Can You See It? -NOP! A Practitioners Study

Diego Soi[1], Leonardo Regano[1], Davide Maiorca[1], Giorgio Giacinto[1], Harel Berger [2]

[1] University of Cagliari, [2] Georgetown University

NOP = No-operation

- Command or structure that doesn't change the semantics of the program
- It deceives both machines and humans, increasing the difficulty of spotting an evasion

Research Questions

RQ1. What is the correlation between the kind of evasion attacks based on NOPs' visibility and the detection rate by a human expert?

RQ2. What is the correlation between the detection time, practitioner expertise and success rate?

Methodology (in progress)

- Online **anonymous survey (100 partecipants)**
- Java source code snippet with and without evasive NOPs

```
public class M{
    public static void main(String[] args){
        ...
        d = 3;
        System.out.println(c(4,7));
        if d<2{
            System.exit(0);
        }
    }
}
```

Data Analysis

- **Quantitatively**: statistics and correlation between {visibility, time, expertise} vs detection rate
  - Expected direct proportion since higher visibility, time, and expertise enhance the ability of detection
- **Qualitatively**: analysis of the ways in which human experts recognized the presence of evasive NOP

Anticipated contributions

1. Practical evaluation of the relationship between evasion attacks and detection rate
2. Incorporation of the "human factor" into the malware detection process