En una muestra más de un próspero ecosistema de crimeware como servicio (CaaS), investigadores de ciberseguridad han descubierto un nuevo malware para robo de información basado en Windows llamado Meduza Stealer, que está siendo activamente desarrollado por su creador para evitar ser detectado por soluciones de software.

«El objetivo principal de Meduza Stealer es el robo exhaustivo de datos. Se apropia de las actividades de navegación de los usuarios, extrayendo una amplia gama de datos relacionados con los navegadores», informó Uptycs en un nuevo reporte.

> *«Ningún elemento digital está seguro, desde credenciales de inicio de sesión críticas hasta el valioso historial de navegación y marcadores cuidadosamente seleccionados. Incluso las extensiones para carteras criptográficas, gestores de contraseñas y extensiones 2FA son vulnerables».*

A pesar de tener características similares, Meduza presume de tener un diseño operativo «*astuto*» que evita el uso de técnicas de ofuscación y termina rápidamente su ejecución en los dispositivos comprometidos si no puede establecer conexión con el servidor del atacante.

También está diseñado para abortar si la ubicación del usuario se encuentra en la lista predefinida de países excluidos, que incluye a la Comunidad de Estados Independientes (CEI) y Turkmenistán.

Además de recopilar datos de 19 aplicaciones gestoras de contraseñas, 76 carteras criptográficas, 95 navegadores web, Discord, Steam y metadatos del sistema, Meduza Stealer también extrae entradas del Registro de Windows relacionadas con mineros y una lista de juegos instalados, lo que indica un objetivo financiero más amplio.

Actualmente se encuentra en venta en foros clandestinos como XSS y Exploit.in, así como en

un canal exclusivo de Telegram, como una suscripción recurrente que tiene un costo de $199 al mes, $399 por tres meses o $1,199 dólares por una licencia vitalicia. La información sustraída por el malware se ofrece a través de un panel web fácil de usar.

> *«Esta característica permite a los suscriptores descargar o eliminar los datos robados directamente desde la página web, brindándoles un nivel sin precedentes de control sobre su información obtenida ilícitamente»,* señalaron los investigadores.

> *«Este conjunto de funciones detalladas demuestra la naturaleza sofisticada del Meduza Stealer y hasta qué punto están dispuestos a llegar sus creadores para asegurar su éxito».*