Towards ransomware-resilient operating systems

Andrea Continella, Alessandro Guagnelli, Giovanni Zingaro, Stefano Zanero, Federico Maggi

Politecnico di Milano

19-11-2015
@INFOSEK 2015

NECST laboratory

Your personal files are encrypted.

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

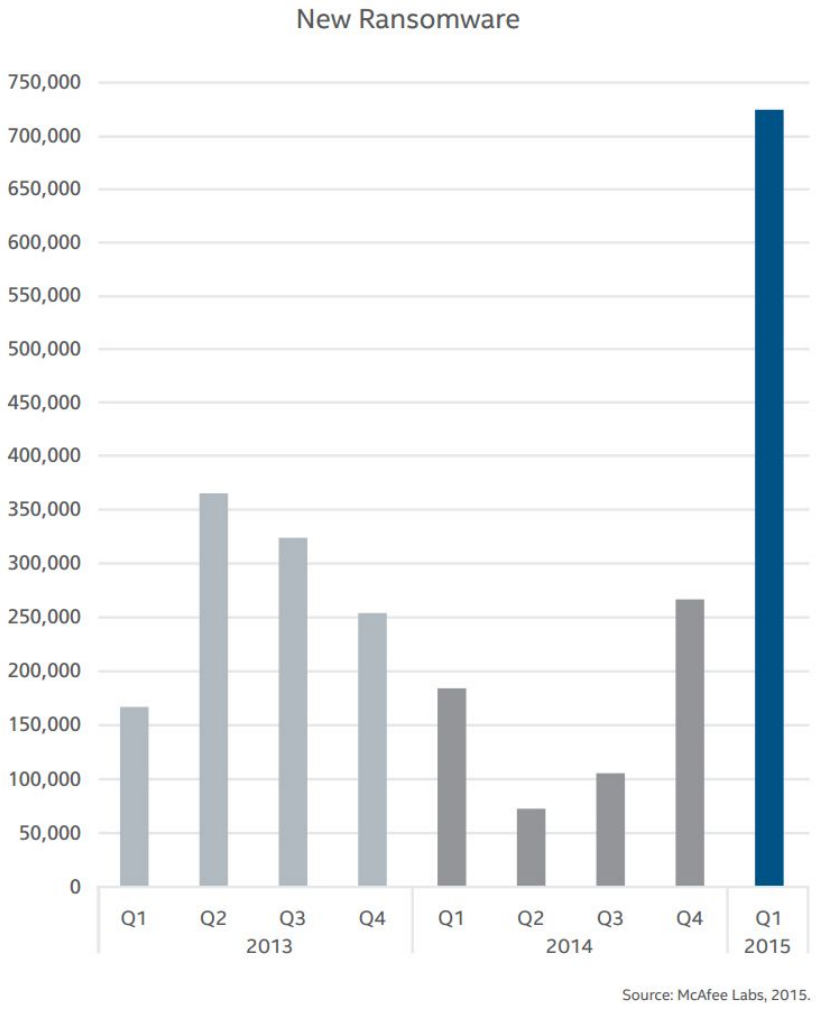
View

71:59:07

Next >>

can open it and use copy-paste for address and key.

Ransomware attacks



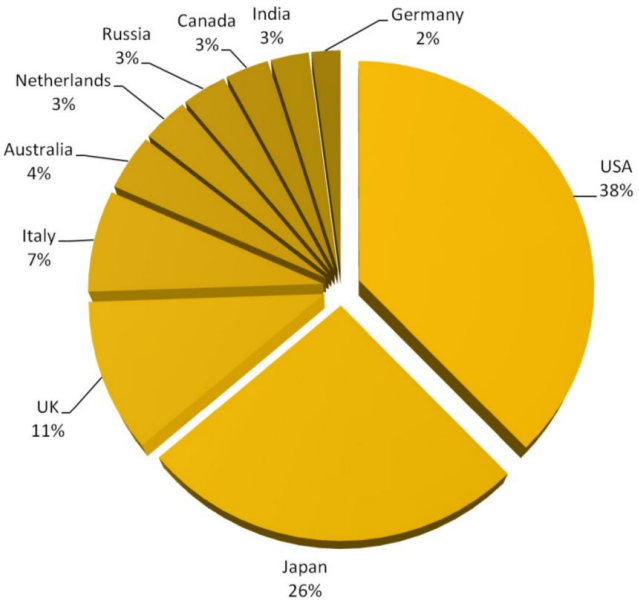
Source: McAfee Labs, 2015.

