BVRIT HYDERABAD College of Engineering for Women

Department Of Information Technology

Ransomware Protection by Adopting Camouflage and Hiding Strategy

Under the guidance of:
Ms. M. Sudha Rani
Assistant Professor

By:
R. Hyndhavi Reddy
21WH1A12A4

CONTENTS

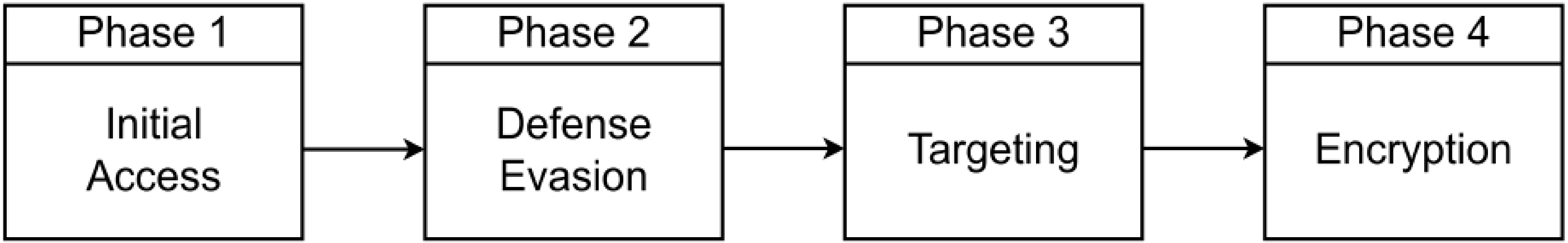
- Abstract
- Introduction
- Existing Methods
- Present Method
- Performance Metrics
- Conclusion
- References

ABSTRACT

To minimize ransomware damage, a proactive defense approach conceals critical files, making them harder for ransomware to locate and encrypt. This technique employs link files and an encrypted database, combined with a linker mechanism to limit the attack surface. By hiding actual file paths, it balances security with user accessibility, allowing legitimate users seamless access while obstructing ransomware’s ability to target important files. The approach has proven effective and cost-efficient, providing resilient protection for essential data even if ransomware infiltrates the system. Rather than relying solely on detection, this strategy emphasizes impact reduction by focusing on preventive file obfuscation techniques. By limiting file visibility to ransomware, it minimizes damage and ensures high-value data remains safeguarded, creating a robust defense against evolving ransomware threats.

