ShieldFS: The Last Word in Ransomware Resilient Filesystems

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi

* US patent pending
2016-17 the "years of extortion"

CRYPTOWALL RANSOMWARE COST USERS $325 MILLION IN 2015
by NewsEditor on November 2nd, 2015 in Industry and Security News.

Ransomware Hackers Blackmail U.S. Police Departments
Chris Francescani
Tuesday, 26 Apr 2016 | 15:30 AM ET
NBC NEWS

Public Service Announcement
CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

WannaCry Ransomware Encrypted Hospital Medical Devices

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating
Do you WannaCry?

Wanna Decryptor 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

Also, if you don’t pay in 7 days, you won’t be able to recover your files forever.

We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>.

Best time to check: 9:00am - 11:00am

How to pay?

Send $300 worth of bitcoin to this address:

115p7UMMngo1pMvkpHijcRdfJN5XJ8LrL

Check Payment

Decrypt

About bitcoin
How to buy bitcoins?

Contact Us
Do you WannaCry?

NOPE
ShieldFS detected WannaCry after it encrypted >=200 files

Files lost: zero, all were recovered automatically
It’s not just WannaCry...

- Detected: 1436/1483, 96.9%
- Files lost: always 0%
Why

ShieldFS is different?
The way ransomware interacts with the filesystem is significantly different than benign applications.
The way ransomware interacts with the filesystem is significantly different than benign applications.

**DETECTION.**

Monitor **filesystem activity**

Usage of **crypto** primitives
The way ransomware interacts with the filesystem is significantly different than benign applications.

**DETECTION.**

Monitor filesystem activity

Usage of crypto primitives

**PROTECTION.** Mere detection is insufficient

➢ Stopping a suspicious process may be too late

➢ We need to protect users’ data, reverting the effects of ransomware attacks.
What does ShieldFS observe?
Windows Kernel module to **monitor** and **log** the file system activity
- Windows Minifilter Driver
- Log IRPs (I/O Request Packets)
Filter Manager API

```c
CONST FLT_OPERATION_REGISTRATION Callbacks[] = {
    {IRP_MJ_CREATE, 0, PreCreateOperationCallback, PostCreateOperationCallback },
    {IRP_MJ_CLOSE, 0, PreCloseOperationCallback, PostCloseOperationCallback },
    {IRP_MJ_READ, 0, PreReadOperationCallback, PostReadOperationCallback },
    {IRP_MJ_WRITE, 0, PreWriteOperationCallback, PostWriteOperationCallback },
};

FltRegisterFilter(DriverObject, &FilterRegistration, &Filter);
```
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>PID</th>
<th>Process</th>
<th>Operation</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:09:47:452</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CLEANUP</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:512</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CREATE</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_NETWORK_QUERY_OPEN</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CREATE</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_QUERY_INFORMATION</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CLEANUP</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CLOSE</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_QUERY_INFORMATION</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_READ</td>
<td>Users\John\AppData\Roaming\Microsoft\Windows\Co</td>
</tr>
<tr>
<td>13:09:47:522</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_READ</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
<tr>
<td>13:09:48:464</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CREATE</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
<tr>
<td>13:09:48:464</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_NETWORK_QUERY_OPEN</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
<tr>
<td>13:09:48:464</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CREATE</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
<tr>
<td>13:09:48:464</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_QUERY_INFORMATION</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
<tr>
<td>13:09:48:464</td>
<td>3284</td>
<td>nokmhcu.exe</td>
<td>IRP_MJ_CLEANUP</td>
<td>Users\John\Documents\decoys\decoy_doc_1.doc</td>
</tr>
</tbody>
</table>
Where do we start from?
➢ IRP logger on 11 clean machines
➢ FS activity under "typical" usage
  ○ ~1 month worth of data
<table>
<thead>
<tr>
<th>Usage</th>
<th>Data [GB]</th>
<th>#IRPs Mln.</th>
<th>#Procs Mln.</th>
<th>Apps</th>
<th>Period [hrs]</th>
<th>Data Rate [MB/min]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>28.2</td>
<td>1,763.0</td>
<td>107.00</td>
<td>2245</td>
<td>643</td>
<td>-</td>
</tr>
</tbody>
</table>
## Collected FS Activity

