

Informe de Endurecimiento del Sistema Operativo y Respuesta al Incidente

Empresa: YummyRecipesForme.com

Analista de Seguridad: Tina Calleja

Incidente: Ataque de Fuerza Bruta e Inyección de Malware

1. Identificación del Protocolo de Red

Protocolo identificado en el registro tcpdump:

- **HTTP (Puerto 80/TCP):**
 - Usado para la comunicación no cifrada entre el navegador y el servidor.
 - Permitía la inyección de código JavaScript malicioso en el código fuente del sitio web.
- **DNS (Puerto 53/UDP):**
 - Utilizado para redirigir a los usuarios a greatrecipesforme.com (dominio malicioso).

Evidencia del ataque:

- Solicitudes HTTP con inyección de JavaScript malicioso (`<script>window.location="greatrecipesforme.com"</script>`).
 - Resoluciones DNS fraudulentas hacia la IP del sitio falso.
-

2. Documentación del Incidente

Resumen del Ataque

1. Fase de Intrusión:

- Un ex-empleado realizó un **ataque de fuerza bruta** al panel administrativo usando credenciales predeterminadas (admin:admin).
- No existían medidas de protección como **límite de intentos** o **autenticación multifactor (MFA)**.

2. Modificación del Código Fuente:

- Se inyectó un script en index.php que forzaba la descarga de un ejecutable malicioso (update_browser.exe).
- El malware redirigía a los usuarios a greatrecipesforme.com (phishing + malware).

3. Impacto:

- **Clientes afectados:** Descarga de malware en sus dispositivos.
- **Reputación:** Pérdida de confianza en la marca.
- **Disponibilidad:** Bloqueo del acceso al panel administrativo (contraseña cambiada por el atacante).

Fuentes de Evidencia

- Registros [tcpdump](#): Mostraban conexiones HTTP/DNS anómalas.
- Análisis forense: Código JavaScript malicioso en el archivo index.php.

3. Recomendaciones de Seguridad

Medida Prioritaria: Autenticación Multifactor (MFA)

¿Por qué?

- Mitiga el riesgo de ataques de fuerza bruta, incluso si las credenciales son comprometidas.
- Ejemplo: Usar [Google Authenticator](#) o [YubiKey](#) para acceder al panel administrativo.

Otras Medidas de Endurecimiento

Área	Acción	Herramienta/Configuración
Contraseñas	Exigir complejidad (mínimo 12 caracteres, símbolos, mayúsculas/minúsculas).	<code>sudo pam-config --add --pwquality (Linux)</code>
Protección Web	Instalar WAF (Web Application Firewall) para bloquear inyecciones de código.	ModSecurity (Apache/Nginx)
Monitoreo	Implementar Fail2Ban para bloquear IPs tras 3 intentos fallidos de login.	<code>sudo apt install fail2ban</code>
Actualizaciones	Parchear el servidor y aplicaciones (PHP, WordPress, plugins).	<code>sudo apt update && sudo apt upgrade -y</code>
Backups	Restaurar el sitio desde una copia limpia y validada.	BorgBackup o rsync (criptografiado)

4. Plan de Acción

1. Recuperación Inmediata (24h):

- Restaurar el sitio desde backup.
- Revocar accesos y cambiar todas las contraseñas.

2. Prevención (72h):

- Implementar MFA en todos los accesos administrativos.
- Configurar WAF (Web Application Firewall)
y Fail2Ban (herramienta que protege a servidores de ataques)

3. Monitoreo Continuo (1 semana):

- Escanear archivos con [Lynis](#) y [ClamAV](#).
 - Auditar logs diarios con [ELK Stack](#).
-


5. Conclusión

El incidente fue causado por **malas prácticas de seguridad** (credenciales predeterminadas, falta de MFA). La implementación de **autenticación multifactor** y **endurecimiento del servidor** evitará futuros ataques.


En caso de sufrir un ataque o cualquier otro incidente de ciberseguridad, es crucial informar a las entidades adecuadas para cumplir con la ley, mitigar daños y prevenir futuros ataques.

❑ **INCIBE (Instituto Nacional de Ciberseguridad):**

 [Formulario de Reporte de Incidentes](#)

 **Teléfono: 017** (Servicio gratuito para empresas y ciudadanos).
Obligatorio si el ataque afecta a datos personales (LOPDGDD) o infraestructuras críticas.

❑ **AEPD (Agencia Española de Protección de Datos):**

 Solo si se filtran datos personales (RGPD).

 canaletico@aepd.es.

Autoridades Policiales (Si hay delito)

❑ **Guardia Civil (España) - Grupo de Delitos Telemáticos:**

 [Formulario online](#).

Clientes y Afectados

❑ Comunicación Transparente:

Si el ataque afectó a usuarios (ej: caída del servicio), enviar un email o anuncio explicando lo ocurrido y medidas tomadas.

 Ejemplo:

"El [fecha], nuestro sitio experimentó interrupciones por un ataque cibernético. Hemos mitigado el problema y reforzado la seguridad. Lamentamos las molestias."