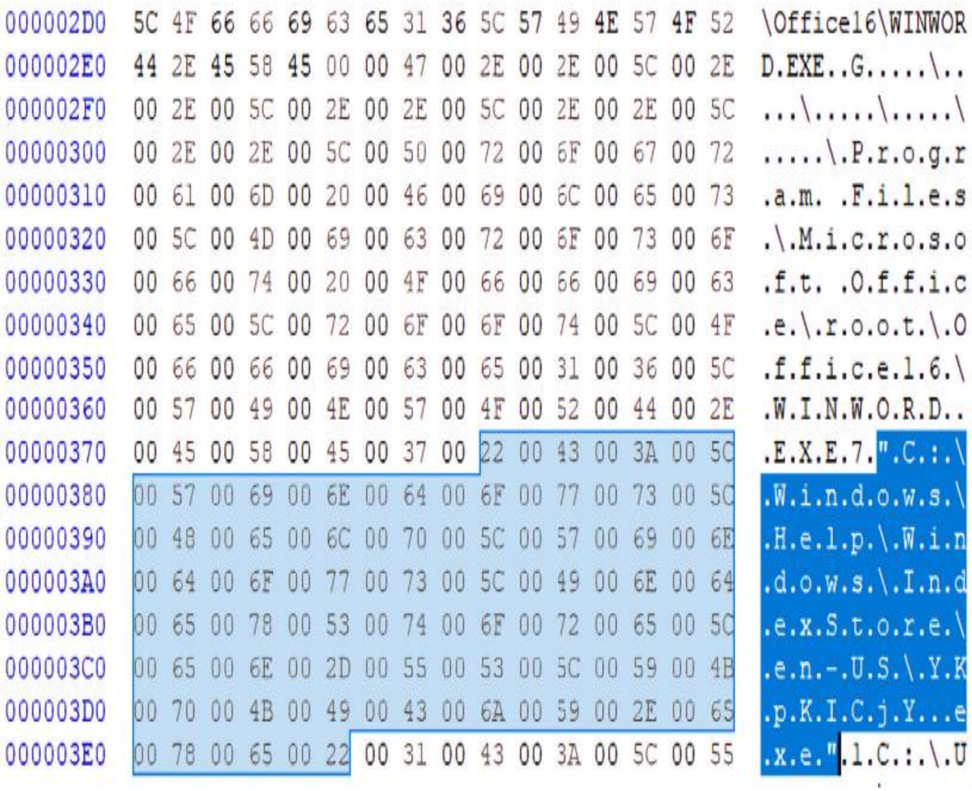
INTRODUCTION

- Ransomware attacks surged in 2022, increasing by nearly 13%, causing data loss, financial damage, and reputational harm.
- Ransomware-as-a-service (RaaS) allows even non-technical criminals to deploy ransomware using user-friendly platforms.
- A proactive, camouflage-based method aims to minimize ransomware damage by hiding critical files, making it difficult for attackers to locate and access them, even with advanced evasion tactics like polymorphism and obfuscation.



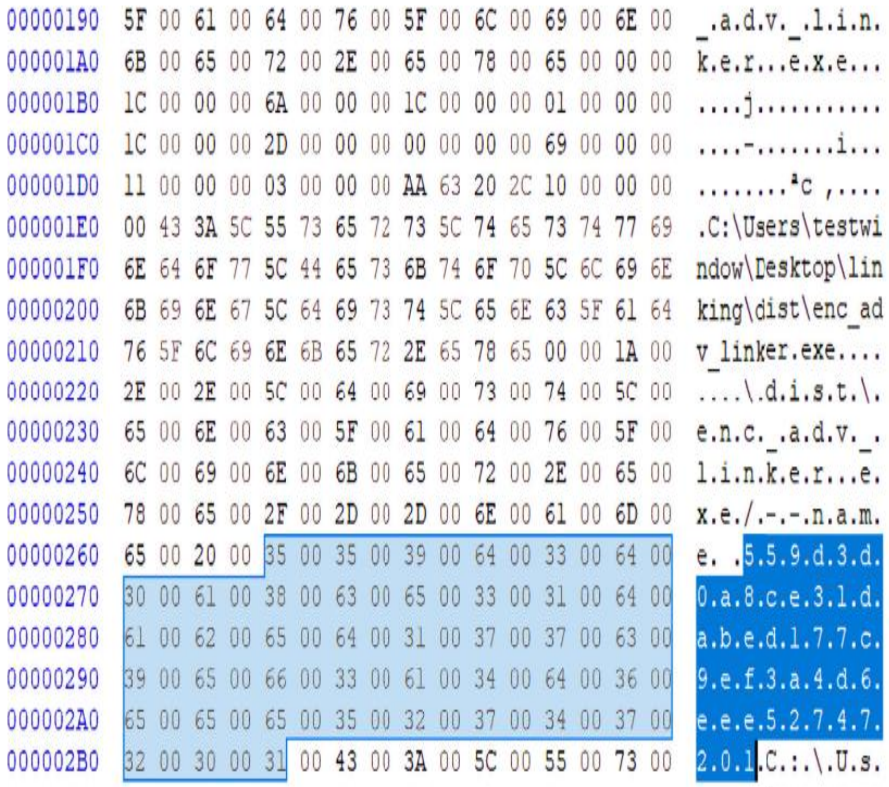
Main phases of the ransomware execution process

