Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The Hypertext Transfer Protocol (HTTP) is the protocol that was affected by the incident.  The evidence required to reach this conclusion was obtained by accessing the yummyrecipesforme.com website and running tcpdump to identify the issue, and recording traffic activity in a DNS and HTTP traffic log file. At the application layer, the malicious file is seen being transferred to users' computers via the HTTP protocol. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Customers reported that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Several customers contacted the website owner. Since then, their personal computers have been running slowly. The owner of the website attempted to log into the web server but discovered that their account was locked out.  The website was tested by the cybersecurity analyst in a sandbox without affecting the company network. The analyst then used tcpdump to record the packets of network and protocol traffic generated by interacting with the website. After being asked to download a file that claimed to update the user's browser, the analyst accepted the download and ran it. The program  then diverted the investigator to a phony site (greatrecipesforme.com) that  appeared to be indistinguishable from the first site (yummyrecipesforme.com).  The cybersecurity analyst looked at the tcpdump log and saw that the browser first requested the yummyrecipesforme.com website's IP address. The analyst recalled downloading and running the file after the HTTP protocol connection with the website was established. The browser requested a new IP resolution for the greatrecipesforme.com URL, which resulted in a sudden change in network traffic, as evidenced by the logs. The traffic on the network was then redirected to the new IP address for the website greatrecipesforme.com.  The senior cybersecurity professional investigated the source code for the  sites and the downloaded document. The examiner found that an assailant had controlled the site to add code that incited the clients to download a malevolent document camouflaged as a program update. The team believes that the attacker used a brute force attack to gain access to the administrator account and modify the administrator password because the owner of the website stated that they had been locked out of their administrator account. The end users' computers were compromised as a result of the malicious file's execution. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Two-factor authentication (2FA) is one security measure that the team intends to implement to defend against brute force attacks. Users will be required to confirm a one-time password (OTP) sent to their email or mobile device as part of this two-factor authentication plan. The user will have access to the system once they verify their identity using the OTP and login credentials. Any noxious entertainer that endeavors a beast force  assault won't almost certainly get close enough to the framework since it requires extra  approval. |