

# Cyber Threat Intelligence Report

This document presents the findings from the threat intelligence analysis carried out on the targeted organization. It offers insights into potential threats and explores the adversary's actions and strategies. Additionally, this document provides a comprehensive breakdown of the Indicators of Compromise (IoCs) and proposes recommendations for future course of actions.

**Note:** The fields marked with *(To edit)* should be customized by the analyst according to their specific requirements. Please delete this note once read.

## Report Details

|                                 |  |
|---------------------------------|--|
| Reporting Author & Designation: |  |
| Reporting Company Name:         |  |
| Reporting Date:                 |  |

## Client Details

|                            |  |
|----------------------------|--|
| Client Name & Designation: |  |
| Client Company Name:       |  |
| Client Industry:           |  |
| Client Location:           |  |
| Client Company Size:       |  |

## Test Details

|                  |  |
|------------------|--|
| Start Date:      |  |
| End Date:        |  |
| Duration:        |  |
| Test Type:       |  |
| Test Team Size:  |  |
| Assets Analyzed: |  |

## Executive Summary

---

*(To edit)* This section deals with summary of the threat intelligence gathered after conducting detailed analysis. *(To edit)*

### Traffic Light Protocol

*(To edit)* The following TLP indicator indicates the number of threats identified by the threat intelligence team, depending on the risk level, threat impact, and potential harmfulness. *(To edit)*

| HIGH             | MEDIUM           | LOW              |
|------------------|------------------|------------------|
| <i>(To edit)</i> | <i>(To edit)</i> | <i>(To edit)</i> |

## Analysis Methodology

---

*(To edit)* This section deals with the methodology followed throughout the course of the threat intelligence project. *(To edit)*

### Threat Data Collection and Processing

- **Tasks Performed:**

*(To edit)*

- **Considerations:**

*(To edit)*

- **Tools Used:**

*(To edit)*

### Threat Analysis

- **Tasks Performed:**

*(To edit)*

- **Considerations:**

*(To edit)*

- **Tools Used:**

*(To edit)*

## Threat Details (Adversary Actions and Tactics)

*(To edit)* This section deals with the findings from the conducted threat intelligence. *(To edit)*

|                     |  |
|---------------------|--|
| Threat Code         |  |
| TLP Rank            |  |
| Threat Name         |  |
| Threat Description  |  |
| Threat Capabilities |  |
| Threat Propagation  |  |
| Target Victims      |  |

## Key Indicators of Compromise (IoCs)

*(To edit)* This section deals with the threat-wise Indicators of Compromise (IoCs) *(To edit)*

|             |         |
|-------------|---------|
| Threat Code |         |
| Threat Name |         |
| Indicator   | Details |
|             |         |

## Recommended Actions

*(To edit)* This section deals with the suggestions and recommendations to the client organization. *(To edit)*

### Areas for Attention

*(To edit)*

### Dissemination Strategy

*(To edit)*

### Integration Strategy

*(To edit)*