# Security incident report submitted by Junior SOC Analyst M.Murtaza

|  |
| --- |
| **The network protocol involved in the incident** |
| The protocol involved in the incident is the Hypertext Transfer Protocol (HTTP). Since the issue pertained to accessing the web server for yummyrecipesforme.com, it's evident that HTTP traffic was involved, as it is the standard protocol for web page requests. Additionally, when we ran tcpdump while accessing the website, the corresponding log file confirmed HTTP traffic activity during communication with the server. The malicious file was observed being delivered to users' systems via the HTTP protocol at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers reported to the website’s helpdesk that upon visiting the site, they were prompted to download and run a file offering access to new recipes. After doing so, their personal computers began to operate unusually slow. When the website owner attempted to log into the web server, they found themselves locked out of their administrator account.  To investigate the incident safely, a cybersecurity analyst used a sandbox environment to interact with the website and ran tcpdump to capture the network traffic. During this test, the analyst was prompted to download a file that claimed to provide free recipes. Upon executing the file, the browser was redirected to a suspicious website: *greatrecipesforme.com*.  The tcpdump log showed that the browser first requested the IP address for *yummyrecipesforme.com*. Once the connection was established over the HTTP protocol and the malicious file was executed, the logs recorded a shift in traffic, with the browser requesting a new IP for *greatrecipesforme.com*, effectively redirecting the session.  A senior cybersecurity professional later analyzed the source code of both the websites and the downloaded file. It was revealed that an attacker had injected malicious code into the original website, disguising the file as a browser update. Given that the website owner was locked out, the team suspects a brute-force attack was used to compromise the admin account and change the credentials. Execution of the malicious file led to the compromise of the end users’ systems. |

|  |
| --- |
| **Recommended remediation for brute force attacks** |
| To protect against future brute force attacks, the security team plans to implement several key measures. First, users will be prevented from reusing previous passwords, especially default passwords, which were exploited in this incident. Enforcing unique and strong new passwords helps mitigate this vulnerability. Second, the team will require all passwords to be at least 15 characters long, as longer passwords significantly increase resistance to brute force attempts. Lastly, the implementation of two-factor authentication (2FA) will add an extra layer of security. With 2FA, users must verify their identity not only through their password but also by entering a one-time passcode (OTP) sent to their registered email or phone. This additional step greatly reduces the chances of unauthorized access, even if a password is compromised. |