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). Since the issue was with accessing the web server for yummyrecipesforme.com, we know that requests to web servers for web pages involve http traffic. Also, when we ran tcpdump and accessed the yummyrecipesforme.com website the corresponding tcpdump log file showed the usage of the http protocol when contacting the . The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

Section 2: Document the incident
The first section of the DNS & HTTP traffic log file shows the source computer (your.machine.52444) using port 52444 to send a DNS resolution request to the DNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL (203.0.113.22). The next section shows the source computer sending a connection request (Flags [S]) from the source computer (your.machine.36086) using port 36086 directly to the destination (yummyrecipesforme.com.http). The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (14:18) and the next DNS resolution request (see below for the 14:20 timestamp). The log entry with the code HTTP: GET / HTTP/1.1 shows the browser is

requesting data from
yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. This
could be the download request for the malicious file.
Then, a sudden change happens in the logs. The traffic is routed from the source computer to
the DNS server again using port .52444 (your.machine.52444 > dns.google.domain) to make
another DNS resolution request. This time, the DNS server routes the traffic to a new IP
address (192.0.2.172) and its associated URL (greatrecipesforme.com.http). The traffic
changes to a route between the source computer and the spoofed website (outgoing traffic:
IP your.machine.56378 > greatrecipesforme.com.http and incoming traffic:
greatrecipesforme.com.http > IP your.machine.56378). Note that the port number (.56378)
on the source computer has changed again when redirected to a new website.

Section 3: Recommend one remediation for brute force attacks
The owner will need to implement MFA in the future to prevent a brute force attack.