RansomWatch

As part of project in ransomware, 236499, Spring 2019

Rafael Wurf, Aviad Gafni

Prof. Eli Biham, Dr. Nir Levy and Assaf Rosenbaum

CYBER LAB
Cyber, Cryptology and Computer Security lab

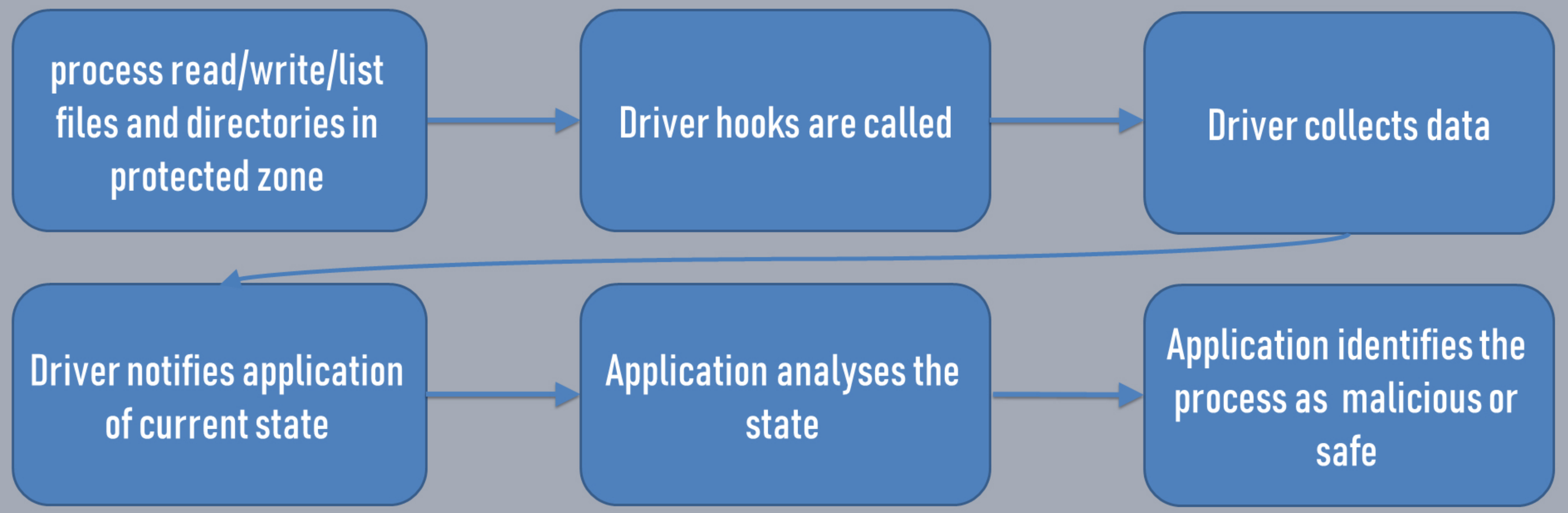
Microsoft

Introduction

RansomWatch is a solution which monitors and analyses data collected from the file system in real time in order to identify suspicious ransomware behavior on the file system.

RansomWatch autonomously stops ransomware applications and backup files and directories to prevent data loss. It innovates by grouping related multi-processes application into a “single-process” for analysis.

