



FLORIDA INTERNATIONAL UNIVERSITY
Knight Foundation School of Computing and
Information Sciences

Fall 2025 Senior Design Project

Profiling Ransomware Attacks via Web Crawling and Textual Analysis

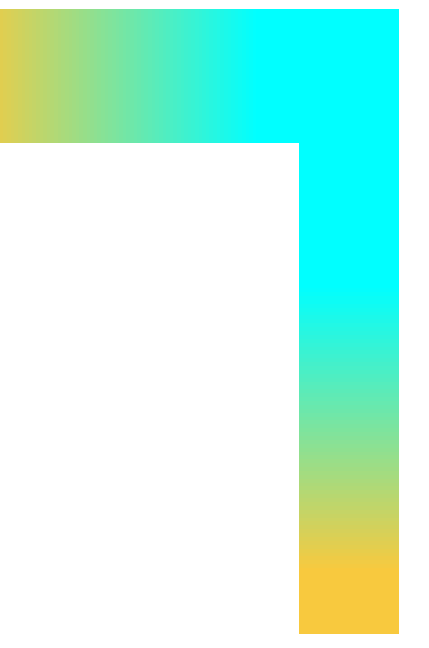
Students: Jordan Arteaga, Pedro Loor, Luis Salgado, Kevin Montenegro, Elvis Nakamura

Mentor: *Weidong Zhu, Assistant Professor*

Instructor/Faculty: *Seyedmasoud Sadjadi, Florida International University*

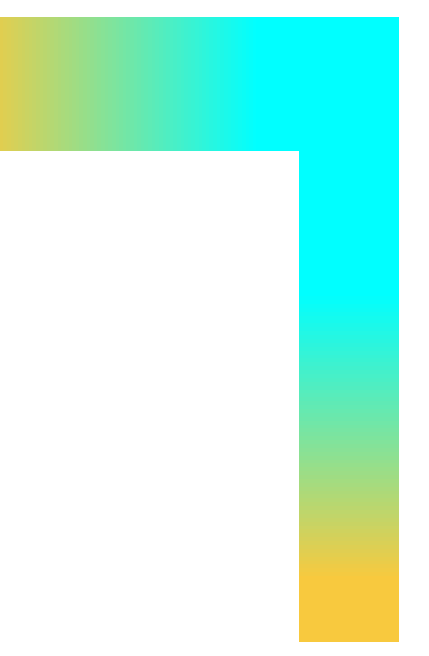
Project Motivation

Analyzing the content from ransomware-related news, posts, and reports can provide heuristics for the defense. Profiling the characteristics of emerging ransomware attacks can inform a more effective ransomware defense.



Approach

Crawling web content to extract ransomware-related contextual descriptions, making attack patterns via the extracted features, and in turn classifying said features to make suggestions for future ransomware defense.



