Security incident report

By Jovworie Tanshi

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst for yummyrecipesforme.com, a website that sells recipes and cookbooks. A former employee has decided to lure users to a fake website with malware.

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 embedding the malware, the baker changed the password to the administrative account. When customers download the file, they are redirected to a fake version of the website that contains the malware.

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 access free recipes. 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 contains the malware.

The logs show the following process:

1. The browser initiates a DNS request: It requests the IP address of the yummyrecipesforme.com URL from the DNS server.
2. The DNS replies with the correct IP address.
3. The browser initiates an HTTP request: It requests the yummyrecipesforme.com webpage using the IP address sent by the DNS server.
4. The browser initiates the download of the malware.
5. The browser initiates a DNS request for greatrecipesforme.com.
6. The DNS server responds with the IP address for greatrecipesforme.com.
7. The browser initiates an HTTP request to the IP address for greatrecipesforme.com.

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.

Section 1: Identify the network protocol involved in the incident

The network protocols involved in the incident are:

1. DNS (Domain Name System): Used to resolve the IP addresses for yummyrecipesforme.com and greatrecipesforme.com.
2. HTTP (Hypertext Transfer Protocol): Used to request and receive web pages and download files from yummyrecipesforme.com and greatrecipesforme.com.

Section 2: Document the incident

Incident Summary

- **Incident Type:** Brute force attack leading to website compromise

- **Date/Time of Incident:** [Specify date/time based on logs]
- **Affected Website:** yummyrecipesforme.com
- **Compromised URL:** greatrecipesforme.com (fake website)
- **Attack Vector:** Brute force attack on administrative account

Attack Description

A former employee, referred to as the disgruntled baker, executed a brute force attack on the administrative account of yummyrecipesforme.com. The attack was successful due to the use of a default password, allowing unauthorized access to the admin panel. The attacker embedded malicious JavaScript code in the website's source code, which prompted visitors to download a malware-laden file. Upon running the file, users were redirected to a fake version of the website, greatrecipesforme.com, which further compromised their personal computers.

1. **Network Protocols Used**

DNS Request: The browser initiated a DNS request to resolve the IP address of yummyrecipesforme.com.

makefile

```
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)
```

2. **HTTP Request:** The browser requested the webpage from the resolved IP address.

wasm

```
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 port 80>...
```

3. **Malware Download:** The browser initiated the download of the malicious file.
4. **DNS Request:** The browser initiated another DNS request for greatrecipesforme.com.

makefile

```
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)
```

HTTP Request: The browser requested the webpage from the resolved IP address, leading to further malware activities.

wasm

```
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 port 80>...
```

Immediate Actions Taken

1. **Account Lockout:** Locked the compromised administrative account.
2. **Password Reset:** Changed all administrative and critical account passwords.
3. **Malicious Code Removal:** Removed the embedded malicious JavaScript from the website's source code.
4. **User Notification:** Informed affected users about the incident and provided instructions for malware removal from their systems.

Section 3: Recommend one remediation for brute force attacks

Implement Multi-Factor Authentication (MFA)

By requiring MFA for all administrative logins, an additional layer of security is added, making it significantly harder for attackers to gain unauthorized access even if they successfully guess or obtain the password. This would prevent brute force attacks from succeeding, as the attacker would also need access to the secondary authentication factor (such as a mobile device or a hardware token).