CRIBA: A Tool for Comprehensive Analysis of Cryptographic Ransomware's I/O Behavior

Tânia Esteves, Bruno Pereira, Rui Pedro Oliveira, João Marco and João Paulo

INESC TEC & University of Minho

42nd International Symposium on Reliable Distributed Systems (SRDS 2023)

INESCTEC

Universidade do Minho

FCT Fundação para a Ciência e a Tecnologia

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.

What is Cryptographic Ransomware?

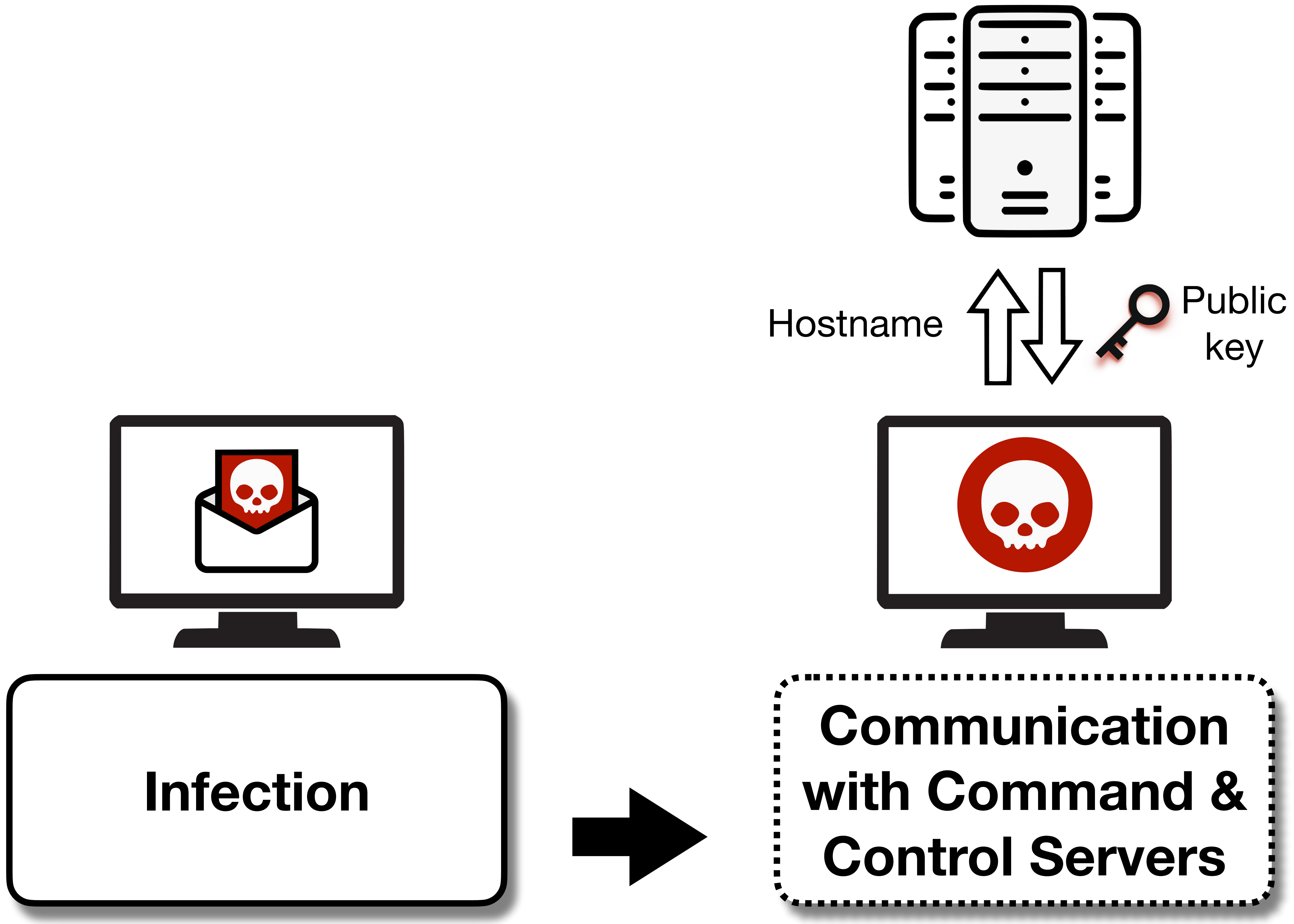
A malicious software that encrypts data at infected servers and demands a ransom to recover it.

Infection

Download and installation of the ransomware sample.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Hostname

Public key

Infection

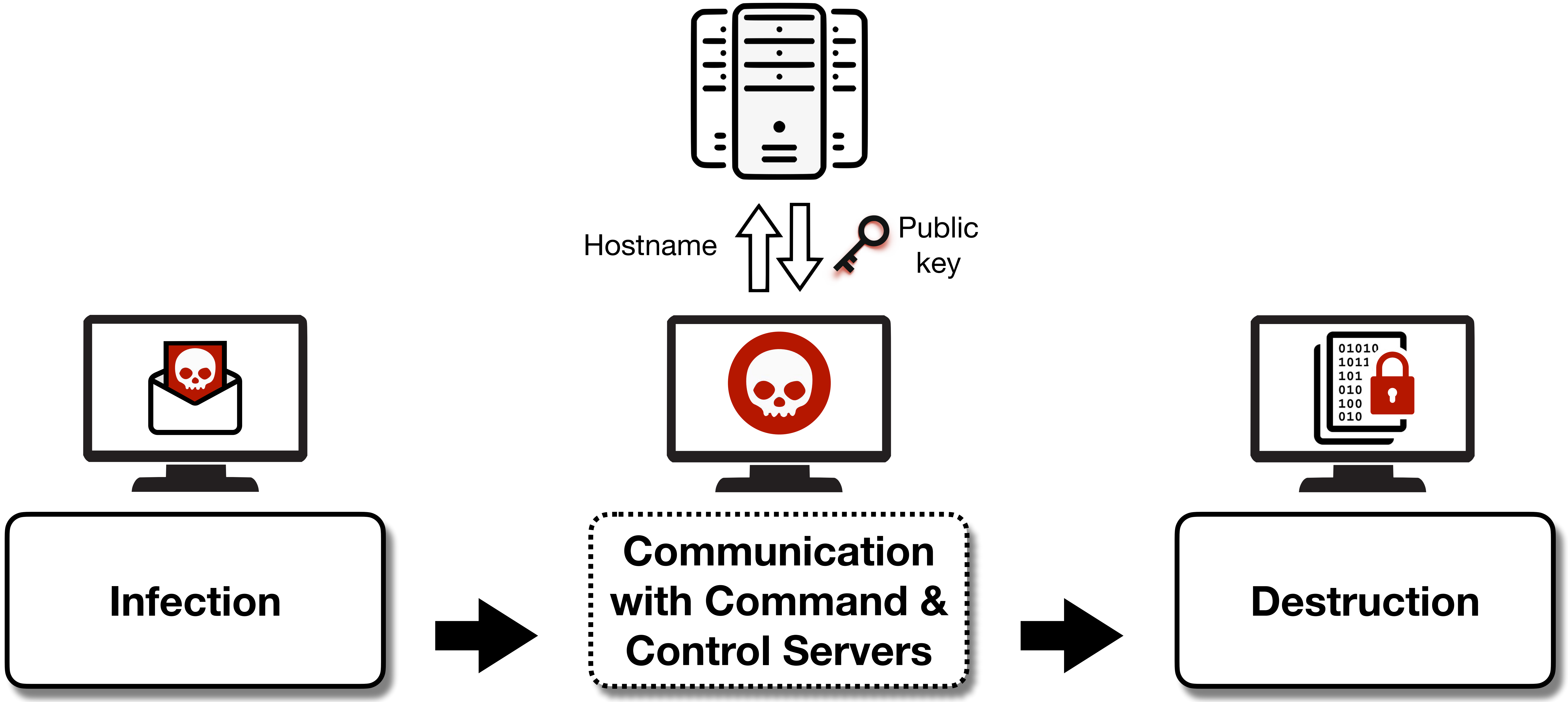
Communication with Command & Control Servers

Download and installation of the ransomware sample.

Exchange of information with the attacker.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Hostname

Public key

Infection

Communication with Command & Control Servers

Destruction

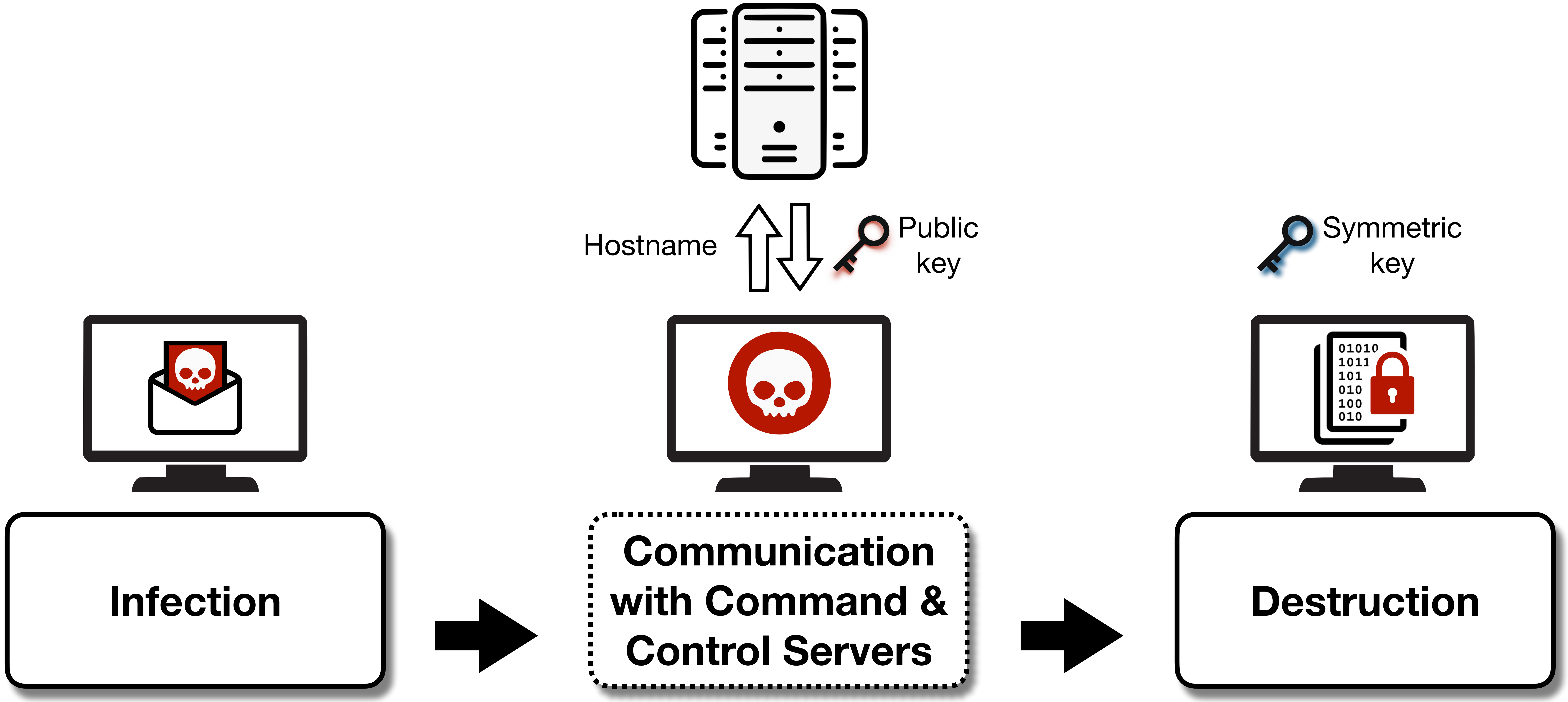
Download and installation of the ransomware sample.

Exchange of information with the attacker.

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Hostname

Public key

Symmetric key

Infection

Communication with Command & Control Servers

Destruction

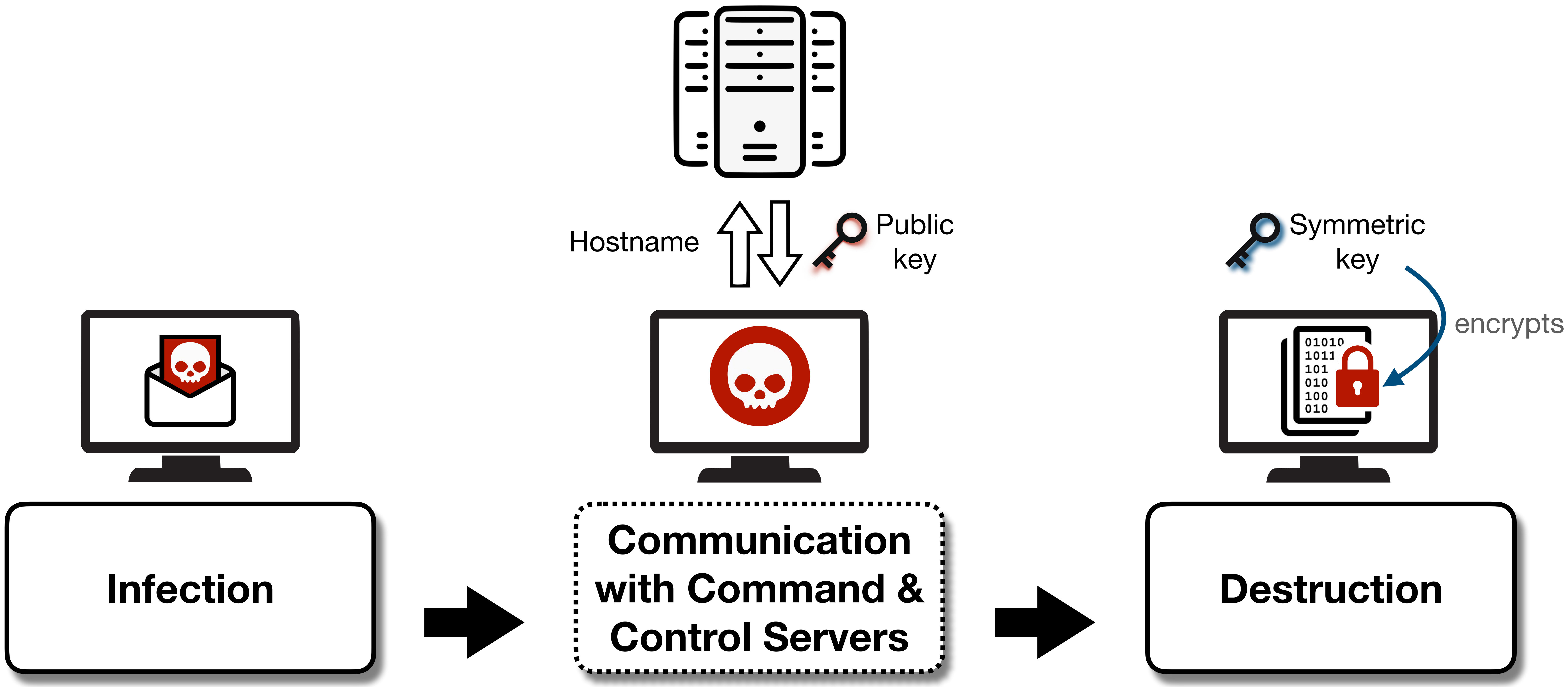
Download and installation of the ransomware sample.

Exchange of information with the attacker.

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Infection

Download and installation of the ransomware sample.

Communication with Command & Control Servers

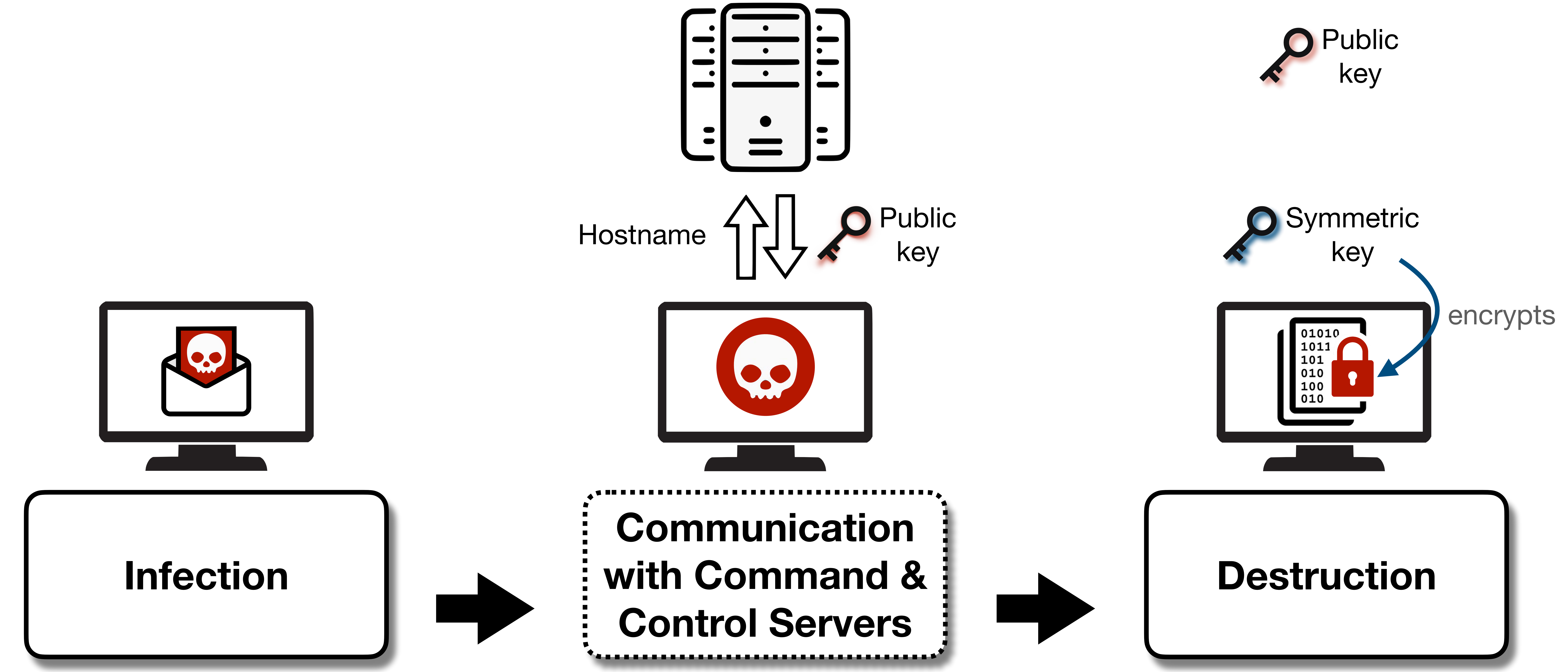
Exchange of information with the attacker.

Destruction

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



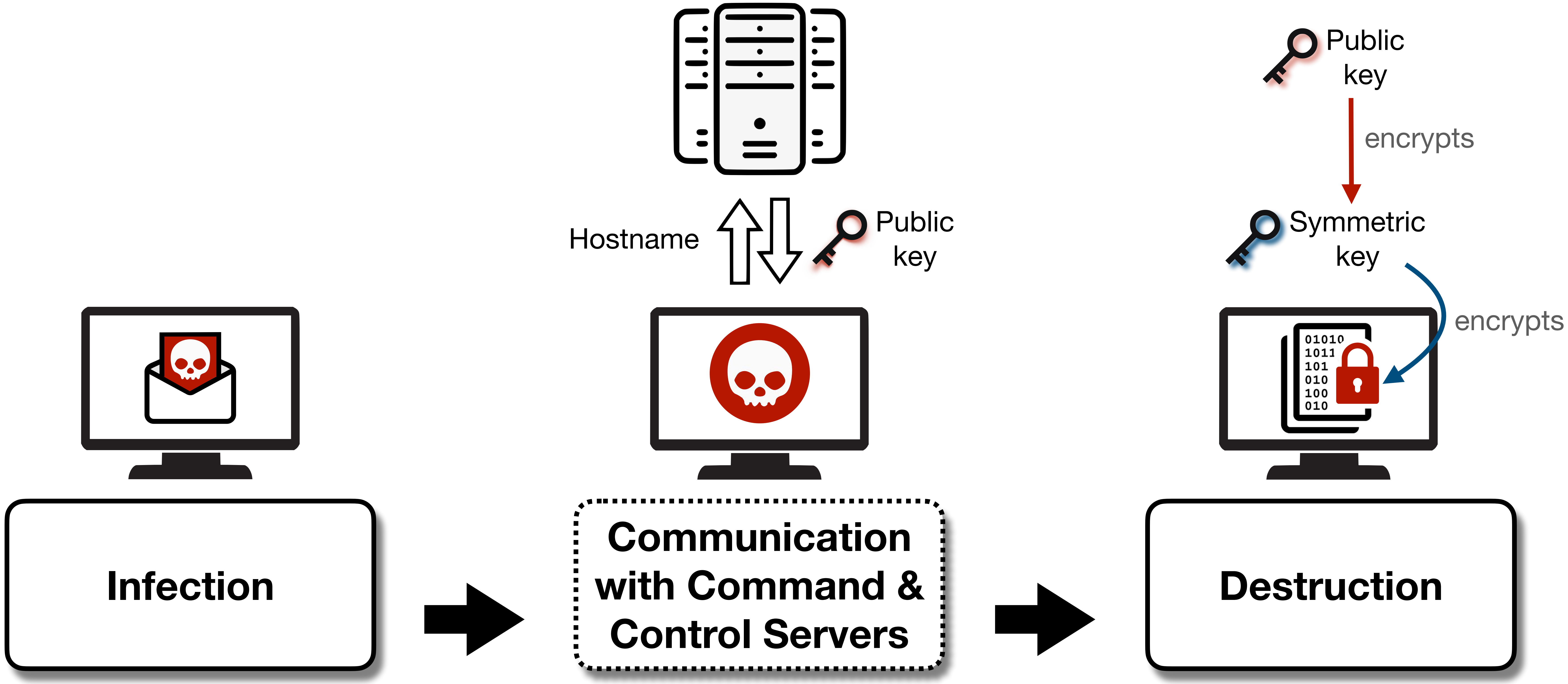
Download and installation of the ransomware sample.

Exchange of information with the attacker.

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Infection

Download and installation of the ransomware sample.

