Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°235	Fecha: 05-10-2023
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los piratas informáticos están abusando de Dropbox para robar credenciales de Microsoft SharePoint		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Ha surgido una creciente amenaza cibernética que involucra a Dropbox y está generando preocupaciones en todo el panorama de la ciberseguridad.

En las dos primeras semanas de septiembre, se detectaron la asombrosa cifra de 5.440 de estos ataques, lo que pone de relieve la alarmante escala de esta amenaza.

2. DETALLES:

Los piratas informáticos están aprovechando Dropbox para crear páginas de inicio de sesión falsas, lo que en última instancia lleva a víctimas desprevenidas a sitios web de recolección de credenciales.

Esta táctica representa una nueva iteración de los ataques Business Email Compromise (BEC), a los que nos referiremos como BEC 3.0.

Los ataques BEC 3.0 implican el uso de plataformas legítimas como Dropbox para enviar y alojar materiales de phishing.

La legitimidad de estas plataformas hace que sea increíblemente difícil para los servicios de seguridad del correo electrónico detectar las amenazas y para los usuarios finales reconocerlas.

Estos ataques van en aumento y los piratas informáticos están empleando varios sitios de productividad, incluidos Google, Dropbox, QuickBooks, PayPal y más, como campos de batalla.

Esta innovación en tácticas de phishing ha demostrado ser muy eficaz y está ganando rápidamente popularidad entre los ciberdelincuentes.

En este ataque en particular, los piratas informáticos utilizan documentos de Dropbox para alojar sitios web diseñados para la recolección de credenciales. Aquí están los detalles clave:

- Vector: correo electrónico
- Tipo: BEC 3.0
- Técnicas: Ingeniería Social, Recolección de Credenciales
- Target: cualquier usuario final

El ataque comienza con un correo electrónico aparentemente de Dropbox, informando al destinatario que hay un documento para ver. Este correo electrónico parece completamente estándar y no despertaría sospechas de inmediato.

Al hacer clic en el correo electrónico, el usuario es dirigido a una página de Dropbox. Aunque el contenido imita una página de inicio de sesión de OneDrive, la URL indica claramente que está alojada en Dropbox.

Al hacer clic en "Obtener documento", se redirige al usuario a la página final, que es la página de recolección de credenciales. Esta página, alojada fuera de Dropbox, es donde los actores de amenazas intentan robar las credenciales de los usuarios.

La evolución de los ataques Business Email Compromise es notable. Comenzó con simples estafas de “tarjetas de regalo” y suplantación de dominios y socios.

Sin embargo, ahora ha llegado a BEC 3.0, donde los ataques se ejecutan a través de servicios legítimos, lo que los hace excepcionalmente difíciles de detectar.

Estos ataques son inmensamente difíciles de detener e identificar, tanto para los servicios de seguridad como para los usuarios finales.

Los indicadores tradicionales de phishing, como lenguaje inusual o dominios falsificados, ya no se aplican cuando los ataques se originan en servicios legítimos.

3. RECOMENDACIONES:

- Cuestionar la autenticidad de los correos electrónicos y considerar si esperan recibir un documento del remitente.
- Pasar el cursor sobre las URL para inspeccionar su destino.
- Adoptar tecnología impulsada por IA capaz de analizar e identificar numerosos indicadores de phishing.
- Implementar soluciones integrales de seguridad con capacidades de escaneo de documentos y archivos.
- Implementar sistemas robustos de protección de URL para escaneos exhaustivos y emulación de páginas web para mejorar la seguridad.

Fuente de Información:	• https://gbhackers.com/hackers-busing-dropbox/