WannaFly: Dummy Ransomware for Red Team Exercises

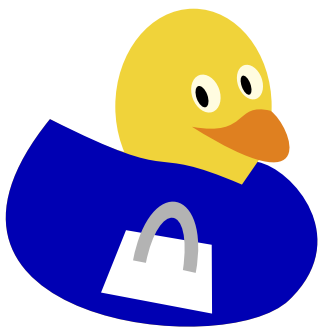
Maman Sani Aboubacar Djibo[1], Hamid Boukerrou[2,3], Dylan Marinho[2], Angelo Saadeh[4] and Benjamin Somers[5,6]

[1] Université de Montpellier, CNRS, LIRMM, Montpellier, France
[2] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
[3] Université de Lorraine, CNRS, CRAN, Nancy, France
[4] Telecom Paris, LTCI, Inria, Paris, France
[5] Crédit Mutuel Arkéa
[6] Lab STICC UMR 6285, IMT Atlantique, Brest, France

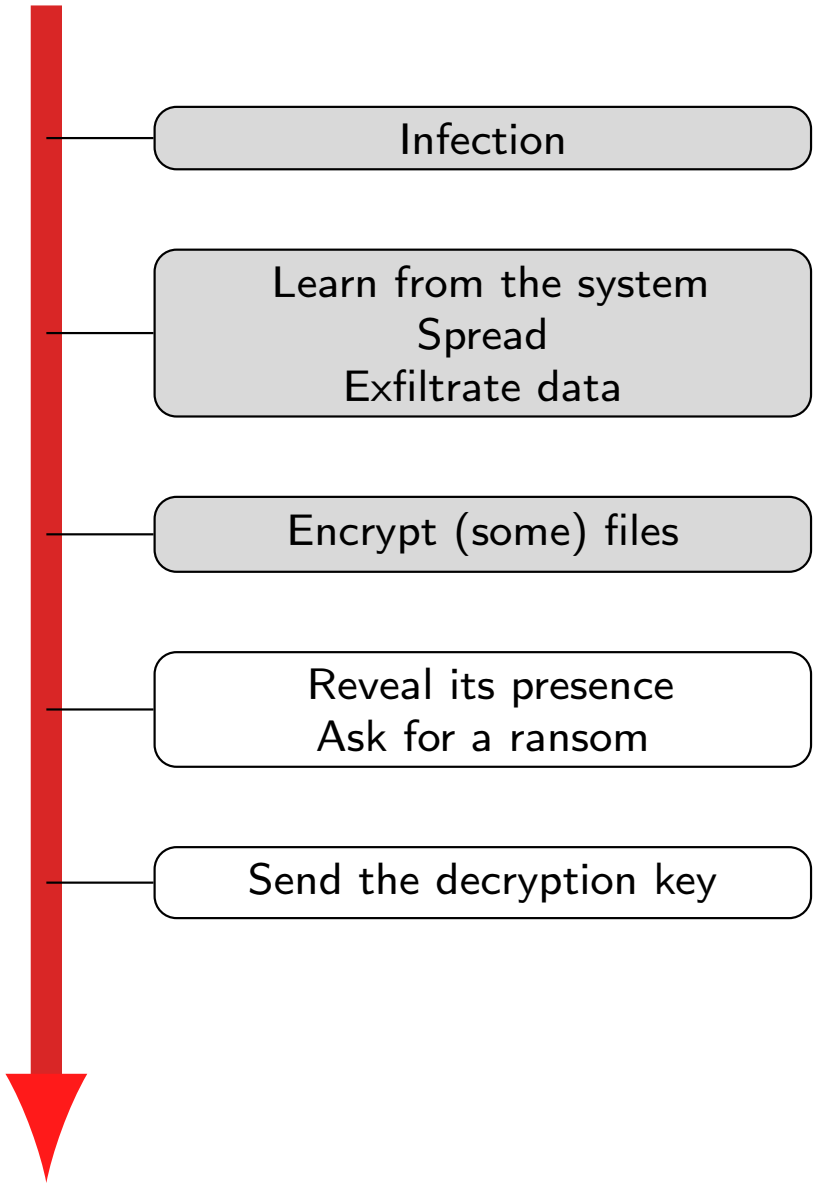
Research topic proposed and supervised by
Jean-Romain Garnier, Airbus

25-29 October 2021
Luminy

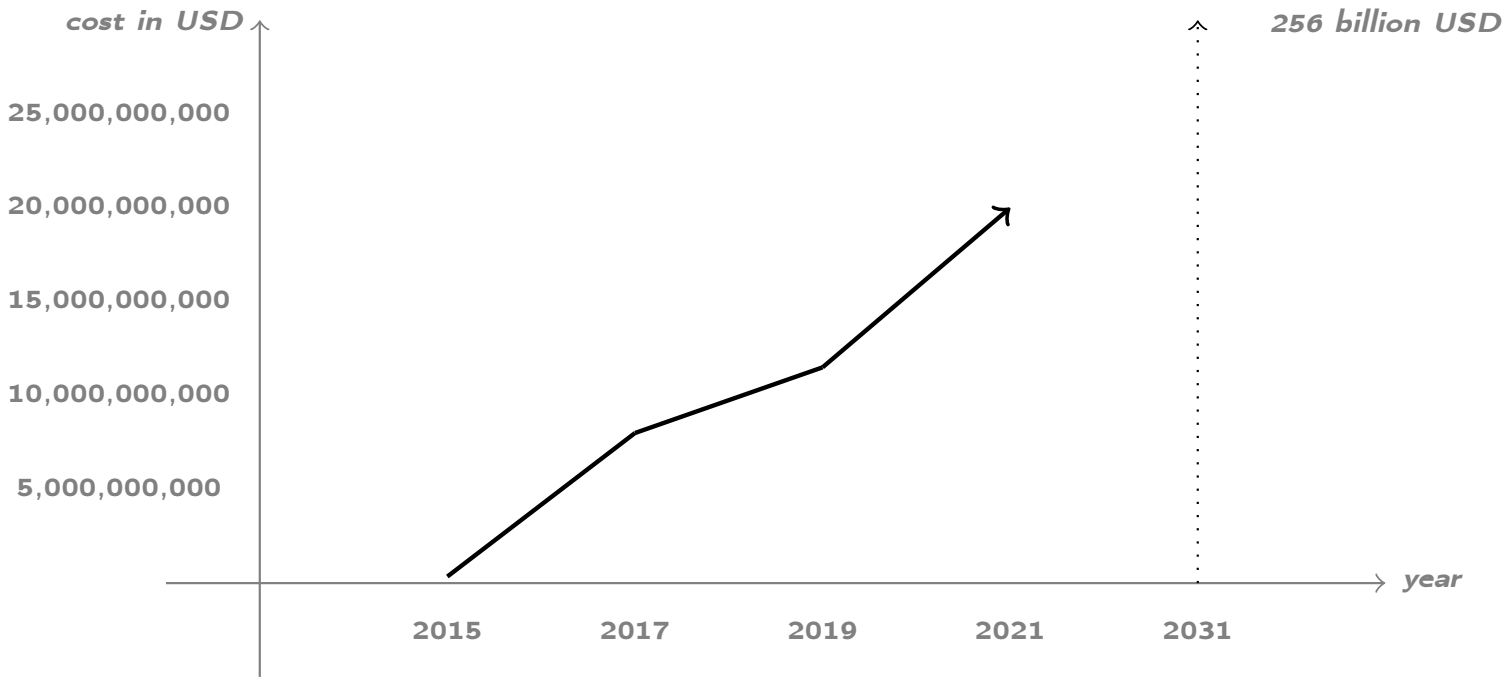
What is a ransomware?



How does a ransomware work?



A story of money



Global Ransomware Damage Costs [Bra21]

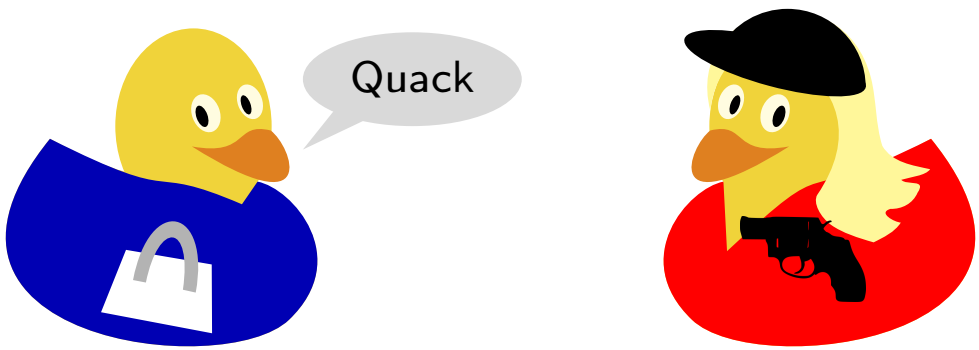
[Bra21] David Braue. Global Ransomware Damage Costs Predicted To Exceed 265 Billion USD By 2031. June 2021

An overview of malware detection techniques

Signature-based analysis

Classify binaries by looking at particular patterns in their code

"Have I already seen this binary?"



Behavioral-based analysis

Detect malware based on their behavior

"What does it want to do?"

A cat and mouse game

[Bio+18]

	Simple malware
No defense	√

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

A cat and mouse game

[Bio+18]

	Simple malware
No defense	√
Signature analysis	×

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

A duck and dodge game

[Bio+18]

	Simple malware	Small variations
No defense	√	√
Signature analysis	×	√

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

A duck and dodge game

[Bio+18]

	Simple malware	Small variations
No defense	√	√
Signature analysis	×	√
Dynamic analysis	×	×

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

A duck and duck game

[Bio+18]

	Simple malware	Small variations	Anti-sandboxing
No defense	√	√	√
Signature analysis	×	√	√
Dynamic analysis	×	×	√

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

A duck and duck game

[Bio+18]

	Simple malware	Small variations	Anti-sandboxing
No defense	√	√	√
Signature analysis	×	√	√
Dynamic analysis	×	×	√
Concolic analysis	×	×	×

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

Quaaaaack

[Bio+18]

	Simple malware	Small variations	Anti-sandboxing	Symbolic explosion
No defense	√	√	√	√
Signature analysis	×	√	√	√
Dynamic analysis	×	×	√	√
Concolic analysis	×	×	×	√

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

Quaaaaack

[Bio+18]

	Simple malware	Small variations	Anti-sandboxing	Symbolic explosion
No defense	√	√	√	√
Signature analysis	×	√	√	√
Dynamic analysis	×	×	√	√
Concolic analysis	×	×	×	√

Most of the widespread anti-malwares only uses signature analysis

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

Quaaaaack

[Bio+18]

	Simple malware	Small variations	Anti-sandboxing	Symbolic explosion
No defense	√	√	√	√
Signature analysis	×	√	√	√
Dynamic analysis	×	×	√	√
Concolic analysis	×	×	×	√

Most of the widespread anti-malwares only uses signature analysis

But, you can imagine more advanced statistical analysis

e.g. checking the imported libraries

[Bio+18] Fabrizio Biondi et al. "Tutorial: an Overview of Malware Detection and Evasion Techniques". In: ISoLA 2018 - 8th International Symposium On Leveraging Applications of Formal Methods, Verification and Validation. Oct. 2018, pp. 1–23

How to organize a reaction?

[Hel21]

Red team

- Serve as the attacker in a simulation
- Use the same techniques and tools of hackers to evade detection and test the defense
- Check the readiness of the internal security team

Blue team

- Detect adversaries
- Prevent them from breaking into the organization's infrastructure

[Hel21] HelpSystems. Red Team. 2021

How to organize a reaction?

[Hel21]

Red team

- Serve as the attacker in a simulation
- Use the same techniques and tools of hackers to evade detection and test the defense
- Check the readiness of the internal security team

Blue team

- Detect adversaries
- Prevent them from breaking into the organization's infrastructure

Why teaming?

