

# Security incident report

## Section 1: Identify the network protocol involved in the incident

The protocol impacted in the incident is Hypertext transfer protocol (HTTP). Running tcpdump and accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file is observed being transported to the users' computers using the HTTP protocol at the application layer.

## Section 2: Document the incident

Several customers contacted the website owner stating that when they visited the website, they were prompted to download and run a file that asked them to update their browsers. Their personal computers have been operating slowly ever since. The website owner tried logging into the web server but noticed they were locked out of their account.

The cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user's browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com).

The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address for the greatrecipesforme.com website. The senior cybersecurity professional analyzed the source code for the websites and the downloaded file. The analyst discovered that an attacker had

manipulated the website to add code that prompted the users to download a malicious file disguised as a browser update. Since the website owner stated that they had been locked out of their administrator account, the team believes the attacker used a brute force attack to access the account and change the admin password. The execution of the malicious file compromised the end users' computers.

### **Section 3: Recommend one remediation for brute force attacks**

One security measure the team plans to implement to protect against brute force attacks is two-factor authentication (2FA). This 2FA plan will include an additional requirement for users to validate their identification by confirming a one-time password (OTP) sent to either their email or phone. Once the user confirms their identity through their login credentials and the OTP, they will gain access to the system. Any malicious actor that attempts a brute force attack will not likely gain access to the system because it requires additional authorization.

# DNS & HTTP traffic log

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)

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

...<a lot of traffic on the port 80>...

14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A?  
greatrecipesforme.com. (24)

14:20:32.204388 IP dns.google.domain > your.machine.52444: 21899 1/0/0 A  
192.0.2.17 (40)

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  
...<a lot of traffic on the port 80>...