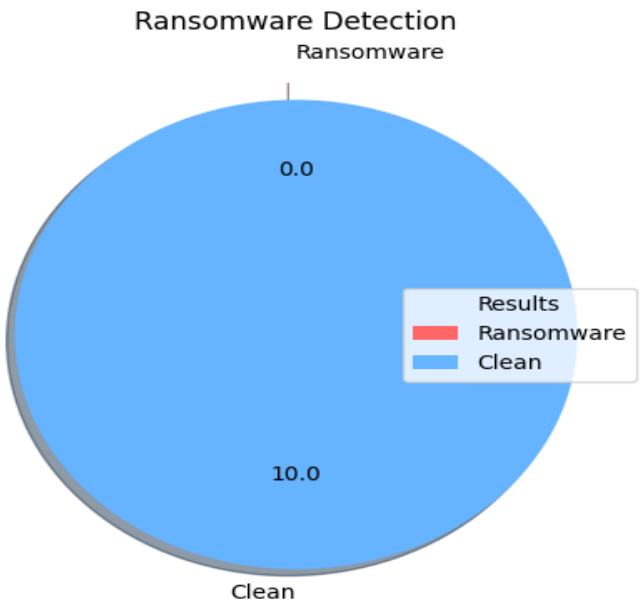
Malware Analysis Report

Overview:

In this report, we analyzed a new strain of ransomware that has been spreading across corporate networks. The ransomware, known as '', is could be spread through malicious emails containing a macro-enabled Word document.

Score rate:



Information related about file

size : 1335

MD5 Hash :6c3b7f076d92a2d2e19cf468d2d293d9

Extension of file :exe

Static Analysis

In Signature algorithme the file has been not detected in signature file

In Entropy algorithme, the file could not be suspect

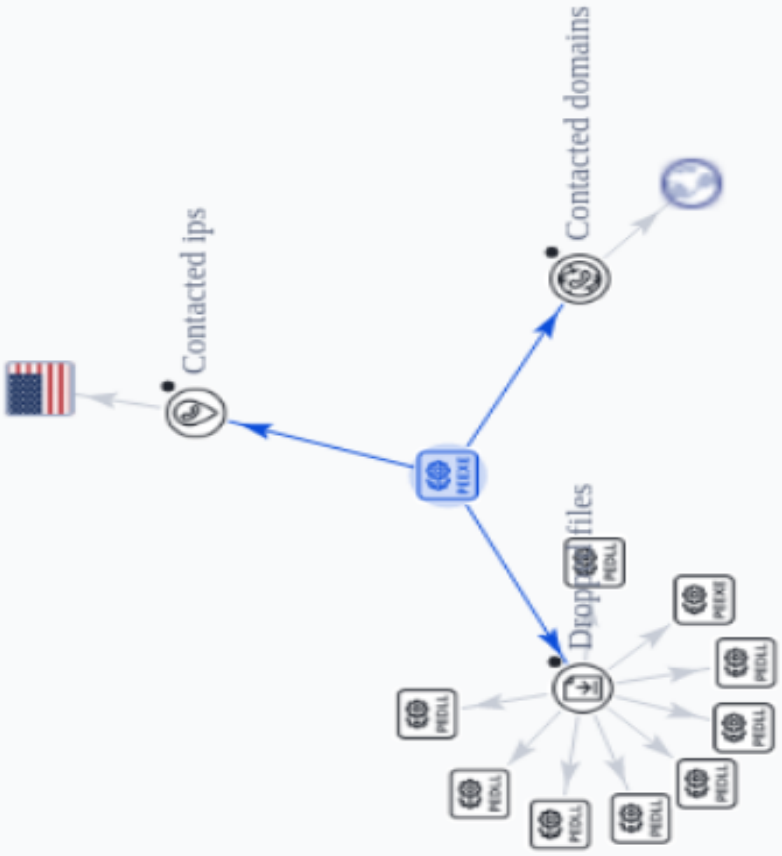
In Encryption algorithme, the file analyzed could not detect the algorithmes

In Anti debugging algorithme, the file analyzed could not detect the anti debugging functions

In Anti vm algorithme, the file analyzed could not detect the vms

In Machine learning algorithme, the file analyzed could not be suspect of ransomwares

Graph:



Recommendations:

To prevent future infections, we recommend implementing security best practices such as :

1. Isolate the infected system
2. Assess the scope of the attack
3. Determine the type of ransomware
4. Backup and restore
5. Consult with security experts
6. Do not pay the ransom beceause it does not guarantee that the data will be restored and may encourage further attacks.
7. Strengthen cybersecurity measures:
    - Updating software and systems.
    - Implementing multi-factor authentication.
    - Enforcing strong password policies.
    - Educating employees on how to detect and report suspicious activity.