INTRODUCTION



```
000002D0  5C 4F 66 66 69 63 65 31 36 5C 57 49 4E 57 4F 52  \Office16\WINWOR
000002E0  44 2E 45 58 45 00 00 47 00 2E 00 2E 00 5C 00 2E  D.EXE..G.....\..
000002F0  00 2E 00 5C 00 2E 00 2E 00 5C 00 2E 00 2E 00 5C  ...\.....\.....\
00000300  00 2E 00 2E 00 5C 00 50 00 72 00 6F 00 67 00 72  .....\.P.r.o.g.r
00000310  00 61 00 6D 00 20 00 46 00 69 00 6C 00 65 00 73  .a.m. .F.i.l.e.s
00000320  00 5C 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F  .\.M.i.c.r.o.s.o
00000330  00 66 00 74 00 20 00 4F 00 66 00 66 00 69 00 63  .f.t. .O.f.f.i.c
00000340  00 65 00 5C 00 72 00 6F 00 6F 00 74 00 5C 00 4F  .e.\.r.o.o.t.\.O
00000350  00 66 00 66 00 69 00 63 00 65 00 31 00 36 00 5C  .f.f.i.c.e.1.6.\
00000360  00 57 00 49 00 4E 00 57 00 4F 00 52 00 44 00 2E  .W.I.N.W.O.R.D..
00000370  00 45 00 58 00 45 00 37 00 22 00 43 00 3A 00 5C  .E.X.E.7.".C.:.\
00000380  00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C  .W.i.n.d.o.w.s.\
00000390  00 48 00 65 00 6C 00 70 00 5C 00 57 00 69 00 6E  .H.e.l.p.\.W.i.n
000003A0  00 64 00 6F 00 77 00 73 00 5C 00 49 00 6E 00 64  .d.o.w.s.\.I.n.d
000003B0  00 65 00 78 00 53 00 74 00 6F 00 72 00 65 00 5C  .e.x.S.t.o.r.e.\
000003C0  00 65 00 6E 00 2D 00 55 00 53 00 5C 00 59 00 4B  .e.n.-.U.S.\.Y.K
000003D0  00 70 00 4B 00 49 00 43 00 6A 00 59 00 2E 00 65  .p.K.I.C.j.Y...e
000003E0  00 78 00 65 00 22 00 31 00 43 00 3A 00 5C 00 55  .x.e.".1.C.:.\.U
```

(a) Previous method (a hidden file path is revealed)



```
00000190  5F 00 61 00 64 00 76 00 5F 00 6C 00 69 00 6E 00  _.a.d.v._.l.i.n.
000001A0  6B 00 65 00 72 00 2E 00 65 00 78 00 65 00 00 00  k.e.r...e.x.e...
000001B0  1C 00 00 00 6A 00 00 00 1C 00 00 00 01 00 00 00  ....j...........
000001C0  1C 00 00 00 2D 00 00 00 00 00 00 00 69 00 00 00  ....-.......i...
000001D0  11 00 00 00 03 00 00 00 AA 63 20 2C 10 00 00 00  ........ªc ,....
000001E0  00 43 3A 5C 55 73 65 72 73 5C 74 65 73 74 77 69  .C:\Users\testwi
000001F0  6E 64 6F 77 5C 44 65 73 6B 74 6F 70 5C 6C 69 6E  ndow\Desktop\lin
00000200  6B 69 6E 67 5C 64 69 73 74 5C 65 6E 63 5F 61 64  king\dist\enc_ad
00000210  76 5F 6C 69 6E 6B 65 72 2E 65 78 65 00 00 1A 00  v_linker.exe....
00000220  2E 00 2E 00 5C 00 64 00 69 00 73 00 74 00 5C 00  ....\.d.i.s.t.\.
00000230  65 00 6E 00 63 00 5F 00 61 00 64 00 76 00 5F 00  e.n.c._.a.d.v._.
00000240  6C 00 69 00 6E 00 6B 00 65 00 72 00 2E 00 65 00  l.i.n.k.e.r...e.
00000250  78 00 65 00 2F 00 2D 00 2D 00 6E 00 61 00 6D 00  x.e./.-.-.n.a.m.
00000260  65 00 20 00 35 00 35 00 39 00 64 00 33 00 64 00  e. .5.5.9.d.3.d.
00000270  30 00 61 00 38 00 63 00 65 00 33 00 31 00 64 00  0.a.8.c.e.3.1.d.
00000280  61 00 62 00 65 00 64 00 31 00 37 00 37 00 63 00  a.b.e.d.1.7.7.c.
00000290  39 00 65 00 66 00 33 00 61 00 34 00 64 00 36 00  9.e.f.3.a.4.d.6.
000002A0  65 00 65 00 65 00 35 00 32 00 37 00 34 00 37 00  e.e.e.5.2.7.4.7.
000002B0  32 00 30 00 31 00 43 00 3A 00 5C 00 55 00 73 00  2.0.1.C.:.\.U.s.
```

