Advertencia

Técnica

Actividad reciente del actor de amenaza Kazu

COLCERT AD-20251113-030

TLP:CLEAR

Resumen Ejecutivo:

Kazu es un actor de amenaza cibernética emergente, identificado por su participación en actividades de **extorsión y filtración de información confidencial** a través de plataformas en la *dark web* y canales de comunicación cifrados. Su modo de operación consiste principalmente en **exfiltrar grandes volúmenes de datos de organizaciones públicas y privadas**, para posteriormente publicar evidencias parciales en sitios de fugas ("leak sites") como mecanismo de presión para el pago de rescates.

Desde mediados de 2025, este actor ha incrementado su actividad y ha sido asociado a múltiples campañas de exposición de datos en diferentes regiones, incluyendo América Latina, Asia y África. Los reportes más recientes lo vinculan con **ataques dirigidos a instituciones gubernamentales**, **organizaciones del sector salud** y empresas privadas, en los que asegura haber sustraído información de gran tamaño, acompañando las filtraciones con exigencias económicas significativas.

En el contexto colombiano, diversas fuentes de inteligencia de amenazas y plataformas de seguimiento de incidentes han documentado que **Kazu ha afectado a varias entidades nacionales**, logrando comprometer información sensible y posteriormente publicarla parcialmente en canales controlados por el actor. Si bien muchas de sus afirmaciones provienen directamente de sus propias publicaciones, el patrón operativo, las evidencias disponibles y la recurrencia de sus campañas sugieren que mantiene un nivel de organización y conocimiento técnico considerable, capaz de realizar intrusiones dirigidas y operaciones de exfiltración de datos a gran escala.

El impacto potencial de sus operaciones incluye exposición de información sensible, afectación reputacional, pérdida de confianza pública y posibles consecuencias legales para las organizaciones afectadas. La persistencia del actor y su enfoque en entidades gubernamentales y sectores críticos evidencian un riesgo alto para instituciones que manejen datos personales o información estratégica.

NIVEL DE RIESGO

ALTO

COLCERT

Kazu concentra la mayor parte de su actividad en **América Latina**, con presencia recurrente en países como Colombia, México, Perú, Argentina y Bolivia, donde ha dirigido múltiples publicaciones y reclamaciones. También muestra actividad significativa en Asia (especialmente Tailandia, Nepal, Sri Lanka e India) y en el Medio Oriente (entre otros Emiratos Árabes Unidos, Kuwait, Arabia Saudita e Irán). De forma adicional, registra incidentes puntuales en Norteamérica (Estados Unidos) y Europa (Italia, Reino Unido), así como algunos casos en África. En conjunto, **su alcance es interregional pero con fuerte concentración regional en América Latina, Asia y Medio Oriente**.

