SAPIENZA
UNIVERSITÀ DI ROMA

BlueTracer: a Robust API Tracer for Evasive Malware

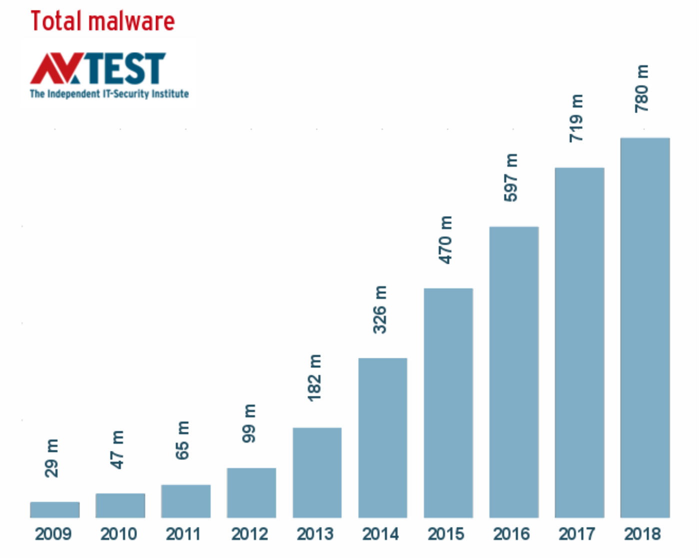
Simone Nicchi

Thesis Advisor: Prof. Camil Demetrescu
Thesis Co-Advisors: Dr. Daniele Cono D'Elia, Dr. Emilio Coppa

Master of Science in Engineering in Computer Science

July 20, 2018

Malware: an increasingly significant problem



Malware Analysis

Two main types:

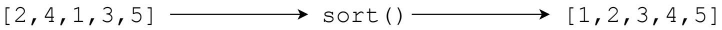
- **Static Analysis:**
  involves the inspection of the different data and code sections of a binary
- **Dynamic Analysis:**
  the malware sample is executed and the actions it performs on the environment are observed

Dynamic analysis strongly favoured as it allows to dodge code obfuscations and deal with a large number of samples

Function call monitoring

Functions can abstract implementation details providing a semantically richer representation of some functionality.

Example:



`[2,4,1,3,5]` → `sort()` → `[1,2,3,4,5]`

The abstractions embodied by **system calls** and **library calls** can be used to grasp the visible behavior of a malicious sample

API Hooking

API Hooking

Generate random values for a and b: execute on these inputs and track path constraints. Negate constraints on the branch in order to generate new inputs that will explore the error path.