# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| Network protocol impacted is TCP over HTTP at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers complained that their traffic was being directed to another website that prompted them to download a file to update their browsers. Once the executable file was run their PS started running slowly.  A tcpdump reveals the client device communicates with the DNS, it responds with the details of the yummyrecipesforme.com IP (203.0.113.22). The next request from the client device goes to the company website(yummyrecipesforme.com) and the three-way handshake is completed and connection established. After this the client requests data from the site VIA a GET request. Upon fulfilling this request by the website, the client contacts the DNS again which then redirects the client to another website(greatrecipesforme.com). Communication then continues with this website. See log details below:  ***14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1***  ***14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 0***  ***…<a lot of traffic on the port 80>...***  ***14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24)***  ***14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A 192.0.2.17 (40)***  ***14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649 ecr 0,nop,wscale 7], length 0***  ***14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS val 3302989649 ecr 3302989649,nop,wscale 7], length 0*** |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| MFA should be made a default security feature for all logins. |