- Uncover vectors that attackers could exploit
- Demonstrate how attackers could move throughout a system
- Provide insight on organization's ability to prevent, detect, and respond to advanced threats

[Hel21] HelpSystems. Red Team. 2021

Outline

Project subject

Our proposal: WannaFly
- The context
  - The goals of the Red Team
- Preliminary steps
- Ransomware structure
- Encrypting files
  - Which files to encrypt?
  - Encryption method
- Impact analysis
- End of life

Evaluation

Conclusion

Outline

Project subject

Our proposal: WannaFly

Evaluation

Conclusion

The project

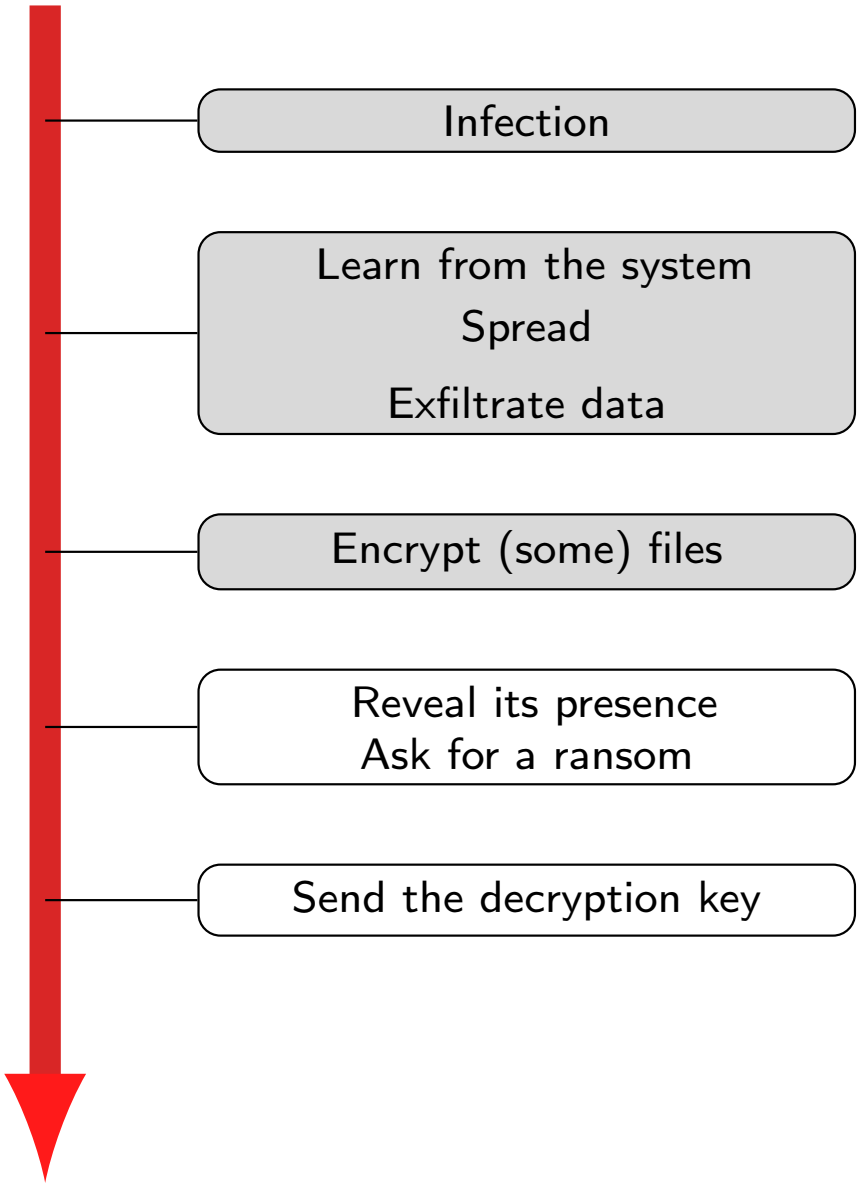
Subject

Dummy Ransomware for
Red Team Exercises

The project

Subject

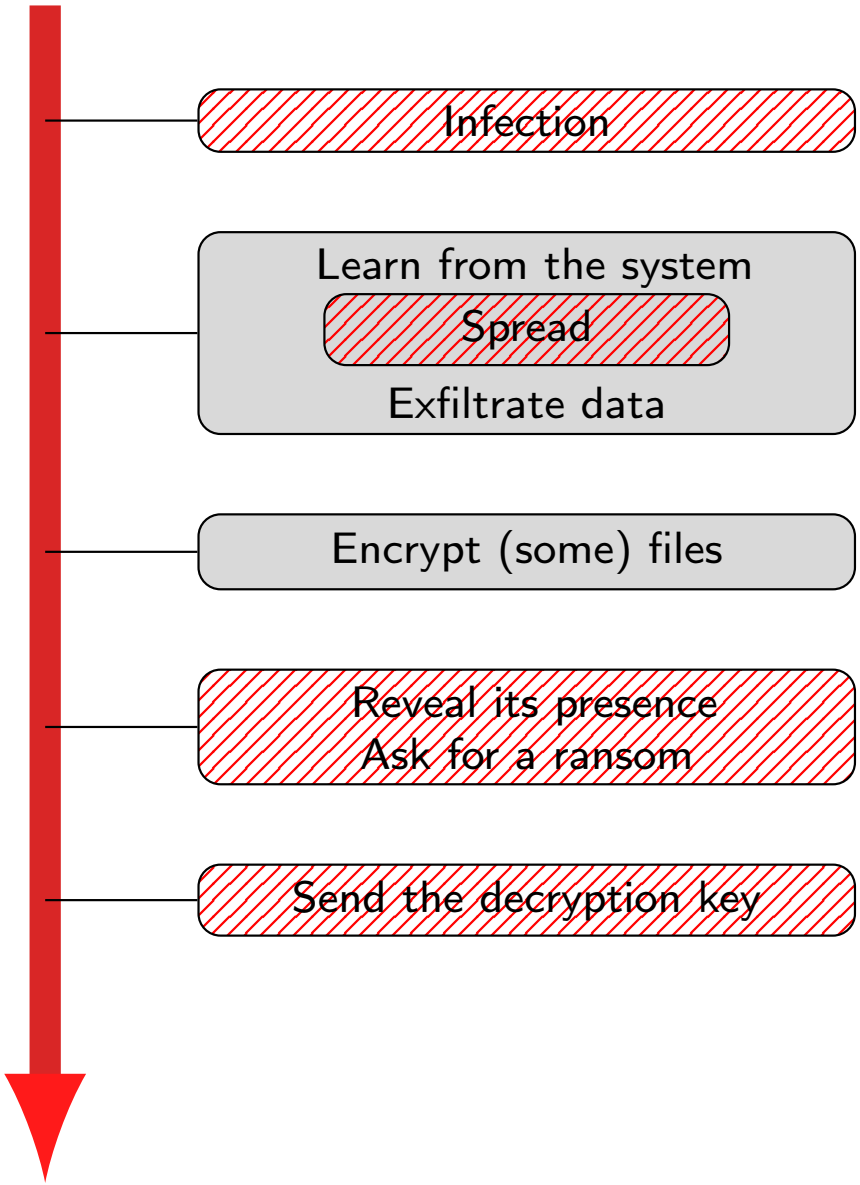
Dummy Ransomware for
Red Team Exercises



The project

Subject

Dummy Ransomware for
Red Team Exercises



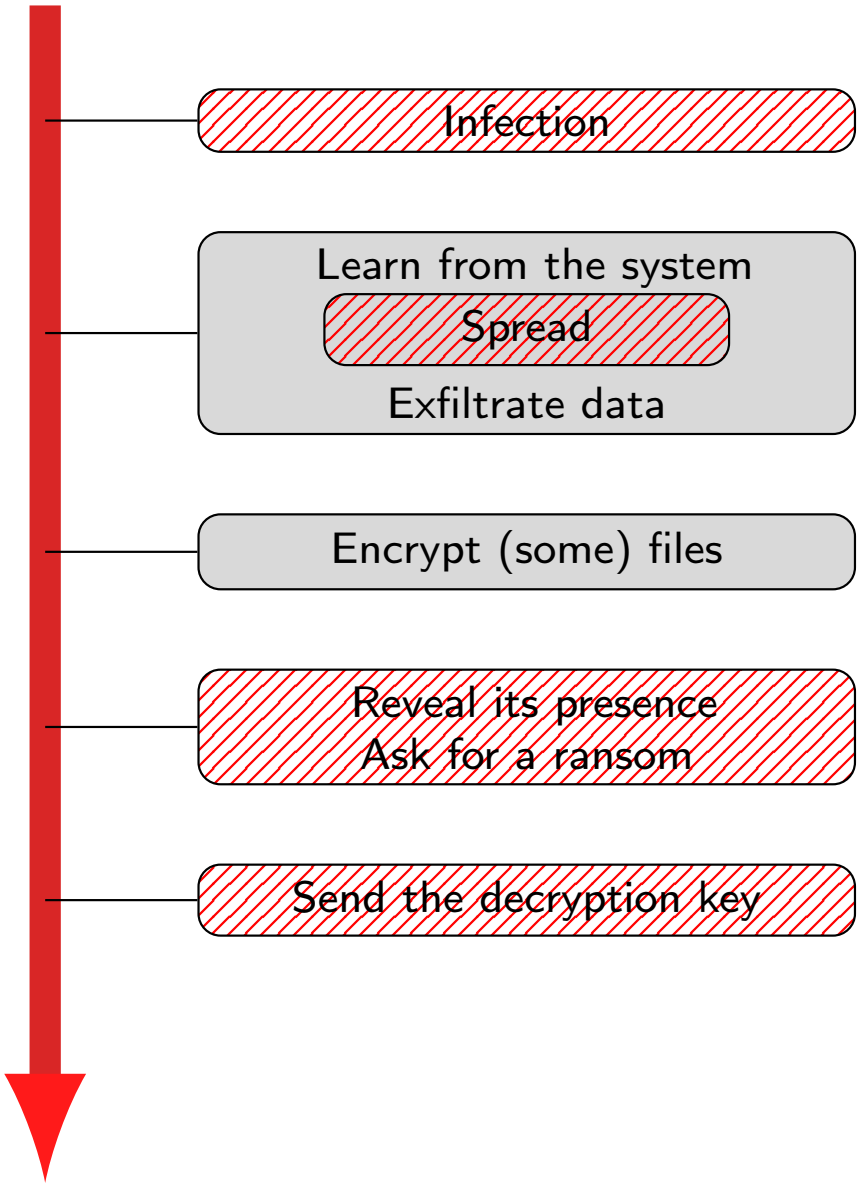
The project

Subject

Dummy Ransomware for Red Team Exercises

Limits

- Not be detected before execution
- Do not make too many assumptions about the target system



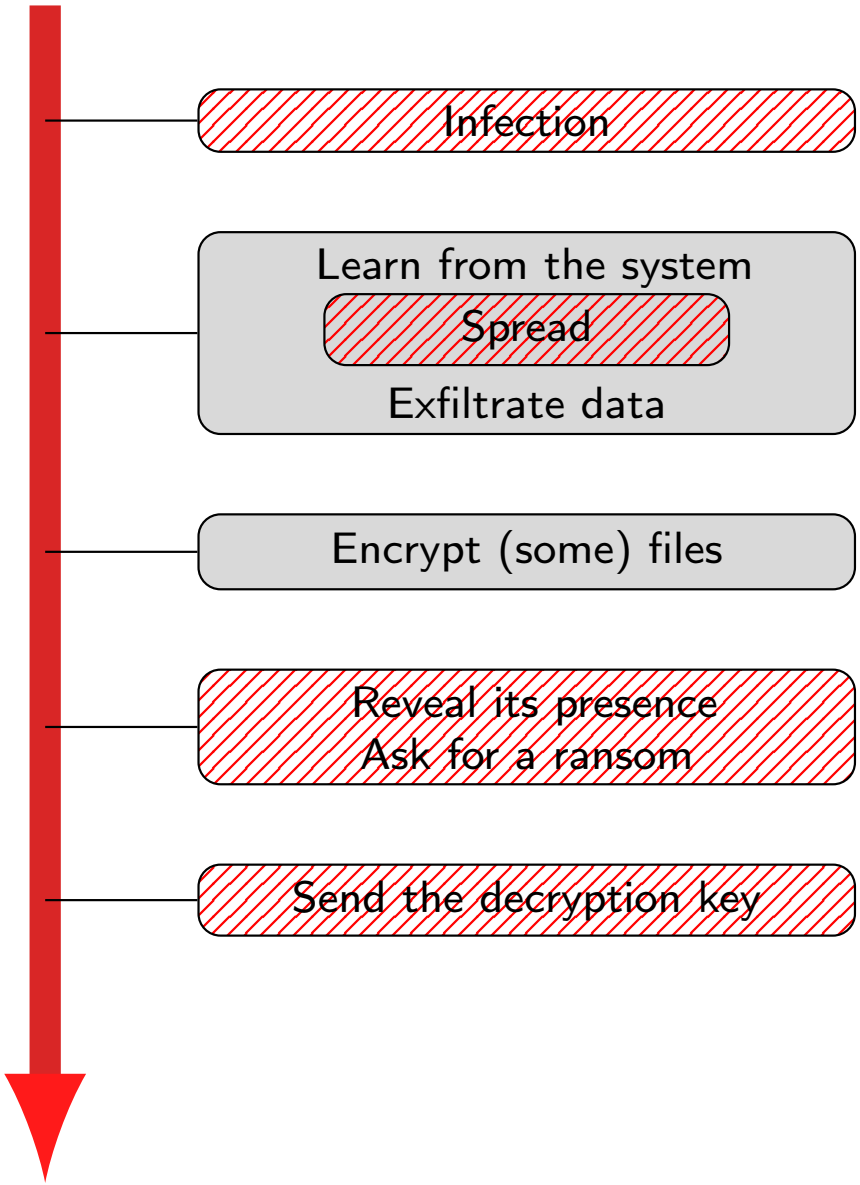
The project

Subject

Dummy Ransomware for Red Team Exercises

Limits

- Not be detected before execution
- Do not make too many assumptions about the target system
- Do not have significant operational impacts
- Do not perform actions that have a permanent impact