$255,000 Stolen

McAfee Labs observed the theft of **$255,000 in a single month** in one CryptoLocker ransomware instance.

2 Million Samples

The total number of ransomware samples in the McAfee Labs zoo surpassed **2 million in Q3 2014.**



Tox Viruses Stats Chat Profile [redacted] Logout

Tox - Viruses

toxic[redacted]qj.onion

Summary

Viruses	1
Infected	2
Of which paid	0

Total profit	0.00 $
To withdraw (net)	0 Ƀ

Your BTC address

Withdraw

Create a virus

Ransom - $ — Ransom in dollars (min. 50)

Notes* — Optional, ex: For Mr. Smith

Message** — Optional message for the victims

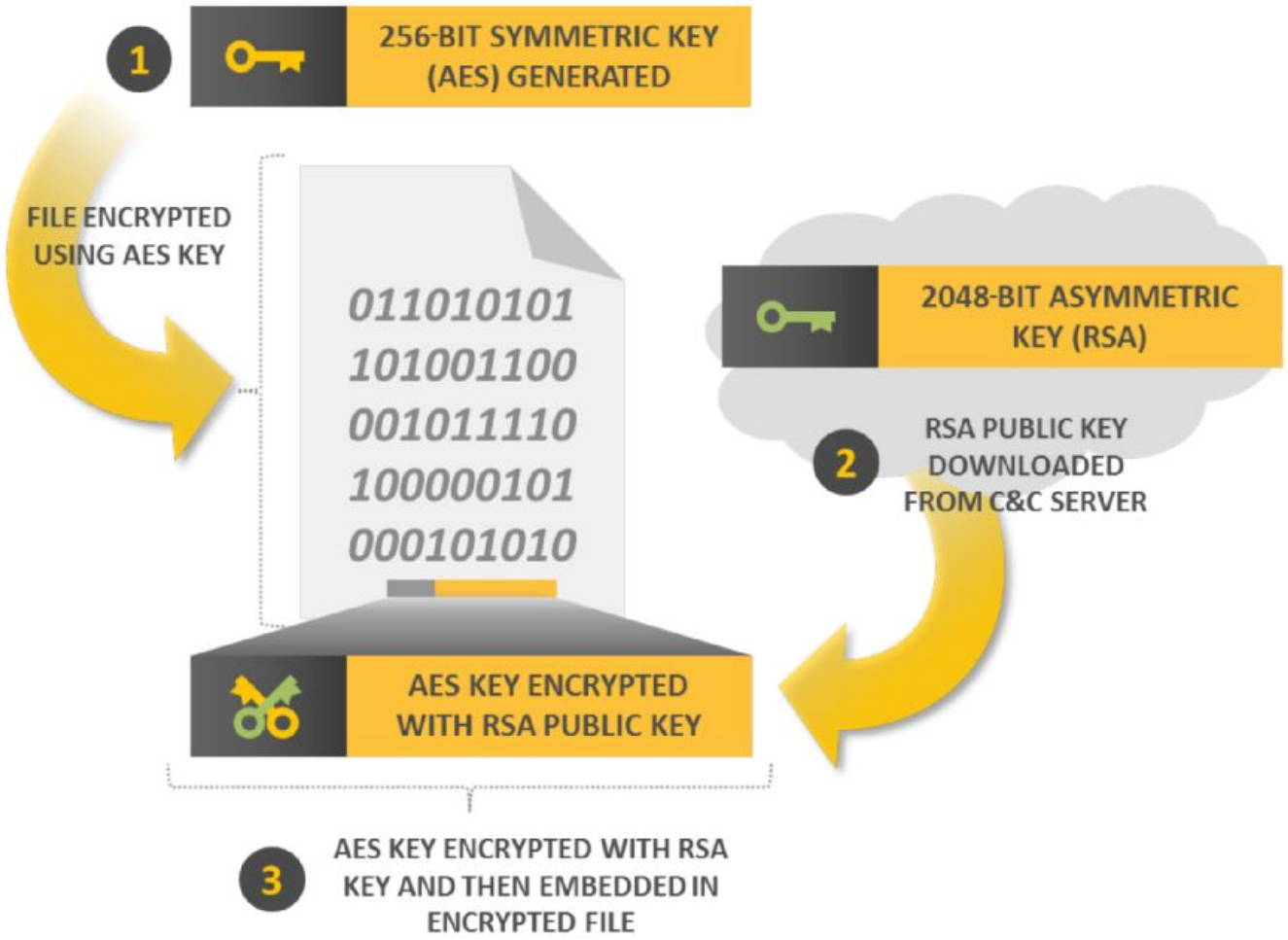
Captcha — Captcha

Create

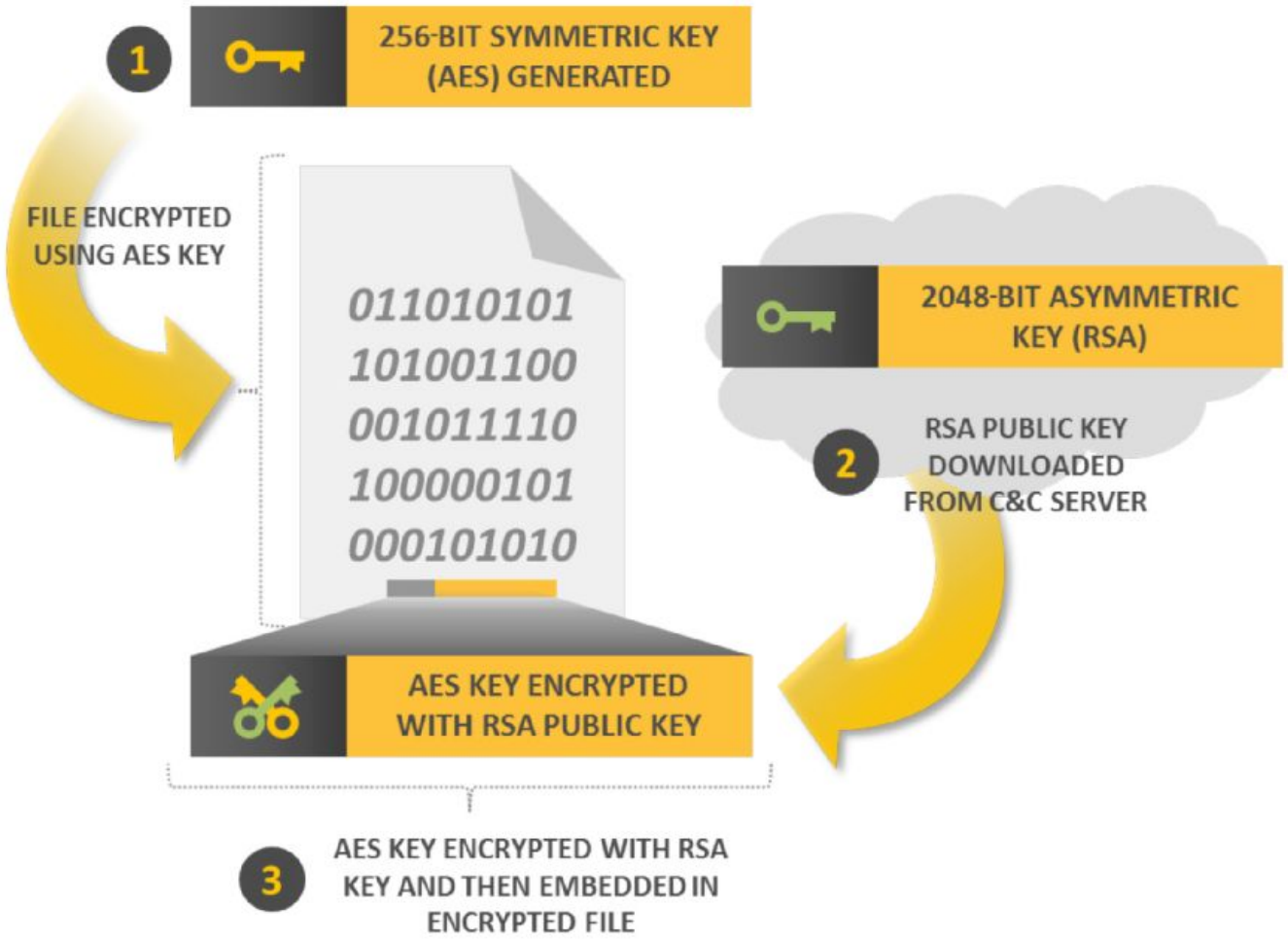
** Notes are private, they're just to keep track of your virus. Victims will not see them! (max 200 chars)*
*** Message will be shown in the ransom page to the victims (max 1500 chars | no html)*

