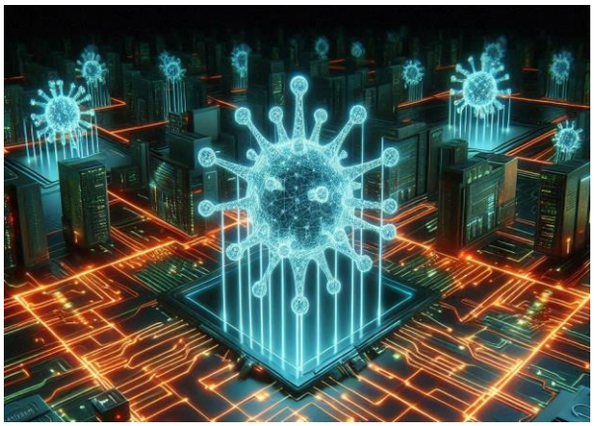
ALERTA

Nuevo Malware Poco RAT Ataca Sector Minero

COLCERT AL-1207-035



RCP/RCE

TLP:CLEAR

" Objetivo: Empresas del sector minero, principalmente de habla hispana"

Poco RAT es un nuevo troyano de acceso remoto (RAT) que se dirige principalmente a empresas del sector minero, particularmente a víctimas de habla hispana. El malware utiliza métodos de entrega evasivos como enlaces de Google Drive y archivos HTML para infectar sistemas. Poco RAT puede descargar y ejecutar malware adicional, lo que lo convierte en una amenaza potencial para ataques más sofisticados como robo de información o ransomware.

Impacto para la Seguridad Digital:

- Robo de información confidencial.
- Instalación de ransomware.
- Disrupción de operaciones.
- Pérdidas financieras.

Características:

•Utiliza bibliotecas POCO C++ para dificultar la detección.

•Se entrega como ejecutable Delphi empaquetado con UPX.

Infección del Malware:

Métodos de entrega:

•Enlaces de Google Drive incrustados en correos electrónicos.

•Archivos HTML con enlaces de Google Drive incrustados.

•Archivos PDF adjuntos con enlaces de Google Drive.

Para protegerse contra esta Ciberamenaza

Mantener el software actualizado: Aplicar parches de seguridad para sistemas operativos y aplicaciones.

Estar atento a la actividad inusual: Monitorear la red y los sistemas para detectar comportamientos sospechosos.

Reportar: Informar sobre cualquier actividad sospechosa al ColCERT.

Revisión de links redireccionados a servicios de Google. De igual manera actualizar versiones en estos productos.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://cofense.com/blog/new-malware-campaign-targeting-spanish-language-victims/

https://www.darkreading.com/cyberattacks-data-breaches/poco-rat-burrows-deep-mining-sector

COLCERT