CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Fraude

Fecha: 02/10/2023

Problemática: Ataques de Suplantación de Identidad (Phishing)

Correlativo: AC-0075

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Ataques de phishing con temática «Cruz Roja» distribuyen puertas traseras (backdoors) a través de documentos con extensión .doc y .docx

SITUACIÓN

Actor de amenazas conocido como «AltasCros» aprovecha señuelos de phishing para entregar dos puertas traseras DangerAds y AtlasAgent previamente instanciadas en documentos de Microsoft Word que contiene macros y que simula estar relacionado con una campaña de donación de sangre de la Cruz Roja. Cuando se abre este documento, se activa una macro maliciosa que establece una persistencia en el sistema y transmite datos del sistema a un servidor remoto llamado data.vectorse[.]com.

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

THE HACKER NEWS
https://thehackernews.com/2023/09/red-cross-themed-phishing-attacks.html