Communication with Command & Control Servers

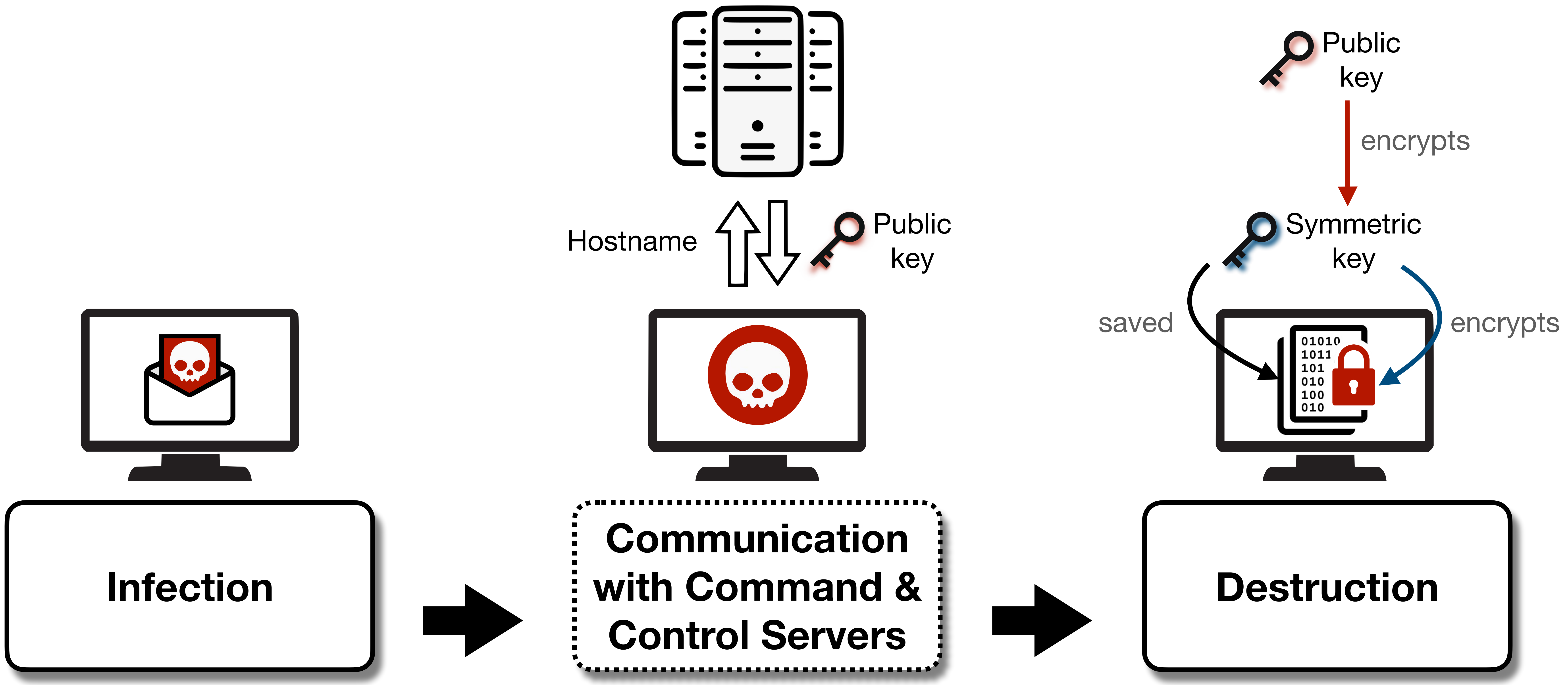
Exchange of information with the attacker.

Destruction

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Infection

Download and installation of the ransomware sample.

Communication with Command & Control Servers

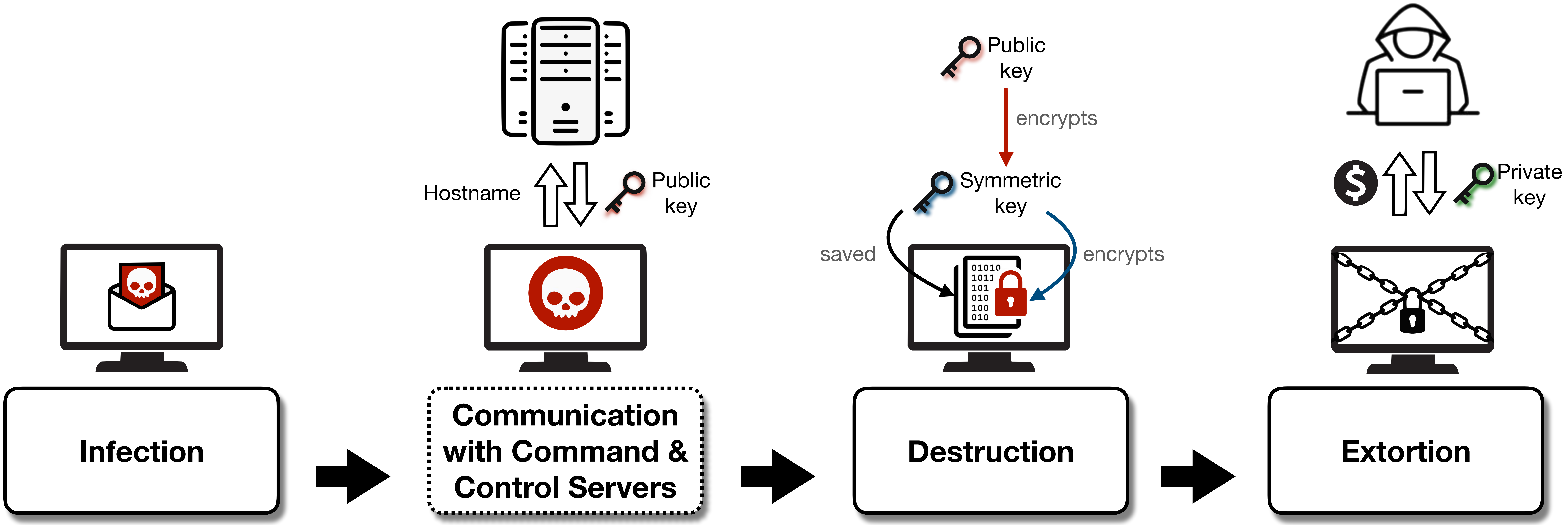
Exchange of information with the attacker.

Destruction

Encryption of victims' files, blocking the access to data.

What is Cryptographic Ransomware?

A malicious software that encrypts data at infected servers and demands a ransom to recover it.



Infection → **Communication with Command & Control Servers** → **Destruction** → **Extortion**

Download and installation of the ransomware sample.

Exchange of information with the attacker.

Encryption of victims’ files, blocking the access to data.

Informs the victim about the attack and discloses payment instructions.

What is Cryptographic Ransomware?

- Now spreading across distinct operating systems: Windows, Android and **Linux**.
- Attacks on Linux infrastructures are causing devastating effects.

EREBUS attack on NAYANA

(Web hosting company)

- Infected 153 Linux servers and over 3,400 websites.
- NAYANA paid ~$ 1M.

REVIL attack on Quanta Computer

(Apple's supplier)

- Stole and leaked blueprints for Apple's latest products.
- Demanded $ 50M.

DARKSIDE attack on Colonial Pipeline

- Near 100 GiB of data stolen.
- Oil pipeline shut down for several days.
- Colonial pipeline paid ~$ 5M.

What is Cryptographic Ransomware?

- Now spreading across distinct operating systems: Windows, Android and **Linux**.
- Attacks on Linux infrastructures are causing devastating effects.

EREBUS attack on NAYANA

(Web hosting company)

- Infected 153 Linux servers and over 3,400 websites.
- NAYANA paid ~$ 1M.

REVIL attack on Quanta Computer

(Apple's supplier)

- Stole and leaked blueprints for Apple's latest products.
- Demanded $ 50M.

DARKSIDE attack on Colonial Pipeline

- Near 100 GiB of data stolen.
- Oil pipeline shut down for several days.
- Colonial pipeline paid ~$ 5M.

Understanding the I/O behavior of Linux Ransomware is crucial!

Analyzing Ransomware I/O Behavior

Current approaches

Analyzing Ransomware I/O Behavior

Current approaches

- **Behavior analysis sandboxes**
  - Controlled environment for running malware samples.
  - Monitor memory state, network traffic and API calls.
  - Generate a summarized report highlighting suspicious activities.
  - Output large raw logs for posterior manual analysis by the user.

Analyzing Ransomware I/O Behavior

Current approaches

- **Behavior analysis sandboxes**
  - Controlled environment for running malware samples.
  - Monitor memory state, network traffic and API calls.
  - Generate a summarized report highlighting suspicious activities.
  - Output large raw logs for posterior manual analysis by the user.

- **Ransomware detection tools**
  - Classify samples as malign/benign.
    - Do not provide further information about their internal behavior.
  - Use behavior analysis sandboxes to collect samples' behavior.
    - Manual analysis of collected logs to extract key characteristics.

Analyzing Ransomware I/O Behavior

Current approaches

◉ **Behavior analysis sandboxes**

- Controlled environment for running malware samples.
- Monitor memory state, network traffic and API calls.
- Generate a summarized report highlighting suspicious activities.
- Output large raw logs for posterior manual analysis by the user.

◉ **Ransomware detection tools**

- Classify samples as malign/benign.
  - Do not provide further information about their internal behavior.
- Use behavior analysis sandboxes to collect samples’ behavior.
  - Manual analysis of collected logs to extract key characteristics.

The majority of these solutions are developed for Windows and Android.

CRIBA

This work

- A tool for simplifying and automating the exploration, analysis, and comparison of I/O patterns for Linux cryptographic ransomware.
  - **Transparent** collection of information about ransomware's execution.
  - **Practical** pipeline for analyzing the collected information.
  - **Automated** and **customizable** analysis for exploring and correlating data.
  - **Visual representations** to ease and summarize data analysis.

