

Jarraian, 2025eko identifikatutako Ransomware-taldeen jardueraren datu kuantitatiboak eta kualitatiboak adierazten dira, egungo egoera eta datozen hilabeteetarako bilakaera-joera ebaluatu ahal izateko.

Txostenean, aztertutako aldian zehar jarduera handiena erakutsi duten ransomware-taldeak nabarmentzen dira, aldi horretako biktima kopuruari dagokionez, baita

iraganean oso aktiboak izan ziren taldeak desagertu edo desegin ondoren sortu diren mehatxu berriak ere. Aurkikuntza horiek azpimarratu egiten dute garrantzitsua dela ransomwaretik babesteko estrategia espezifikoak ezartzea, bai eta gertakari mota horiei erantzuteko ere, horiek gauzatzen direnean.

Ransomware-erasoek kaltetutako biktimak



↑ Gora egin du 2024tik → Berria da 2024arekiko ↓ Behera egin du 2024tik

Biktimen hilabeteko bilakaera

URTARRILA	668	UZTAILA	548
OTSAILA	1.033	ABUZTUA	548
MARTXOA	695	IRAILA	615
APIRILA	554	URRIA	851
MAIATZA	632	AZAROA	729
EKAINA	510	ABENDUA	895

Ransomwarearen biktima gehien izan dituzten 10 herrialde

↑ AEB	%64.45	↑ Espainia	%3.08
↑ Kanada	%6.79	↑ Italia	%3.03
↓ Alemania	%6.30	↑ Brasil	%2.80
↓ Britainia Handia	%4.94	↓ India	%2.63
↑ Frantzia	%3.59	↑ Australia	%2.38

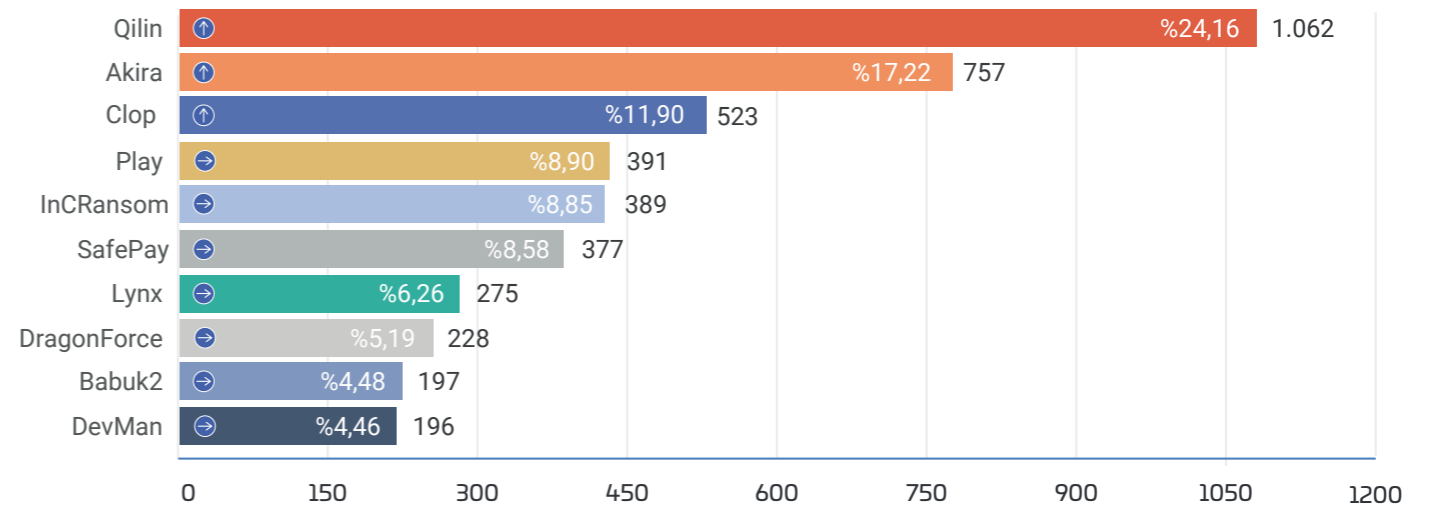
Aldaketak 2024 → 2025

- **RansomHub** desagertu da (2024an liderra zen %9,9arekin).
- **LockBit3** desagertu egin da (2024an 2.a, % 8,6rekin).
- **Dispossessor, Hunters, BlackBasta eta BianLian top10etik desagertzen dira.**

Lider berriak

- **Qilin** da liderra, %12,83rekin.
- **Akira** izugarri hazi da (%5,4 > %9,15).
- **Clop-a** % 6,32arekin agertzen da.

