# 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), in which, the malware uploaded to the websites source code was transferred to connected devices using HTTP. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Some customers notified the website owner that the website prompted and installed software on their computer, and that their computers have been running slower ever since. The owner then tried to login to his website to see what was going on, and was promptly locked out of their account.  The cybersecurity analyst then simulated a sandbox environment to test the website, and found that the website would prompt the user to update their browser, so they said yes and download the file – which redirected them to a replica fake page greatrecipesforme.com. The analyst then inspected the tcpdump logs and found that browser first requested the IP address of yummyrecipesforme.com – then, using the HTTP protocol the analyst installed and executed a file. At that point, according to the logs, there was a shift in network traffic, and the browser instead requested in the IP for greatrecipesforme.com.  The team has determined that most likely the attack was caused by a brute force attack to gain and change access to the websites admin account, to which they setup a script for malicious software to be installed when users visited the page and accepted a fake update prompt. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| More extensive and tight password policies would certainly help, as well as the implementation of two-factor authentication as a technical security control. The 2FA can be a one time code, sent to the users authorized email/phone, used to confirm their identity and/or access permissions. This will certainly aid against brute force attacks by reducing the attack surface area by promoting more complex passwords and secure access. |