The Bureau
Cyber Consulting

“In tenebras leviter ingredimur”

Executive Summary

Objective: Overview of the report's purpose.

Key Findings: Summary of major threats, including potential impact.

Recommendations: Strategic recommendations for risk mitigation.

Threat Actor Overview

Name/Alias: Known names or aliases.

Associated Groups: Links to larger threat groups.

Motivation: Financial, political, ideological, etc.

Known Operations: Summary of past significant operations.

Detailed Threat Analysis

Attribution and Relationships

- **Attribution Confidence**: Level of certainty in attribution.
- **Nation-State Ties**: Links to governments, if any.
- **Collaborations**: Alliances with other threat actors.

Tactics, Techniques, and Procedures (TTPs)

- **Attack Vectors: Common methods used (e.g., phishing, malware).**
- **Exploited Vulnerabilities: Known weaknesses exploited.**
- **Tools Used: Malware, exploits, etc.**
- **Operational Style: Behavioral patterns and tendencies.**

Indicators of Compromise (IOCs)

- **IP Addresses**: Known malicious IPs.
- **Domains**: Malicious or compromised domains.
- **File Hashes**: Hashes of malicious files.
- **Signatures**: Behavioral signatures.

Threat Actor Capabilities

- **Technical Capabilities**: Skill level and resources.
- **Infrastructure**: Command-and-control servers, botnets, etc.
- **Operational Reach**: Geographical impact, industries targeted.

Impact assessment

Affected Sectors: Industries at risk.

Geopolitical Impact: Broader implications.

Financial/Economic Impact: Potential financial loss.

Mitigation Strategies

Defensive Measures: Security controls to implement.

Detection Methods: How to identify this actor’s activity.

Incident Response Plan: Steps to take if compromised.

Report contributors & sources

Author(s): Names, titles, and roles of those who prepared the report.
Reviewers: Names, titles, and roles of those who reviewed the report.
Acknowledgements: Any sources or supporting teams.