



JUAN IGNACIO ALBERDI

Vendedor Especialista de Servicios Cloud y Seguridad en Telefónica de Argentina S.A. Investigador Alumno en el Grupo de Investigación en Informática Forense y Sistemas Operativos.

in <http://ar.linkedin.com/in/juanignacioalberdi>

Recientemente incorporado como investigador al Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA. El proyecto final de graduación que están realizando se llama *BIP-M: Búsqueda de Información de Procesos en Memoria*. Es un proyecto de I+D que comenzó a finales del año 2012 para responder a la necesidad de generar conocimiento sobre la memoria, las estructuras que se pueden encontrar en ésta y la información que es posible extraer de sus artefactos. Teniendo como base el conocimiento adquirido, se desarrolló un framework de análisis de memoria que desde su diseño permite su extensión para soportar distintos sistemas operativos y versiones, distintos formatos de archivos de volcado de memoria y nuevas estructuras. De esta manera, se busca contar con una herramienta que facilite la búsqueda y análisis de malware, generar conocimiento sólido sobre la materia y seguir recorriendo este camino para poder responder a las futuras necesidades en el campo.

Además, es actualmente Vendedor Especialista de Servicios de Seguridad y Ciberseguridad, a su vez vendedor especialista y consultor de servicios de IT del datacenter de Telefónica de Argentina S.A. Anteriormente dentro de la misma empresa, desempeñó como líder operativo de los servicios de Atención Telefónica de Emergencias 911 brindados por Telefónica de Argentina S.A. a entes gubernamentales.

¿Por qué participar en el CIBSI / TIBETS?

Por su relevancia y prestigio en el ambiente de la seguridad informática para Latinoamérica, así como también la posibilidad de interactuar con referentes del sector. A su vez, es una gran oportunidad de presentar nuestro trabajo a colegas e intercambiar conocimiento.

En su opinión, ¿cuál es la relevancia

de su investigación en este Congreso?

Hoy en día desde las PyMes hasta las grandes empresas, entidades gubernamentales, usuarios hogareños, etc., poseen sistemas informáticos accesibles desde Internet en su mayoría, redes sociales, smartphones, incluso con el advenimiento de IoT, todo tiende a estar conectado y cada elemento, físico o lógico, es susceptible de vulnerabilidades que pueden ser explotadas con diversos fines. La Seguridad de la Información ha tomado gran relevancia en los últimos años en los cuales empresas líderes del mercado invierten millones de dólares año a año en el desarrollo de nuevas tecnologías (software y hardware) con el objetivo de combatir el ciberdelito, el cual siempre encuentra nuevas formas de realizar un daño. La Seguridad de la Información hoy es una preocupación a nivel global y se está tomando conciencia de ello en todos los ámbitos, aplicando soluciones conocidas y en busca de nuevas, ya sea para prevenir o mitigar ataques, que pongan en riesgo la continuidad de nuestros negocios o incluso afecten nuestro ámbito privado más íntimo.

¿Cuál es el mayor riesgo que tiene una sociedad como la Iberoamericana en materia de ciberseguridad?

En la actualidad, si bien hay ataques a la reputación y marca, fraudes online, ataques de disrupción del negocio, el

foco no está puesto sobre Latinoamérica lo cual es una ventaja ya que nos da tiempo desarrollarnos más en la rama de la ciberseguridad. Lamentablemente no somos conscientes aún del riesgo al cual nos enfrentamos y en su mayoría, se sigue pensando que estamos exentos de estos ataques. Tenemos la oportunidad de generar conciencia con el tiempo suficiente para tomar medidas de seguridad que acompañen nuestros negocios y el día a día como simples usuarios.

¿Cómo ve a Latinoamérica en materia de seguridad de la información frente al resto del mundo?

Latinoamérica en general está recién comenzando a interiorizarse en la materia (en comparación con otros países más avanzados como EEUU) y comprendiendo que la información que se encuentra en la red es un activo que debemos proteger. Grandes empresas ya son conscientes de ello están avanzando en incorporar sistemas y/o servicios que aumenten su nivel de seguridad y mejor aún, han adoptado alguna política para generar conciencia en la sociedad como así también en el ambiente privado y público. Creo que aún nos falta mucho camino por recorrer, pero ya lo hemos comenzado a transitar.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

Quitando el Velo a la Memoria: Estructuras Ocultas y Malware BIP-M, un Framework de Extracción de Información de Memoria. *Short Paper*

Miércoles, 11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras críticas.