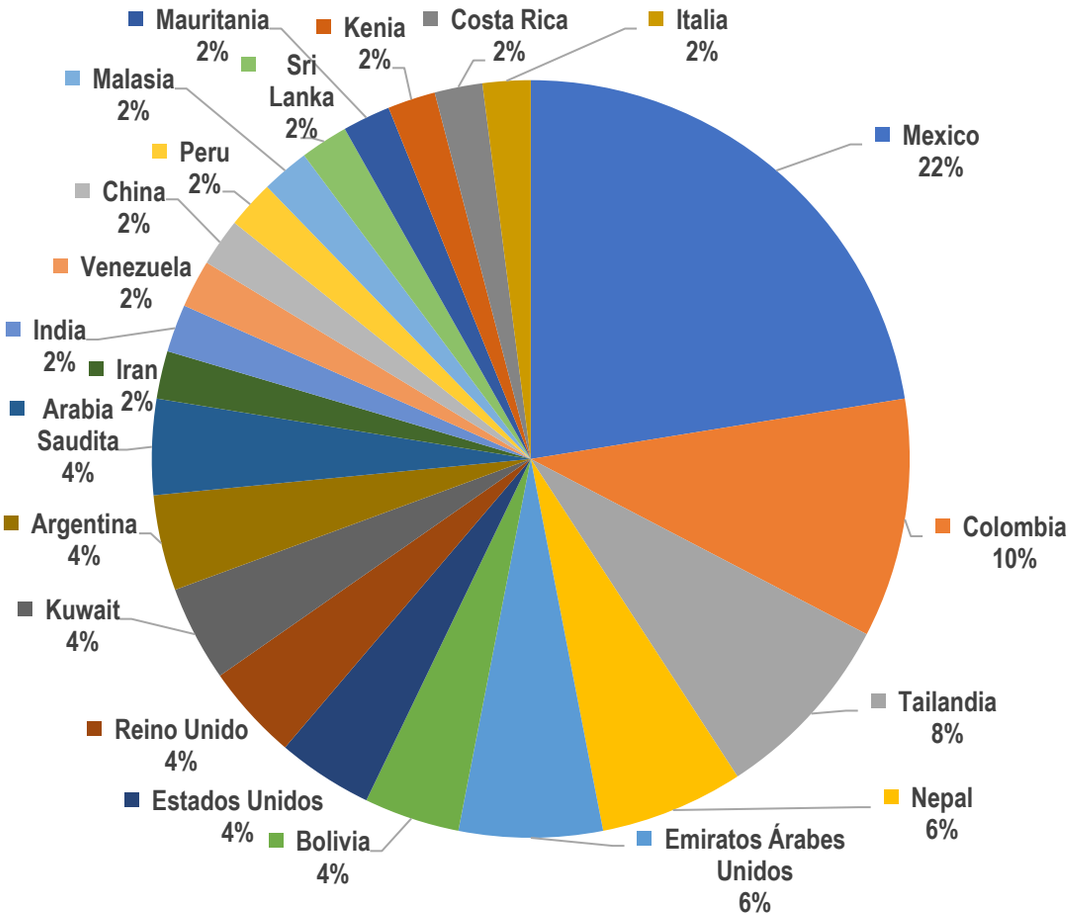

Gráfico 2. Países afectados por Kazu. Fuente: ColCERT.

Patrón de operación del actor

El modus operandi de Kazu se puede resumir en las siguientes fases:

- **Acceso inicial**: aún no se dispone de información técnica confirmada sobre las técnicas de intrusión, aunque se presume el uso de credenciales comprometidas o accesos expuestos (NAS, FTP, paneles administrativos), tal como lo reflejan sus publicaciones.
- **Exfiltración de datos**: el grupo sustrae volúmenes significativos de información sensible, usualmente entre 10 GB y 1 TB, según sus propias declaraciones.
- **Publicación parcial y extorsión**: se publica una muestra de los archivos robados para demostrar la intrusión y aumentar la presión sobre la víctima.
- **Comercialización o exposición total**: en caso de no concretar una negociación, los datos son puestos a la venta o liberados completamente.

Historial de aparición y principales campañas conocidas

El registro más antiguo atribuido a **Kazu** corresponde a junio de 2025, con publicaciones dirigidas al sector salud y gobierno en América Latina. Desde entonces, su actividad ha mostrado una tendencia de expansión geográfica rápida, afectando a más de 30 organizaciones en menos de cinco meses, distribuidas principalmente en América Latina, Asia y Medio Oriente, con presencia esporádica en Europa y África. El patrón cronológico evidencia una evolución progresiva en complejidad y alcance, pasando de instituciones regionales a organismos gubernamentales y entidades de defensa. En octubre y noviembre de 2025, se observa un incremento significativo en la frecuencia de sus publicaciones y en el tamaño de las brechas reclamadas.

Ámbitos geográficos y sectores objetivo

Kazu mantiene un enfoque global con clara prioridad hacia el sector gubernamental (53% de los casos), seguido de salud (15%), defensa (14%) y comercio. Los registros muestran actividad en más de 15 países, entre ellos **Colombia**.

En el contexto latinoamericano, el grupo ha demostrado una presencia sostenida y reiterada en 2025, afectando múltiples entidades nacionales, lo que refuerza la hipótesis de que **Kazu** mantiene un interés operativo en la región y dispone de acceso a infraestructuras o intermediarios con alcance continental.

