



2026ko lehen seihilekoan identifikatutako ransomware-jarduerak

Infografia honek 2026ko lehen seihilekoan ikusitako ransomware-jarduera laburbiltzen du. Analisiak talde kriminalek argitaratutako biktimen hileko bilakaera, banaketa geografikoa eta sektore kaltetuenak jasotzen ditu, baita aldi horretan jarduera-maila handiena izan duten eragileak ere.

Era berean, haien eragiketei publikoki lotutako ahultasunak, taldeen rankingean erregistratutako aldaketak eta eragile berrien agerpena aztertzen dira. Informazio horri esker, ransomwarearen ekosistemaren bilakaeraren eta haren jarduera-eredu nagusien ikuspegi orokorra lor daiteke.

4.929

Biktimak guztira

▲ +20,78% vs S1 2025

108

Talde aktiboak

▲ +13,68% vs S1 2025

100

Biktimak estatu mailan

▲ +21,95% vs S1 2025

9

Kasuak Euskadin

→ Mantentzen dira vs 2025

Biktimen hileko bilakaera

Hilekoa	Biktimak
Urt	795
Ots	886
Mar	844
Api	870
Mai	809
Eka	725

Seihileko datu nabarmenak

50%

top 10tik sarrera berriak dira

×3

biktimak Qilin vs S1 2025

4

CVE-2024-55591ri lotutako taldeak

▼2,99%

Top 10ean sartutako estatu mailako kasuak, biktimen guztizko bolumenaren arabera

Top 10 herrialde

Identifikatutako herrialdea duten erregistroak bakarrik

1	AEB	61,41%	▼
2	Alemania	7,20%	▲
3	Britainia Handia	6,15%	▲
4	Kanada	5,06%	▼
5	Frantzia	4,65%	▲
6	Italia	4,13%	▲
7	Espainia	2,99%	▼
8	Brasil	2,97%	▼
9	India	2,79%	▼
10	Australia	2,65%	▼

Jarduera handieneko top 10 taldeak

Argitaratutako biktima guztiak kontuan hartuta

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

▲ Gora egin du 2025etik · ▼ Behera egin du 2025etik · → Berria 2026an



Eragina Euskadin — S1 2026

9

baieztatutako kasuak · S1 2025en zifra bera

S1 2026an baieztatutako 9 kasu erregistratu dira Euskadin, eta 2025eko aldi bereko zifra bera mantendu da. NightSpire izan da eskualdean eragin handiena izan duen taldea, batez ere garraio, industria eta finantza-zerbitzuen sektoreetako erakundeei eraginez.

Finantzario

Industrial

Garraioa

Ransomware-familia aktiboenek ustiatutako ahultasunak 2026ko lehen sei hilekoan



Qilin

x3

1.121 biktima

9.8

CVE-2024-55591

Fortinet FortiOS/FortiProxy

9.6

CVE-2024-21762

Fortinet FortiOS

9.3

CVE-2026-50751

Check Point VPN

9.3

CVE-2025-5777

Citrix NetScaler ADC/GW

8.8

CVE-2024-1708

ConnectWise ScreenConnect

7.5

CVE-2023-27532

Veeam Backup & Replication

Thegentlemen

BERRIA

710 biktima

10.0

CVE-2026-20131

Cisco Secure Firewall FMC (RCE)

10.0

CVE-2025-32433

Erlang/OTP SSH

9.8

CVE-2024-55591

Fortinet FortiOS/FortiProxy

9.3

CVE-2026-50751

Check Point Security GW

8.8

CVE-2025-33073

Windows SMB/Kerberos Relay

Akira

+43%

533 biktima

9.3

CVE-2024-40766

SonicWall SonicOS SSL VPN

9.1

CVE-2023-20269

Cisco ASA

7.5

CVE-2020-3259

Cisco AnyConnect

7.5

CVE-2023-27532

Veeam Backup & Replication

Dragonforce

BERRIA

425 biktima

9.8

CVE-2024-57726/27/28

SimpleHelp RMM

9.3

CVE-2025-5777

Citrix NetScaler (CitrixBleed 2)

8.2

CVE-2023-46805

Ivanti Connect Secure

5.5

CVE-2025-61155

Tower of Fantasy driver (BYOVD)

Incransom

+217%

425 biktima

9.8

CVE-2023-3519

Citrix NetScaler ADC/Gateway

NightSpire

BERRIA

351 biktima

9.8

CVE-2024-55591

Fortinet FortiOS/FortiProxy

Lockbit5

BERRIA

326 biktima

9.8

CVE-2023-27350

PaperCut MF/NG

9.8

CVE-2024-55591

Fortinet FortiOS/FortiProxy

9.3

CVE-2023-0669

Fortra GoAnywhere MFT

Play

+36%

288 biktima

9.8

CVE-2020-12812

Fortinet SSL VPN

9.8

CVE-2024-57727

SimpleHelp RMM

9.1

CVE-2018-13379

Fortinet FortiOS

8.8

CVE-2022-41040

Microsoft Exchange

8.8

CVE-2022-41080

Microsoft Exchange

8.0

CVE-2022-41082

Microsoft Exchange RCE

7.8

CVE-2025-29824

Microsoft Windows CLFS

Clop

-37%

256 biktima

9.8

CVE-2024-50623

Cleo (carga/descarga)

9.3

CVE-2023-0669

GoAnywhere MFT

9.1

CVE-2023-34362

MOVEit Transfer SQL injection

9.1

CVE-2024-55956

Cleo RCE

9.1

CVE-2021-27101/02/03/04

Accellion FTA

CoinBase Cartel

BERRIA

224 biktima

Publikoki esleitutako CVErik gabe



CVE-2024-55591 (FortiOS/FortiProxy · CVSS 9.8 kritikoa) – sei hileko ahultasun ustiatuena: rankingeko 10 taldeetatik 4tan gutxienez baieztatu da (Qilin, Thegentlemen, NightSpire eta Lockbit5). CISA KEV katalogoan sartuta dago.