Method


process read/write/list files and directories in protected zone

Driver hooks are called

Driver collects data

Driver notifies application of current state

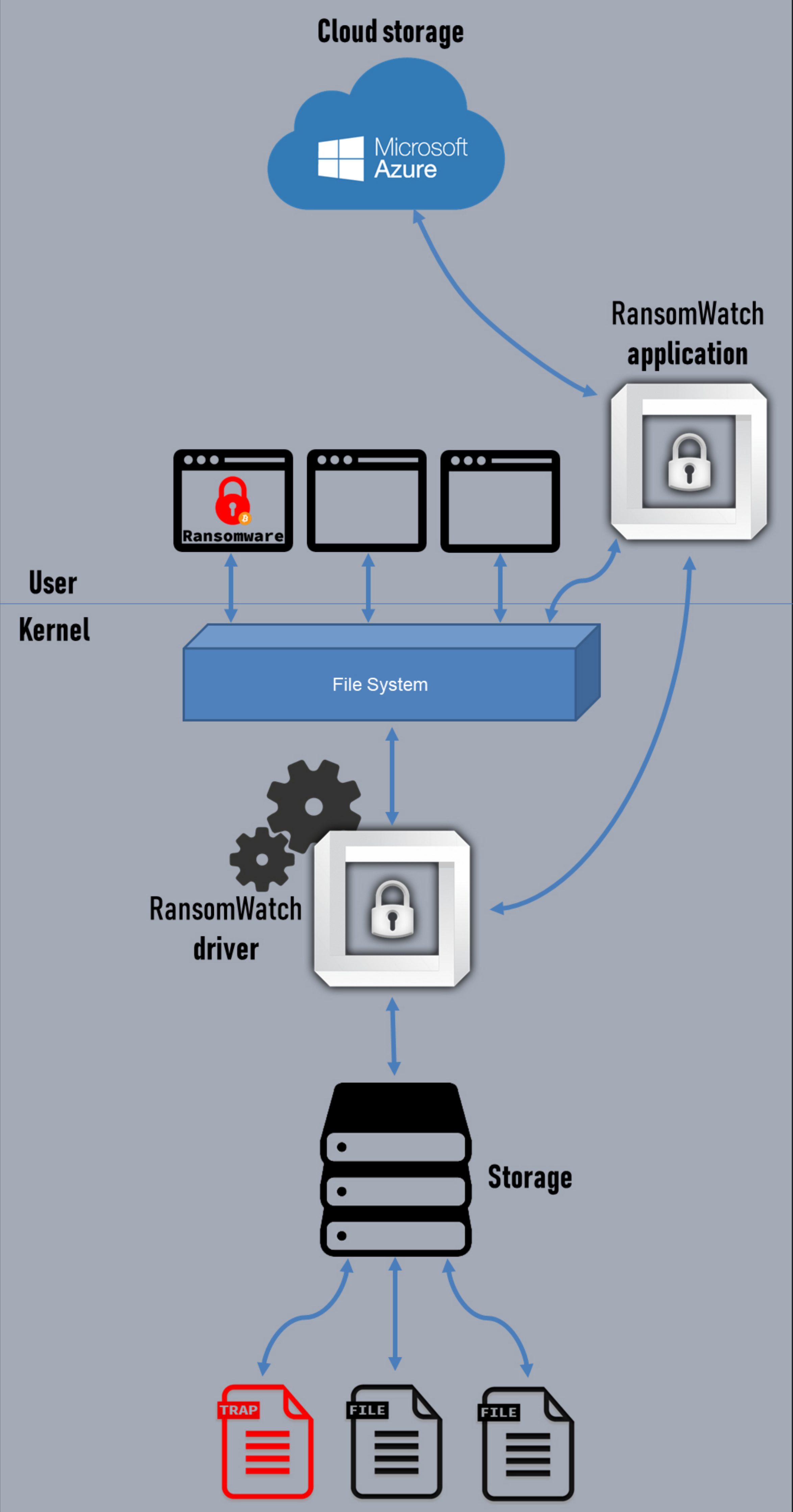
Application analyses the state

Application identifies the process as malicious or safe

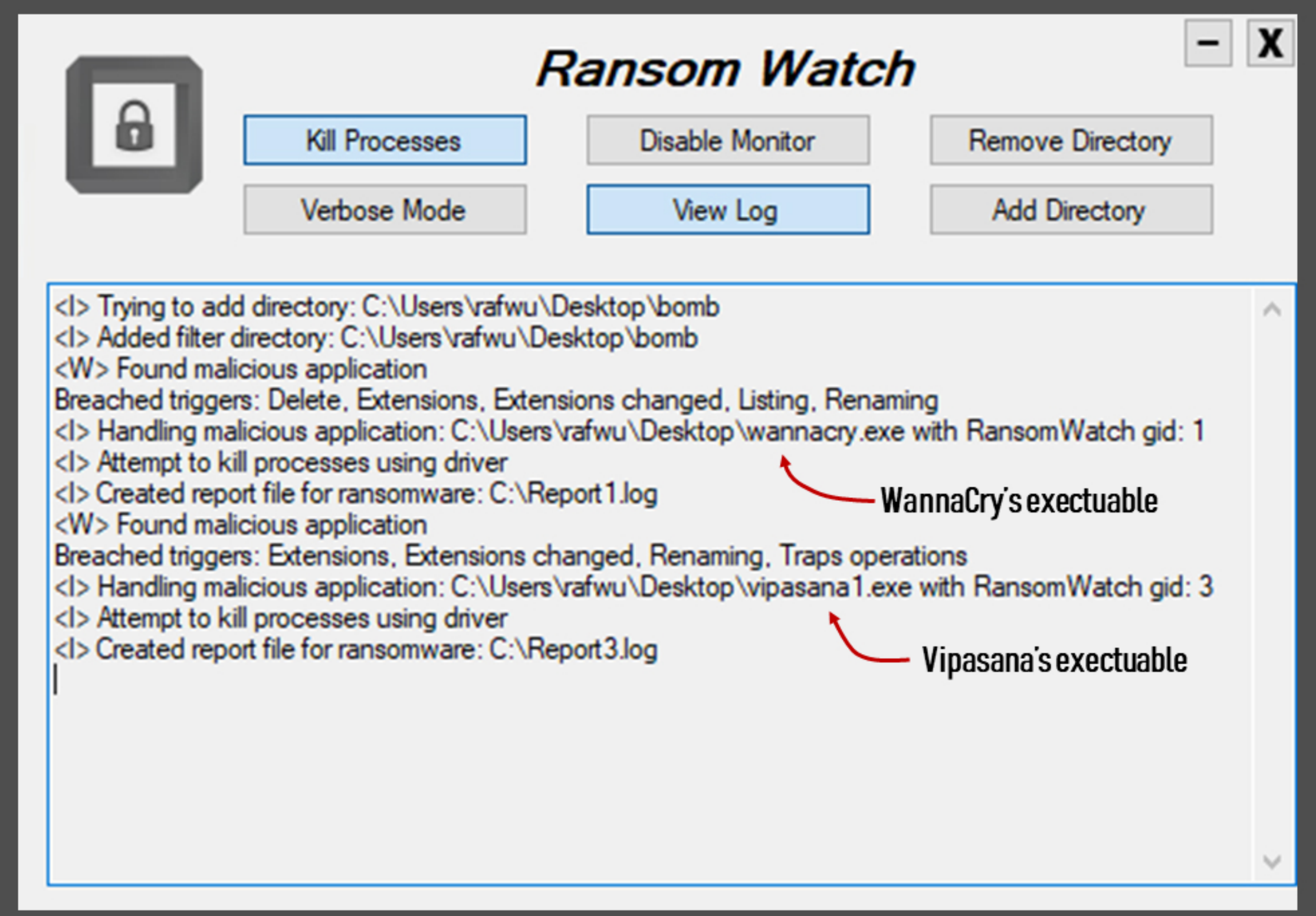
Ransom Watch uses the following measures to identify suspicious ransomware behavior:

Feature	Description	Rationale
Write entropy	Average entropy of write operation, compared to the entropy of read.	Encryption generates high entropy data, compared to the entropy of its read operation.
Files access	Number of files read or changed.	Ransomware programs often read and write approximately the same amount of files. Also, ransomware processes must read files before encrypting.
Folder listing	Number of folder-listing operations.	Ransomware programs traverse the filesystem looking for target files.
File type coverage	Number of file type categories accessed (RansomWatch categorizes file types based on regular use scenarios).	Ransomware programs access numerous file types unlike regular applications which usually use only few file type categories.
Traps access	Number of traps files changed (RansomWatch plants traps throughout the protected zones).	Benign application typically will not change many trap files since these files are not user generated. Ransomware cannot differentiate trap files from regular files, thus will attempt to encrypt them as well.
Extension change	Number of file extension changes, compared to the number of files accessed.	Ransomware programs often change file extensions before/after encrypting files, appending an extension to the file.
Files rename	Number of files renamed or moved.	Ransomware programs often change files location or rename files.
Files deletion	Number of files deleted.	Ransomware programs often read files before encrypting and writing a new encrypted files before deleting the original files.
Multi-Processing	RansomWatch groups multi processes into one record group for analysis, increasing the accountability of multi processes applications.	Some ransomware evade detection by splitting the work among multiple processes, leading to reduced accountability and lower detection rate of each single measure.

