# Security incident report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| The protocol involved in this incident is the Hypertext Transfer Protocol (HTTP). Since the issue pertained to accessing the web server for yummyrecipesforme.com, it is evident that web server requests for webpages involve HTTP traffic. Additionally, during the tcpdump analysis, when accessing the yummyrecipesforme.com website, the corresponding tcpdump log confirmed the use of the HTTP protocol for communication with the server. The malicious file was observed being delivered to users' computers via the HTTP protocol at the application layer. |

| Section 2: Document the incident |
| --- |
| The company has received numerous incident reports indicating that after downloading a file containing free recipes from the main website (yummyrecipesforme.com), users are being redirected to an unknown site (greatrecipesforme.com). Subsequently, users have reported noticeable decreases in their computers' performance.<br><br>In an effort to investigate, the website owner attempted to log in to the admin console of their hosting platform but was denied access. After regaining access through their cloud service provider (CSP), the website owner contacted our Incident Response (IR) team for assistance.<br><br>With the client's authorization, the domain was placed in maintenance mode to prevent further impact on website visitors. A Virtual Machine (VM) environment was established to monitor and analyze the behavior of the compromised domain.<br><br>The IR team set up a network analyzer, **tcpdump**, to capture traffic generated when visiting the affected website. At 14:18:32, DNS successfully resolved the |

domain, and we accessed yummyrecipesforme.com using our IP address and port 52444. A connection was established between our IP and the client's website via port 36086 at 14:18:36.786517. Shortly after accessing the site, a GET request initiated at 14:18:36.786589 triggered a file download over port 80 at 14:18:36.786595. Approximately two minutes later, the browser was redirected to greatrecipesforme.com via port 56378. Similar to the initial interaction with yummyrecipesforme.com, a GET request was issued, leading to the download of another malicious file.

The IR team reviewed the source code of the website and the downloaded file. The analysis revealed that an attacker had altered the website's code to prompt users to download a malicious file disguised as a browser update. Since the website owner reported being locked out of their administrator account, the team suspects that the attacker used a brute force attack to gain access and reset the admin password. The execution of the malicious file subsequently compromised the computers of end users.

**Section 3: Recommend one remediation for brute force attacks**

To mitigate future brute force attacks, it is strongly advised to implement an account lockout policy. This policy should define an appropriate threshold, such as a maximum of five failed login attempts, the time frame within which these attempts occur, and a lockout duration. Introducing random intervals for the lockout period can further deter the use of automated tools. Additionally, implementing a CAPTCHA can provide an added layer of protection.

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>...