The project

Subject

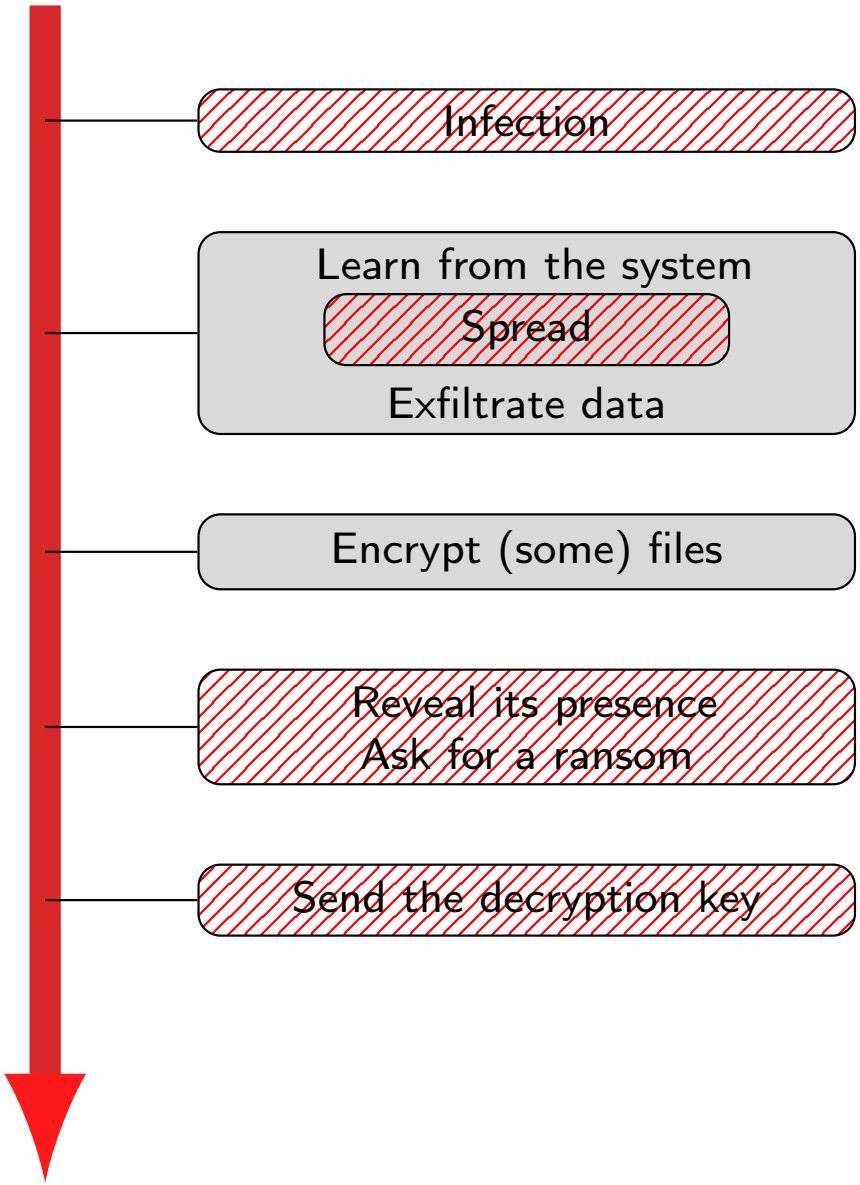
Dummy Ransomware for Red Team Exercises

Limits

- Not be detected before execution
- Do not make too many assumptions about the target system
- Do not have significant operational impacts
- Do not perform actions that have a permanent impact

Keep a track

- Leave evidence of compromise
- Keep logs of all actions



State-of-the-art: Open-source ransomwares

Name	File selection	Key per file	Encrypt. file key	Required attacker communication
Ransom0	extension	×	×sent to server	encryption and decryption
RAASNet	extension	×	×sent to server	encryption and decryption
CryptSKY	extension	×	×sent to server	encryption and decryption
CryptoTrooper	directories	×	yes (White-box)	decryption
GonnaCry	extension	√	(√) RSA – 1 time	decryption

State-of-the-art: Open-source ransomwares

Name	File selection	Key per file	Encrypt. file key	Required attacker communication
Ransom0	extension	×	×sent to server	encryption and decryption
RAASNet	extension	×	×sent to server	encryption and decryption
CryptSKY	extension	×	×sent to server	encryption and decryption
CryptoTrooper	directories	×	yes (White-box)	decryption
GonnaCry	extension	√	(√) RSA – 1 time	decryption

WannaFly	extension, duplicated, recently used, ...	√	√ RSA – immediately	decryption

Outline

Project subject

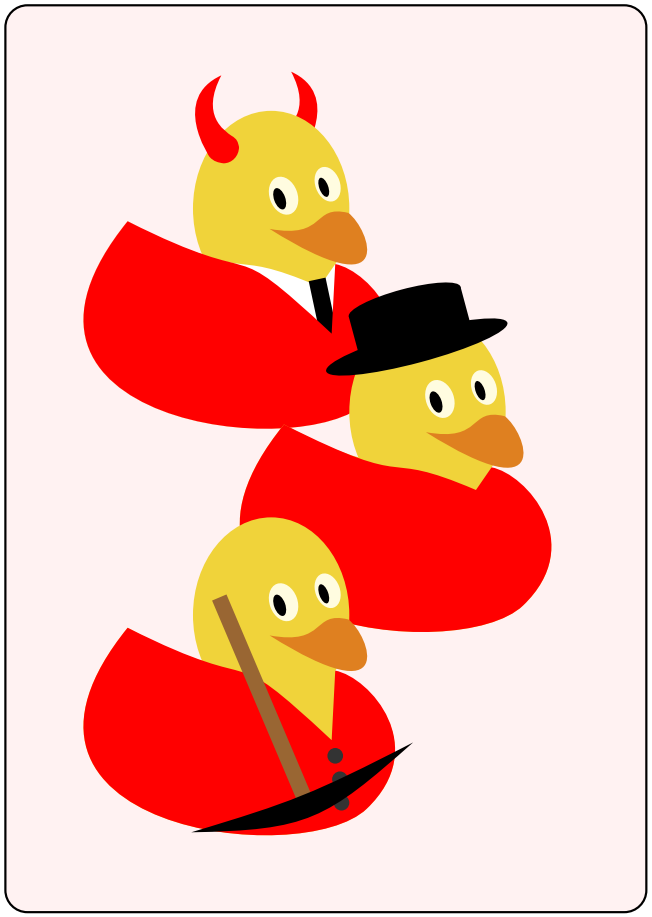
Our proposal: WannaFly
- The context
- Preliminary steps
- Ransomware structure
- Encrypting files
- Impact analysis
- End of life