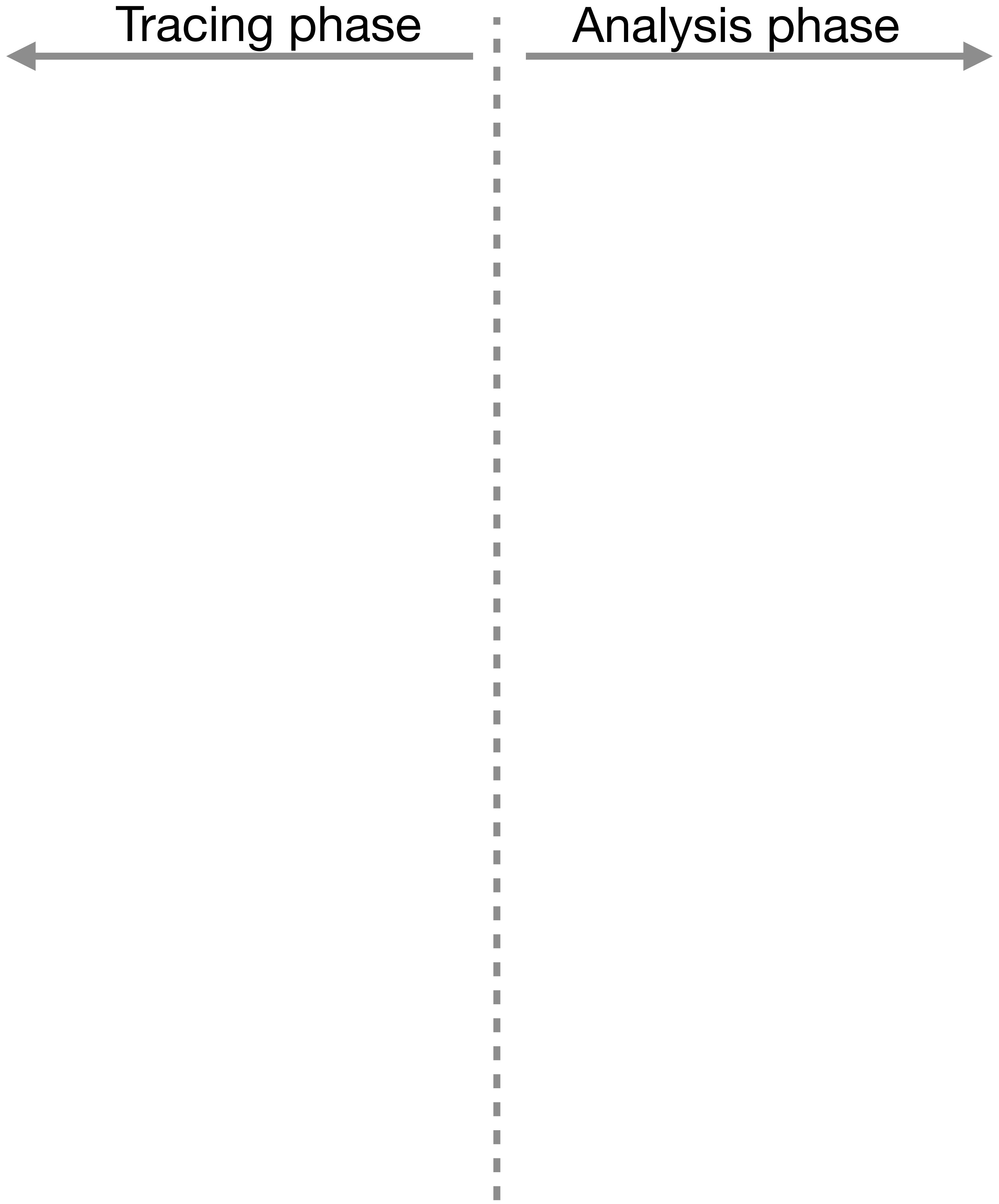
CRIBA

System overview

⬛ DIO’s components 🟦 New components

CRIBA

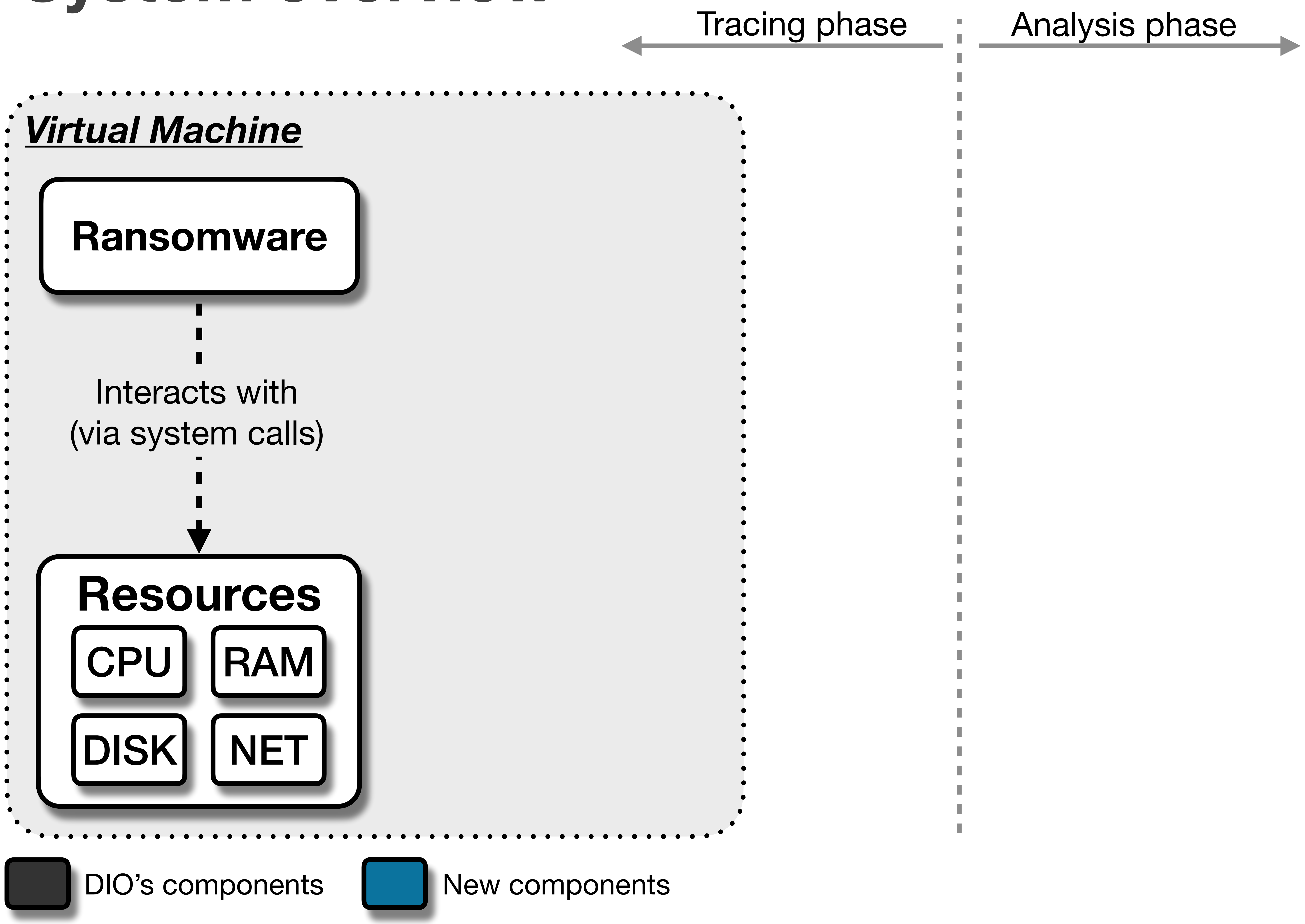
System overview



⬛ DIO’s components 🟦 New components

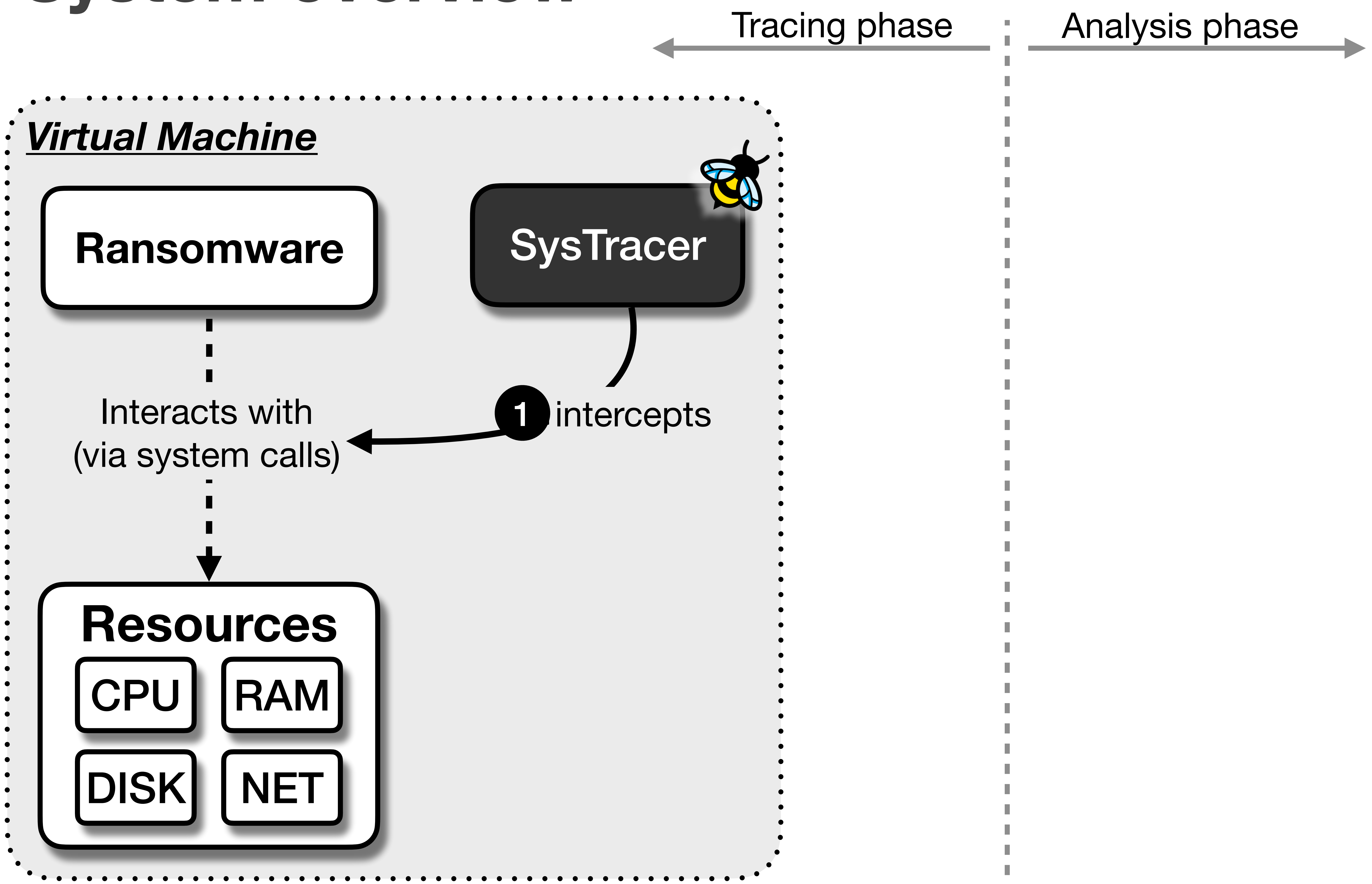
CRIBA

System overview



CRIBA

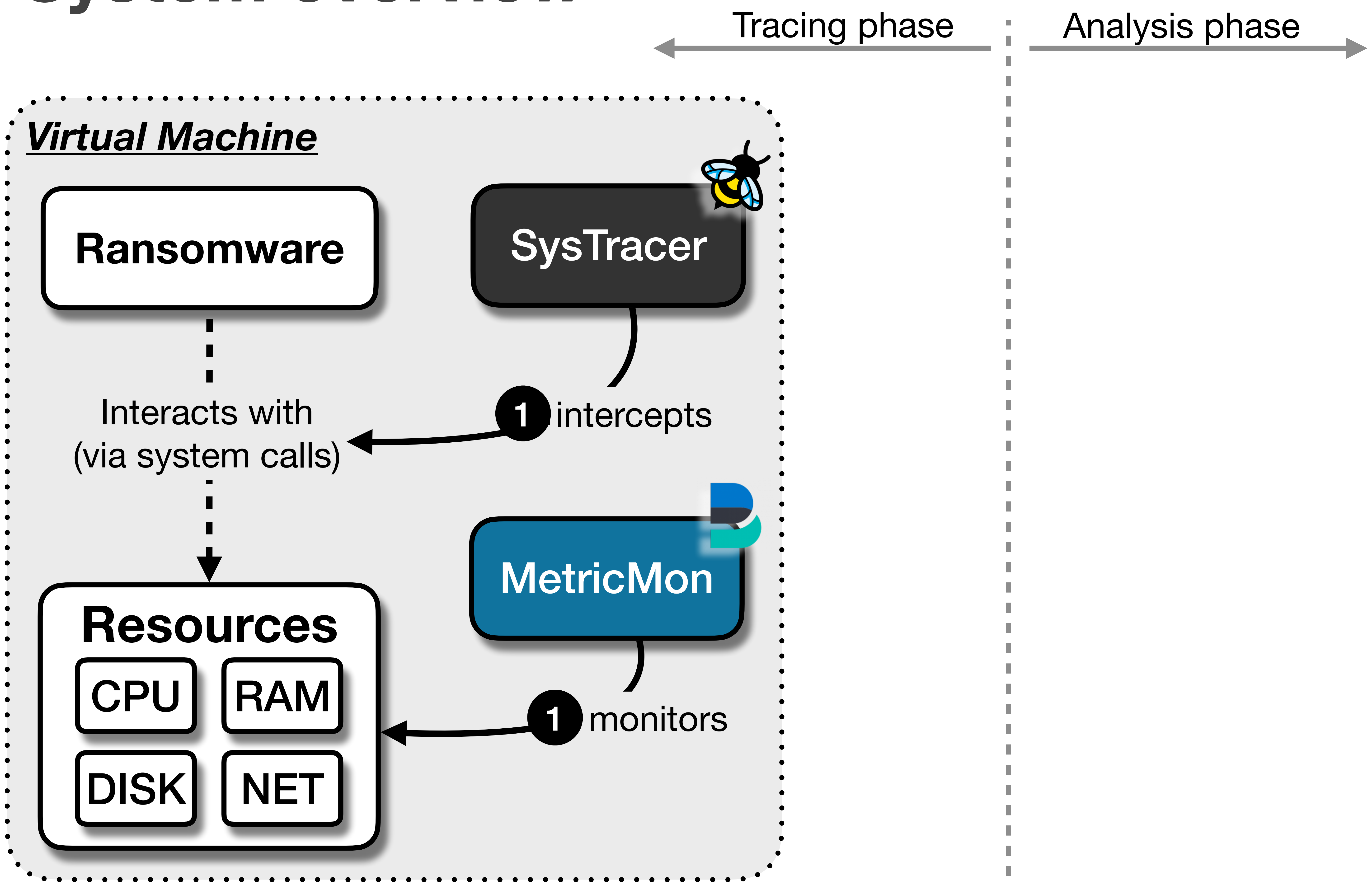
System overview



■ DIO's components ■ New components

CRIBA

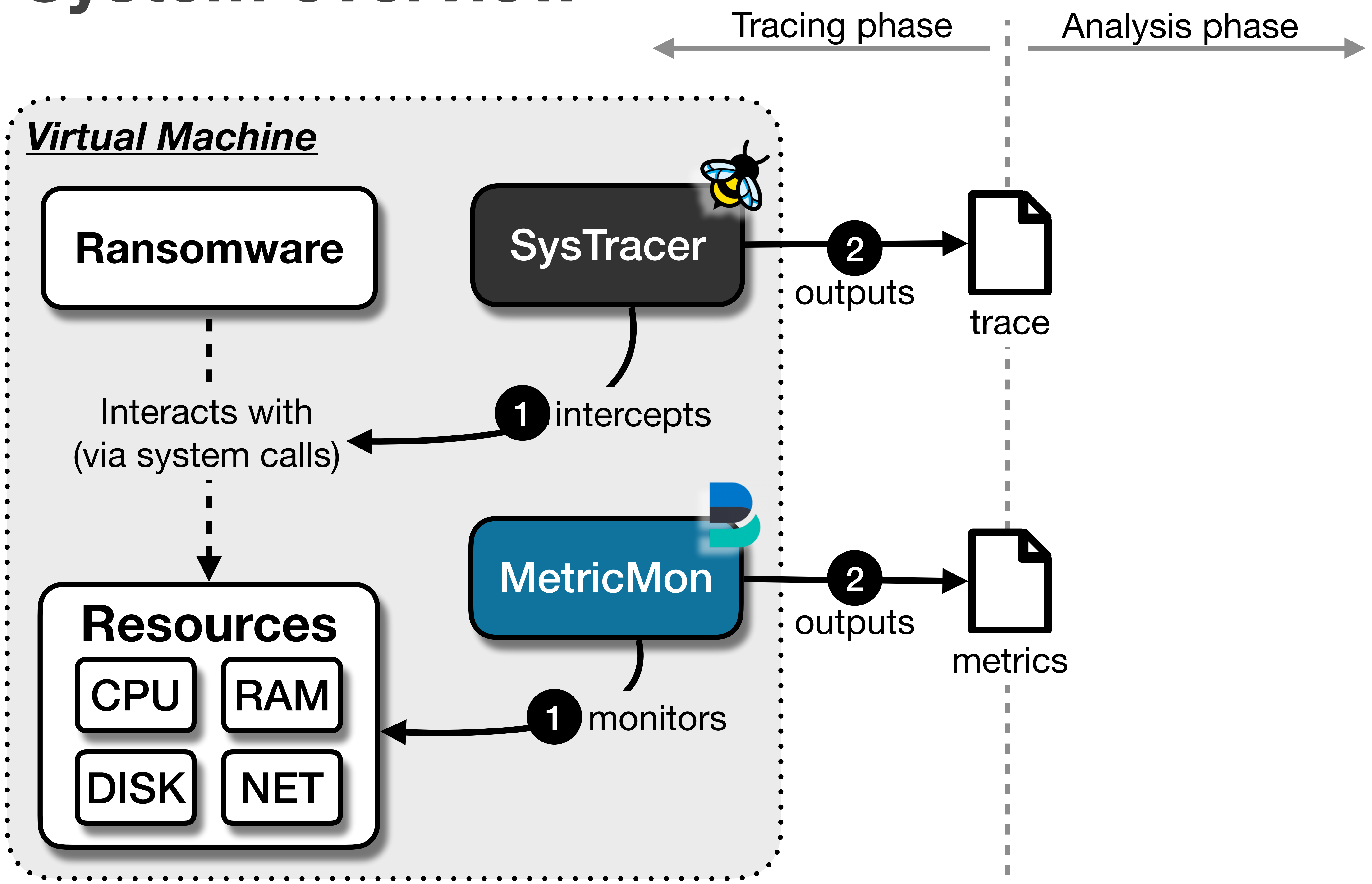
System overview



⬛ DIO's components 🟦 New components

CRIBA

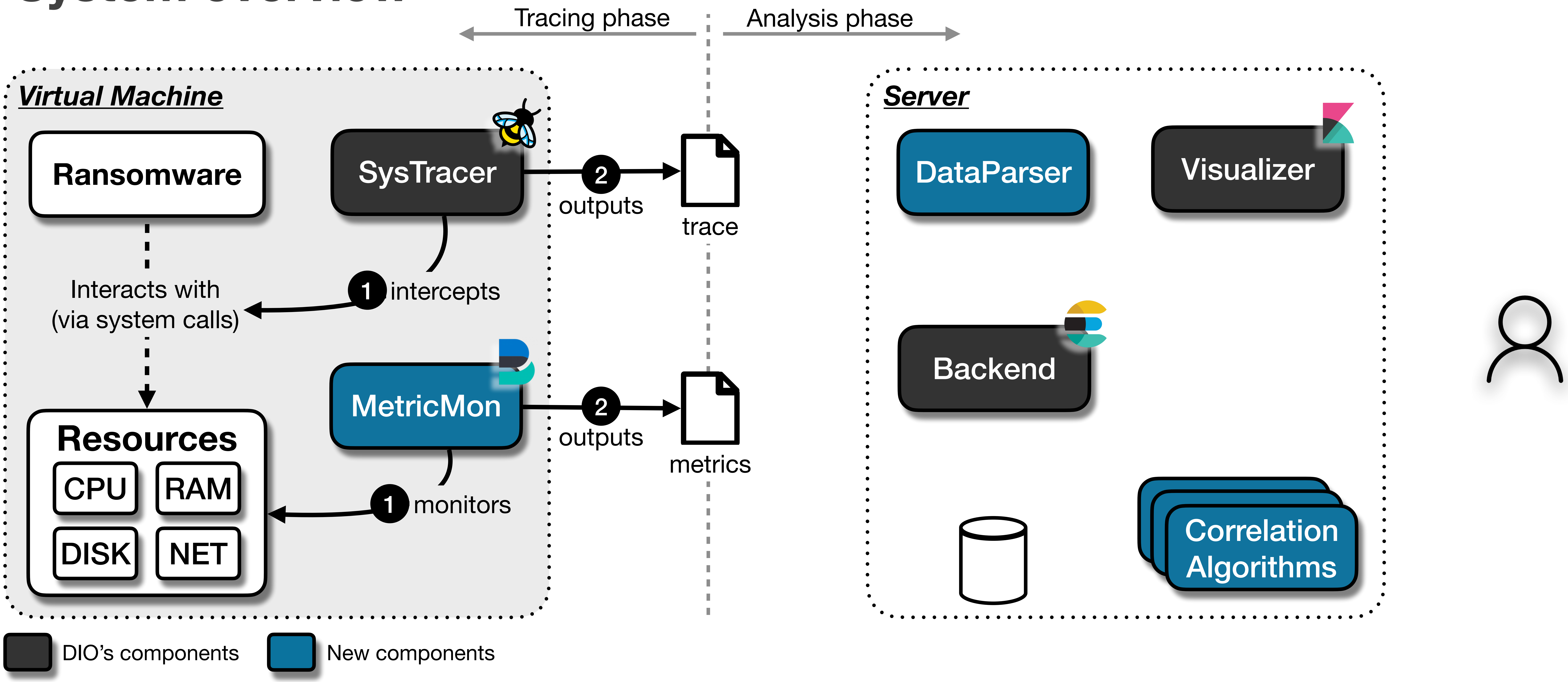
System overview



⬛ DIO's components 🟦 New components

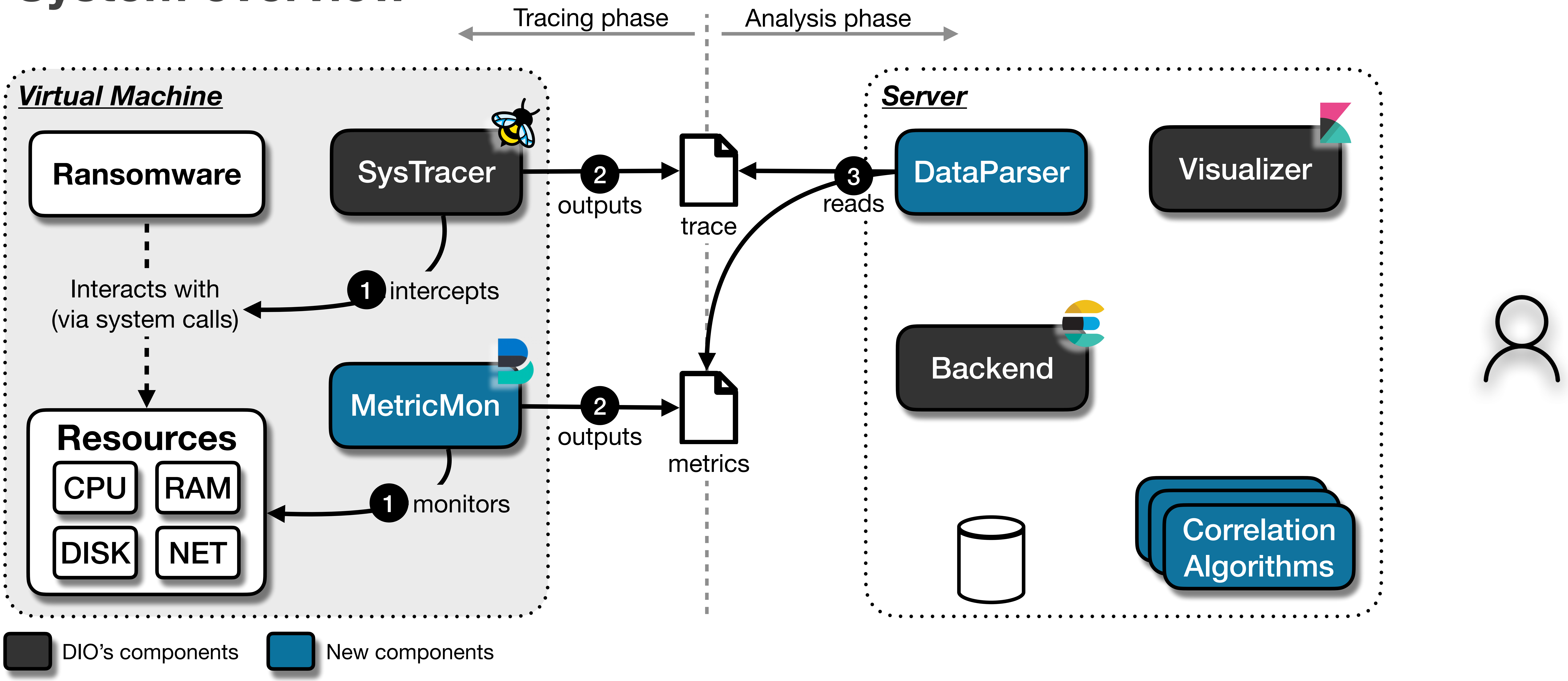
CRIBA

System overview



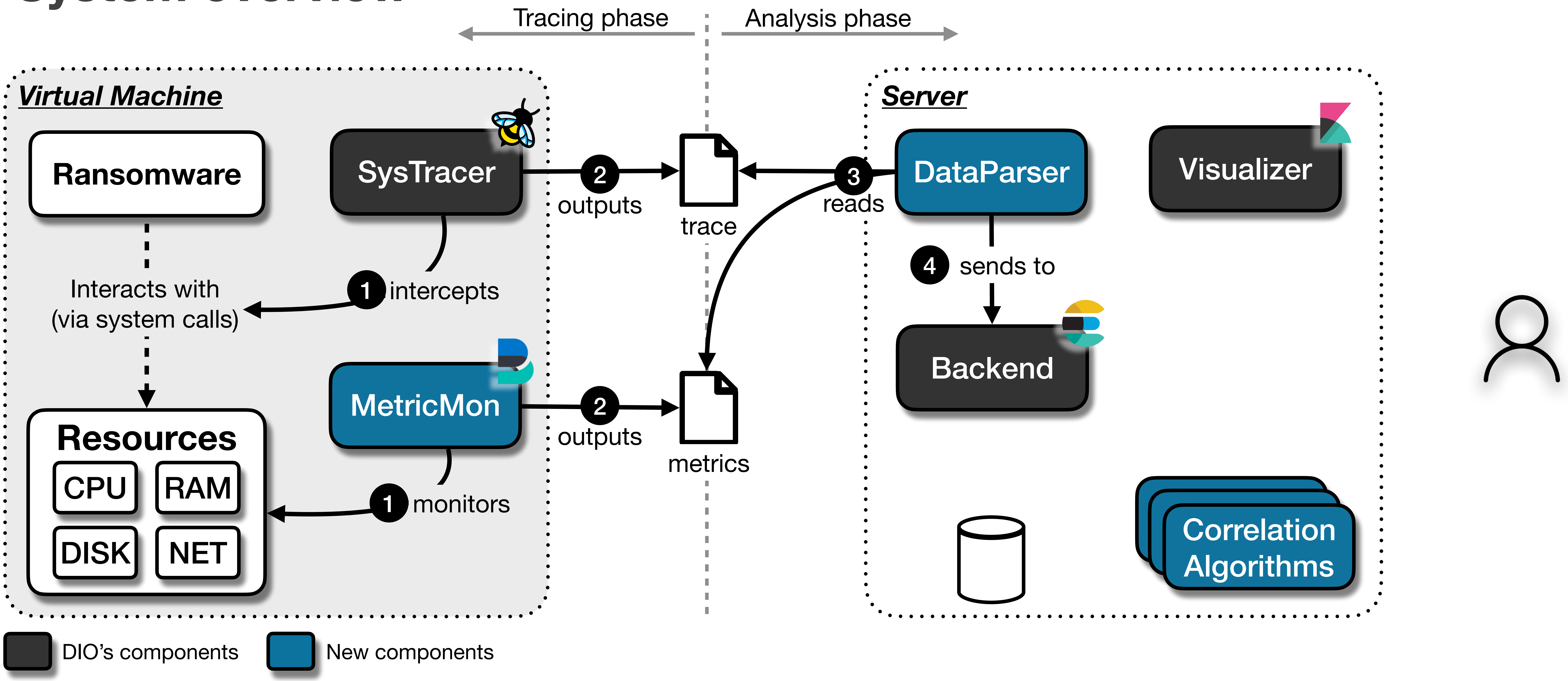
CRIBA

System overview



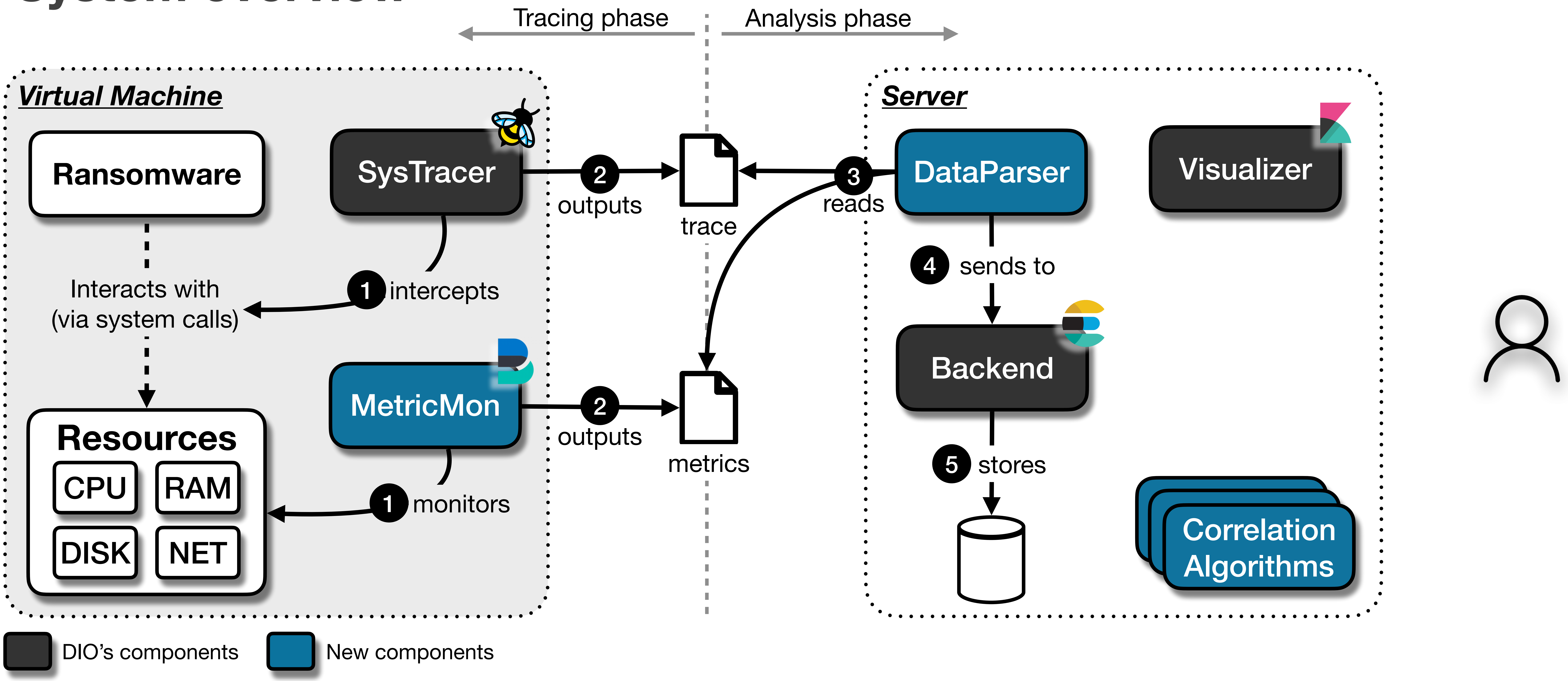
CRIBA

System overview



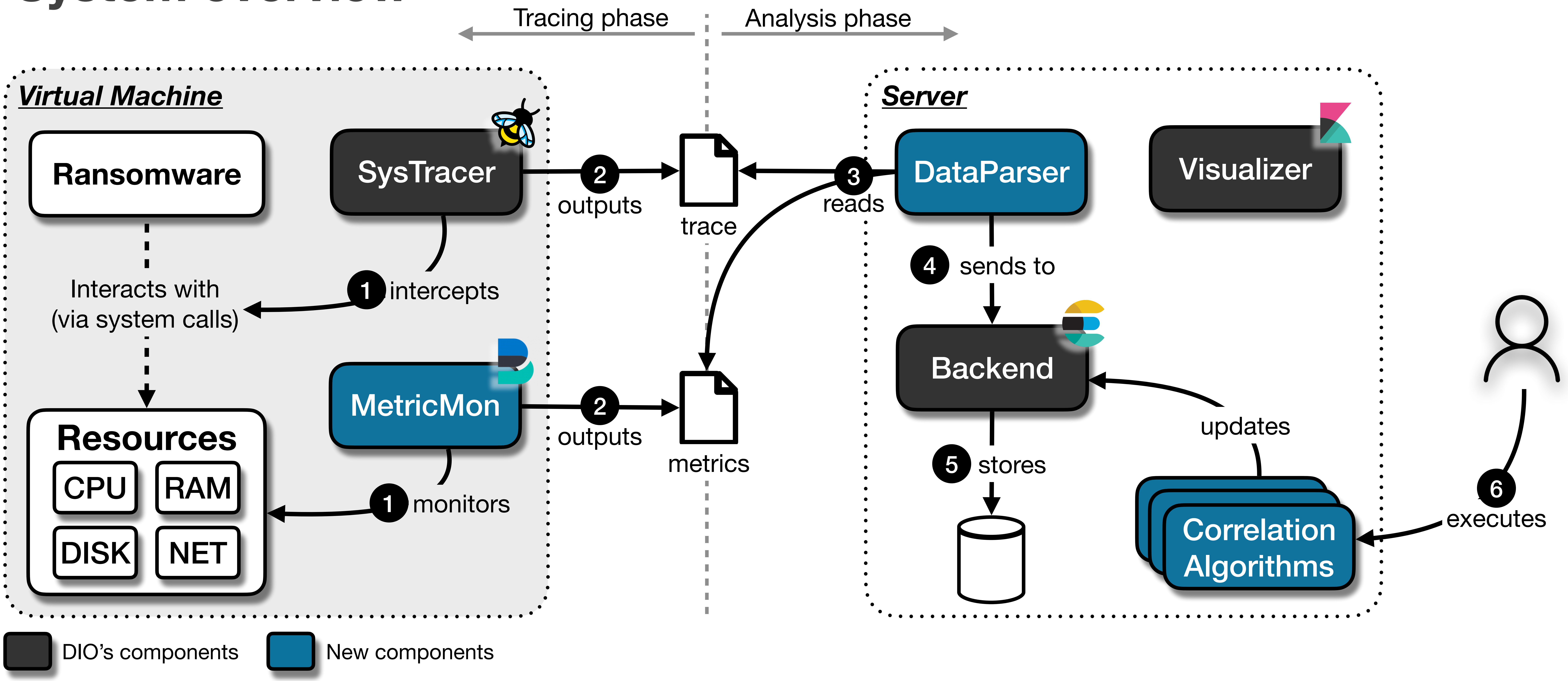
CRIBA

System overview



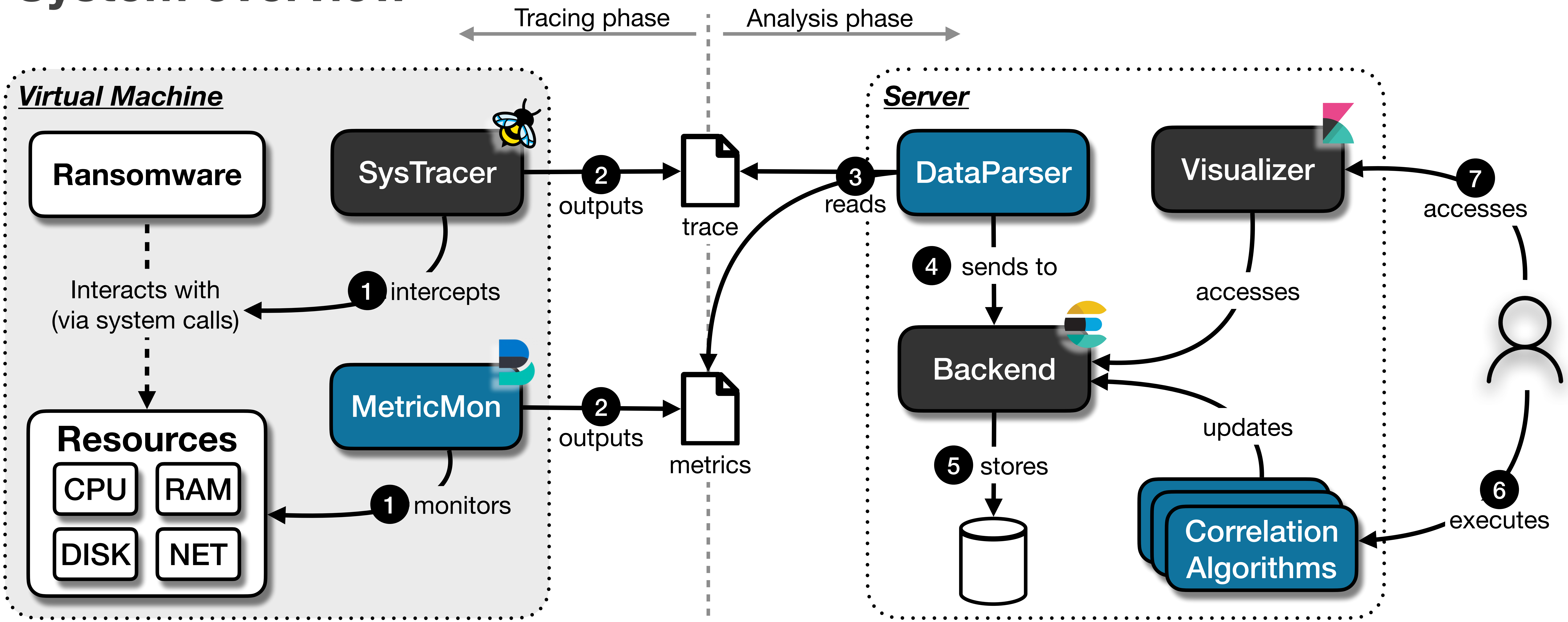
CRIBA

System overview



CRIBA

System overview



⬛ DIO's components 🟦 New components

Linux Ransomware Study

[1] Agrawal, N., Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2009). *Generating realistic impressions for file-system benchmarking*. ACM Transactions on Storage (TOS), 5(4), 1-30.

