Security Incident Report

Section 1: Identify the network protocol involved in the incident

The network protocols identified during the investigation are DNS and HTTP. DNS was used to resolve the IP address of yummyrecipesforme.com when users attempted to access the website. After the malicious file was executed, an additional DNS request was observed for greatrecipesforme.com, which is a malicious domain.

HTTP was used to request the original website, download the malicious executable file, and later communicate with the malicious website after the redirection. These protocols were identified through analysis of the tcpdump traffic logs.

Section 2: Document the incident

The incident occurred after multiple users reported being redirected to an unfamiliar website and experiencing slow system performance. The website yummyrecipesforme.com was compromised following a successful brute force attack against an administrative account.

The attacker repeatedly attempted known or default passwords until valid credentials were obtained. Once access was gained, the attacker logged into the administrative panel and modified the website's source code by inserting malicious JavaScript. This script prompted visitors to download and execute an executable file under the pretense of accessing free recipes.

Analysis of the tcpdump traffic logs showed the following sequence of events: a DNS request resolving yummyrecipesforme.com, an HTTP request to load the website, a download of a malicious executable file, a DNS request for greatrecipesforme.com, and an HTTP request to the malicious website. Further analysis confirmed that the executable redirected users to the malicious domain and caused system performance degradation.

Section 3: Recommend one remediation for brute force attacks

A recommended remediation to prevent future brute force attacks is the implementation of two-factor authentication (2FA) for all administrative accounts. Two-factor authentication requires users to provide an additional verification factor beyond a password, such as a one-time code or authentication application approval.

This additional security layer significantly reduces the effectiveness of brute force attacks, as attackers cannot gain access with a password alone. Implementing 2FA strengthens account security and helps prevent unauthorized access even if credentials are compromised.