Evaluation

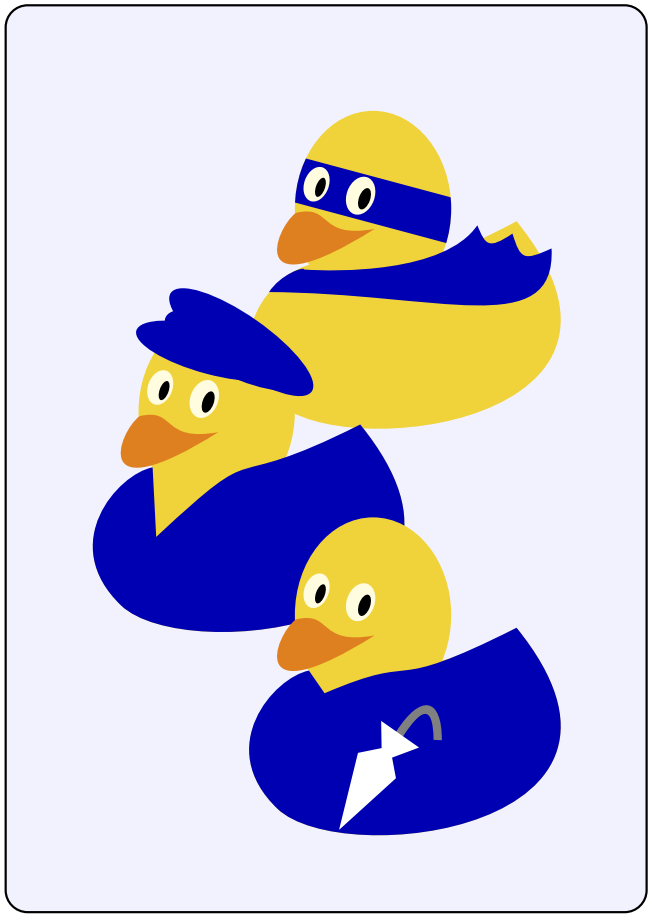
Conclusion

The context

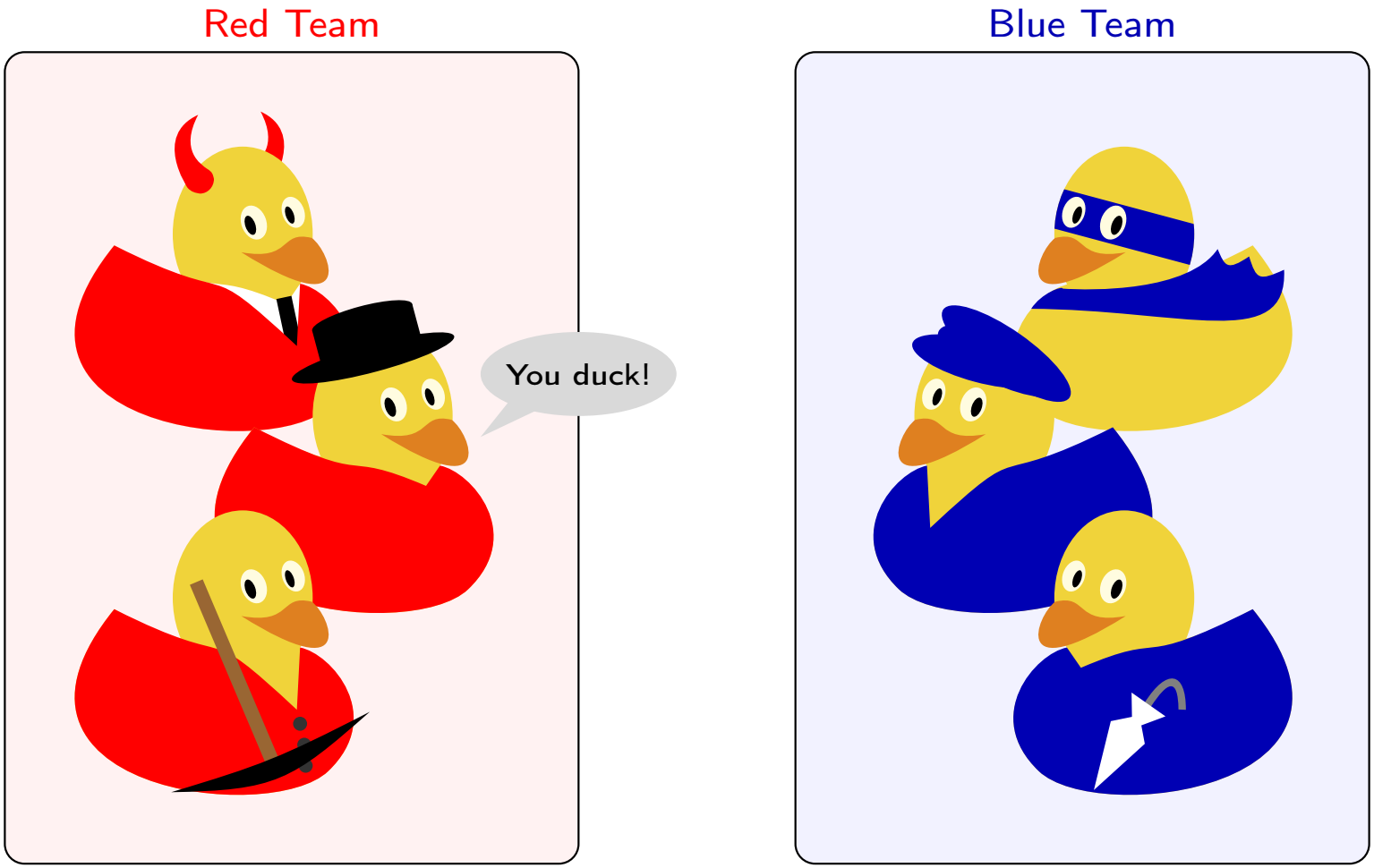
Red Team



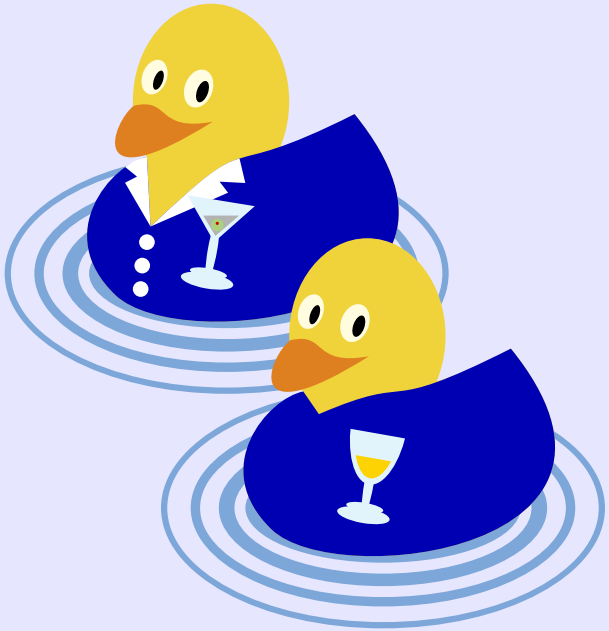
Blue Team



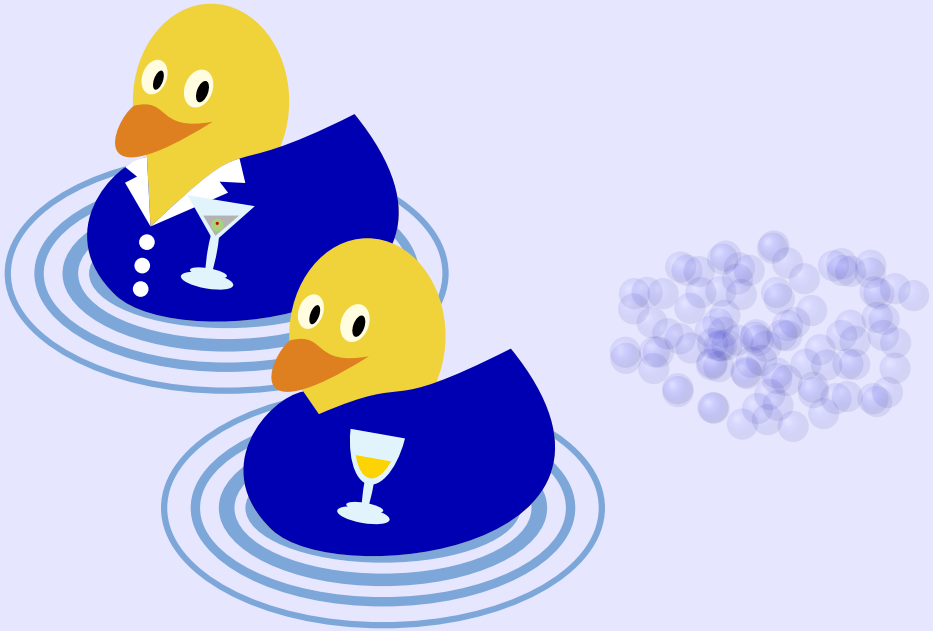
The context



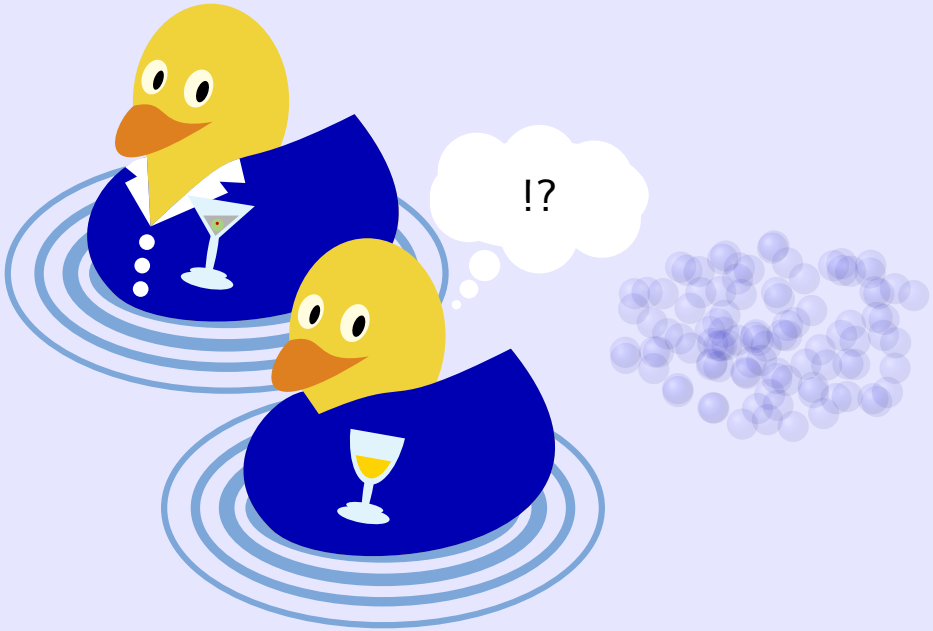
The goals of the Red Team



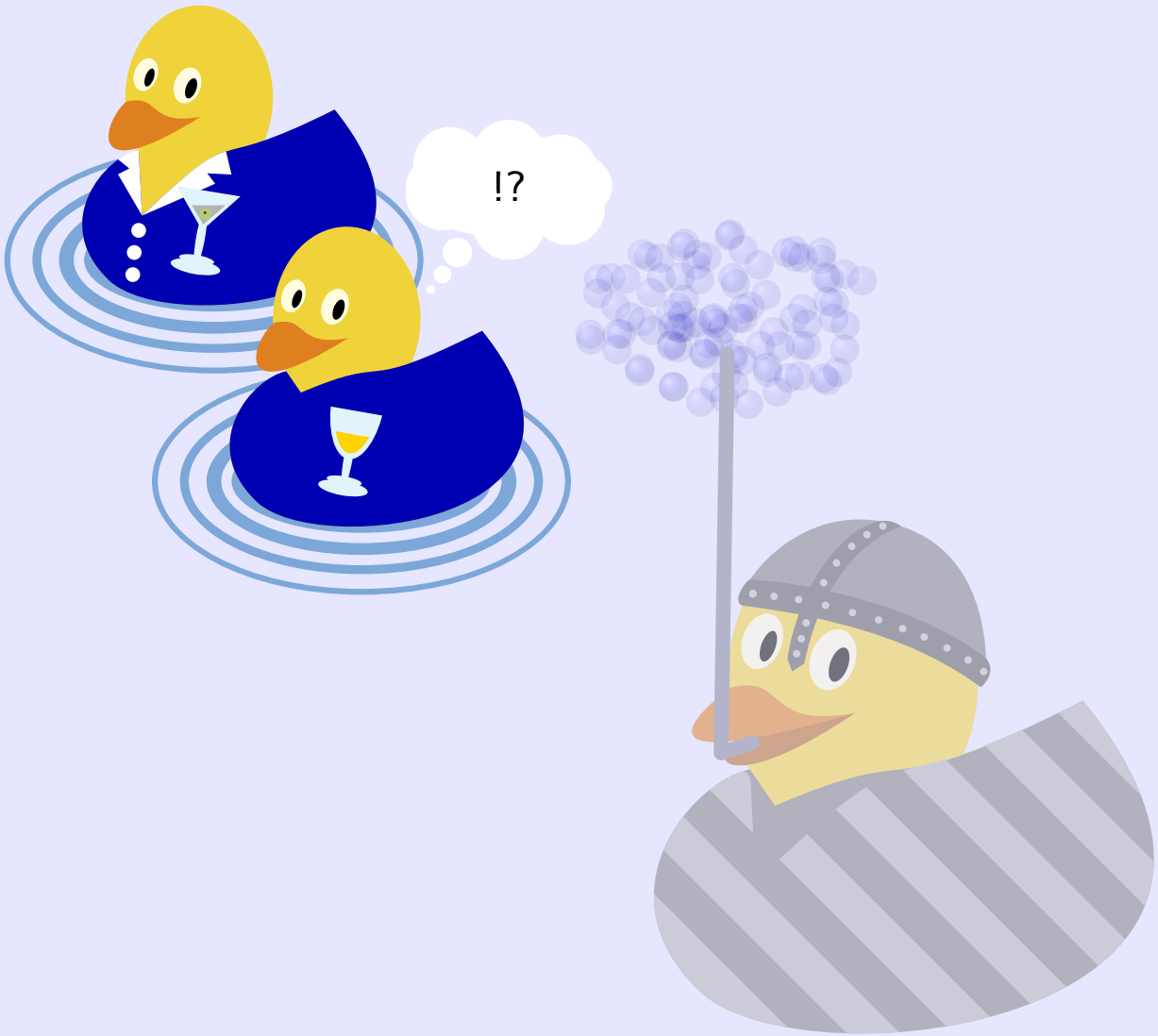
The goals of the Red Team



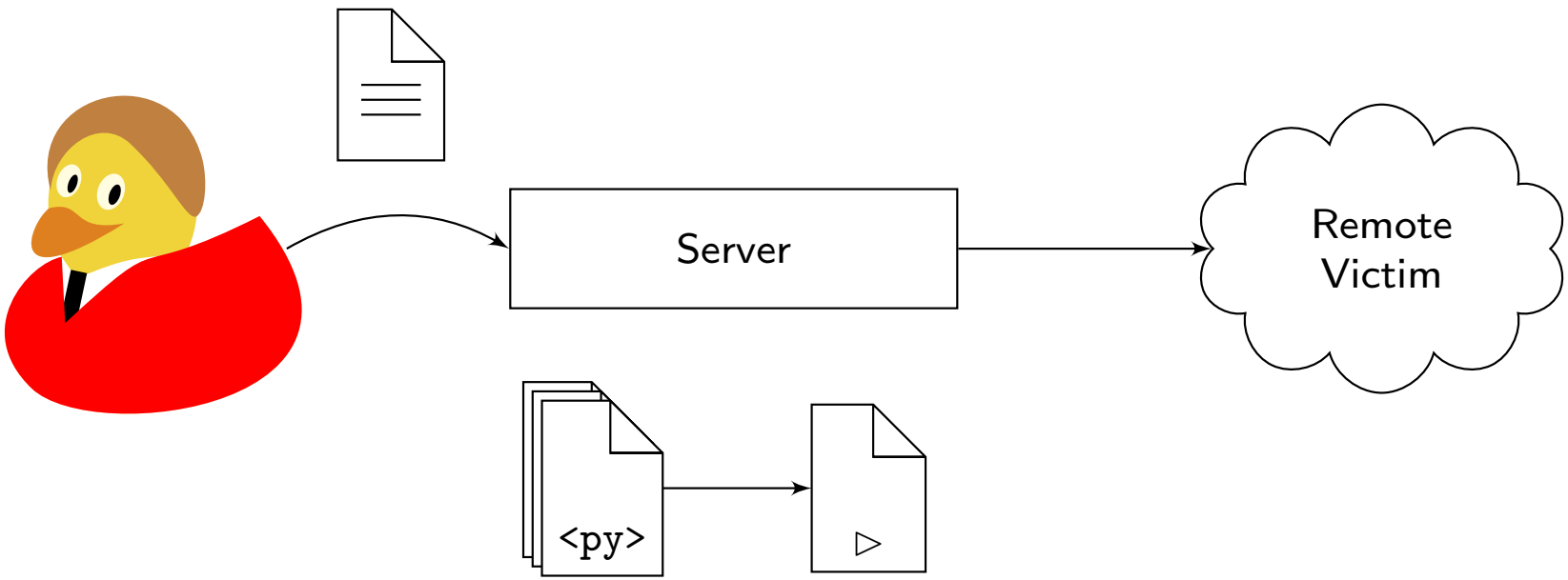
The goals of the Red Team



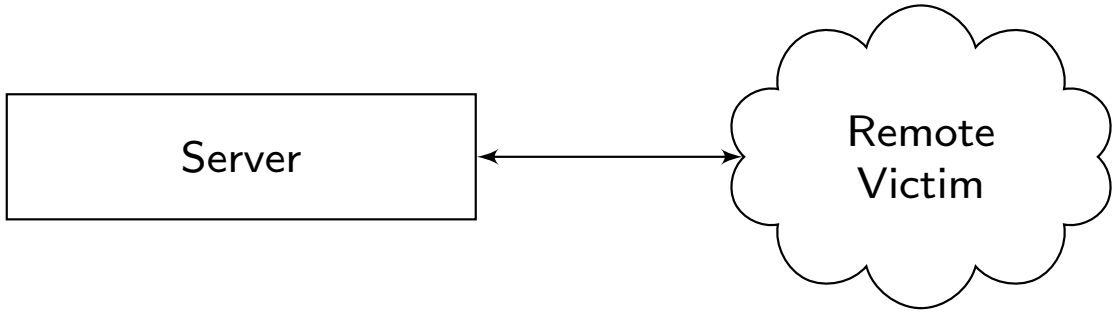
The goals of the Red Team

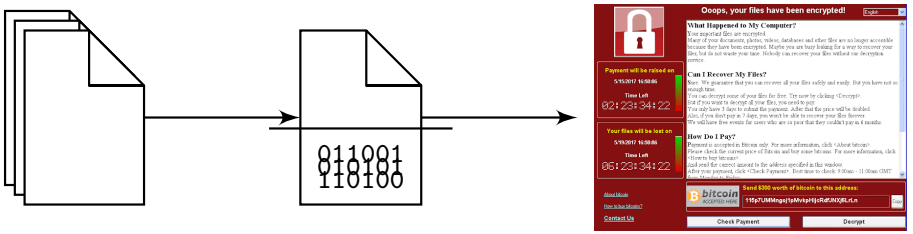


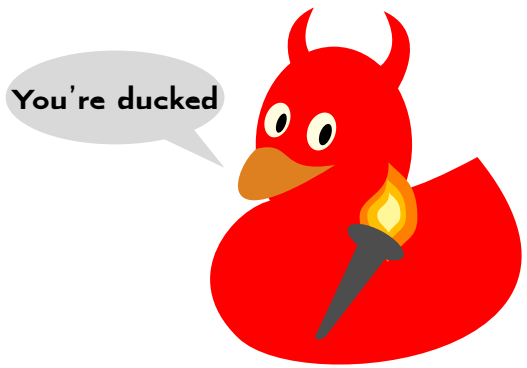
Preliminary steps



Ransomware structure







Outline

Project subject

Our proposal: WannaFly
- The context
  - The goals of the Red Team
- Preliminary steps
- Ransomware structure
- Encrypting files
  - Which files to encrypt?
  - Encryption method
- Impact analysis
- End of life

Evaluation

Conclusion

Which files to encrypt?