(b) Secure version (a hidden file path is not revealed)

EXISTING METHOS

- **Signature-Based Detection**: Identifies known ransomware patterns but struggles with new or unknown variants.
- **Static Analysis**: Analyzes file structure for suspicious code but is limited by evasion techniques like obfuscation.
- **Dynamic Analysis**: Observes program behavior in a sandbox environment, though advanced ransomware may alter its behavior to evade detection.
- **Behavior-Based Detection**: Monitors system activity for typical ransomware behaviors but may fail if the malware halts monitoring or encrypts files quickly.
- **Decoy Files**: Deploys honey files to detect ransomware access, though advanced versions may bypass them.

LIMITATIONS IN EXISTING METHODS

- Bypass of Behavior-Based Detection
- Disruption of Real-Time Monitoring
- Ineffectiveness of Signature-Based and Static Analysis
- Difficulty Detecting New or Unknown Ransomware
- Recognition and Avoidance of Decoy Files

PRESENT METHOD

Camouflage and Hiding of Files:

- Critical files are camouflaged by changing extensions and moving them to directories that ransomware typically avoids.

Link File Creation for Accessibility:

- Link files are created in accessible directories, allowing users to access hidden files without revealing actual paths.

Encrypted Database for Security:

- An encrypted database stores mappings between original and hidden file paths, using a Hash Table and Mapping Table for secure reference.

Linker Function:

- The Linker function retrieves hidden paths from the database, ensuring files open with the correct application.

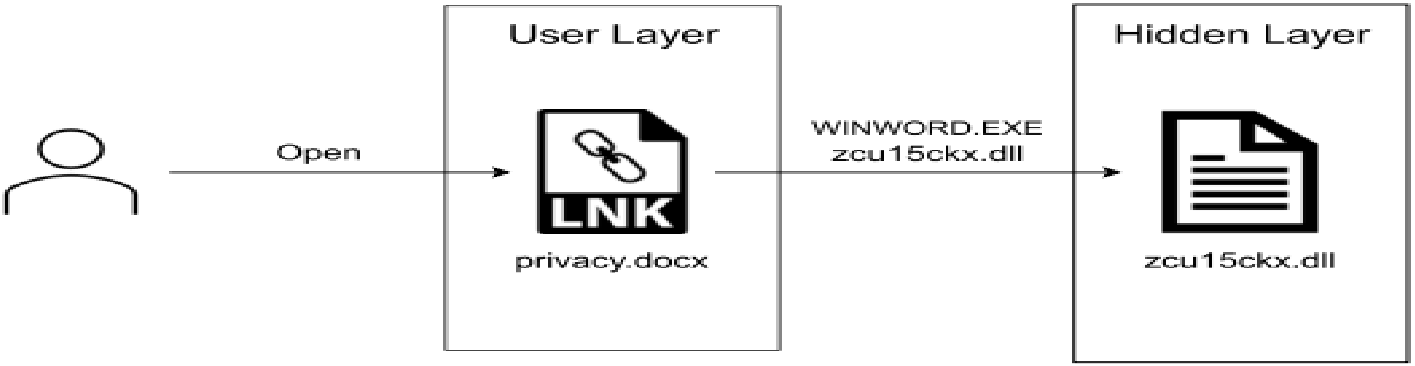
PRESENT METHOD

File Recovery Process:

- If files need to be restored to their original locations, the Mapping Table allows for easy recovery, moving files back to their user-accessible paths as needed.