Your viruses

Encryption mechanism



Encryption mechanism



No way to retrieve files without the key after encryption!

How can we stop ransomware?

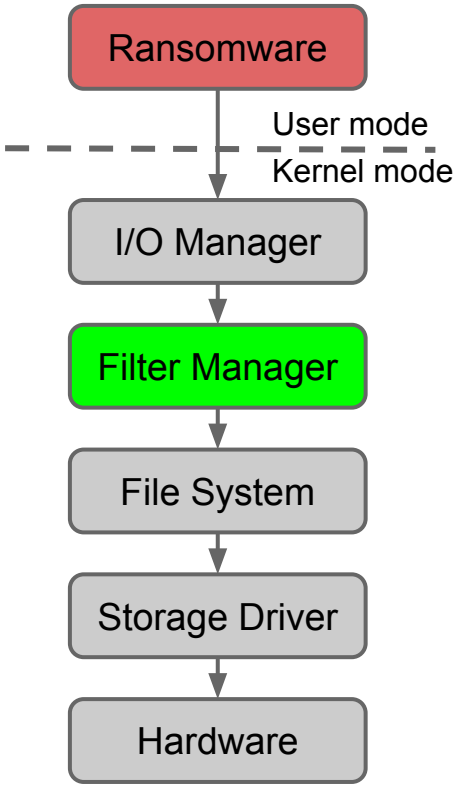
- Is a classical antivirus enough?
  - Unfortunately no
  - Signatures must be updated
  - Executables are obfuscated and encrypted
  - New families require manual reverse engineering
- Why don’t we monitor Crypto API call?
  - Malware can easily implement its own crypto functions
- The Operating System should be able to detect malicious ransomware
  - Idea: Look at the **File System’s activity**!

Our research

- Observe the ransomware attacks looking at the file system's activity
- Identify ransomware common features
  - **High Entropy** Writes
  - **Wide access** to the file system
  - **Repeated** access **patterns** (e.g., Read, Write, Delete)
- Design a **generic** detection model
- Modify the OS to be able to **detect** and **revert** ransomware attacks

Data Collection

- Develop a Windows Kernel module to monitor and log the file system activity
  - Windows Minifilter Driver
  - Log IRPs (I/O Request Packets)
- Run ransomware samples and collect data about the activity of the file system during their execution
- Distribute the IRP logger to clean users
  - Collect data about the activity of the file system during “normal” clean executions

