FASTREANDO

¡No apruebes sin pensar! Los ataques de fatiga MFA están en aumento

Riesgo actual

En los últimos meses, se ha incrementado significativamente el uso de ataques conocidos como **MFA Fatigue** o **bombardeo de autenticación multifactor**.

En este tipo de ataque, el ciberdelincuente primero obtiene las credenciales de un usuario (por ejemplo, mediante phishing previo o filtraciones) y luego intenta iniciar sesión repetidamente en sistemas corporativos. Cada intento genera una notificación de autenticación MFA (push) al usuario legítimo.

El objetivo es que el colaborador, por cansancio, confusión o error, **apruebe la solicitud de acceso sin verificarla**.

Este tipo de ataque puede incluir técnicas adicionales como:

- Llamadas telefónicas haciéndose pasar por TI.
- Mensajes indicando urgencia para aprobar la solicitud.
- Uso de horarios fuera de oficina para aumentar el descuido.

Debido a que el acceso se realiza con credenciales válidas y un MFA aprobado, es más difícil detectar el acceso como malicioso.

Señales de alerta

- Recepción repetida de solicitudes MFA sin haber intentado iniciar sesión.
- Notificaciones de autenticación fuera del horario laboral.
- Llamadas o mensajes solicitando aprobar una autenticación inesperada.
- Mensajes urgentes como "Apruebe para evitar bloqueo de cuenta".
- Alertas de inicio de sesión desde ubicaciones o dispositivos desconocidos.

FASTREANDO

Ejemplo de ataque

Un colaborador recibe múltiples notificaciones en su celular para aprobar un acceso a Microsoft 365, aunque no está intentando ingresar.

Minutos después, recibe una llamada de alguien que se identifica como soporte técnico indicando: "Estamos verificando tu cuenta, por favor aprueba la solicitud que acabas de recibir".

El colaborador aprueba la notificación y, en ese momento, el atacante obtiene acceso completo a su cuenta corporativa.

4. ¿Cómo afecta el entorno PCI o los datos de tarjeta?

El uso indebido de accesos legítimos autorizados mediante MFA representa un riesgo crítico para entornos regulados como PCI DSS.

Con una autenticación aprobada, el atacante podría:

- Acceder a aplicaciones corporativas críticas.
- Ingresar a la VPN o entornos internos seguros.
- Escalar privilegios dentro de la red.
- Acceder a sistemas que almacenan o procesan datos de tarjeta.
- Extraer información sensible sin ser detectado fácilmente.

Si el usuario comprometido tiene acceso al entorno PCI, existe riesgo de:

- Exposición de datos de tarjeta (PAN).
- Incumplimiento de controles de autenticación fuerte.
- Incidentes de seguridad con impacto legal y financiero.

FASTREANDO

5. ¿Qué debe hacer el colaborador?

- **Nunca aprobar solicitudes MFA que no haya iniciado.**
- Si recibe muchas solicitudes seguidas, rechazar todas inmediatamente.
- Reportar el incidente al área de Seguridad o TI.
- No confiar en llamadas o mensajes solicitando aprobar accesos.
- Verificar siempre que el origen del acceso sea legítimo antes de aprobar.
- Activar factores de autenticación más seguros cuando sea posible (como llaves físicas o biometría).
- Cambiar su contraseña inmediatamente si sospecha compromiso.
- Mantener el dispositivo móvil seguro y bloqueado.

Fuente: https://ctresources.com/2026/02/mfa-fatigue-attacks-prevention/

https://ransomnews.com/mfa-fatigue-attacks-2026/