# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The following network protocols were involved in the security incident:   1. **DNS (Domain Name System)**:    * **Query**: 14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)    * **Response**: 14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)    * **Query**: 14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)    * **Response**: 14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40) 2. **HTTP (HyperText Transfer Protocol)**:    * **Request**: 14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0    * **Response**: 14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS val 3302576859 ecr 3302576859,nop,wscale 7], length 0    * **Request**: 14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0    * **Response**: 14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0 | |
|

| **Section 2: Document the incident** |
| --- |
| **Incident Overview**:   * **Date/Time**: Incident observed during log review on [specific date/time]. * **Affected Website**: yummyrecipesforme.com * **Attacker**: Former employee (referred to as "the baker"). * **Impact**: Customers were prompted to download a malicious file which, when executed, redirected them to a fake website (greatrecipesforme.com) containing malware.   **Incident Details**:   * The attacker executed a brute force attack to guess the administrative account password, which was still set to the default value. * After gaining access, the attacker modified the website's source code to include a JavaScript function prompting visitors to download and execute a malicious file. * When visitors downloaded and executed the file, their browsers were redirected to greatrecipesforme.com, which contained malware. * The legitimate admin account password was changed by the attacker to prevent immediate remediation by the website owner.   **Technical Details**:   * **DNS Requests**:   + DNS query for yummyrecipesforme.com returned IP address 203.0.113.22.   + DNS query for greatrecipesforme.com returned IP address 192.0.2.17. * **HTTP Traffic**:   + The browser initiated HTTP requests to yummyrecipesforme.com and then to greatrecipesforme.com after being redirected by the malware.   + The traffic log shows standard TCP handshake and HTTP GET requests for both domains.   **Customer Impact**:   * Multiple customers reported being prompted to download a file for "free recipes" and experienced slower computer performance after running the file. * The redirected URL (greatrecipesforme.com) contained malware that could further compromise the customers' systems. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To prevent future brute force attacks, implement the following security measure:  **Enforce Strong Password Policies and Account Lockout Mechanisms**:   * **Strong Password Policies**: Ensure that all administrative accounts require strong, complex passwords that include a combination of letters, numbers, and special characters. Passwords should be changed regularly and should not be easily guessable. * **Account Lockout Mechanisms**: Implement an account lockout policy that temporarily locks an account after a specified number of failed login attempts. This will help to prevent automated brute force attacks by making it difficult for attackers to repeatedly guess passwords.   Additionally, consider implementing Multi-Factor Authentication (MFA) for all administrative accounts to provide an extra layer of security beyond just the password. |