| Centro Nacional de Seguridad Digital | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°309 | Fecha: 29-12-2023 |
|---|---|---|
| | | Página: 4 de 10 |

| | | | |
|---|---|---|---|
| Componente que reporta | **CENTRO NACIONAL DE SEGURIDAD DIGITAL** | | |
| Nombre de la alerta | Nuevo Medusa Stealer Ataca A Los Usuarios Para Robar Credenciales De Inicio De Sesión | | |
| Tipo de Ataque | Intento de acceso con vulneración de credenciales | Abreviatura | IAVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

**1. ANTECEDENTES:**

Mientras el mundo celebraba la Navidad, el hampa del cibercrimen se deleitaba con un tipo diferente de regalo: el lanzamiento de Meduza 2.2, un ladrón de contraseñas significativamente mejorado, listo para causar estragos en víctimas desprevenidas.

Los investigadores de ciberseguridad de Resecurity descubrieron los detalles del malware New Medusa Stealer.

Resecurity es una empresa de ciberseguridad especializada en protección de endpoints, gestión de riesgos e inteligencia sobre amenazas cibernéticas.

**2. DETALLES:**

Meduza 2.2 cuenta con una verdadera variedad de mejoras, que incluyen:

- Cobertura de software ampliada: el ladrón ahora apunta a más de 100 navegadores, 100 billeteras de criptomonedas y muchas otras aplicaciones como Telegram, Discord y administradores de contraseñas. Este alcance más amplio aumenta su potencial de victimización.
- Extracción de credenciales mejorada: Meduza 2.2 profundiza, capturando datos de los volcados de almacenamiento local del navegador, Windows Credential Manager y Windows Vault, desbloqueando un tesoro de información confidencial.
- Google Token Grabber: esta nueva función captura los tokens de las cuentas de Google, lo que permite a los atacantes manipular las cookies y obtener acceso a las cuentas comprometidas.
- Enfoque criptográfico mejorado: la compatibilidad con nuevas carteras de criptomonedas basadas en navegador como OKX y Enrypt, junto con la extracción de tokens de cuentas de Google, convierte a Meduza en una potente herramienta para el fraude financiero.
- Evasión mejorada: el ladrón cuenta con un código auxiliar de cifrado optimizado y técnicas de evasión AV mejoradas, lo que lo hace más difícil de detectar y eliminar.

Estos avances posicionan a Meduza como un competidor serio para jugadores establecidos como Azorult y Redline Stealer .

Su configuración flexible, amplia cobertura de aplicaciones y precio competitivo ($199 por mes) lo convierten en una opción atractiva para ciberdelincuentes de todos los niveles.

Las consecuencias de la adopción generalizada de Meduza son sombrías.

- Apropiación de cuentas (ATO): las credenciales robadas se pueden utilizar para secuestrar cuentas de correo electrónico, perfiles de redes sociales, cuentas bancarias y otros servicios en línea.
- Robo bancario en línea: los datos financieros obtenidos de máquinas infectadas pueden usarse para vaciar cuentas bancarias e iniciar transacciones fraudulentas.
- Robo de identidad: la información confidencial como nombres, direcciones y números de Seguro Social puede explotarse para robo de identidad y fraude financiero.

**3. RECOMENDACIONES:**

- Practicar una higiene estricta de las contraseñas. Utilizar contraseñas únicas y complejas para todas las cuentas.
- Habilitar la autenticación de dos factores cuando esté disponible.
- No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.
- Mantener el software actualizado. Actualizar periódicamente los sistemas operativos, las aplicaciones y el software de seguridad para corregir las vulnerabilidades.
- Implementar soluciones de seguridad integrales que puedan detectar y bloquear malware como Meduza.

| | |
|---|---|
| Fuente de Información: | • hxxps://gbhackers.com/new-medusa-stealer/#google_vignette |