Encrypting all the files is a bad idea

Might encrypt system files

Which files to encrypt?

Encrypting all the files is a bad idea

Might encrypt system files

How to know if a file is interesting?

$\longrightarrow$ Extensions: *Problem: Rename text.txt to text.py*

Which files to encrypt?

Encrypting all the files is a bad idea

Might encrypt system files

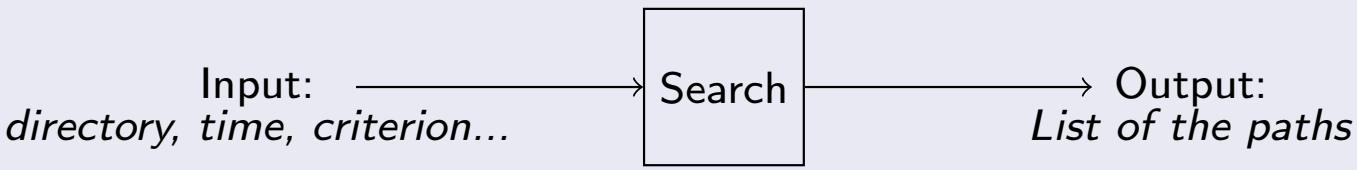
How to know if a file is interesting?

⟶ ~~Extensions:~~ *Problem: Rename text.txt to text.py*

⟶ MIME: *MIME(text.py) = 'text/plain'*

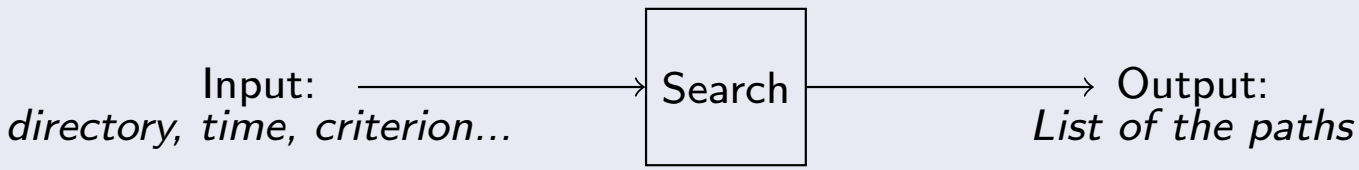
Search for a file to encrypt

Objective

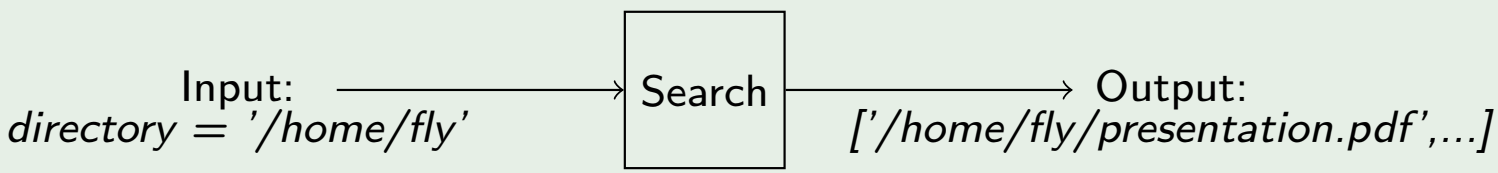


Search for a file to encrypt

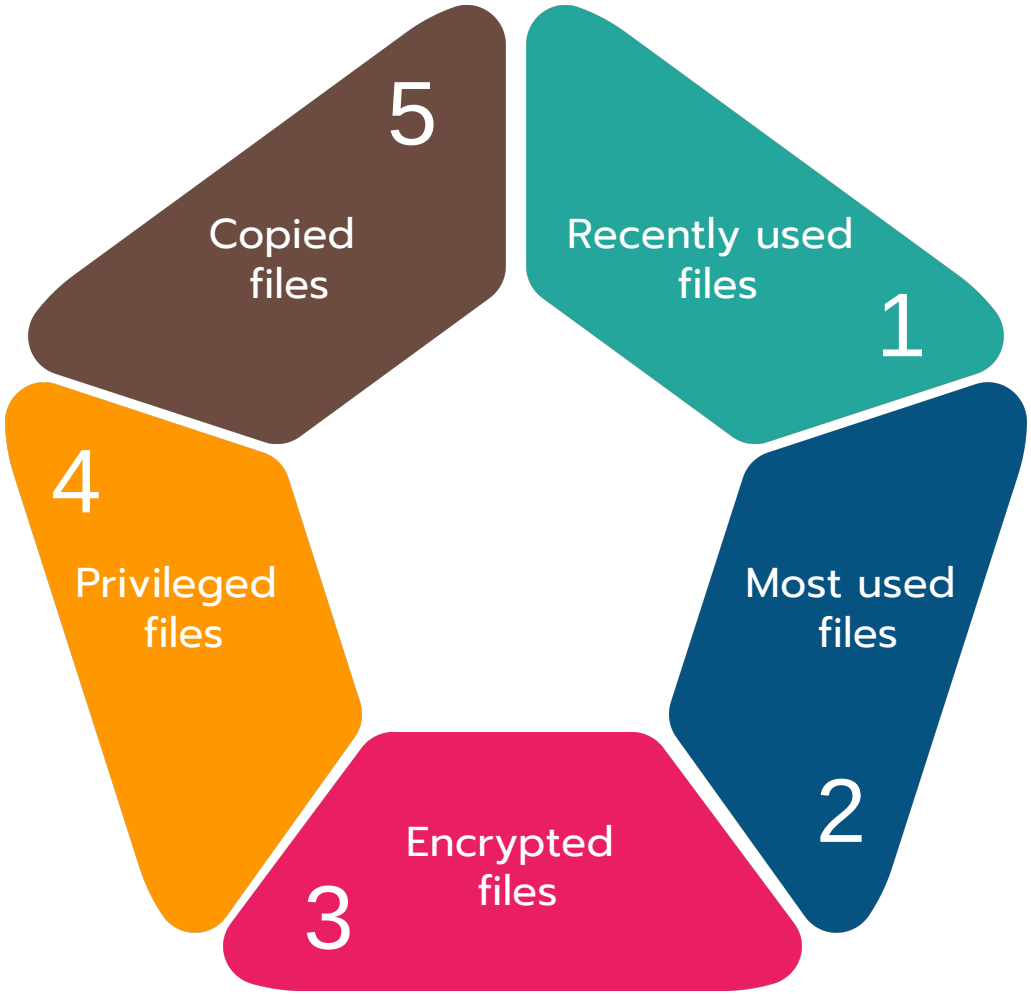
Objective



Example

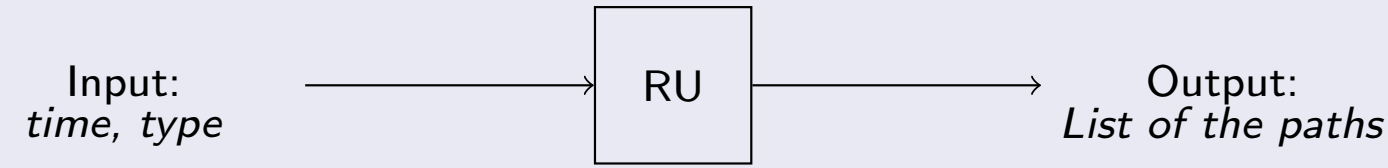


Several search options



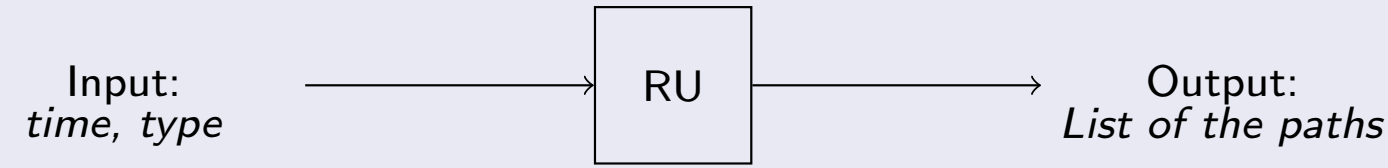
Time-based targeting of files

Recently Used Files

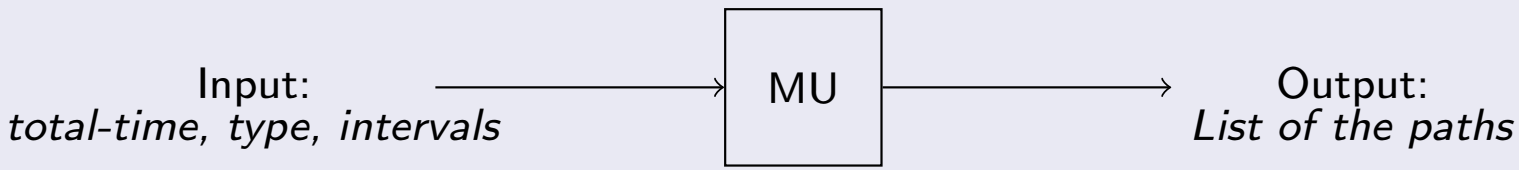


Time-based targeting of files

Recently Used Files

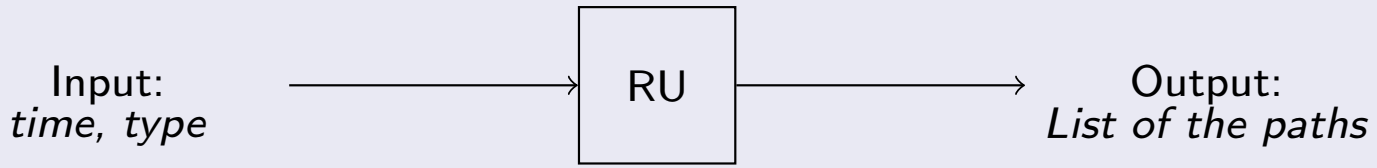


Most Used Files

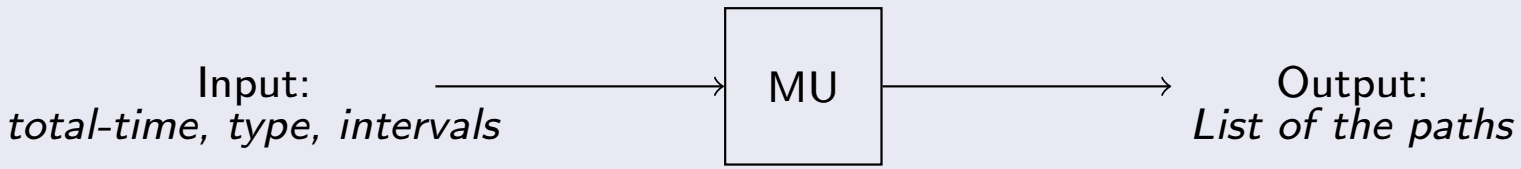


Time-based targeting of files

Recently Used Files



Most Used Files

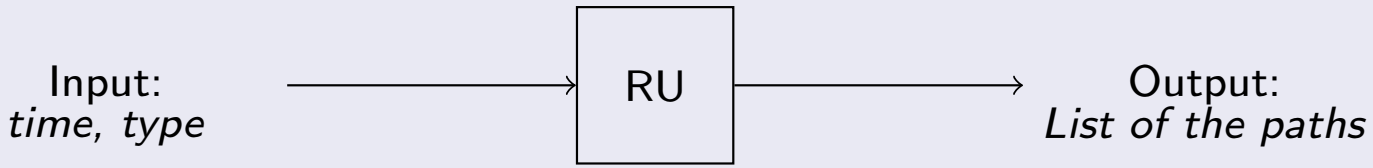


Example

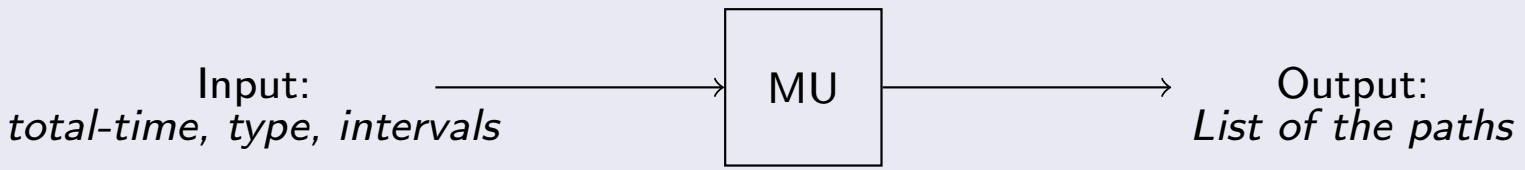
$\mathrm{MU}(\text{total-time} = 5\text{minutes}, \text{intervals} = 5)$

