# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The network protocols involved in this attack were the DNS (domain name service) protocol and the HTTP (hypertext transfer protocol) protocol. The DNS protocol was used and manipulated to redirect traffic to the malicious site, [greatrecipesforme.com](http://greatrecipesforme.com), and HTTP was used maliciously to have visitors download the malware. | |
|

| **Section 2: Document the incident** |
| --- |
| A former employee or a hacker initiated this incident by accessing the administrative account on the webhost for [yummyrecipesforme.com](http://yummyrecipesforme.com) via a brute force attack. They obtained the login credentials by guessing previously known default passwords. The hacker then changed the website’s source code to automatically prompt visitors to download and run a file upon visiting the website. Then the hacker changed the password to the admin account.  Multiple customers then emailed the customer service helpdesk to complain about the website redirection and the file download making their computers run slowly. This is how the company was made aware of the attack.  Running the website in a sandbox environment, we found this is how the attack worked.  The browser initiates a DNS request for the IP address of [yummyrecipesforme.com](http://yummyrecipesforme.com) and DNS replies with the correct IP address 203.0.113.22. The port used was 52444  14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A?  yummyrecipesforme.com. (24)  14:18:32.204388 IP dns.google.domain > your.machine.52444: 35084 1/0/0 A  203.0.113.22 (40)  The browser then runs an HTTP request via port 80 to the site which is normal, however it initiates the malicious code placed by the hacker which begins the download of the malware.  14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: Flags  [S], seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859  ecr 0,nop,wscale 7], length 0  14:18:36.786517 IP yummyrecipesforme.com.http > your.machine.36086: Flags  [S.], seq 3984334959, ack 2873951609, win 65483, options [mss 65495,sackOK,TS  val 3302576859 ecr 3302576859,nop,wscale 7], length 0  14:18:36.786529 IP your.machine.36086 > yummyrecipesforme.com.http: Flags  [.], ack 1, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],  length 0  14:18:36.786589 IP your.machine.36086 > yummyrecipesforme.com.http: Flags  [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302576859 ecr  3302576859], length 73: HTTP: GET / HTTP/1.1  14:18:36.786595 IP yummyrecipesforme.com.http > your.machine.36086: Flags  [.], ack 74, win 512, options [nop,nop,TS val 3302576859 ecr 3302576859],  length 0  Then a new DNS request is initiated for [greatrecipesforme.com](http://greatrecipesforme.com), a malicious clone website. The DNS server responds with the IP address for the clone website via a new port, port 56378.  The browser initiates the HTTP request to the new website ip address for [greatrecipesforme.com](http://greatrecipesforme.com)  14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags  [S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649  ecr 0,nop,wscale 7], length 0  14:25:29.576510 IP greatrecipesforme.com.http > your.machine.56378: Flags  [S.], seq 1993648018, ack 1020702884, win 65483, options [mss 65495,sackOK,TS  val 3302989649 ecr 3302989649,nop,wscale 7], length 0  14:25:29.576524 IP your.machine.56378 > greatrecipesforme.com.http: Flags  [.], ack 1, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],  length 0  14:25:29.576590 IP your.machine.56378 > greatrecipesforme.com.http: Flags  [P.], seq 1:74, ack 1, win 512, options [nop,nop,TS val 3302989649 ecr  3302989649], length 73: HTTP: GET / HTTP/1.1  14:25:29.576597 IP greatrecipesforme.com.http > your.machine.56378: Flags  [.], ack 74, win 512, options [nop,nop,TS val 3302989649 ecr 3302989649],  length 0  At this point any visitor would have downloaded malicious malware to their computer. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| To avoid brute force attacks, it is recommended to disallow previous passwords from being used, which is exactly what happened in this situation. We recommend stronger password policies, more frequent password changes, limiting the number of login attempts, and even enforcing MFA or 2FA.  This will be very effective in preventing any of this to happen by never allowing the threat actor to even access the website’s administrative account. |