UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

Detecting Network Beaconing with Convolutional Networks and Zeek Logs

Ignacio Arnaldo Lucas
Corelight (https://corelight.com/)

Facultad de Informática
On line - https://meet.google.com/qkb-zpud-cgg - miércoles 8 de noviembre de 2023 - 13:00
Entrada libre hasta completar el aforo

Resumen:

We will introduce a robust approach to detect network beaconing across DNS, SSL, and HTTP using Zeek logs. We will start by analyzing patterns exhibited by C2 frameworks such as Meterpreter, Empire, Sliver, or Caldera. The wide range of observed behaviors will motivate a machine learning approach that consists in a) generating synthetic data that accounts for different beaconing frequencies, jittering, and latencies, and b) training a Convolutional Neural Network that analyzes the intervals between activities. Finally, we will showcase real-world detections and equip the audience with all the tools needed to apply the approach to their data.

Sobre Ignacio Arnaldo Lucas:

I am lucky to work as a principal data scientist at Corelight with the creators and maintainers of Zeek (https://zeek.org/), the open source network security monitoring tool. My focus is to use machine learning to solve network security challenges (and there are quite a few!). I am interested in building systems that can put machine learning to use, threat detection and pentesting. Before Corelight, I worked at PatternEx, an early stage AI startup focused on threat detection. In another life, I was a researcher at CSAIL, MIT and received my PhD in computer science from Universidad Complutense in 2013.