Time-based targeting of files

Recently Used Files



Most Used Files

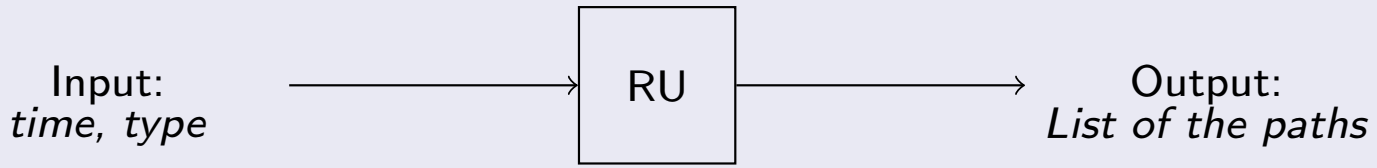


Example

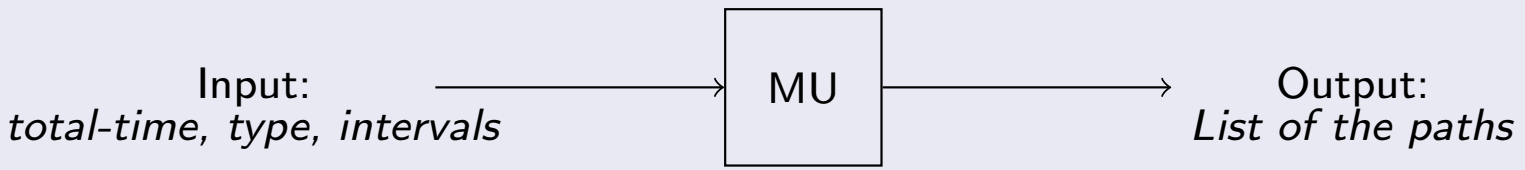
$\mathrm{MU}(\text{total-time} = 5\text{minutes}, \text{intervals} = 5)$

Time-based targeting of files

Recently Used Files



Most Used Files



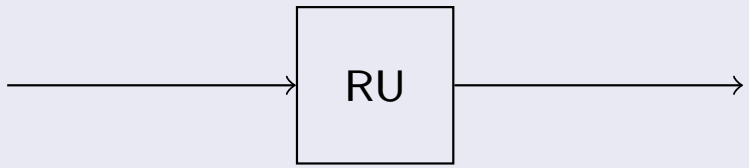
Example

$\mathrm{MU}(\text{total-time} = 5\text{minutes}, \text{intervals} = 5)$

Time-based targeting of files

Recently Used Files

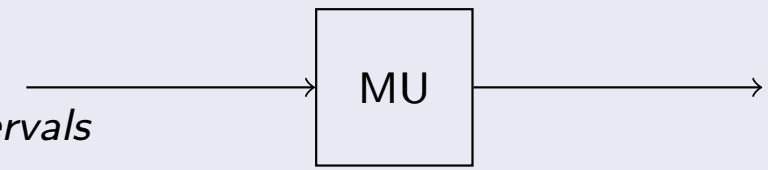
Input:
time, type



Output:
List of the paths

Most Used Files

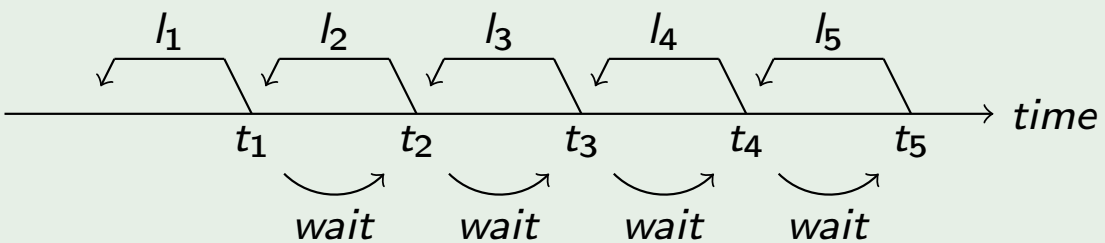
Input:
total-time, type, intervals



Output:
List of the paths

Example

$\mathrm{MU}(\text{total-time} = 5\text{minutes}, \text{intervals} = 5)$



Encrypt files that are already encrypted

How to know if a file is encrypted?

$\longrightarrow$ Entropy:

Entropy('test.txt') = 3
Entropy('test.txt.gpg') = 6

Entropy('test.odt') = 7.85
Entropy('test.odt.gpg') = 7.98

Encrypt files that are already encrypted

How to know if a file is encrypted?

⟶ Entropy:

Entropy('test.txt') = 3
Entropy('test.txt.gpg') = 6

Entropy('test.odt') = 7.85
Entropy('test.odt.gpg') = 7.98

⟶ "file" Command:

fly@PC: **file** test1.pdf
PDF document, version 1.3

fly@PC: **file** test2.pdf
GPG symmetrically encrypted data

Encrypt privileged files

File permissions

File permissions: $\underbrace{\text{rwx}}_{\text{owner}} - \underbrace{\text{rwx}}_{\text{members}} - \underbrace{\text{rwx}}_{\text{others}}$

Encrypt privileged files

File permissions

File permissions: $\underbrace{\text{rwx}}_{\text{owner}}$ - $\underbrace{\text{rwx}}_{\text{members}}$ - $\underbrace{\text{rwx}}_{\text{others}}$

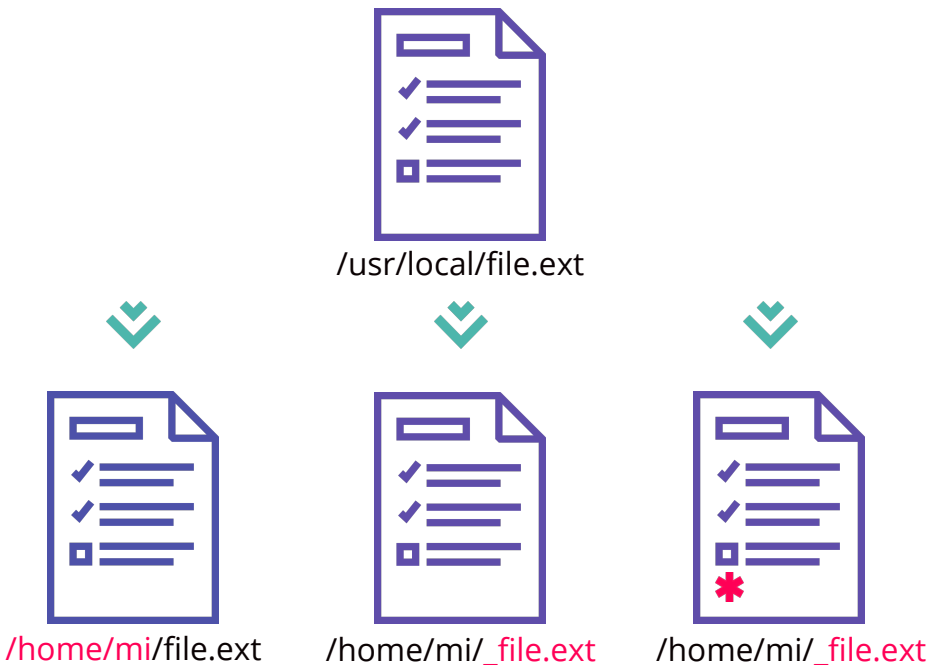
Examples

File 1:	rwx	-	rwx	-	- - -		+
File 2:	rwx	-	- - -	-	- - -		++
File 3:	- - -	-	- - -	-	- - -		+++

Encrypt copied files

Objective

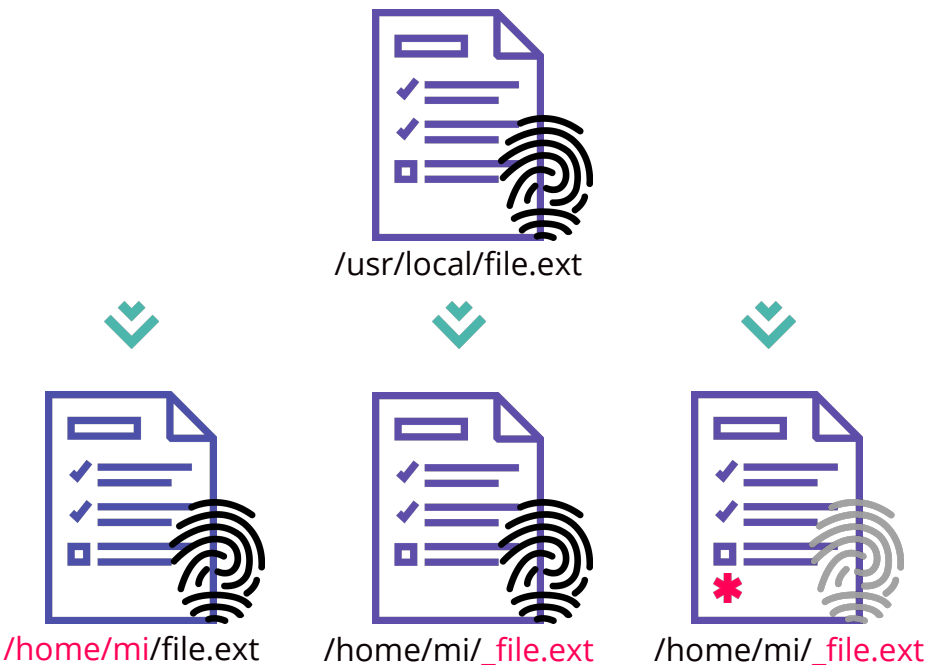
Find files that exist in multiple copies



Encrypt copied files

Objective

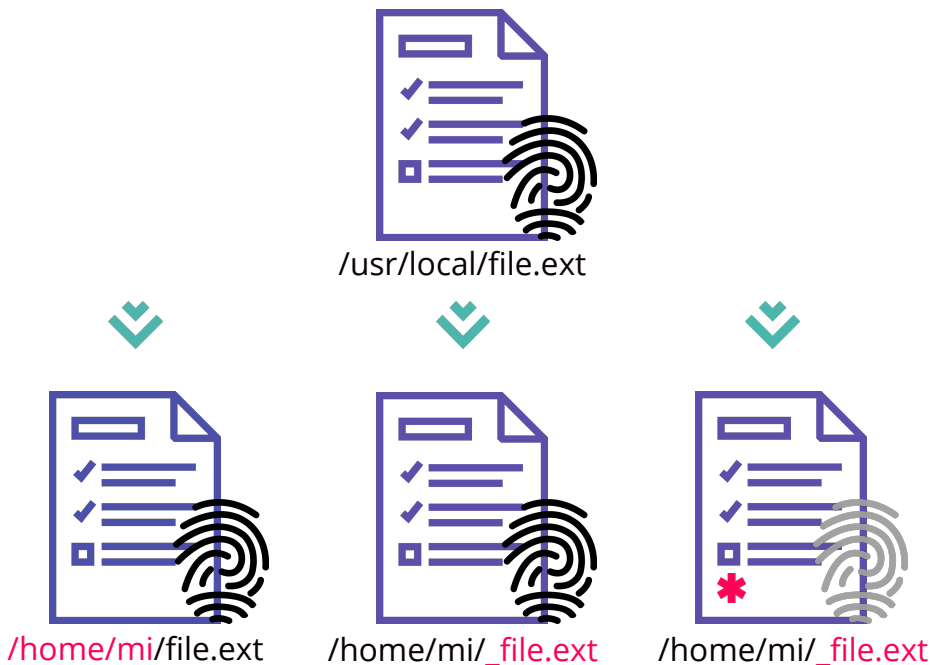
Find files that exist in multiple copies



Encrypt copied files

Objective

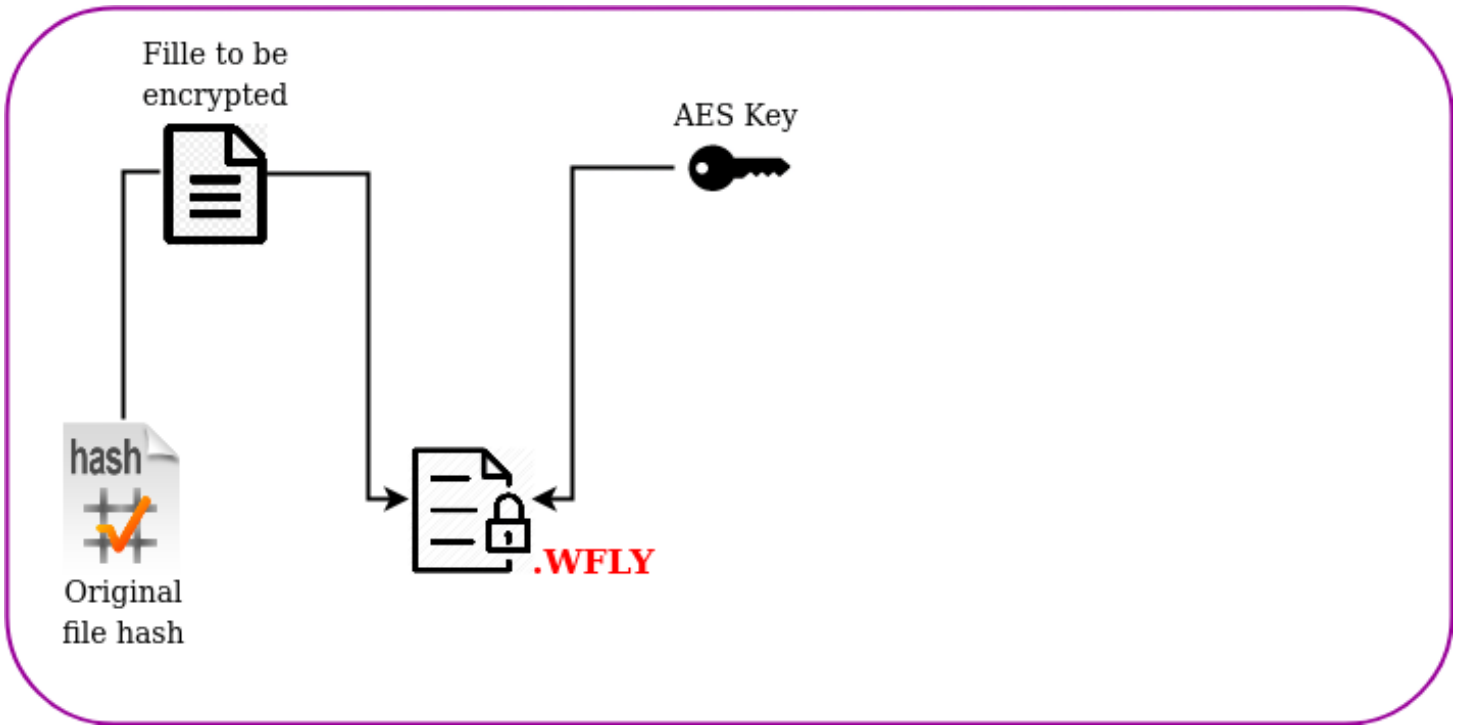
Find files that exist in multiple copies



