CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Actividad Cibernética

Fecha: 05/03/2024

Problemática: **Secuestro DNS para realizar estafas en bolsas de inversión**

Correlativo: AC-0013

Institución / Sector: **Público y Privado**

SITUACIÓN

El actor de amenazas «Savvy Seahorse» está empleando técnicas sofisticadas para atraer a sus victimamos a plataformas de inversión falsas con el objetivo de robar los fondos.

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	Alto	Alto

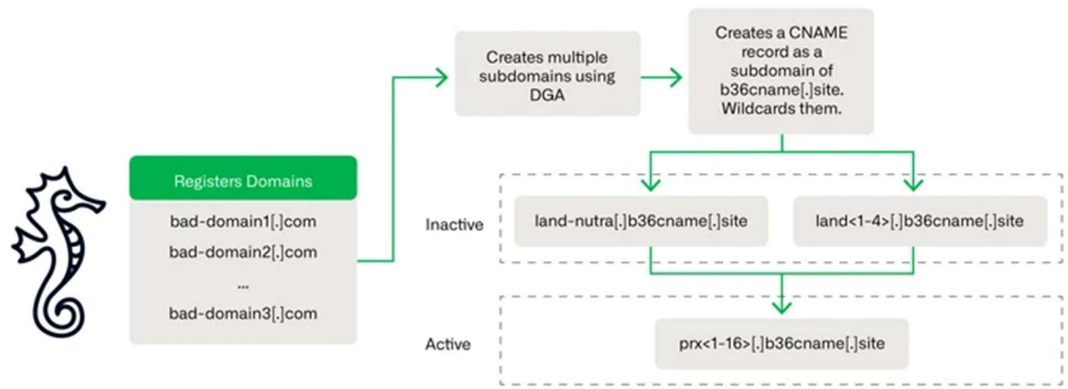
RIESGOS

- Ejecución de malware a través del proceso de Redireccionamiento abierto
- Afectación en la integridad y confidencialidad del sitio
- Cifrado y perdida de información
- Ciberextorsión
- Exfiltración de datos

RECOMENDACIONES

- Implementar procesos de restauración de copia de seguridad
- Actualizar el administrador de contenidos y el servidor web a la última versión
- Modificar contraseñas: FTP, e-mail, bases de datos y de acceso al panel de administración
- Utilizar únicamente los plugins necesarios y eliminar el resto
- Eliminar todos los archivos maliciosos

ANEXO



REFERENCIAS

Fuentes:

The hackers news https://thehackernews.com/2024/03/cybercriminals-using-novel-dns.html

Canal de extorsión **https://t[.]me/yanz54321**

Evidencia existencia código malicioso www.virustotal.com/gui/url/9771a84d9d7e080480c932a5a99d28727fade400f9a07cee9a17f1e443e56d36?nocache=1