Informe de Incidente de Seguridad.

HTTP

1. Información General del Incidente:

Fecha y hora del incidente:
20/03/2012 13:37:42

Descripción del incidente:
El incidente comenzó cuando varios clientes del sitio web **yummyrecipesforme.com** informaron que al intentar acceder al sitio web, se les solicitaba descargar un archivo para poder acceder a las nuevas recetas. Después de ejecutar el archivo, los sistemas de los usuarios comenzaron a experimentar lentitud. Además, el propietario del sitio web notó que su cuenta de administrador fue bloqueada.

Ubicación del incidente:
El incidente ocurrió en el servidor web de **yummyrecipesforme.com**, y afectó tanto a los clientes como a la infraestructura interna del sitio web.

Tipo de incidente:
Exploits de acceso no autorizado (Ataque de fuerza bruta) y Distribución de malware.

2. Identificación del Protocolo de Red Involucrado:

El protocolo involucrado en este incidente fue el Protocolo de Transferencia de Hipertexto (HTTP). El ataque ocurrió a través de una manipulación del tráfico HTTP entre los usuarios y el servidor web. Durante la inspección de los registros de tráfico, utilizando tcpdump, se identificó que el archivo malicioso fue transportado a las computadoras de los usuarios a través de solicitudes HTTP en la capa de aplicación.

3. Análisis Detallado del Incidente:

Descripción Técnica:

1. Acceso a sitio web malicioso:
   Los usuarios que accedían a yummyrecipesforme.com fueron redirigidos automáticamente para descargar un archivo malicioso que aparentaba ofrecer recetas gratuitas. Este archivo fue diseñado para ejecutar un código malicioso que afectaba el rendimiento de sus dispositivos.
2. Captura de tráfico de red (tcpdump):
   Se utilizó tcpdump para monitorear el tráfico de red generado cuando los usuarios accedieron al sitio web. Inicialmente, el tráfico se dirigió a la dirección IP de yummyrecipesforme.com. Sin embargo, después de la ejecución del archivo malicioso, se observó un cambio en la dirección IP solicitada, redirigiendo el tráfico a

un servidor distinto, greatrecipesforme.com, lo que indica una posible manipulación de DNS o un ataque de tipo "man-in-the-middle".

3. Análisis del ataque:
   se revisó el código fuente del sitio web comprometido y el archivo descargado. Se descubrió que un atacante había introducido código malicioso en el sitio legítimo, lo que permitió que el archivo malicioso fuera descargado sin la intervención del usuario.
4. Acceso no autorizado al servidor:
   Según el propietario del sitio, su cuenta de administrador fue bloqueada después del ataque. El equipo de seguridad determinó que un ataque de fuerza bruta se utilizó para acceder a la cuenta de administrador, lo que permitió al atacante cambiar la contraseña y manipular el sitio.

4. Impacto y Alcance del Incidente:

- **Usuarios afectados:**
  El incidente afectó a varios usuarios del sitio web, quienes descargaron el archivo malicioso. Aparentemente, los usuarios experimentaron una disminución del rendimiento en sus dispositivos.
- **Recursos comprometidos:**
  - Cuentas de usuario: Se sospecha que las credenciales del administrador fueron comprometidas.
  - Datos de usuario: El incidente no ha indicado pérdida de datos personales de clientes hasta el momento.
  - Infraestructura de servidor: El servidor web y la infraestructura relacionada fueron comprometidos debido al acceso no autorizado.
- **Tiempo de exposición:**
  El incidente estuvo activo durante 6 horas antes de ser detectado y mitigado.

5. Medidas Correctivas y Prevención:

1. **Recomendaciones para mitigar ataques de fuerza bruta:**
   - No permitir contraseñas anteriores:
     Prohibir el uso de contraseñas antiguas durante el proceso de restablecimiento de la contraseña, evitando que los atacantes utilicen contraseñas predeterminadas.
   - Contraseñas más largas y complejas:
     Se recomienda utilizar contraseñas de al menos 15 caracteres, que combinan letras mayúsculas, minúsculas, números y caracteres especiales.
   - Autenticación de dos factores (2FA):
     Implementar un sistema de autenticación de dos factores, que requiera tanto una contraseña como un código enviado al correo electrónico o teléfono móvil del usuario, lo que dificultará los ataques de fuerza bruta.

2. **Solución a la distribución de malware:**
    - Auditoría y revisión de código:
      Se debe realizar una auditoría exhaustiva de todo el código fuente y los archivos distribuidos en el sitio web. Debe bloquearse la capacidad de los atacantes para insertar código malicioso.
    - Revisión de la infraestructura de red:
      Implementar un sistema de firewall para evitar redirecciones no autorizadas y para bloquear las IPs sospechosas.
3. **Revisión de accesos y cuentas de administrador:**
    - Cambio inmediato de contraseñas de cuentas críticas
      Realizar un cambio forzado de contraseñas de todas las cuentas de administración y realizar una revisión exhaustiva de los accesos para evitar futuros ataques.

6. Lecciones Aprendidas:

- Importancia de la autenticación fuerte: El ataque de fuerza bruta se facilitó por el uso de contraseñas débiles. La implementación de políticas más estrictas de contraseñas y autenticación de dos factores podría haber prevenido el acceso no autorizado.
- Vulnerabilidades en la manipulación de tráfico HTTP: La redirección a un sitio web falso a través de HTTP muestra la necesidad de una mayor vigilancia de los dominios y tráfico de la red.

7. Plan de Acción:

- Investigación adicional: Se continuará con la investigación para determinar el alcance completo del incidente y cualquier otro vector de ataque que pueda haber sido utilizado.
- Implementación de medidas de seguridad: Las recomendaciones de seguridad serán implementadas de inmediato para proteger los sistemas y datos de usuarios en el futuro.
- Monitoreo constante: Se establecerán medidas de monitoreo continuo para detectar cualquier actividad sospechosa y mitigar posibles futuros incidentes.