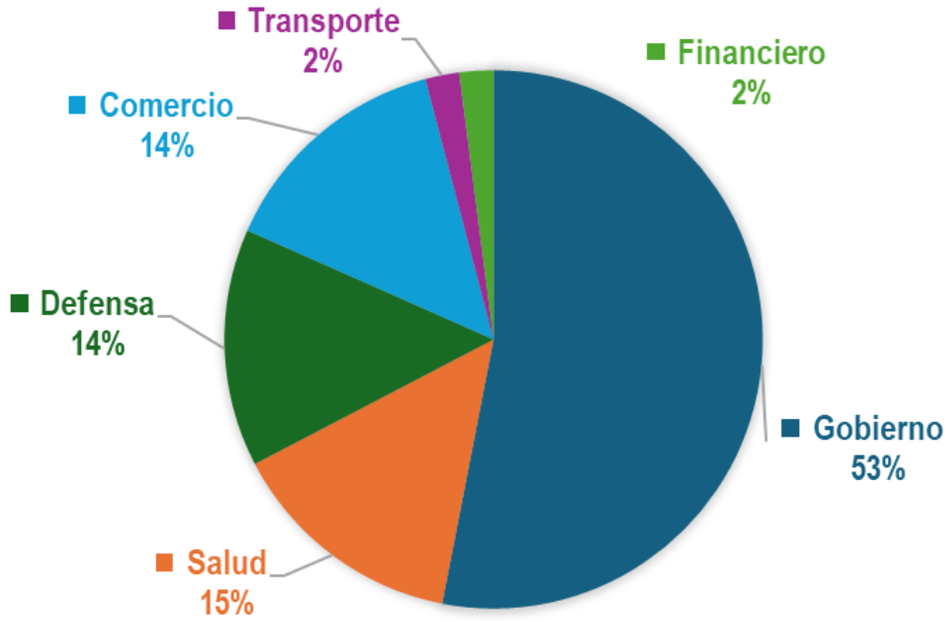

Gráfico 1. Sectores afectados por Kazu. Fuente: ColCERT.

Comportamiento y motivación

La motivación principal de **Kazu** parece ser económica, basada en la venta de información y en la obtención de beneficios a través del chantaje digital. Su estrategia de visibilidad pública **busca construir reputación** dentro de la comunidad cibercriminal para reforzar la credibilidad de sus amenazas. Asimismo, el grupo ha demostrado una capacidad de adaptación regional, alternando entre sectores y países con rapidez, lo que sugiere que **podría operar mediante intermediarios o afiliados** que ejecutan los ataques y luego canalizan los datos al grupo principal.

Plataformas y canales operativos

El actor **Kazu** mantiene una presencia activa en diferentes espacios digitales que utiliza para divulgar filtraciones, negociar con víctimas y comercializar información sustraída. Sus principales plataformas identificadas son

- **Sitio de filtraciones (leak site)**: es su principal medio de exposición pública. Publica listados de víctimas, fragmentos de datos exfiltrados y enlaces de descarga parcial. Utiliza este espacio como mecanismo de presión reputacional y demostración de legitimidad.
- **Canal en Telegram**: utilizada para difundir nuevos casos, actualizaciones y mensajes dirigidos a las víctimas. Se han observado anuncios de venta de accesos o bases de datos. Favorece la comunicación directa y la coordinación con intermediarios o afiliados.
- **Foros y mercados clandestinos**: espacios como DarkForums y Exploit.In son utilizados para ofrecer datos o accesos comprometidos. Estos entornos ayuda a mantener anonimato y diversificar canales de monetización.

Técnicas, Tácticas y Procedimientos (TTP) observados

Basado en patrones de víctimas y filtraciones asociadas, **Kazu** puede utilizar las siguientes técnicas que coinciden con el marco MITRE ATT&CK.

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Discovery	Collection	Command and Control	Exfiltration
T1190: Exploit Public-Facing Application	T1133: External Remote Services	T1078: Valid Accounts	T1078: Valid Accounts	T1083: File and Directory Discovery	T1005: Data from Local System	T1102: Web Service	T1041: Exfiltration Over C2 Channel
T1133: External Remote Services	T1078: Valid Accounts			T1018: Remote System Discovery			T1567: Exfiltration Over Web Service
T1078: Valid Accounts				T1082: System Information Discovery			T1567.002: Exfiltration to Cloud Storage

Tabla 1. TTP identificadas. Fuente: ColCERT.

Conclusiones

- **Kazu** se ha consolidado como un actor de amenaza emergente y persistente, caracterizado por su enfoque en la exfiltración, exposición y comercialización de información confidencial. Su actividad se centra más en la publicación de datos que en el despliegue de ransomware o herramientas de cifrado.

