Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°164	Fecha: 12-07-2023
		Página: 4 de 27

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Vulnerabilidad de Día Cero de MS Office Explotada para Espionaje		
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:

Microsoft está investigando una serie de vulnerabilidades de ejecución remota de código que afectan a los productos de Windows y Office. La empresa es consciente de los ataques dirigidos que intentan aprovechar estas vulnerabilidades mediante el uso de documentos de Microsoft Office especialmente diseñados.

Una vez finalizada esta investigación, Microsoft tomará las medidas adecuadas para ayudar a proteger a sus usuarios, lo cual podría incluir proporcionar una actualización de seguridad a través del proceso de lanzamiento mensual o una actualización de seguridad fuera de ciclo, según las necesidades de sus usuarios.

Microsoft ha identificado una campaña de phishing realizada por el actor de amenazas rastreado como Storm-0978 dirigida a entidades gubernamentales y defensa en Europa y América del Norte.

Storm-0978, también conocido como RomCom, el nombre de su puerta trasera, por otros proveedores, es un grupo de ciberdelincuentes con sede en Rusia, conocido por realizar operaciones oportunistas de ransomware y extorsión, así como campañas de recolección, probablemente en apoyo de operaciones de inteligencia.

El grupo opera, desarrolla y distribuye el backdoor RomCom. También implementa el ransomware Underground, que está estrechamente relacionado con el ransomware Industrial Spy.

2. DETALLES:

Un atacante podría crear un documento de Microsoft Office especialmente diseñado que le permita realizar la ejecución remota de código en el contexto de la víctima. Sin embargo, el atacante tendría que convencer a la víctima para que abra el archivo malicioso.

Storm-0978 llevó a cabo una campaña de phishing que contenía un cargador OneDrive falso para ofrecer una puerta trasera con similitudes con RomCom. Estos correos electrónicos de phishing estaban dirigidos a entidades gubernamentales y defensa en Europa y América del Norte, con señuelos relacionados con el Congreso Mundial de Ucrania. Estos correos electrónicos condujeron a la explotación de la vulnerabilidad CVE-2023-36884.

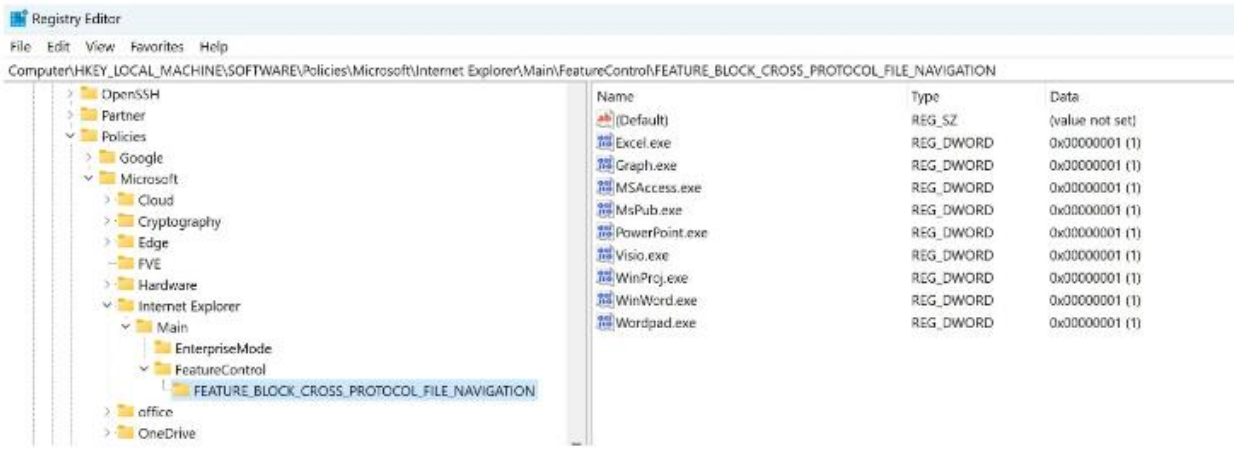
Con respecto a la actividad de phishing atribuida, Storm-0978 ha adquirido exploits dirigidos a vulnerabilidades de zero day. La actividad identificada incluye la explotación de CVE-2023-36884, además de una vulnerabilidad de ejecución remota de código explotada a través de documentos de Microsoft Word en junio de 2023, así como la explotación de otras vulnerabilidades que contribuyen a la omisión de una función de seguridad.

Microsoft Defender para Office 365 detectó el uso inicial de Storm-0978 del exploit dirigido a CVE-2023-36884 en esta actividad de phishing.

3. RECOMENDACIONES:

- Consultar el blog de inteligencia sobre amenazas de Microsoft en el link https://aka.ms/Storm-0978 para obtener información importante sobre los pasos que debe seguir para proteger su sistema de esta vulnerabilidad.
- Activar la protección proporcionada por la nube en Microsoft Defender Antivirus, o el equivalente para su producto antivirus, con el fin de cubrir las herramientas y técnicas de atacantes que evolucionan rápidamente.
- Usar la regla de "Reducción de la superficie a Ataques por Tipo" y elegir "Impedir que todas las aplicaciones de Office creen procesos secundarios" para evitar que se explote la vulnerabilidad.
- Configurar la clave de registro FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION para evitar la explotación; siempre tomando en consideración que podría afectar la funcionalidad normal para ciertos casos de uso relacionados con las aplicaciones mencionadas a continuación. Agregar los siguientes nombres de aplicación a esta clave de registro como valores de tipo REG_DWORD con data 1: excel.exe, Graph.exe, MSAccess.exe, MsPub.exe, PowerPoint.exe, Visio.exe, WinProj.exe, winword.exe, wordpad.exe.

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION
```



Fuente de Información:	• hxxps://www.cvedetails.com/cve/CVE-2023-36884/?q=CVE-2023-36884 • hxxps://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/ • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884 • hxxps://thehackernews.com/2023/07/microsoft-releases-patches-for-130.html