Linux Ransomware Study

- **Goals**
  - Explore and understand characteristic I/O behaviors exhibited by ransomware.
  - Compare different families to find their distinct and common patterns.

[1] Agrawal, N., Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2009). *Generating realistic impressions for file-system benchmarking*. ACM Transactions on Storage (TOS), 5(4), 1-30.

Linux Ransomware Study

- **Goals**
  - Explore and understand characteristic I/O behaviors exhibited by ransomware.
  - Compare different families to find their distinct and common patterns.

- **5 Linux Ransomware Families**
  - AvosLocker, RansomEXX, REvil, Erebus, Darkside

[1] Agrawal, N., Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2009). *Generating realistic impressions for file-system benchmarking*. ACM Transactions on Storage (TOS), 5(4), 1-30.

Linux Ransomware Study

◉ Goals

- ▸ Explore and understand characteristic I/O behaviors exhibited by ransomware.
- ▸ Compare different families to find their distinct and common patterns.

◉ 5 Linux Ransomware Families

- ▸ AVOSLOCKER, RANSOMEXX, REVIL, EREBUS, DARKSIDE

◉ File Dataset

- ▸ File system image with realistic metadata and content generated with the Impressions framework [1].
- ▸ Adapted to include file extensions targeted by some ransomware families.
- ▸ *35,418* files, *3,510* directories, and *8,267* unique file extensions.

[1] Agrawal, N., Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2009). *Generating realistic impressions for file-system benchmarking*. ACM Transactions on Storage (TOS), 5(4), 1-30.

Linux Ransomware Study

◉ Goals

- Explore and understand characteristic I/O behaviors exhibited by ransomware.
- Compare different families to find their distinct and common patterns.

◉ 5 Linux Ransomware Families

- AVOSLOCKER, RANSOMEXX, REVIL, EREBUS, DARKSIDE

◉ File Dataset

- File system image with realistic metadata and content generated with the Impressions framework [1].
- Adapted to include file extensions targeted by some ransomware families.
- *35,418* files, *3,510* directories, and *8,267* unique file extensions.

◉ 6 Correlation algorithms 7 Visualization dashboards

[1] Agrawal, N., Arpaci-Dusseau, A. C., & Arpaci-Dusseau, R. H. (2009). *Generating realistic impressions for file-system benchmarking*. ACM Transactions on Storage (TOS), 5(4), 1-30.

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

◉ Different execution time, process/thread creation, and file/extension access patterns.

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

- Different execution time, process/thread creation, and file/extension access patterns.

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

- Different execution time, process/thread creation, and file/extension access patterns.

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

◉ Different execution time, process/thread creation, and file/extension access patterns.

◉ Metadata-related operations are the most predominant.

Linux Ransomware Study

Generic statistics

Ransomware Family	Execution time (mins)	Process		Accesses		Syscalls		
		#PIDs	#TIDs	Paths	Extensions	Types	Data-Metadata (%)	Storage-Network (%)
AvosLocker	1.481	1	2	11,646	3,044	8	34 - **66**	100 - 0
RansomExx	3.126	1	5	85,583	**19,341**	9	32 - **68**	100 - 0
REvil	8.719	**12**	**13**	39,384	8,275	9	42 - **58**	100 - 0
Erebus	**10.361**	3	12	**107,307**	8,482	**17**	27 - **73**	99.96 - **0.04**
DarkSide	0.386	1	6	11,244	12	19	25 - **75**	99.79 - **0.21**

- Different execution time, process/thread creation, and file/extension access patterns.
- Metadata-related operations are the most predominant.
- Network-related calls are only issued by a few families.

Linux Ransomware Study

Ransom notes

Ransomware Family	File name	System call sequence	# Files
AvosLocker	README_FOR_RESTORE	OP→ST→WR→CL	1,019
RansomExx	!NEWS_FOR_STJ!.txt	ST→OP→ST→WR→CL	3,513
REvil	qoxaq-readme.txt	OP→ST→WR→CL	3,501
Erebus	_DECRYPT_FILE.html	OP→WR→CL→RN→OP→WR→CL	8,430
	_DECRYPT_FILE.txt	OP→WR→CL	4,000
Darkside	darkside_readme.txt	ST ST→OP→WR→CL ST→OP→WR→CL→ST	274

◉ Similar behaviors

- Same name for files across directories.
- Similar set of system calls (OP-open, ST-stat, WR-write, CL-close).

◉ Distinct patterns

- Number of ransom notes created.
- Multiple file extensions (Erebus).
- Multiple system call sequences by DarkSide.

Linux Ransomware Study

Ransom notes

Ransomware Family	File name	System call sequence	# Files
AvosLocker	README_FOR_RESTORE	OP→ST→WR→CL	1,019
RansomExx	!NEWS_FOR_STJ!.txt	ST→OP→ST→WR→CL	3,513
REvil	qoxaq-readme.txt	OP→ST→WR→CL	3,501
Erebus	_DECRYPT_FILE.html	OP→WR→CL→RN→OP→WR→CL	8,430
	_DECRYPT_FILE.txt	OP→WR→CL	4,000
DarkSide	darkside_readme.txt	ST ST→OP→WR→CL ST→OP→WR→CL→ST	274

◉ Similar behaviors

- Same name for files across directories.
- Similar set of system calls (OP-open, ST-stat, WR-write, CL-close).

◉ Distinct patterns

- Number of ransom notes created.
- Multiple file extensions (Erebus).
- Multiple system call sequences by DarkSide.

Linux Ransomware Study

Ransom notes

Ransomware Family	File name	System call sequence	# Files
AvosLocker	README_FOR_RESTORE	OP→ST→WR→CL	1,019
RansomExx	!NEWS_FOR_STJ!.txt	ST→OP→ST→WR→CL	3,513
REvil	qoxaq-readme.txt	OP→ST→WR→CL	3,501
Erebus	_DECRYPT_FILE.html	OP→WR→CL→RN→OP→WR→CL	8,430
	_DECRYPT_FILE.txt	OP→WR→CL	4,000
DarkSide	darkside_readme.txt	ST ST→OP→WR→CL ST→OP→WR→CL→ST	274

◉ Similar behaviors

- Same name for files across directories.
- Similar set of system calls (OP-open, ST-stat, WR-write, CL-close).

◉ Distinct patterns

- Number of ransom notes created.
- Multiple file extensions (Erebus).
- Multiple system call sequences by DarkSide.

Linux Ransomware Study

Ransom notes

Ransomware Family	File name	System call sequence	# Files
AvosLocker	README_FOR_RESTORE	OP→ST→WR→CL	1,019
RansomExx	!NEWS_FOR_STJ!.txt	ST→OP→ST→WR→CL	3,513
REvil	qoxaq-readme.txt	OP→ST→WR→CL	3,501
Erebus	_DECRYPT_FILE.html	OP→WR→CL→RN→OP→WR→CL	8,430
	_DECRYPT_FILE.txt	OP→WR→CL	4,000
DarkSide	darkside_readme.txt	ST ST→OP→WR→CL ST→OP→WR→CL→ST	274

◉ Similar behaviors

- Same name for files across directories.
- Similar set of system calls (OP-open, ST-stat, WR-write, CL-close).

◉ Distinct patterns

- Number of ransom notes created.
- Multiple file extensions (Erebus).
- Multiple system call sequences by DarkSide.

Linux Ransomware Study

Ransom notes

Ransomware Family	File name	System call sequence	# Files
AvosLocker	README_FOR_RESTORE	OP→ST→WR→CL	1,019
RansomExx	!NEWS_FOR_STJ!.txt	ST→OP→ST→WR→CL	3,513
REvil	qoxaq-readme.txt	OP→ST→WR→CL	3,501
Erebus	_DECRYPT_FILE.html	OP→WR→CL→RN→OP→WR→CL	8,430
	_DECRYPT_FILE.txt	OP→WR→CL	4,000
DarkSide	darkside_readme.txt	ST ST→OP→WR→CL ST→OP→WR→CL→ST	274

◉ Similar behaviors

- Same name for files across directories.
- Similar set of system calls (OP-open, ST-stat, WR-write, CL-close).

◉ Distinct patterns

- Number of ransom notes created.
- Multiple file extensions (Erebus).
- Multiple system call sequences by DarkSide.

Linux Ransomware Study

Dataset's File Access and Encryption

Linux Ransomware Study

Dataset’s File Access and Encryption

- ◉ System calls’ sequences change based on the targeted file and family.
  - ▸ Influenced by the file size and file extension.

Linux Ransomware Study

Dataset’s File Access and Encryption

- System calls’ sequences change based on the targeted file and family.
  - Influenced by the file size and file extension.
- Different patterns for:
  - the timing and placement of encryption keys at infected files.
  - the extensions used by each family when renaming encrypted files.

Linux Ransomware Study

Dataset's File Access and Encryption

- System calls' sequences change based on the targeted file and family.
  - Influenced by the file size and file extension.
- Different patterns for:
  - the timing and placement of encryption keys at infected files.
  - the extensions used by each family when renaming encrypted files.
- */dev/urandom* always accessed before each file encryption (REVIL and EREBUS).

Linux Ransomware Study

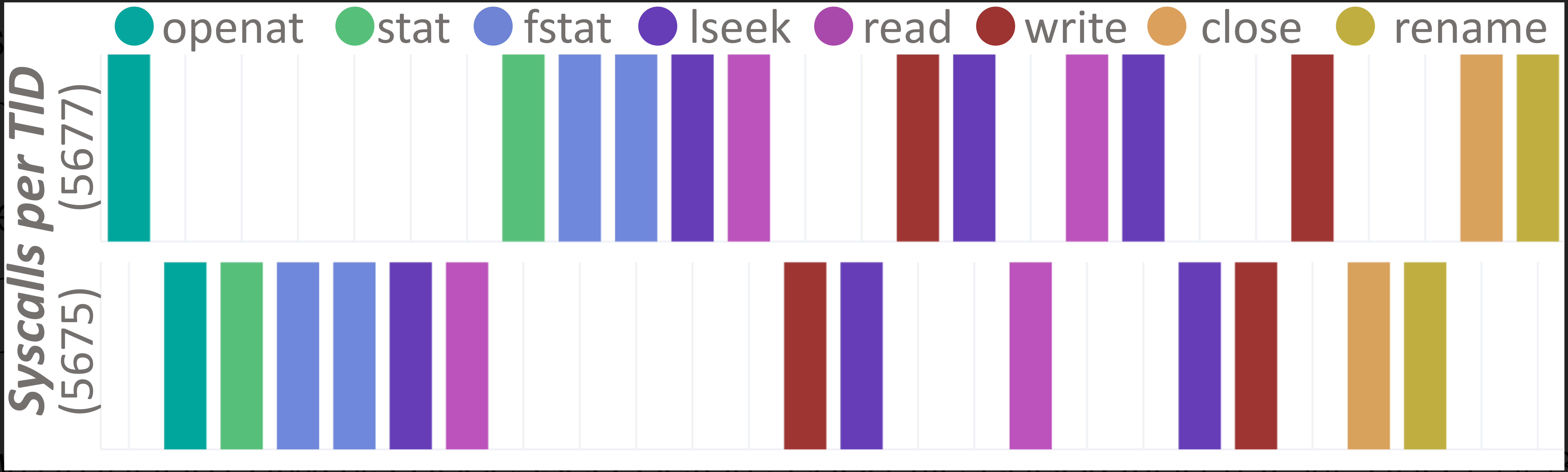
Dataset's File Access and Encryption

- ◉ System calls' sequences change based on the targeted file and family.
  - Influenced by the file size and file extension.
- ◉ Different patterns for:
  - the timing and placement of encryption keys at infected files.
  - the extensions used by each family when renaming encrypted files.
- ◉ */dev/urandom* always accessed before each file encryption (REvil and Erebus).
- ◉ RansomEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

Linux Ransomware Study

Dataset’s File Access and Encryption

- Sys
  - In
- Diff
  - th
  - th



- */dev/urandom* always accessed before each file encryption (REVIL and EREBUS).
- RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

Linux Ransomware Study

Dataset’s File Access and Encryption

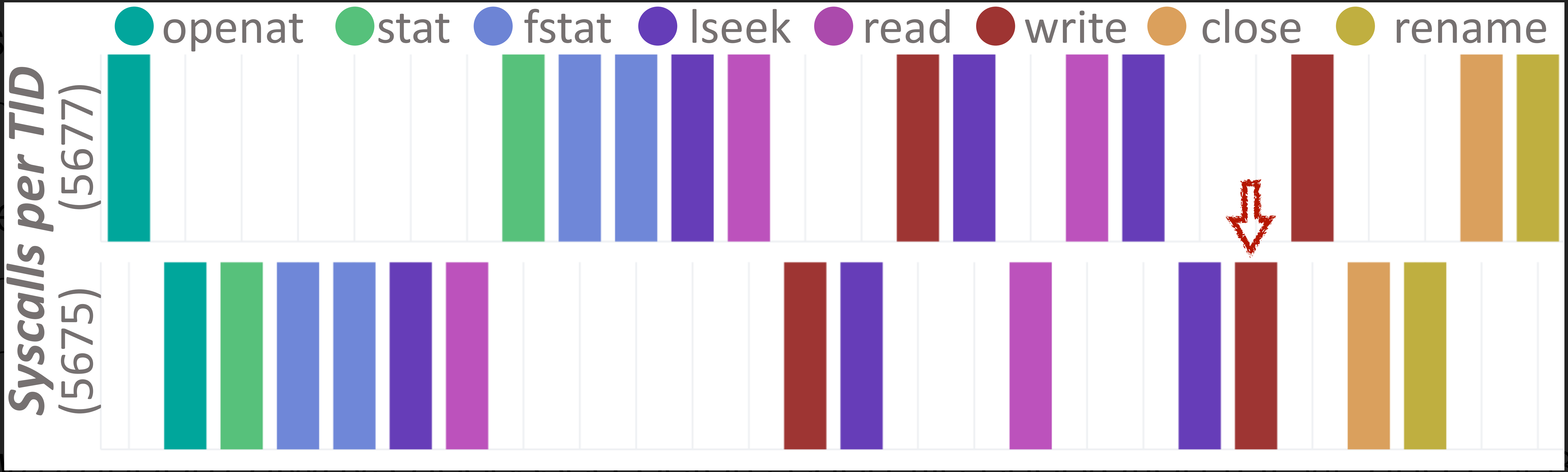
TID: 5675
Operation: Write
Offset: 0
Size: 1MB
Content: AAAA

◉ Sys

- In

◉ Diff

- th
- th



◉ /dev/urandom always accessed before each file encryption (REVIL and EREBUS).

◉ RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

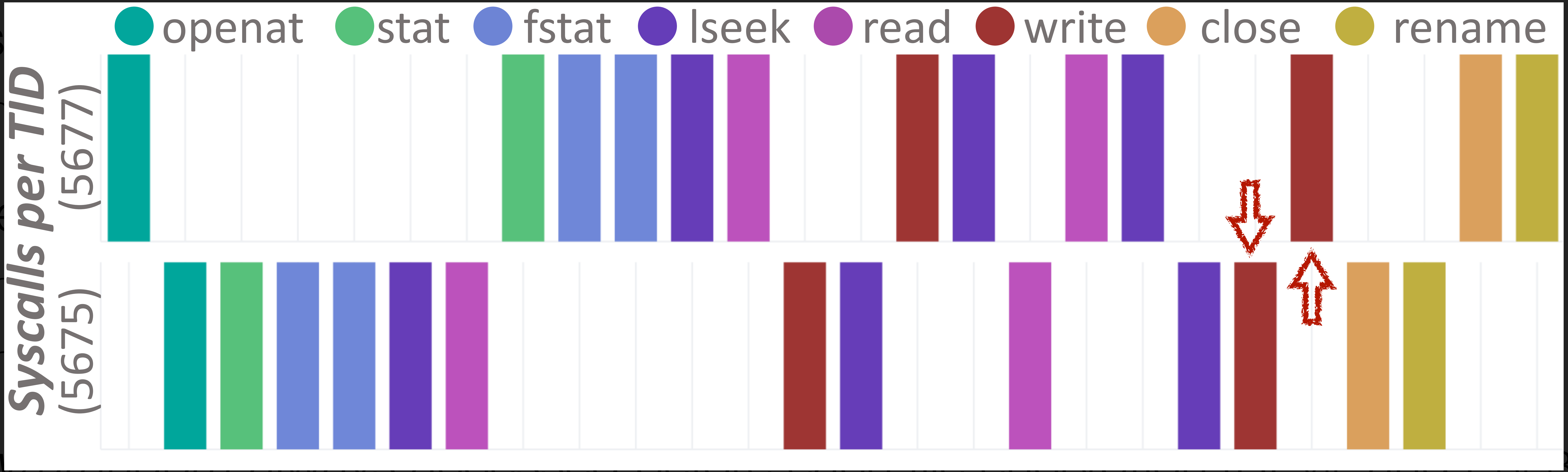
Linux Ransomware Study

Dataset’s File Access and Encryption

TID: 5675
Operation: Write
Offset: 0
Size: 1MB
Content: AAAA

TID: 5675
Operation: Write
Offset: 0
Size: 1MB
Content: BBBB

- Sys
  - In
- Diff
  - th
  - th

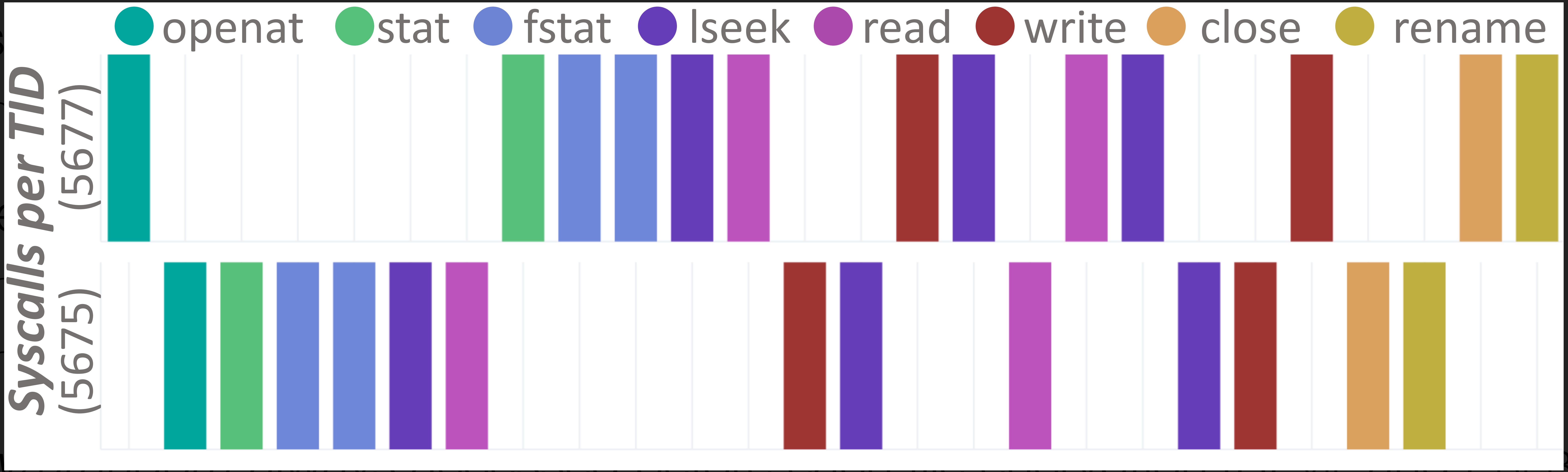


- */dev/urandom* always accessed before each file encryption (REVIL and EREBUS).
- RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

Linux Ransomware Study

Dataset’s File Access and Encryption

- Sys
  - In
- Diffe
  - th
  - th



- */dev/urandom* always accessed before each file encryption (REVIL and EREBUS).

- RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

Linux Ransomware Study

Dataset’s File Access and Encryption

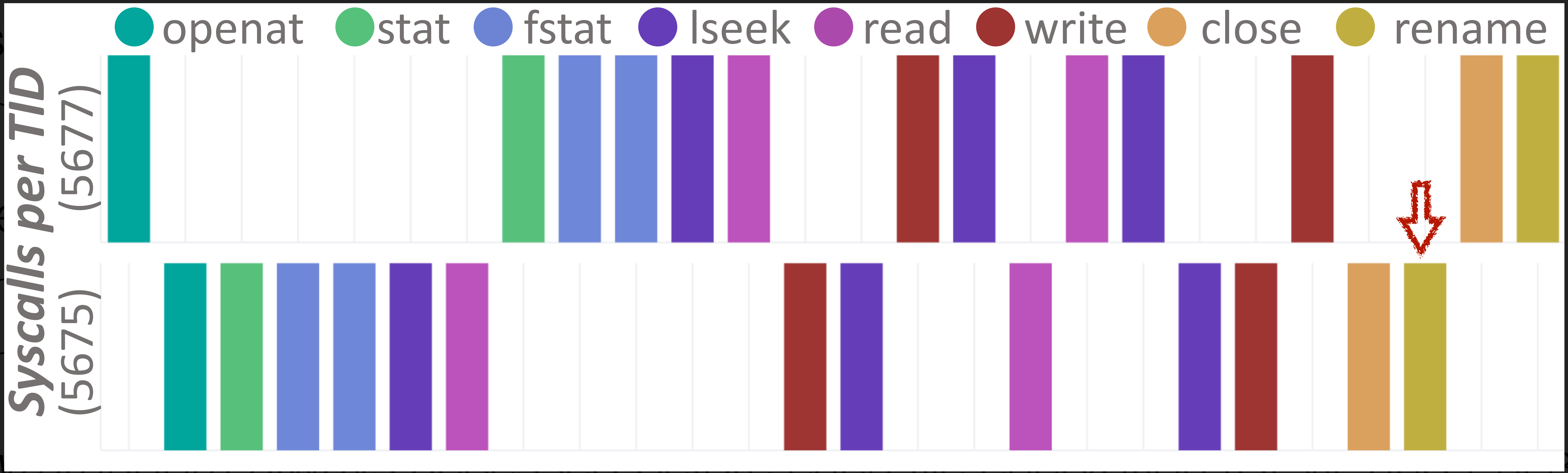
TID: 5675
Operation: Rename
Old file name: XXX.txt
New file name:
XXX.txt.stj888-36acf3f1
Result: success

◉ Sys

- In

◉ Diff

- th
- th



◉ */dev/urandom* always accessed before each file encryption (REVIL and EREBUS).