- Aunque no existen evidencias públicas que vinculen a **Kazu** con una familia específica de *malware*, sus patrones de publicación y comunicación sugieren el uso de tácticas de intrusión y exfiltración discretas, posiblemente aprovechando accesos legítimos comprometidos, herramientas administrativas y técnicas de evasión de detección en entornos corporativos.

- En sus campañas recientes, **Kazu** ha diversificado las víctimas en múltiples sectores, abarcando principalmente organizaciones gubernamentales, salud y defensa, lo que sugiere una orientación oportunista y motivada económicamente, sin una ideología aparente.

- La evidencia en fuentes abiertas indica que Kazu opera principalmente en foros clandestinos y plataformas de filtración de datos, donde mantiene un canal de comunicación constante y un estilo de publicación que busca credibilidad frente a otros grupos, empleando un lenguaje técnico y mensajes de extorsión que apuntan a la exposición pública como medio de presión.

- Dada la falta de información técnica pública sobre su infraestructura o herramientas específicas, se recomienda mantener una vigilancia basada en comportamientos y patrones de exfiltración, complementada con inteligencia táctica (TTP, cronología, alias y estilo de comunicación) para fortalecer la atribución y detección temprana.

- En síntesis, Kazu representa una amenaza activa en el panorama de exposición de datos y extorsión digital, cuyo impacto puede aumentar a medida que amplía su presencia en foros y perfecciona sus tácticas de acceso. La anticipación frente a este tipo de actores requiere una coordinación constante entre unidades de inteligencia cibernética, Csirt y equipos de respuesta a incidentes, así como el monitoreo permanente de fuentes clandestinas y canales de fuga de información.

Recomendaciones para prevenir compromisos similares

- Fortalecer la seguridad de los servicios y portales accesibles públicamente mediante actualizaciones constantes, análisis de vulnerabilidades y revisión periódica de configuraciones.

- Implementar autenticación multifactor (MFA) en todos los accesos administrativos, portales de gestión, paneles de control y servicios en la nube.

- Restringir la exposición de servicios (FTP, NAS, RDP, paneles de administración) sólo a redes internas o mediante túneles seguros (VPN o Zero Trust).

- Monitorear continuamente los registros de acceso y tráfico de salida para detectar comportamientos anómalos que puedan indicar exfiltración de datos o movimiento lateral.
- Capacitar al personal técnico y administrativo en prácticas de seguridad y respuesta ante incidentes, reforzando la detección temprana de comportamientos sospechosos.
- Evaluar periódicamente los respaldos y planes de recuperación ante desastres, asegurando su disponibilidad y su aislamiento de la red principal.
- Realizar auditorías de seguridad, pruebas de penetración y ejercicios de Red Team y Blue Team para identificar debilidades antes de que sean explotadas por actores externos.
- Establecer políticas de gestión de vulnerabilidades y parches con tiempos máximos de corrección acordes al nivel de criticidad de cada sistema.
- Clasificar y proteger la información sensible mediante cifrado en reposo y en tránsito, controles de acceso basados en roles y registro de actividades.
- Mantener canales de comunicación con los equipos de respuesta nacionales y con fuentes de inteligencia de amenazas para recibir alertas tempranas sobre campañas activas.

Indicador de Compromiso

- familia trojan.amn/bondat
- SHA256 743120e97bdbe63ba6138c56eff6ba6c07ed1c403b8bfa75bf1b4cfa2c1ccd18

Fuentes

CyHawk Africa, 25/10/2025, “Threat Actor Advertises Alleged 2.15 TB Data from Kenya’s Mobile Health Platform M-TIBA”, OSINT / blog.
https://cyhawk-africa.com/database/threat-actor-advertises-alleged-2-15tb-data-from-kenyas-mobile-health-platform-m-tiba/
Cyber Intelligence House, 21/07/2025, “Leak of the Week – July 21st”, OSINT / blog.
https://cyberintelligencehouse.com/leak-of-the-week-july-21st/
CYFIRMA, 24/10/2025, “Weekly Intelligence Report – 24 October 2025”, OSINT / newsanalysis.
https://www.cyfirma.com/news/weekly-intelligence-report-24-october-2025