CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Fraude

Fecha: 03/10/2023

Problemática: Ataques de Suplantación de Identidad (Phishing) engaña a Outlook

Correlativo: AC-0076

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Ataques de phishing con un falso escaneo AV engañan a Outlook para que correos electrónicos maliciosos aparezcan como escaneados de forma segura por las herramientas de seguridad.

SITUACIÓN

Actor de amenazas utiliza nueva técnica ZeroFont en correos electrónicos maliciosos, este ataque tiene como objetivo evadir los filtros de seguridad insertando términos benignos invisibles que se mezclan con contenido visible sospechoso, sesgando la interpretación de AI del contenido y el resultado de los controles de seguridad.

Esta técnica de phishing explota fallas en la forma en que la Inteligencia Artificial (IA) y los sistemas de procesamiento de lenguaje natural (NLP) en las plataformas de seguridad de correo electrónico analizan el texto. Implica insertar palabras o caracteres ocultos en los correos electrónicos estableciendo el tamaño de fuente en cero

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

- Verifique la fuente de información de los documentos que recibe
- Nunca entre en la web de su banco pulsando en links incluidos en correos electrónicos
- El phishing sabe idiomas, por lo que puede atacarte por medio de distintos idiomas

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.
- Puerta Trasera: Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.
- Phishing: Estafa o fraude informático mediante correo electrónico, mensaje de texto u otro medio tecnológico donde se suplanta la identidad de una persona o empresa de confianza

REFERENCIAS

BLEEPING COMPUTER
https://www.bleepingcomputer.com/news/security/new-zerofont-phishing-tricks-outlook-into-showing-fake-av-scans/