<table>
<thead>
<tr>
<th>Usage</th>
<th>Data [GB]</th>
<th>#IRPs Mln.</th>
<th>#Procs Mln.</th>
<th>Apps</th>
<th>Period [hrs]</th>
<th>Data Rate [MB/min]</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev</td>
<td>3.4</td>
<td>230.8</td>
<td>16.60</td>
<td>317</td>
<td>34</td>
<td>7.85</td>
</tr>
<tr>
<td>home</td>
<td>2.4</td>
<td>132.1</td>
<td>9.67</td>
<td>132</td>
<td>87</td>
<td>2.04</td>
</tr>
<tr>
<td>office</td>
<td>0.9</td>
<td>54.2</td>
<td>5.56</td>
<td>225</td>
<td>17</td>
<td>0.83</td>
</tr>
<tr>
<td>home</td>
<td>4.7</td>
<td>279.9</td>
<td>18.70</td>
<td>255</td>
<td>122</td>
<td>5.18</td>
</tr>
<tr>
<td>home</td>
<td>2.2</td>
<td>138.1</td>
<td>5.04</td>
<td>141</td>
<td>47</td>
<td>4.10</td>
</tr>
<tr>
<td>dev</td>
<td>1.8</td>
<td>100.4</td>
<td>10.30</td>
<td>225</td>
<td>35</td>
<td>2.42</td>
</tr>
<tr>
<td>dev</td>
<td>0.8</td>
<td>49.0</td>
<td>3.28</td>
<td>166</td>
<td>8</td>
<td>5.62</td>
</tr>
<tr>
<td>home</td>
<td>0.8</td>
<td>43.9</td>
<td>6.33</td>
<td>148</td>
<td>32</td>
<td>2.16</td>
</tr>
<tr>
<td>home</td>
<td>7.7</td>
<td>501.8</td>
<td>24.20</td>
<td>314</td>
<td>215</td>
<td>3.21</td>
</tr>
<tr>
<td>home</td>
<td>0.9</td>
<td>57.6</td>
<td>2.63</td>
<td>151</td>
<td>18</td>
<td>4.60</td>
</tr>
<tr>
<td>office</td>
<td>2.6</td>
<td>175.2</td>
<td>4.69</td>
<td>171</td>
<td>28</td>
<td>8.51</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>28.2</strong></td>
<td><strong>1,763.0</strong></td>
<td><strong>107.00</strong></td>
<td><strong>2245</strong></td>
<td><strong>643</strong></td>
<td>-</td>
</tr>
</tbody>
</table>
Analysis Environment

383 samples of 5 distinct families

- CryptoWall
- Crowti
- CryptoDefense
- Critroni
- TeslaCrypt

Windows 7 VM

Ransomware

User mode
Kernel mode

I/O Manager

IRPLogger

File System

Disk drive

VirtualBox

Cuckoo Sandbox
● Trigger ransomware activity
● Avoid anti-sandbox tricks
Ransomware vs Benign apps

- Benign
  - User mode
  - Kernel mode

- Ransomware

  - I/O Manager
  - IRPLogger
  - File System
  - Storage Driver
  - Disk drive
ShieldFS
Self-healing
Ransomware-aware
Filesystem
Ransomware vs Benign apps
Ransomware vs Benign apps

Many programs exhibit low value

Many programs exhibit high value

Few programs exhibit low value

Few programs exhibit high value
Ransomware vs Benign apps

(1) #Folder-listing

Graph showing the comparison between Ransomware and Benign apps.
Ransomware vs Benign apps

(2) #Files-Read

Graph showing the comparison between Ransomware and Benign apps. The graph indicates the percentage of files read over a range of values.
Ransomware vs Benign apps

(3) #Files-Written

![Graph comparing Ransomware and Benign apps](image-url)
Ransomware vs Benign apps

(4) #Files-Renamed

decoy_jpg_9.jpg

decoy_jpg_9.jpg.WNCRY

decoy_jpg_10.jpg

decoy_jpg_10.jpg.WNCRY
Ransomware vs Benign apps

(5) File type coverage
(6) Write-Entropy

Ransomware vs Benign apps

Ransomware
Benign
Learned classification model
ShieldFS
Self-healing
Ransomware-aware Filesystem
ShieldFS: Healing Approach
ShieldFS: Healing Approach
THIS SLIDE IS TO PROVE THAT WE CAN CREATE COMPLEX ANIMATION FLOWS
THIS SLIDE IS TO PROVE THAT WE CAN CREATE COMPLEX ANIMATION FLOWS
Detection Models

