Investigación y protección contra el malware y el cibercrimen

El malware (generalmente conocido como virus) es la principal herramienta con la que cuentan los cibercriminales para cometer robos, estafas y fraudes a través de las redes.

Objetivos generales

Este curso está orientado a conocer los distintos tipos de malware actuales y cómo los cibercriminales organizados en grupos delictivos realizan su desarrollo y lo utilizan contra los usuarios de internet para generar ganancias económicas. Se analiza cómo combatirlos a través de la utilización de métodos manuales y automáticos, utilizados por los mejores laboratorios antivirus del mundo.

Requisitos previos

Conocimiento básico sobre Seguridad de la Información.

Público Objetivo

El curso está orientado a administradores de IT, responsables de seguridad y cualquier persona comprometida con el análisis interno o externo de seguridad en una organización. También está orientado a personas interesadas en la investigación del cibercrimen.

Finalizado el curso, el asistente será capaz de:

- Conocer los distintos tipos de malware
- Conocer cómo funciona el cibercrimen organizado internacional
- Conocer las metodologías de análisis de malware
- Conocer las herramientas para llevar adelante un análisis de malware
- Detectar y eliminar cualquier rastro de malware en un sistema y organización en forma manual y automática

Este curso complementa los cursos **"Aspectos Legales de las Tecnologías de la Información en el marco de la Seguridad de la información"** y **"Delitos informáticos y prevención del cibercrimen"** dictados por **Segu-Info.**

Material a entregar

Presentaciones utilizadas durante el curso y certificado de asistencia y aprobación, ambos en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **24 horas** y la modalidad de cursada es presencial.

Instructor

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.
Actualmente es Director de **Segu-Info** y **Segu-Kids** y se desempeña como consultor independiente en Seguridad de la Información.
Ha trabajado en la investigación de malware durante más de 15 años y escribe para diversos medios especializados e investiga en forma independiente sobre Seguridad Informática y de la Información.
Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre la temática.

Temario

Introducción al Malware

- Historia y definiciones
- Tipos de malware (virus, troyano, gusano, rogue, spyware, adware, etc.)
- Tipos de troyanos (downloader, spy, keylogger, spammer, etc.)

Cibercrimen

- Cibercrimen, ciberactivismo y ciberguerra
- Ingeniería social
- Spam y Phishing
- Botnets
- Metodologías de infección
- Uso del malware como herramienta del cibercrimen

Antivirus

- Funcionamiento y metodologías de detección
- Tipos de análisis
- Generación de firmas
- Tipos de heurística
- Nombres y nomeclaturas del malware

Detección y análisis

- Análisis pasivo
- Análisis activo
- Análisis black-box
- Análisis white-box

Análisis de malware - Práctica

- Análisis práctico de troyanos, gusanos, virus, rogue y otros tipos de malware
- Utilización de herramientas de análisis pasivo y activo

Herramientas avanzadas del cibercrimen

- Funcionamiento de zombies y botnets
- Scripting
- Empaquetamiento
- Ofuscamiento
- Drive-by-download
- Criptovirología
- Generación de malware automático
- Explotación de vulnerabilidades
- Generación de exploits
- Generación de archivos HTML, PDF, Flash y Java dañinos

Análisis de técnicas avanzadas - Práctica

- Descompilación
- Desofuscamiento
- Desempaquetado de archivos
- Ingeniería reversa
- Análisis de archivos HTML, PDF, Flash y Java dañinos
- Análisis y técnicas de detección para evitar Drive-by-download
- Utilización de herramientas de detección y bloqueos