Architecture



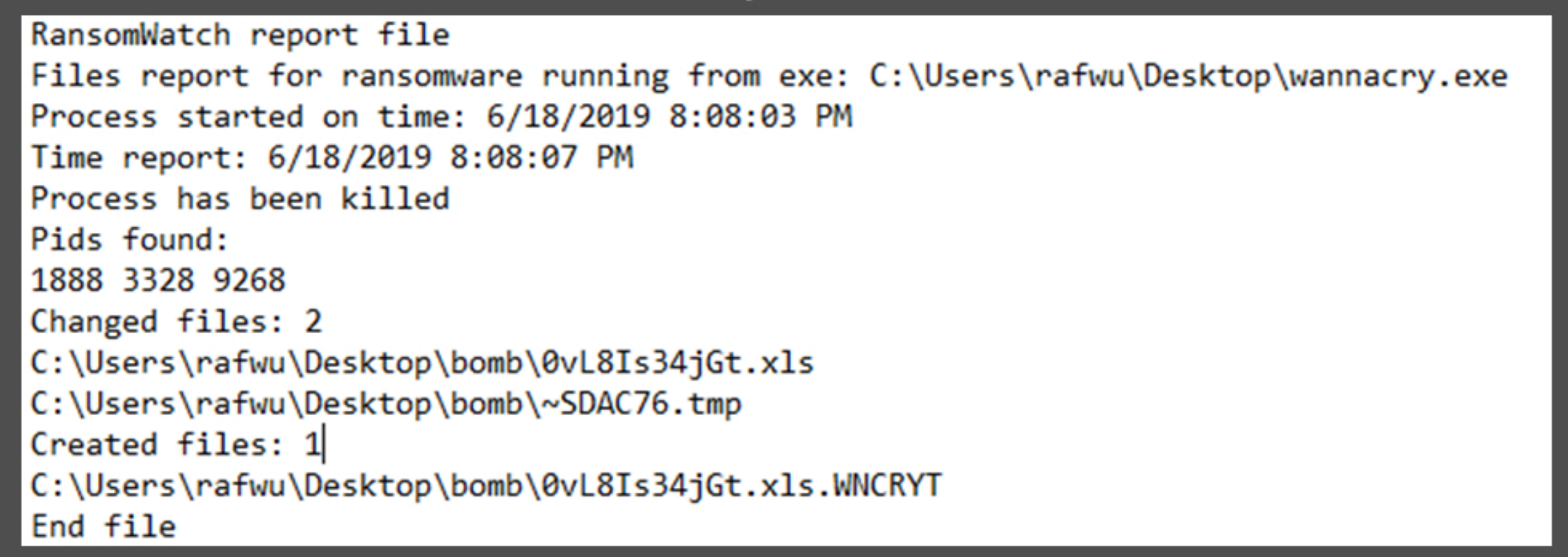
Results



```
<I> Trying to add directory: C:\Users\rafwu\Desktop\bomb
<I> Added filter directory: C:\Users\rafwu\Desktop\bomb
<W> Found malicious application
Breached triggers: Delete, Extensions, Extensions changed, Listing, Renaming
<I> Handling malicious application: C:\Users\rafwu\Desktop\wannacry.exe with RansomWatch gid: 1
<I> Attempt to kill processes using driver
<I> Created report file for ransomware: C:\Report1.log
<W> Found malicious application
Breached triggers: Extensions, Extensions changed, Renaming, Traps operations
<I> Handling malicious application: C:\Users\rafwu\Desktop\vipasana1.exe with RansomWatch gid: 3
<I> Attempt to kill processes using driver
<I> Created report file for ransomware: C:\Report3.log
```