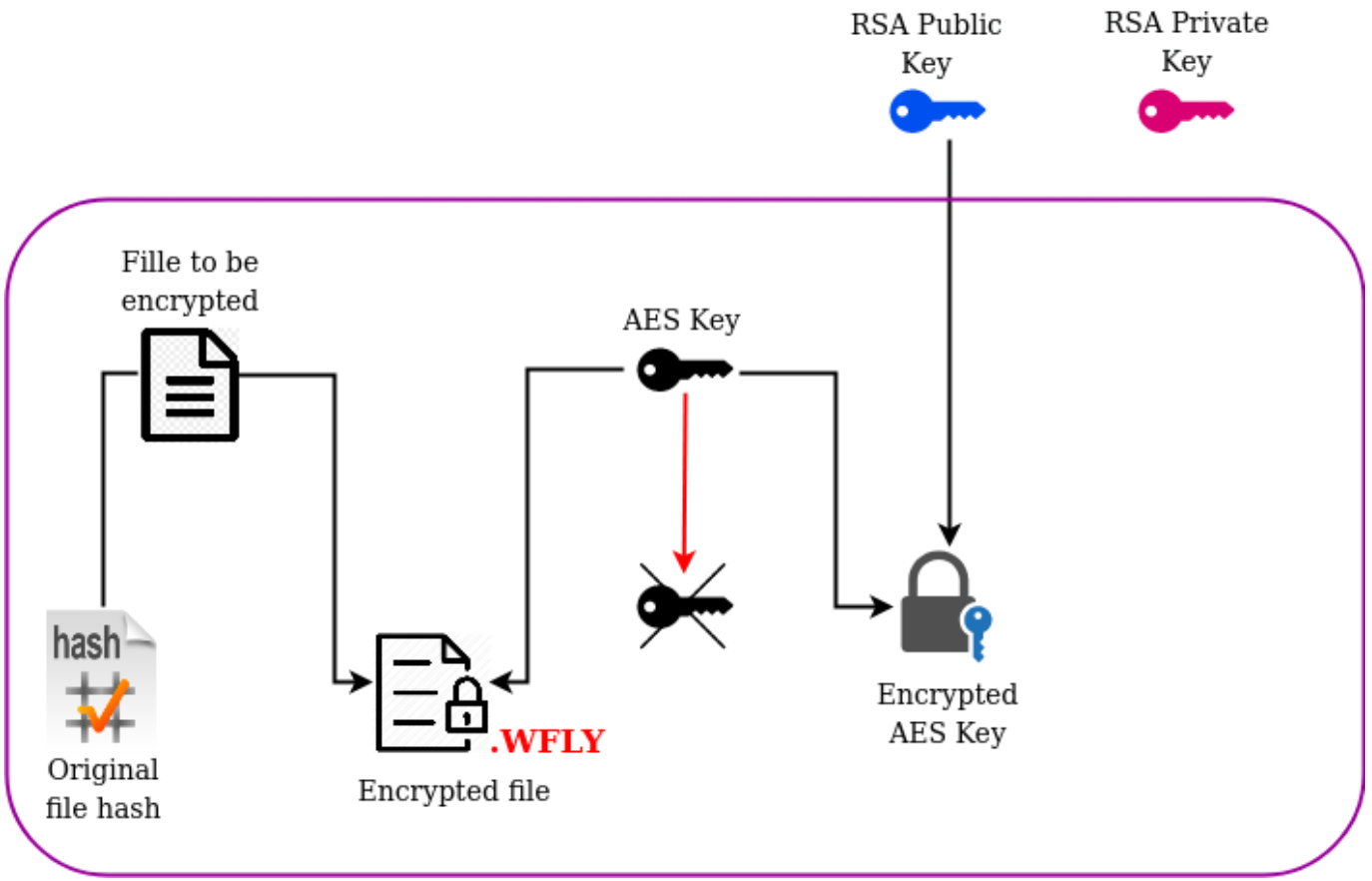
- TLSH generates a hash value which can be used for similarity comparisons

