IFT 381

**Group Project Update**

**William - Leader**

*Ideas:*

* Lockbit3 - Remains one of the most prolific ransomware groups, noted for targeting various industries.
* BlackCat - Known for creative breaches, utilizing innovative attack strategies.

*Assignments:*

* Continued focus on the GoAnywhere MFT Attack; analysis of its impact and vulnerabilities exploited.

**Louie - Researcher**

*Ideas:*

* BlackBasta - A diverse ransomware group with a wide range of targets, from financial to industrial sectors.
* Bianlian - Continues to target critical infrastructure with sophisticated techniques.

*Assignments:*

* Completed research on the Moveit exploitation and its consequences on data security.

**Zack - Contributor**

*Ideas:*

* Clop Ransomware Group - A persistent extortion group focusing on high-profile victims.
* Akira - Aimed at exploiting public-facing services, with an increase in phishing attacks.

*Assignments:*

* Research on the fiscal damage caused by CL0P has been expanded to include a comparison with similar ransomware groups.

**Brandon - Quality Assurance**

*Ideas:*

* MalasLocker - A notable emerging threat focusing on small to medium enterprises.
* Royal - Maintains a strong focus on targeting critical infrastructure, with emphasis on high-impact attacks.

*Assignments:*

* Initial research on the CVE exploits of CL0P has been validated and cross-referenced. Added focus on 2023 trends for accuracy.

**Final Project Direction:**

Our team has chosen to focus on the CL0P Ransomware Group, particularly analyzing the 2023 ransomware attacks. The emphasis will be on attacks that involve significant human intervention and hacking skills. The research paper will center on the 2023 GoAnywhere MFT Attack and the Moveit exploitation, highlighting the methods used and their impacts on industries.

**Action Plan:**

* Research will continue, with the team pooling ideas and findings weekly.
* Role adjustments will be made based on workload and research depth before the next team update.
* Weekly quality assurance checks will ensure accuracy and factual integrity.
* The contributor will provide additional resources to deepen our understanding of selected topics.
* The researcher will maintain focus on the latest developments involving the CL0P group, updating the team accordingly.
* The leader will continue task delegation, keeping the project aligned with deadlines.

**Project Summary:**

This page serves as a centralized hub for our group's brainstorming and decision-making as we solidify our project's scope, focusing on malware. Our objective is to deliver a comprehensive analysis of ransomware, with a specific focus on the CL0P group's activities and techniques throughout 2023.