Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol involved in the incident is the Hypertext transfer protocol (HTTP).  Since the issue was with accessing the web server for  yummyrecipesforme.com, we know that requests to web servers for web  pages involve http traffic. Also, when we ran tcpdump and accessed the  yummyrecipesforme.com website, the corresponding tcpdump log file showed  the usage of the http protocol when contacting it . The malicious file is  observed being transported to the users’ computers using the HTTP protocol  at the application layer. |
|  |

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers contacted the website’s helpdesk stating that when they visited  the website, they were prompted to download and run a file that contained access to  new recipes. Their personal computers have been operating slowly ever since. The  website owner tried logging into the web server but noticed they were locked out of  their account.  The cybersecurity analyst used a sandbox environment to open the website without  impacting the company network. Then, the analyst ran tcpdump to capture the  network traffic packets produced by interacting with the website. The analyst was  prompted to download a file claiming it would provide access to free recipes,  accepted the download and ran it. The browser then redirected the analyst to a fake  website (greatrecipesforme.com).  The cybersecurity analyst inspected the tcpdump log and observed that the browser  initially requested the IP address for the yummyrecipesforme.com website. Once the  connection with the website was established over the HTTP protocol, the analyst  recalled downloading and executing the file. The logs showed a sudden change in  network traffic as the browser requested a new IP address for the  greatrecipesforme.com URL. The network traffic was then rerouted to the new IP  address for the greatrecipesforme.com website.  The senior cybersecurity professional analyzed the source code for the websites and  the downloaded file. The analyst discovered that an attacker had manipulated the  website to add code 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** |
| One security measure the team plans to implement to protect against brute force  attacks is to disallow previous passwords from being used. Since the vulnerability  that led to this attack was the attacker’s ability to use a default password to log in, it’s  important that we prevent any old passwords such as default passwords from being  used to reset the password. Another supportive measure is to require longer  passwords. Passwords that are 15 characters or longer offer greater protection  against brute force attacks. Finally, another helpful solution is to implement  two-factor authentication (2FA). 2FA requires authentication via a password and also  by confirming a one-time passcode (OTP) sent to either their email or phone. Once  the user confirms their identity through their login credentials and the OTP, they will  gain access to the system. Any malicious actor that attempts a brute force attack will  not likely gain access to the system because it requires additional authentication. |