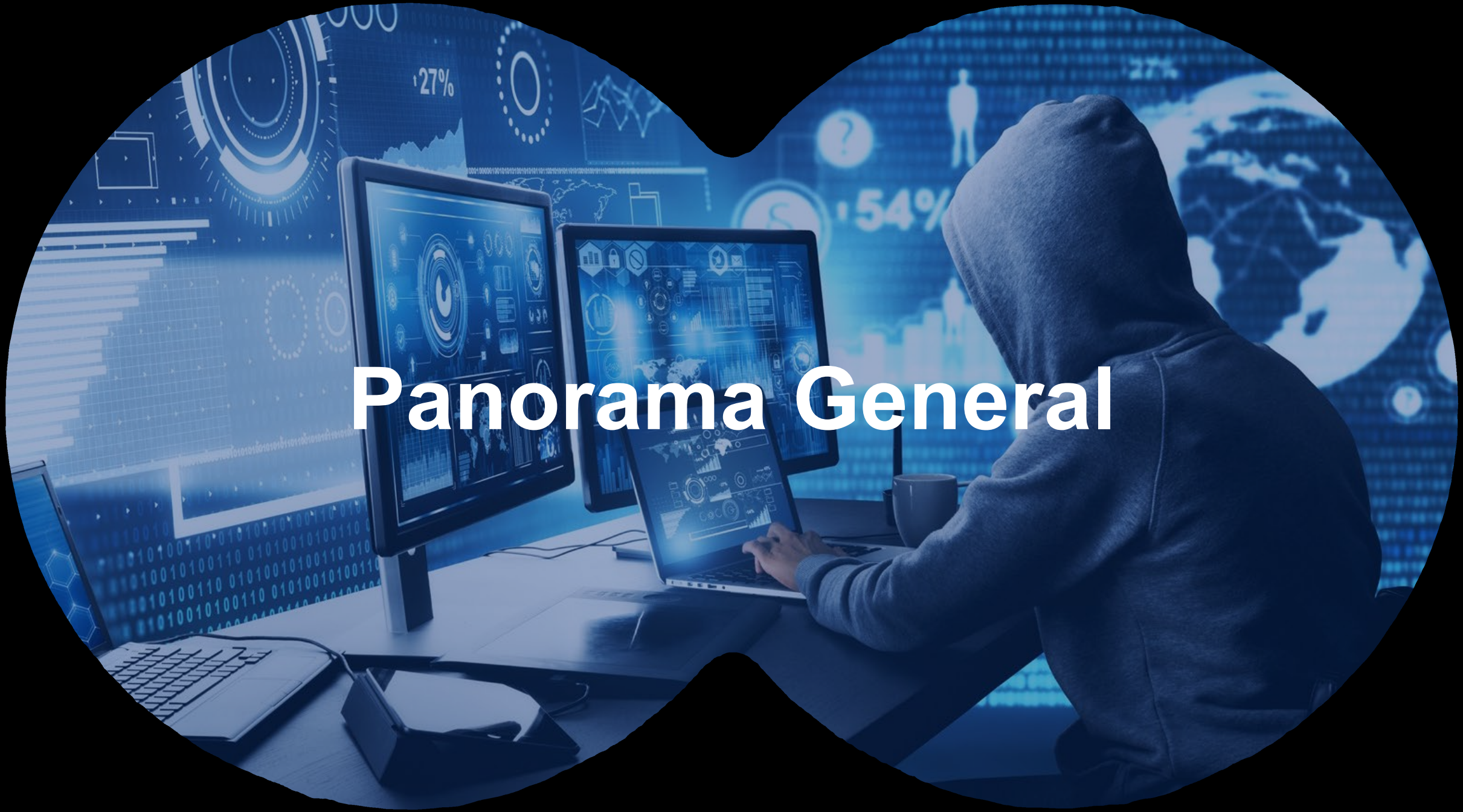
Marsh

Infostealers una amenaza creciente en Latinoamérica

Caso de estudio

Latinoamérica
Mayo 2025

Cyber Risk Consulting
Marsh Advisory



Panorama General

Descripción General

Los infostealers son programas maliciosos utilizados por los ciberdelincuentes para robar información, sobrepasando los controles antimalware.

