

Actividades de ransomware identificadas en el primer semestre de 2026



Esta infografía resume la actividad de ransomware observada durante el primer semestre de 2026. El análisis recoge la evolución mensual de las víctimas publicadas por los grupos criminales, su distribución geográfica y los sectores más afectados, así como los actores con mayor nivel de actividad durante el periodo.

Así mismo, se examinan las vulnerabilidades asociadas públicamente a sus operaciones, los cambios registrados en el ranking de grupos y la aparición de nuevos actores. Esta información permite obtener una visión general de la evolución del ecosistema del ransomware y de sus principales patrones de actuación.

4.929

Víctimas en total
▲ +20,78% vs S1 2025

108

Grupos activos
▲ +13,68% vs S1 2025

100

Víctimas a nivel estatal
▲ +21,95% vs S1 2025

9

Casos en Euskadi
→ Se mantiene vs 2025

Evolución mensual de víctimas

Mes	Víctimas
Ene	795
Feb	886
Mar	844
Abr	870
May	809
Jun	725

Datos destacados del semestre

50%

del top 10 son nuevas entradas

×3

víctimas Qilin vs S1 2025

4

grupos asociados a CVE-2024-55591

▼2,99%

Casos a nivel estatal incluidos en el Top 10 por volumen total de víctimas

Top 10 países

Solo registros con país identificado

1	EE.UU.	61,41%	▼
2	Alemania	7,20%	▲
3	Gran Bretaña	6,15%	▲
4	Canadá	5,06%	▼
5	Francia	4,65%	▲
6	Italia	4,13%	▲
7	España	2,99%	▼
8	Brasil	2,97%	▼
9	India	2,79%	▼
10	Australia	2,65%	▼

Top 10 grupos con mayor actividad

Por total de víctimas publicadas

1	▲ Qilin	24,06%	1.121
2	→ Thegentlemen	15,24%	710
3	▲ Akira	11,44%	533
4	→ Dragonforce	9,12%	425
5	▲ Incransom	9,12%	425
6	→ NightSpire	7,53%	351
7	→ Lockbit5	7,00%	326
8	▲ Play	6,18%	288
9	▼ Clop	5,49%	256
10	→ Coinbase Cartel	4,81%	224

▲ Sube respecto a 2025 · ▼ Baja respecto a 2025 · → Nuevo en 2026



Impacto en Euskadi — S1 2026

9

casos confirmados · misma cifra que S1 2025

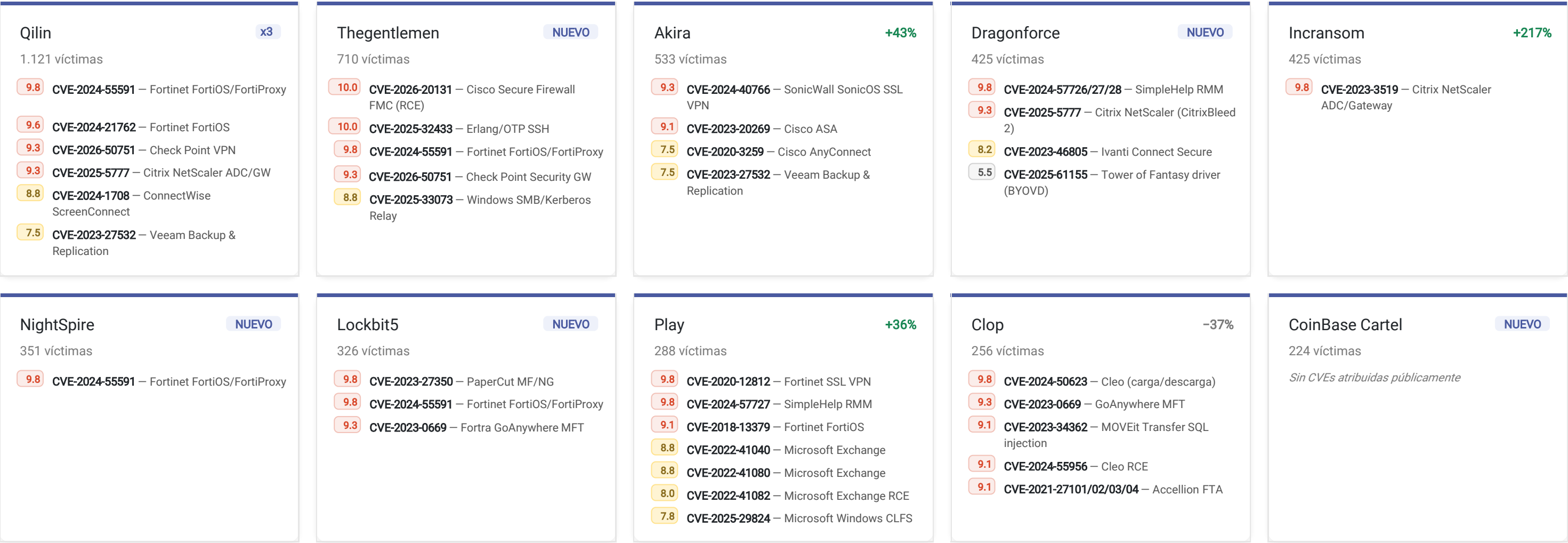
En el S1 2026 se han registrado 9 casos confirmados en Euskadi, manteniéndose la misma cifra que en el mismo período de 2025. NightSpire ha sido el grupo con mayor impacto en la región, afectando principalmente a organizaciones de los sectores de transporte, industria y servicios financieros.