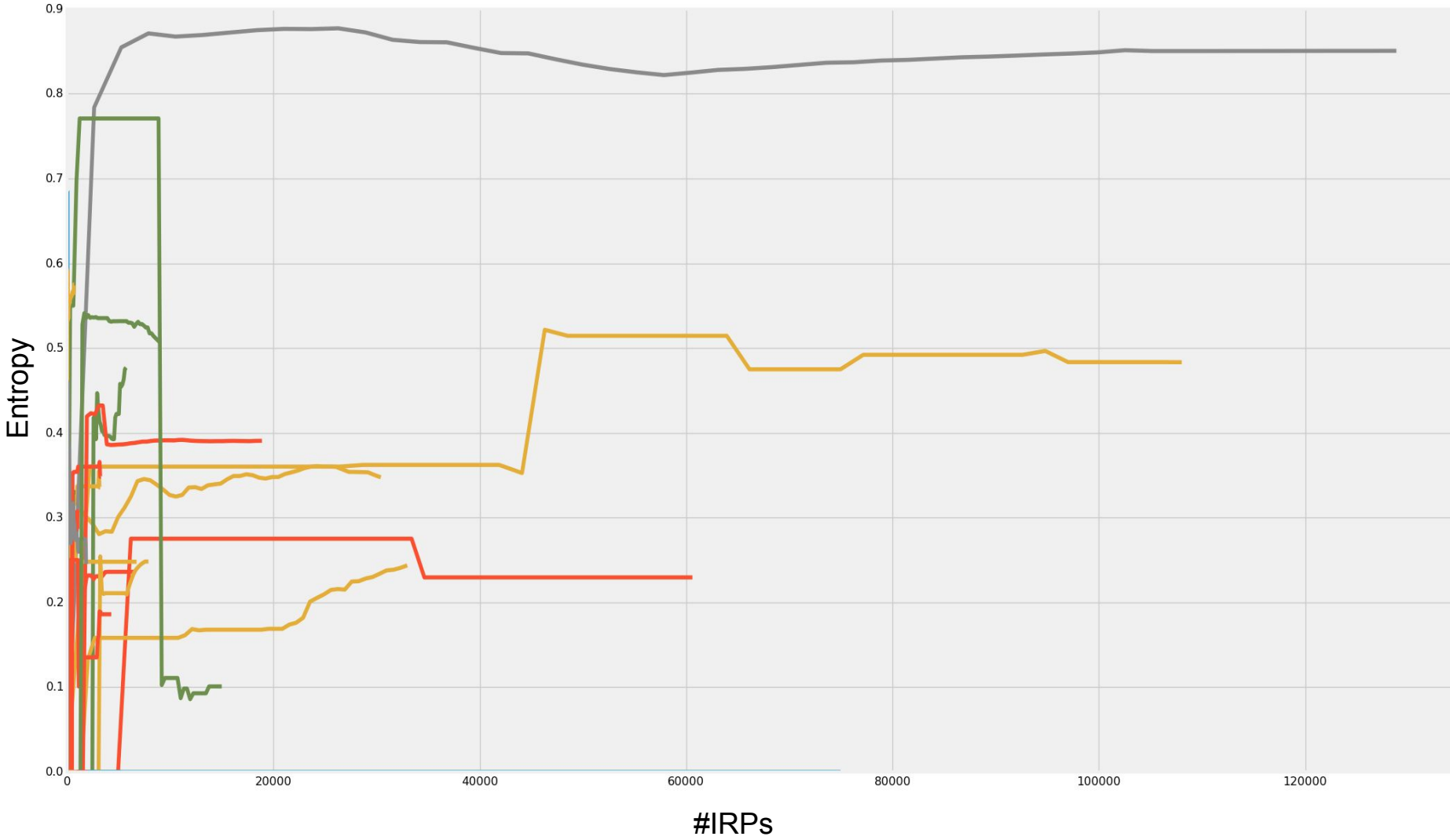


Opr	*Process.Thread*		*ProcessName*	*Operation*		*Buffer*	*Entropy*	*Name*
				Major	*Minor*			
IRP	3116	3120	C:\Program Files\..\wmpnscfg.exe	Create		0	0.00000	..\WMPNSCFG-FC0D39BF.pf
IRP	1772	1088	C:\Windows\..\SearchIndexer.exe	Read	Normal	32768	0.43402	..\BootCKCL.etl
FIO	824	2532	C:\Windows\System32\svchost.exe	Read	Normal	17920	0.43748	..\vssadmin.exe.mui
IRP	3116	3120	C:\Program Files\..\wmpnscfg.exe	Read	Normal	22516	0.49521	..\WMPNSCFG-FC0D39BF.pf
IRP	4	168	System	Write	Normal	131072	0.54708	..\..\LogFiles\BootCKCL.etl
IRP	796	2692	C:\Windows\System32\svchost.exe	Close		0	0.00000	..\..\CSC\v2.0.6\namespace
FSF	3180	3184	C:\Windows\System32\mobsync.exe	Release		0	0.00000	..\..\System32\winsta.dll

