Security Incident Report

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>...
```

Section 1: Identify the network protocol involved in the incident
Incident involves HTTP protocol, based on log files (HTTP: GET / HTTP/1.1 shows the browser is requesting data from yummyrecipesforme.com with HTTP:GET method using HTTP protocol version 1.1). This could potentially be a download request for a malicious file done at the application layer of the TCP/IP model. After the user downloads and runs the file, logs show the user's browser sends a new request to the DNS server to retrieve IP address for different URL: greatrecipesforme.com.

Section 2: Document the incident
Customers contact the website's helpdesk stating they were prompted to download a file to access free recipes. After running the downloaded file, the address of the website changed (i.e. from yummyrecipesforme.com to greatrecipesforme.com) and their PCs began to run more slowly. Also, the website owner reported that they were locked out of their account. To address this, a sandbox environment was run to observe suspicious website behavior and tcpdump was run to reproduce the issue. Browser initially requested IP address for yummyrecipesforme.com. However, after downloading and executing the file on the website, logs showed a change in network traffic as the browser now requested a new IP address for greatrecipesforme.com, which network traffic was routed to. Source code was analyzed and it was discovered that an attacker manipulated the website to prompt the user to download the malicious file, compromising users' computers. Additionally, an attacker may have brute forced access into account to change the admin password.

Section 3: Recommend one remediation for brute force attacks
In order to prevent this in the future, a security measure that can be implemented is MFA or multi-factor authentication and ensuring use of longer passwords to prevent brute force attacks.