	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 144	**Fecha: 20-06-2023**
		Página 6 de 29

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Mystic Stealer nuevo malware cada vez más utilizado en ataques.		
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		

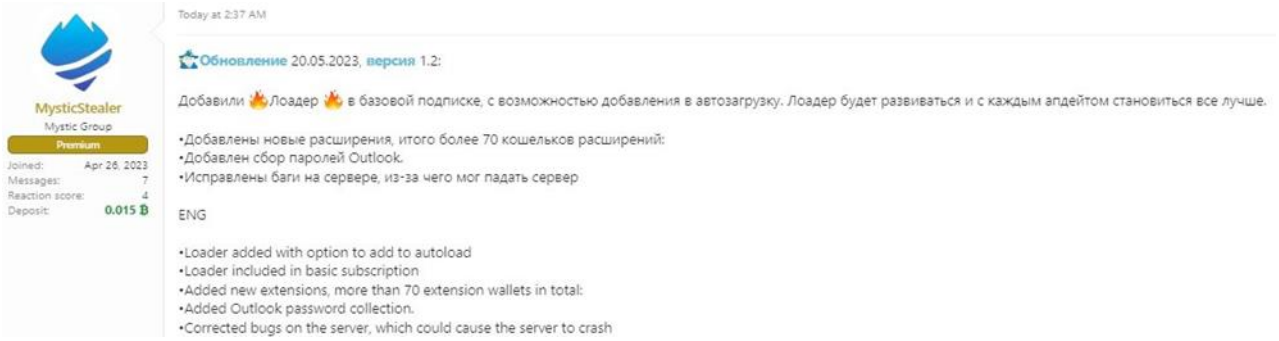
Descripción

ANTECEDENTES:

El 18 de junio del 2023, a través del monitoreo y búsqueda de amenazas en el ciberespacio los investigadores de seguridad cibernética han observado un nuevo malware de robo de información llamado 'Mystic Stealer' se ha promocionado en foros de piratería y mercados de darknet desde abril de 2023, ganando terreno rápidamente en la comunidad de delitos cibernéticos.

DETALLES:

El malware, alquilado por $ 150 / mes, se dirige a 40 navegadores web, 70 extensiones de navegador, 21 aplicaciones de criptomonedas, 9 aplicaciones de administración de contraseñas y MFA, 55 extensiones de navegador de criptomonedas, credenciales de Steam y Telegram, y más.



'Mystic Stealer' puede apuntar a todas las versiones de Windows, incluidas las de XP a 11, y admite arquitecturas de SO de 32 y 64 bits, el malware no necesita dependencias, por lo que su huella en los sistemas infectados es mínima, mientras que opera en la memoria para evitar la detección de los productos antivirus. Además, Mystic realiza varias comprobaciones de anti virtualización, como inspeccionar los detalles de CPUID para asegurarse de que no se ejecute en entornos de espacio aislado, el informe de Zscaler brinda la lista completa de aplicaciones específicas, que incluye navegadores web populares, administradores de contraseñas y aplicaciones de billetera de criptomonedas. Las entradas notables en la lista incluyen:

- Google Chrome.
- Mozilla Firefox.
- Borde de Microsoft.
- Ópera.

RECOMENDACIONES:

- Ser consciente de los enlaces y archivos adjuntos sospechosos.
- Examinar regularmente tus dispositivos.

Fuentes de información	hxxps://www.bleepingcomputer.com/news/security/new-mystic-stealer-malware-increasingly-used-in-attacks/