	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°160	Fecha: 07-07-2023
		Página: 8 de 27

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	RedEnergy Stealer-as-a-Ransomware Amenaza dirigida a los sectores de energía y telecomunicaciones		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

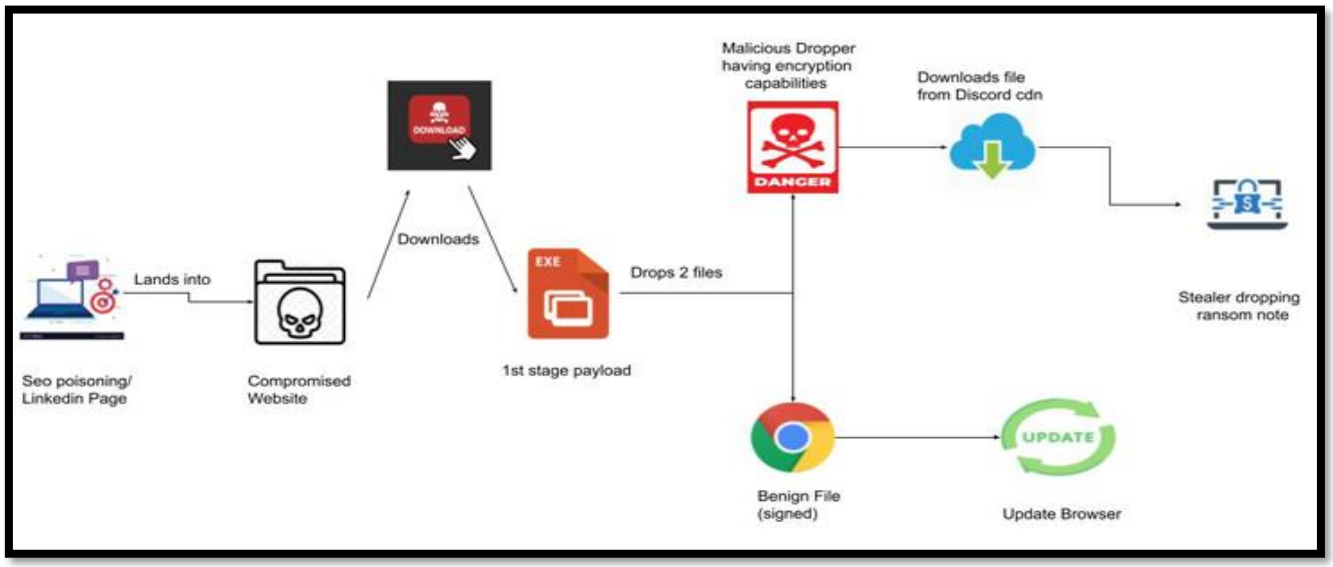
1. **ANTECEDENTES**

El 05 de julio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio, se ha tomado conocimiento de una sofisticada amenaza de un ransomware denominada RedEnergy, que ha sido detectada en los sectores de servicios públicos de energía, petróleo, gas, telecomunicaciones y maquinaria a través de sus páginas de LinkedIn.

2. **DETALLES**:

El malware posee la capacidad de robar información de varios navegadores, lo que permite la ex filtración de datos confidenciales, al tiempo que incorpora diferentes módulos para llevar a cabo actividades de ransomware.

Lo que lo hace novedoso es el uso de páginas acreditadas de LinkedIn para apuntar a las víctimas, redirigiendo a los usuarios que hacen clic en las URL del sitio web a una página de destino falsa que les pide que actualicen sus navegadores web haciendo clic en el ícono apropiado (Google Chrome, Microsoft Edge, Mozilla Firefox, u Opera), lo que resulta en la descarga de un ejecutable malicioso.



Los ciberdelinduentes esperan que las victimas realizan un pago de 0,005 BTC (alrededor de $151.00) a una billetera de criptomonedas mencionada en la nota para recuperar el acceso a los archivos, el desarrollo también sigue a la aparición de una nueva categoría de amenazas RAT como ransomware en la que los troyanos de acceso remoto como Venom RAT y Anarchy Panel RAT se han equipado con módulos de ransomware para bloquear varias extensiones de archivo detrás de barreras de cifrado.

3. **RECOMENDACIONES**:

- Evitar acceder a sitios vinculados desde los perfiles de LinkedIn.
- Mantener los firewalls actualizados.
- Descargar archivos de fuentes confiables.

Fuente de Información:	• hxxps://thehackernews.com/2023/07/redenergy-stealer-as-ransomware-threat.html • hxxps://www.hualkana.com/redenergy-stealer-as-a-ransomware-amenaza-dirigida-a-los-sectores-de-energia-y-telecomunicaciones/