Cybersecurity Incident Report

Identification of the network protocol involved in the incident.

The security incident involved the following network protocols:

- DNS (Domain Name System): DNS protocol, used to translate domain names into IP addresses and facilitate network request resolution.
- HTTPS (Hypertext Transfer Protocol Secure): Protocol used for secure access and data transfer on the web.

Incident Documentation

The security incident occurred as follows, based on the traffic log:

1. At 14:18:32, a DNS query was recorded from our machine (your.machine) to dns.google.domain to obtain the IP address of yummyrecipesforme.com. The query was made using identification number 35084.
2. At 14:18:32, a response was received from the DNS server (dns.google.domain) to our machine. The response indicated that the IP address associated with yummyrecipesforme.com was 203.0.113.22.
3. At 14:18:36, our machine (your.machine) initiated a TCP connection to yummyrecipesforme.com on port 80 using the HTTP protocol. Packets with the

[S] flag were sent to synchronize the start of the connection.

4. At 14:18:36, yummyrecipesforme.com responded to our machine with [S.] packets to establish the TCP connection. Synchronization packets were exchanged and acknowledged.
5. At 14:18:36, our machine sent an HTTP GET request to obtain the main page of the website yummyrecipesforme.com. The request was made over port 80.
6. Continuous traffic was recorded on port 80, indicating normal interaction between our machine and the website yummyrecipesforme.com.
7. At 14:20:32, a new DNS query was recorded from our machine (your.machine) to dns.google.domain. This time, the query was made to obtain the IP address of greatrecipesforme.com using identification number 21899.
8. At 14:20:32, a response was received from the DNS server (dns.google.domain) to our machine. The response indicated that the IP address

associated with greatrecipesforme.com was 192.0.2.17.

9. At 14:25:29, our machine (your.machine) initiated a TCP connection to greatrecipesforme.com on port 80 using the HTTP protocol. Packets with the [S] flag were sent to synchronize the start of the connection.

10. At 14:25:29, greatrecipesforme.com responded to our machine with [S.] packets to establish the TCP connection. Synchronization packets were exchanged and acknowledged.

11. At 14:25:29, our machine sent an HTTP GET request to obtain the main page of the website greatrecipesforme.com. The request was made over port 80.

12. Continuous traffic was recorded on port 80, indicating normal interaction between our machine and the website greatrecipesforme.com.

Tools implemented

For network traffic monitoring, the tcpdump protocol was used to capture and analyze HTTPS and DNS traffic. This allowed for the identification of key events related to the security incident.

Framework and Playbook implemented

During the analysis of this security incident, the NIST (National Institute of Standards and Technology) framework was applied for cybersecurity incident handling and to guide response and mitigation actions.

A customized playbook based on the NIST framework was used to address this scenario and coordinate the response to the security incident and apply appropriate security measures. The playbook outlines the steps and actions to be taken in the event of a brute force incident and provides guidance on incident identification, response, mitigation, and recovery.

To mitigate this security incident, the following tools from the NIST CSF (Cybersecurity Framework) were used:

1. **Identify**: A risk assessment was conducted to identify potential vulnerabilities in the website, and measures were implemented to strengthen security. Additionally, a network infrastructure analysis was performed, identifying critical assets and system dependencies.

2. **Protect**: Protection measures were implemented, such as enforcing strong

password policies, two-factor authentication (2FA), and account lockout after a certain number of failed login attempts. Proper access controls were established to limit administrative privileges, and systems and applications were secured with up-to-date security patches.

3. **Detect**: Security monitoring tools, such as an Intrusion Detection System (IDS) and packet capture, were implemented to identify suspicious activity in real-time. Audit logs were established, and an early warning system was implemented to detect attack attempts and anomalous behavior.

4. **Respond**: A security incident response team was established to promptly handle the incident, including coordination with the web hosting provider and communication with affected customers. A customized playbook based on the NIST CSF was applied to guide response and mitigation actions.

5. **Recover**: A recovery process was conducted to restore the functionality of the website and remove any malicious code or unauthorized modifications. Proper backups were performed to ensure data availability, and additional measures were implemented to prevent future brute force attacks.

Recommendations and Solutions for Brute Force Attacks

To prevent future brute force attacks, the following solutions are recommended:

1. Change the default password: It is crucial to change the default administrator password to prevent attackers from easily guessing the password. A strong and unique password should be used for each administrator account.
2. Implement access control measures: It is necessary to establish account lockout policies after a certain number of failed login attempts. This will make brute force attempts more difficult by limiting the number of attempts that can be made.
3. Continuous security monitoring: Implementing an Intrusion Detection System (IDS) and a packet capture tool to monitor network activity for suspicious behavior is essential. This will allow for real-time identification of brute force attacks and the ability to take action to stop them.
4. Staff education and awareness: It is important to train staff on security best practices, including the importance of using strong passwords, not sharing login credentials, and being vigilant against possible attack attempts.

Conclusions

Following the incident, swift actions were taken to mitigate the attack's impact and restore the website's functionality. The compromised server was temporarily taken offline to prevent further unauthorized access and modifications. The website's source code was thoroughly reviewed and restored to its original state, ensuring the removal of the embedded JavaScript function. Additional security measures, such as implementing account lockout policies, enforcing strong passwords, enabling two-factor authentication (2FA), and deploying intrusion detection and prevention systems (IDPS), were recommended to strengthen the website's resilience against future brute force attacks. By implementing these measures, the organization aims to enhance the security posture of its online platform and safeguard customer data.