Security incident report

Section 1: Network Protocol Involved in the Incident
The network protocol impacted in the incident was Hypertext Transfer Protocol (HTTP). By running tcpdump and accessing the yummyrecipesforme.com website, the analyst was able to capture the DNS and HTTP traffic logs, which revealed that the malicious file was being transmitted to users' computers using the HTTP protocol at the application layer.

Section 2: Incident Documentation
Multiple customers reported being prompted to download a file when visiting the website, claiming it was an update for their browsers. After running the file, their personal computers started experiencing slow performance. The website owner attempted to log into the web server but was locked out of their account. To investigate, a cybersecurity analyst created a sandbox environment and used tcpdump to capture network and protocol traffic while interacting with the website. During the analysis, the analyst accepted and executed the file, resulting in a browser redirection to a fake website (greatrecipesforme.com) that closely resembled the original site (yummyrecipesforme.com). Analyzing the tcpdump log revealed that the browser initially requested the IP address for yummyrecipesforme.com. Once the connection was established via the HTTP protocol, the analyst downloaded and executed the file. Subsequently, the browser requested a new IP resolution for the greatrecipesforme.com URL, and the network traffic was redirected to the new IP address. Further examination of the source code for both websites and the downloaded file revealed that the attacker had added code to prompt users to download a malicious file disguised as a browser update. The website owner's inability to access their administrator account suggested that the attacker gained unauthorized access through a brute force attack, compromising the end users' computers.

Section 3: Recommended Remediation for the Brute Force Attacks
To mitigate future brute force attacks, the recommended security measure is the implementation of two-factor authentication (2FA). This approach adds an additional layer of security by requiring users to verify their identity through a one-time password (OTP) sent to their email or phone. Users would need to provide their login credentials along with the OTP to gain access to the system. This added authentication step significantly reduces the likelihood of a successful brute force attack since it requires an extra level of authorization.

DNS & HTTP traffic log

```
14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?
yummyrecipesforme.com. (24)
14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A
203.0.113.22 (40)


14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859
ecr 0,nop,wscale 7], length 0
14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags
[S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS
val 3302576859 ecr 3302576859,nop,wscale 7], length 0
14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],
length 0
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
14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags
[P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr
3302989649], length 73: HTTP: GET / HTTP/1.1
14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags
[.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],
length 0
…<a lot of traffic on the port 80>...
```