CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenazas cibernéticas

Fecha: **18/01/2024**

Problemática: **Utilización de TeamViewer para violar redes en ataques de ransomware**

Correlativo: **AC-0001**

Institución / Sector: **Público y Privado**

SITUACIÓN

Plataforma de seguridad «Huntress», detectó que ciberdelincuentes están utilizando TeamViewer para obtener acceso inicial a los puntos finales de las organizaciones e intentar implementar diferentes tipos de malware o ransomware.

El proveedor informó que la mayoría de casos están relacionados a un debilitamiento de la configuración de la seguridad predeterminada del software.

Nivel de priorización

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

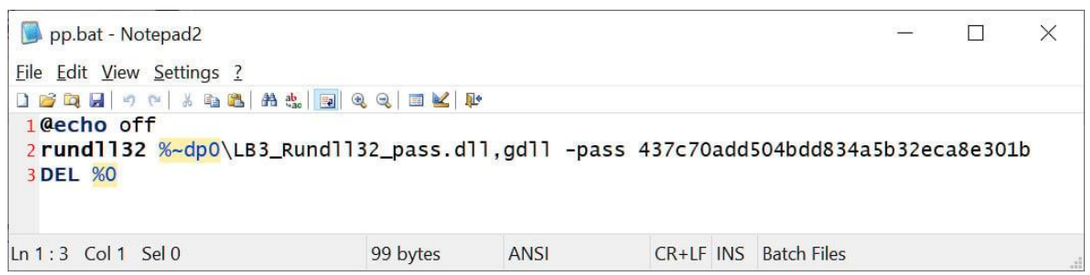
Matriz de Evaluación

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

RECOMENDACIONES

- Utilizar contraseñas seguras para cuentas de TeamViewer.
- Monitorear todos los puntos finales de TeamViewer, incluso los que no se utilizan con frecuencia.
- Realizar copias de seguridad periódicas.
- Mantener los sistemas de seguridad actualizados.
- Implementar la actualización de dos factores.

ANEXO



Archivo PP.bat utilizado para la ejecución del cifrador de ransomware en TeamViewer.

REFERENCIAS

Fuente: TeamViewer
https://www.bleepingcomputer.com/news/security/teamviewer-abused-to-breach-networks-in-new-ransomware-attacks/