Se han identificado diversas amenazas como los infostealers RedLine, LummaC2 o StealC, que cuentan con las mismas funciones. En algunos casos, nuevas variantes son solo clones de los anteriores.

Los cibercriminales utilizan estas amenazas para robar información bancaria o confidencial o, en algunos casos, son utilizados como vector de acceso inicial a las organizaciones.

Amenazas como RedLine Stealer fueron desmanteladas en el 2024; sin embargo otros infostealers han tomado su lugar como LummaC2 y StealC.

Principales objetivos de los infostealers

- Robo de credenciales
- Robo de datos financieros
- Robo de información sensible que pueda ser monetizada
- Extorsión
- Daño reputacional

Caso de estudio

Robo de información

Contexto: Los actores de amenazas se infiltraron en la red de la víctima usando credenciales válidas obtenidas de campañas de malware infostealer, con una ventaja mayor a 5 meses.

Vector de acceso inicial: Diversas campañas de malware, como MetaStealer y Vidar Stealer, LummaC2, RisePro Stealer, Vidar Steal, etc., comprometieron equipos corporativos y personales de empleados clave.

Detección del incidente: La organización detectó accesos comprometidos, lo que llevó a forzar el cambio de contraseñas y revisar registros para identificar otros posibles compromisos.

Duración del incidente: El incidente duró aproximadamente 2 meses, desde su detección hasta su contención, aunque el acceso inicial pudo ocurrir con varios meses de anticipación.

Afectaciones: La organización sufrió presión mediática y daño reputacional por la posible exfiltración de datos de clientes, además de enfrentar interrupciones operativas y potenciales multas.

Presencia en Latinoamérica: De acuerdo con análisis del Equipo de Respuesta ante Ciberincidentes de Marsh Advisory y nuestro centro de ciberinteligencia, se ha observado que los cibercriminales utilizan accesos comprometidos por infostealers como un medio inicial para infiltrarse en las organizaciones. Además, ha habido un aumento significativo en la infección de usuarios en equipos personales dentro de las organizaciones, debido al mal mal uso de sus cuentas corporativas, así como la capacidad de este software maliciosos para sobrepasar las medidas tradicionales de protección, además de su capacidad para permanecer ocultos por largos periodos de tiempo.

Línea de tiempo y actividad del atacante en el caso de estudio

Durante nuestros análisis de ciberinteligencia se observa que las organizaciones afectadas por infostealers tienen un tiempo promedio de detección de la amenaza (MTTD) mayor a 3 meses.

Etapa inicial del ataque | **Etapa de pre-ejecución del ataque** | **Etapa de impacto**

Ciclo de ataque general

Mes 1 - 4

- Usuarios de alto valor son comprometidos por infostealers
- Múltiples credenciales de acceso son ofertadas en la Deep y DarkWeb
- Usuarios secundarios son comprometidos con diversas campañas de infostealers.

Mes 5 - 6

- Atacante compra / accede a credenciales de acceso identificados en campañas de infostealers
- Campañas de infostealers siguen recopilando nuevos accesos de la organización
- Atacante ingresa a la organización y extrae información critica

Mes 7

- El atacante intenta realizar movimientos laterales en la red corporativa.

  Se inician acciones de contención y detección.
- Nuevos usuarios son comprometidos por campañas de infostealers
- Atacante continua con actividades de reconocimiento así como intentos de explotación y movimientos laterales

