Fighting Malware with Artificial Intelligenge and Deep Learning

BSIDES SÃO PAULO

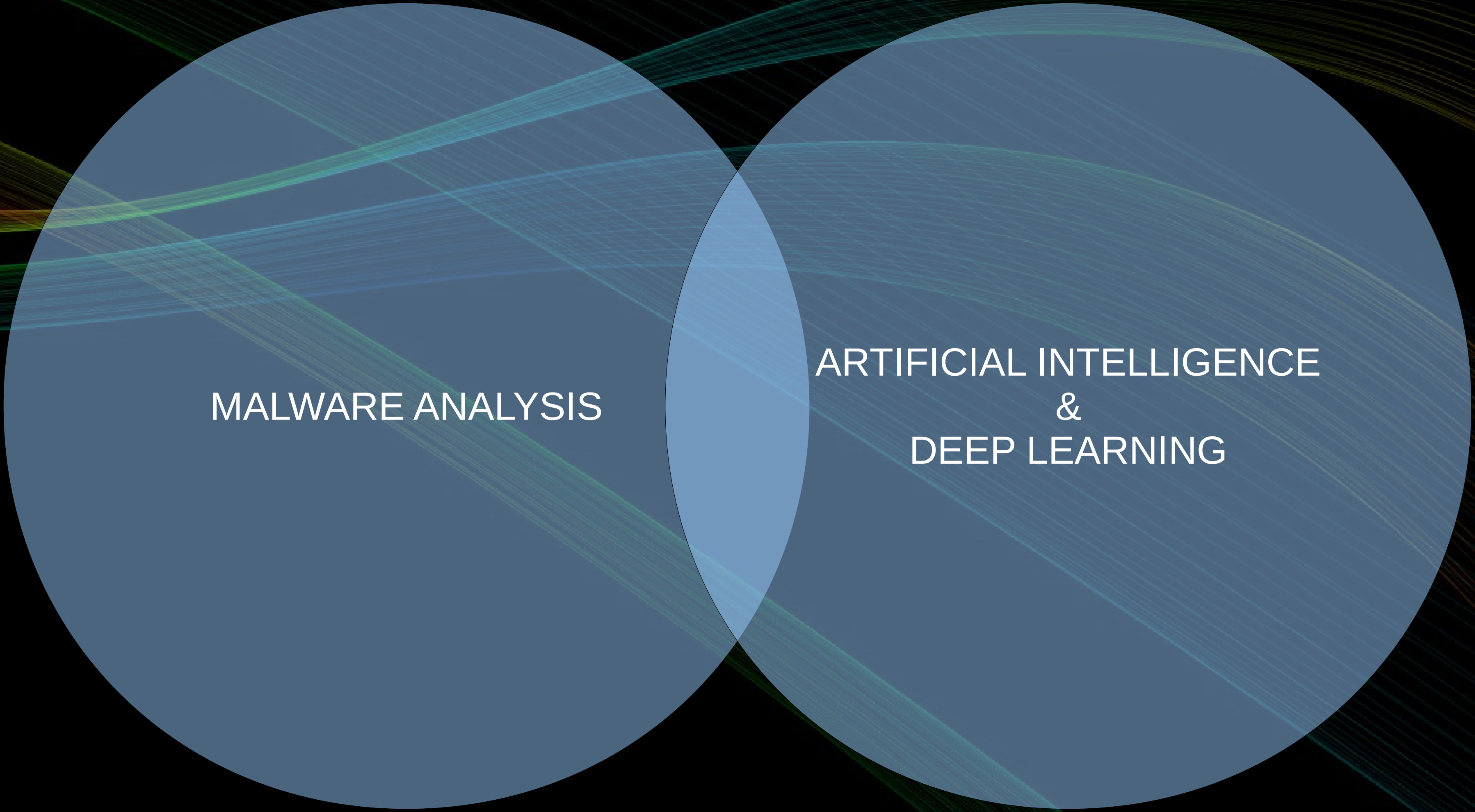
Angelo Oliveira

alpha@angeloliveira.net

Who Am I?

- 20+ years in the IT field
- Ethical Hacker (Applications)
- Offensive Security Certified: OSCP, OSCE and OSWP
- Independent Malware + AI Researcher
- Masters Degree (Unconventional Computing) and PhD student (Artificial Intelligence)
- Connect! Linkedin: www.angeloliveira.net

