SAPIENZA
UNIVERSITÀ DI ROMA

BlueTracer: a Robust API Tracer for Evasive Malware

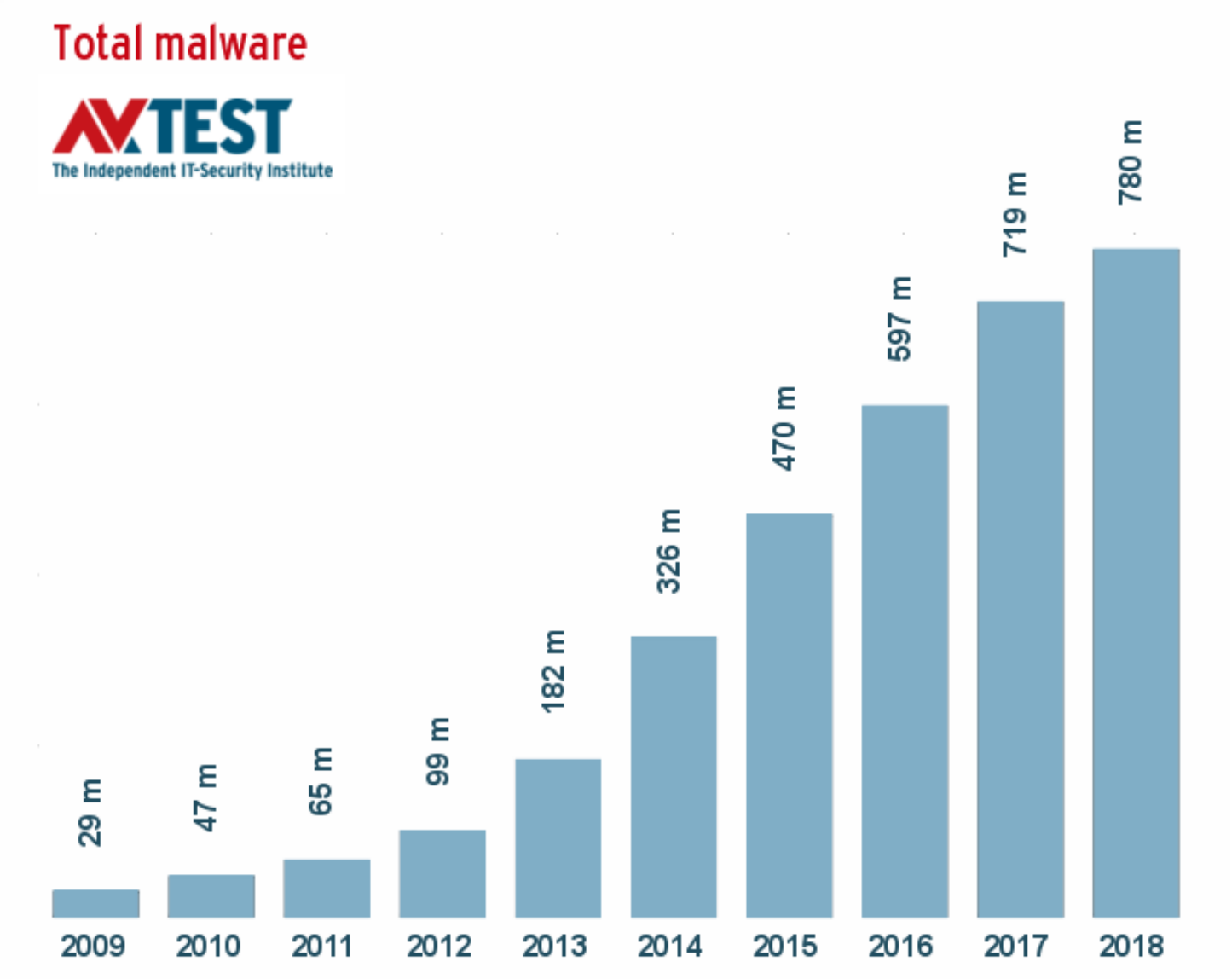
Simone Nicchi

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:

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

Implementation of function call monitoring

API Hooking

The interception of function calls provided by dynamically linked libraries (DLLs)

Three broad categories:

- Binary Rewriting
  - Call Redirection
  - Function Rewriting
- Virtual Machine Introspection (VMI)
- **Dynamic Binary Instrumentation (DBI)**

Dynamic Binary Instrumentation (DBI)

A dynamic binary analysis technique in which the behaviour of an application is inspected at run-time via the injection of analysis code.

```
record(arg1)
retval = libcall(arg1, &arg2)
record(retval, *arg2)
```

Problem 1: existing products have limited logging capabilites

The threat posed by evasive malware

API Hooking

The interception of function calls provided by dynamically linked libraries (DLLs)

Our solution: BlueTracer

Intel Pin

Integration with BluePill

BlueTracer's architecture

Al-Khaser

Sample tracked evasive check

Evasive malware samples

Conclusion and future developments

Thanks for the attention.