Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°001	Fecha: 01-01-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	CARBANAK: El malware bancario que se convierte en ransomware		
Tipo de Ataque	Malware	Abreviatura	Malware
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 malware bancario conocido como Carbanak se ha utilizado en ataques de ransomware con tácticas actualizadas. El malware se ha adaptado para incorporar proveedores de ataques y técnicas para diversificar su efectividad.

Carbanak regresó el mes pasado a través de nuevas cadenas de distribución y se ha distribuido a través de sitios web comprometidos para hacerse pasar por varios programas relacionados con el negocio. Algunas de las herramientas suplantadas incluyen software popular relacionado con los negocios, como HubSpot, Veeam y Xero.

Carbanak, detectado en la naturaleza desde al menos 2014, es conocido por sus funciones de exfiltración de datos y control remoto. Comenzando como un malware bancario, ha sido utilizado por el sindicato de ciberdelincuencia FIN7.

2. DETALLES:

Los ataques de Carbanak suelen comenzar con una campaña de phishing que engaña a los usuarios para que abran un archivo adjunto malicioso o hagan clic en un enlace malicioso. Una vez que el malware se ejecuta en el sistema de una víctima, puede robar datos, instalar malware adicional o tomar el control del sistema.

En los ataques recientes, Carbanak se ha distribuido a través de sitios web comprometidos que se hacen pasar por sitios web legítimos. Estos sitios web pueden alojar archivos de instalación maliciosos que se disfrazan como software legítimo. Cuando un usuario descarga e instala uno de estos archivos, se instala Carbanak en el sistema de la víctima.

Los sectores industriales (33%), cíclicos de consumo (18%), y atención médica (11%) se encuentran entre los más afectados. América del Norte lidera con el 50% de los ataques, seguido por Europa (30%) y Asia (10%).

En cuanto a las familias de ransomware detectadas con más frecuencia, LockBit , BlackCat y Play contribuyeron al 47% (o 206 ataques) de 442 ataques. Con BlackCat desmantelado por las autoridades este mes, queda por ver qué impacto tendrá la medida en el panorama de amenazas en el futuro cercano.

3. RECOMENDACIONES:

- Hacer uso del doble factor de autentificación.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos no solicitados o mensajes de redes sociales.
- Mantener el software actualizado con las últimas correcciones de seguridad.
- Implementar soluciones antivirus y antimalware.
- Implementar un firewall para controlar el tráfico de entrada y salida.
- Educar a los empleados sobre las amenazas de correo electrónico malicioso y cómo identificarlo.
- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- No pagar el rescate ni contactar con los ciberdelincuentes, en caso de infección, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados.

Fuente de Información:	• hxxps://widefense.com/observatorio-de-amenazas/carbanak-el-malware-que-se-convierte-en-ransomware • hxxps://devel.group/blog/carbanak-combina-el-robo-bancario-con-el-secuestro-de-datos/