CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas cibernéticas

Fecha: 07/11/2023

Problemática: SideCopy explotó falla de WinRAR en ataques dirigidos a entidades gubernamentales Indias

Correlativo: AC-0095

Institución / Sector: Público y Privado

CONTEXTO

El actor de amenazas SideCopy, vinculado a Pakistán, aprovechó la vulnerabilidad de seguridad de WinRAR para atacar a entidades gubernamentales de la India para enviar troyanos de acceso remoto (AllaKore RAT, Ares RAT y DRat). Además, los ataques también fueron diseñados para infiltrarse en sistemas Linux con una versión compatible de Ares RAT.

RECOMENDACIÓN

- Desactivar el servicio SLP en sistemas que se ejecutan en redes que no son de confianza.
- Realizar respaldos de la información de los sistemas de su organización en forma regular.
- Mantener el sistema de respaldos de forma separada.
- Mantener los sistemas actualizados a la última versión.
- Monitorear sus sistemas en busca de actividad sospechosa.

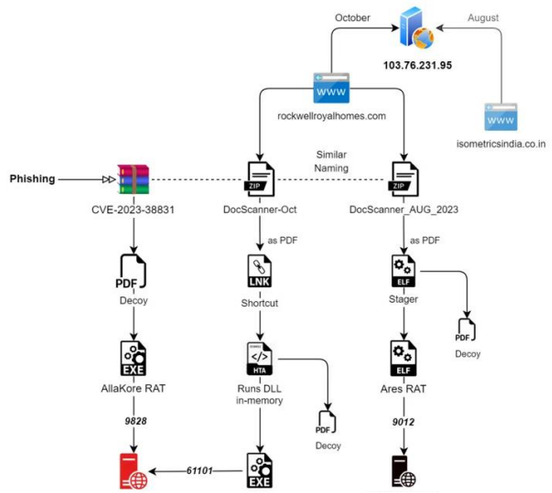
Nivel de priorización

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

Matriz de Evaluación

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

ANEXO



REFERENCIAS

The hacker News
https://thehackernews.com/2023/11/sidecopy-exploiting-winrar-flaw-in.html