Security Incident Report. HTTP

1. Incident Overview

- **Date and Time of Incident:**
  March 20, 2012, 13:37:42
- **Incident Description:**
  The incident began when several customers of the website YummyRecipesForMe.com reported being prompted to download a file in order to access new recipes. After executing the file, users experienced a significant slowdown in system performance. Additionally, the website owner noticed that their administrator account was locked out.
- **Incident Location:**
  The incident occurred on the YummyRecipesForMe.com web server, affecting both customers and the internal infrastructure of the website.
- **Type of Incident:**
  Unauthorized access exploit (brute-force attack) and malware distribution.

2. Identification of the Network Protocol Involved

The protocol involved in this incident was the Hypertext Transfer Protocol (HTTP). The attack occurred through manipulation of HTTP traffic between users and the web server. During the review of traffic logs, using tcpdump, it was identified that the malicious file was delivered to users' computers via HTTP requests at the application layer.

3. Detailed Incident Analysis

Technical Description:

1. Access to a Malicious Website: Users accessing YummyRecipesForMe.com were automatically redirected to download a malicious file that appeared to offer free recipes. This file was designed to execute malicious code, affecting the performance of their devices.
2. Network Traffic Capture (tcpdump): tcpdump was used to monitor the network traffic generated when users accessed the website. Initially, traffic was directed to the IP address of YummyRecipesForMe.com. However, after the malicious file was executed, a change in the requested IP address was observed, redirecting traffic to a different server, GreatRecipesForMe.com, indicating potential DNS manipulation or a "man-in-the-middle" attack.
3. Attack Analysis: The compromised website's source code and the downloaded file were thoroughly reviewed. It was discovered that an attacker had inserted malicious code into the legitimate website, allowing the malicious file to be downloaded without user intervention.

4. Unauthorized Server Access: According to the website owner, their admin account was locked out after the attack. The security team determined that a brute-force attack was used to gain access to the admin account, allowing the attacker to change the password and manipulate the website.

4. Impact and Scope of the Incident

- **Affected Users:**
  Several users who visited the website and downloaded the malicious file experienced decreased performance on their devices.
- **Compromised Resources:**
  - User Accounts: It is suspected that the administrator's credentials were compromised.
  - User Data: There is no indication so far that personal customer data was lost during the incident.
  - Server Infrastructure: The web server and related infrastructure were compromised due to unauthorized access.
- **Exposure Duration:**
  The incident remained active for 6 hours before being detected and mitigated.

5. Corrective Measures and Prevention

1. Recommendations to Mitigate Brute-Force Attacks:

- Prohibit the Use of Previous Passwords:
  Restrict the use of old passwords during the password reset process, preventing attackers from using default or previous passwords.
- Longer and More Complex Passwords:
  Require passwords of at least 15 characters, combining uppercase and lowercase letters, numbers, and special characters.
- Two-Factor Authentication (2FA):
  Implement a 2FA system that requires both a password and a code sent to the user's email or mobile phone, making brute-force attacks more difficult.

2. Solution for Malware Distribution:

- Code Audit and Review:
  Conduct a thorough audit of all source code and distributed files on the website. Block any attacker's ability to insert malicious code.
- Network Infrastructure Review:
  Implement a firewall system to prevent unauthorized redirects and block suspicious IP addresses.

3. Review of Administrator Access and Accounts:

- Immediate Password Change for Critical Accounts:
  Enforce immediate password changes for all admin accounts and conduct an in-depth access review to prevent future attacks.

6. Lessons Learned

- Importance of Strong Authentication:
  The brute-force attack was facilitated by weak passwords. Implementing stricter password policies and two-factor authentication could have prevented the unauthorized access.
- Vulnerabilities in HTTP Traffic Handling:
  The redirection to a fraudulent website via HTTP demonstrates the need for heightened monitoring of domain and network traffic.

7. Action Plan

- Further Investigation:
  Continue investigating to determine the full extent of the incident and identify any additional attack vectors that may have been used.
- Implementation of Security Measures:
  Security recommendations will be implemented immediately to protect systems and user data in the future.
- Continuous Monitoring:
  Ongoing monitoring will be established to detect any suspicious activity and mitigate potential future incidents.