**Security Incident Report**

**Section 1: Identify the Network Protocol Involved in the Incident**

The protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). This is evidenced by the traffic logs which show HTTP requests made to both the compromised website (yummyrecipesforme.com) and the malicious redirect (greatrecipesforme.com). HTTP was used to transmit the malicious file and redirect users to the fake website.

**Section 2: Document the Incident**

**Incident Overview:** Several customers of yummyrecipesforme.com reported being prompted to download a file to access free recipes. After running the file, their computers became slow and the website address changed to greatrecipesforme.com. The website owner was unable to log in to the admin panel and contacted the web hosting provider for assistance. The cybersecurity team was tasked with investigating the incident.

**Incident Timeline:**

1. **Initial DNS Request for yummyrecipesforme.com:**
   * 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)
2. **HTTP Request to yummyrecipesforme.com:**
   * 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 [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859], length 73: HTTP: GET / HTTP/1.1
   * <...lots of traffic on port 80...>
3. **DNS Request for greatrecipesforme.com:**
   * 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)
4. **HTTP Request to greatrecipesforme.com:**
   * 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 [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649], length 73: HTTP: GET / HTTP/1.1
   * <...lots of traffic on port 80...>

**Attack Details:**

* A former employee executed a brute force attack to gain access to the web host's administrative account by guessing the default password.
* After gaining access, the attacker modified the website's source code to include a JavaScript function that prompted visitors to download and run a malicious file.
* This malicious file redirected users to a fake website (greatrecipesforme.com) containing malware.

**Analysis:**

* The incident was confirmed by observing the behavior in a sandbox environment and analyzing the tcpdump logs.
* The logs show HTTP requests to the legitimate and fake websites, indicating the use of HTTP for delivering the malicious payload.
* The senior analyst confirmed the malicious JavaScript code and identified the brute force attack as the method of compromise.

**Section 3: Recommend One Remediation for Brute Force Attacks**

**Recommended Security Measures:**

1. **Implement Multi-Factor Authentication (MFA):**
   * Requires additional verification steps, making it more difficult for attackers to gain unauthorized access even if they obtain the password.
2. **Disallow Previous Passwords:**
   * Prevents the use of default or old passwords during password resets, reducing the risk of successful brute force attacks.
3. **Frequent Password Updates:**
   * Regularly updating passwords limits the window of opportunity for attackers to exploit compromised credentials.

By implementing these security measures, the risk of brute force attacks and similar incidents can be significantly reduced, enhancing the overall security posture of the web host and protecting users from malicious activities.

4o