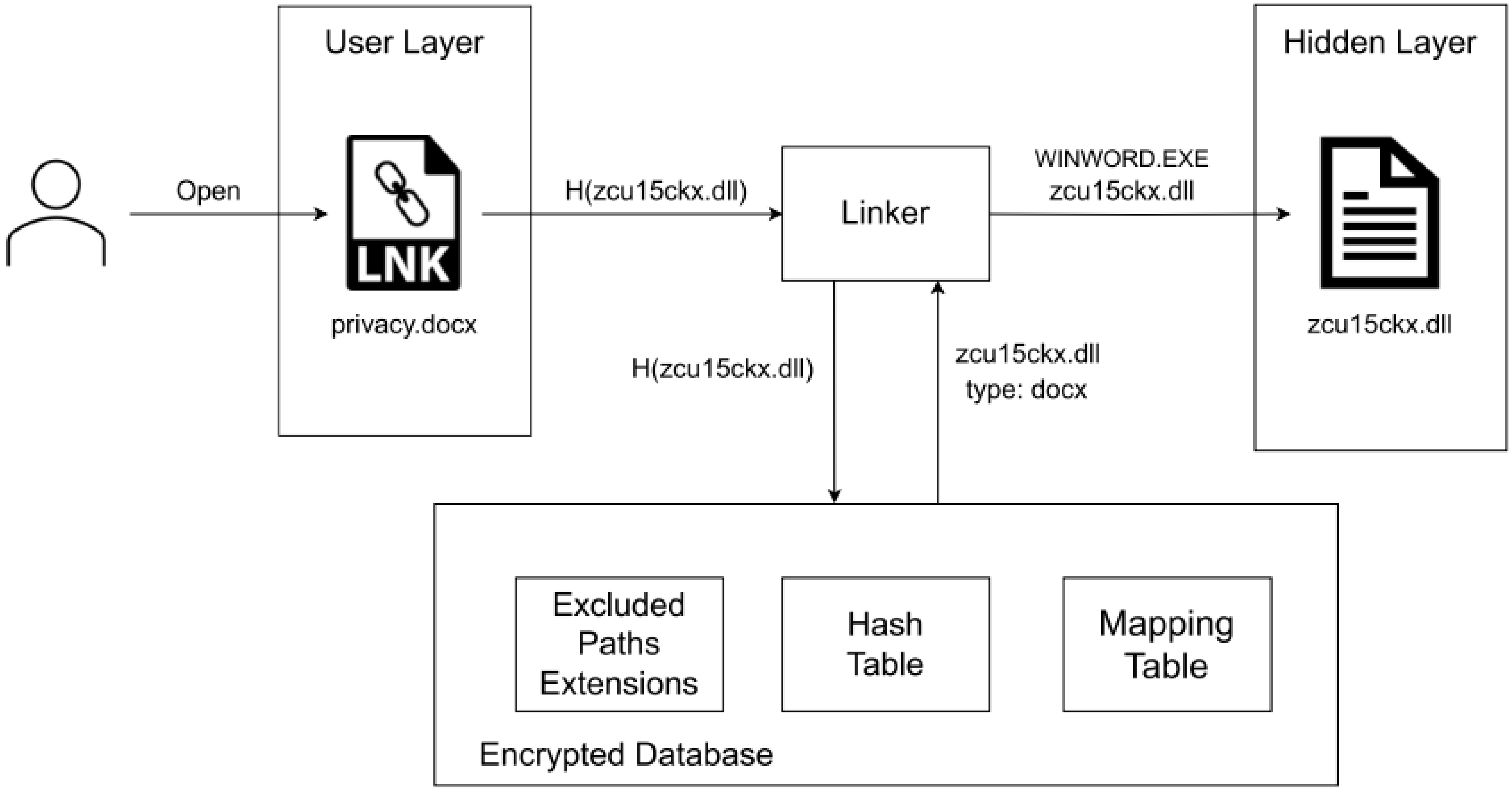
Enhanced Security against Advanced Attackers:

- Hashed references and encryption prevent attackers from easily uncovering hidden files, even if they access link files or system components.



