Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°060	Fecha: 09-03-2024
		Página: 4 de 8

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Microsoft dice que piratas informáticos rusos violaron sus sistemas y accedieron al código fuente		
Tipo de Ataque	Robo de información	Abreviatura	RobInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K01
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. **ANTECEDENTES:**

Microsoft dice que el grupo de hackers ruso 'Midnight Blizzard' accedió recientemente a algunos de sus sistemas internos y repositorios de código fuente utilizando secretos de autenticación robados durante un ciberataque en enero.

Midnight Blizzard (también conocido como Nobelium, APT29 y Cozy Bear) es un grupo de piratería patrocinado por el estado y vinculado al Servicio de Inteligencia Exterior de Rusia (SVR). Los piratas informáticos ganaron prominencia después de realizar el ataque a la cadena de suministro de SolarWinds de 2020, que permitió a los actores de amenazas violar numerosas empresas, incluida Microsoft.

2. **DETALLES:**

En enero, Microsoft reveló que Midnight Blizzard (también conocido como NOBELIUM) había violado los servidores de correo electrónico corporativo después de realizar un ataque de pulverización de contraseñas que permitía el acceso a una cuenta de inquilino de prueba heredada que no era de producción. Una publicación de blog posterior reveló que esta cuenta de prueba no tenía habilitada la autenticación multifactor, lo que permitió a los actores de amenazas obtener acceso para violar los sistemas de Microsoft.

Esta cuenta de inquilino de prueba también tenía acceso a una aplicación OAuth con acceso elevado al entorno corporativo de Microsoft, lo que permitía a los actores de amenazas acceder y robar datos de los buzones de correo corporativos, incluidos miembros del equipo de liderazgo de Microsoft y empleados de los departamentos legal y de ciberseguridad.

Hoy, Microsoft dice que Midnight Blizzard está utilizando secretos encontrados en los datos robados para obtener acceso a algunos de los sistemas y repositorios de código fuente de la compañía en las últimas semanas. "En las últimas semanas, hemos visto evidencia de que Midnight Blizzard está utilizando información inicialmente extraída de nuestros sistemas de correo electrónico corporativo para obtener, o intentar obtener, acceso no autorizado", se lee en una nueva publicación de blog del Centro de respuesta de seguridad de Microsoft.

"Esto ha incluido el acceso a algunos de los repositorios de código fuente y sistemas internos de la compañía. Hasta la fecha no hemos encontrado evidencia de que los sistemas de cara al cliente alojados en Microsoft hayan sido comprometidos".

Si bien Microsoft no ha explicado con precisión qué incluyen estos "secretos", es probable que sean tokens de autenticación, claves API o credenciales.

La compañía dice que Midnight Blizzard también está intensificando sus ataques de pulverización de contraseñas contra sistemas específicos, observando un aumento de 10 veces en febrero en comparación con el volumen que vieron en enero de 2024.

3. **RECOMENDACIONES:**

- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/microsoft/microsoft-says-russian-hackers-breached-its-systems-accessed-source-code/#google_vignette