# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| DNS (Domain Name System): Used to resolved domain names ([yummyrecipesforme.com](http://yummyrecipesforme.com)) into IP address   HTTP (Hypertext Transfer Protocol) Used by the browser to request web pages from both domains and download the malicious file. | |
|

| **Section 2: Document the incident** |
| --- |
| Security team were made aware of an incident where owner of [yummyrecipesforme.com](http://yummyrecipesforme.com) stated they’ve been receiving complaints from customers that are being redirected to [greatrecipesforme.com](http://greatrecipesforme.com). They are then being prompted to download a free recipe, and after opening it they complain of their devices slowing down. The owner also stated that having been altered to this, they attempted to log into their admin panel and were unable to.  The responding team created a sandbox envirioemnt and ran network protocol analyser tcpdump, and visited [www.yummyrecipesforme.com](http://www.yummyrecipesforme.com). The website prompts the user to download a free recipe. The file was executed and the browser then redirects to a malicious domain, [www.greatreciesforme.com](http://www.greatreciesforme.com) where additional malware was hosted.   Network logs confirmed the following sequence:  Browser issued a DNS request for yummyrecipesforme.com.  DNS server returned the legitimate IP address.  Browser issued an HTTP request to retrieve the webpage.  Browser initiated download of the malicious executable.  Browser issued a DNS request for greatrecipesforme.com.  DNS server returned the IP address.  Browser issued an HTTP request to the malicious site.  The root cause was poor password security,retaining the default password and lack of safeguards against brute force attempts. The attacker also locked out legitimate administrators by resetting the admin password. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Enforce HTTPS-only connections with TLS and enable HSTS to ensure encrypted traffic.  Replace all default credentials with strong, unique passwords.  Implement multi-factor authentication (MFA) for all administrative accounts.  Configure account lockout policies and rate-limiting to prevent brute force attacks.  Apply regular security updates and patches to the web server and applications. |