The proposed method of linking the user layer to a hidden layer.

PRESENT METHOD



A secure version of the proposed method considering an advanced attacker.

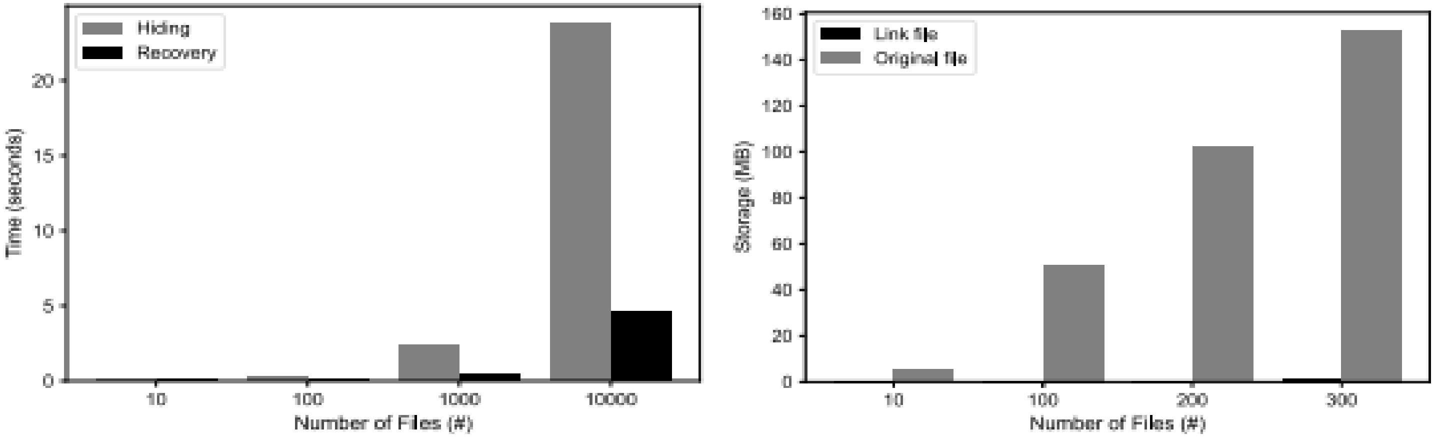
DATASETS USED

Ransomware Family	Ransomware Type	Key Characteristics	Success of Camouflage Method	Notes on Specific Evasion Techniques
LockBit	Ransomware-as-a-Service	Fast encryption, avoids system files	Yes	Utilizes API unhooking to evade detection
BlackCat/ALPHV	Double-extortion	Encrypts critical and sensitive data	Yes	Known for targeting backups
CLOP	Targeted ransomware	Targets enterprise networks	Yes	Uses evasion techniques in Linux and Windows
DarkSide/BlackMatter	Double-extortion	Encrypts with partial file encryption	Yes	Custom encryption patterns

DATASETS USED

Ransomware Family	Ransomware Type	Key Characteristics	Success of Camouflage Method	Notes on Specific Evasion Techniques
AvosLocker	RaaS	Supports negotiation, data leaks	Yes	Targets organizations
Magniber	Targeted ransomware	Encrypted based on specific extensions	Yes	Avoids high-visibility encryption
Phobos	Standard ransomware	Targets smaller businesses and individuals	Partial	Limited evasion, focuses on accessible files
ONYX	Destructive ransomware	Targets larger files for destruction	Partial	Bypasses typical hiding spots

