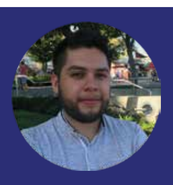
UAD360

Programa de Ponencias

Día 1 - Viernes 10 Junio 2022

Marcos Arjona
Security Technical Program Manager en VirusTotal y Google Cloud

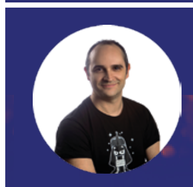


Santiago Rocha
Cyber Threat Intelligence Analyst at Telefonica

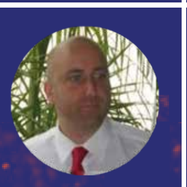
09:30 - 10:30

Dank-OP: Calor rojo y malware en los foros

Actualmente existen millones de espacios en Internet dedicados al intercambio y comercio de malware, generando una cantidad inmensurable de información sobre amenazas que podría usarse en ciberinteligencia. Los foros son plataformas muy usadas para este propósito y contienen valiosos metadatos y una variedad de TTPs usados en ataques reales y que podrían ser la clave para prevenir y anticipar ataques que afecten al "status quo" de las empresas. Por ello presentaremos Dank-Op, un sistema automatizado para extraer información de foros privados, aplicando técnicas anti-bot, enmascarando sus pasos y recopilando todo tipo de indicadores enriquecidos que son analizados para localizar evidencias de preparativos o actividades maliciosas.



Jesús Pacheco
Product Manager en Hispasec



Luciano Miguel
Cyber Threat Intelligence Analyst at Hispasec

10:30 - 11:30

Campaña Anniversary: Resolviendo el Puzzle

Durante el segundo trimestre de 2021 se detectaron los primeros indicios de varias campañas de fraude con difusión internacional que simulaban una promoción especial con motivo del aniversario de múltiples empresas de reconocido prestigio a nivel mundial. Lo que inicialmente parecía tratarse de diversas campañas con distintos objetivos tanto de marcas afectadas como de países destino, se acabó comprobando que en realidad era una única campaña de fraude con la capacidad de adaptar el idioma y la moneda a los usados por las víctimas.
En esta charla se abordarán los aspectos técnicos de la campaña de fraude Anniversaire así como de algunas de las herramientas empleadas para la detección precoz de nuevas infraestructuras y la mitigación de la propia campaña.

Joel Serna
Delivery Consultant en Deloitte

12:00 - 13:00

Hardware Keyloggers around the world

Mostrará el uso de keyloggers físicos en hacking ético/red team desde un enfoque técnico, mostrando su desarrollo, funcionamiento, configuración, etc.
Los asistentes podrán ver los diferentes keyloggers comerciales y el desarrollo de keyloggers propios más avanzados y específicos, usando hardware de bajo coste, con el fin de desarrollar dispositivos keyloggers con otras funcionalidades añadidas: hacking WiFi, BadUSB, ADB, etc.
Finalmente se mostrará otro dispositivo, todavía en desarrollo, capaz de capturar la imagen en vídeo del equipo víctima y controlar el mismo remotamente, consiguiendo un vector de ataque más amplio sin tener las limitaciones que tienen los dispositivos keyloggers/badusb

Alfonso Muñóz
Head of Cybersecurity Unit & cybersecurity research Principal Offensive Security.

13:00 - 14:00

Privacidad en Telegram - Criptografía bajo estudio

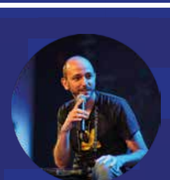
La mensajería instantánea se ha convertido en un pilar fundalmental en las comunicaciones del día a día, personales, corporativas e incluso confidenciales. El auge de la privacidad ha hecho que muchas de estas tecnologías hayan tenido que ser revisadas y actualizadas con protocolos y tecnologías de cifrado. Una aplicación de mensajería instantánea habitual es Telegram usada por actores y objetivos variados. Comprender su seguridad es útil para usarla eficazmente, descartarla por otras alternativas o diseñar nuevos vectores de ataque.
En esta charla analizaremos la privacidad y criptografía utilizada en Telegram y su protocolo de comunicación MTProto 2.0.

Antonio Sanz
Threat Intelligence, incident response & forensics senior analyst

16:00 - 17:00

Respuesta ante incidentes: lo que no te cuentan los libros

La respuesta ante incidentes es uno de los campos más apasionantes de la ciberseguridad. En esta charla intentaremos ir un poco más allá de lo que se cuenta en los libros y en las formaciones "clásicas", aportando consejos prácticos (casi todos aprendidos a palos, es lo que tiene la experiencia), trucos y batallitas que os ayuden a poder apagar vuestros fuegos de la mejor forma posible.



Víctor Álvarez
Staff software engineer en VirusTotal

17:00 - 18:00

YARA: lo que no te cuenta la documentación

YARA es un software open source que se ha convertido en estándar de facto de la industria de ciberseguridad para la detección de malware. Hoy en día YARA se utiliza en múltiples contextos, y se encuentra integrado en productos y soluciones de importantes empresas de este sector. Esta ponencia cuenta la historia de YARA, cómo y por qué surgió, y cuáles fueron las motivaciones de su autor para emprender dicho proyecto.

