DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 133**	**Fecha: 07-06-2023**
		Página 5 de 10

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Nueva campaña de ransomware como servicio dirigido a equipos con sistema operativo Windows, Linux y macOS		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. **Resumen:**

Investigadores de la firma de seguridad Uptycs, han informado que los actores de amenazas vinculados al ransomware "Cyclops" están ofreciendo un ladrón de información (Stealer) basado en Go y desarrollado para dirigir sus ataques a sistemas Windows, Linux y macOS. El actor de amenazas detrás de este RaaS (Ransomware como servicio) promueve su oferta en foros de delitos informáticos a cambio de una parte de las ganancias. El ransomware admite un proceso de cifrado complejo. Un ataque exitoso podría permitir a un atacante robar datos confidenciales de los sistemas infectados.

2. **Detalles:**

- Los investigadores informaron que los actores de amenazas vinculados al ransomware Cyclops están ofreciendo un ladrón de información basado en Go.
- El grupo Cyclops ha desarrollado ransomware multiplataforma que puede infectar sistemas Windows, Linux y macOS. El desarrollador de amenazas proporciona un panel separado para facilitar la distribución de su ransomware para los tres sistemas operativos antes mencionados. Dentro del mismo panel hay distintos binarios disponibles para el componente de ladrón auxiliar que está diseñado específicamente para Linux y Windows.
- El grupo ofrece un malware de ladrón de información separado que se puede usar para robar datos confidenciales de los sistemas infectados. Este ladrón de información basado en Go fue desarrollado para apuntar a archivos específicos tanto en Windows como en Linux. El ladrón es un binario ejecutable para sistemas x64 que extrae información del sistema de las máquinas infectadas.
- El ransomware admite un proceso de cifrado complejo, todas las funciones implementadas estáticamente usando una combinación de encriptaciones asimétricas y simétricas. Después del cifrado en Windows y Linux usando la clave pública, se agregan CRC32 y un marcador de archivo al final del archivo. Usado para identificar si el archivo ya ha sido encriptado (para no repetir el encriptado), el marcador de archivo de Linux es 00ABCDEF, mientras que en Windows es 00000000000000000000000000".
- La versión de Windows del ladrón de información se puede descargar desde el panel de administración de Cyclops como parte de un archivo que contiene el archivo stealer.exe y config.json. Tras la ejecución, el ladrón lee el archivo config. json ubicado en el mismo directorio que su ejecución. El archivo de configuración contiene una lista de nombres de archivo junto con las extensiones y tamaños correspondientes.
- Luego, el ladrón enumera los directorios y verifica la presencia de archivos específicos y extensiones de archivos específicas. Si se encuentran coincidencias, crea un nuevo archivo Zip protegido con contraseña (nombre de archivo zip-n.zip) que incluye una copia exacta del archivo identificado junto con su estructura de árbol de carpetas correspondiente. En seguida, los datos se extraen al servidor del atacante.
- La versión de Linux del ladrón de información también se obtiene del panel de administración de Cyclops como un archivo que contiene el archivo stealer.linux y config.json. Esta funcionalidad de ladrón es similar a la versión de Windows.
- El binario de Linux es un archivo compilado por Golang, donde los nombres de sus funciones se eliminan para dificultar la ingeniería inversa. Está basado en CGO, donde el código fuente está escrito en C y construido en Golang. Al ejecutar la muestra, proporciona opciones para cifrar archivos en una ruta específica, máquinas virtuales o habilitar la salida detallada. Los archivos presentes en /proc y /boot no están encriptados. Más bien, cifra los archivos que tienen extensiones. vmcx, .vmdk, .vmem, .vmrs, .vmsd, .vmsn, .txt, .csv, .lock, .pdb, .csv y muchos otros. Y deja caer una nota de rescate en cada carpeta que encripta.
- Los investigadores notaron que la lógica de cifrado del ransomware Cyclops comparte similitudes con el ransomware Babuk. Ambos usan Curve25519 y HC-256 para el cifrado de Windows y una combinación de Curve25519 y ChaCha. Las cadenas ejecutables se codifican y almacenan como una cadena de pila en el ransomware Cyclops.

- El mensaje de la nota de rescate apunta a un sitio de Onion que la víctima puede visitar para recuperar potencialmente sus archivos cifrados.

3. Productos afectados:

- Sistemas operativos: Windows, Linux y macOS.

4. Recomendaciones:

Los investigadores recomiendan:

- Promover la concientización y la educación de los usuarios es crucial para prevenir ataques exitosos. Los usuarios deben tener cuidado al manejar archivos adjuntos de correo electrónico, visitar sitios web sospechosos o descargar archivos de fuentes no confiables. La implementación de un filtrado de correo electrónico sólido y la capacitación sobre técnicas de phishing pueden mitigar de manera efectiva dichos riesgos;
- Realizar copias de seguridad periódicas de los datos críticos para mitigar el impacto de los ataques de ransomware. Sus copias de seguridad deben almacenarse de forma segura y probarse periódicamente para garantizar la integridad y disponibilidad de los datos;
- La actualización periódica de su software de seguridad y la realización de análisis del sistema pueden ayudar a detectar y prevenir tales amenazas;
- La transmisión de datos robados al servidor de un atacante destaca la importancia de la supervisión de la red y los sistemas de detección de intrusos (IDS). Las organizaciones deben invertir en medidas sólidas de seguridad de la red para identificar y bloquear el tráfico saliente sospechoso;
- Las organizaciones deben priorizar la implementación de la autenticación multifactor (MFA) para los sistemas críticos y el acceso a datos confidenciales. MFA agrega una capa adicional de seguridad, lo que hace que sea más difícil para los atacantes obtener acceso no autorizado al requerir factores de autenticación adicionales.

Fuentes de información	▪ hxxps://www.uptycs.com/blog/cyclops-ransomware-stealer-combo