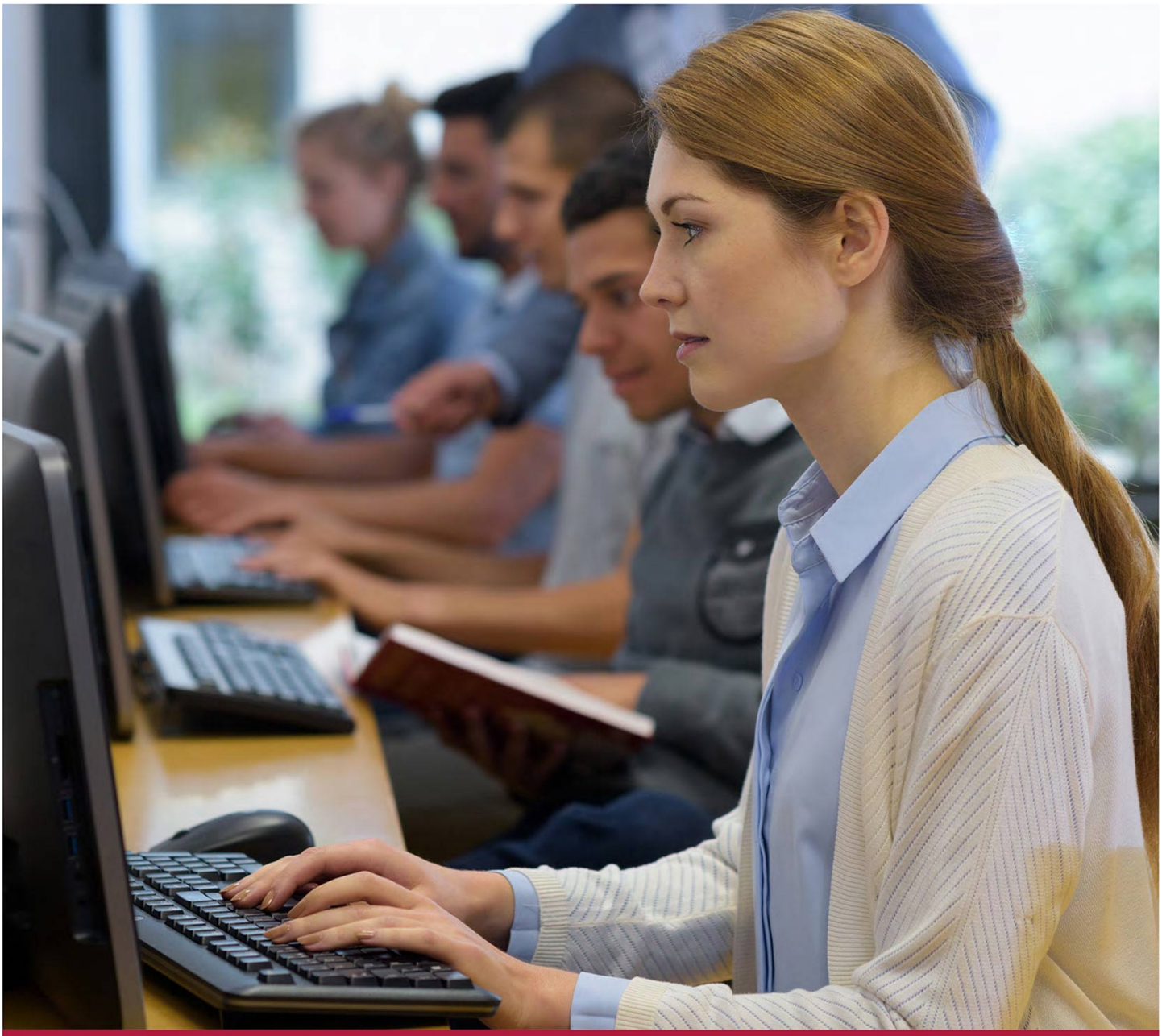
softline®

Учебный центр Softline



# Анализ и обратная разработка вредоносного ПО

Код курса: KL-AREKU

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

© Softline 2020

**Анализ и обратная разработка вредоносного ПО**

Код курса: KL-AREKU

| | |
|---|---|
| **Длительность** | 40 ак. часов |
| **Формат** | |
| **Разработчик курса** | Лаборатория Касперского |
| **Тип** | Учебный курс |
| **Способ обучения** | Под руководством тренера |

## О курсе

Курс предназначен для специалистов, желающих получить практические знания в анализе вредоносных программ. В курсе дается вся необходимая информация о современном ландшафте вредоносного и антивирусного программного обеспечения. Слушатели узнают о том, как работает современное вредоносное ПО и его проникновении в ИТ-инфраструктуру компаний, как происходит инфицирование. Слушатели научатся основным методам анализа вредоносного ПО. Программа курса предназначена для специалистов, желающих получить практический опыт анализа вредоносного ПО. Слушатели должны обладать опытом программирования. Во время выполнения лабораторных работ слушатели научатся использовать такие утилиты, как IDA, Immunity debugger, OllyDdg, WireShark, Fiddler Proxy, набор утилит Sysinternals и др. Практические знания тесно связаны с теоретическим материалом. Слушатели должны понимать, что находится за применяемыми утилитами и техниками. Все инструкторы являются практиками, их опыт основан на ежедневно выполняемых задачах. Данный курс проводит Kaspersky Lab, привлекая собственных тренеров (только очно, г. Москва)

## Подробная информация

**Профиль аудитории:**

- Системные и сетевые инженеры, администраторы и специалисты в области сетевой безопасности, архитекторы безопасности.

