Security incident report

Section 1: Identify the network protocol involved in the incident

The attacker used Brute force attack and guessed the username password of the admin and then added a script in the application code that redirects the website users to another spoof website and downloads malware. They sent an HTTP request to fetch another website which downloaded the malware and redirected the user to another website.

Section 2: Document the incident

At around 2:18pm, we noted the following in the tcpdump logs:

1. The first section of the DNS & HTTP traffic log file shows the source computer (**your.machine.52444**) using port **52444** **(this port is dynamic / unregistered. Less secure. port blocking not enabled/check firewall config)** to send a DNS resolution request to the DNS server (**dns.google.domain**) for the destination URL (**yummyrecipesforme.com**).
2. 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**).
3. The next section shows the source computer sending a connection request (**Flags [S]**) from the source computer (**your.machine.36086**) using port **36086** **(this port is dynamic / unregistered. Less secure. port blocking not enabled/check firewall config)** 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.]**).
4. The communication between the source and the intended destination continues for about 2 minutes, according to the timestamps between this block (**14:18**) and the next DNS resolution request (see below for the **14:20** timestamp).
5. 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.**

6. 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

Strong passwords

Frequent changing passwords for employees

Multi Factor authentication

Restrict previous passwords from being used

Limit number of Login attempts

Check login attempts