Mes 8

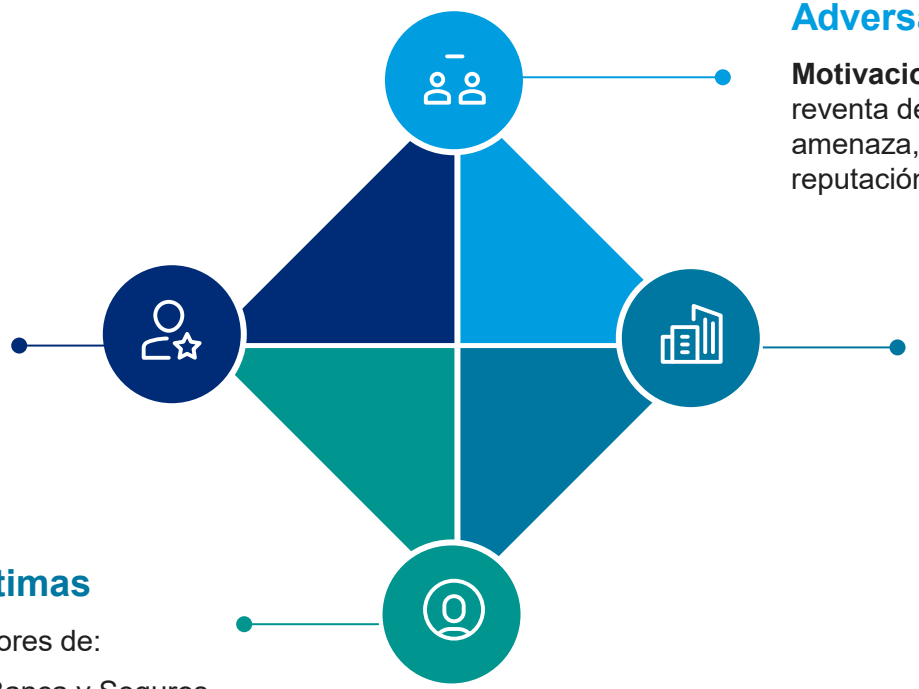
- Se observan múltiples intentos de abuso de credenciales
- Se continua acciones de contención y remediación y se finaliza e incidente

Modelo Diamante

De acuerdo con las capacidades y herramientas observadas, en el caso de estudio se aprecia que el actor de amenaza cuenta con conocimientos, capacidades e infraestructura de nivel medio.

Capacidades

- Identificación de vulnerabilidades de día cero (desconocidas) en herramientas de software utilizadas por personas y organizaciones
- Explotación de vulnerabilidades a nivel de infraestructura y aplicaciones web
- Personalización y uso de infostealers
- Uso de técnicas de anonimización para encubrir su origen
- Campañas de phishing



Adversario – MCTI2025001

Motivaciones: Robo de información, reventa de información a otros actores de amenaza, ciberextorsión y mejora de su reputación en la Dark Web.

Infraestructura

- Código malicioso capaz de capturar información y supervisar las actividades de las victimas
- Direcciones IP
- Servicios de hosting
- Servicios de alojamiento temporal
- Múltiples rutas de persistencia para la comunicación con sus servidores de Comando y Control

Víctimas

Sectores de:

- Banca y Seguros
- Manufactura
- Retail
- Alimentos y bebidas
- Gubernamental
- Telecomunicaciones
- Educativo
- Tecnología

Industrias afectadas

Top 10 infostealers observados en Latinoamérica entre 2024 - 2025

- Stealc Stealer
- LummaC2 Stealer
- Redline Stealer
- Cryptopbot Stealer
- RisePro Stealer
- Russian Password Stealer
- Vidar Stealer
- Dark Crystal Stealer
- Nexus Stealer
- MetaStealer

Marsh

Industrias con posible compromiso de infostealers en Latinoamérica 2024 – 2025

Usuarios por sector que han sido comprometidos por algún tipo de infostealer

El equipo de Ciberinteligencia de Marsh Advisory llevó a cabo un análisis de las diversas campañas de infostealers que han afectado a múltiples organizaciones en Latinoamérica entre 2024 y abril de 2025.

Se identifica que los actores de amenaza utilizan accesos comprometidos como un vector inicial para infiltrarse, lo que puede llevar a riesgos adicionales, como la fuga de información, el ransomware y accesos no autorizados.