Encryption and decryption process

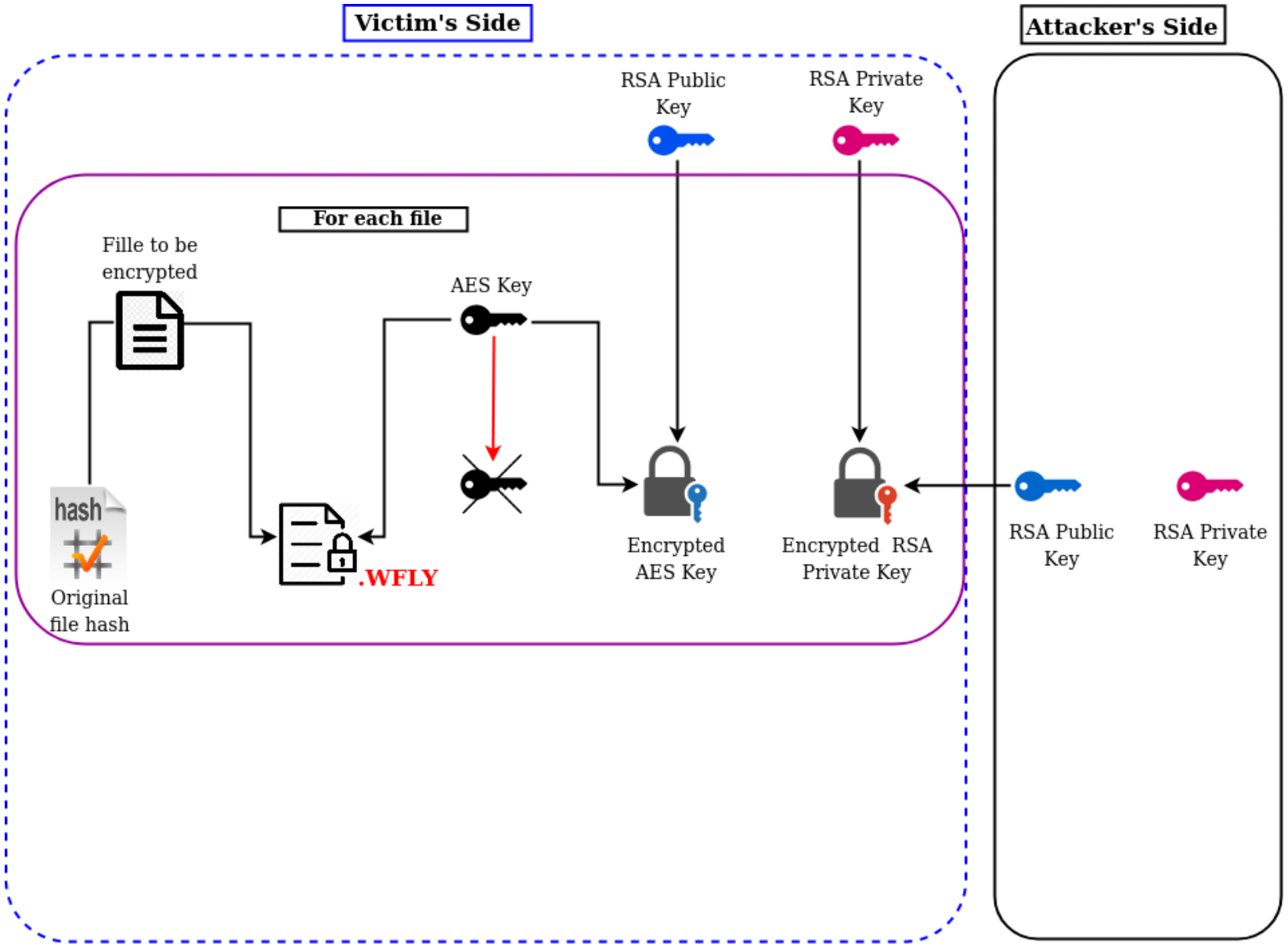
Encryption and decryption process



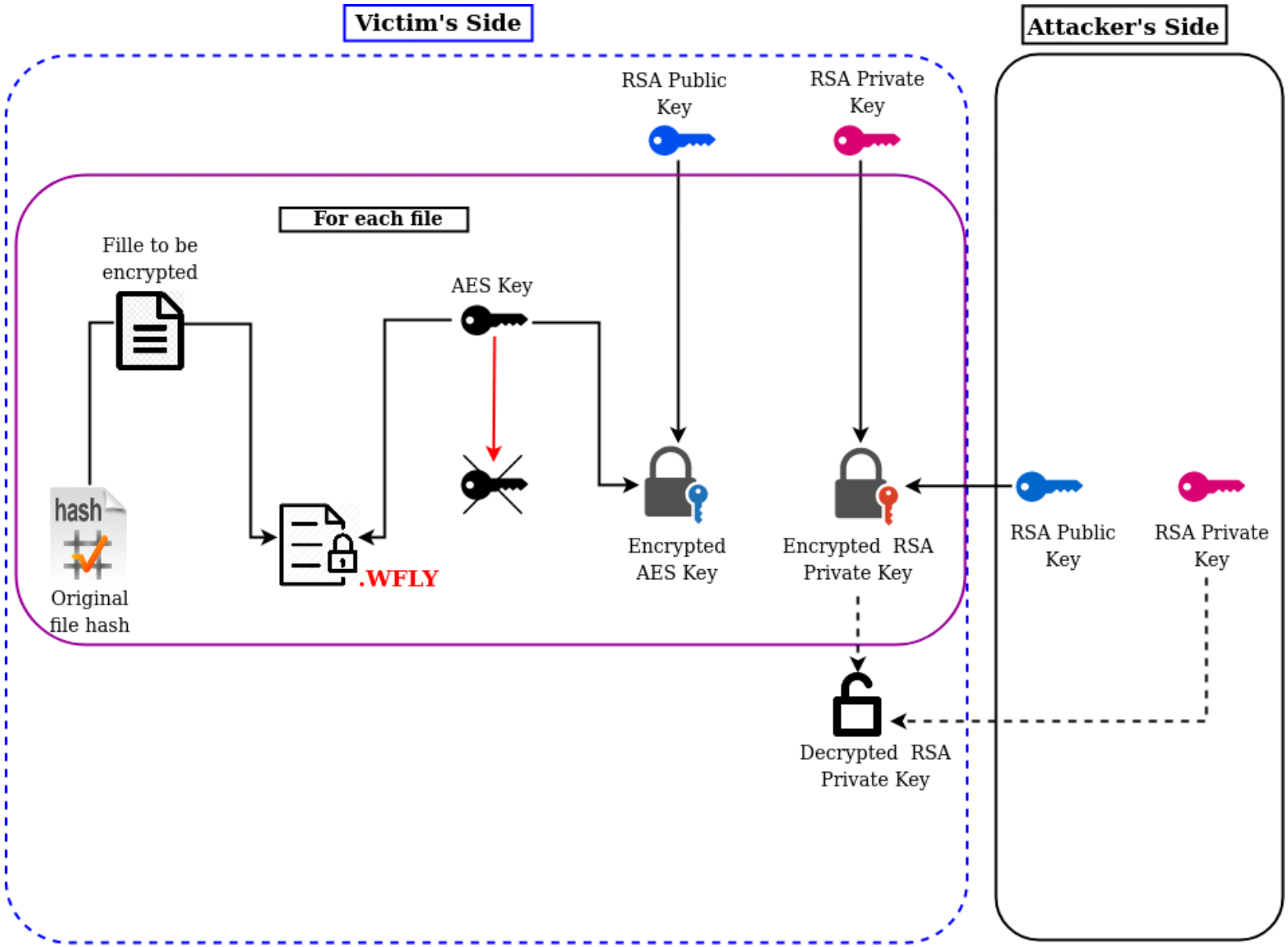
Encryption and decryption process



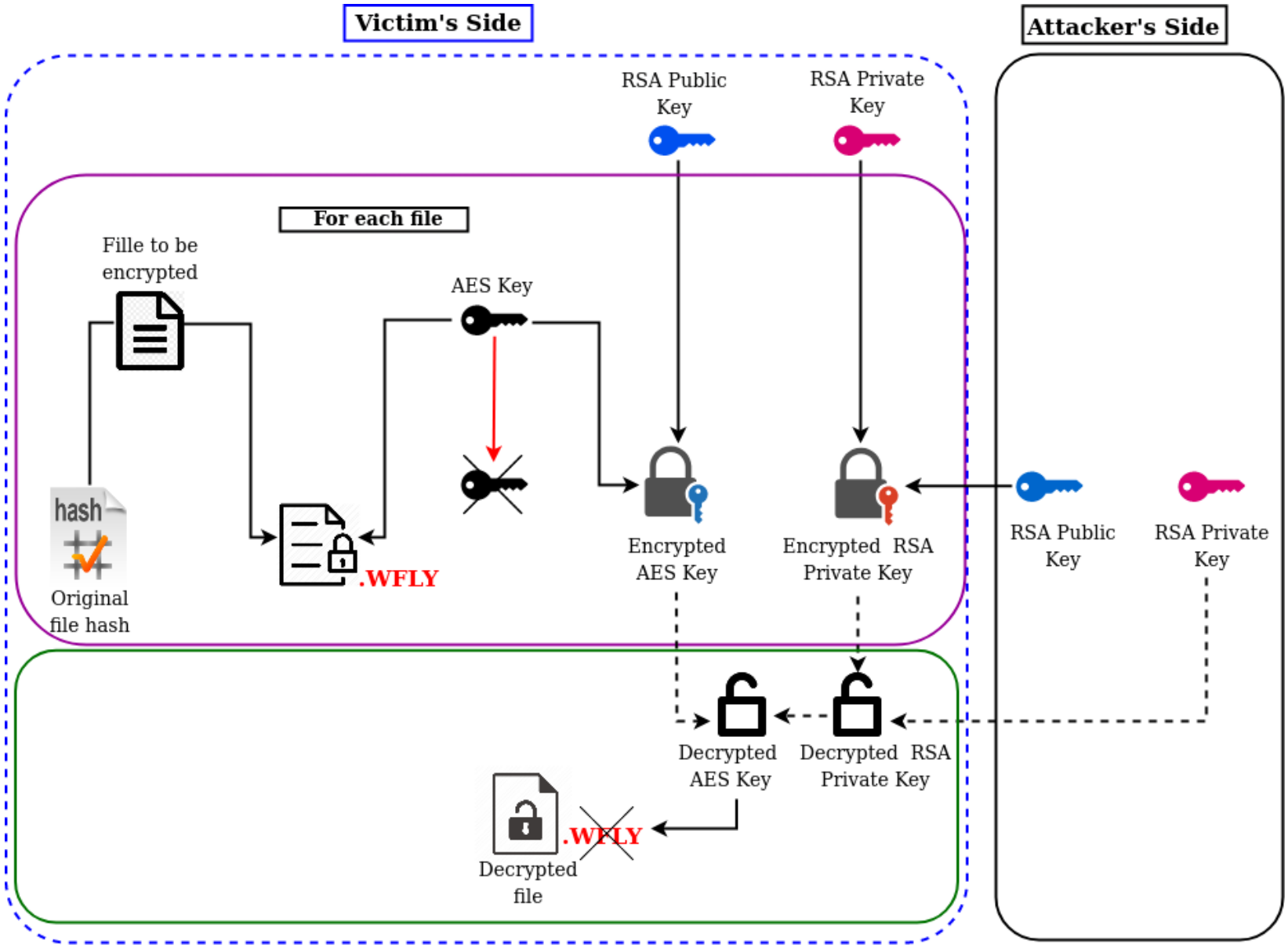
Encryption and decryption process



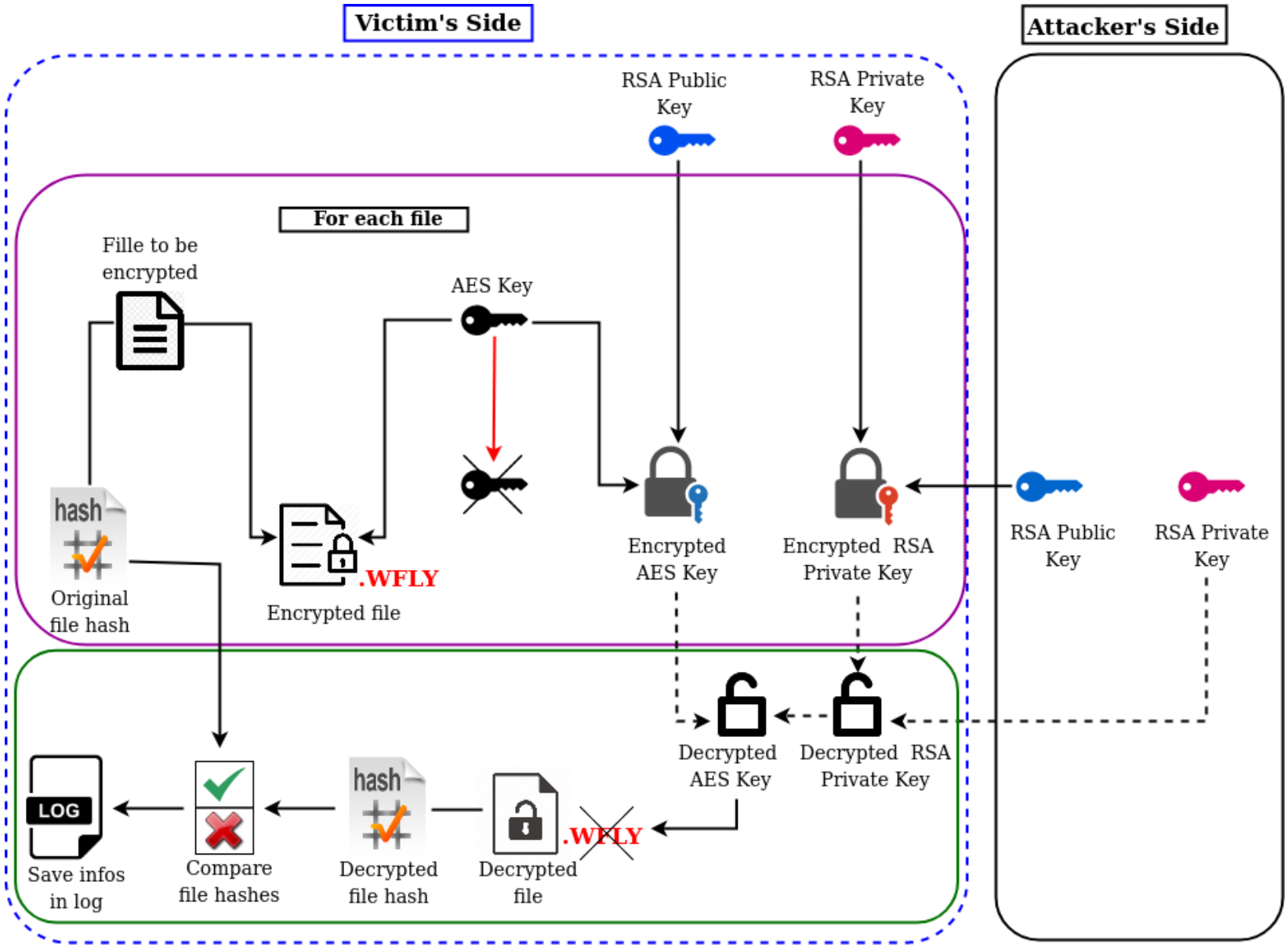
Encryption and decryption process



Encryption and decryption process



Encryption and decryption process



Impact analysis

Constraint

Audit what happened and when, to confirm or deny the claims of the blue team

End of life

It is an exercise!

Must be able to restore the system to its original state

Abilities

- No file is deleted during the deployment
- Files can be decryted (if attacker private key is known)
- Red team has a constant access
  - Advancement
  - Destruction

End of life

It is an exercise!

Must be able to restore the system to its original state

Abilities

- No file is deleted during the deployment
- Files can be decryted (if attacker private key is known)
- Red team has a constant access
  - Advancement
  - Destruction

One study, one ransomware, one deployment, one cleanup

Outline

Project subject

Our proposal: WannaFly

Evaluation

Conclusion

VirusTotal check

[Vir21]

VirusTotal

- Aggregate many anti-malware products
- Analyze suspicious files to detect types of malware

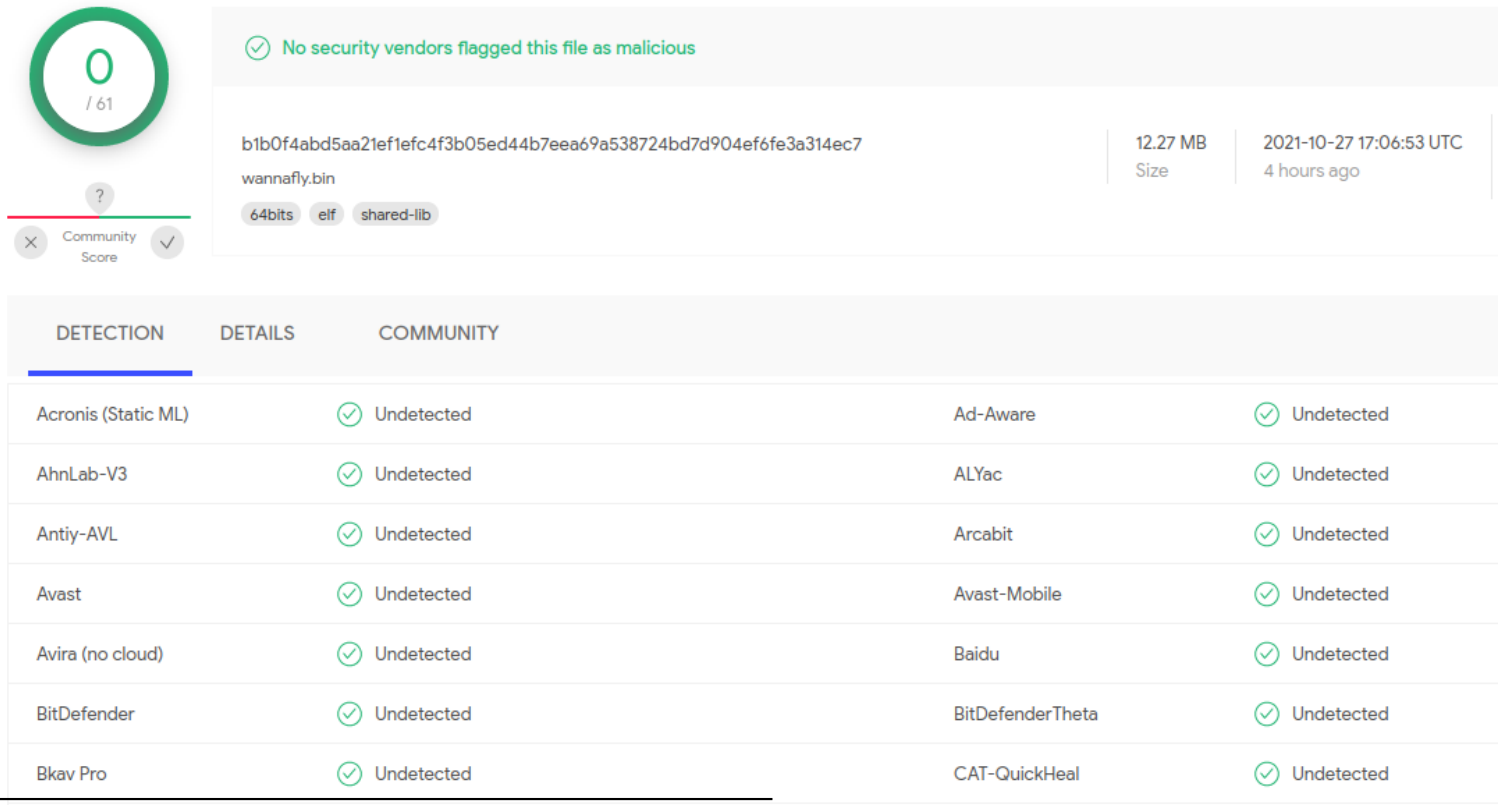
[Vir21] VirusTotal. 2021

VirusTotal check

[Vir21]

VirusTotal

- Aggregate many anti-malware products
- Analyze suspicious files to detect types of malware



[Vir21] VirusTotal. 2021

Outline

Project subject

Our proposal: WannaFly

Evaluation

Conclusion

Conclusion

What we have done

- Bypass signature-based detection
- Respect red team exercise constraints
- Encrypt only files that are deemed critical
- Remain efficient even if the encrypting process is detected and interrupted by the victim
- Use one encryption key per file
- Guarantee that one decrypted key cannot help other victims

Conclusion

What we have not done

- Injection and spread are not considered
- More advanced static methods and dynamic analysis must permit detection

Future work

- Develop strategies to dissimulate ransomware
- Limit process resource usage
- Avoid reading special file types
- Avoid scanning network storage
- Generate a key pair for client-server communications
- Use configuration files