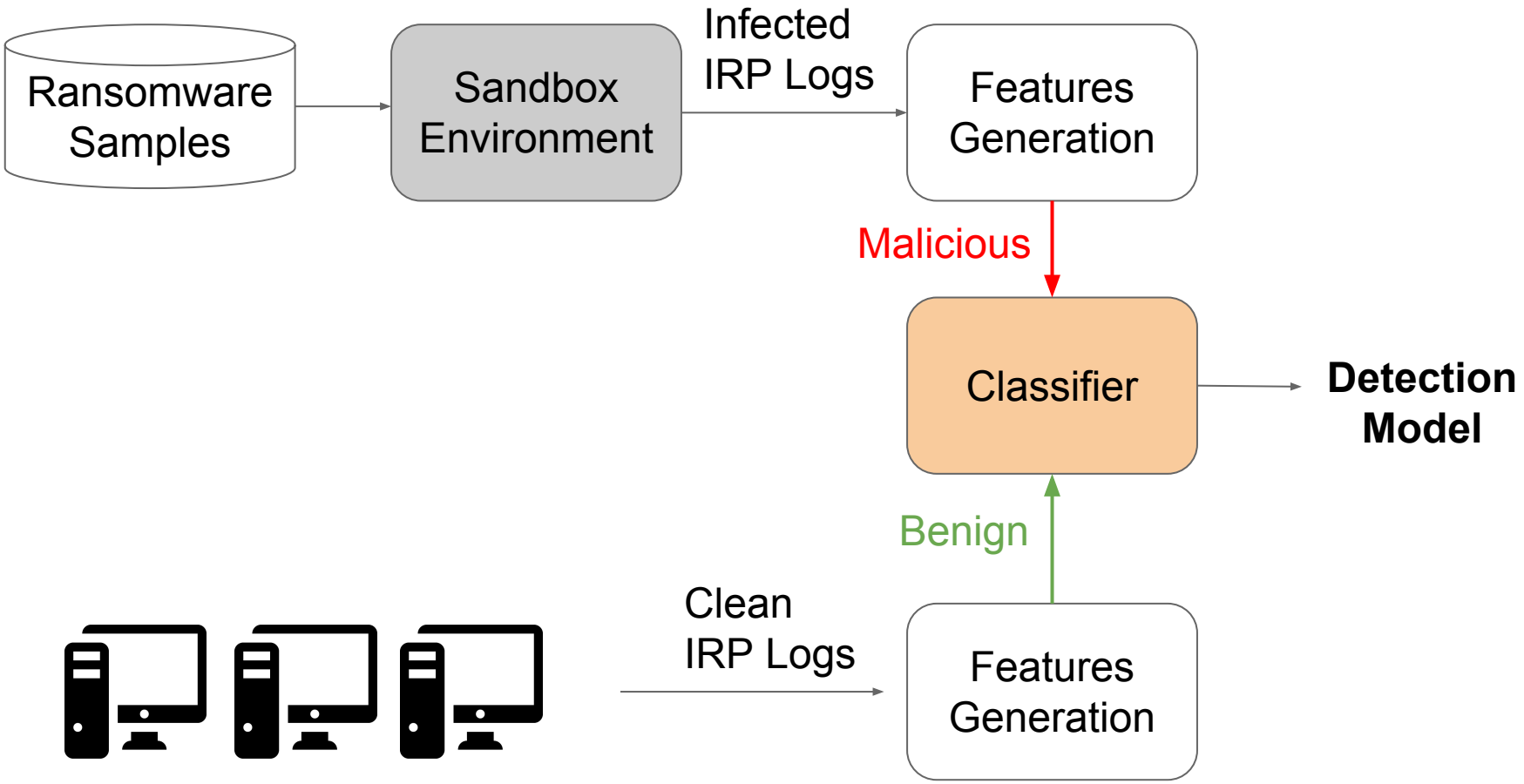
Features extraction

- Entropy evaluation
  - Calculate entropy of the buffers to be written
- Amount of IRP generated
  - Amount of read operations
  - Amount of write operations
- Spread access to the file system
  - Number of different files a process is reading/writing
- Feature normalization
  - Spread access score is weighted by the total number of files

