# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol impacted in the incident is Hypertext transfer protocol (HTTP).  Running tcpdump and accessing the website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users’ computers using the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Our customers brought to our attention that our website was giving them a prompt to download a file to update their browser. Following that, their computers started working slowly, and they would be taken to another site.  The website owner tried logging into the web server but noticed they were locked out of their account.  That prompted an investigation, where we replicated the scenario in a sand-box environment, and used tcpdump to read/capture data packets. Once we downloaded the file, it redirected us to a fake website.  Our logs reported that after the browser initially requested the IP address for our website. After the connection was acknowledged over the HTTP protocol, that prompted our machine to download malware. Once our virtual machine was infected, our DNS resolution request re-directed to a malicious page. 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** |
| The implementation of 2FA is strongly suggested. The 2FA will plan will send a text or email code to verify the user’s identity to access the system. Which will deter most malicious actors. |