# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Using tcpdump to capture the packets, we make the request for yummyrecipesforme.com and found that the malicious file is using the Hypertext transfer protocol (HTTP) to reach the user’s computers. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The yummyrecipesforme helpdesk received numerous customer complaints regarding a suspicious incident on the company's website. Customers reported being prompted to download a file, ostensibly to update their web browsers. Subsequently, after running the downloaded file, they experienced a slowdown in their computer's performance and were redirected to an unknown website.  Upon receiving the complaints, the yummyrecipesforme security team promptly initiated an investigation to assess the nature and scope of the incident. To begin, the team decided to conduct their investigation in a secure sandbox environment, using tcpdump to capture network packets for further analysis.  The team replicated a standard website request to YummyRecipesForMe.com and observed that the DNS server accurately responded with the legitimate IP address of the website, allowing them to access the site without any apparent issues. However, upon entering the webpage, the team encountered an immediate prompt to download a file purporting to be a browser update. Out of concern for potential risks, the security team decided to download and execute the file.  During the execution of the downloaded file, the web browser was redirected to an unfamiliar URL. Analyzing the network packets captured by tcpdump, the team identified requests made to a deceptive site named greatrecipesforme.com. This finding raised serious concerns about a potential cyberattack.  To understand the nature and origin of the attack, the security team performed an in-depth analysis of both the yummyrecipesforme website's source code and the downloaded file. Their examination revealed the presence of a malicious code injected into the website's pages. This code appeared to be coercing unsuspecting users into downloading the file, thus exposing them to possible risks and unauthorized redirections.  Additionally, the team discovered indications of a potential brute force attack. The attack, seemingly targeted at the website's administrator account, likely enabled unauthorized access to modify the site's source code and changing the password denying access to the administrator account. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To enhance the security posture and mitigate the risk of future similar incidents, we strongly recommend implementing the following measures:   * Require strong password. * Enforce two-factor authentication (2FA). * Monitor login attempts. * Limit login attempts. |