Introduction



MALWARE ANALYSIS

ARTIFICIAL INTELLIGENCE
&
DEEP LEARNING

AUTOMATIC MALWARE DETECTION AND CLASSIFICATION

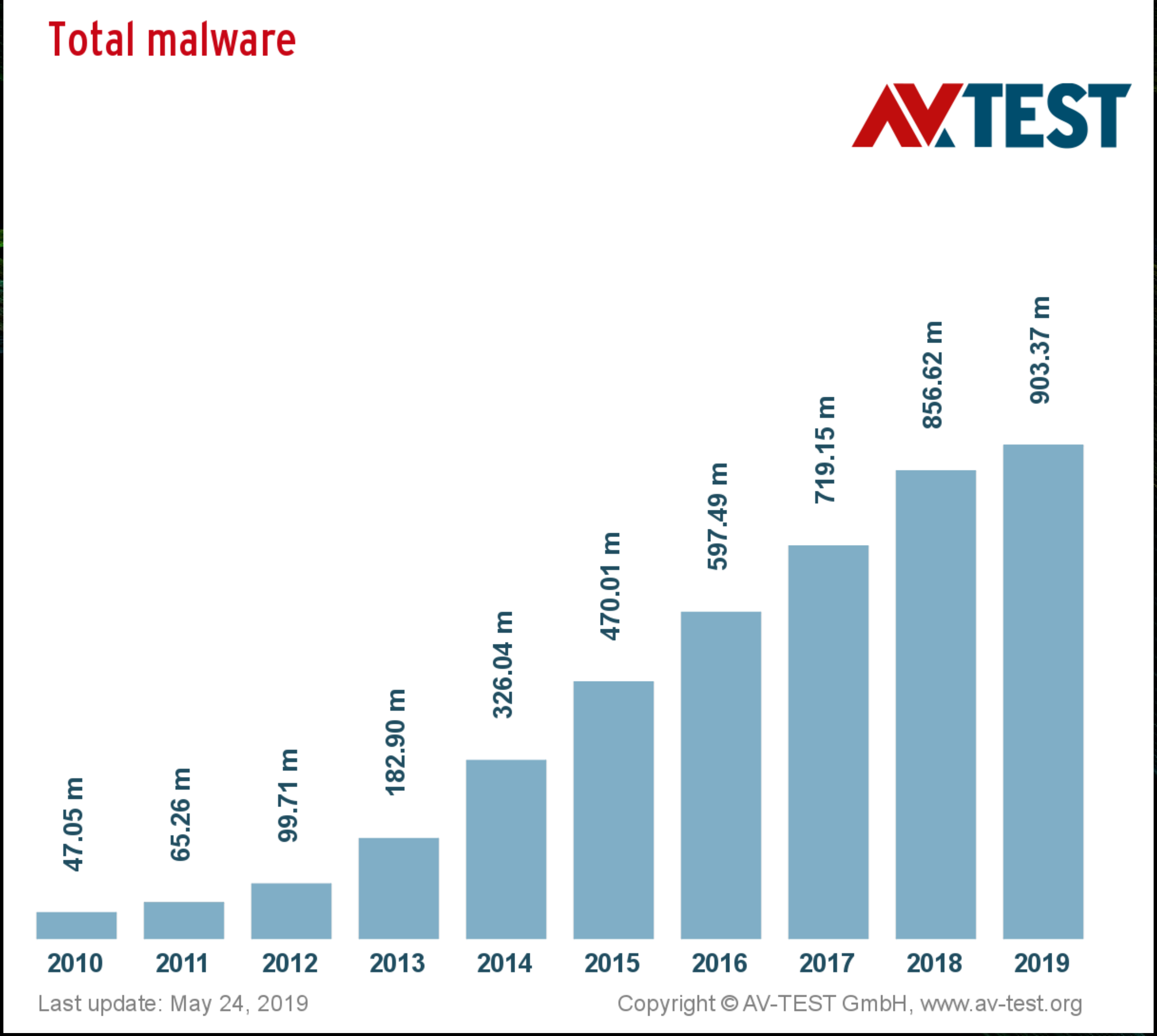
What is Malware?

- Any software intentionally designed to cause damage to a system (hardware or software) or user
- In most cases, the main motivation of malware creators is to make money: Ex. Wannacry
- In some cases, industrial espionage and cyberwarfare: Ex: Stuxnet

