The Bureau
Cyber Consulting

"In tenebras leviter ingredimur"

Executive Summary

Campaign Overview: Brief description of the campaign.

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

Recommendations: Strategic recommendations for risk mitigation.

Campaign Background

Initiator: Who is behind the campaign (if known).

Objective: Purpose or goals of the campaign.

Target Sectors/Regions: Industries or locations targeted.

Campaign Timeline: Start and end dates, or ongoing status.

Detailed Threat Analysis

Techniques and Tools Used

- **Attack Vectors**: Methods used (phishing, watering hole, etc.).
- **Malware/Exploits**: Specific malware or vulnerabilities used.
- **Infrastructure**: Command-and-control servers, hosting services.

Tactics, Techniques, and Procedures (TTPs)

- **Patterns of Behavior**: Common TTPs associated with the campaign.
- **Indicators of Compromise (IOCs)**: IOCs tied to the campaign.
- **Notable Variations**: Any unique or evolving methods.

Attribution

- **Attribution Confidence**: Level of certainty in linking to known actors.
- **Connections to Previous Campaigns**: Links to past operations.
- **Nation-State Involvement**: Any government sponsorship or involvement.

Impact assessment

Affected Entities: Organizations impacted by the campaign.

Data Compromised: Information stolen or at risk.

Operational Disruption: Impact on operations of affected entities.

Financial Impact: Estimated or known financial losses.

Recommendations

Summary of Findings: Recap of the investigation's findings.

Mitigation Strategies: Detailed, specific actions to mitigate identified threats.

Security Improvements: Long-term recommendations for improving security posture.
Detection Methods: How to detect similar activity in the future.

Final Thoughts: Final recommendations or observations.

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.