Security Incident Report: Yummy Recipes

Section 1: Identification of the Network Protocol Involved in the Incident

The incident primarily impacted the Hypertext Transfer Protocol (HTTP). Through the utilization of tcpdump and accessing the yummyrecipesforme.com website, the investigation aimed to identify the problem and capture protocol and traffic activity in the DNS and HTTP traffic log files. The logs revealed that a malicious file was being delivered to users' computers using the HTTP protocol at the application layer.

Section 2: Incident Documentation

Several customers reported contacting the website owner, stating that upon visiting the website, they were prompted to download and run a file that appeared to be a browser update. As a result, their personal computers began operating slowly. The website owner attempted to log into the web server but discovered that they were locked out of their account.

To investigate the incident, a cybersecurity analyst utilized a sandbox environment to test the website without impacting the company network. By running tcpdump, the analyst captured network and protocol traffic packets generated by interacting with the website. During the analysis, the analyst encountered a file download prompt claiming to update the browser. Accepting the download and executing the file resulted in the browser redirecting to a fake website (greatrecipesforme.com) that closely resembled the original site (yummyrecipesforme.com).

Upon inspecting the tcpdump log, the cybersecurity analyst observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. Notably, the logs indicated a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. Subsequently, the network traffic was rerouted to the new IP address associated with the greatrecipesforme.com website.

A senior cybersecurity professional further examined the source code for both websites and the downloaded file. It was discovered that an attacker had manipulated the website by adding code that prompted users to download a malicious file disguised as a browser update. Additionally, since the website owner reported being locked out of their administrator account, the team suspects that the attacker gained access through a brute force attack, subsequently changing the admin password. The execution of the malicious file compromised the end users' computers.

Section 3: Recommendation for Brute Force Attack Mitigation

To enhance security and mitigate the risk of brute force attacks, the team plans to implement two-factor authentication (2FA). This 2FA solution will require users to provide additional verification of their identity by confirming a one-time password (OTP) sent to either their email or phone. Users will need to enter their login credentials along with the OTP to gain access to the system. This additional layer of authorization significantly reduces the likelihood of malicious actors successfully executing brute force attacks against the system.

DNS and HTTP 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
14:18:36.786529 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>...