# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| During the security incident on the website yummyrecipesforme.com, the following network protocols were identified as being involved:   1. **DNS (Domain Name System) Protocol:**   **Description:** DNS is used to translate domain names (like yummyrecipesforme.com) into IP addresses that computers use to identify each other on the network.  **Role in the Incident:** The browser initiated a DNS request to resolve the IP address of yummyrecipesforme.com.  - After the initial download of the malware, another DNS request was made to resolve the IP address for greatrecipesforme.com, the malicious website.   1. **HTTP (Hypertext Transfer Protocol):**   **Description:** HTTP is the protocol used for transmitting hypertext requests and information on the World Wide Web.  **Role in the Incident:** After receiving the IP address from the DNS response, the browser initiated an HTTP request to load the webpage of yummyrecipesforme.com.  -Following the malware download and execution, the browser then made another HTTP request to greatrecipesforme.com after being redirected by the malicious script.  These protocols facilitated the initial communication and subsequent malware activity during the security breach. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| several customers reported suspicious activity on the website yummyrecipesforme.com. Upon visiting the site, customers were prompted to download an executable file, which claimed to be a necessary update for their browser. After downloading and running the file, users noticed their computers slowing down, and the website URL automatically changed from yummyrecipesforme.com to greatrecipesforme.com. This redirected site contained malware, further compromising user systems.  **Incident Details:**  1. **Attack Vector:** A former employee executed a brute force attack against the web host's administrative account. The attacker exploited the fact that the admin password was still set to its default, which is a common vulnerability that was not protected against brute force attempts.  2. **Compromise of the Admin Panel:** Once the attacker gained access to the administrative panel, they embedded a malicious JavaScript code into the website's source code. This script was designed to trigger a download prompt for an executable file whenever a user accessed yummyrecipesforme.com.  3. **Malware Distribution:** The executable file contained malware that, once run, redirected users' browsers to a fake website, greatrecipesforme.com. This fake website further compromised user systems by hosting additional malicious content.  4. **Indicators of Compromise:**  - Multiple customer complaints of unauthorized download prompts.  - Redirection of website visitors from yummyrecipesforme.com to greatrecipesforme.com.  - Slower performance of users' personal computers post-incident.  5. **Internal Investigation:**  - The cybersecurity team recreated the incident in a sandbox environment using tcpdump to monitor network traffic.  - The logs showed multiple DNS requests and HTTP communications that confirmed the redirection and malware delivery.  6. **Conclusion:**  - The website was compromised due to inadequate password security (default admin password) and lack of protection against brute force attacks.  - Malicious actors leveraged network protocols such as DNS and HTTP to execute and propagate the attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| 1. **Implement Strong Password Policies:** Ensure that all administrative accounts use complex, non-default passwords. Enforce regular password changes and use password managers to maintain secure credentials.  2. **Deploy Brute Force Attack Mitigation Tools:** Implement security measures such as rate limiting, account lockout mechanisms, and CAPTCHAs to prevent brute force attacks.  3. **Enhance Monitoring and Logging:** Utilize advanced monitoring tools to detect unusual traffic patterns and unauthorized changes to website code.  4. **Conduct Regular Security Audits:** Periodically review and update security protocols, ensuring that all systems and applications are compliant with the latest security standards.  By implementing these recommendations, yummyrecipesforme.com can significantly reduce the risk of future security incidents and enhance overall website security. |