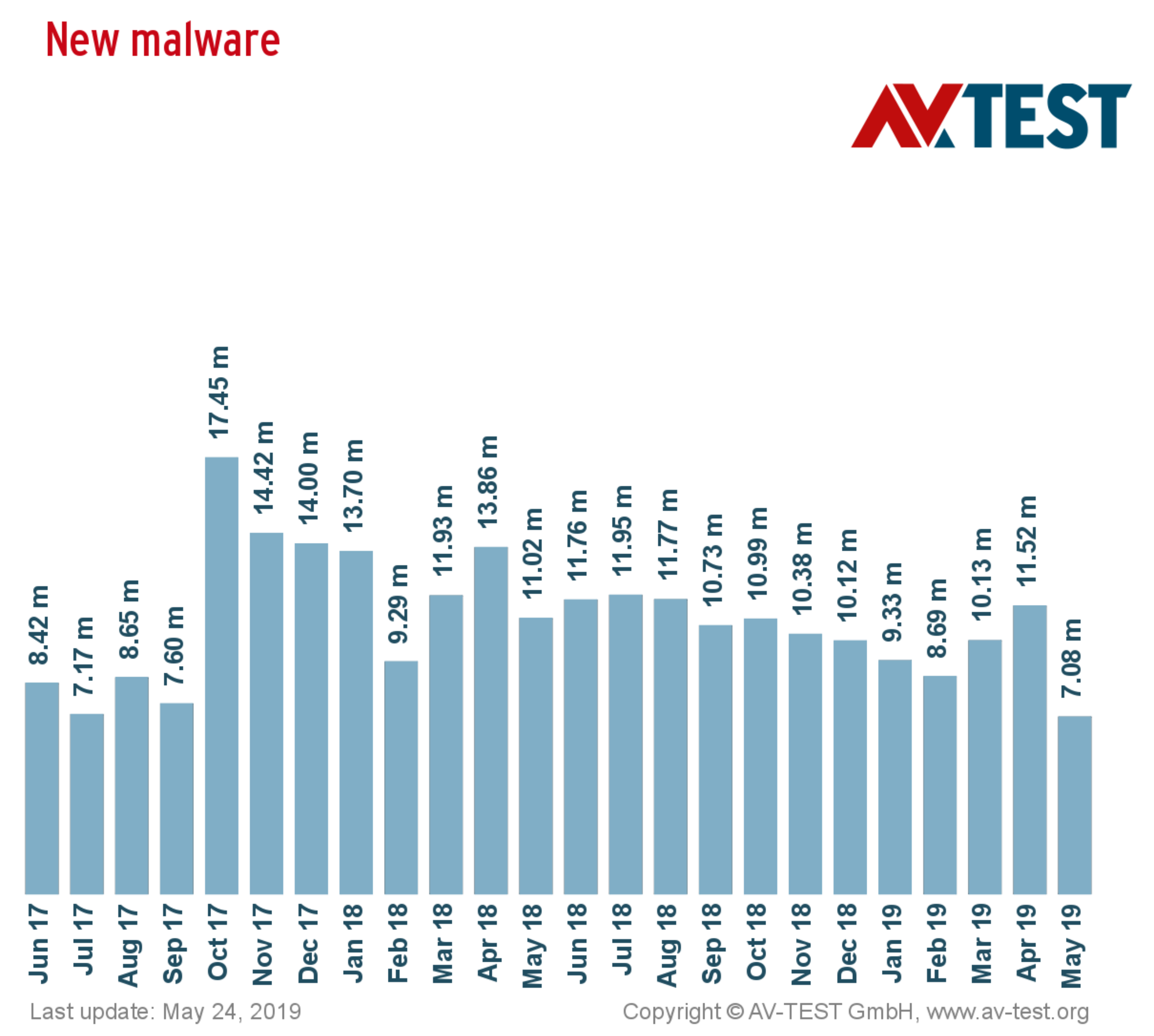
Malware Families

- Malware can be loosely classified into families
- Each family has a set of behaviors associated
- A malware can belong to several families
- Virus: Infect files
- Worms: Self-replicants
- Trojans: Hide inside legitimate programs
- Ransomware: Demands a ransom from you to get things back on track
- Etc, etc

Statistics


Total malware
AV-TEST
47.05 m
65.26 m
99.71 m
182.90 m
326.04 m
470.01 m
597.49 m
719.15 m
856.62 m
903.37 m
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
Last update: May 24, 2019
Copyright © AV-TEST GmbH, www.av-test.org

Statistics


New malware
AV-TEST
8.42 m
7.17 m
8.65 m
7.60 m
17.45 m
14.42 m
14.00 m
13.70 m
9.29 m
11.93 m
13.86 m
11.02 m
11.76 m
11.95 m
11.77 m
10.73 m
10.99 m
10.38 m
10.12 m
9.33 m
8.69 m
10.13 m
11.52 m
7.08 m
Jun 17
Jul 17
Aug 17
Sep 17
Oct 17
Nov 17
Dec 17
Jan 18
Feb 18
Mar 18
Apr 18
May 18
Jun 18
Jul 18
Aug 18
Sep 18
Oct 18
Nov 18
Dec 18
Jan 19
Feb 19
Mar 19
Apr 19
May 19
Last update: May 24, 2019
Copyright © AV-TEST GmbH, www.av-test.org

Malware Analysis

- Understand malware behavior (how it works, what it does) by analysing its structure, assembly code and execution in order to take preventive measures (defensive) or incident response.
- The most common methods for malware analysis are: Static and Dynamic Analysis

