DeepSec 2017 Talk: Malware Analysis: A Machine Learning Approach – Chiheb Chebbi

Posted on **August 26,2017** by **sanna**

Software has a character. It can be beneficial. It can also be malicious. A networked business world and the Internet of connected individuals make life for malicious software, also known as malware, easier. Just like international travel facilitates the spread of diseases and parasites, the networked globe is a big advantage for malware. Researcher can hardly keep up with the numbers of detected viruses, worms, and trojan horses. So why not let machines look for malware on their own? Certainly automation already benefits the hunt for malicious code. Chiheb Chebbi has some ideas that can help.

> Threats are a growing problem for people and organizations across the globe. With millions of malicious programs in the wild it has become hard to detect zero-day attacks and polymorphic viruses.This is why the need for machine learning-based detection arises. A good understanding of malware analysis and machine learning models is vital to ensure taking wise decisions and building a secure environment by being capable of correctly identifying and mitigating such potential threats. During the talk the audience will be introduced to machine learning models in cyber security and explore two different cutting edge models to detect malware and threats as case studies:
>
> First, 'Hidden Markov Models (HMM) for malware classification' which is a very useful technique to detect certain challenging classes of malware, starting from the mathematics behind Markov chains, to HMM models training and evaluating clustering results.
>
> The second case study is deep learning malware detection. The audience will dive deep into artificial neural networks and will learn how to build and optimize deep learning networks using machine learning libraries and tools (Tensorflow, Theano, Keras, Scikitlearn, etc.) and will discover how deep learning can be designed for intelligent malware detection.

We are looking forward to see his talk. If you have any connections to malware, you should probably attend, too. .

Image not found http://blog.deepsec.net/wp-content/uploads/2017/08/chihebchebbi.png

Chiheb Chebbi is an InfoSec enthusiast and Security Researcher with experience in various aspects of Information Security, focusing on investigation of advanced cyber attacks and researching cyber espionage and APT attacks.His core interest lies in "Web Applications security" and "Industrial Control Systems". 2016 he was included in the Alibaba Security Research Center Hall Of Fame. He gave talks at the 4th Annual BSides Tampa IT Security Conference 2017 Florida USA, Black Hat Europe London 2016, NASA Space

Apps Challenge 2015 and 2016, Global Windows Azure Boot camp 2014: Revolutionizing Education using cloud Computing, International Institute of technologies Sfax 2014: Introduction to Cloud Computing, Research Center in Informatics, Multimedia and Digital Data Processing of Sfax 2014: the future of Software industry.

Posted in:Conference,Security | Tagged:DeepSec,Machine Learning,Malware,Research,Talk | With 0 comments