Destacando varios puntos críticos que requieren atención:

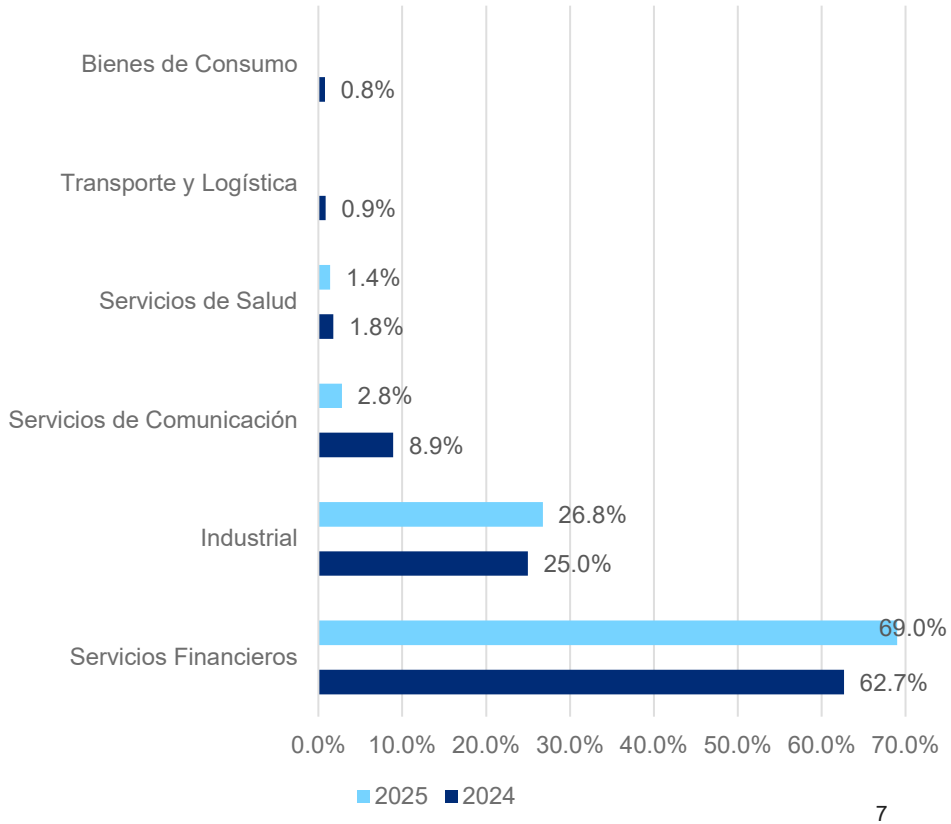
Uso de cuentas corporativas en servicios de terceros: Muchos usuarios registran sus cuentas corporativas en plataformas externas, aumentando la exposición a riesgos de seguridad.

Abuso de cuentas corporativas: Los usuarios utilizan los correos electrónicos corporativos para acceder a aplicaciones de terceros, comprometiendo la seguridad de la información.

Uso de cuentas corporativas en equipos no gestionados o inseguros: El uso de equipos personales o con inadecuados controles de seguridad para acceder a cuentas corporativas puede incrementar el riesgo de infección por software malicioso.

Estas prácticas pueden comprometer la integridad y confidencialidad de la información del usuario y de la organización. Es crucial que las empresas implementen políticas de seguridad más estrictas, programas de concienciación para mitigar estos riesgos y proteger sus activos críticos, así como estrategias de monitoreo más acordes a este tipo de amenazas.

