Informe del incidente de seguridad

Sección 1: Identificación del protocolo de red involucrado en el incidente
Protocolos de red: 1. DNS: Consultas DNS para resolver las direcciones IP: a. 14:18:32.192571 IP your.machine.52444 > dns.google.domain: 35084+ A? yummyrecipesforme.com. (24) b. 14:20:32.192571 IP your.machine.52444 > dns.google.domain: 21899+ A? greatrecipesforme.com. (24) 2. HTTP, Comunicaciones entre los navegadores y los servidores web. a. 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 b. 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

Sección 2: Documentación del incidente
Un panadero descontento realizó un ataque de fuerza bruta para acceder al panel de administración de yummyrecipesforme.com. Después de obtener las credenciales correctas, modificó el código fuente del sitio web para insertar un script malicioso en JavaScript. Este script solicitaba a los visitantes que descargaran y ejecutaran un archivo ejecutable. Al ejecutar este archivo, los usuarios eran redirigidos a greatrecipesforme.com, un sitio web falso que mostraba las recetas de yummyrecipesforme.com de manera gratuita. Características y efectos del atacante.

- El atacante utiliza técnicas de fuerza bruta.
- Modifica el código fuente para que los visitantes cuando accedan a la web les salga un mensaje para bajar un Script.
- Ejecución de Script, Los visitantes ejecutan el Script
- Redirección. Una vez es ejecutado se accede al sitio “greatrecipesforme.com.”

Consecuencias del ataque:

- Reputación.
- Rendimiento

Sección 3: Recomendación de una solución para los ataques de fuerza bruta

Se pueden realizar unas series de medidas:

- Implementación de autenticación multifactor.
- Usar contraseñas más fuertes.
- Limitar intentos de inicio de sesión.
- Monitorear y alertas sobre actividades sospechosas.
- Revisar y actualizar el sistema operativo y las credenciales.