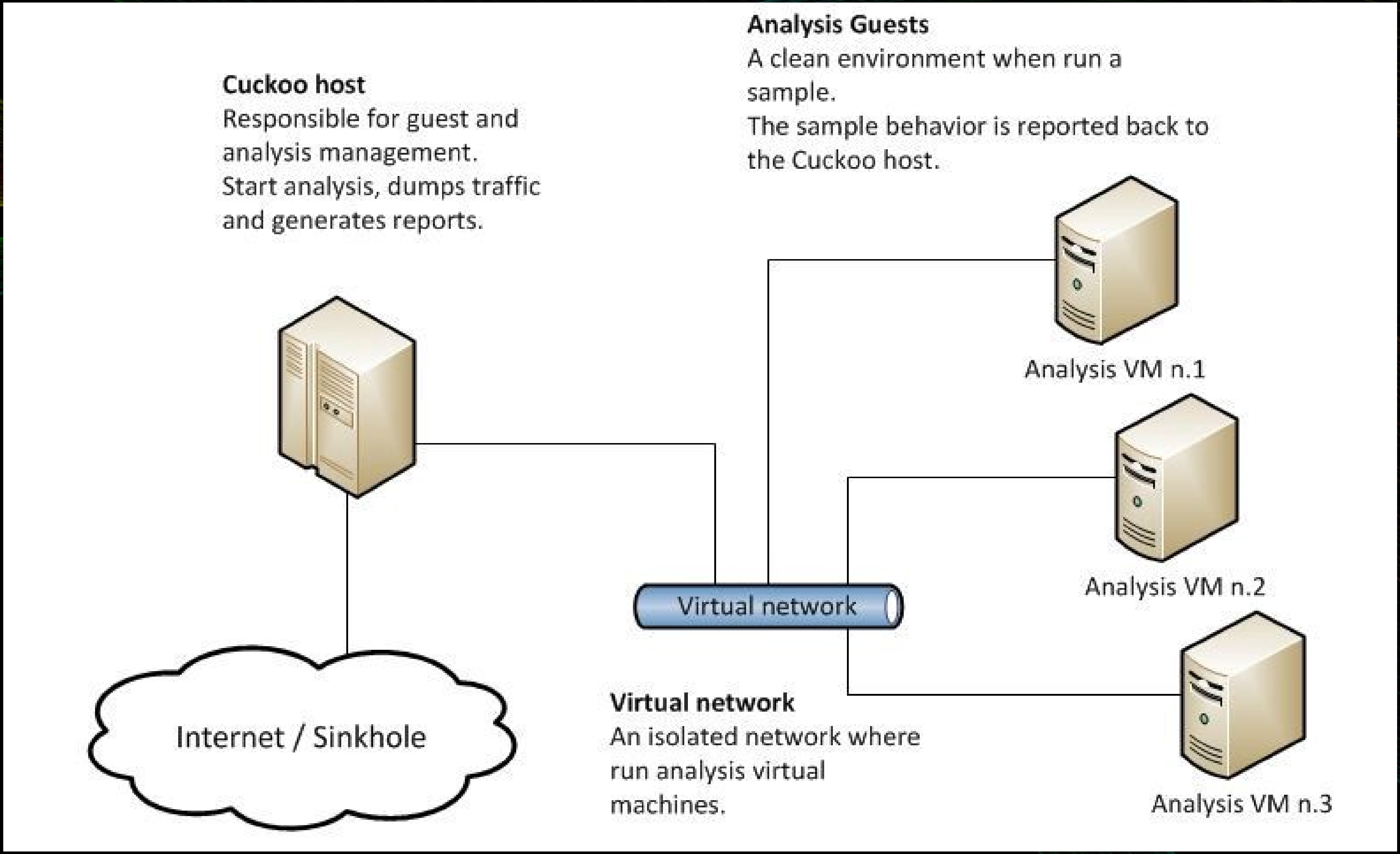
Static Analysis

- What kind of information can we get without executing the malware?
- Static Properties (Hash, file structure, sections, imported functions, etc)
- Reverse Engineering: Disassemble the code using tools such as IDA Pro and analyse it end-to-end: Hard, time consuming and usually impractical (packers)

Dynamic Analysis

- What kind of information can we get by executing the malware?
- API calls: Interactions with the OS: Processes, Memory, I/O, Registry, Kernel, etc
- Network activity
- Dropped files
- Screenshots
- Etc, etc
- How to perform Dynamic Analysis: Sandbox!

Cuckoo Sandbox



Cuckoo host
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

Analysis Guests
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.

Virtual network
An isolated network where run analysis virtual machines.

Source: https://medium.com/@warunikaamali/cuckoo-sandbox-installation-guide-d7a09bd4ee1f

Where to find Malware?

- https://thezoo.morirt.com/
- https://virusshare.com/
- Google: malware repository

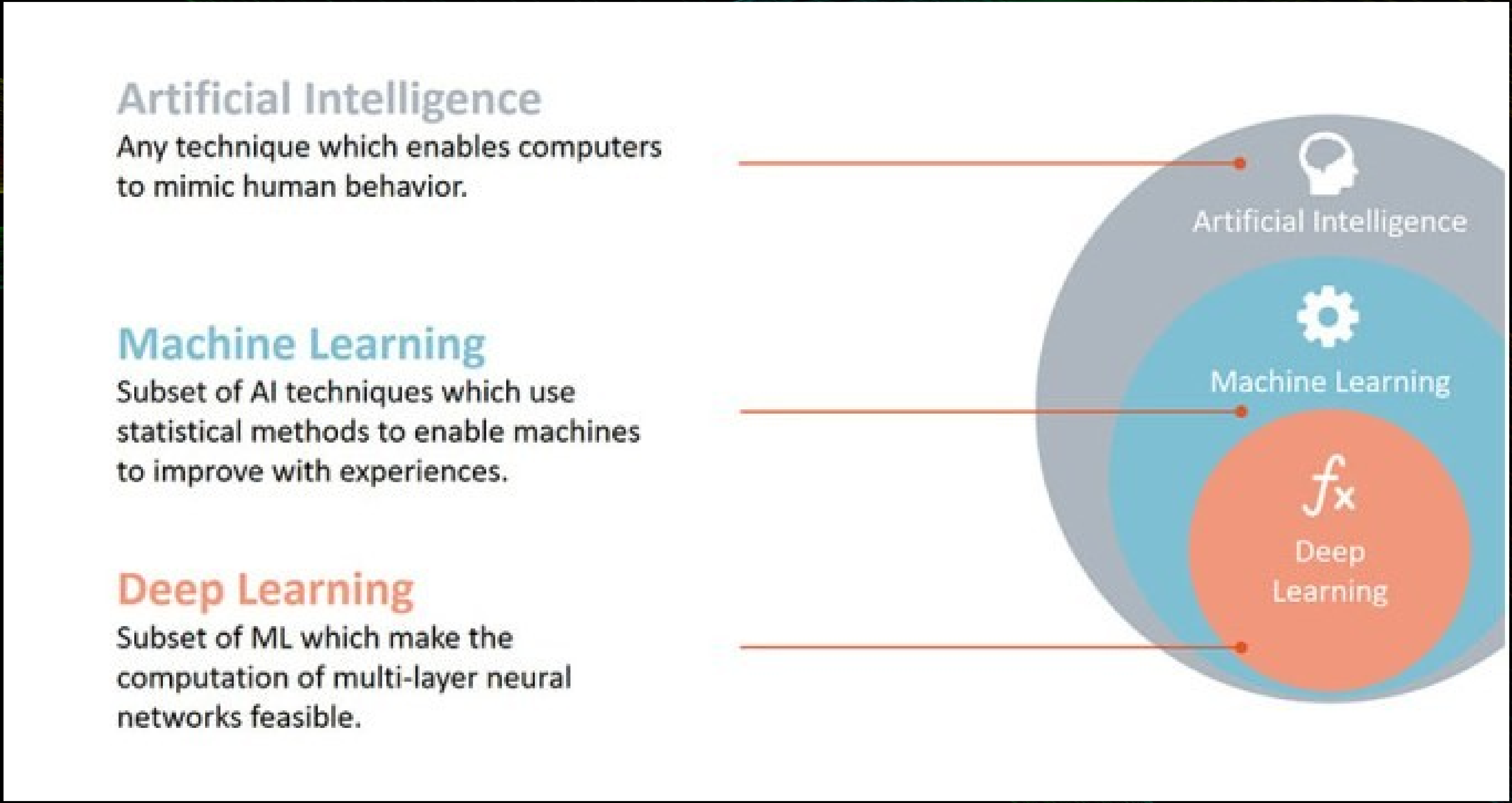
Where to learn more?

- Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware
- Blackstorm Security Trainings (Alexandre Borges): www.blackstormsecurity.com

Artificial Intelligence (AI) and Deep Learning (DL)

- Artificial Intelligence: Using programs to do cognitive work that usually requires a human
- Machine Learning (ML): Programs with the capability to learn by example as opposed to explicit instructions. Different programming paradigm
- Deep Learning: Class of Machine Learning algorithms that take advantage of multiple layers of processing, better algorithms, huge amounts of data and computational power

IA x ML x DL



Artificial Intelligence

Any technique which enables computers to mimic human behavior.

Machine Learning

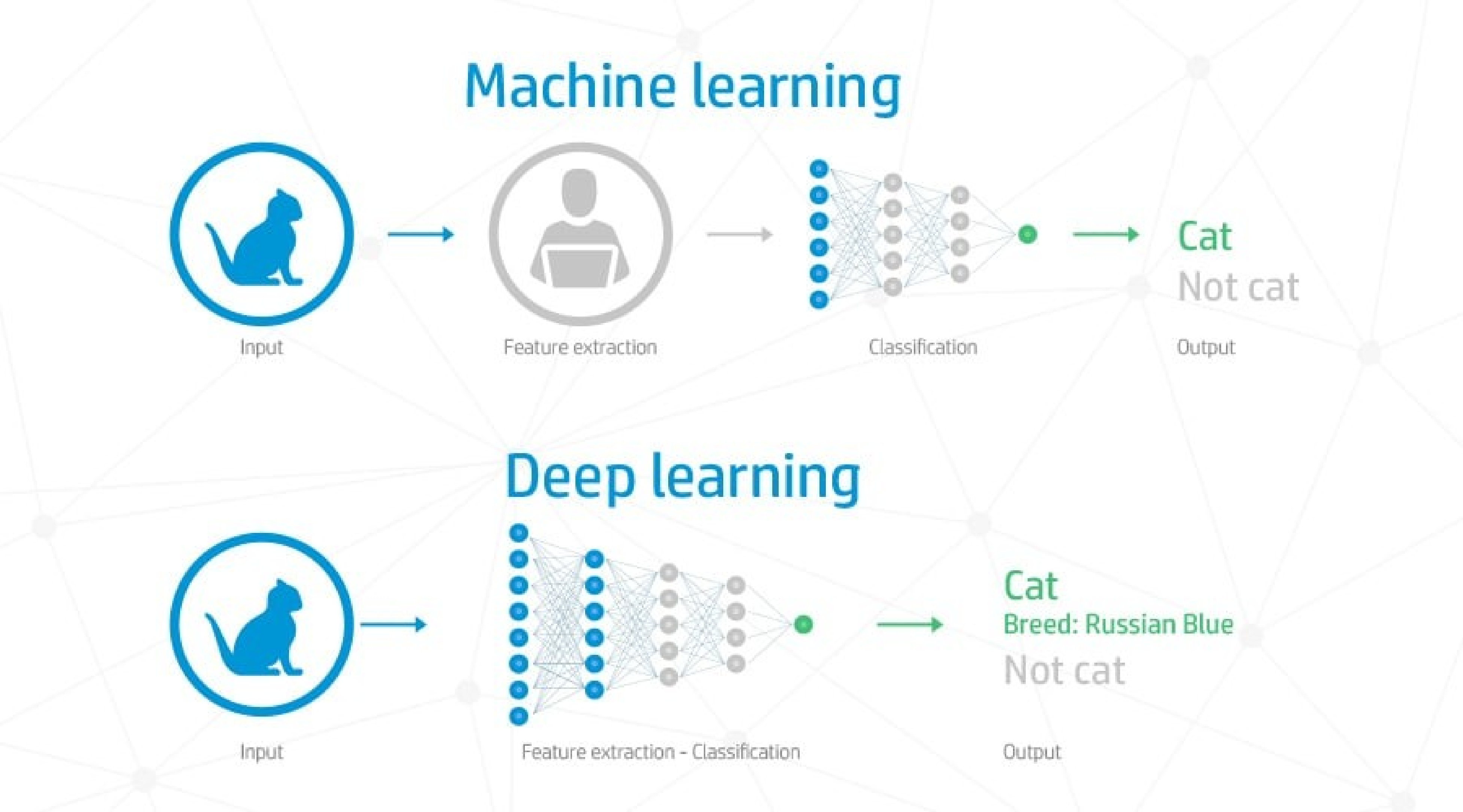
Subset of AI techniques which use statistical methods to enable machines to improve with experiences.

Deep Learning

Subset of ML which make the computation of multi-layer neural networks feasible.

