# CLASSIFIED - FOR OFFICIAL USE ONLY

# Advanced Persistent Threat Analysis - APT-2025-001

## Executive Summary:

A sophisticated threat actor, designated APT-2025-001, has been identified targeting critical infrastructure across multiple sectors. The group exhibits advanced capabilities including zero-day exploits, custom malware, and sophisticated social engineering techniques.

## Key Findings:

• Initial access via spear-phishing campaigns
• Lateral movement using legitimate administrative tools
• Data exfiltration over encrypted channels
• Persistence through registry modifications

## Affected Sectors:

• Energy and utilities - 45% of incidents
• Financial services - 30% of incidents
• Government agencies - 15% of incidents
• Healthcare systems - 10% of incidents

## Technical Analysis:

The threat actor employs a multi-stage malware framework consisting of:

### *Stage 1 - Initial Dropper:*

MD5: 3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d
SHA256: 1234567890abcdef1234567890abcdef12345678
File size: 2.3MB

### *Stage 2 - Persistence Module:*

Registry key: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Service installation: Windows Security Update Service

### *Stage 3 - Command and Control:*

C2 servers: 192.168.45.123, 10.0.0.245
Communication protocol: HTTPS over port 443
Beacon interval: 30-120 minutes (randomized)

## Recommendations and Mitigation:

• Deploy updated IOCs to all security tools
• Enhance email security filtering
• Implement additional network monitoring
• Conduct threat hunting activities

Classification: CONFIDENTIAL
Report Date: November 11, 2025