Financiero

Industrial

Transporte

Vulnerabilidades explotadas por las familias de ransomware más activas en el primer semestre de 2026



CVE-2024-55591 (FortiOS/FortiProxy · CVSS 9.8 crítica) — la vulnerabilidad más explotada del semestre: confirmada en al menos 4 de los 10 grupos del ranking (Qilin, Thegentlemen, NightSpire y Lockbit5). Incluida en el catálogo CISA KEV.

Top controles CyberOrratz y ENS asociados

Controles que más contribuyen a prevenir, detectar y responder a esta tipología de incidente.

CYBERORRATZ	CONTROL	ENS	IMPACTO
G2.7 / P1.2	Política antimalware / control de código malicioso	op.exp.6	Reduce vulnerabilidad
P2.7	Comunicaciones externas cifradas	mp.com.3/4	Reduce vulnerabilidad
P2.5	Parches de seguridad	op.exp.2	Reduce vulnerabilidad
P2.8	Administración segura	op.mon.1/2	Detecta actividad
P2.2	Política de contraseñas	op.acc.2	Evita acceso inicial
P3.5	2FA / MFA	op.acc.6	Evita acceso inicial
G2.4	Política de gestión de identidades (IAM)	op.acc.2/4	Evita acceso inicial
P1.4	Identidades únicas	op.acc.4/org.4	Evita acceso inicial
P1.2	Control de código malicioso	op.exp.6	Reduce vulnerabilidad
P1.5	Instalación segura	op.exp.2	Reduce vulnerabilidad

Conclusiones

- 01

Incremento en el número de víctimas. ↑ +20,78% víctimas globales (4.081→4.929) y ↑ +21,95% en el Estado (82→100). El ransomware sigue creciendo a nivel global, con un incremento significativo respecto al mismo período del año anterior.
- 02

Liderazgo de Qilin en un ecosistema fragmentado. Qilin encabeza la actividad observada con el 24% de las víctimas publicadas. Sin embargo, la existencia de 108 grupos activos y la entrada de cinco actores en el top 10 evidencian una elevada fragmentación y rotación del ecosistema.
- 03

Especialización y nuevos actores. Qilin pivota hacia manufactura y finanzas; DragonForce se especializa en Proveedores de Servicios Gestionados (MSPs) como multiplicador; Thegentlemen concentra el 40% en manufactura. Manufactura y Sanidad mantienen vulnerabilidad persistente independientemente de la geografía.
- 04

Impacto en Euskadi. 9 casos confirmados en S1 2026, misma cifra que el año anterior, lo que indica estabilización, pero no descenso de la amenaza. El grupo con mayor impacto en Euskadi ha sido NightSpire, con víctimas en los sectores de transporte, industria y servicios financieros. NightSpire explota principalmente CVE-2024-55591 (Fortinet FortiOS/FortiProxy, CVSS 9.8 crítica) como vector de acceso inicial, lo que hace prioritario verificar y parchear dispositivos Fortinet expuestos en el perímetro de las organizaciones vascas.

Recomendaciones — estrategias prioritarias

- ▶ Backups periódicos aislados y probados.

▶ Autenticación multifactor robusta (FIDO2).
- ▶ Parcheo urgente de vulnerabilidades de perímetro.

▶ Segmentación de redes (bloquear SMB/RDP/WinRM).
- ▶ Ley del mínimo privilegio.

▶ Formación en ciberseguridad.
- ▶ Planes de Continuidad de Negocio e Incidentes.

▶ Monitorización sectorial de amenazas.

Sectores de especial impacto

Manufactura y Sanidad

Energía y Sector Público

Servicios Financieros

Predicciones — segundo semestre 2026

Más grupos, más amenazas

El modelo RaaS sigue atrayendo nuevos actores. Nuevas entradas en el top 10 son previsibles en el segundo semestre.

Ataques más dirigidos

Manufactura, sanidad, energía y sector público seguirán siendo los sectores más atacados. Los Proveedores de Servicios Gestionados (MSPs) se consolidan como objetivo multiplicador de impacto.

Explotación de vulnerabilidades de perímetro

Se intensificará el uso de CVEs en VPNs, firewalls y herramientas RMM. El patrón de CVE compartida entre múltiples grupos (CVE-2024-55591) se repetirá con nuevas vulnerabilidades.

Euskadi

La estabilidad en el número de incidentes no implica una reducción de la amenaza. La exposición de organizaciones industriales y públicas exige mantener las medidas preventivas y la vigilancia.