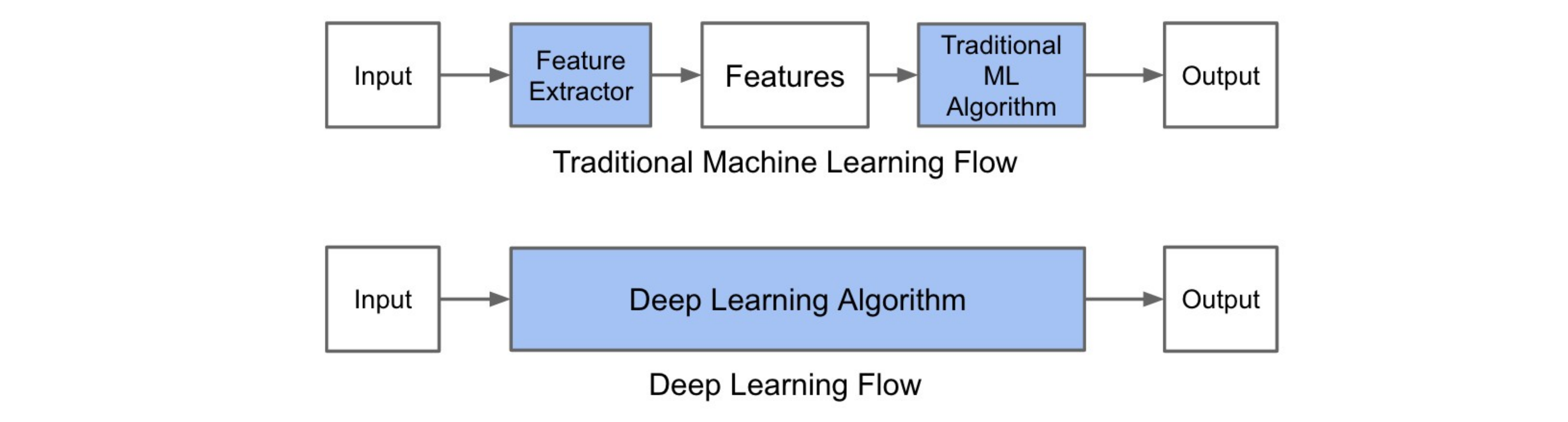
Source: https://www.quora.com/Which-is-better-to-start-AI-ML-or-DL

ML x DL



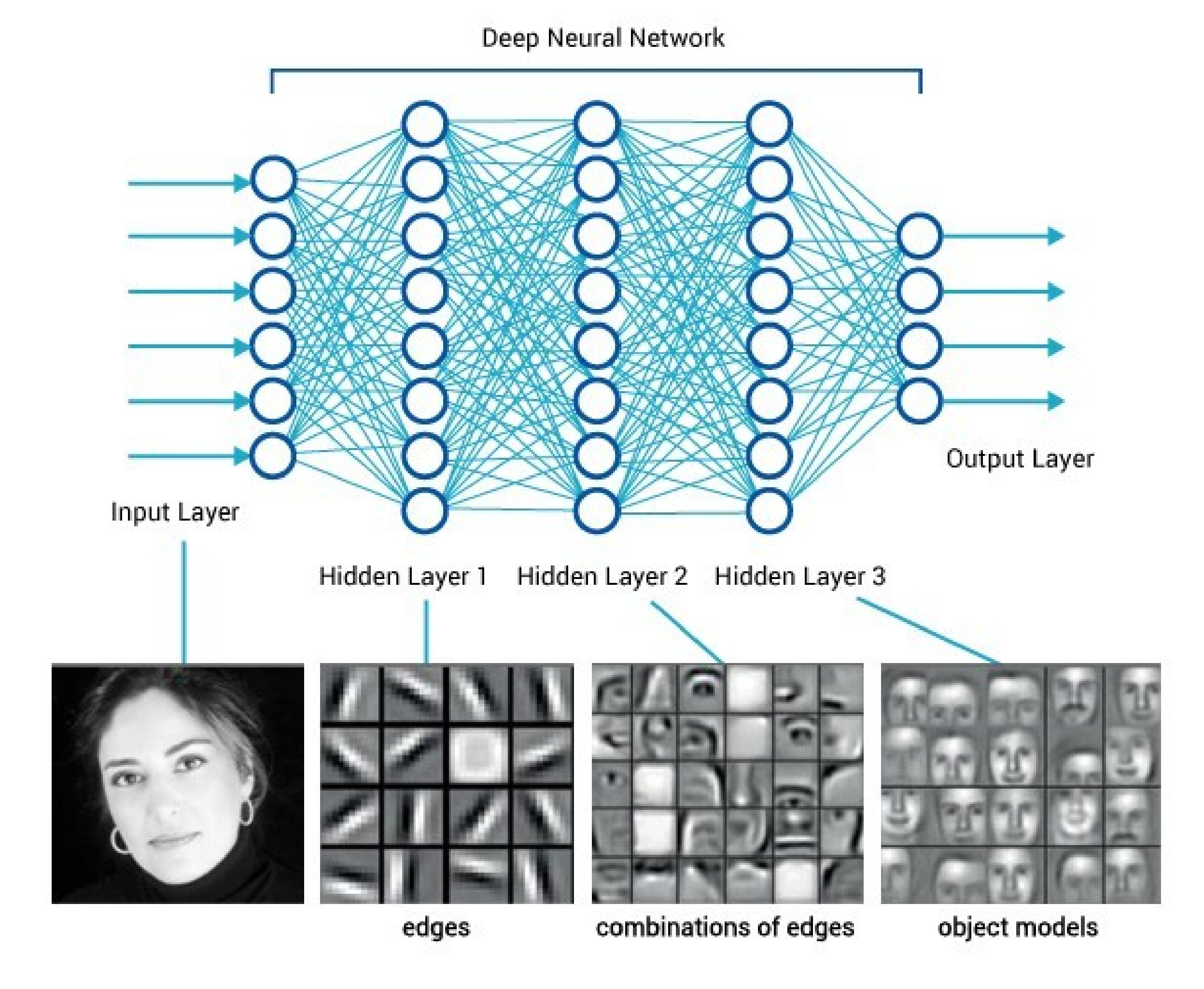
Source: https://www.net-cloud.com/blog/machine-learning-and-deep-learning-101/

ML x DL


Input
Feature Extractor
Features
Traditional ML Algorithm
Output
Traditional Machine Learning Flow
Input
Deep Learning Algorithm
Output
Deep Learning Flow

Deep Neural Networks (DNN)

