# Security incident report

| Section 1: Identify the network protocol involved in the incident |
| --- |
| Hypertext Transfer Protocol (HTTP) was the network protocol involved in this incident.<br><br>By running tcpdump and visiting the yummyrecipesforme.com website, we were able to identify the issue and record information about the protocols and traffic in a DNS and HTTP log file.<br><br>This evidence led us to the conclusion that the malicious file was delivered to users' computers through the HTTP protocol at the application layer. |

| Section 2: Document the incident |
| --- |
| Numerous customers contacted the website owner reporting that when they visited the website, they were prompted to download and run a file which claimed to be a browser update. Following the download their personal computers began to operate sluggishly. The website owner attempted to log into the web server and soon discovered that he was locked out of their account.<br><br>To investigate the situation, we created a controlled testing environment (sandbox) to assess the website without affecting the corporate network. Using tcpdump, we captured network and protocol traffic packets generated during interactions with the website. We then accepted the prompt to download a file (allegedly for a browser update) and executed it. This action led the browser to redirect to an external website (greatrecipesforme.com), which was clearly created to closely resemble the original site (yummyrecipesforme.com) but with free access instead to the paid content on the original website.<br><br>Reviewing the tcpdump log, it became clear that the browser initially requested the IP address for the yummyrecipesforme.com website. After establishing a connection through the HTTP protocol, although after downloading and running the file, the logs indicated an abrupt change in |

network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL, resulting in network traffic being rerouted to the new IP address for the greatrecipesforme.com website.

The logs show the following process:

1. The browser requests a DNS resolution of the yummyrecipesforme.com URL.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request for the webpage.
4. The browser initiates the download of the malware.
5. The browser requests another DNS resolution for greatrecipesforme.com.
6. The DNS server responds with the new IP address.
7. The browser initiates an HTTP request to the new IP address.

An examination of the source code for both websites and the downloaded file revealed that an attacker had manipulated the website by incorporating code that prompted users to download a malicious file disguised as a browser update. Given the website owner's claim of being locked out of their administrator account, it is suspected that the attacker used a brute force attack to gain access to the account and change the admin password.

Consequently, the execution of the malicious file compromised the end users' computers.

| **Section 3: Recommend remediations for brute force attacks** |
| --- |
| To enhance security and guard against brute force attacks, the team is planning to implement two-factor authentication (2FA). This 2FA strategy will introduce an extra layer of security, necessitating users to verify their identity by confirming a one-time password (OTP) sent to either their email or phone. Once the user successfully authenticates their identity using their login credentials and the OTP, they will be granted access to the system. This added security step means that malicious actors attempting a brute force attack are unlikely to gain access to the system because it demands additional authorization.<br><br>Additionally, In response to being targeted, the team also intends to bolster the security of the admin panel. They plan to enforce a limit on the number of login |

attempts, helping prevent potential brute force attacks. By imposing a login attempt threshold, the system will temporarily lock out any user or attacker after a specified number of unsuccessful login tries. This proactive measure further safeguards the admin panel from unauthorized access attempts.

Moreover, going the extra mile, we are considering the adoption of CAPTCHA services for general login procedures throughout the website. By implementing CAPTCHA challenges, they aim to distinguish between legitimate users and automated scripts or bots. This additional layer of security can help prevent unauthorized access and protect the website from potential malicious activities.