# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Traffic in port 80 indicates continual usage of the Hypertext transfer protocol (HTTP).  The malicious file is also seen being sent to users’ computers by the protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The incident happened at around 2:15 pm.  We found out about the incident from customers emailing yummyrecipesforme’s helpdesk. They complained that the website had pompted them to download a file to access free recipes, and after downloading the file they are redirected to a fake vesrsion of the website that contains the malware.  We used a sandbox environment to open the website without affecting the company’s network. And then we ran tcpdum to capture network traffic packets which were produced by interacting with the website. Similar to the above we were prompted to download a file claiming it would provide access to free recipes. We accepted the download and ran it, which redirected the team to the fake website (greatrecipesforme.com)  The tcpdump log confirms the customer reports. Initial connection requests have the correct IP address of yummyrecipesforme.com (203.0.113.22). However, around 14:20, the DNS server has routed the traffic to a different IP address (192.0.2.172) indicating that a connection has been established with another website.  The senior cybersecurity expert analysed thee source code for the websites and the file. They found that the malicious attacker had added code to the website that prompted the users to download a malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users’ computers. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Using stronger password policies would help—since the default admin password is still in use and has not been updated in a while, this made the system very vulnerable to a brute force attack.  At least 8 characters, one number, one symbol.  Admin password also needs to be updated regularly (every 2 months)  Prevent the same password from being reused.  Users should also only be allowed a maximum of three attempts before their access to the website is revoked.  2FA could also be implemented whereby a one-time passcode (OTP) is sent to the user to authenticate their identity.  These measures will limit the amount of access a brute force attacker can have to the website as the 2FA and password measures limits the amount of attempts they have at accessing the website. |