Proyectos de la Secretaría de Investigación, Internacionales y Posgrado

Convocatoria: PROYECTO SIIP TIPO 1 BIENAL 2019
Titulo: Aplicación de Redes Neuronales Profundas para la Detección Automática de Nombres de Dominio generados de manera aleatoria

Director: CATANIA, CARLOS
Codirector: MARCHETTA FERNANDEZ, MARTIN GONZALO
Área: INFORMATICA-REDES DE COMPUTACION, TELEPROCE

Resumen de Proyecto:

En el contexto de la seguridad de redes de datos, un nombre de dominio generado de manera algorítmica (DGA, de sus siglas en inglés) es utilizado por el software malicioso (malware) para generar de manera dinámica un gran número de nombres de dominios de manera pseudo aleatoria, y luego utilizar un subconjunto de estos como parte del canal de Comando y Control (C&C). Este canal podrá luego ser utilizado para indicar, a las máquinas infectadas con el malware, diferentes acciones maliciosas como ser SPAM, campañas de Clicks, Denegación de servicio, etc. El presente proyecto propone el desarrollo de algoritmos de detección de DGA mediante la utilización de algoritmos de aprendizaje de máquinas en general y las redes neuronales profundas en particular. En los últimos 10 años la utilización de redes neuronales profundas ha sido la causa detrás de los mayores avances en el reconocimiento automático de imágenes, audio, video y análisis de texto. Se espera que la aplicación de redes neuronales profundas para el aprendizaje de los patrones comunes a los DGA permita desarrollar herramientas de detección no solo con una baja tasa de falsos positivos sino también con la capacidad de operar en tiempo real. Esto último resulta fundamental para lidiar con las amenazas de seguridad de hoy.

Palabras Claves : 1- Redes Neuronales 2- Seguridad Informatica 3- Aprendizaje de Máquinas

Titulo (Inglés): An application of Deep Neural Networks for automatic detection of randomly generated Domain Names

Resumen de Proyecto (inglés):

A domain generation algorithm (DGA) is used to dynamically generate a large number of pseudo random domain names and then selecting a small subset of these domains for the Command Control (C&C) communication channel. The idea behind the dynamic nature of DGA was to avoid the inclusion of hard-coded domain names inside malware binaries, complicating the extraction of this information by reverse engineering. The C&C channel can be used for instructing the botnet to take different malicious actions such as SPAM, click campaign, DDOS, etc. The present project proposes the development of an algorithm for DGA detection based on machine learning algorithms. In particular, we propose the use of Deep Neural Networks. In the last 10 years, deep learning techniques has been the cause behind the major advances in the automatic recognition of images, audio, video and text. We expect the ability of deep neural networks for recognizing common patterns in DGA facilitates the development of a detection tool. A tool what will operate not only with a low false positive rate but also in real time. Both requirements are fundamental for dealing with today security threats.

Palabras Claves : 1- Neuronal Networks 2- Network Security 3- Machine Learning

EQUIPO DE TRABAJO

CATANIA, CARLOS

harpomaxx@gmail.com	Director
FACULTAD DE INGENIERIA	

PALAU, FRANCO DAVID

palaufranco12@gmail.com	Estudiante de Grado
UNIVERSIDAD NACIONAL DE CUYO	

CAFFARATTI, GABRIEL

gcaffaratti@fing.uncu.edu.ar	Becario de Posgrado
CENT.DE ESTUDIOS Y APLICACIONES LOGISTICAS	

GUERRA TORRES, JORGE LUIS

jguerra@uncu.edu.ar	Becario de Posgrado
FACULTAD DE INGENIERIA	

CORTÉS, LUCÍA

luciacortes5519@gmail.com	Investigador en formacion
FACULTAD DE INGENIERIA	

REZINOVSKY, ALFREDO DANIEL

alfrenovsky@gmail.com	Integrante de entidad publica ó privada
FACULTAD DE INGENIERIA	

MARCHETTA FERNANDEZ, MARTIN GONZALO

mmarchetta@fing.uncu.edu.ar	Codirector
FACULTAD DE INGENIERIA	