Counter Threat Intelligence Bootcamp

/Rooted CON 2017

/Rooted®

Introducción

Las amenazas en Internet han evolucionado de manera que ya no se producen apenas ataques desde un punto de vista clásico hoy en día, es decir atacando directamente la infraestructura expuesta a internet.

Las amenazas actuales utilizan capas de infraestructura, productos y servicios capaces de evadir los controles de seguridad tradicionales, como los productos basados en firmas o en heurísticas clásicas.

El enfoque actual de seguridad de la información debe evolucionar hacia un modelo más agresivo y dinámico basado en el conocimiento profundo de este tipo de amenazas para defender nuestra infraestructura e información.

Objetivos

Counter Threat Intelligence - Bootcamp ofrece a los profesionales de la seguridad de información acceso a una nueva mentalidad a la hora de tratar la inteligencia y hacer frente a las amenazas emergentes. Esta visión analítica proporciona a los analistas y responders de la capacidad de detectar y defenderse contra las nuevas amenazas en Internet, mientras que todavía están madurando.

Finalmente el objetivo de **Counter Threat Intelligence - Bootcamp** es el de proporcionar metodologías prácticas y proactivas que den visibilidad sobre las nuevas amenazas sofisticadas y evasivas.

A quién va dirigido

Este Bootcamp no pretende ser un manual académico sobre fundamentos de seguridad y amenazas. No busca ceñirse a una estructura rígida, sino ir evolucionando desde una visión básica, hacia un entendimiento más profundo de las amenazas y presentar distintas técnicas para mantenernos un paso por delante.

Son bienvenidas al training todas aquellas personas que tengan interés en el funcionamiento de las amenazas en Internet y cómo operan las personas que hay detrás de dichas amenazas.

Durante el training se aplicarán técnicas de Reversing, Exploiting/Pentest y Programación para analizar y realizar el seguimiento de amenazas. Se requerirán conocimientos básicos previos en las áreas mencionadas.

Sobre los autores

Jorge Capmany

Jorge es un entusiasta y profesional de la seguridad con más de una década de experiencia a sus espaldas.

Ha desempeñado funciones en varios roles (pentester, respuesta a incidentes e intelligence) en entornos exigentes, donde ha podido ver (y limpiar) bastantes tipos de malware. En la actualidad se dedica a la respuesta a incidentes e inteligencia en una organización centroeuropea.

Jorge es miembro fundador de MLW.RE (Non-Profit-Organisation) la cual está focalizada en investigar y compartir el conocimiento sobre amenazas en Internet con organizaciones y fuerzas de seguridad de diversos países.

Manu Quintans

Malware Researcher vinculado desde hace muchos años a la escena como colaborador de grupos DC4420-Defcon (UK), Hacktimes.com o MalwareIntelligence, entre otros.

Ha desarrollado su experiencia en diferentes sectores tecnológicos adquiriendo conocimientos en diversas disciplinas relacionadas con la seguridad de la información.

Durante su carrera, ha tenido la oportunidad de trabajar en equipos de respuesta a incidentes en zonas como Oriente Medio, Estados Unidos y Europa, siempre centrado en reversing y el análisis de amenazas. En la actualidad se dedica a investigar amenazas relacionadas con Malware e Intelligence .

Además cabe resaltar que es miembro fundador de MLW.RE (Non-Profit-Organisation) la cual está focalizada en investigar y compartir el conocimiento sobre amenazas en Internet con organizaciones y fuerzas de seguridad de diversos países.

Requisitos

Conocimientos y aptitudes

Conocimientos básicos de:

- Análisis de Malware
- Reversing
- Exploiting
- Redes
- Sistemas Operativos
- Programación: nodejs, python, asm, c

*No se requieren conocimientos avanzados los puntos enumerados anteriormente. Como ya se ha comentado se empezarán todas las temáticas desde 0 y se avanzará según el ritmo general de la clase.

Requisitos técnicos

- Para el correcto funcionamiento de los labs será necesario que los alumnos dispongan de equipos con las siguientes características o similares.

- Equipo portátil con VMWARE o Virtualbox. **(Se recomienda VMWARE ya que algunas prácticas se realizarán con este sistema de virtualización.)**
- 4GB de RAM mínimo y para correr 2 máquinas virtuales al mismo tiempo.
- Sistema operativo con arquitectura de 64bits.
- Sistema operativo Linux like*

Contenido

Introducción

Durante el bootcamp se trabajará sobre una misma metodología pero con diferentes entornos de trabajo.

- Los siguientes puntos pueden variar en función de la dinámica del grupo de trabajo.

- Todos los asistentes irán al mismo ritmo y no se avanzará en los temas hasta que el grupo haya cumplido en sus totalidad los objetivos de cada uno de los puntos.

Agenda

- El training transcurría durante “3 largos días”
- Os recomendamos que os provisionéis de agua, bebidas energéticas, fruta, snacks, etc...

Counter Threat Intelligence Bootcamp

Introducción:

- Conoce a tu enemigo
- Teoría de las amenazas
- Tipos de amenazas
- Evolución de las amenazas
- Estado actual de las amenazas
- Conclusiones. (Estado del arte)

Metodología:

- Intelligence
- Modelado de amenazas
- Ciclo de vida de las amenazas
- Malware Research
- Intelligence Research
- Prevención de fraude, IR, APT's
- Fundamentos de Ingeniería Invers
- Fundamentos de Exploiting

Hands-On Lab Intelligence

- Threat Intelligence
- Inducción al mundo Underground
- Open Source Intelligence
- Intelligence Crawling
- Malware Crawling
- Monitorización de actores
- Monitorización de campañas
- Monitorización de Botnets
- Extracción de indicadores de compromiso IOC's
- Detección de patrones
- Correlación de información
- Procesa tu Intelligence: procesamiento y clasificaci

Hands-On Lab Malware

- Introducción análisis estático
- Antivirus, como, ¿Por qué? Y cuando.
- Fingerprinting.
- Strings
- Yara
- Packers/Crypters
- Introducción análisis dinámico.
- El Debugger
- Análisis de red
- Registro y sistema de ficheros
- Sandboxing, , como, ¿Por qué? Y cuando.
- Tricks & Cheats
- Reporting.

Hands-On Lab Hunting

- Introduccion a la caza de amenazas.
- Buscando.
- Enriqueciendo tus datos
- Tips & Tricks.
- Opsec.

Hands-On Lab Counter OPS

#GreyOPS

- SinkHoling
- Vias de comunicación con CERTs
- Gestion de Abuses

#BlackOPS

- Offensive Tracking
- Atacando infraestructuras de amenazas
- Tú y tú adversario

Costes

Costes

- El coste de la formación es de 1200€
- **IMPORTANTE**: se requiere un mínimo de diez (10) asistentes para que el curso tenga lugar.

Costes

Aquí tienes el detalle de los costes:

CTI BOOTCAMP	Día 1	Día 2	Día 3	Cost (€)
Asistente al CTI Bootcamp	X	X	X	1200€
Con entrada confirmada a RootedCON (10%)				-200 €
Descuento de patrocinio				*TBD*
Coste final (€):				**1200€**
Coste final con entrada a RootedCON (€)				**1080€**

Contacto

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#RC17**
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rooted y #RC17*

/Rooted®

Muchas gracias