AI in Antivirus

What AI do in your antivirus

Who I am?

Arcangelo Saracino

Student of Computer Science at Uniba

Three years of experience in web development

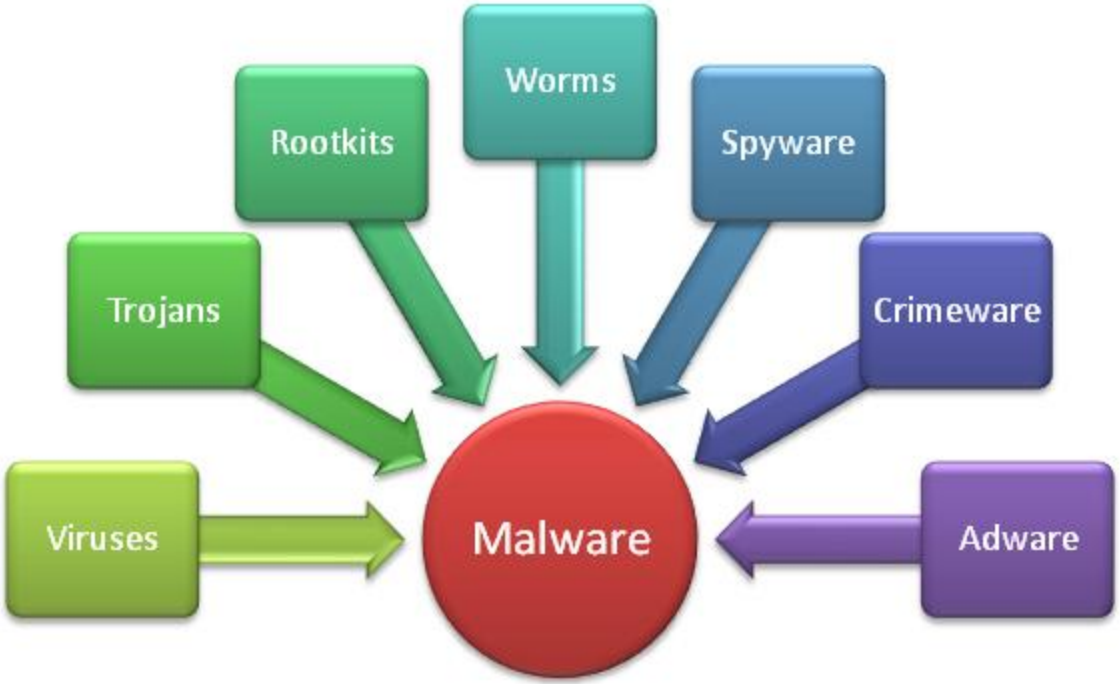
Cybersecurity and Linux appassionate

Mail: saracinoarcangelo@gmail.com

Outline

- Malware Classification
- AI overview
- How Security Companies Use AI in Antivirus

Types of Malware



https://www.akashtrehan.com/my-other-computer-is-your-computer/

Virus

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Trojan

A **Trojan** horse or **Trojan** is a type of malware that is often disguised as legitimate software. **Trojans** can be employed by cyber-thieves and hackers trying to gain access to users' systems.

Rootkit

A **rootkit** is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.

Worm

A computer **worm** is a standalone malware computer program that replicates itself in order to spread to other computers.

Spyware

Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information.

Crimeware

Crimeware is any computer program or set of programs designed expressly to facilitate illegal activity online.

Adware

Adware is a form of malware that hides on your device and serves you advertisements. Some **adware** also monitors your behavior online

