**IFT 381**

**Group Project Update**

### **Project Summary**

Our project focuses on analyzing the CL0P ransomware group, with an emphasis on their high-profile 2023 attacks, including the GoAnywhere MFT and Moveit exploitations. CL0P has become a persistent threat due to its sophisticated human-operated techniques targeting critical vulnerabilities in enterprise systems. This research explores the group's tactics, techniques, and procedures (TTPs) to provide a deeper understanding of their attack strategies. The final report will encompass the economic impact of these attacks, detailed case studies of affected organizations, and practical recommendations to strengthen defenses against such cyber threats.

### **Team Update**

This week, the team has completed the research phase and is now focused on finalizing the executive review. The drafting process has begun, as we integrate our findings into a cohesive report. Our efforts are now directed towards preparing a polished draft for review.

**Leader: Louie**

* Coordinated the team's transition from research to drafting, ensuring efficient workflow and alignment with project deadlines. Louie has also been setting clear milestones to keep the project on track.

**Researcher: Zack**

* Expanded the scope of research to include recent updates on CL0P's tactics, gathering data on their evolving attack patterns and the industries most affected by their 2023 exploits.

**Contributor: Brandon**

* Focused on integrating case studies into the draft, drawing on real-world examples to enrich the analysis. Also worked on compiling additional resources to support the report's conclusions.

**Quality Assurance: William**

* Conducted thorough reviews of preliminary sections to validate data accuracy and ensure adherence to academic standards. Continued quality checks throughout the drafting process to maintain the integrity of the report.

### **Next Steps**

* Complete the executive review and finalize a full draft of the report by the end of the week to allow ample time for peer review and revisions.
* Continue quality assurance checks weekly to validate new information, ensuring factual accuracy and consistency with project objectives.
* Prepare for a final presentation summarizing key findings and actionable recommendations for defending against CL0P-style attacks.