◉ RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

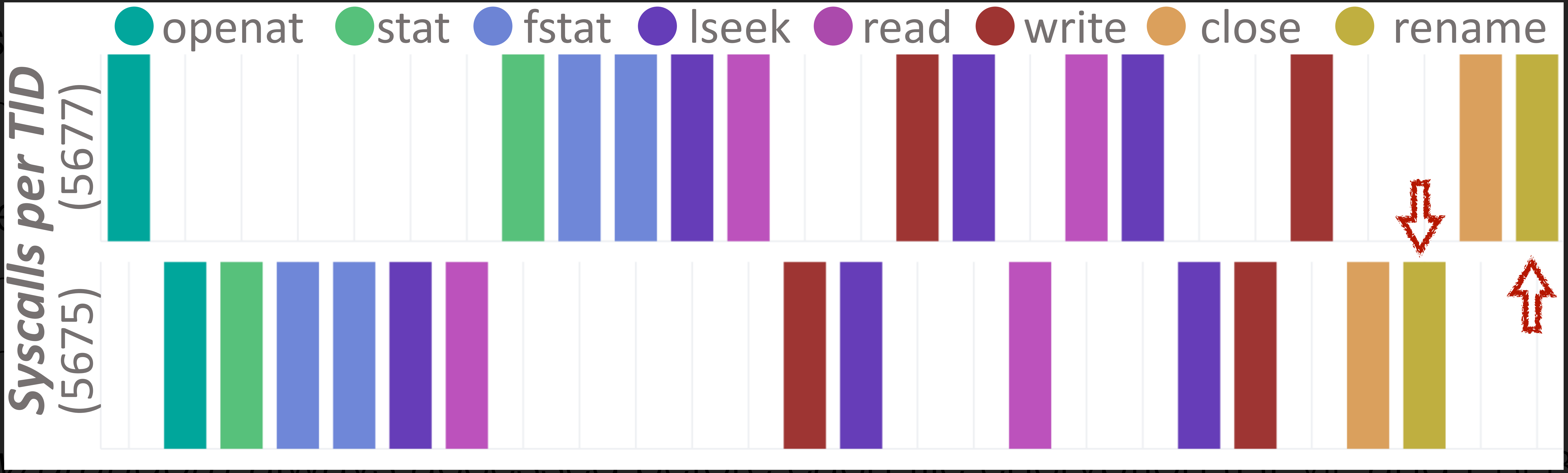
Linux Ransomware Study

Dataset's File Access and Encryption

TID: 5675
Operation: Rename
Old file name: XXX.txt
New file name:
XXX.txt.stj888-36acf3f1
Result: success

TID: 5677
Operation: Rename
Old file name: XXX.txt
New file name:
XXX.txt.stj888-40aa97db
Result: fail

- Sys
  - In
- Diffe
  - th
  - th



- /dev/urandom always accessed before each file encryption (REVIL and EREBUS).

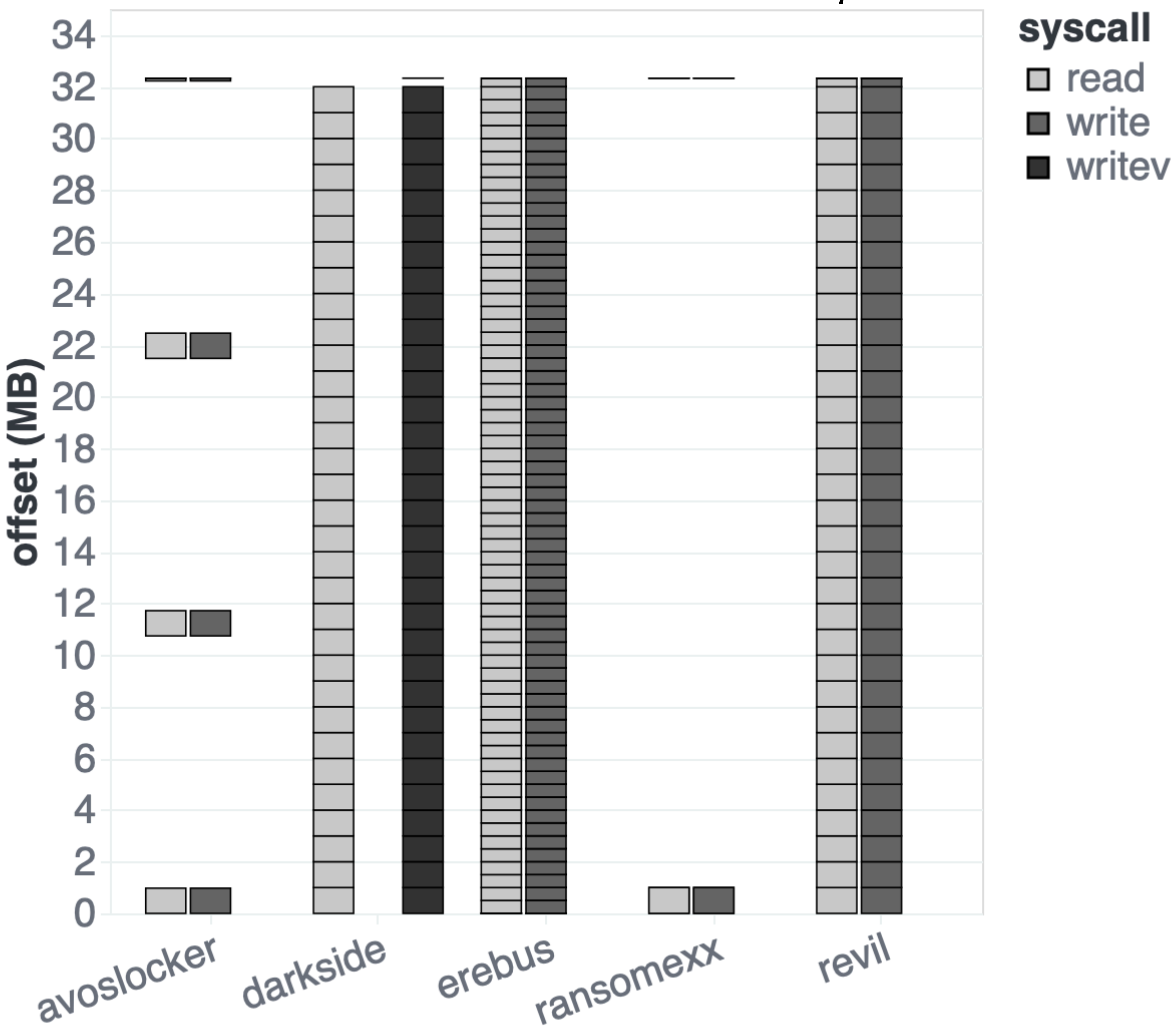
- RANSOMEXX has two threads concurrently encrypting the same files, a pattern that may lead to data corruption.

Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

- ◉ Only REVIL and EREBUS overwrite the full content of files.
- ◉ Other families process partial content of files and/or target specific file extensions.
- ◉ These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

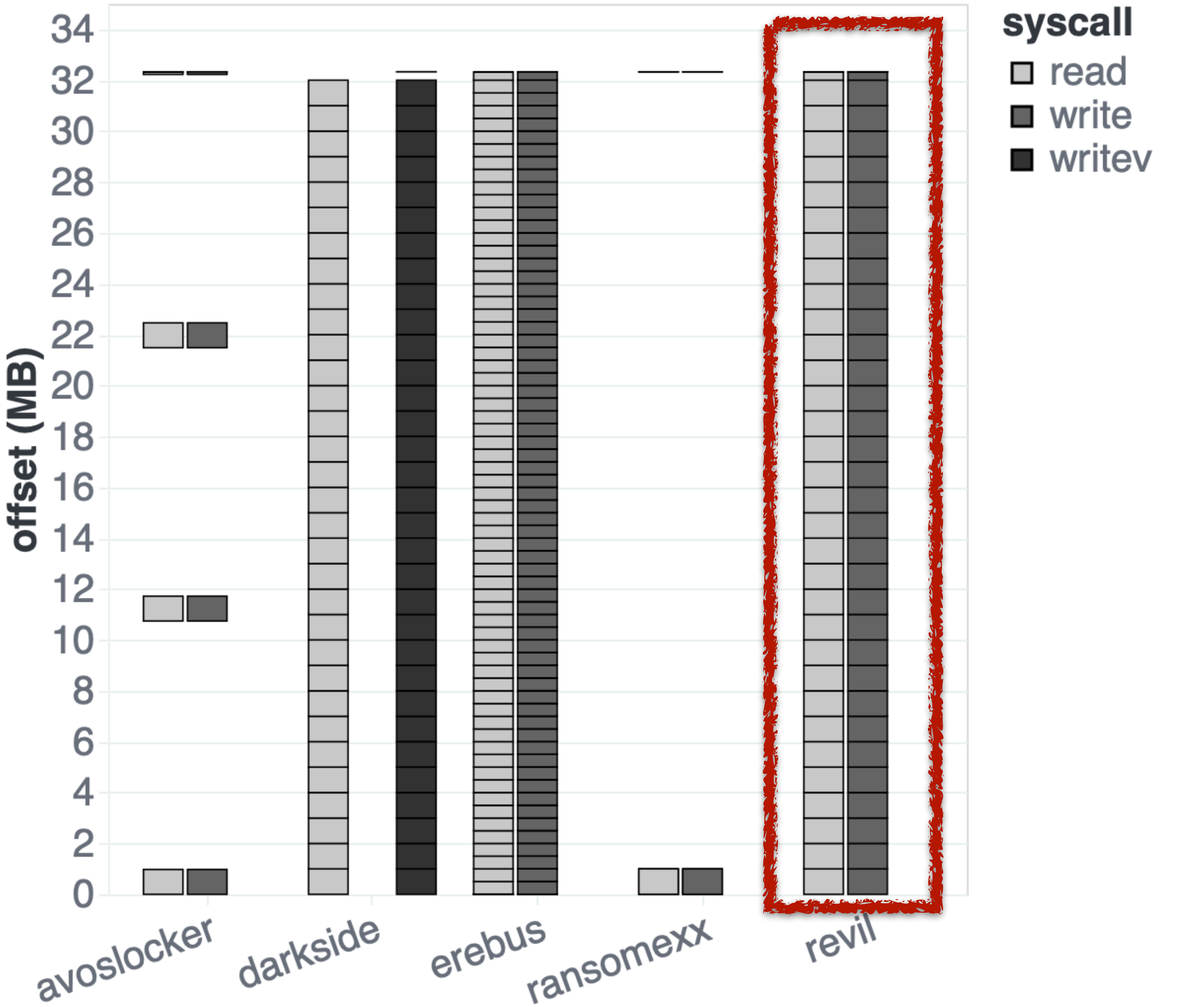
- Processes full content.
- Uses blocks of 1MiB.
- Processes all dataset.

◉ Only REVIL and EREBUS overwrite the full content of files.

◉ Other families process partial content of files and/or target specific file extensions.

◉ These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



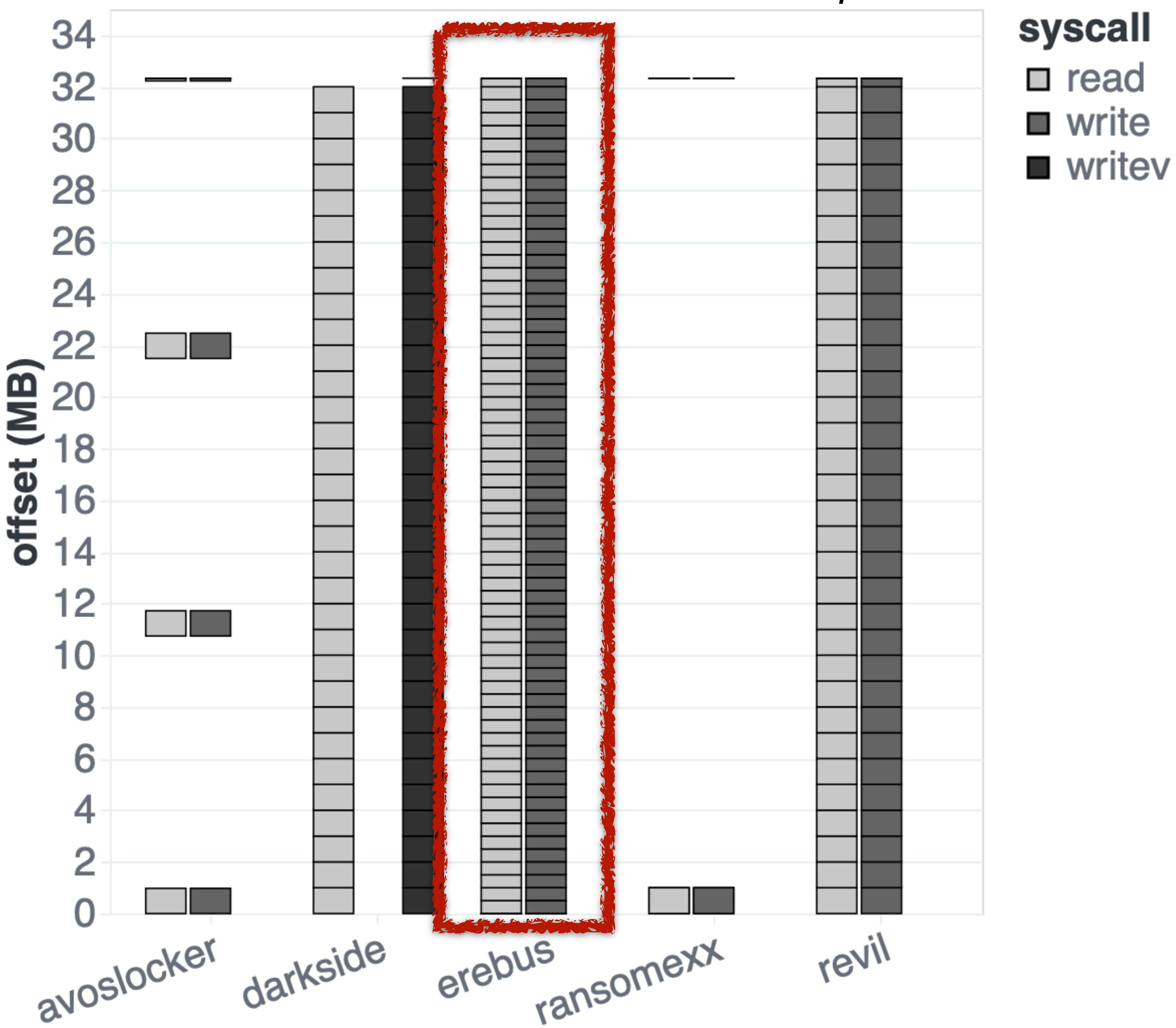
Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

- Processes full content.
- Uses blocks of 512KiB.
- Processes 33% of the dataset.

- Only REVIL and EREBUS overwrite the full content of files.
- Other families process partial content of files and/or target specific file extensions.
- These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



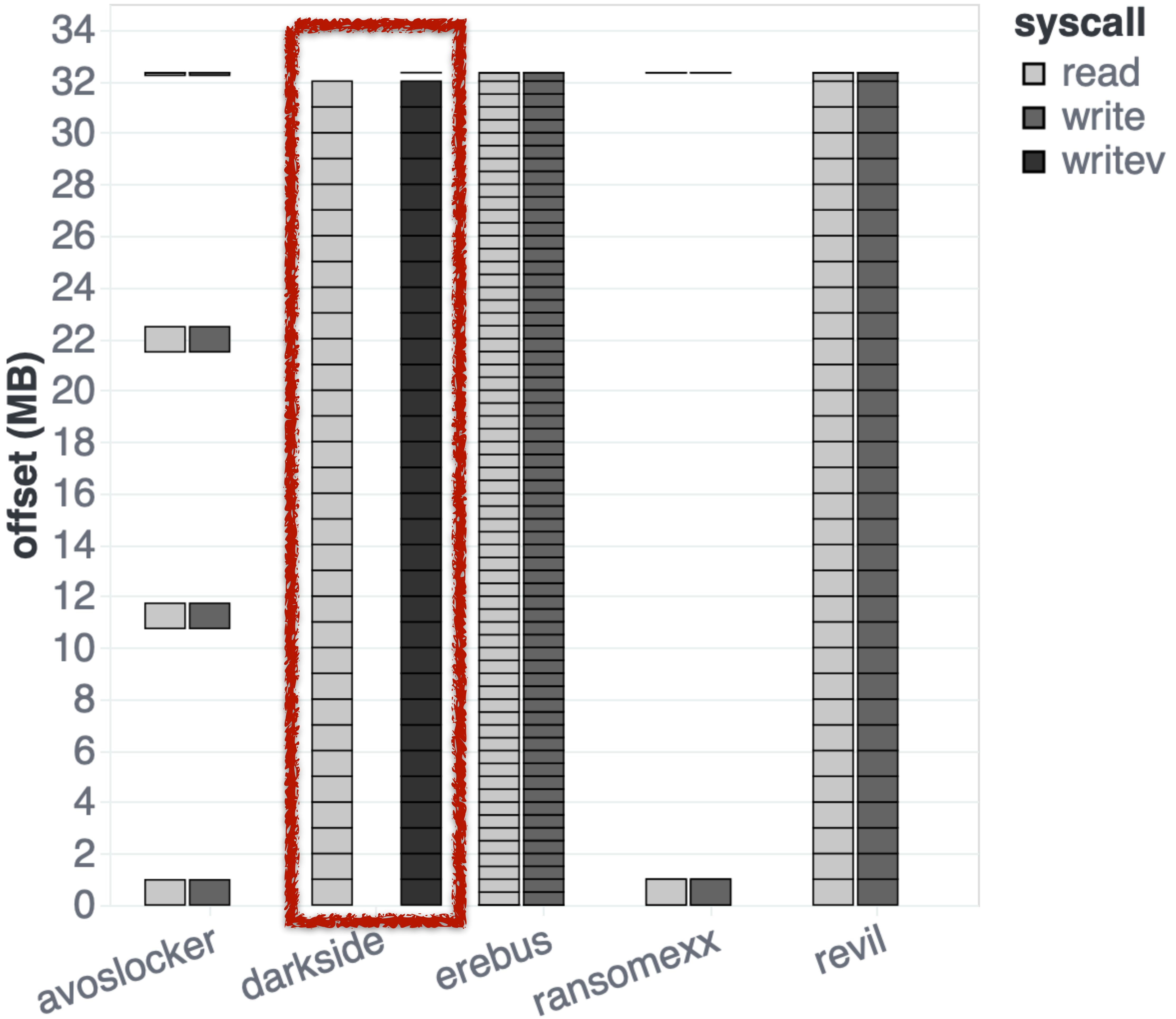
Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

- Last incomplete block in plaintext.
- Uses blocks of 1MiB.
- Targeted extensions: *.vmem*, *.vswp*, *.log* and *.vmdk*.

- Only REvil and Erebus overwrite the full content of files.
- Other families process partial content of files and/or target specific file extensions.
- These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



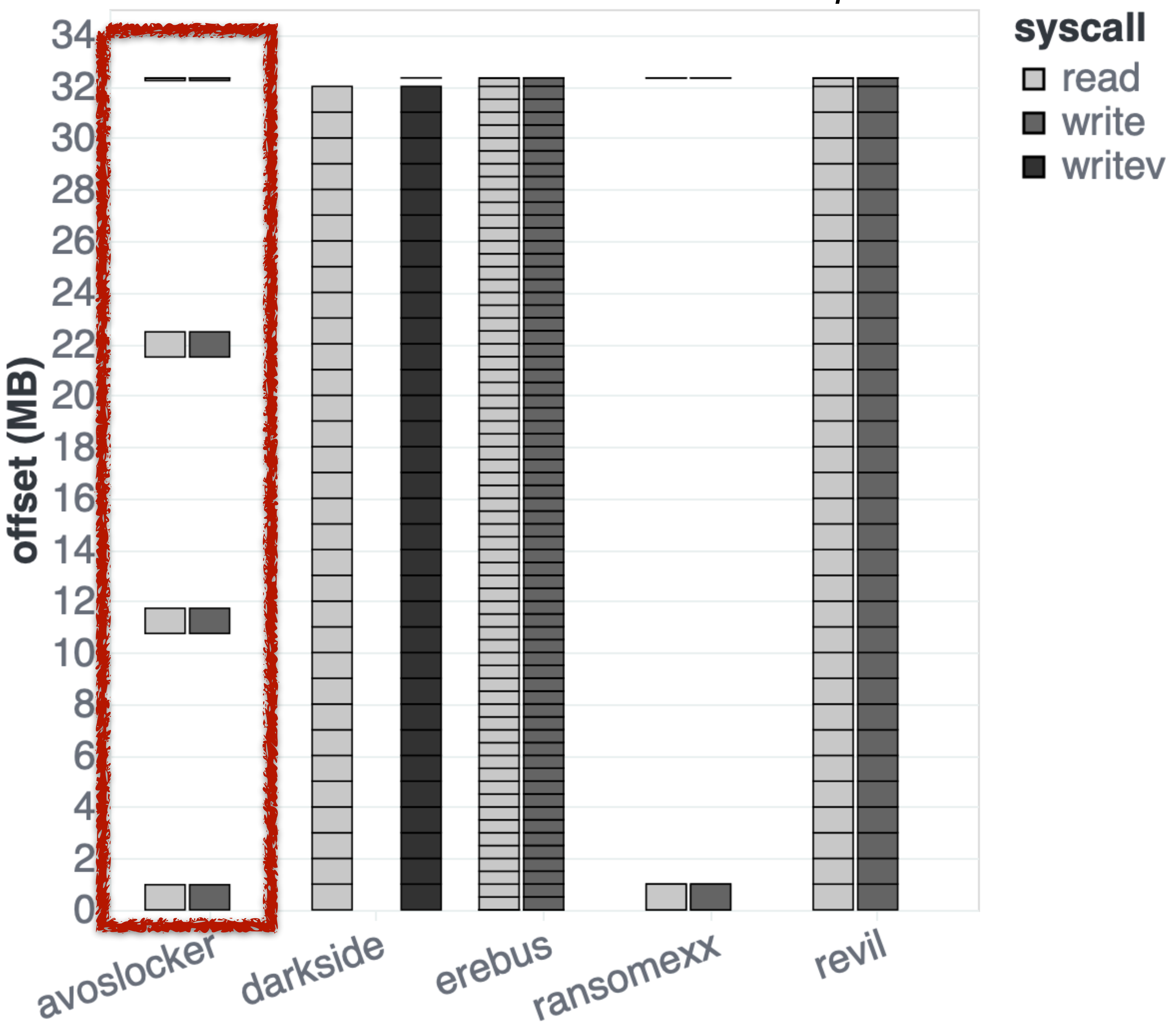
Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

- Processes a block of 0.89MiB for every 10.78MiB.
- Accesses 30% of the dataset.