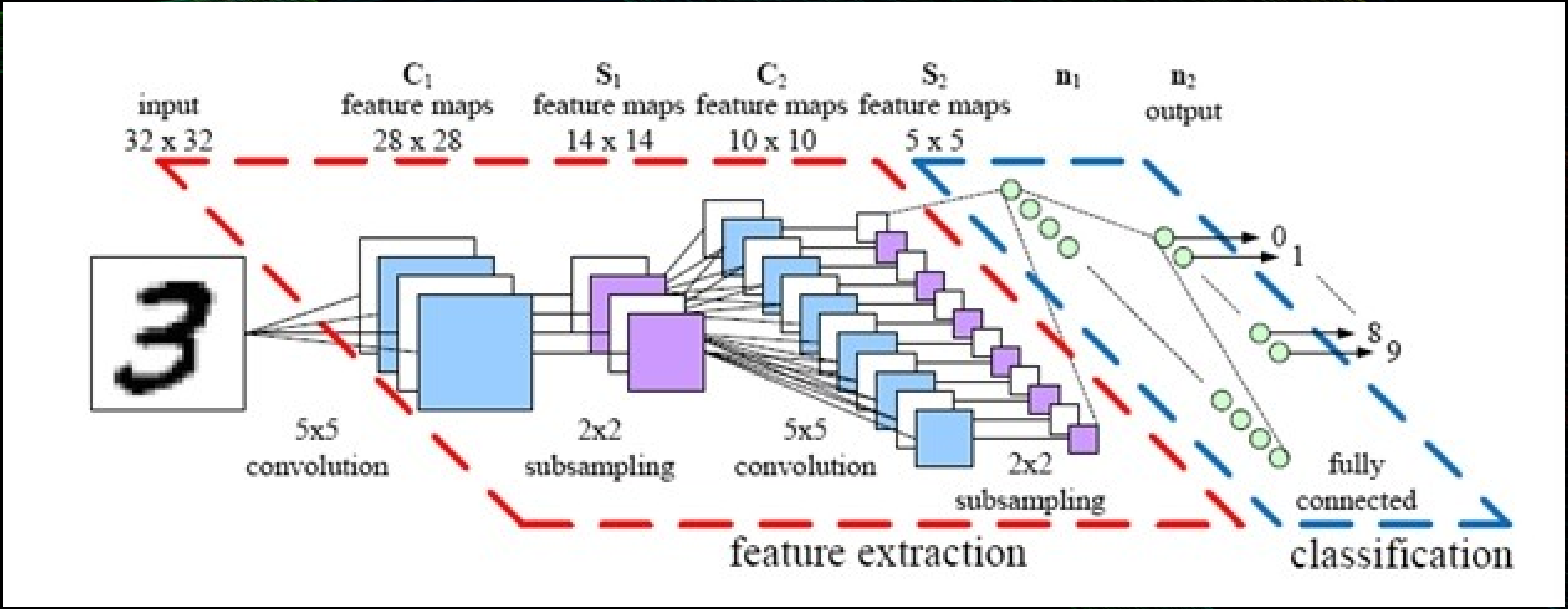
- General purpose classification and prediction



Source: https://medium.com/diaryofawannapreneur/deep-learning-for-computer-vision-for-the-average-person-861661d8aa61

Convolutional Neural Networks (CNN)

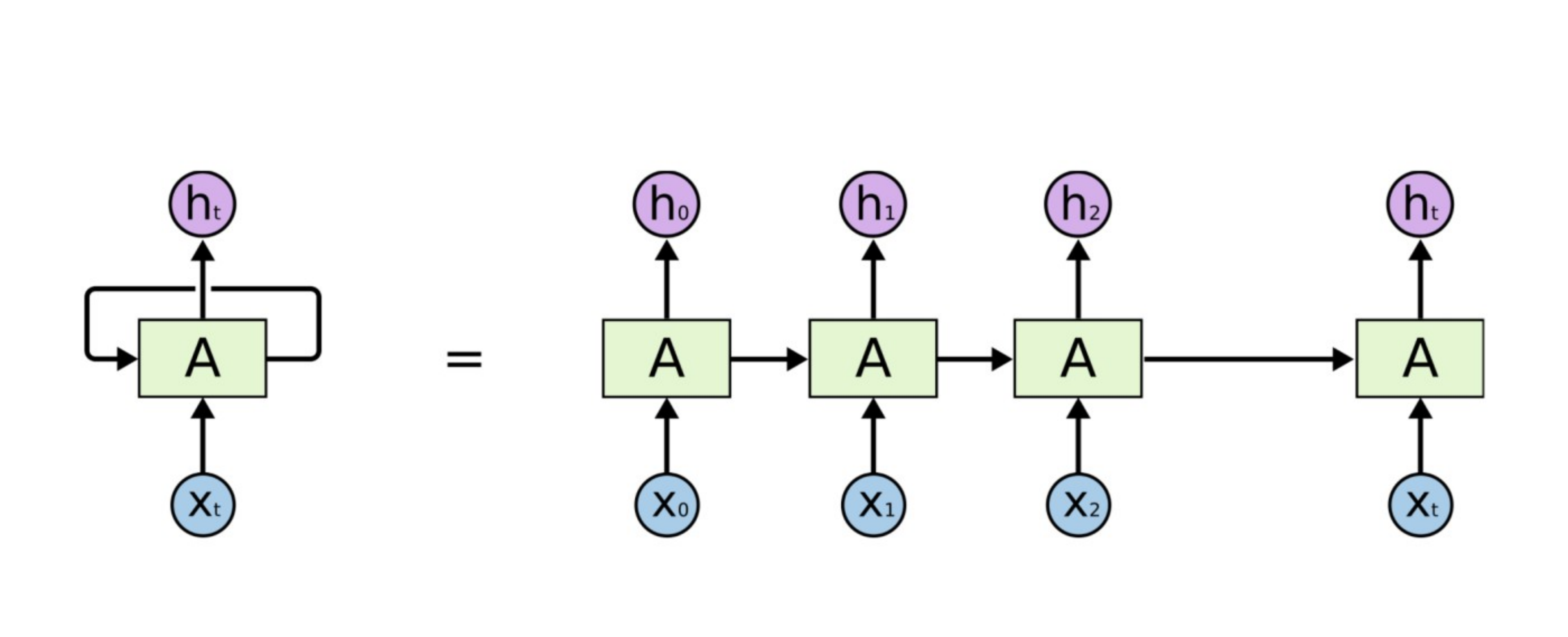
- Spatial pattern recognition. Object detection and classification. Self-driven cars, etc.