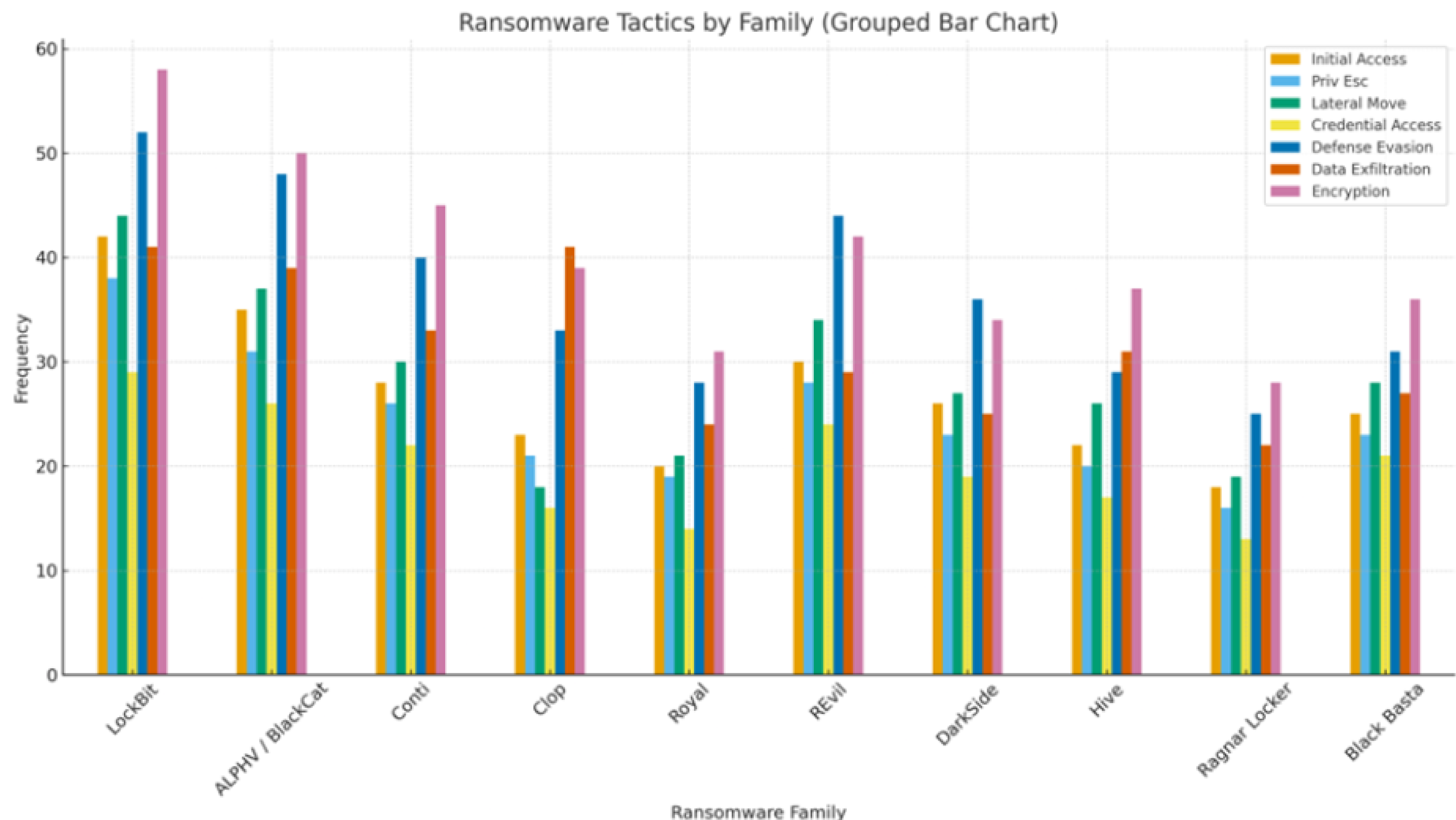
Conceptualization

- **Web Crawling**
 - **Features**
- **Contextual Analysis**
- **Pattern Classification**

Web Crawler Implementation

- 4 iterations before final product
- Creation of an inhouse web crawler utilizing python
- Keyword based search regardless of site
- Data storage and processing in Amazon AWS