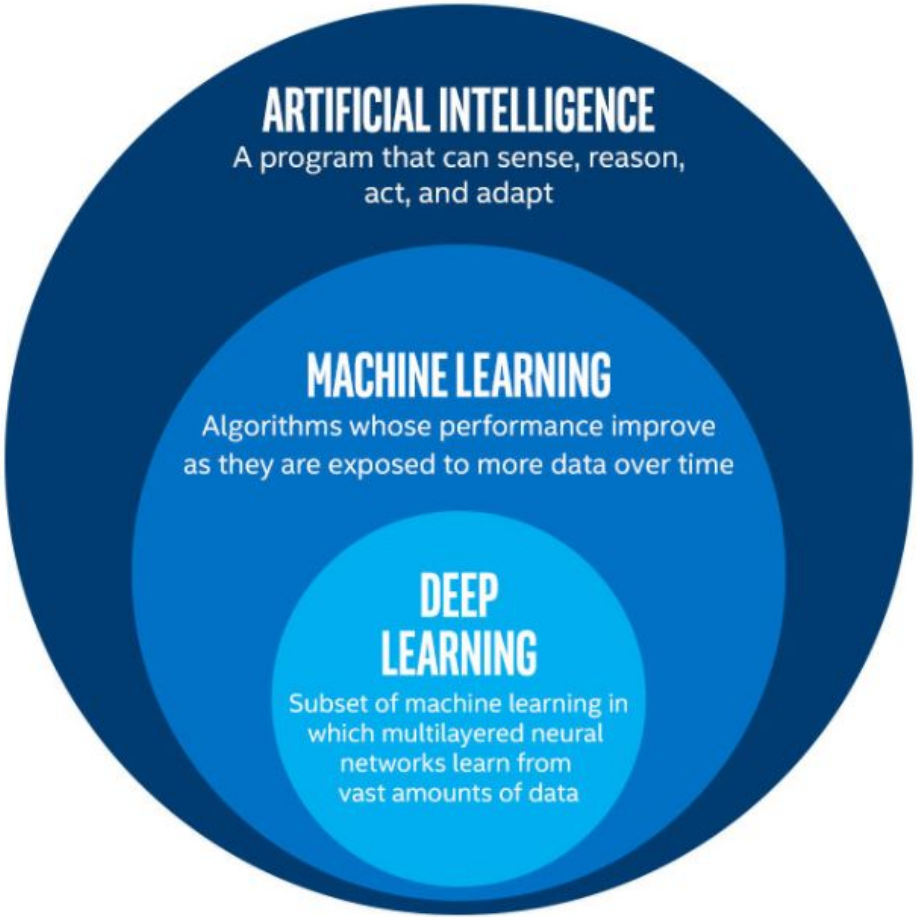
AI overview

AI definition

Artificial intelligence (AI) is the simulation of human **intelligence** processes by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions) and self-correction.

https://searchenterpriseai.techtarget.com/definition/AI-Artificial-Intelligence

AI > ML > DL



https://towardsdatascience.com/cousins-of-artificial-intelligence-dda4edc27b55

Machine Learning

Machine learning is the scientific study of algorithms and statistical models that computer systems use to perform a specific task without using explicit instructions, relying on patterns and inference instead.

Machine learning algorithms build a mathematical model based on sample data, known as "training data", in order to make predictions or decisions without being explicitly programmed to perform the task. Machine learning algorithms are used in a wide variety of applications, such as email filtering and computer vision, where it is difficult or infeasible to develop a conventional algorithm for effectively performing the task.

https://en.wikipedia.org/wiki/Machine_learning

Deep Learning

Deep learning (also known as **deep structured learning** or **hierarchical learning**) is part of a broader family of machine learning methods based on artificial neural networks. Learning can be supervised, semi-supervised or unsupervised.

Deep learning architectures such as deep neural networks, deep belief networks, recurrent neural networks and convolutional neural networks have been applied to fields including computer vision, speech recognition, natural language processing, audio recognition, social network filtering, machine translation, bioinformatics, drug design, medical image analysis, material inspection and board game programs, where they have produced results comparable to and in some cases superior to human experts.

https://en.wikipedia.org/wiki/Deep_learning

How Security Companies Use AI in Antivirus

Cylance Smart Antivirus

Cylance Smart Antivirus relies entirely on AI and ML to distinguish malware from legitimate data. The result is an antivirus that doesn’t bog your system down by constantly scanning and analyzing files. Rather, Cylance Smart Antivirus waits until the moment of execution and immediately kills the threat—without human intervention.

We identify behaviours of “would-be” attacks and prevent them before they can ever happen.

https://www.makeuseof.com/tag/artificial-intelligence-antivirus-tools/

Deep Instinct D-Client

Deep Instinct uses deep learning (a machine learning technique) to detect “any file before it is accessed or executed” on your system. The Deep Instinct D-Client makes use of static file analysis in conjunction with a threat prediction model that allows it to eliminate malware and other system threats autonomously.

Avast Free Antivirus

The Avast Research Lab announced three powerful backend tools for their products. (from 2012)

- The “Malware Similarity Search” allows almost instantaneous categorization of huge samples of incoming malware. Avast Free Antivirus quickly analyzes similarities between existing malware files using both static and dynamic analysis.
- “Evo-Gen” is similar “but a bit subtler in nature.” Evo-Gen is a genetic algorithm that works to find short and generic descriptions of malware in massive datasets.
- “MDE” is a database that works on top of the indexed data, allowing heavy parallel access.

These three machine learning technologies collectively evolved as the foundation for Avast’s CyberCapture

Questions ?

Thanks !