# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| **The network protocols identified in the tcpdump log during the investigation include:**  1. DNS (Domain Name System): Used for resolving domain names to IP addresses.  Example from log:  14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24)  14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A 203.0.113.22 (40)  2. HTTP (Hypertext Transfer Protocol): Used for communication between the browser and web servers.  Example from log:  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  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  14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1 |
|

|  |
| --- |
| **Section 2: Document the incident** |
| **Summary of Incident:**  On [insert date], multiple customers of yummyrecipesforme.com reported being prompted to download a file upon visiting the website. After running the file, they were redirected to a different website, greatrecipesforme.com, and noticed performance issues on their personal computers.  **Details:**   * Location: yummyrecipesforme.com * Incident Type: Web server compromise and malware distribution * Date and Time of Incident: [insert date and time] * Discovery: The issue was discovered following customer complaints received by the helpdesk. * Incident Description:   + A former employee, referred to as the "disgruntled baker," executed a brute force attack on the web server hosting the website. By repeatedly attempting default passwords, they successfully gained administrative access.   + Upon gaining access, they embedded malicious JavaScript code into the website’s source code. This script prompted visitors to download an executable file that contained malware.   + The malware redirected the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com, a fake website designed to look like the original but containing further malicious content.   + The former employee changed the administrative password post-compromise, locking out legitimate access.   **Investigation Findings:**   * Initial DNS Request: The user’s machine queried the DNS server for the IP address of yummyrecipesforme.com, and the DNS server responded with the IP address 203.0.113.22. * HTTP Request: The user's browser then made an HTTP request to yummyrecipesforme.com. * Malware Download: The website prompted the user to download an executable file. * Redirection: After executing the file, another DNS request was made for greatrecipesforme.com, and the DNS server responded with the IP address 192.0.2.17. Subsequently, an HTTP request was made to this address.   **Sources of Information:**   * Customer helpdesk reports. * Tcpdump log analysis. * Senior analyst review of website source code. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| **Recommendation:** Implement Two-Factor Authentication (2FA)  **Explanation:**  Two-factor authentication adds an additional layer of security beyond just the password. It requires users to provide a second form of verification, such as a code sent to their phone or generated by an authentication app. This significantly reduces the risk of unauthorized access through brute force attacks because even if the attacker guesses the correct password, they still need the second form of verification, which is generally much harder to obtain.  **Benefits:**   * Enhances security by adding an extra step in the authentication process. * Reduces the likelihood of successful brute force attacks. * Provides real-time alerts of attempted unauthorized access when the second factor is not provided.   Implementing 2FA will help prevent similar incidents in the future by ensuring that access to critical systems requires more than just a password, making it much more difficult for attackers to compromise the system through brute force methods. |