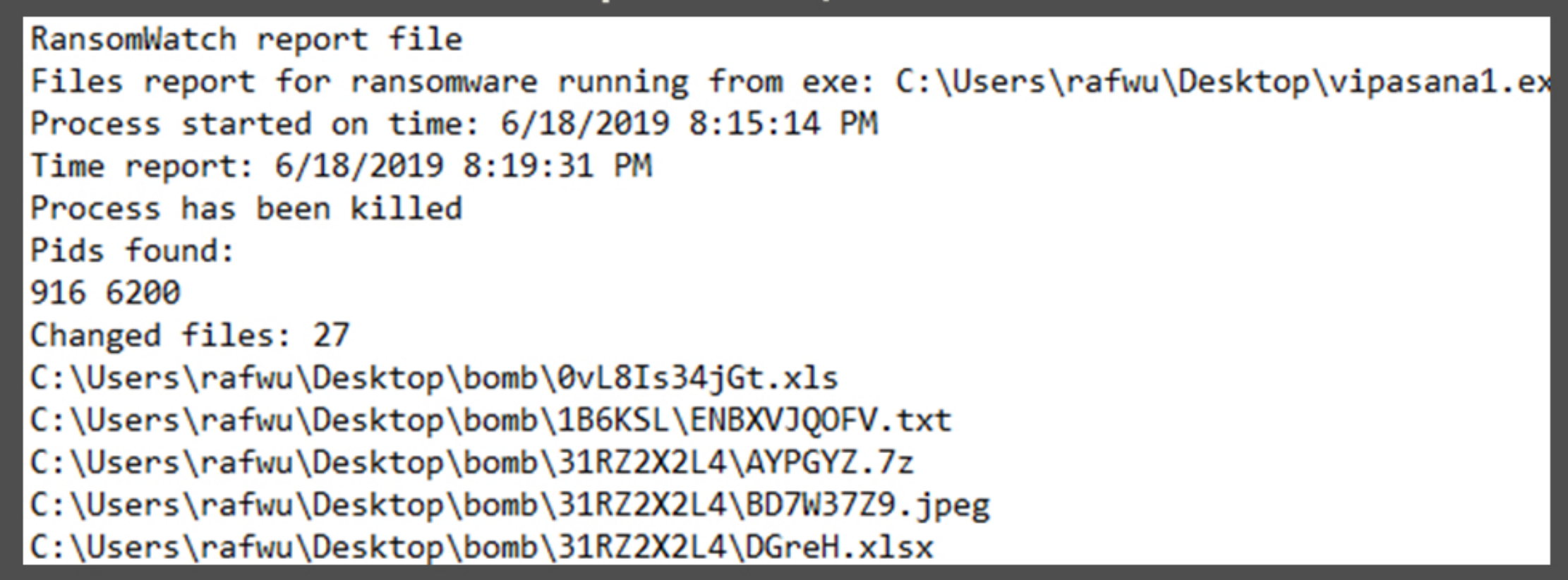
RansomWatch detected WannaCry and Vipasana and stopped them. It logged why it had stopped the applications: created, deleted and accessed large number of files, accessed large number of file types, changed large number of file extensions, listed folders large number of times and wrote with high entropy.

WannaCry Report File



```
RansomWatch report file
Files report for ransomware running from exe: C:\Users\rafwu\Desktop\wannacry.exe
Process started on time: 6/18/2019 8:08:03 PM
Time report: 6/18/2019 8:08:07 PM
Process has been killed
Pids found:
1888 3328 9268
Changed files: 2
C:\Users\rafwu\Desktop\bomb\0vL8Is34jGt.xls
C:\Users\rafwu\Desktop\bomb\~SDAC76.tmp
Created files: 1
C:\Users\rafwu\Desktop\bomb\0vL8Is34jGt.xls.WNCRYT
End file
```

Vipasana Report File



```
RansomWatch report file
Files report for ransomware running from exe: C:\Users\rafwu\Desktop\vipasana1.ex
Process started on time: 6/18/2019 8:15:14 PM
Time report: 6/18/2019 8:19:31 PM
Process has been killed
Pids found:
916 6200
Changed files: 27
C:\Users\rafwu\Desktop\bomb\0vL8Is34jGt.xls
C:\Users\rafwu\Desktop\bomb\1B6KSL\ENBXVJQOFV.txt
C:\Users\rafwu\Desktop\bomb\31RZ2X2L4\AYPGYZ.7z
C:\Users\rafwu\Desktop\bomb\31RZ2X2L4\BD7W37Z9.jpeg
C:\Users\rafwu\Desktop\bomb\31RZ2X2L4\DGreH.xlsx
```

The log file contains the path to the executable of the process which RansomWatch detected and terminated, the related process identifiers (processes that correspond to the same group identifier) and a list of all files that the application succeeded to change in the protected zone before RansomWatch detected and stopped its operation.