Ransomware Families and Tactics

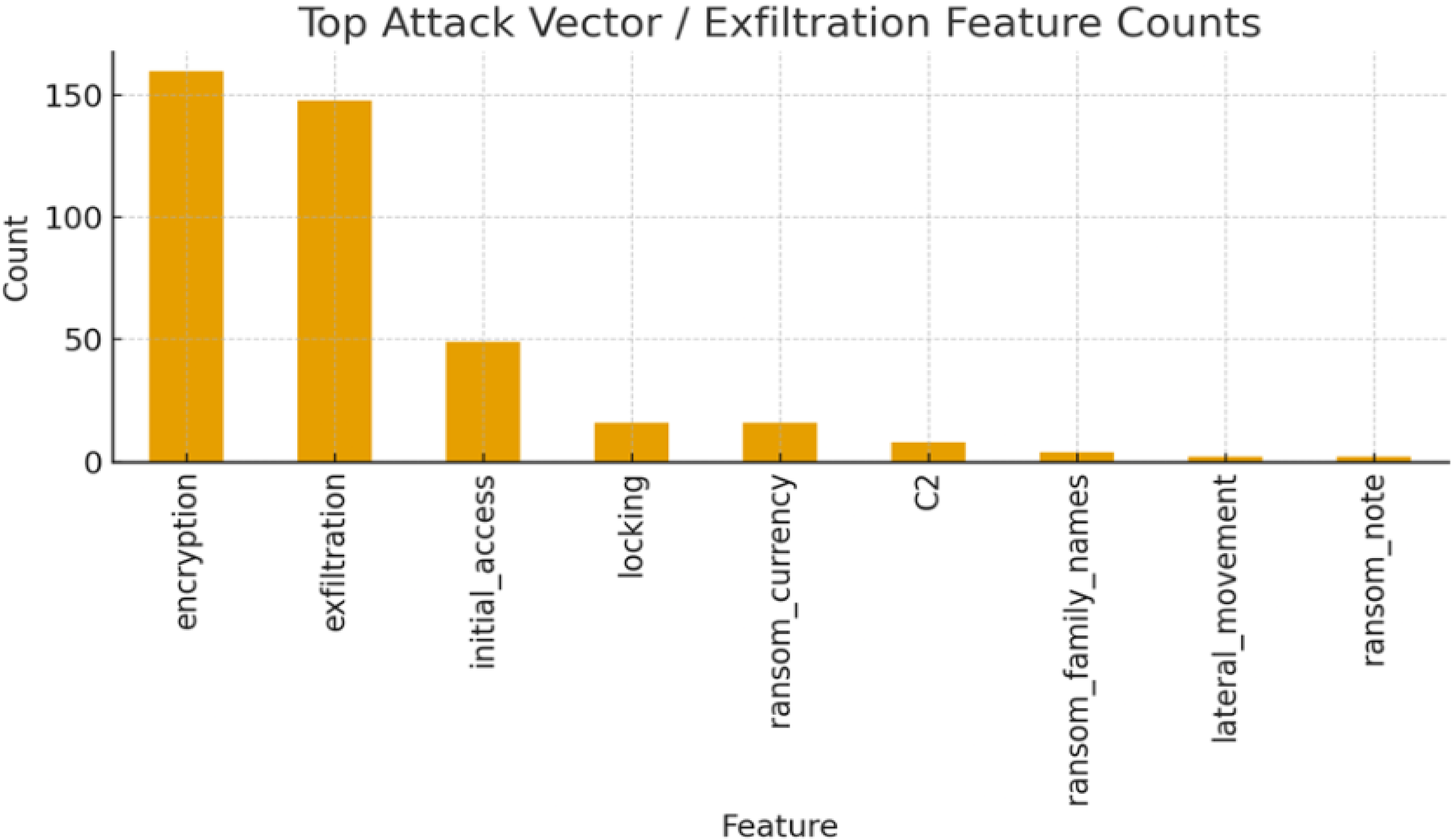


classic ransomware playbook.

Ransomware Families and Tactics cont.

- **LockBit and ALPHV remain the most sophisticated and active ransomware families across all tactics.**
 - **Encryption, defense evasion, and lateral movement are the most common tactics across all families.**
- **Clop and Hive rely heavily on data exfiltration over complex movement or privilege escalation.**
- **Less-resourced families (Royal, Ragnar Locker) still follow the classic ransomware playbook.**

