MACHINE LEARNING

MALWARE ANALYSIS

An examination of cutting edge malware detection strategies

Over 75% of wesbites on the internet aren't safe... why?

- 20% of breaches are politically motivated
- 70% of breaches are financially motivated
- 50% of breaches get small business

- 7000 new malware variants captured every hour

How do we know we are secure?

THREE VIABLE SOLUTIONS

DEEP LEARNING

The current popular technique for classifying data for tasks like image analysis or predictions

contains dog: 90%

SEMANTIC REASONING

Defines axiomatic statements across a theoretical "world" that exists within imposed those constraints

Dog.Has_A(Toy)

MARKOV LOGIC

Markov Logic combines statistical weights from deep learning with axiomatic expressions

Dog.Has_A(Toy, 90%)

THREE WEIGHING CRITERIA

Tractability

How much power do we have behind the wheel? Is it easy to manipulate our solution?

Speed

Our solution needs to be fast. The ouptut must be speedy and not hold up the line.

Open World

Encountering data we haven't seen before is the name of the game. Criminals are constantly trying to slip through the net

PEDRO DOMINGOS

“Homo sapiens is the species that adapts the world to itself instead of adapting itself to the world.”

Bibliography

Chebyshev, Victor, et al. IT Threat Evolution Q2 2019. Statistics. 19 August 2019. Securelist

Columbus, Louis. 76% of IT Security Breaches are Motivated by Money First. 15 May 2018. Forbes.

Domingos, Pedro and Daniel Lowd. "Unifying Logical and Statistical AI with Markov Logic." Communications of the ACM (2019)