Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Network Protocol Identified:  The primary network protocol involved in this incident is HTTP (Hypertext Transfer Protocol). This protocol operates at the Application Layer of the TCP/IP model and is used for communication between the user's browser and the web server. The following observations from the tcpdump log confirm the use of HTTP:  DNS Requests and Responses:  The browser initiated a DNS request to resolve the IP address for yummyrecipesforme.com. DNS (Domain Name System) operates at the Application Layer and is responsible for translating domain names into IP addresses.  The DNS server responded with the correct IP address for yummyrecipesforme.com.  HTTP Requests and Responses:  The browser initiated an HTTP request to the IP address of yummyrecipesforme.com to load the webpage.  The server responded with the webpage content, which included the malicious JavaScript code prompting the user to download an executable file.  After the malware was executed, the browser initiated another DNS request for greatrecipesforme.com, followed by an HTTP request to the new IP address.  TCP (Transmission Control Protocol):  TCP, which operates at the Transport Layer, was used to establish a reliable connection between the user's browser and the web server. This ensured that the HTTP requests and responses were delivered accurately. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A security incident occurred involving the compromise of the yummyrecipesforme.com website. The incident was discovered after multiple customers reported being prompted to download a file while visiting the website. Upon executing the file, their browsers were redirected to a malicious website, greatrecipesforme.com, and their systems began experiencing performance issues.  Details of the Incident:  How the Incident Occurred:  A former employee executed a brute force attack on the website's administrative account. The attacker repeatedly tried default passwords until they successfully guessed the correct one.  Once access was gained, the attacker modified the website's source code to embed malicious JavaScript. This script prompted visitors to download an executable file under the guise of a browser update.  The downloaded file contained a script that redirected users to greatrecipesforme.com, a fake website hosting malware.  The attacker also changed the administrative account password, locking out the legitimate website owner.  Discovery of the Incident:  The incident was discovered when customers reported the suspicious behavior to the company's helpdesk.  The website owner attempted to log in to the admin panel but was unable to, prompting them to contact the web hosting provider.  Cybersecurity analysts investigated the issue and confirmed the compromise by analyzing the website's source code and the downloaded file.  Impact of the Incident:  Customers who downloaded and executed the malicious file were redirected to a fake website and exposed to malware.  The website's reputation was damaged, and customer trust was compromised.  The website owner lost access to the admin panel, disrupting normal operations.  Evidence and Sources:  tcpdump Logs: Captured network traffic showing DNS and HTTP requests/responses.  Source Code Analysis: Identified the malicious JavaScript embedded in the website's code.  Malware Analysis: Confirmed the presence of a script that redirected users to greatrecipesforme.com.  Customer Reports: Multiple customers reported the suspicious download prompt and subsequent system issues. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Based on the incident and the need to strengthen security measures, the following recommendations are provided to prevent future brute force attacks and enhance the overall security posture of yummyrecipesforme.com:  Enforce Strong Password Policies:  Require the use of strong, complex passwords for all administrative accounts. Passwords should include a combination of uppercase and lowercase letters, numbers, and special characters.  Set a minimum password length (e.g., 12 characters) to ensure complexity.  Limit Login Attempts:  Implement account lockout mechanisms that temporarily lock an account after a specified number of failed login attempts (e.g., 5 attempts). This will deter brute force attacks by making it harder for attackers to guess passwords.  Frequent Password Changes:  Enforce regular password changes for administrative accounts, such as every 30 days. This reduces the risk of compromised passwords being used over an extended period.  Disallow Previous Passwords:  Prevent users from reusing previously used passwords. This ensures that even if an old password is compromised, it cannot be reused.  Enforce Multi-Factor Authentication (MFA):  Require MFA for all administrative accounts. This adds an additional layer of security by requiring a second form of verification (e.g., a one-time code sent to a mobile device) in addition to the password.  Monitor Login Attempts:  Implement logging and monitoring of all login attempts. This will help detect suspicious activity, such as repeated failed login attempts, and allow for timely response to potential brute force attacks.  Implement the Principle of Least Privilege:  Restrict access to administrative accounts and sensitive systems to only those employees who absolutely need it. Ensure that employees only have access to the resources necessary for their job functions.  Deploy Web Application Firewalls (WAFs):  Use a WAF to monitor and filter incoming traffic. A WAF can help detect and block brute force attempts and other malicious activities targeting the website.  Regularly Update and Patch Systems:  Ensure that all software, including the web server, content management system, and any plugins, is kept up to date with the latest security patches. This reduces the risk of vulnerabilities being exploited.  Conduct Security Audits and Penetration Testing:  Perform regular security audits and penetration testing to identify and address vulnerabilities in the website and its infrastructure.  Educate Employees and Customers:  Provide cybersecurity training to employees to help them recognize and respond to potential threats, such as phishing attempts or suspicious login activity.  Inform customers about safe browsing practices and advise them not to download files from untrusted sources. |