Muestra de usuarios por sector comprometidos por infostealers 2024 - 2025

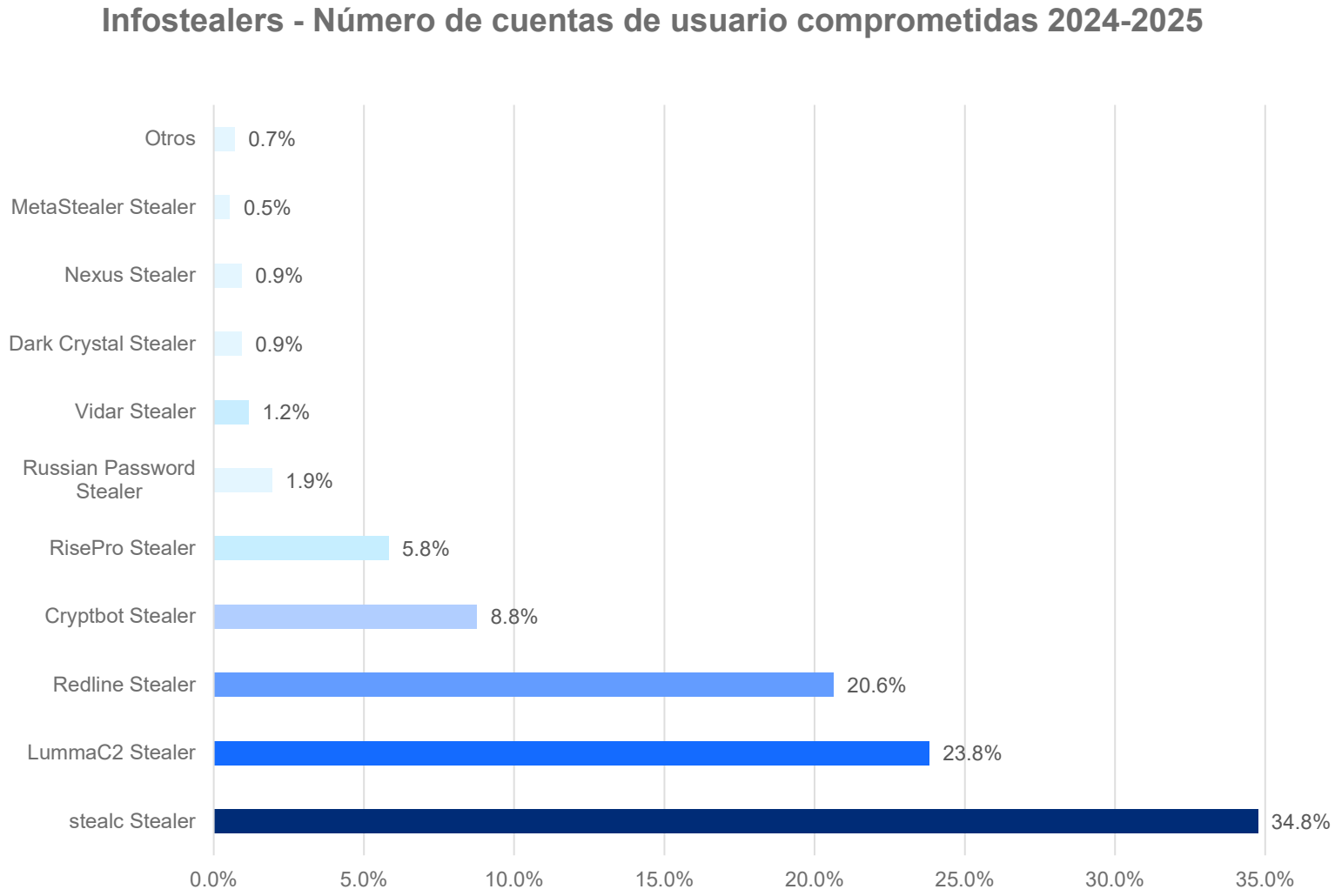


16 Campañas de malware (infostealers) fueron analizadas

El top 5 de amenazas con mayor actividad:

- Stealc Stealer
- LummaC2
- Redline Stealer (Desactivado en 2024)
- Cryptobot Stealer
- RisePro Stealer

StealC presentó el mayor número de cuentas de usuario comprometidas



Marsh

Recomendaciones para reducir el riesgo ante infostealers

A continuación se presentan algunas recomendaciones clave para enfrentar el riesgo relacionado con los infosteales, divididos en cuatro aspectos críticos:

01

Evaluación de riesgos

- Realizar auditorías de seguridad periódicas para identificar vulnerabilidades en los activos de la organización.
- Evaluar el uso de cuentas corporativas en servicios de terceros y su exposición a riesgos.
- Análisis y perfilamiento de usuarios para detectar aquellos con mayor nivel de exposición.