Disk drive

Process #1
Process #n

Process-centric Models
System-centric Model

#BHUSA / @BLACKHATEVENTS
Multi-tier Incremental Models

Global Model

Model 3

Model 2

Model 1

Long-term horizon

Short-term horizon

log (% accessed files)
Multi-tier Incremental Models

tick #0

- Global Model
- Model 1
- Model 2
- Model 3

Long-term horizon
Short-term horizon

log (% accessed files)

#0 #1 #2 #3
Multi-tier Incremental Models

tick #1

- Global Model
- Model 3
- Model 2
- Model 1

Tiers:
- Long-term horizon
- Short-term horizon

Log (% accessed files):
- #0
- #1
- #2
- #3
Multi-tier Incremental Models

tick #2

Global Model

Model 3

Model 2

Model 1

#0 #1 #2 #3

log (% accessed files)

Long-term horizon

Short-term horizon
Multi-tier Incremental Models

- Model 1
- Model 2
- Model 3

Global Model

- Long-term horizon
- Short-term horizon

#0, #1, #2, #3

log (% accessed files)

tick #3
Multi-tier Incremental Models

```
<table>
<thead>
<tr>
<th>tick #4</th>
</tr>
</thead>
<tbody>
<tr>
<td>#0</td>
</tr>
<tr>
<td>#1</td>
</tr>
<tr>
<td>#2</td>
</tr>
<tr>
<td>#3</td>
</tr>
</tbody>
</table>

Long-term horizon

Short-term horizon

Global Model

Model 1

Model 2

Model 3

log (% accessed files)
Multi-tier Incremental Models

tick #5

Global Model

Model 3

Model 2

Model 1

#0 #1 #2 #3

log (% accessed files)

Long-term horizon

Short-term horizon

Model 1

Model 2

Model 3

Model 1

Model 2

Model 3
Multi-tier Incremental Models

Malicious data transitions through different tiers with varying long-term and short-term horizons.
Multi-tier Incremental Models

- Model 1
- Model 2
- Model 3

Global Model

- Long-term horizon
- Short-term horizon

#0 #1 #2 #3

Benign

log (% accessed files)
Multi-tier Incremental Models

Suspicious

Global Model

Model 1  Model 1  Model 1  Model 1  Model 1  Model 1

Model 2  Model 2  Model 2  Model 3  Model 3  Model 3

#0  #1  #2  #3  Long-term horizon  Short-term horizon

log (% accessed files)
I’m Confused..

Suspicious

Process #1

Process-centric Models

System-centric Model

Process #n
I’m Confused..

Suspicious

Process #1

Process #n

LOOK FOR TRACES OF CRYPTO FUNCTIONS
Key Expansion: Part 1

I need lots of keys for use in later rounds. I derive all of them from the initial key using a simple mixing technique that’s really fast. Despite its critics, it’s good enough.

* By far, most complaints against AES’s design focus on this simplicity.
Traces of Crypto Primitives

Key schedules

77 3f 9d 50 2a 91 d5 86
a0 89 42 b2 f3 de b8 d3
32 f2 16 b0 88 e3 7e b4
1d 2d f4 b2 fa 6f 51 64
bd ce c7 e5 16 1b e1 dc
8f db 81 e5 50 8b c0 1a
7b 93 8f f4 64 c9 bf f3
a5 f8 25 be f5 9a 48 c8

Encryption Rounds

Round 1
Round 2
Round 3
Round N
Traces of Crypto Primitives

Key schedules

Encryption Rounds

Round 1

Round 2

Round 3

Round N

False Positives for AES: $2^{-1344}$
ShieldFS: Architecture

Process 1
address space

Process 2
address space

... Virtual memory

Process 1
open("file.txt")

Process 2
read(fp1)

... User space

I/O Manager (minifilter driver interface)

Kernel space
ShieldFS: Architecture

I/O Manager (mini-filter driver interface)

Process centric model 1

"Process 1 is suspicious"

System centric model

Virtual memory

User space

Kernel space
ShieldFS: Architecture

- Process 1 address space
- Process 2 address space
- ... Virtual memory

- Process 1
- Process 2
- ...

- I/O Manager (minifilter driver interface)