CyberOrratz kontrol nagusiak eta lotutako ENS kontrolak

Intzidente mota honi aurreko prebentzioa, detekzioa eta erantzuna ematen gehien laguntzen duten kontrolak.

CYBERORRATZ	KONTROLA	ENS	ERAGINA
G2.7 / P1.2	Malwarearen aurkako politika / kode kaltegarriaren kontrola	op.exp.6	Ahultasuna murriztu
P2.7	Zifratutako kanpo-komunikazioak	mp.com.3/4	Ahultasuna murriztu
P2.5	Segurtasun-partxeak	op.exp.2	Ahultasuna murriztu
P2.8	Administrazio segurua	op.mon.1/2	Jarduera detektatu
P2.2	Pasahitzen politika	op.acc.2	Hasierako sarbidea ekidin
P3.5	2FA / MFA	op.acc.6	Hasierako sarbidea ekidin
G2.4	Identitateak kudeatzeko politika (MIA)	op.acc.2/4	Hasierako sarbidea ekidin
P1.4	Nortasun bakarrak	op.acc.4/org.4	Hasierako sarbidea ekidin
P1.2	Kode maltzuraren kontrola	op.exp.6	Ahultasuna murriztu
P1.5	Instalazio segurua	op.exp.2	Ahultasuna murriztu

Aurreikuspenak — 2026ko bigarren sei hilekoa

Talde gehiago, mehatxu gehiago

RaaS modeloak aktore berriak erakartzen jarraitzen du. Top 10ean sarrera berriak aurreikusten dira bigarren sei hilekoan.

Eraso gidatuagoak

Manufaktura, osasuna, energia eta sektore publikoa dira oraindik ere sektore erasotuenak. Kudeatutako zerbitzuen hornitzaileak inpaktua biderkatzeko helburu gisa finkatzen dira.

Perimetroko ahuleziak ustiatzea

VPN, firewall eta RMM erremintetan CVEen erabilera areagotuko da. Talde askoren artean partekatutako CVE ereduak (CVE-2024-55591) kalteberatasun berriekin errepikatuko da.

Euskadi

Istilu-kopuruaren egonkortasunak ez dakar mehatxua murriztea. Antolakunde industrialak eta publikoak erakusteko, prebentzio-neurriak eta zaintza mantendu behar dira.

Ondorioak

- 01

Biktima-kopuruaren igoera. ↑ +20,78% biktima globalak (4.081→4.929) eta ↑ +21,95% Estatuan (82→100). Ransomwareak gora egiten jarraitzen du maila globalean, eta igoera nabarmena izan du aurreko urteko aldi beraren aldean.
- 02

Qilinen lidergoa ekosistema zatikatu batean. Qilin da nagusi behatutako jardueran, argitaratutako biktimen % 24rekin. Hala ere, 108 talde aktibo egoteak eta top 10ean bost eragile sartzeak ekosistemaren zatiketa eta errotazio handia erakusten dute.
- 03

Espezializazioa eta aktore berriak. Qilin manufaktura eta finantzetara bideratuta dago; DragonForce Kudeatutako Zerbitzuen Hornitzaileetan (MSP) espezializatzen da biderkatzaile gisa; Thegentlemen manufakturan kontzentratzen da % 40. Manufaktura eta Osasunak ahultasun iraunkorra dute, geografia edozein dela ere.
- 04

Eragina Euskadin. 9 kasu baieztatu dira S1-2026an, aurreko urteko zifra bera; horrek esan nahi du mehatxua egonkortu egin dela, baina ez jaitsi. Euskadin eragin handiena izan duen taldea NightSpire izan da, eta biktimak izan dira garraioaren, industriaren eta finantza-zerbitzuen sektoreetan. NightSpirek CVE-2024-55591 (Fortinet FortiOS/FortiProxy, GZEK 9.8 kritikoa) ustiatzen du nagusiki hasierako sarbide-bektore gisa, eta, beraz, lehentasunezkoa da EAEko erakundearen perimetroan dauden Fortinet gailuak egiaztatzea eta adabakiak jartzea.

Gomendioak — lehentasunezko estrategiak

- Aldizkako backup isolatuak eta probatuak.

▸ Perimetroko ahulezien premiazko adabakia.

▸ Gutxieneko pribilegioaren legea.

▸ Negozioarekin jarraitzeko planak eta gorabeherak.
- Faktore anitzeko autentifikazio sendoa (FIDO2).

▸ Sareen segmentazioa (blokeatu SMB/RDP/WinRM).

▸ Zibersegurtasuneko prestakuntza.

▸ Mehatxuen monitorizazio sektoriala.

Eragin bereziko sektoreak

Manufaktura eta Osasuna

Energia eta Sektore Publikoa

Finantza Zerbitzuak