UAD360

Programa de Ponencias

Día 2 - Sábado 11 Junio 2022

Isaac Agudo
Associate Professor en la Universidad de Málaga y miembro del NICS Lab Research Group

09:30 - 10:30

Éxitos, fracasos y ataques sobre Blockchain

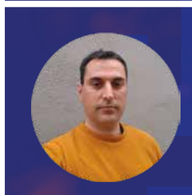
No hay duda de que Blockchain se ha convertido en una tecnología disruptiva, sumando adeptos día a día, y también detractores. Aún está por ver si podrá desplegar todo su potencial pero podemos decir que el camino recorrido hasta hoy ha estado plagado de obstáculos, en forma de fracasos y multiples ataques a diferentes proyectos e infraestructuras, así como éxitos e hitos remarcables. En esta charla haremos un repaso histórico a la evaluación de la tecnología blockchain, centrándonos principalmente en las diferentes amenazas que ha sufrido y cómo estas han afectado a su desarrollo.

David Santos
Independent cybersecurity research and assesments

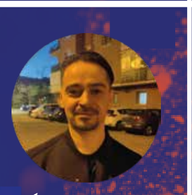
10:30 - 11:30

Prying bad stuff with Kaitai += GCP

Esta charla trata sobre un problema real que me encontré para analizar mucha información de formatos de red antiguos y no había nada hecho para automatizarlo, además no solo se analizaban capturas de red, también llegaban binarios, volcados de discos, etc...
Lo que se hizo fue sin usar herramientas pesadas o librerías de matar moscas a cañonazos que relentizan el procesado, buscar una solución para analizar esa información con kaitai struct (muchísimo más rápido) adaptando y compilando los distintos parsers en raw. Lo mejor es como se llevo a Google Cloud (Functions,Colas de mensajes, Firebase, y alguna cosita mas...todo en el TIER gratuito a priori) para automatizarlo y que se catalogase solo para que alguien no técnico pudiese ver los datos y las relaciones.



Luis Vacas
Cybersecurity analyst, risk advisory en Atento España

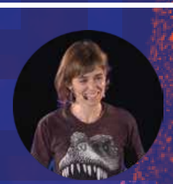


Óscar Alfonso
Líder técnico en GMV

12:00 - 13:00

Hackers Windozers

Charla en la que los ponentes recopilan un variado popurrí de técnicas, herramientas, y otros menesteres relacionados siempre con el hacking y sistemas Microsoft Windows. En algunos casos se repasará alguna técnica o vulnerabilidad conocida clásica y en otros se verá alguna técnica moderna, incluyendo evasión de antivirus, PE Backdooring, y algunos temas relacionados con Active Directory que nos harán replantearnos algunas configuraciones si somos administradores de sistemas.



Mónica Salas
Founder & security analyst en Dinosec

13:00 - 14:00

El curioso incidente del Zero-Trust y el cifrado E2E a medianoche

Los términos "zero-trust" y "End to End Encryption" han pasado a formar parte de la jerga técnica en multitud de servicios de la nube, todos con idea de infundirnos confianza en ellos. Pero... ¿es "zero-trust" y E2E todo lo que reluce? ¿O hay que tener cuidado antes de optar por una solución destinada a proteger nuestros datos más sensibles, sin fiarnos de los mensajes comerciales?
Aplicando el principio "never trust, always verify", la ponencia se orienta a proporcionar, desde un punto de vista teórico pero principalmente apoyándonos en demos, una serie de recursos y técnicas para poder auditar soluciones web que, jactándose de ser seguras y ofrecer cifrado E2E, pueden hacer que nos llevemos algunas sorpresas... Y también ejemplos de implementaciones que sí respetan esos principios.

Chema Alonso
Chief digital officer en Telefónica

16:00 - 17:00

Inteligencia Artificial & CiberSeguridad en la Sociedad

La Inteligencia Artificial en general, y los Cognitives Services en particular, han sufrido una evolución exponencial, el reconocimiento facial, la comprensión lectora, la traducción de textos, pero también la creación de personas con DeepFakes en tiempo real, los bots de conversación general con algoritmos basados en datos masivos como GPT3 o MS Turing, nos llevan a un mundo que está lleno de retos, y lleno de investigaciones y avances tecnológicos por crear. En esta sesión Chema Alonso dará una visión del mundo al que vamos, los retos, y las necesidades de avanzar.

Ismael Valenzuela
Sr. principal engineer. Head of AC3 team en Trellix. Sans author & senior instructor

17:00 - 18:00

Think Red, Act Blue - Mis Estrategias Favoritas de Ciberdefensa

Si algo he aprendido en mis 22 años de experiencia, es que una buena defensa comienza con el conocimiento del adversario. Pero analizar al atacante no sirve de nada si no somos capaces de usar esta información para trazar una estrategia defensiva, y asegurarnos que tenemos suficientes capacidades de protección, visibilidad, detección y respuesta.
Si quieres aprender cuáles son mis estrategias favoritas, no te pierdas esta sesión en la que compartiré algunas de las lecciones más importantes que he aprendido como blueteamer, incluyendo técnicas prácticas y efectivas como el análisis de las herramientas del atacante o ciber-balística, la exploración de datos con Pandas y Jupyter notebooks, o cómo transformar los TTPs en controles accionables.