- Process centric model 1
- Process centric model 2
- ...

- "process 1 is suspicious"

- System centric model
- "search for crypto key schedule"

- User space
- Kernel space
- I/O Request Packets (IRPs)

- Feature values
- Detector

- open("file.txt")
- read(fp1)
- ...

- User space
- Kernel space
- Virtual memory
ShieldFS: Architecture

- Shielder
  - Disk drive
  - Shadow drive

- Process 1
  - Process centric model 1
  - "I/O Request Packets (IRPs)"
  - "search for crypto key schedule"
  - "process 1 is suspicious"
  - "process 2 is benign", "process 1 is malicious: kill it and restore files"

- Process 2
  - Process centric model 2
  - "delete process 2 file copies"
  - "restore process 1 files copies"

- System centric model
  - "open("file.txt")"
  - "read(fp1)"

- User space
  - I/O Manager (minifilter driver interface)
  - "I/O Request Packets (IRPs)"
  - "process 2 is benign"
ShieldFS: Architecture

- Process 1 address space
- Process 2 address space
- Disk drive
- I/O Manager (minifilter driver interface)

**Process-centric model 1**: "process 1 is suspicious"
**Process-centric model 2**: "process 2 is benign", "process 1 is malicious: kill it and restore files"

**System-centric model**: "restore process 1 files copies" "delete process 2 file copies"

**Shielder**

**Feature values**

**CryptoFinder**

"search for crypto key schedule"

**Detector**

"open("file.txt") read(fp1)"

**User space**
**Kernel space**

**Virtual memory**

**Shadow drive**
**Disk drive**

User space

Virtual memory

Kernel space
File Recovery Workflow

Start

Unknown

Monitor & COW on first write

File 2

offended file

MW

R

copy

File 2
File Recovery Workflow

Start

Unknown

Monitor & COW on first write

ShieldFS Detector
File Recovery Workflow

Start

Unknown

Monitor & COW on first write

ShieldFS Detector

Malicious

Restore original copies
File Recovery Workflow

Start

Unknown

Monitor & COW on first write

Malicious
Rollback

ShieldFS Detector

Benign

Clean old copies

Restore original copies
File Recovery Workflow

Start

Unknown

Monitor & COW on first write

Malicious

ShieldFS Detector

Benign

Restore original copies

Clean old copies
## Storage Overhead

<table>
<thead>
<tr>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>44.2¢</td>
</tr>
<tr>
<td>1.86¢</td>
</tr>
<tr>
<td>27.3¢</td>
</tr>
<tr>
<td>7.23¢</td>
</tr>
<tr>
<td>3.00¢</td>
</tr>
</tbody>
</table>
## Storage Overhead

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>34</td>
<td>14.73</td>
<td>0.63</td>
<td>4.29</td>
<td>0.18</td>
<td>44.2¢</td>
</tr>
<tr>
<td>2</td>
<td>87</td>
<td>0.62</td>
<td>0.19</td>
<td>0.95</td>
<td>0.29</td>
<td>1.86¢</td>
</tr>
<tr>
<td>4</td>
<td>122</td>
<td>9.11</td>
<td>0.73</td>
<td>8.53</td>
<td>0.68</td>
<td>27.3¢</td>
</tr>
<tr>
<td>5</td>
<td>47</td>
<td>2.41</td>
<td>0.56</td>
<td>5.49</td>
<td>1.29</td>
<td>7.23¢</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>1.00</td>
<td>0.39</td>
<td>3.35</td>
<td>1.28</td>
<td>3.00¢</td>
</tr>
</tbody>
</table>
## Storage Overhead

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>34</td>
<td>14.73</td>
<td>4.29</td>
<td>0.18</td>
<td>44.2¢</td>
</tr>
<tr>
<td>2</td>
<td>87</td>
<td>0.62</td>
<td>0.95</td>
<td>0.29</td>
<td>1.86¢</td>
</tr>
<tr>
<td>4</td>
<td>122</td>
<td>9.11</td>
<td>8.53</td>
<td>0.68</td>
<td>27.3¢</td>
</tr>
<tr>
<td>5</td>
<td>47</td>
<td>2.41</td>
<td>5.49</td>