Source: https://www.kdnuggets.com/2017/08/convolutional-neural-networks-image-recognition.html

Recurrent Neural Networks (RNN): Long-Short Term Memory (LSTM)

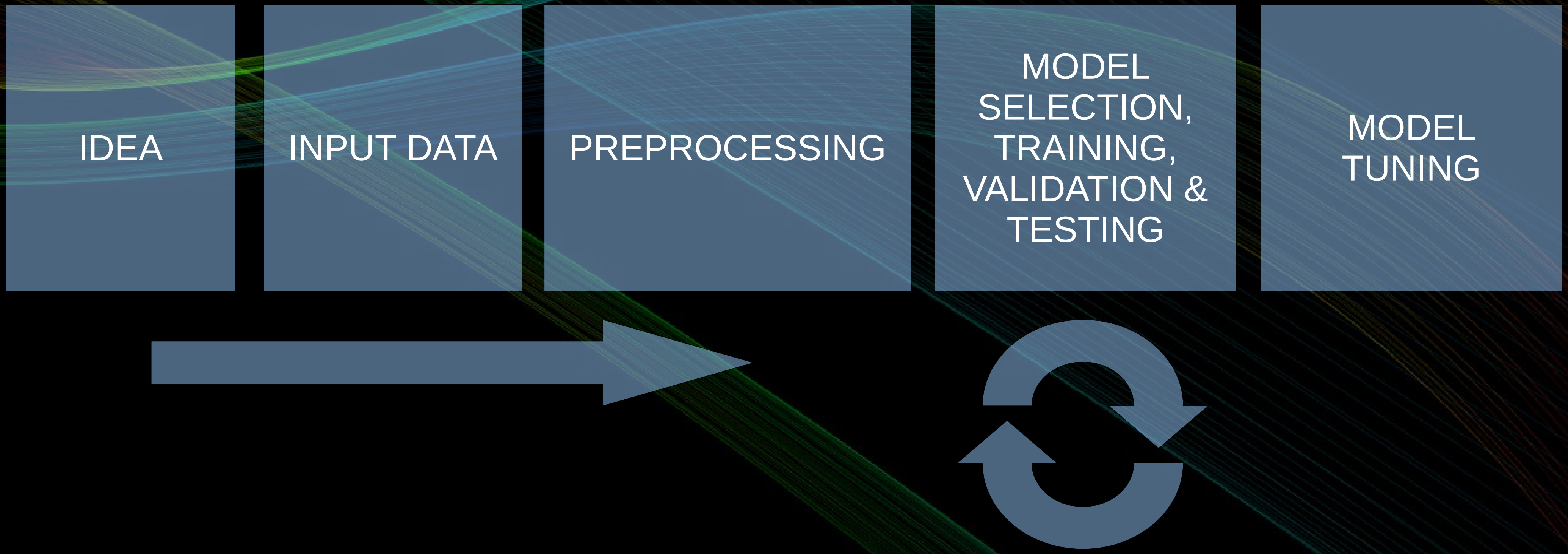
- Sequence learning. Temporal pattern recognition. NLP (Natural Language Processing). Speech recognition. Automatic Translation, etc.



Applications to Malware Detection and Classification
Why?

- Exponential increase in number and complexity of malware. Human workforce will never be enough neither in number nor specialization
- Traditional signature / heuristic methods are becoming more and more inefficient
- Attackers are already using AI to design adversarial malware instances to bypass both traditional AV as well as AI based detectors!

Deep Learning Model Development



IDEA

INPUT DATA

PREPROCESSING

MODEL SELECTION, TRAINING, VALIDATION & TESTING

MODEL TUNING

Deep Learning Model Scratch

- Model the input vector to represent your data
- Model the output vector to represent the desired result: Regression or Classification
- Model the network to reconize the desired kind of pattern(s)

Complex LEGO set

- Binary / Multiclass classification? Add a Fully connected / DNN Layer
- Spatial Patterns? Add a CNN Layer
- Temporal Patterns? Add a LSTM Layer
- Hybrid patterns? Combine the layers above with many others...
- Inception Network

Aplications to Malware Detection and Classification

- Raw data: DNN, CNN, LSTM
- Static Features: DNN
- Dynamic Features: LSTM
- Hybrid Models: Conv-LSTM / LSTM-Conv
- Fireeye
- DNN Example
- Deep Instinct
- Much more...

Challenges

- Adaptability: The model should adapt to new malware without the need to retrain it using the whole dataset
- Interpretability: The model should provide information on how the classification/detection was made
- Anti-Adversarial Model: The model should be robust against adversarial examples

Deep Learning Environment

- Python + Numpy + Pandas + ... = Anaconda
- Deep Learning Framework: Tensorflow + Keras
- Buy a GPU!

Where to start?

- Google ML Course
- Coursera:
  - Machine Learning
  - Deep Learning Specialization
  - Tensorflow Specialization
- Tutorials from Towards Data Science website

THANKS!

- Please do reach out!
- Linkedin: http://www.angeloliveira.net
- Email: alpha@angeloliveira.net