02

Políticas de seguridad

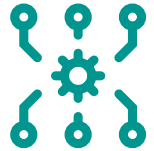
- Establecer políticas claras sobre el uso de cuentas corporativas en aplicaciones externas y servicios de terceros.
- Prohibir el registro de cuentas corporativas en plataformas y dispositivos no autorizados.
- Forzar el uso de múltiple factor de autentificación (MFA).
- Implementar políticas de contraseñas robustas.

03

Capacitación del personal

- Implementar programas de formación continua sobre ciberseguridad para todos los empleados.
- Fomentar la concienciación sobre los riesgos asociados con el uso de equipos personales y aplicaciones no autorizadas.
- Realizar pruebas periódicas de ingeniería social.

04



Monitoreo y Respuesta

- Establecer un proceso de monitoreo de ciberinteligencia.
- Realizar un monitoreo continuo para detectar accesos no autorizados y actividades sospechosas.
- Desarrollar un plan de respuesta a incidentes que incluya protocolos para la contención y remediación de este tipo de amenazas.

¿Cómo puede ayudar Marsh?

Cyber Incident Management

Prevención

- Evaluación de las capacidades de respuesta ante ciberincidentes
- Implementación de capacidades de ciberinteligencia
- Desarrollo del Plan de Respuesta ante Ciberincidentes y Playbooks
- Desarrollo del protocolo de respuesta organizacional frente a ransomware
- Desarrollo del plan de recuperación tecnológica en caso de ransomware
- Entrenamiento en gestión de cibercrisis
- Implementación de CYGNVS
- Evaluación y remediación de riesgos en la superficie de ataque (ASM)
- Cyber Threat Hunting

Prueba

- Simulación de cibercrisis a nivel del Comité de Crisis
- Simulación de respuesta ante ciberincidentes a nivel táctico/operativo
- Pruebas de Red Team
- Simulación de adversarios y malware

Respuesta

- Respuesta ante ciberincidentes y análisis forense digital, incluyendo:
  - Gestión de cibercrisis
  - Orquestación de la gestión de crisis cibernética y terceros involucrados
  - Análisis forense digital
  - Ciberinteligencia
  - Cyber Threat Hunting
  - Entre otros

Post

- Cyber Claims
- Taller de lecciones aprendidas
- Implementación de mejoras de seguridad

Marsh

Centro de Respuesta ante Ciberincidentes

Cyber Risk Consulting
Marsh Advisory

¿Está siendo o piensa que puede ser víctima de un ciberataque?

Você acha que foi ou pode ter sido vítima de um ataque cibernético?

Are you being or do you think you can be a victim of a cyberattack?

Agrega como contacto al Centro de Respuesta ante Ciberincidentes

Correo
cyberincident@marsh.com

Número de teléfono
+1 213 656 0333

Para conocer cómo podemos apoyar a su organización en la gestión del riesgo cibernético, póngase en contacto con nuestros profesionales.

Edson Villar

Líder de Consultoría en Riesgo Cibernético para Latinoamérica
Marsh Advisory
Edson.Villar@Marsh.com

Oscar Santoyo

Líder de Servicios de Respuesta ante Ciberincidentes para Latinoamérica
Marsh Advisory
Oscar.Santoyo@Marsh.com

Alberto Martinez

Líder de Consultoría en Riesgo Cibernético para México
Marsh Advisory
Alberto.Martinez01@Marsh.com

Armando Pérez

Consultor Senior de Servicios de Respuesta ante Ciberincidentes
Marsh Advisory
Armando.Perez@Marsh.com

Leonardo Nery

Consultor Senior de Servicios de Respuesta ante Ciberincidentes
Marsh Advisory
Leonardo.Nery@Marsh.com

Marsh

A business of Marsh McLennan