<td>1.29</td>
<td>7.23¢</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td>1.00</td>
<td>3.35</td>
<td>1.28</td>
<td>3.00¢</td>
</tr>
</tbody>
</table>
More Numbers?
Detection & Recovery Capabilities

➢ 1483 unseen samples (from VT + Trend)
   ○ Locky, TeslaCrypt, CryptoLocker, Critroni, TorrentLocker, CryptoWall, Troldeh, CryptoDefense, PayCrypt, DirtyDecrypt, ZeroLocker, Cerber, WannaCry

➢ Files protected: always 100%
   ○ Even in case of missed detection

➢ Detection rate: 1436/1483, 96.9%
1483 unseen samples (from VT + Trend)
- **Locky**, **TeslaCrypt**, **CryptoLocker**, **Critroni**, **TorrentLocker**, **CryptoWall**, **Troldesh**, **CryptoDefense**, **PayCrypt**, **DirtyDecrypt**, **ZeroLocker**, **Cerber**, **WannaCry**

Files protected: always 100%
- Even in case of missed detection

Detection rate: 1436/1483, **96.9%**
False Positive Evaluation

FPR with One-machine-off Cross Validation
# False Positive Evaluation

## FPR with One-machine-off Cross Validation

<table>
<thead>
<tr>
<th>User Machine</th>
<th>False positive rate [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Process</td>
</tr>
<tr>
<td>1</td>
<td>0.53</td>
</tr>
<tr>
<td>2</td>
<td>0.00</td>
</tr>
<tr>
<td>3</td>
<td>0.00</td>
</tr>
<tr>
<td>4</td>
<td>0.00</td>
</tr>
<tr>
<td>5</td>
<td>0.22</td>
</tr>
<tr>
<td>6</td>
<td>0.00</td>
</tr>
<tr>
<td>7</td>
<td>0.00</td>
</tr>
<tr>
<td>8</td>
<td>0.00</td>
</tr>
<tr>
<td>9</td>
<td>0.00</td>
</tr>
<tr>
<td>10</td>
<td>0.00</td>
</tr>
<tr>
<td>11</td>
<td>0.00</td>
</tr>
</tbody>
</table>
Overhead: Micro-benchmark

- **Sequence 1 = Open + Read**
- **Sequence 2 = Open + Write (and backup)**
- **Sequence 3 = Open + Write (no backup)**

File size:

- $1KB$, $2KB$, $4KB$, $8KB$, $16KB$, $32KB$, $64KB$, $128KB$, $256KB$, $512KB$, $1MB$, $2MB$, $4MB$, $8MB$, $16MB$, $32MB$, $64MB$, $128MB$
...however...
Average estimated overhead = 0.26×
User-Perceived Overhead

Average estimated overhead = 0.26×
Demo Time!

WannaCry Sample: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Ransomware significantly differs from benign software from the filesystem’s viewpoint.

**DETECTION.** Generic ML models to identify ransomware
- Filesystem activity
- Use of symmetric crypto primitives

**PROTECTION.** Pure detection is not enough
- Self-healing virtual FS
- Transparently revert the effects of ransomware
Questions?

Andrea Continella
andrea.continella@polimi.it
@_conand

Federico Maggi
federico_maggi@trendmicro.com
@phretor

http://shieldfs.necst.it

* This work is subject to a US patent (pending) no. 27019

ShieldFS: A Self-healing, Ransomware-aware Filesystem

Andrea Continella
andrea.continella@polimi.it

Alessandro Guagnelli
alessandro.guagnelli@polimi.it

Giovanni Zingaro
giovanni.zingaro@polimi.it

Giulio De Pasquale
giulio.depasquale@polimi.it

Alessandro Barenghi
alessandro.barenghi@polimi.it

Stefano Zanero
stefano.zanero@polimi.it

Federico Maggi
federico.maggi@polimi.it

DEIB, Politecnico di Milano, Milan, Italy

ABSTRACT
Preventive and reactive security measures can only partially mitigate the damage caused by modern ransomware attacks.

1 INTRODUCTION
Ransomware [20] is a class of malware that encrypts valuable files found on the victim’s machine and asks for a ransom to recover them.
ShieldFS: The Last Word in Ransomware Resilient Filesystems

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, Federico Maggi