- Only REvil and Erebus overwrite the full content of files.
- Other families process partial content of files and/or target specific file extensions.
- These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



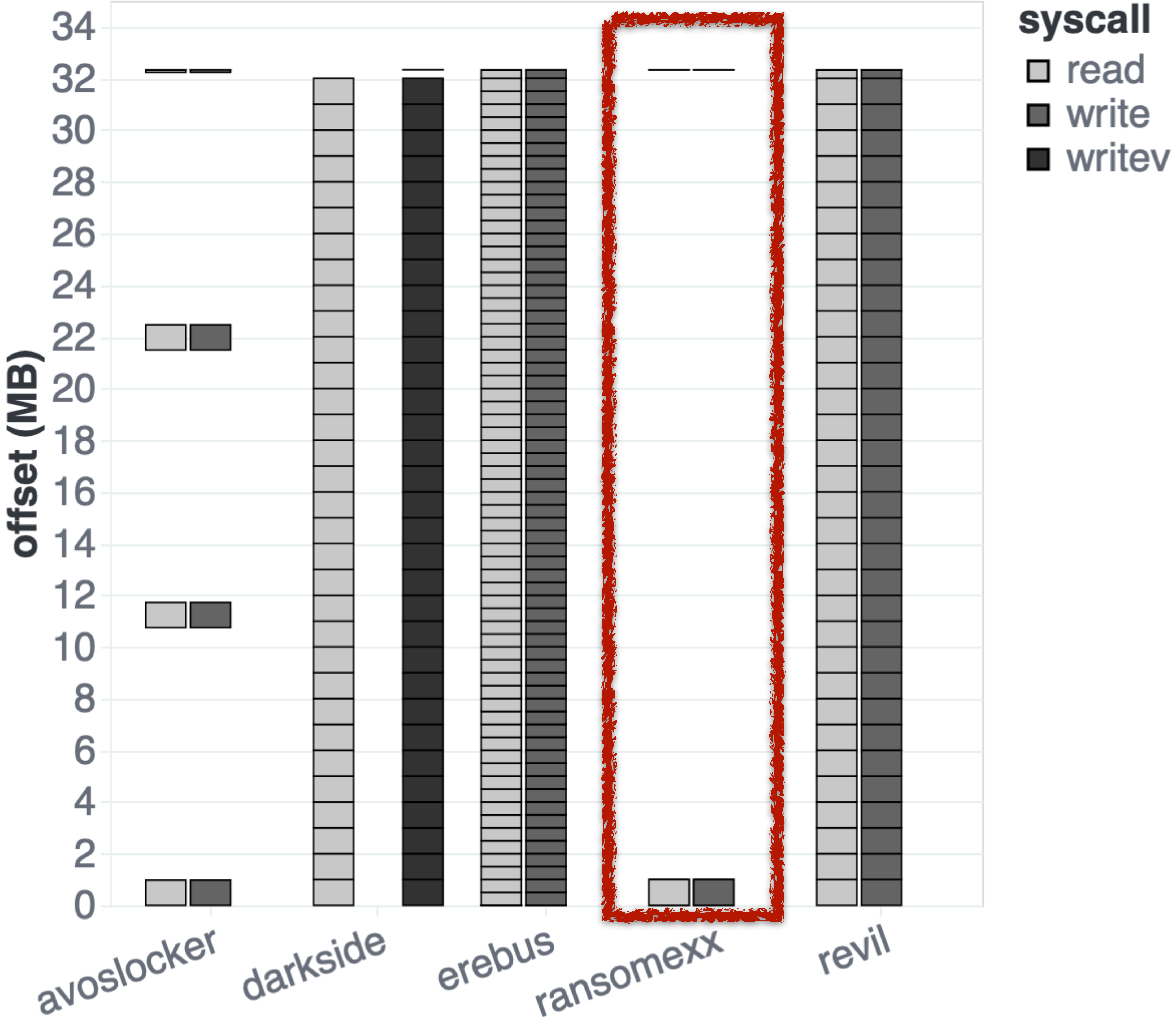
- For some files only encrypts the first 1MiB block.
- For others, sparsely processes multiple blocks of 1MiB.

Linux Ransomware Study

Dataset's File Selection and Evasion Techniques

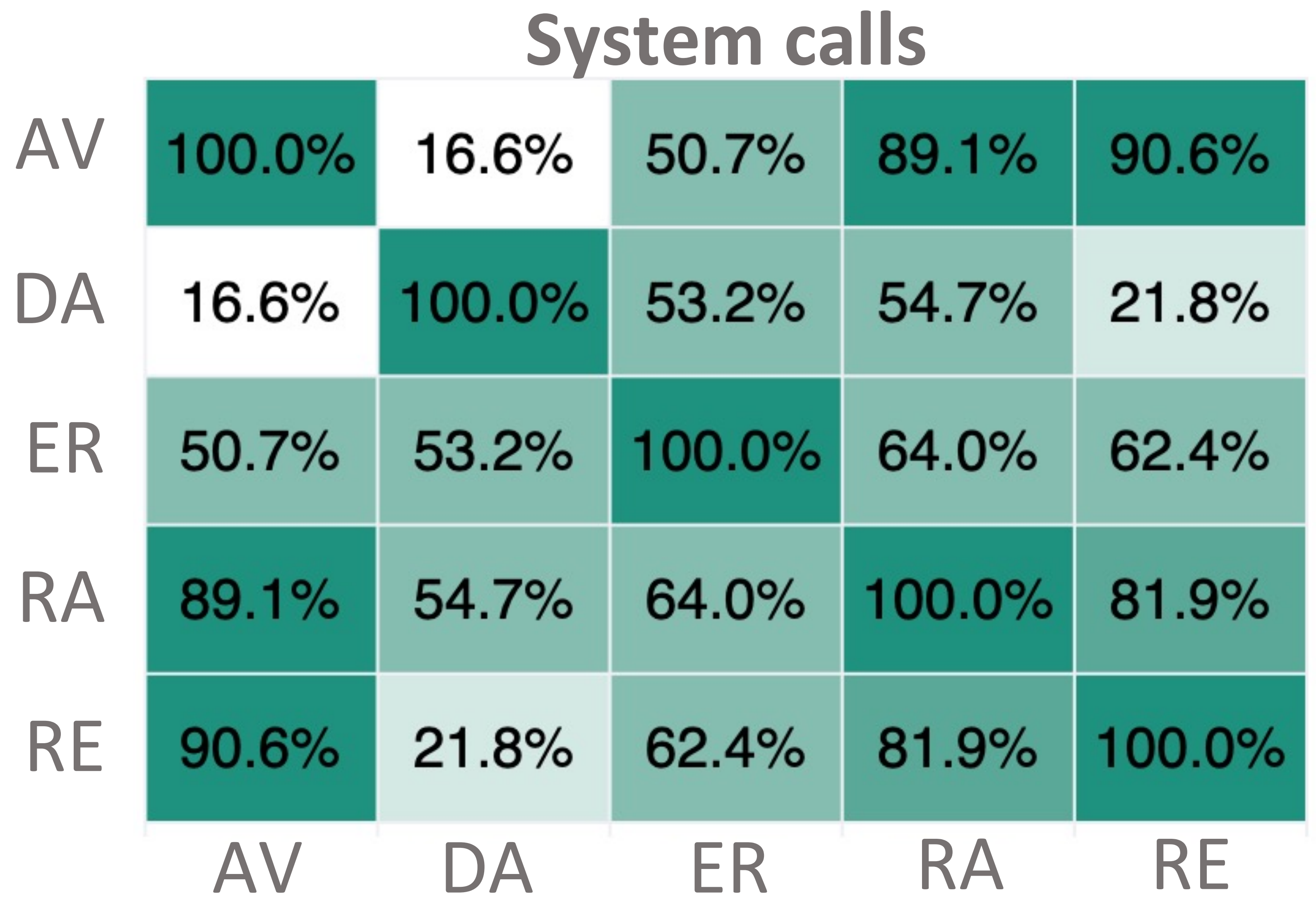
- Only REvil and Erebus overwrite the full content of files.
- Other families process partial content of files and/or target specific file extensions.
- These patterns enable faster execution and lower CPU usage, and are used to deceive detection tools.

Accessed file offsets for file F10573.bqt.vmdk



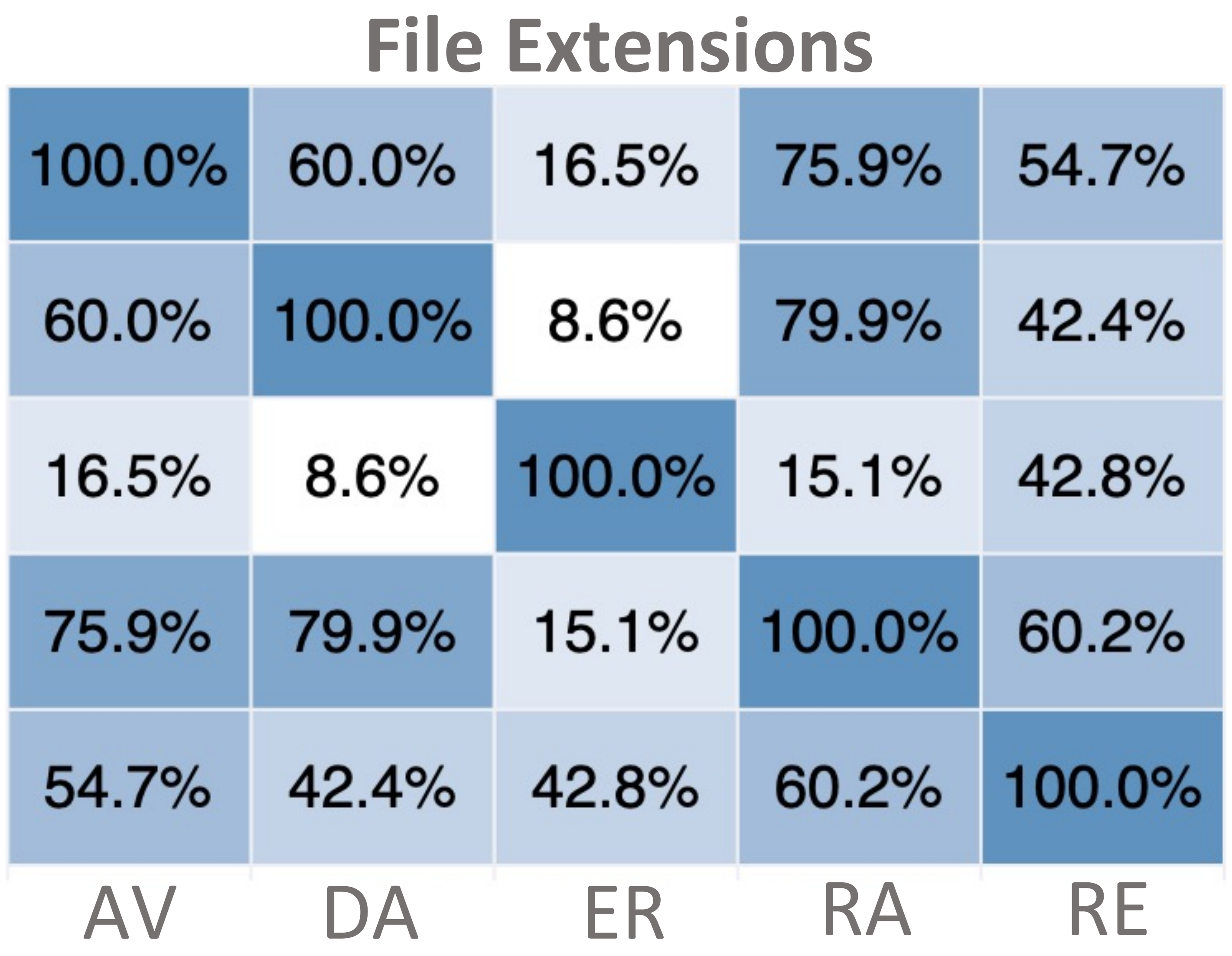
Linux Ransomware Study

Families Similarity



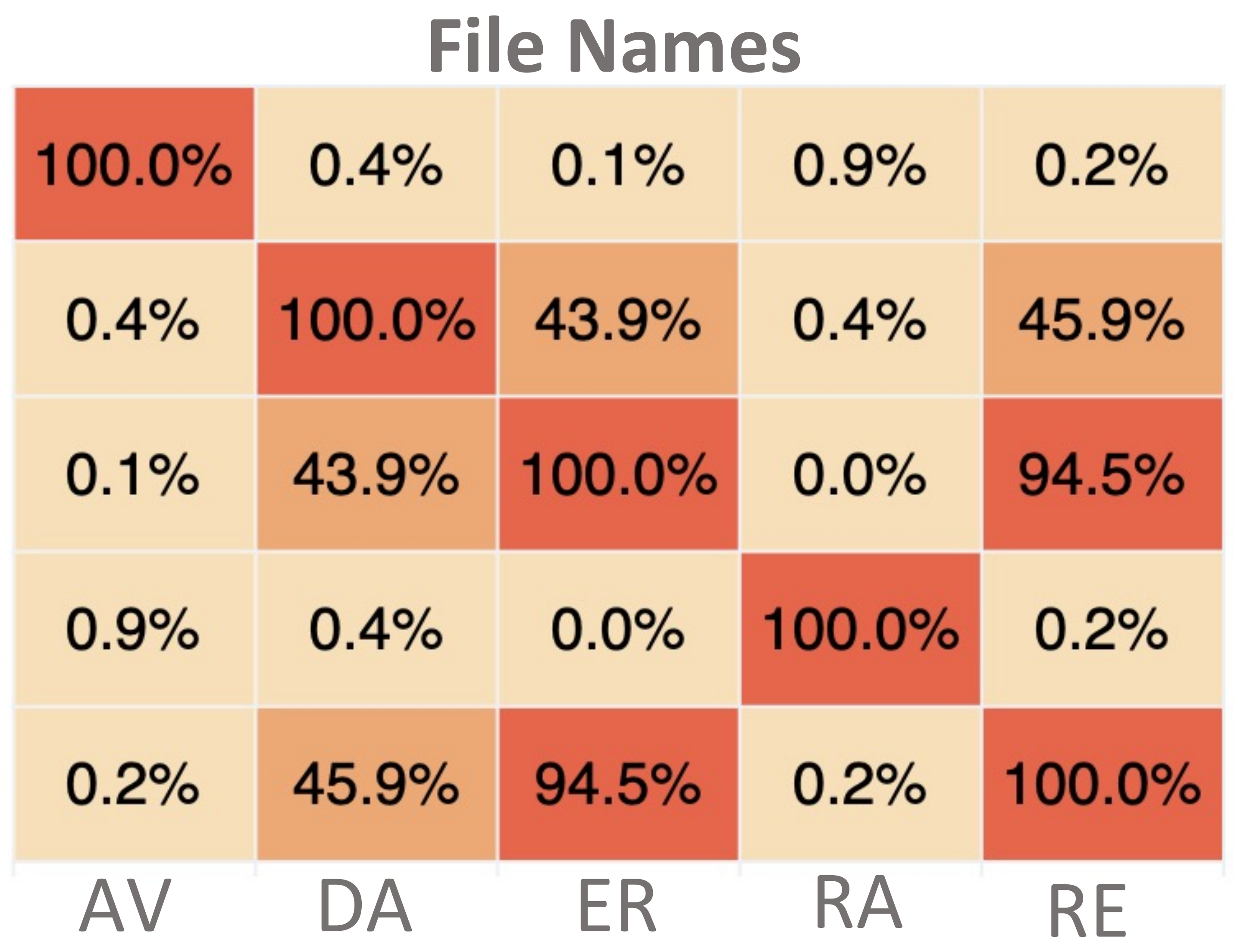
System calls

	AV	DA	ER	RA	RE
AV	100.0%	16.6%	50.7%	89.1%	90.6%
DA	16.6%	100.0%	53.2%	54.7%	21.8%
ER	50.7%	53.2%	100.0%	64.0%	62.4%
RA	89.1%	54.7%	64.0%	100.0%	81.9%
RE	90.6%	21.8%	62.4%	81.9%	100.0%



File Extensions

	AV	DA	ER	RA	RE
AV	100.0%	60.0%	16.5%	75.9%	54.7%
DA	60.0%	100.0%	8.6%	79.9%	42.4%
ER	16.5%	8.6%	100.0%	15.1%	42.8%
RA	75.9%	79.9%	15.1%	100.0%	60.2%
RE	54.7%	42.4%	42.8%	60.2%	100.0%



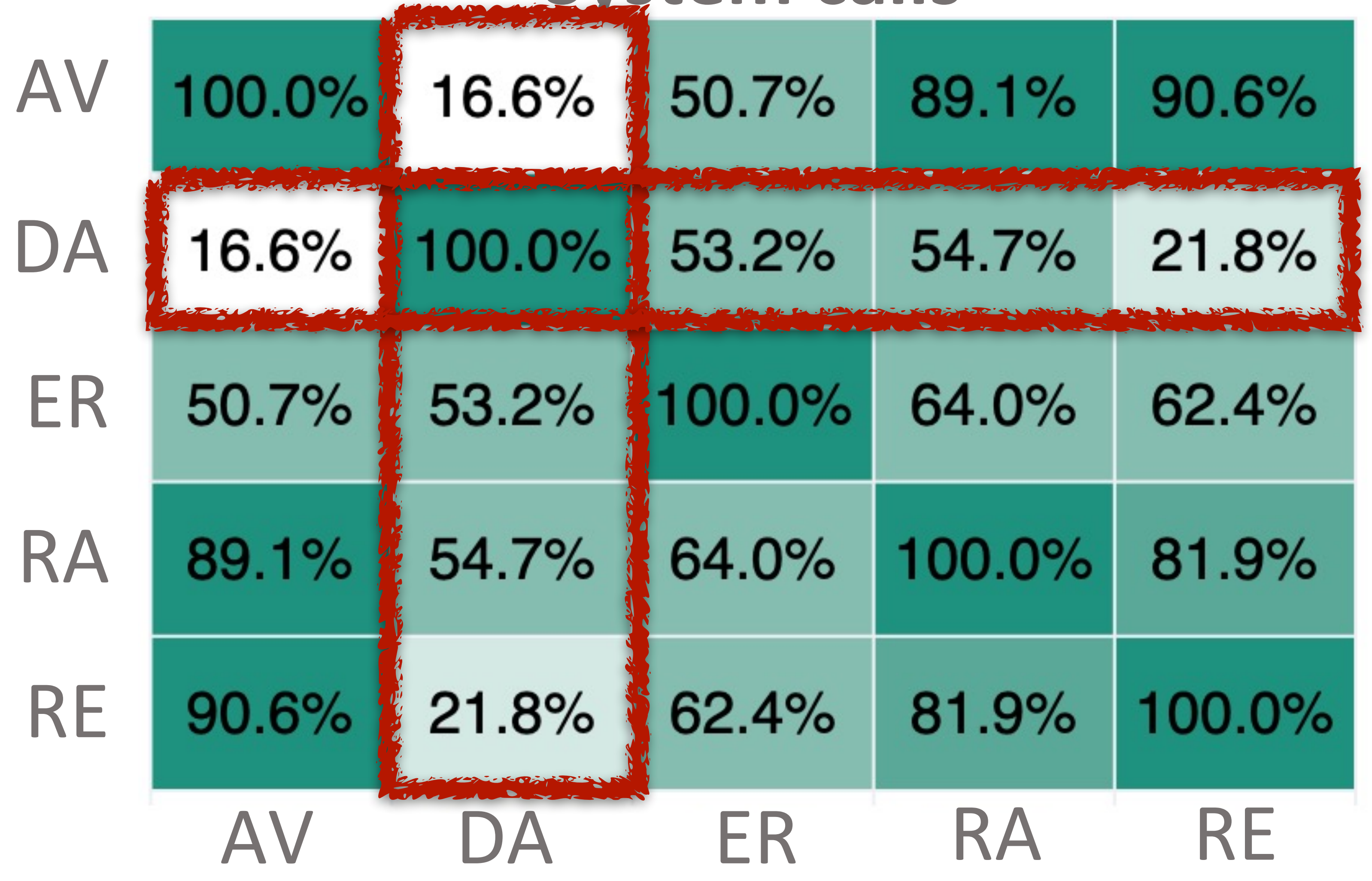
File Names

	AV	DA	ER	RA	RE
AV	100.0%	0.4%	0.1%	0.9%	0.2%
DA	0.4%	100.0%	43.9%	0.4%	45.9%
ER	0.1%	43.9%	100.0%	0.0%	94.5%
RA	0.9%	0.4%	0.0%	100.0%	0.2%
RE	0.2%	45.9%	94.5%	0.2%	100.0%

