# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Identified Protocols:   * HTTP/1.1 (Cleartext protocol - High Risk)   + GET /HTTP/1.1 request observed   + No encryption of transmitted data   + Vulnerable to MITM attacks   Additional Protocol Evidence:   * DNS queries preceding HTTP traffic (potential DNS tunneling) * Port switching (52444 → 36086 → 56378) indicating possible evasion behavior | |
|

| Section 2: Document the incident |
| --- |
| 1. Initial Compromise (14:18:32)    * DNS query for yummyrecipesforme.com (203.0.113.22)    * HTTP connection established on port 80 2. Malicious Activity (14:18:36)    * GET / request observed    * 2-minute sustained connection (data exfiltration likely) 3. Lateral Movement (14:20:32)    * DNS redirection to greatrecipesforme.com (192.0.2.172)    * New ephemeral port usage (56378)   Technical Indicators of Compromise (IoC):   * Malicious IPs: 203.0.113.22, 192.0.2.172 * Suspicious Domains:   + yummyrecipesforme.com (Initial C2)   + greatrecipesforme.com (Secondary C2) * Anomalous Port Activity: Multiple source port changes   Impact Assessment:   * Credential brute-forcing potential * Possible malware download via HTTP GET * Network persistence established |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| 1. Brute Force Specific Defenses:    * Password Policy Enhancements:      + Minimum 12-character complexity requirements      + Password blacklisting of common patterns    * Account Lockout:      + 5 failed attempts → 15 minute lockout      + Subsequent failures → exponential backoff    * Multi-Factor Authentication:      + Mandatory TOTP or hardware tokens for all external access |