# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| 1. DNS (Domain Name System): It is used for the browser's initial request for DNS resolution of the "yummyrecipesforme.com" and "greatrecipesforme.com" URLs. The DNS server replies with the correct IP addresses for both URLs. 2. HTTP (Hypertext Transfer Protocol): It is used for the browser's initiation of HTTP requests to retrieve webpages and initiate the download of malware. The browser initiates an HTTP request for the webpage and later initiates another HTTP request to the new IP address. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The incident was first discovered by multiple customers to the help desk who tried to access the website [www.yummyrecepiesforme.com](http://www.yummyrecepiesforme.com) but were then prompted to download a file and after it run their computers started to run slow. The website owner tries to log in to the admin panel but is unable to, that is when the owner reaches out to the hosting provider in which the security analysts load run the website in a sandbox environment and confirm what the customers were experiencing and how now the company’s recipes were posted on a new website for free. When the website is analyzed using the network analysis protocol, tcpdump, it showed that:   1. The DNS & HTTP traffic log file shows the source computer (your.machine.52444) using port 52444 to send a DNS resolution request to the DNS server (dns.google.domain) for the destination URL (yummyrecipesforme.com). Then the reply comes back from the DNS server to the source computer with the IP address of the destination URL (203.0.113.22). 2. The source computer sending a connection request (Flags [S]) from the source computer (your.machine.36086) using port 36086 directly to the destination (yummyrecipesforme.com.http). The .http suffix is the port number; http is commonly associated with port 80. The reply shows the destination acknowledging it received the connection request (Flags [S.]). 3. The log entry with the code HTTP: GET / HTTP/1.1 shows the browser is requesting data from yummyrecipesforme.com with the HTTP: GET method using HTTP protocol version 1.1. This could be the download request for the malicious file. 4. Then, a sudden change happens in the logs. The traffic is routed from the source computer to the DNS server again using port .52444 (your.machine.52444 > dns.google.domain) to make another DNS resolution request. This time, the DNS server routes the traffic to a new IP address (192.0.2.172) and its associated URL greatrecipesforme.com.http). The traffic changes to a route between the source computer and the spoofed website (outgoing traffic: IP your.machine.56378 > greatrecipesforme.com.http and incoming traffic: greatrecipesforme.com.http > IP your.machine.56378). Note that the port number (.56378) on the source computer has changed again when redirected to a new website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| To ensure the safety of the company’s assets in the future, an effective remediation to thwart future brute force attacks could be enforcing two-factor authentication (2FA). This way any login attempts to the would be monitored by one person, the owner, who would have the best interest for the success of the company. And other common security methods could be still bypasses, such as implementing strong password policies which could still be targeted by brute force attacks, but it would just take longer for the attacker to gain access, but there is still a possibility. Monitoring login attempts would just be a detective control in which it just provides the owner with information regarding if an incident has occurred or is ongoing, but it does nothing to prevent damage. And limiting the number of login attempts is a preventative control and still leaves it to chance that the attacker exhausts the number of login attempts. But 2FA gives control to the owner to allow or deny successful login attempts, in which it would also serve as a detective tool which could provide information on if someone is trying to login who hasn’t been previously authorized to. |