TECNOLOGÍA | SISTEMAS MÁS SEGUROS

**Microsoft Authenticator   
se actualiza con valiosas mejoras de seguridad**

*Microsoft Authenticator se actualiza con mejoras de seguridad; ahora, aplicará la coincidencia de números en todas las notificaciones push para que la autenticación multifactor sea menos susceptible a los ataques de ingeniería social.*

**Por Julián M. Zappia.  
Diplomatic Week.**

Ciberdelincuentes sofisticados han tenido éxito atacando métodos de seguridad multifactor mediante ataques de fatiga MFA.

Estos ataques consisten en enviar un aluvión de solicitudes de notificaciones push de MFA al personal de las organizaciones, a menudo en horas intempestivas, con el fin de manipularlos para que autentifiquen un intento de inicio de sesión sólo para eliminar las frustrantes notificaciones.

La coincidencia de números consiste en abrir una notificación push, iniciar Microsoft Authenticator e introducir una serie de números que aparecen en la aplicación para aprobar el intento de inicio de sesión.

Esta técnica existe desde hace años y combina los métodos de autenticación MFA y de doble factor (2FA).

**Un nuevo método de phishing.**

Estos números suelen restablecerse después de un periodo de tiempo determinado, como 30 segundos, y añaden una capa adicional de interacción para ayudar a reducir el riesgo de ataques de ingeniería social con éxito.

En un escenario de ataque típico, los destinatarios de las notificaciones constantes suelen estar dormidos y se despiertan con una serie de alertas ruidosas desde su smartphone.

**Cuidado al quedarse dormido.**

Cuando nos atacan en una situación vulnerable o en la que dedicamos poca atención, como cuando estamos medio dormidos, el ataque puede tener éxito cuando el personal se limita a aprobar los intentos de inicio de sesión y así poder volver a dormir, por ejemplo.

De hecho, se recomienda añadir otra capa manual, que aumenta la dificultad para aprobar rápidamente las solicitudes. Así, el proceso se hace más tedioso y agrega más tiempo al usuario para darse cuenta de que la solicitud está siendo provocado por un ciberdelincuente.

**Mejoras de seguridad.**

Microsoft dijo que la coincidencia de números se aplicará como estándar a una serie de diferentes escenarios de autenticación.

“A medida que se desplieguen los servicios pertinentes, los usuarios de todo el mundo que estén habilitados para las notificaciones push de Authenticator, empezarán a ver coincidencias de números en sus solicitudes de aprobación”, informaron desde la empresa.

**Microsoft en su documentación de Active Directory.**

Los usuarios que intenten un restablecimiento de contraseña de autoservicio (SSR) también tendrán que utilizar la coincidencia de número MFA para completar el proceso. La coincidencia de números también se aplicará para el registro combinado en Azure AD y el adaptador AD FS para Windows Server.

Microsoft aclaró que los usuarios no pueden optar por no utilizar la coincidencia de números, pero puede haber algunos escenarios que no la apliquen, como en MFA Server, que está obsoleto, y con versiones antiguas de Authenticator que ya no funcionarán, lo que requerirá una actualización.

El portal de Active Directory también puede seguir mostrando la configuración para activar la coincidencia de números manualmente, pero Microsoft dijo que puede que sólo tenga que actualizar el navegador con el fin de ver la actualización.