Attack Vectors and Exfiltration Techniques

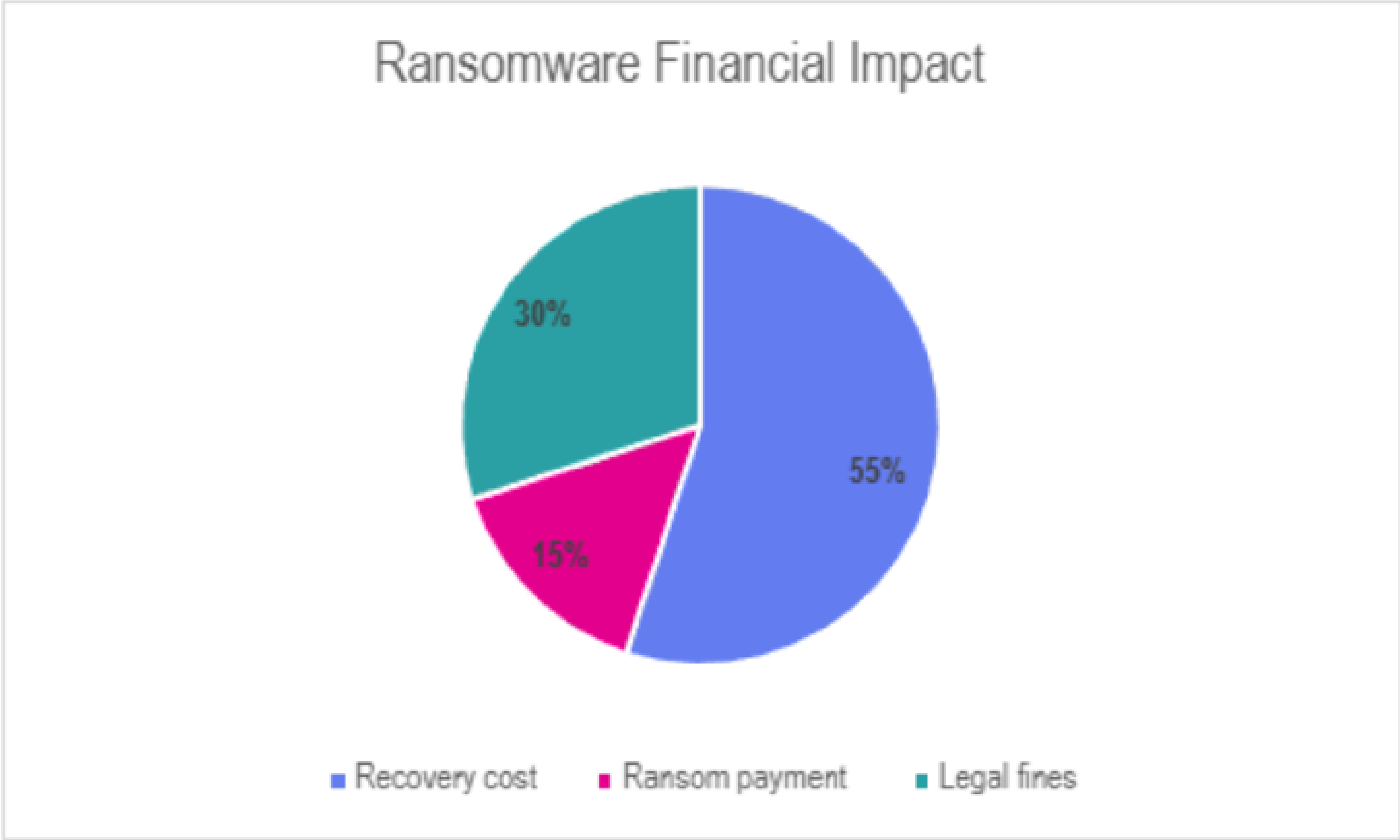


Attack Vectors and Exfiltration Techniques

cont.

- **Exfiltration and Encryption Remain Dominant Techniques**
 - **Initial Access Techniques Are Shifting**
 - **Increasing Use of Ransomware Locking & Cryptocurrency Demands**
- **Command-and-Control (C2) and Lateral Movement Still Play Key Roles**

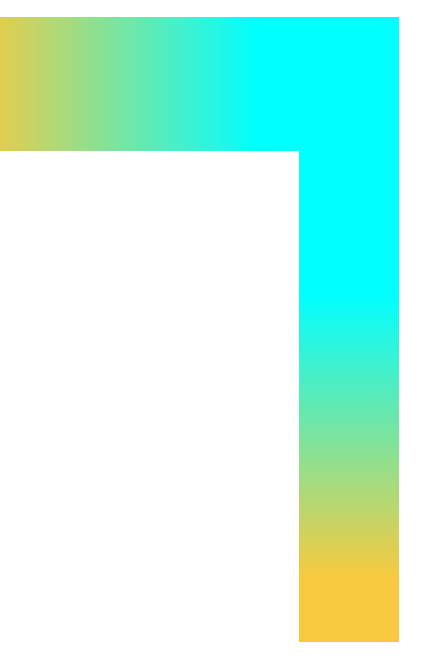
Financial and Economic Impact of Ransomware



Financial and Economic Impact of Ransomware

cont.

- 85% of cost are internally Controllable
- Threat actors prioritize value over volume
- Insurance disputes drive an unnecessary increase in recovery time
- Ransomware costs are becoming “one-size-fits-all” across industries



Summary

This project sought to provide a means of data collection and analyzation to in turn derive usable real time data that can help aid in the detection of ransomware deployment.

Acknowledgement

Thank you to Professor Zhu for presenting the project and giving the team the opportunity to create something that could help build a better future.

Supporting Applications

