Cybersecurity Incident Report: OS Hardening

Scenario

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A disgruntled baker has decided to publish the website's best-selling recipes for the public to access for free. The baker executed a brute force attack to gain access to the web host. They repeatedly entered several known default passwords for the administrative account until they correctly guessed the right one. After they obtained the login credentials, they were able to access the admin panel and change the website's source code. They embedded a javascript function in the source code that prompted visitors to download and run a file upon visiting the website. After running the downloaded file, the customers are redirected to a fake version of the website where the seller's recipes are now available for free. Several hours after the attack, multiple customers emailed yummyrecipesforme's helpdesk. They complained that the company's website had prompted them to download a file to update their browsers. The customers claimed that, after running the file, the address of the website changed and their personal computers began running more slowly. In response to this incident, the website owner tries to log in to the admin panel but is unable to, so they reach out to the website hosting provider. You and other cybersecurity analysts are tasked with investigating this security event. To address the incident, you create a sandbox environment to observe the suspicious website behavior. You run the network protocol analyzer tcpdump, then type in the URL for the website, yummyrecipesforme.com. As soon as the website loads, you are prompted to download an executable file to update your browser. You accept the download and allow the file to run. You then observe that your browser redirects you to a different URL, greatrecipesforme.com, which is designed to look like the original site. However, the recipes your company sells are now posted for free on the new 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

A senior analyst confirms that the website was compromised. The analyst checks the source code for the website. They notice that javascript code had been added to prompt website visitors to download an executable file. Analysis of the downloaded file found a script that redirects the visitors' browsers from yummyrecipesforme.com to greatrecipesforme.com. The cybersecurity team reports that the web server was impacted by a brute force attack. The disgruntled baker was able to guess the password easily because the admin password was still set to the default password. Additionally, there were no controls in place to prevent a brute force attack. Your job is to document the incident in detail, including identifying the network protocols used to establish the connection between the user and the website. You should also recommend a security action to take to prevent brute force attacks in the future.

How to read DNS & HTTP Traffic log (Modified version)

No	Description
1	***14:18:32.192571*** *(A)* IP ***your.machine.52444*** *(B)* > ***dns.google.domain:*** *(C)* 35084+ A? ***yummyrecipesforme.com*** *(D)*. (24) A: Timestamps B: The source computer (IP your.machine) using port 52444 C: DNS server (dns.google.domain) D: The destination URL
2	14:18:32.204388 IP dns.google.domain > ***your.machine.52444***: *(E)* 35084 1/0/0 A 203.0.113.22 (40) E: Reply comes back from the DNS server to the source computer with the IP address of the destination URL of yummyrecipesforme.com (203.0.113.22).
3	TCP Flag codes include: Flags [S] - Connection Start Flags [F] - Connection Finish Flags [P] - Data Push Flags [R] - Connection Reset Flags [.] - Acknowledgment 14:18:36.786501 IP your.machine.36086 > yummyrecipesforme.com.http: ***Flags [S]*** *(F)*, seq 2873951608, win 65495, options [mss 65495,sackOK,TS val 3302576859 ecr 0,nop,wscale 7], length 0 F: The connection has been started.

Traffic Log:

Description
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 A203.0.113.22 (40)

Description

```
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 ecr3302576859], 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>...
```

Description

```
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 A192.0.2.17 (40)

14:25:29.576493 IP your.machine.56378 > greatrecipesforme.com.http: Flags[S], seq 1020702883, win 65495, options [mss 65495,sackOK,TS val 3302989649ecr 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,TSval 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
```

Description

```
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 ecr3302989649], 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>...
```

Respond:

Part 1 : Identify the network protocol involved in the incident

The protocol that got impacted is HTTP or commonly found in port 80. TCPdump detected the problem, captured the protocol and traffic activity in DNS (Port 53) and HTTP traffic log. Since the malicious file is being transported to users, this incident occurred at the application layer.

Part 2 : Document the incident

Several customers reported that when they visited the website, they were prompted/given one option: Download and run a file to update their browsers. Soon after, they were locked out of their account.

The security team used a sandbox to test the website in an isolated environment. They ran tcpdump to capture the network and protocol traffic packets when interacting with the website. They saw a prompt asking them to update the browser and ran it. Then, the fake website(greatreceipesforme.com) is generated and looks identical to the real one. (yummyrecipesforme.com).

Based on the logs, initially, the browser requested the IP address for yummyreceipesforme.com. Once the connection was established over the HTTP protocol, the prompt was to persuade the analyst to download and execute the file. After that, the logs showed a sudden change in network traffic as the new IP resolution for "websites" was generated.

When the senior team received this, he discovered the attack had manipulated the website to inject code that prompted users to download a malicious file disguised as a browser update. Since the administrator account was compromised, everyone's account was locked out. The team believed that it was a brute force attack. Now, the malicious file has spread to further damage other computers.

Part 3: Recommend one remediation for brute force attacks

2-factor authentication (2FA). One-time password OTP to either their email or phone. Once the user confirms their identity via credential and 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.