# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The Protocol involved in this incident was HTTP. This protocol was used to download and deliver malicious software when users visited a specific website as "yummyrecipesforme.com". When the user visited this particular website , it automatically redirects to a fake website "greatrecipesforme.com" once the malicious code was execute | |
|

| **Section 2: Document the incident** |
| --- |
| To analyze this behavior, a sandbox environment was created to observe the suspicious website behavior. The tool used to analyze this behavior was tcpdump  At 14:18:32.192571 was the first time to visit the website requesting to DNS server a specific domain. At 14:18:32.204388 DNS server sent back the acknowledge of google domain. Everything changed once we tried to visit the website "yummyrecipesforme.com" at 14:18:36.786517 was the first intent to access. A suspicious activity in this observation was at 14:18:36.786589 when a HTTP GET method request was sent. This was the start of the malware when it was executed. After this event happened , there the domain name was switched and our source IP was redirected to another destination.  At 14:25:29.576510 "greatrecipesforme.com" was redirected to the website we visited. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| One effective implementation is Multi Factor authentication (MFA) which is very important in case of bruce force attacks. This will help to authenticate the user’s permission by adding a extra layer of security by requiring something that you know, you have, you are. This action will improve security and reduces the chances of getting into the network even though the attacker guessed the password. It will a good help for the organization and employees for security purposes. |