**2entFOX**

Build a Bayesian network that contains a CPT conditional probability that contains probabilities of certain weaknesses based on studies of most frequently validated points (such as trying to undo the most important mechanism for windows to store users' backup files, make changes to the service, the victim has no way to recover its encrypted data Paying ransom One of the behaviors we encountered when analyzing ransom components was gaining access to special libraries.) In the study, 6 different scenarios were carried out, but the article itself only talks about the first scenario:

After extracting each feature independently and step by step.

The default of the software is to take 20 cases and in the case of a number of cases the system warns that it is a ransom attack (over 85% probability)

**Detecting crypto‑ransomware in IoT networks based on energy**

This article is based on a learning machine so that every app has a certain need, after lots of experimentation we build a model so run on lots of dataset and thus the model knows by the energy of the device which should be after popular apps (by model) whether the app is malicious or me

**CryptoLock (and Drop It) Stopping Ransomware Attacks on User Data**

There were several authorities that fell into ransom!

**Indicator based cryptolock software has 3 main indicators**

1. Change the file type - These signatures describe the order

And location of specific byte values ​​unique to the file type, and no

Simply enter the title information. Because files usually keep theirs

Bulk file type and formatting during existence

Such data should be considered as suspicious.

2. Copy source file - When copying it should be like probability 0.

3. Shannon's Dear Brother

**Secondary indicator**

1. Delete system files

2. I didn't understand