Security incident report

Section 1: Identify the network protocol involved in the incident
HTTP (HyperText Transfer Protocol) is the main network protocol involved in the incident. The logs show an HTTP GET request (GET / HTTP/1.1) sent from the local machine to the domain yummyrecipesforme.com. Prior to the request, DNS resolution is used to obtain the IP address of the server. After the initial interaction, the website redirects the user to greatrecipesforme.com, which is identified as the malicious domain. This redirection and subsequent traffic over port 80 confirm the use of HTTP over TCP/IP.

Section 2: Document the incident
After several customers emailed yummyrecipesforme's helpdesk, claiming that the company's website had prompted them to download a file to access free recipes and, after running the file, the address of the website changed and their personal computers began running more slowly. The IT team tried to access the admin panel but they were unable to, so they contacted the hosting provider to disable the server. Then, a sandbox provider and tcpdump were used to test the website behavior, and analyze the logs of the protocols used. As soon as the website loads, the user is prompted to download an executable file to update your browser, and by downloading and accepting the file to run, the browser redirects to a different URL, greatrecipesforme.com, which contains the malware. The logs show this behaviour in the next section: 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

Section 3: Recommend one remediation for brute force attacks
To mitigate brute force attacks, it is essential to enforce strong password policies and change default credentials immediately after deployment. The admin user should use a complex, unique password combining uppercase, lowercase, numbers, and symbols. Additionally, implementing two-factor authentication (2FA) provides an extra layer of protection, making it significantly harder for attackers to gain unauthorized access even if they obtain valid credentials.