**Предварительные требования:**

- Продвинутые навыки системного администрирования;
- Знания языков программирования.

**По окончании курса слушатели смогут:**

- Знать типы вредоносного ПО;
- Знать основные методы анализа вредоносного ПО;
- Применять статический и динамический анализ;
- Выполнять анализ скриптов.


© Softline 2020

# Программа курса

## День 1

Для применения реверсного инжиниринга к вредоносному коду, требуется понимать, как функционируют современные операционные системы и процессорные инструкции. Данный курс начинается с обзора архитектуры Windows, Application Programming Interface (API), режимы пользователя и ядра, компоненты режима ядра (Hardware Abstraction Level HAL, драйверы устройств, режим Windows PE) и основные системные файлы Windows. Будут также кратко рассмотрены популярные системные библиотеки (DLLs), функции WinAPI. Рекомендуется иметь доступ к подписке MSDN.

Слушатели в деталях изучат основные компоненты ОС: процессы, потоки, process environment blocks (PEB) и thread environments blocks (TEB). Будет дано описание многозадачности, переключения между контекстами, scheduling и другие механизмы ОС.

**Модуль 1 Введение в анализ вредоносного ПО**

- Типы вредоносного ПО
- Цели анализа
- Основы реверс-инжиниринга

**Модуль 2 Основы Windows**

- Основные системные файлы Windows
- Формат файла PE (Portable Executable), секции импорта и экспорта
- Функции Windows API, используемые при анализе
- Архитектура Intel 32-bit (AI-32)

## День 2

Существуют два основных типа анализа статический и динамический. Статический анализ выполняется без реального запуска программ и обычно используется для быстрого предварительного анализа. Слушатели получат опыт в поверхностном (surface) анализе аномалии в заголовках PE, подозрительные строки, ресурсы и импортированные функции. Они научатся использовать различные алгоритмы хэширования для проверки целостности файлов, проверять цифровые подписи, искать информацию о подозрительных объектах в Интернете. Используя реальные сэмплы, слушатели научатся обнаружению защитных мер, вставленных упаковщиками и удалять их. Слушатели также научатся методам повышения читабельности деассемблированного вредоносного кода и быстрой навигации по нему. Участники курса научатся понимать алгоритмы вредоносного кожа и находить такой код внутри программ.

**Модуль 3 Статический анализ приложений**

- Когда применим?
- Преимущества и недостатки данного метода

**Модуль 4 Техники статического анализа**

- Извлечение строковых значений и web-поиск


© Softline 2020

- Хэширование и проверка цифровой подписи
- Извлечение метаданных и обнаружение аномалий
- Импорт, экспорт и анализ ресурсов
- Анализ кода
- Автоматическая распаковка (unpacking)

## День 3

Динамический анализ позволяет изучить поведение программ в процессе ее работы, включая такие характеристики, как сетевой трафик, используемые API, взаимодействие с реестром и др. Слушатели научатся выполнять отладку программ, снимать дампы памяти, осуществлять мониторинг вызовов функций Windows API, доступа к реестру, создавать виртуальные сети и эмулировать реальную сетевую активность в лабораторной среде и инспектировать сетевой трафик. Все перечисленные действия выполняются в лабораторных работах. После того, как инструктор покажет, как использовать тот или иной инструмент, слушатели самостоятельно опробуют его для анализа реальных сэмплов.

**Модуль 5 Динамический анализ локальных данных**

- Активность процессов и дампы памяти
- API мониторинга
- Мониторинг событий
- Выполнение в песочнице
- Отладка
- Активность реестра

**Модуль 6 Динамический анализ сетевых данных**

- Создание виртуальной сети
- Инспектирование трафика
- Оффлайн анализ трафика
- Симуляция сети

## День 4

Windows API не является единственным программным интерфейсом для вредоносного ПО, поэтому участники курса также познакомятся с NET, Java и другими популярными языками. Слушатели получат необходимые знания соответствующих инструментов для анализа и декомпиляции.

**Модуль 7 Анализ Non-Win32**

- .NET
- Visual Basic
- Java
- Win64

## День 4

Вредоносный код использует не только исполняемые файлы. Даже легальные веб-сайты могут быть скомпрометированы различными скриптами. Слушатели научатся анализу языков для написания


© Softline 2020

скриптов. Данный анализ включает в себя скрипты автоматизации, установщики и др.

**Модуль 8 Анализ скриптов**

- Пакетные файлы
- Autolt
- Python
- Скрипты Java и VBS
- Visual Basic Script

**Посмотреть расписание курса и записаться на обучение**

**Обращайтесь по любым вопросам**
к менеджерам Учебного центра Softline

**8 (800) 505-05-07** | edusales@softline.com

**Ждём вас на занятиях в Учебном центре Softline!**


© Softline 2020

## Почему Учебный центр Softline?

**Лидер** на рынке корпоративного обучения.

**Более 300 тысяч** подготовленных IT-специалистов.

**Гибкий индивидуальный подход** в обучении, скидки и акции.

**Широкая сеть представительств** в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

**Высокотехнологичное** оборудование

Более **17 лет** опыта работы

**Международные сертификаты** для IT-специалистов и пользователей в Центрах тестирования

**Сертифицированные тренеры** с богатым практическим опытом работы

**Авторизации от мировых производителей ПО** (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперсокого, Oracle, Autodesk, Код безопасности и других).

**Разработка курсов и тестов под заказ**, внедрение корпоративных систем обучения.

**Подробнее об Учебном центре Softline**
Вы можете узнать из профайла и презентации


© Softline 2020