AV – avoslocker, DA – darkside, ER – erebus, RA – ransomexx, RE - revil

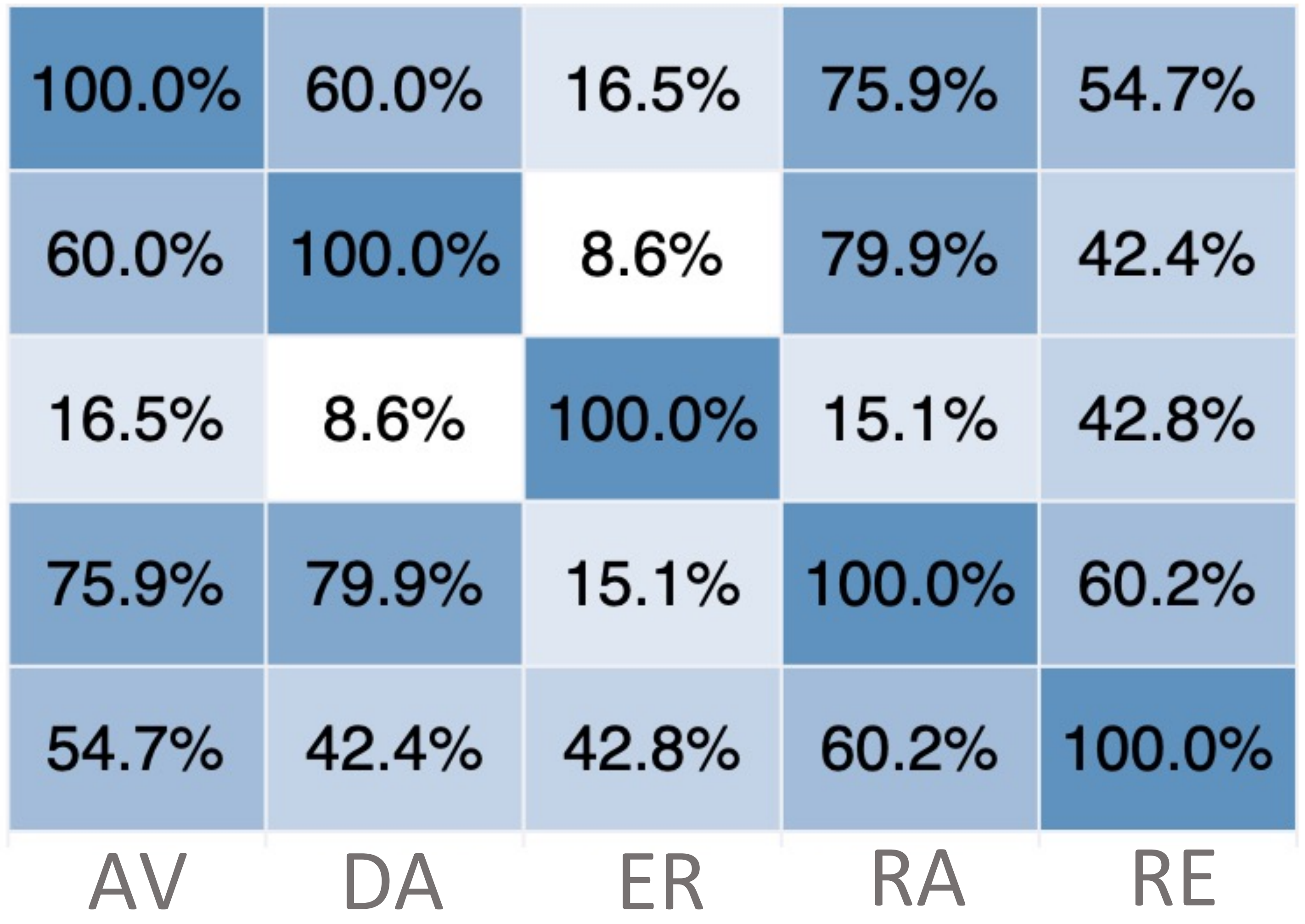
Linux Ransomware Study

Families Similarity



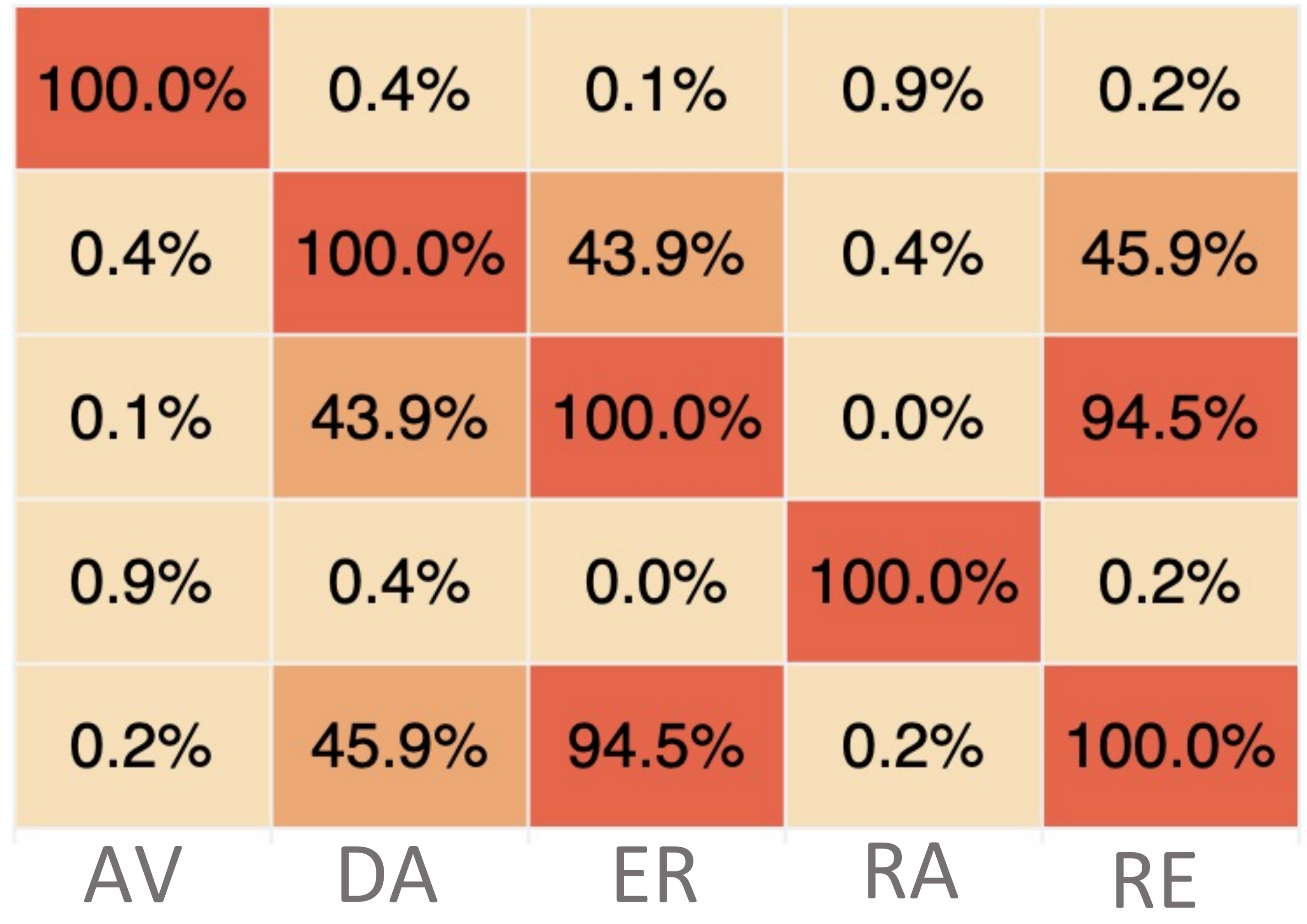
System calls

	AV	DA	ER	RA	RE
AV	100.0%	16.6%	50.7%	89.1%	90.6%
DA	16.6%	100.0%	53.2%	54.7%	21.8%
ER	50.7%	53.2%	100.0%	64.0%	62.4%
RA	89.1%	54.7%	64.0%	100.0%	81.9%
RE	90.6%	21.8%	62.4%	81.9%	100.0%



File Extensions

	AV	DA	ER	RA	RE
AV	100.0%	60.0%	16.5%	75.9%	54.7%
DA	60.0%	100.0%	8.6%	79.9%	42.4%
ER	16.5%	8.6%	100.0%	15.1%	42.8%
RA	75.9%	79.9%	15.1%	100.0%	60.2%
RE	54.7%	42.4%	42.8%	60.2%	100.0%



File Names

	AV	DA	ER	RA	RE
AV	100.0%	0.4%	0.1%	0.9%	0.2%
DA	0.4%	100.0%	43.9%	0.4%	45.9%
ER	0.1%	43.9%	100.0%	0.0%	94.5%
RA	0.9%	0.4%	0.0%	100.0%	0.2%
RE	0.2%	45.9%	94.5%	0.2%	100.0%

AV – avoslocker, DA – darkside, ER – erebus, RA – ransomexx, RE - revil

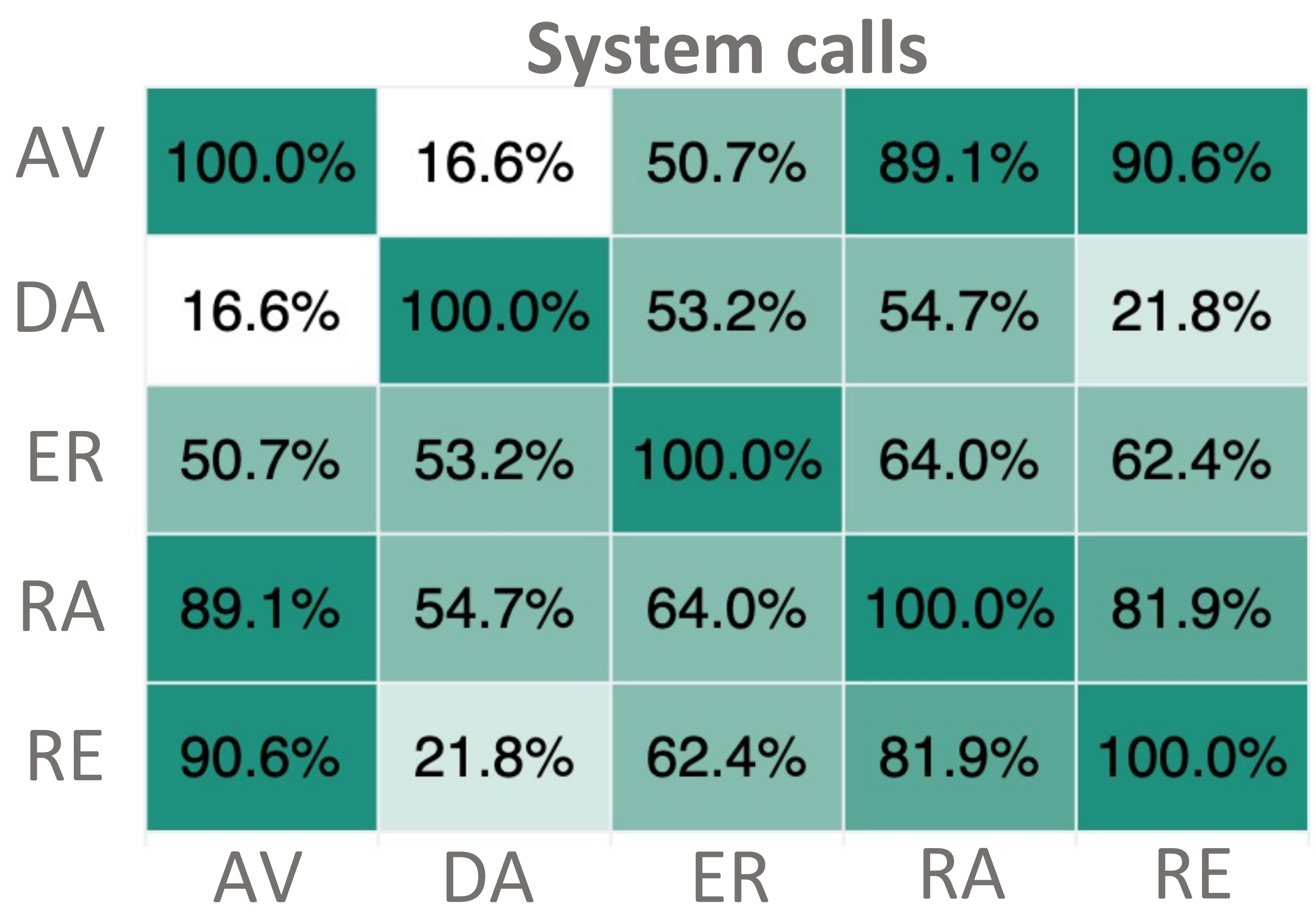
System calls

DARKSIDE is the most dissimilar.

DARKSIDE uses more system call types, including network-related.

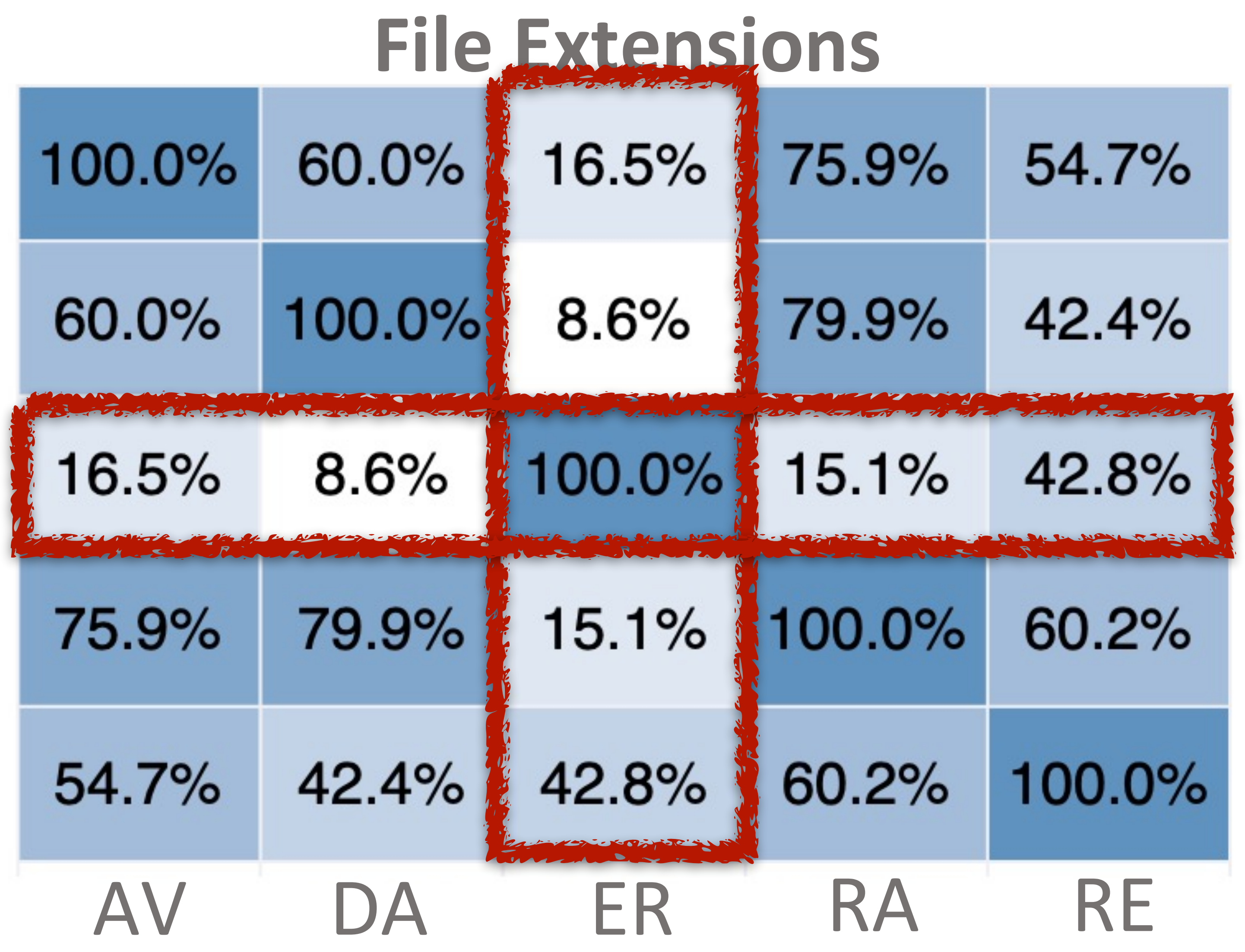
Linux Ransomware Study

Families Similarity



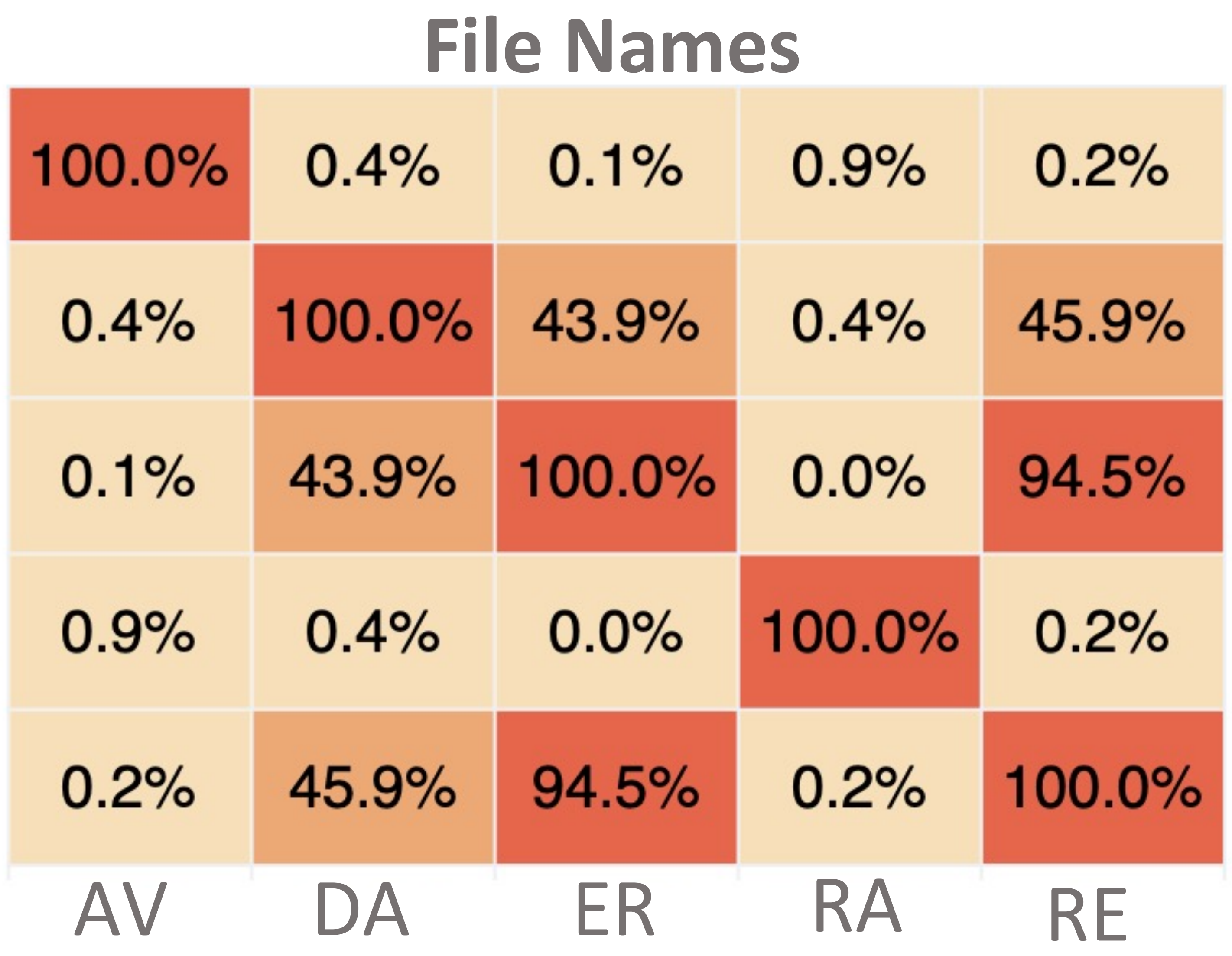
System calls

	AV	DA	ER	RA	RE
AV	100.0%	16.6%	50.7%	89.1%	90.6%
DA	16.6%	100.0%	53.2%	54.7%	21.8%
ER	50.7%	53.2%	100.0%	64.0%	62.4%
RA	89.1%	54.7%	64.0%	100.0%	81.9%
RE	90.6%	21.8%	62.4%	81.9%	100.0%



File Extensions

	AV	DA	ER	RA	RE
AV	100.0%	60.0%	16.5%	75.9%	54.7%
DA	60.0%	100.0%	8.6%	79.9%	42.4%
ER	16.5%	8.6%	100.0%	15.1%	42.8%
RA	75.9%	79.9%	15.1%	100.0%	60.2%
RE	54.7%	42.4%	42.8%	60.2%	100.0%



File Names

	AV	DA	ER	RA	RE
AV	100.0%	0.4%	0.1%	0.9%	0.2%
DA	0.4%	100.0%	43.9%	0.4%	45.9%
ER	0.1%	43.9%	100.0%	0.0%	94.5%
RA	0.9%	0.4%	0.0%	100.0%	0.2%
RE	0.2%	45.9%	94.5%	0.2%	100.0%

AV – avoslocker, DA – darkside, ER – erebus, RA – ransomexx, RE - revil

<u>System calls</u>

DarkSide is the most dissimilar.

DarkSide uses more system call types, including network-related.

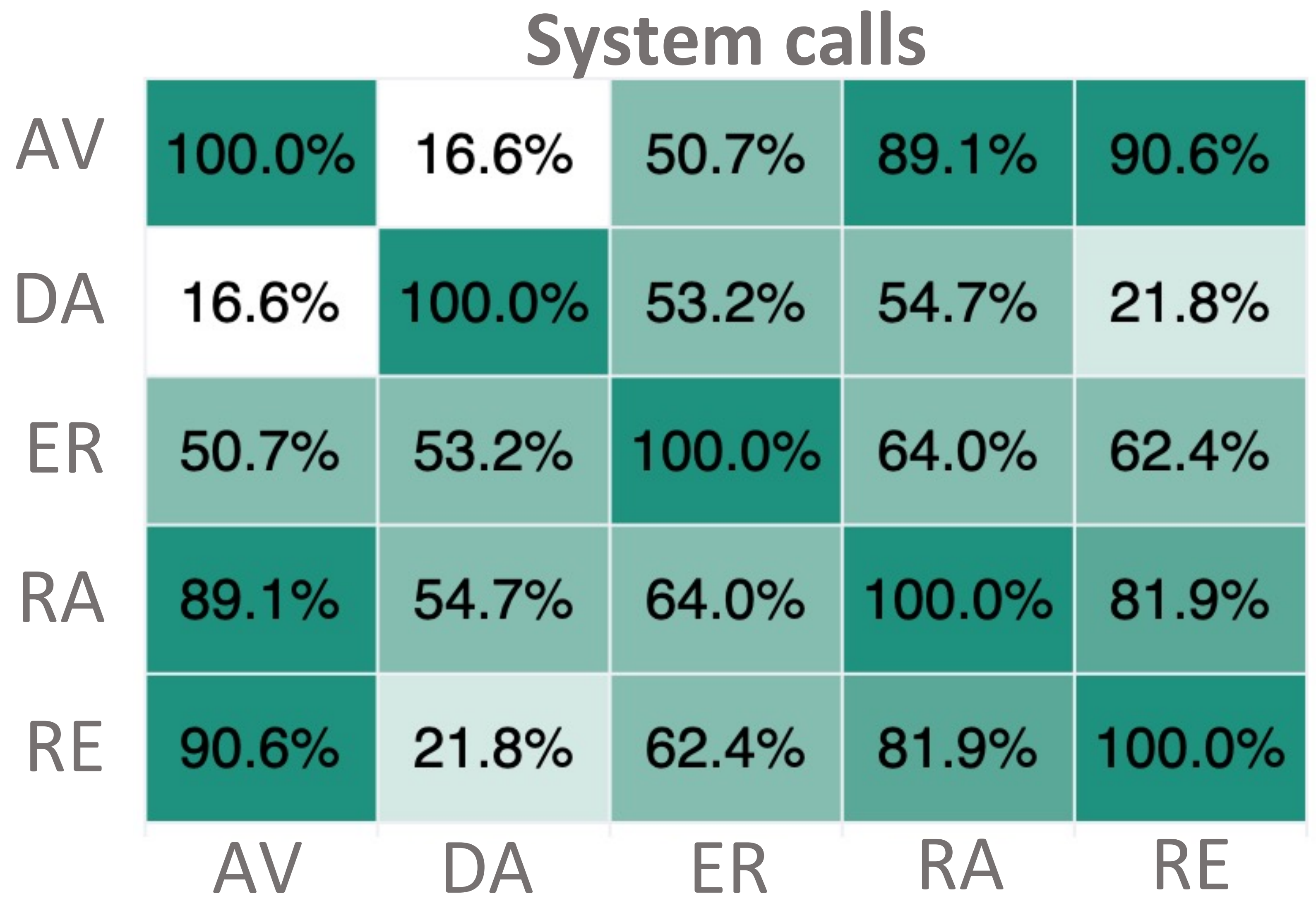
<u>File extensions</u>

Erebus is the most dissimilar.

