Data Aware Defense
From research to product on the market

David Lubicz

Table of content

Contenu

The ransomwares

The ransomewares are a form of malware:

- personal data are made unavailable (by cyphering) and a ransom is reclaimed in order to (perhaps) get them back;
- the number of attacks by ransomware grows consistently (36% between 2016 and 2017) ;
- 60% of all malawares;
- $5 worth of cumulated damages;
- Examples : NotPetya, WannaCry have made big headlines.

The ransomwares

The ransomwares can be characterized by:

- an important infectious activity and high speed of propagation;
- but they do not enter in the deep layers of the systems (userland execution);
- do not target a particular user of system, attack personal data.

Dynamic analysis is well adapted to the detection of ransomwares.

Contenu

The High Security Laboratory (HSL)

A research project started in 2015 with a thesis:

- funded by DGA and carried out by the HSL;
- HSL is the fruit of a partnership between CentraleSupelec, CNRS, Inria, DGA, and Britanny region;
- its role is to develop and organize the research in cybersecurity and boost innovation.

The project rely on the competences and the platforms of the HSL.

Contenu

Aims of the solution

The objectives :

- being able to detect quickly any malicious activity;
- to adapt to the evolution (counter measures to the detection) of this activity;
- to protect the data which are targeted by the ransomware;
- in case of attack, stop the malicious activity and carry out an instant restoration of data.

and limiting side effects:

- limit the rate of false alarm;
- have a large detection span;
- small memory and cpu consumption;
- in all cases behave in the most transparent way for the user.

The difficulties

It's difficult to reach these goals:

- some of these goals are conflicting: reactivity and data protection implies a rise in the number of false alarms;
- our solution allows in a way not to do any trade off.

Technical explanation

The originality of our solution lie in the dynamic analysis part:

- a driver which is run in the kernel out of reach of malicious activity;
- monitor a relevant activity probe;
- learning machine techniques in order to distinguish normal and abnormal behaviours;
- optimality theorems (reactivity, relevance, small rate of false alarm) for a large class of detection algorithms;
- a gradual kick off of the protection mechanisms with respect to the level of certainty that we have a real attack.

A prototype

Development of a prototype and rigorous evaluation of our solution:

- with the Mom platform of the HSL;
- an extensive malware data base;
- with computers that we can infect at will;
- compare favorably to other known public solutions.

Thousands of hours of use without a bug!

Contenu

Start-up creation

From the prototype to the product to the market:

- protection of the intellectual property with (pending) patents;
- creation of a start up via Inriahub facility;
- development of a product.

And the research keeps going...

At the same time:

- Improve the malware platform of the HSL;
- better understanding of malware (infection mechanisms, counter measures to the detection, improvement of the detection etc.)

In order to improve and extend the capacity of our product.