# Brute Force Attack: Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| This was an application layer attack, targeting DNS and HTTP vulnerabilities to download malicious updates to the user’s browser. The malware redirected the user to a fake copy of yummyrecipesforme.com |
|

|  |
| --- |
| **Section 2: Document the incident** |
| A former employee of yummyrecipesforme.com executed a brute force attack on the administrative account of the webserver. Upon entry and obtaining the correct password, the attacker was able to access the admin panel and rights, allowing changes to the website’s source code. The attacker added a JavaScript function to the source code, prompting visitors to download a file to gain access to free recipes. Customers complained after running the downloaded file, they were redirected to a different website and their computers began to run noticeably slower.  The cybersecurity analyst team simulated the customers experience utilizing virtual machine (VM) sandbox and recorded the following:   1. Source computer browser directs DNS for yummyrecipesforme.com. 2. DNS replies to source computer with correct IP address. 3. Browser initiates HTTP request for yummyrecipesforme.com. 4. Browser initiates download of attacker’s malware. 5. Browser directs DNS for greatrecipesforme.com. 6. DNS server responds with new IP. 7. Browser initiates HTTP request to new IP. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| Upon investigation, the attacker gained access by using brute force attack methods and using previous default passwords that were already known. The best way to protect against brute force attacks is implementing organization wide strong password policies for both administrator and user accounts. In addition to a strong password policy, implement the following.   1. Failed login attempts: block specific IPs after too many failed attempts. 2. Require frequent user password updates using letters, numbers and special characters. 3. Update password requirements 4. Require Multi-Factor Authentication or 2-Factor Authentication (2FA)   A policy to strictly enforce would be to implement a failed password attempt limit. Once the number of failed attempts is reached, the specific IP is restricted. The attacker attempted to brute force with previously known passwords, without a limit restriction, allowing attempt until entry. |