Friday Overtime

## 📝 **Mini Incident Report – Friday Overtime**

**Lab Name:** Friday Overtime  
**Category:** Cyber Threat Intelligence – Small Case Report

### **1. Summary of Incident**

During routine SOC monitoring late on a Friday evening, an analyst detects unusual network activity from an internal workstation. The pattern of connections and IOC matches suggests possible **Command and Control (C2)** communication related to a known malware campaign.

### **2. Key Observations**

* **Initial Alert:** Outbound traffic to suspicious IP addresses flagged by threat intel feed.
* **Source System:** Workstation in Finance Department.
* **IOC Matches:**
  + Two IP addresses from Abuse.ch threat feed.
  + One SHA256 hash matching a known malware sample.
* **Timeline:**
  + 19:43 – Alert triggered by SIEM (ELK/Splunk).
  + 19:45 – Analyst confirms IOC matches via MISP.
  + 19:52 – Endpoint scanning begins.

### **3. Analysis Steps Taken**

1. **IOC Verification**
   * Checked in MISP for event correlation — matched to a recent phishing campaign targeting finance sectors.
2. **Endpoint Review**
   * Used Sysinternals and Sysmon logs to identify suspicious process tree.
   * Found invoice\_update.exe running from C:\Users\Public\.
3. **Network Review**
   * Verified outbound traffic to known C2 servers over port 443 with irregular beaconing pattern.

### **4. Findings**

* Infection likely started via phishing email with malicious attachment.
* Malware established persistence using a registry run key.
* C2 infrastructure matched known threat actor TTPs documented in MITRE ATT&CK (T1071.001 – Application Layer Protocol: Web Traffic).

### **5. Mitigation & Containment**

* Isolated affected workstation from network.
* Blocked malicious IPs at firewall.
* Created SIEM rule to alert on similar outbound patterns.

### **6. Lessons Learned**

* Need better **email filtering rules** to block malicious attachments.
* SIEM correlation rules should be tuned to detect beaconing patterns faster.
* Increase analyst shift overlap during off-hours to reduce response time.

