Security Incident Report Based on TCPDump 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

14:18:36.786589 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**

**14:20**: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 **192.0.2.172** (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

**Section 1: Identify the network protocol involved in the incident**

The incident protocol in question is the Hypertext Transfer Protocol (HTTP). Given the issue with accessing the web server for yummyrecipesforme.com, we can confirm that requests to web servers for web pages involve HTTP traffic. Additionally, when we ran tcpdump and accessed the yummyrecipesforme.com website, the corresponding tcpdump log file indicated the use of the HTTP protocol. The malicious file was seen being transferred to users' computers using HTTP at the application layer.

* The tcpdump log reveals that a request is sent to the DNS server to resolve the IP address for the yummyrecipesforme.com URL. The DNS server responds with the correct IP address, which the browser then uses to direct users to the correct website.
* According to the scenario, when the website loads, a function prompts users to download a file to access free recipes. Both the scenario and the logs show that this activity occurs over the HTTP protocol.
* After the user downloads and runs the file, the logs indicate that the user’s browser sends a new request to the DNS server to obtain the IP address for a different URL: greatrecipesforme.com. The DNS server responds with the IP address, and the users are redirected to this new website via HTTP.

**Section 2: Document the Incident**

Several customers contacted the website’s helpdesk, reporting that when they visited the site, they were prompted to download and run a file to access new recipes. Since then, their personal computers have been running slowly. The website owner attempted to log into the web server but found they were locked out of their account.

The cybersecurity analyst utilized a sandbox environment to access the website without affecting the company network. Using tcpdump, the analyst captured the network traffic generated by interacting with the site. When prompted to download a file offering free recipes, the analyst accepted the download and executed it. Subsequently, the browser redirected the analyst to a fake website (greatrecipesforme.com).

The cybersecurity analyst reviewed the tcpdump log and noted that the browser initially requested the IP address for the yummyrecipesforme.com website. After establishing a connection over the HTTP protocol, the analyst downloaded and executed the file. The logs revealed a sudden shift in network traffic as the browser requested a new IP address for the greatrecipesforme.com URL, redirecting the traffic to the new IP address associated with the greatrecipesforme.com website.

The senior cybersecurity professional examined the source code for the websites and the downloaded file. The analysis revealed that an attacker had modified the website to include code prompting users to download a malicious file disguised as a browser update. Given that the website owner reported being locked out of their administrator account, the team suspects the attacker used a brute force attack to gain access and change the admin password. The execution of the malicious file subsequently compromised the end users' computers.

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

To protect against brute force attacks, several security measures need to be implemented. One key measure is to prevent the reuse of previous passwords. Since the attack exploited the use of a default password, it's crucial to ensure that old or default passwords cannot be used for resetting passwords. Additionally, requiring more frequent password updates will reduce the risk of unauthorized access, as any compromised passwords will be invalidated sooner. Another effective solution is implementing two-factor authentication (2FA), which requires both a password and a one-time passcode (OTP) sent to the user's email or phone. This ensures that even if an attacker manages to obtain the password, they still need the OTP to gain access, significantly reducing the likelihood of a successful brute force attack.