Erebus encrypts files only after adding the .ecrypt extension.

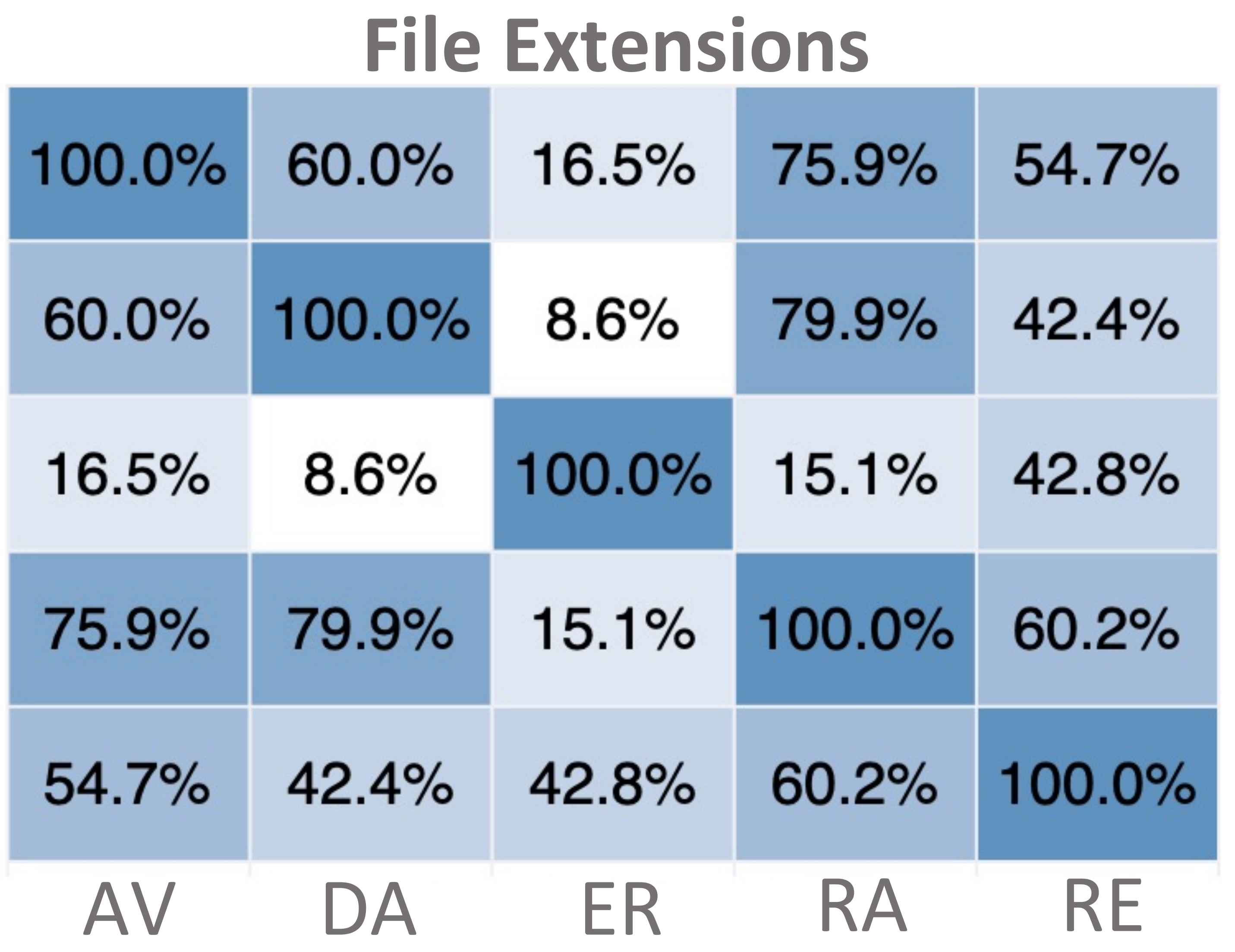
Linux Ransomware Study

Families Similarity



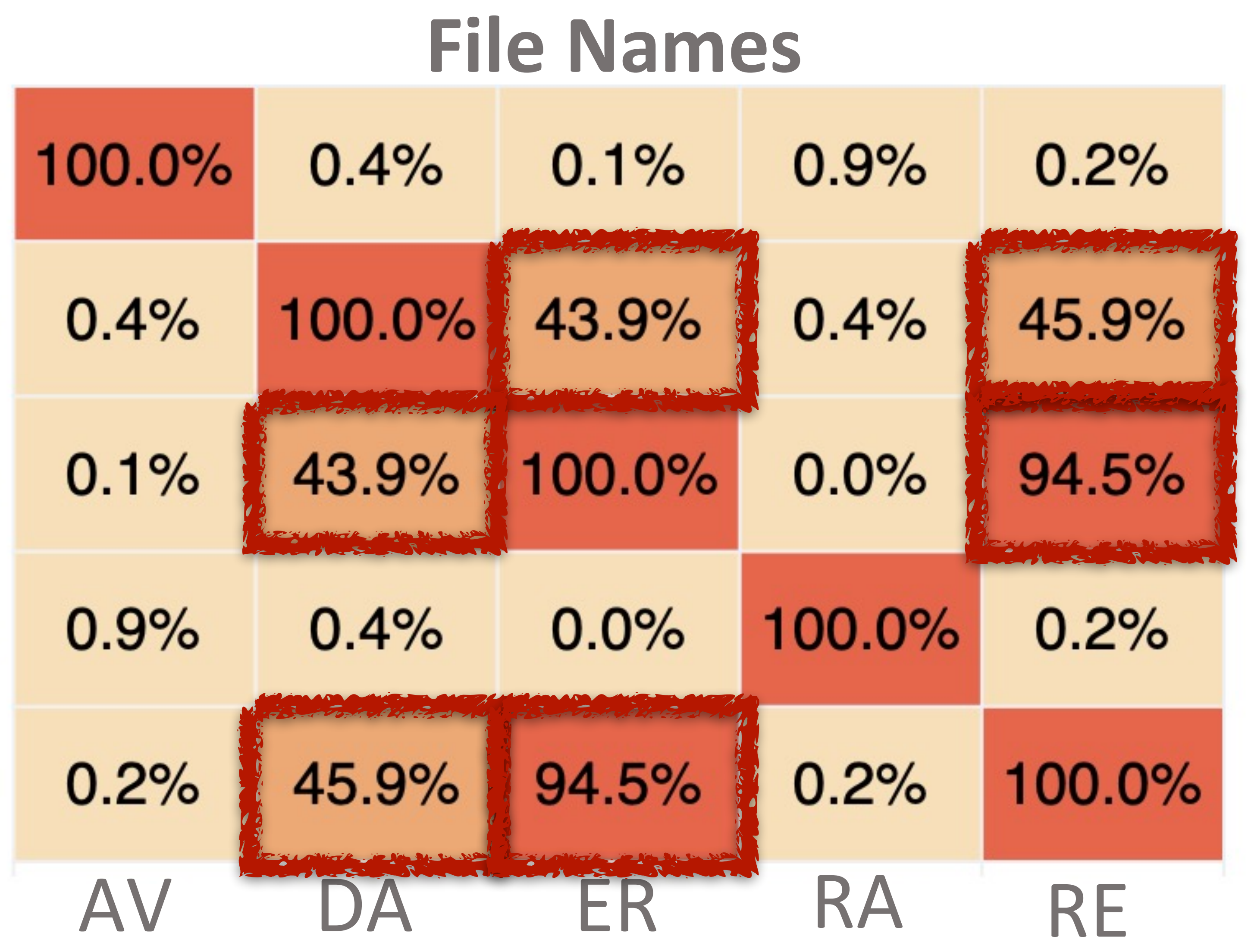
System calls

	AV	DA	ER	RA	RE
AV	100.0%	16.6%	50.7%	89.1%	90.6%
DA	16.6%	100.0%	53.2%	54.7%	21.8%
ER	50.7%	53.2%	100.0%	64.0%	62.4%
RA	89.1%	54.7%	64.0%	100.0%	81.9%
RE	90.6%	21.8%	62.4%	81.9%	100.0%



File Extensions

	AV	DA	ER	RA	RE
AV	100.0%	60.0%	16.5%	75.9%	54.7%
DA	60.0%	100.0%	8.6%	79.9%	42.4%
ER	16.5%	8.6%	100.0%	15.1%	42.8%
RA	75.9%	79.9%	15.1%	100.0%	60.2%
RE	54.7%	42.4%	42.8%	60.2%	100.0%



File Names

	AV	DA	ER	RA	RE
AV	100.0%	0.4%	0.1%	0.9%	0.2%
DA	0.4%	100.0%	43.9%	0.4%	45.9%
ER	0.1%	43.9%	100.0%	0.0%	94.5%
RA	0.9%	0.4%	0.0%	100.0%	0.2%
RE	0.2%	45.9%	94.5%	0.2%	100.0%

AV – avoslocker, DA – darkside, ER – erebus, RA – ransomexx, RE - revil

<u>**System calls**</u>

DarkSide is the most dissimilar.

DarkSide uses more system call types, including network-related.

<u>**File extensions**</u>

Erebus is the most dissimilar.

Erebus encrypts files only after adding the .ecrypt extension.

<u>**File names**</u>

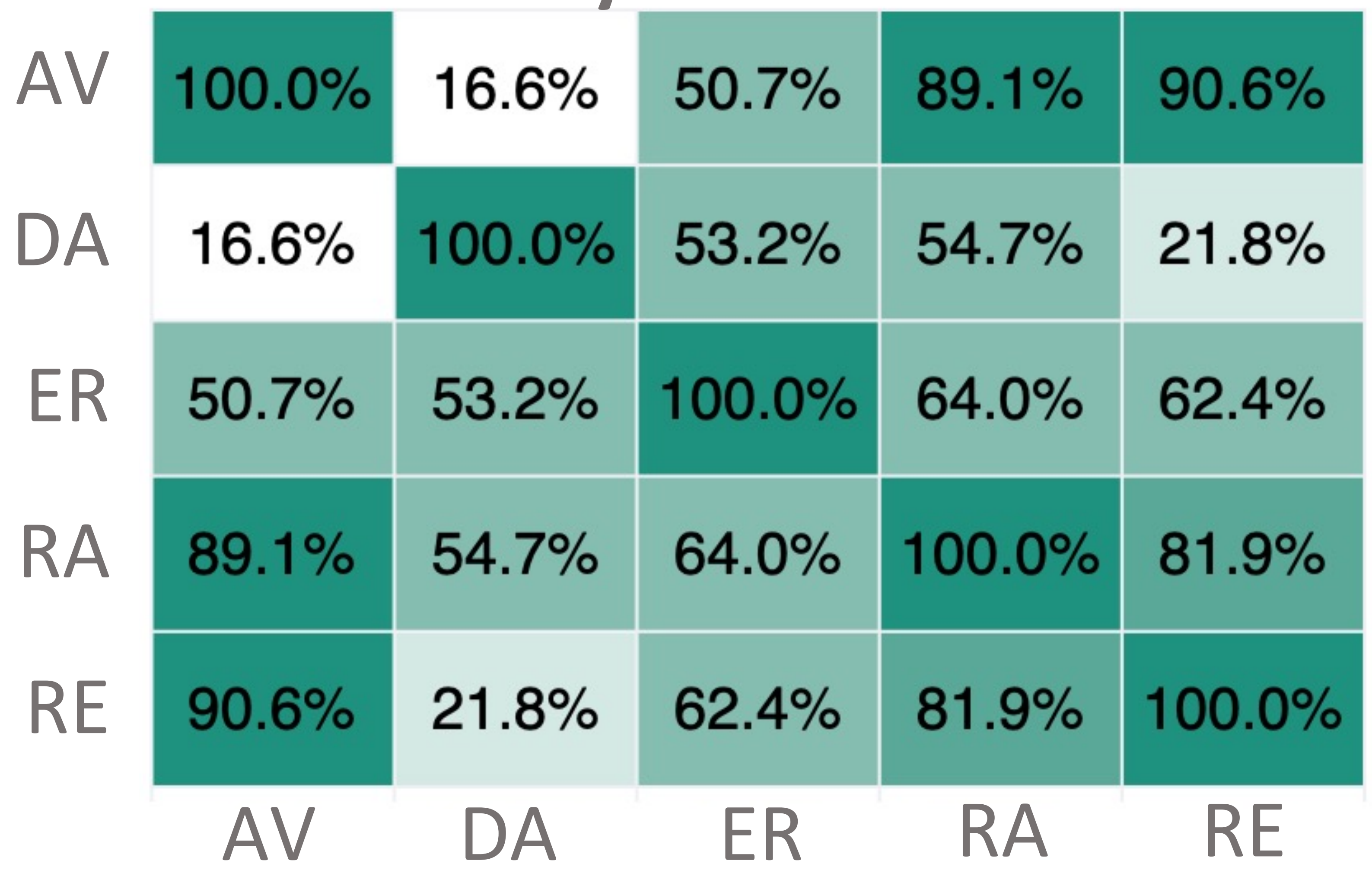
Families are very dissimilar.

Only REvil, Erebus and DarkSide share similarities due to their access to /dev/urandom.

Linux Ransomware Study

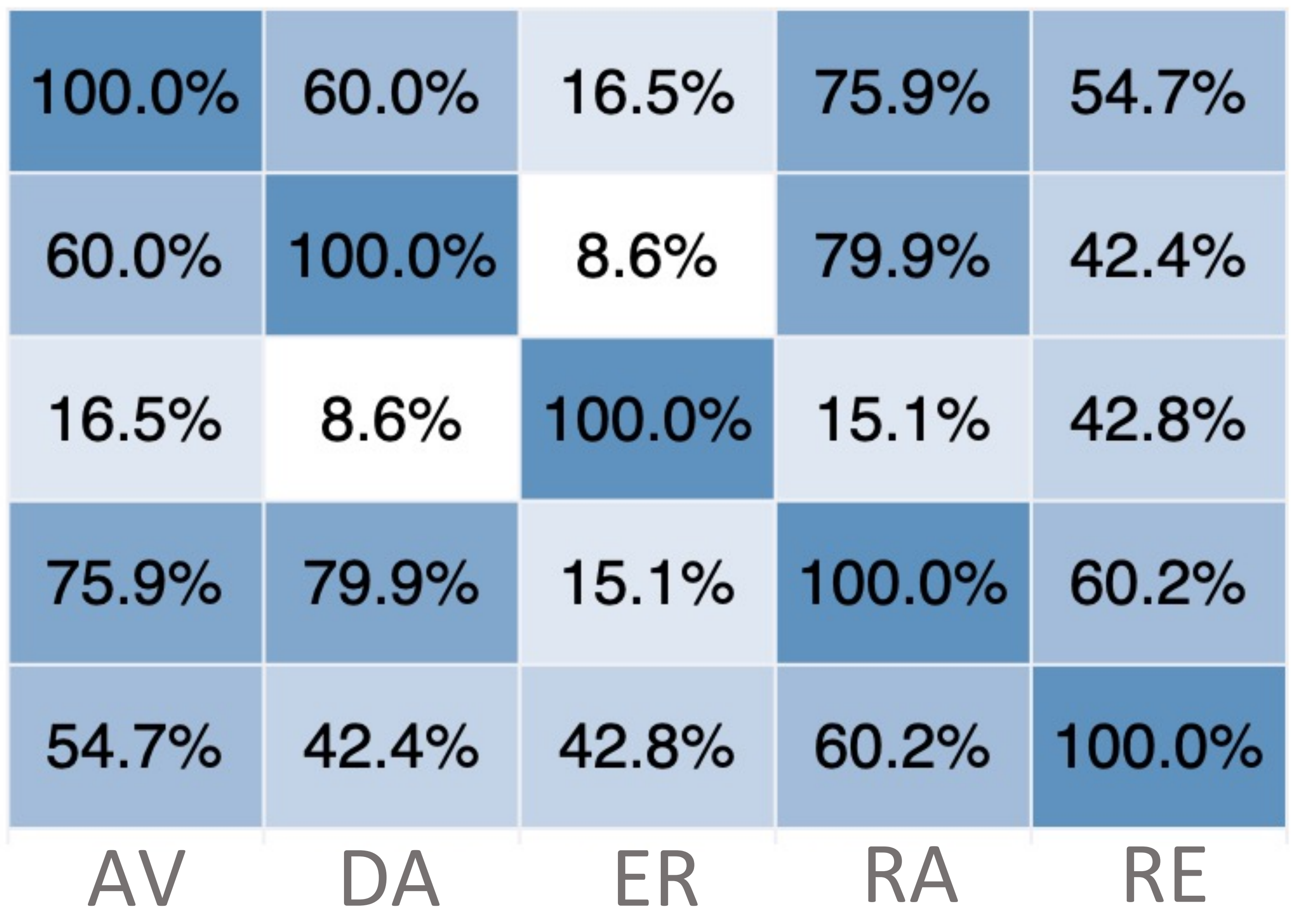
Families Similarity

System calls



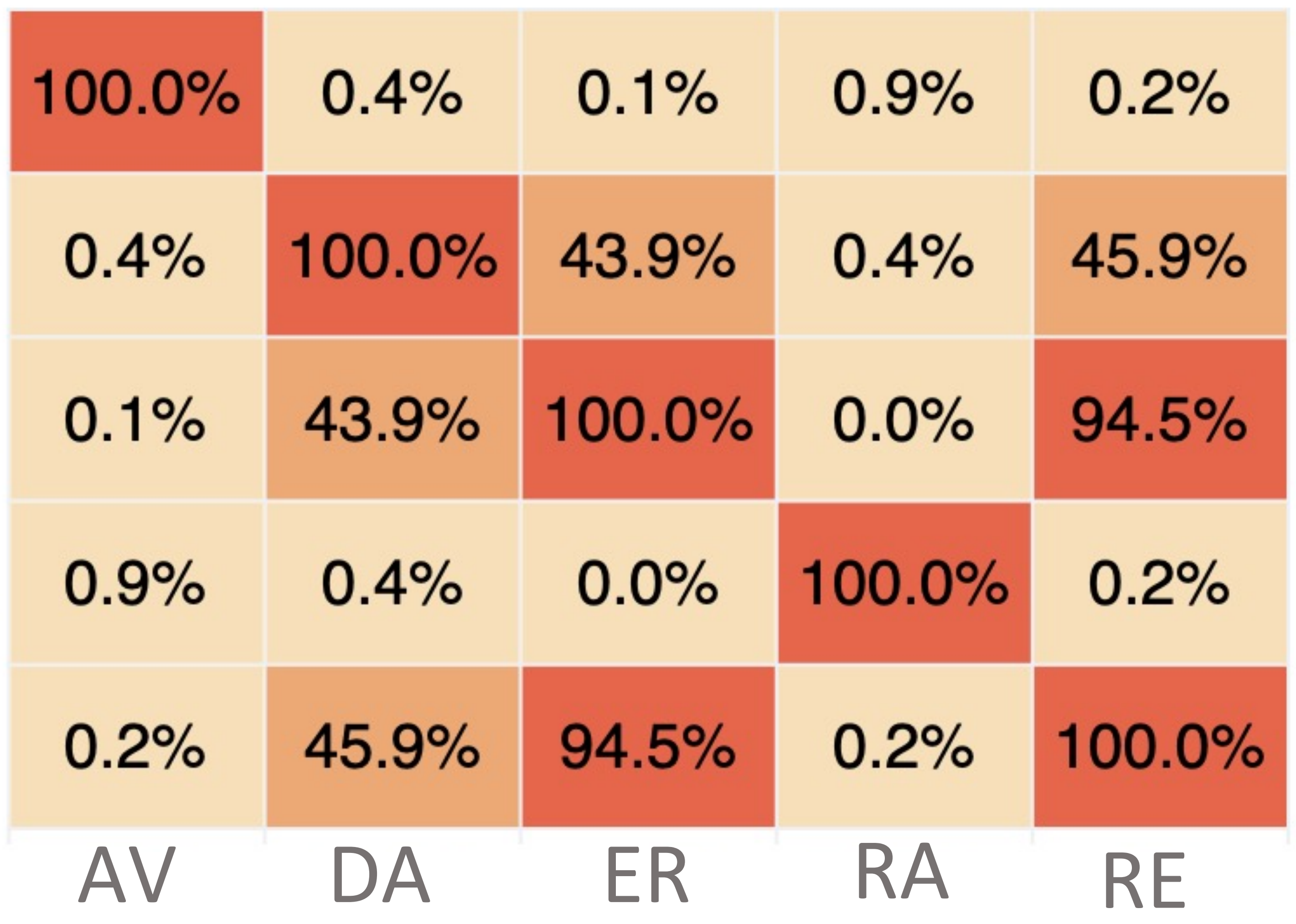
	AV	DA	ER	RA	RE
AV	100.0%	16.6%	50.7%	89.1%	90.6%
DA	16.6%	100.0%	53.2%	54.7%	21.8%
ER	50.7%	53.2%	100.0%	64.0%	62.4%
RA	89.1%	54.7%	64.0%	100.0%	81.9%
RE	90.6%	21.8%	62.4%	81.9%	100.0%

File Extensions



	AV	DA	ER	RA	RE
AV	100.0%	60.0%	16.5%	75.9%	54.7%
DA	60.0%	100.0%	8.6%	79.9%	42.4%
ER	16.5%	8.6%	100.0%	15.1%	42.8%
RA	75.9%	79.9%	15.1%	100.0%	60.2%
RE	54.7%	42.4%	42.8%	60.2%	100.0%

File Names



	AV	DA	ER	RA	RE
AV	100.0%	0.4%	0.1%	0.9%	0.2%
DA	0.4%	100.0%	43.9%	0.4%	45.9%
ER	0.1%	43.9%	100.0%	0.0%	94.5%
RA	0.9%	0.4%	0.0%	100.0%	0.2%
RE	0.2%	45.9%	94.5%	0.2%	100.0%

AV – avoslocker, DA – darkside, ER – erebus, RA – ransomexx, RE - revil

System calls

DARKSIDE is the most dissimilar.

DARKSIDE uses more system call types, including network-related.

File extensions

EREBUS is the most dissimilar.

EREBUS encrypts files only after adding the .ecrypt extension.

File names

Families are very dissimilar.

Only REVIL, EREBUS and DARKSIDE share similarities due to their access to /dev/urandom.

Different features must be considered for a clear understanding of ransomware's intrinsic behavior!

Conclusion

- Through a transparent, practical and automated analysis pipeline, CRIBA allows:
  - Automating the analysis of ransomware families.
  - Understanding complex and intrinsic behavior of ransomware samples.
  - Pinpointing common and distinct traits across families.
- The knowledge provided by CRIBA is key for building and improving detection tools for Linux cryptographic ransomware.

CRIBA: A Tool for Comprehensive Analysis of Cryptographic Ransomware's I/O Behavior

- CRIBA is publicly available at:
  - **Github**: github.com/dsrhaslab/criba
  - **Contact**: tania.c.araujo@inesctec.pt