	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 140	Fecha: 14-06-2023
		Página 9 de 34

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Malware basado en Golang con el nombre de Skuld vienen afectando los sistemas operativos Windows.		
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

ANTECEDENTES:

El 13 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tomó conocimiento acerca de un nuevo ladrón de información basado malware basado en Golang, llamado Skuld que viene comprometiendo los sistemas Windows en Europa, el sudeste asiático y los EE. UU.

DETALLES:

Esta nueva cepa de malware intenta robar información confidencial de sus víctimas, mediante la búsqueda de datos almacenados en aplicaciones como Discord y navegadores web; por otro lado, también la información del sistema y archivos almacenados en las carpetas de la víctima.

Skuld, viene compartiendo superposiciones con ladrones disponibles públicamente como Emperador de cereales, Luna Grabber, y BlackCap Grabber, este malware es la obra de un desarrollador que se presenta en línea como Deathined y en varias plataformas de redes sociales como GitHub, Twitter, Reddit y Tumblr.

El malware, tras la ejecución, verifica si se está ejecutando en un entorno virtual en un intento de frustrar el análisis. Extrae además la lista de procesos en ejecución y la compara con una lista de bloques predefinida. Si algún proceso coincide con los presentes en la lista de bloques, Skuld procede a terminar el proceso coincidente en lugar de terminar.

Además de recopilar metadatos del sistema, el malware posee capacidades para cosechar cookies y credenciales almacenadas en navegadores web, así como archivos presentes en las carpetas de perfiles de usuario de Windows, incluidos Escritorio, Documentos, Descargas, Imágenes, música, videos y OneDrive.

Este malware muestra un diseñado versátil para corromper archivos legítimos asociados con Better Discord y Discord Token Protector e inyectar código JavaScript en la aplicación Discord para desviar códigos de respaldo, reflejando una técnica similar a la de otro infostealer basado en óxido. Por su naturaleza compilada de Golang permite a los autores de malware producir ejecutables binarios que son más desafiantes de analizar, lo que dificulta que los investigadores de seguridad encuentren soluciones eficaces para que detecten y mitiguen este malware de manera efectiva.

RECOMENDACIONES:

- Mantener actualizado el sistema operativo.
- Instalar un software antivirus/malware.

Fuentes de información	hxxps://thehackernews.com/2023/06/new-golang-based-skuld-malware-stealing.html