# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| Tcpdump identified the HTTP protocol as the impacted protocol when connecting to greatrecipesforme.com. A malicious file is observed being downloaded from the destination computer by the source computer. | |
|

| **Section 2: Document the incident** |
| --- |
| The incident was first reported on 06/05/23 when multiple customers contacted the helpdesk via e-mail to report the website yummyrecipesforme.com was prompting them to download a file, was redirecting them to a different website, and that their computers were running slowly.  The network security team created a sandbox environment and accessed yummyrecipesforme.com from within. Upon connecting, the website prompted the user to download and run a file. The website stated the file was an update for the user’s browser. The network team allowed the file to be downloaded and run.  Afterward, when attempting to connect to yummyrecipesforme.com, the browser was redirected to greatrecipesforme.com. Greatrecipesforme.com appears to be a copy of yummyrecipesforme.com.  The packet sniffer tcpdump was ran during the connection attempt in the sandbox environment. The source computer initially requested a DNS lookup for yummyrecipesforme.com and received the correct information. After downloading and running the file, subsequent DNS lookups provided the wrong information directing visitors to greatrecipesforme.com.  The website administrator was contacted. The admin attempted to log in to the website control panel and found that he was locked out. It was later determined the account was using the default password for that particular software. An analyst examined the code on yummyrecipesforme.com and determined a malicious javascript file was prompting visitors to download a file under the guise of updating their browser. The file would then compromise the user’s computer if ran and redirect subsequent visits to yummyrecipesforme.com to greatrecipesforme.com. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Password policies should be reviewed to ensure they are following best practices. All systems using password authentication should be reviewed to ensure they are not using default passwords and are compliant with password best practices. Additionally, it is recommended to enable MFA/2FA authentication for accounts. In the future, should a password become compromised for any reason, it will not allow access to the account without the additional authentication method(s). |