Entropy evaluation



Ransomware Detection

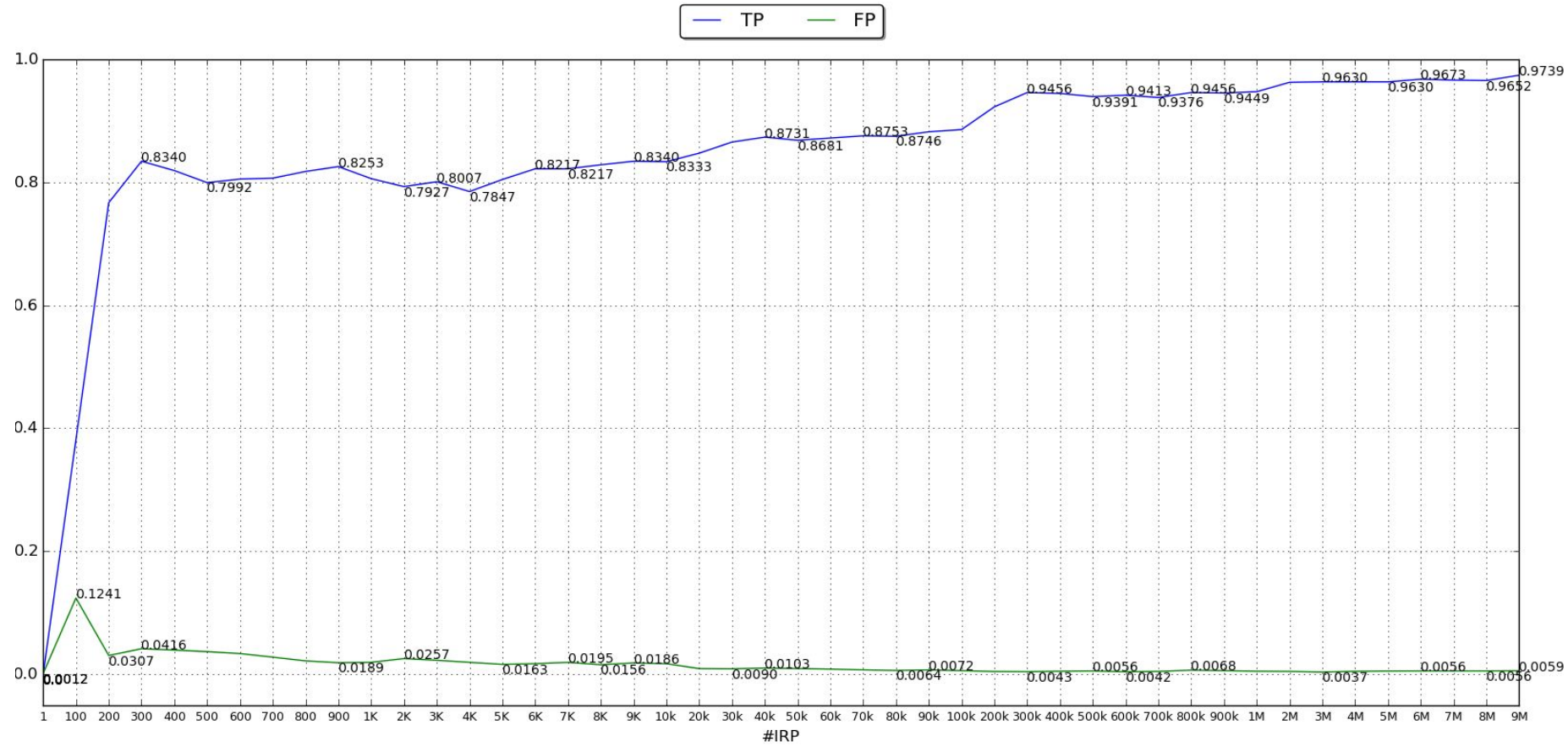


Dataset

- 124 samples of different ransomware families (CryptoLocker, TeslaCrypt, CTBLocker, CryptoWall)
- clean data collected from 5 users

Machine	*Usage*	*Compressed Data (GB)*	*#IRPs (x10^6)*	*Time*	
				(hour)	*Total (day)*
1	dev	0.52	33.48	10	18
2	dev	3.11	234.71	37	12
3	home	0.52	20.49	5.3	5
4	home	1.16	76.25	27.4	12
5	home	0.14	8.94	15.3	6

Detection Results



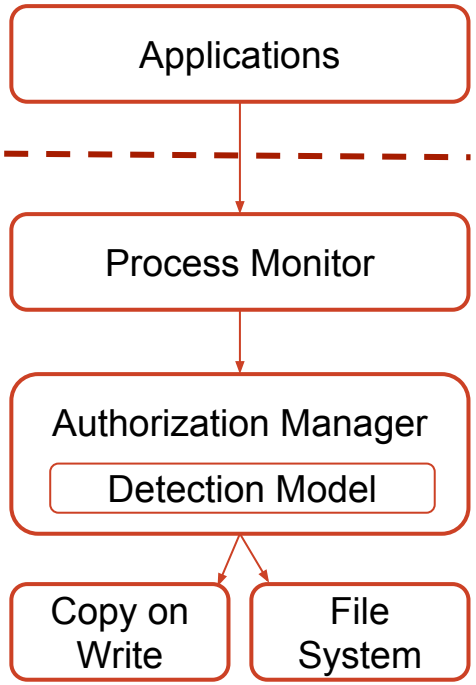
- Ten-fold cross validation
- Classifier: Random Forest

What if we detect a ransomware too late?

Provide a further layer upon the file system able to revert the effects of ransomware once detected

Ransomware-resilient file system

- Extend the file system with a component able to revert the effects of ransomware
  - Monitor processes activity on the file system
  - Let process access the real file system only if authorized
  - Use a Copy on Write approach for unknown processes
  - Restore original data if a process is detected as ransomware
  - Commit modifications to the real file system if a process is identified as legitimate



Future work

- Extend the dataset and perform further evaluations
- Design a system-centric model and compare the performance respect to the process-centric model
- Deeper study of the dataset of benign IRPs, focusing the attention on access patterns
- Detect uses of cryptographic functions

Conclusions

- Modern Operating Systems should detect ransomware and be able to **revert their effects**, once detected
- **Generic** model to identify ransomware behaviours observing the file system activity

Thank you!
Questions?

andrea.continella@polimi.it

@_conand

NECST laboratory