# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Based on the dump logs the network protocols involved in this incident are  DNS, TCP and HTTP. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| It is likely that a malicious actor had executed a brute force attack on an administrative account of the webserver and gained access to the admin panel to change the part of the source code which embedded a javascript function that prompts the user to download and run a file upon visiting the website.  This file redirected the users to a fake website (greatrecipiesforme.com) that contains additional malware which can be confirmed by customers reported the slow performances on their computers after accessing the website.  Cybersecurity analyst has simulated the customer action in a sandbox and confirmed that when visiting yummyrecipiesforme.com that the following occurs and has found the following occurs:   * The browser intitates a DNS request and requests the IP address of yummyrecipiesforme.com from the DNS server * The DNS replies with the correct IP address * The browser initites an HTTP request: it requests the yummyrecipiesforme.com webpage using the IP address sent by the DNS server * The browser initiates the download of the malware * The browser initiess a DNS request for greatrecipiesforme.com * The browser initiates an HTTP request to the IP address for greatrecpiesforme.com |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| In order to prevent brute for attacks like this one it is recommended to carryout some form of remediation.  This may include failed login attempt thresholds which includes a reasonable number of failed login attempts allowed within a specific time window i.e 5 failed attempt within 30minutes. This may also be used in conjunction with a lockout duration for when the attempt threshold has been breached. |