## Курс «Анализ вредоносного программного обеспечения»

На базе ТОО «INTELLA» с 21 по 25 октября 2019 года пройдет СПЕЦИАЛИЗИРОВАННЫЙ КУРС ОБУЧЕНИЯ – **«Анализ вредоносного программного обеспечения»**.

**Цель курса:**

- осветить возможности актуальных вредоносных программ и современное состояние киберугроз;
- обучить созданию лабораторного стенда на базе ПО VMware;
- подготовить к работе с утилитами, предназначенными для анализа кода;
- развить навыки идентификации основных управляющих конструкций в ассемблерном коде;
- предоставить понимание методов противодействия анализу, применяемых вредоносным ПО, а также, способов решения, связанных с подобным функционалом, проблем;
- научить применению техник динамического анализа подозрительных объектов.

**Полученные знания позволят слушателям решать следующие задачи:**

- создать мини-лабораторию по анализу вредоносного ПО, позволяющую провести экспресс-анализ неизвестных подозрительных объектов, выявленных на предприятиях заказчика;
- определять функционал неизвестных средствам контроля (антивирусам и т.д.) вредоносных объектов;
- формулировать порядок противодействия (методов нейтрализации угрозы и препятствования дальнейшему распространению в сети предприятия) обнаруженному заражению еще до реакции производителя антивирусного ПО, а также в случаях, когда отправка образца в антивирусную лабораторию нежелательна (из соображений секретности и т.д.) или затруднительна (нет возможности своевременно получить доступ к сети Интернет – на объектах, где использование данной сети ограниченно);
- проводить расследования инцидентов, связанных с воздействием вредоносного ПО (использованные каналы заражения, цели вредоносного ПО, атакованные объекты и реально причиненный ущерб), в том числе, с современными средствами кибершпионажа.

**Целевая аудитория:**

Начальники служб ИТ и/или ИБ; технические специалисты, ответственные за защиту информации и информационных технологий.

- **Статус:** Авторский курс Олега БИЛЬ, РГП «ГТС»
- **Длительность обучения** – 5 дней (40 академических часов)
- **Форма обучения** – аудиторные занятия
- **Стоимость курса:** с одного слушателя 500 000 тг. без НДС
- **На базе центра повышения квалификации:** ТОО «INTELLA»
- **Место и даты проведения** – г. Нур-Султан, с 21 по 25 октября 2019 г.

**Требования для прохождения практического курса**

Наличие Ноутбука со следующими характеристиками:

1. Минимум 4 Гб оперативной памяти;
2. Минимум 10 Гб свободного места на диске;
3. На ноутбуке должна быть установлена среда виртуализации VirtualBox.

**Минимальные требования к подготовке слушателей:**

- квалификация слушателя – администратор Windows (установка и основная настройка операционной системы, свободная работа с основными приложениями (Office, браузеры, архиваторы, файловые менеджеры, почтовые клиенты и т.д. – установка, настройка);
- навыки программирования – базовые, хотя бы на одном языке программирования (знание управляющих структур if-then, case, циклов, функций, умение писать простейшие программы (решение квадратного уравнения и т.д.);
- желательно базовое знание ПО для виртуализации (VMware);
- желательны базовые знания английского языка (хотя бы уверенное владение словарем), так как интерфейс большинства используемых утилит реализован на английском языке.

**Пакет слушателя:**

- Фирменное учебное пособие в электронном виде
- Организационно-распорядительные и основные нормативно-правовые акты, и методические материалы, на основе которых ведется обучение, дополнительная и справочная информация по тематике курса в электронном виде

