# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident is HTTP (Hyper-Text Transfer Protocol). Running the tcpdump network protocol analyzer tool and attempting to reach the website yummyrecipesforme.com detected the problem, captured protocol, and traffic activity in a DNS and HTTP log to provide the necessary information to reach this conclusion. The malicious file is shown being transported to the user’s computer through HTTP at the application layer. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Multiple customers contacted yummyrecipesforme’s helpdesk and notified them that the file they were prompted to download from the website changed the web address and slowed down their computers. The website owner tried logging into the admin panel but was unable to do so, and reached out the website hosting provider.  The cybersecurity analyst created a sandbox environment to observe the suspicious website behavior. The analyst ran the network protocol analyzer tcpdump, and then attempted to browse the yummyrecipesforme website. When the website loads, it prompted the analyst to download an .EXE file to update the browser. The analyst accepted the download and ran the file. After running, the browser was then directed to a different URL, greatrecipesforme.com, which retains the original website’s design, but now the recipes are available for free rather than purchase.  The analyst inspected the tcpdump log and observed the browser initially requesting the IP address for yummyrecipesforme.com. Once the connection was established over HTTP, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffics was then rerouted to the new IP address for greatrecipesforme.com’s website.  The analyst inspected the source code for the websites and the downloaded file. He discovered that the website had been manipulated by a malicious actor who injected new code that prompted the users to download a file disguised as a browser update. Since the website owner stated that they were locked out of their admin account, the team believes that the attacker used a brute force attack to access the account and change the admin password. Running the file compromised end users’ computers. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One solution to defend and prevent an attack like this from happening again is to implement multifactor authentication (MFA) or two-factor authentication (2FA). By doing this, we can create a multi-step process in order to access sensitive information/restricted areas within a system. With the authentication process, we can have the system admin enter their login credentials, and then have a unique code sent to their phone/email to verify their identity and help protect against malicious actors since a brute force attack will very likely be unsuccessful due to additional authorization. |