijaniem kompetencji w zakresie technologii oraz budowaniem świadomości na temat zagrożeń internetowych.

W naszej **ofercie** znajdą Państwo **interesujące kursy i szkolenia**, które prowadzą **wysoko wyspecjalizowani** pracownicy i **eksperci** w dziedzinie telekomunikacji. Zakres tematyczny ustalany jest zgodnie z zapotrzebowaniem merytorycznym klienta i pod konkretną grupę słuchaczy. Każdego traktujemy indywidualnie, badamy jego potrzeby tak, aby przekazać najbardziej aktualną wiedzę.

Serdecznie zapraszamy do kontaktu.

Zespół Edukacji i Szkoleń
Akademii NASK

www.akademia.nask.pl
szkolenia@nask.pl

NASK

NASK akademia

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

Kazdy uczestnik warsztatów powinien posiadac własny komputer, który:

- posiada 64-bitowy system operacyjny (sugerowany Windows lub Ubuntu Linux)
- posiada karte Ethernet lub WiFi
- posiada minimum 4 GB (sugerowane 8GB) pamieci RAM
- posiada minimum 2-rdzeniowy procesor
- posiada przynajmniej 20GB wolnego miejsca na dysku
- zainstalowane oprogramowanie VirtualBox
- konto administratora w systemie operacyjnym
- brak oprogramowania antywirusowego lub mozliwosc jego wyłaczenia

Kazdy uczestnik warsztatów powinien posiadac:

- podstawowa znajomosc obsługi i kon1guracji srodowiska wirtualizacji VirtualBox
- podstawowa znajomosc obsługi narzedzia do analizy ruchu sieciowego – Wireshark
- podstawowa znajomosc protokołów sieciowych
- podstawowa umiejetnosc pracy w systemie Linux i Windows

Uczestnik warsztatów musi posiadać maszynę wirtualną z zainstalowanym systemem operacyjnym (Windows 10).

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
- 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.