kaspersky

Реверс-инжиниринг целевого вредоносного ПО

Онлайн-тренинг для специалистов по кибербезопасности

Бывает, что автоматический анализ вредоносного ПО не приносит должных результатов, а помощь внешних экспертов недоступна. На этот случай крупному бизнесу нужны собственные специалисты по обратной разработке, способные эффективно решать сложные задачи. Неважно, кто вы. Руководитель бизнеса или глава ИБ-департамента, который хочет обучить свою ИБ-команду борьбе с современным целевым вредоносным ПО. Специалист по кибербезопасности, отлично владеющий методологией и инструментами для анализа вредоносных программ, но желающий более уверенно применять свои навыки на практике. В любом случае этот тренинг будет полезен вам для отражения целевых кибератак, которые наносят большой ущерб бизнесу.

Это тренинг среднего уровня сложности. В его основе лежит анализ 10 экземпляров вредоносного ПО, использованного известными APT-группами в недавних целевых атаках. Изучением некоторых из них, например атак MontysThree, LuckyMouse и Lazarus, инструкторы курса лично занимались в нашем глобальном центре исследований и анализа угроз (GReAT). Вы получите ценные знания и практические наработки из первых рук.

На занятиях в специальной виртуальной лаборатории вы будете работать с реальными образцами целевого вредоносного ПО, используя целый ряд таких инструментов, как дизассемблер IDA Pro, декомпилятор Hex-Rays, редакторы Hiew и 010Editor и многие другие. Это поможет вам улучшить навыки анализа и обратной разработки вредоносных программ, а также актуализировать их для работы с современным ландшафтом угроз.

Программа тренинга

- Анализ реальных образцов вредоносного ПО, использованного APT-группами
- Обратная разработка вредоносных документов и эксплойтов
- Знакомство с инструментами для обратной разработки ПО; вредоносными программами, написанными на разных языках программирования (C, .NET, Delphi, C++), в том числе скриптовыми (Powershell, JavaScript); сэмплами, собранными различными компиляторами для архитектур x86/x64 и операционных систем Windows и Linux
- Изучение расширенных возможностей инструментов для обратной разработки, в том числе функции создания скриптов в IDA Pro.
- Детальный разбор стеганографии
- Работа с обфусцированным и зашифрованным кодом вредоносного ПО
- Углубленное знакомство с ассемблированием
- Разбор обходных путей, которые киберпреступники используют для запуска своих программ
- Анализ шелл-кода.

Требования

Владение по крайней мере одним языком программирования (в том числе скриптовым), в идеале – Python; базовое понимание языка ассемблера для процессоров Intel; знание основ обратной разработки и базовых принципов работы целевого вредоносного ПО

Как проходит тренинг

Видеолекции экспертов «Лаборатории Касперского»
Вашими преподавателями будут Иван Квятковски и Денис Легезо – старшие исследователи кибербезопасности, сотрудники глобального центра исследований и анализа угроз (GReAT).

Практические занятия в виртуальной лаборатории
Вы узнаете, как использовать инструменты, такие как IDA Pro, на примере реальных целевых атак Lazarus, LuckyMouse и MontysThree.

Итеративный подход
Тренинги построены на принципах прогрессивного обучения и состоят из согласованных модулей. Каждый из них включает объяснение задачи инструктором, практическое занятие в виртуальной лаборатории и детальный разбор решения.

Особенности тренинга

Доступ	Курс доступен в течение 6 месяцев с момента активации кода
Язык	Все материалы предоставляются на английском языке (включая субтитры)
Темп	Составьте график, который подходит именно вам
Занятия в виртуальной лаборатории	100 часов практических занятий
Скачиваемые материалы	Материалы тренинга и рекомендации в формате PDF
Технические требования	Браузер на компьютере, телефоне или планшете
Авторы тренинга	Иван Квятковски и Денис Легезо – старшие исследователи кибербезопасности, сотрудники глобального центра исследований и анализа угроз (GReAT) «Лаборатории Касперского»
Видеоматериалы	Более 50 видео, которые помогут вам пройти курс
Поддержка и обратная связь	Получайте поддержку и помощь профильных специалистов. Задайте вопрос через форму на сайте help.kasperskyxtraining.com, и мы ответим вам на электронную почту
Специальное предложение от Hex-Rays	Эксклюзивная скидка 10% на IDA Pro, IDA Home и декомпилятор Hex-Rays для участников тренинга

Авторы тренинга

Денис Легезо,
старший исследователь кибербезопасности

Денис Легезо занимает должность старшего исследователя кибербезопасности в нашем глобальном центре исследований и анализа угроз (GReAT) с 2014 года. Он прошел сертификацию GIAC в области цифровой криминалистики и специализируется на исследовании целевых атак и статической обратной разработке.

Денис регулярно проводит тренинги для клиентов по этим направлениям, а также представляет результаты своих исследований вредоносного ПО на конференциях SAS, RSA, HITB и в журнале VirusBulletin.

Иван Квятковски,
старший исследователь кибербезопасности

Иван Квятковски – эксперт по тестированию на проникновение и анализу вредоносного ПО, имеющий сертификаты OSCP и OSCE. С 2018 года является старшим исследователем кибербезопасности в глобальном центре исследований и анализа угроз (GReAT).

Иван помогает поддерживать инструмент для анализа открытого исходного кода исполняемых файлов Windows. Результаты его исследований были представлены на нескольких конференциях по кибербезопасности. Он также управляет выходным узлом сети Tor и ведет тренинги «Лаборатории Касперского» по обратной разработке в Европе.

Тренинги по кибербезопасности:
kaspersky.com/enterprise-security/cyber-security-training