GONZALO RUIZ DE ANGELI

Analista de Sistemas de Planificación, Programación e Información en Telefónica de Argentina S.A. Investigador Alumno en el Grupo de Investigación en Informática Forense y Sistemas Operativos.

@ruizgon

http://ar.linkedin.com/in/gonzaloruizdeangeli

Investigador en el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la Universidad FASTA en Mar del Plata, Argentina.

El proyecto final de graduación que estamos 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.

Últimas publicaciones:

Proceso Unificado de Recuperación de Información (PURI) en Redes Informáticas. Autores: Ing. Ana Haydée Di Iorio, Ing. Hugo Curti, Ing. Fernando Greco, Ing. Juan Ignacio Iturriaga, Sr. Gonzalo Ruiz De Angeli, Ing. Ariel Podestá, Ing. Martín Castellote, Ing. Bruno Constanzo Congreso 44JAIIO (44º Jornadas Argentinas de Informática) Fecha: 30/08/2015
Url: http://44jaiio.sadio.org.ar/
ISSN: 2451-7526

¿Por qué participar en el CIBSI / TIBETS?
Es un congreso de gran importancia en la región en lo que respecta a Seguridad Informática, por lo que es un honor poder participar del mismo, mostrando nuestro trabajo a otros colegas y conociendo más a fondo otras investigaciones en la materia.

En su opinión, ¿cuál es la relevancia de su investigación en este Congreso?

Nuestra investigación se basa en el conocimiento de los diferentes artefactos que se pueden encontrar en memoria y la relación que puede existir entre ellos. Dichos artefactos, en su mayoría, sólo existen en la memoria y que proveen información de gran importancia en una investigación de informática forense. El software mal intencionado (malware), lleva a cabo su trabajo en memoria, por lo que la búsqueda de estructuras que "a simple vista" están ocultas como, por ejemplo, los procesos ocultos pueden dar indicios de la presencia de rootkits en un sistema o algún otro tipo de malware. Es por eso que nuestro trabajo apunta a generar conocimiento sobre la temática, entendiendo que las nuevas formas de amenazas dejan su rastro en memoria, en vez de dejarlos en otros medios como el disco rígido.

¿Cuál piensa que será el devenir de la Seguridad de la Información?

La informática, por su naturaleza, es víctima de amenazas que evolucionan a la par del desarrollo tecnológico, por lo que desafían constantemente la Seguridad de la Información. Actualmente, cada vez son más los casos donde la información no se encuentre almacenada en dispositivos informáticos y, casi en igual medida, donde dicha información es accesibles desde una red o desde Internet. Es sumamente importante entender este contexto y su evolución, resultando imprescindible informarse, investigar y desarrollar en pos de generar conocimiento y herramientas que permitan evitar ataques informáticos, detectar presencia de software malintencionado (malware) o estar preparados para poder tener una respuesta rápida y efectiva a un incidente (Incident Response).

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

El mayor riesgo es no estar preparados. El mundo cambia de manera acelerada, sobre todo en lo que respecta a como la información se almacena y comparte. Para adaptarse a esto, se debe tener conocimiento sobre las amenazas existentes, cómo detectarlas o cómo responder ante un ataque. Es por eso que hablar de seguridad informática, ciber defensa e informática forense tiene que ser una práctica del día a día, en todos los ámbitos, propiciando el debate, la investigación y la capacitación en estas ramas.

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

En los últimos años, tanto Latinoamérica como el resto del mundo han tomado una mayor conciencia de la importancia de la seguridad de la información, de los riesgos que existen y de las medidas que se deben tomar. A nivel regional y en línea con este pensamiento, se intenta alcanzar cada día un mayor conocimiento sobre la materia y esto se hace cada vez más notorio, tanto en el ámbito privado, como en el público.

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.

Universidad FASTA - ARGENTINA
Grupo de Investigación en Informática Forense
http://www.ufasta.edu.ar
investigacion.ingenieria@ufasta.edu.ar

El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) es una iniciativa conjunta de la Universidad FASTA, el Ministerio Público Fiscal de la Provincia de Buenos Aires y la Municipalidad de General Pueyrredon, que nuclea en la ciudad de Mar del Plata a un equipo interdisciplinario de investigadores científicos y tecnológicos, profesionales y técnicos altamente calificados, con el objeto de desarrollar soluciones a las demandas en el campo de la Informática Forense y su aplicación.
El Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab) es la sede del Grupo de Investigación en Informática Forense y Sistemas Operativos de la Facultad de Ingeniería de la Universidad FASTA.

Con la Organización de