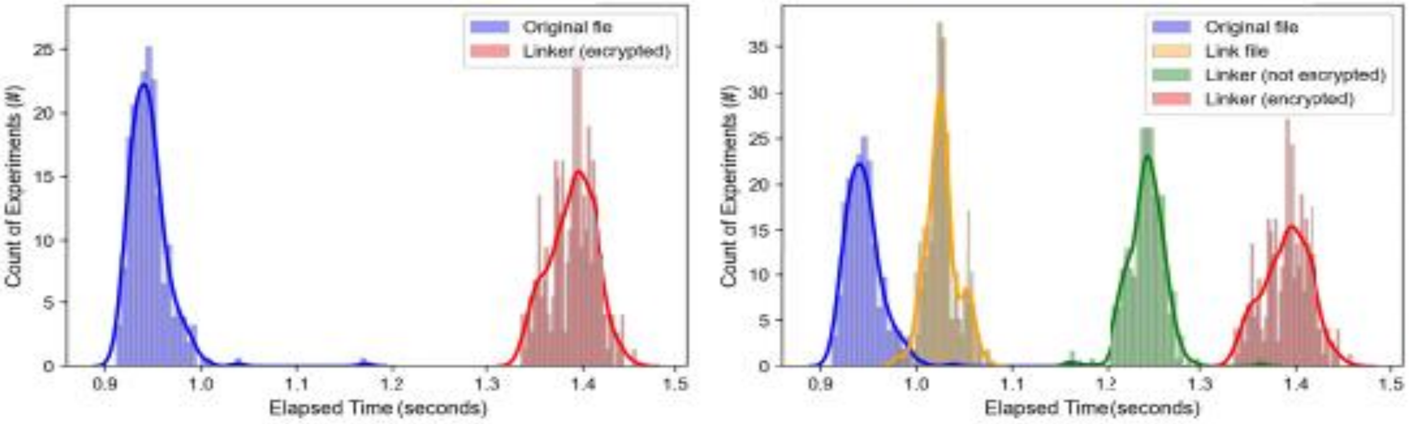
PERFORMANCE METRICS



(a) Hiding / Recovery time

(b) Size on disk

Time and storage required for hiding/recovering files based on the number of files



(a) General access and our approach

(b) Entire method

Comparison of file access time when applying the proposed method with general access.

BENEFITS

- Proactive Protection Against Ransomware
- Resilience to Evasion Tactics
- Reduces Dependence on Real-Time Detection
- Minimal System Impact
- Improved Security Through Encrypted Database
- Usability Through Link Files
- Cost-Effective and Simple to Implement
- Effective Against Various Ransomware Families

CONCLUSION

- The camouflage and hiding strategy effectively protects critical files from ransomware by making them difficult to locate and encrypt. Through file disguising, hidden directories, and an encrypted database with link files, this method provides proactive, low-cost protection without relying on traditional detection techniques. Experiments confirm its effectiveness across various ransomware types, balancing security with usability. This approach serves as a resilient secondary defense, reducing potential damage even when malware infiltrates the system.

.

REFERENCES

- Lee, S., Lee, S., Park, J., Kim, K., & Lee, K. (2023). **"Hiding in the Crowd: Ransomware Protection by Adopting Camouflage and Hiding Strategy With the Link File."** *IEEE Access*, *11*, 92693-92704. https://doi.org/10.1109/ACCESS.2023.3309879
- **Verizon Business**. (2022). *2022 Data Breach Investigations Report*. Accessed: 2023. [Online]. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
- **Alwashali, A. A. M. A., Rahman, N. A. A., & Ismail, N.** (2021). "A survey of ransomware as a service (RaaS) and methods to mitigate the attack." In *14th International Conference on Developments in eSystems Engineering (DeSE)*, Sharjah, UAE, 2021, pp. 92–96. https://doi.org/10.1109/DeSE54285.2021.9719456
- Khan, M. M., Hyder, M. F., Khan, S. M., Arshad, J., & Khan, M. M. (2021). **"Ransomware prevention using a moving target defense-based approach."** *Concurrency and Computation: Practice and Experience*, 35(7), e7592. https://doi.org/10.1002/cpe.7592

THANK YOU