**Программа курса:**

| Модуль | Тема |
|---|---|
| **1. Введение и настройка среды анализа** | 1. Введение. Статистика. Угрозы. Меры безопасной работы. Начальное тестирование (2 цели: определение уровня квалификации и осознание слушателем роста своей квалификации (в конце курса задаются те же вопросы, слушатель отвечает, после этого ему показывают его ответы начального тестирования, и он видит свой прогресс).<br>2. VMware. Установка, настройка.<br>3. Установка и настройка VMware, Windows и пакета утилит, используемых в процессе обучения (ProcMon, Process Explorer, RegShot, PE Explorer, CaptureBat, All-Seeing Eye, ApateDNS, Wireshark, IDA Pro free, OllyDbg). |
| **2. Основы статического анализа исполняемых файлов** | 1. Начальный статический анализ (сканирование антивирусным ПО, поиск репутации файлов по их md5 хэшам в Интернет, обнаружение и анализ строк, содержащихся в исполняемом файле, определение компилятора или упаковщика (протектора), с помощью которого был создан исполняемый файл).<br>2. Системы счисления. Формат PE-файла (структура, основные параметры, секции). Анализ с использованием CFF Explorer.<br>3. Динамические библиотеки (способы линковки, экспорт, импорт функций из библиотек).<br>4. Анализ (строки, компилятор/упаковщик, PE заголовки, импортируемые функции) нескольких файлов (упакованные/неупакованные). |
| **3. Основы динамического анализа исполняемых файлов** | 1. Использование инструментов для комплексного анализа поведения исполняемых модулей (песочниц) (Anubis, Norman Sandbox, GFI Sandbox).<br>2.Утилиты для мониторинга поведения исполняемых файлов (ProcMon, Process Explorer, RegShot, CaptureBat, All-Seeing Eye). Основные методы обеспечения автозапуска. |

| | |
|---|---|
| | 3. Утилиты для анализа сетевой активности подозрительных файлов (ApateDNS, Wireshark). Возможности.<br>4. Анализ поведения нескольких вредоносных объектов (Trojan-Downloader, Trojan-Dropper), с использованием песочниц и утилит для мониторинга (локальной и сетевой активности). |
| **4. Углубленный статический анализ I. Основы ассемблера** | 1. Регистры, виды адресации.<br>2. Команды языка Assembler: команды обмена данными (mov, xchg), арифметические команды (add, sub…), управления потоком выполнения (jmp, loop, call, jxx…), прочие (in, out, int).<br>3. Соответствие структур языков высокого уровня (ЯВУ) коду на ассемблере (циклы, ветвления…).<br>4. Поиск аналогов приведенного кода на ассемблере, коду на ЯВУ. |
| **5. Углубленный статический анализ II. Дизассемблирование** | 1. IDA Pro free. Интерфейс, возможности.<br>2. Анализ в IDA простых вредоносов. Trojan-Downloader, Trojan-Dropper<br>3. Анти-дизассемблирование. Методы противодействия. |
| **6. Углубленный динамический анализ** | 1. Повторение. Дизассемблирование дроппера, использующего анти-дизассемблирование.<br>2. Отладка программ. Возможности. OllyDbg. Интерфейс, функции, плагины. Точки останова. Виды.<br>3. Антиотладка. Методы. Противодействие.<br>4. Отладка - практика. |
| **7. Упаковщики** | 1. Принципы работы, автоматическая распаковка (специализированные утилиты для различных упаковщиков – ASPack Die, UnFSGи т.д., универсальный инструмент – QuickUnpack).<br>2. Ручная распаковка (лекция): нахождение OEP, дамп файла, восстановление таблицы импорта.<br>3. Ручная распаковка (практика) некоторых пакеров (UPX, ASPack, FSG, WinUpack). |
| **8. Подведение итогов** | 1. Повторение.<br>2. Итоговая контрольная работа (или тест).<br>3. Осознанный выбор продуктов, обеспечивающих безопасность (антивирусов и т.д.) – анализ независимых тестов, выбор значимых и не значимых показателей, указанных в отчетах, с учетом влияния их на уровень защищенности.<br>4. Объявление результатов итогового контроля (если нужно). Мнения, отзывы, вопросы – ответы. |

**Дополнительная информация:**

***Телефон:*** +7 (727) 355 02 34

***Электронная почта:*** asel@intella.kz

Директор учебного центра ТОО «INTELLA», Муханмеджанова Асель

ТОО «INTELLA»
010000 г. Нур-Султан,
ул. Д. Кунаева, 29/1,
ГК «Дипломат», оф. 1903
БИН 080840000052

+7 (7172) 28 00 82
+7 (727) 355 02 34

info@intella.kz
www.intella.kz