# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| After analyzing the tcpdump logs, HTTP and DNS are two main protocols, which are Involved in the process. Both protocols reside in Application layer, Whereas for communication TCP is utilized. | |
|

| **Section 2: Document the incident** |
| --- |
| At first, I set up my sandbox for malware behavior analysis, then I turned on my network analysis protocol, which in this case was Tcpdump. I processed with visiting the website, downloading the prompted update requirement and suddenly redirecting to a malware website. Later I analyze logs taken during the process, which also act as evidence for this documentation. The following were the insight from logs-  At 14:18 my machine sended a dns query using port number “52444” for domain “yummyrecipesforme.com” to google domain name server(dns.google.domain) with a query id “35084”, “+” indicating a standard query and mentioning “A?” for A record for the given domain which is used to obtain IPv4 address associated with a domain name.  At same time I got a response back from dns mentioning the requested ip address, which in this case was “203.0.113.22. Almost the same time, with a matter of seconds, my machine initiated a tcp handshake with “yummyrecipesforme” website from its port number “36086” to server port number “80” which represents http protocol, using the domain ip address, resulting in a successful connection. After successful connection, my machine quickly sended a GET HTTP request using HTTP version 1.1 and utilizing the same port number as tcp handshake. this sudden GET request indicates a request for a file from the server to download it on my machine. After 2 minutes of communication on port 80, I noticed a different dns query request using my machine port number “5244” with query id “21899” for greatrecipesforme.com on its port “80”, This reflect the aftermath of file download and the browser redirecting to malicious site, it does so after requesting ip address from dns server. The Ip address for “greatrecipesforme” was “192.0.2.17”.  At 14:25:29 tcp connection process began with the same port numbers used in dns resolution, followed by a HTTP GET request in a matter of seconds, generally indicating malware begin download on my machine. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Brute force attacks are common attack vectors, in a sense , that username and password are the first inline defense and easy attack surface, It is very important to harden security measures concerning this. The following are few but powerful remediation that can be implement against brute force attacks-  Enforcing two-factor authentication (2FA), updating password policies for stronger passwords, monitoring login attempts and disallowing previous passwords from being used. |