# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| TCP: allows two devices to form a connection and stream data, it isn’t limited to two devices, it established a direct connection between two endpoints but the underlying network infrastructure can handle routing data packets across multiple devices. DNS: translates internet domain names into IP addresses. HTTP: provides a method of communication between clients and website servers, it doesn’t use encryption. The issue was with accessing the web server for yummyrecipesforme.com we know that requests to web servers for web pages involve https traffic. The tcpdump logs showed the usage of the http protocol when contacting the malicious file via application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Multiple customers emailed yummyrecipesforme complaining about our website, because in order to get in they had to download a file to access free recipes. After running the file, the address of the website changed and their personal computers began running more slowly.  The IT team used a sandbox environment to open the website without touching the company network. Then, we ran tcpdump to look up all the network traffic packets produced by interacting with the website. We downloaded the file claiming it would provide acces to free recipes and we were redirected to the fake website.  The tcpdump logs show that the source computer (your.machine.52444) sends a DNS resolution via 52444 port to the dNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com). Then reply comes back with the IP address of the destination URL (203.0.113.22).  Next, the source computer sends a connection request directly to the destination, the reply shows that it acknowledges the received connection and it continues for about 2 minutes. Then, the logs show that the browser is requesting data from yummyrecipesforme.com using HTTP, here is where the download request appears with the malicious file.  From now on the logs change completely, there is an unusual request from the source computer to the DNS server to make another DNS request but to a different IP address of the destination URL (192.0.2.17) that redirects the traffic to greatrecipesforme.com instead of yummyrecipesforme.com. We discovered that the attacker manipulated the website adding javascript code that prompted the users to download a malicious file disguised as a browser update. The attacker used a brute force attack to access the account and change the admin password due to the fact that they have been locked out of their administrator account. The execution of the malicious file compromised the end users’ computers. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Improve the firewall, use HTTPS, create an intrusion detection system (IDS), require multi-factor authentication, implementing strict password policies (longer and more complex), disallow previous passwords from being used, lock user accounts if they fail numerous login attempts, limit access to particular resources for workers, hashing (to convert info into a unique value that can be used to determine its integrity) and salting (adds random characters to hashed passwords). |