Top 10 talde aktiboak biktima globalen guztizkoa kontuan hartuta



Ransomware-familia aktiboek ustiatutako kalteberatasunak

Qilin - 1.062 biktima <ul style="list-style-type: none"> • CVE-2023-27532 (7.5 handia) – Veeam Backup & Replication 	Play - 391 biktima <ul style="list-style-type: none"> • CVE-2020-12812 (9.8 kritikoa) – Fortinet • CVE-2024-57727 (9.8 kritikoa) – SimpleHelp RMM • CVE-2018-13379 (9.1 kritikoa) – Fortinet • CVE-2022-41040 (8.8 handia) – Microsoft • CVE-2022-41082 (8.0 handia) – Microsoft • CVE-2025-29824 (7.8 handia) – Microsoft Windows CLFS 	DragonForce - 228 biktima <ul style="list-style-type: none"> • Ustiatutako cve ezagunik gabe
Akira - 757 biktima <ul style="list-style-type: none"> • CVE-2023-20269 (9.1 kritikoa) – Cisco • CVE-2020-3259 (7.5 handia) – Cisco • CVE-2023-27532 (7.5 handia) – Veeam Backup & Replication 	InCRansom - 389 biktima <ul style="list-style-type: none"> • CVE-2023-3519 (9.8 kritikoa) – Citrix 	Babuk - 219 biktima <ul style="list-style-type: none"> • CVE-2021-21974 (9.8 kritikoa) – VMware ESXi • CVE-2021-27876/27877/27878 (9.8 kritikoa) – Veritas Backup Exec
Clop - 523 biktima <ul style="list-style-type: none"> • CVE-2024-50623 (9.8 kritikoa) – Cleo • CVE-2023-0669 (9.3 kritikoa) – GoAnywhere MFT • CVE-2023-34362 (9.1 kritikoa) – MOVEit Transfer • CVE-2024-55956 (9.1 kritikoa) – Cleo • CVE-2021-27101/27102/27103/27104 (9.1 kritikoa) – Accellion FTA 	SafePay - 377 biktima <ul style="list-style-type: none"> • Ustiatutako cve ezagunik gabe 	DevMan - 196 biktima <ul style="list-style-type: none"> • Ustiatutako cve ezagunik gabe
Lynx - 275 biktima <ul style="list-style-type: none"> • Ustiatutako cve ezagunik gabe 		

Ondorioa: Merkatu oso zatikatua, sortzen ari diren lider berriekin eta espezializazio sektorial handiagorekin.

Top lotutako SEN kontrolak dituzten taldeak

Biktima gehien dituzten ransomware-taldeen analitik abiatuta, gertakari mota hori prebenitzen, detektatzen eta hari neurri handiagoan erantzuten laguntzen duten SENen kontrolak adierazten dira:

SEN KONTROLA (ID)	SEN O/E/A	ERAGIKETA-INPAKTUA
■ Segurtasun-gakoa (mp.inf.2)	OINARRIZKOA	Kalteberatasunak murrizten ditu
■ Bidegabe sartzea detektatzea (op.mon.1)	ERTAINA	Jarduera detektatzen du
■ Babeskopiak (backup) (op.cont.1)	OINARRIZKOA	Berreskuratzea ziurtatzen du
■ Aldaketak kudeatzea (op.exp.2)	OINARRIZKOA	Kalteberatasunak murrizten ditu
■ Eraginaren azterketa (op.exp.6)	OINARRIZKOA	Berreskuratzea ziurtatzen du
■ Segurtasun-arkitektura (mp.s.1)	ALTUA	Kalteberatasunak murrizten ditu
■ Sartzeko baldintzak (op.acc.2)	OINARRIZKOA	Hasierako sarbidea saihesten du
■ Sarbide-eskubideak kudeatzeko prozesua (op.acc.3)	ERTAINA	Hasierako sarbidea saihesten du
■ Autentifikazio-mekanismoa (kanpoko erabiltzaileak) (op.acc.5)	ERTAINA	Hasierako sarbidea saihesten du
■ Mantentze-lanak eta segurtasun-eguneratzeak (mp.si.2)	OINARRIZKOA	Kalteberatasunak murrizten ditu
■ Kode kaltegarriaren aurkako babesa (mp.cod.1)	OINARRIZKOA	Kalteberatasunak murrizten ditu
■ Urruneko sarbidea (remote login) (op.acc.7)	ERTAINA	Hasierako sarbidea saihesten du
■ Osotasunaren babesa (mp.info.4)	ERTAINA	Informazioa babesten du
■ Jarduera-erregistroa (op.exp.8)	OINARRIZKOA	Jarduera detektatzen du
■ Kontzientziazioa (mp.per.3)	OINARRIZKOA	Hasierako sarbidea saihesten du
■ Posta elektronikoaren babesa (mp.s.4)	OINARRIZKOA	Hasierako sarbidea saihesten du

2026ko Aurreikuspenak

- **Atomizazio handiagoa:** Zatiketak jarraituko du, eta talde espezializatu berriak agertuko dira.
- **Sektorekako hiperespezializazioa:** taldeek TTP espezifikoak hobetuko dituzte, industriaren eta geografiaren arabera.
- **IAren ustiapena:** Adimen artifizialaren erabilera erasoen ezagutza eta pertsonalizazioa optimizatzeke.
- **Euskadi:** Hazkunde jarraitua, manufakturan, retailen eta sektore publikoan arreta jarrita.

Ondorioak

1. Biktimen kopurua handitzea

- Ransomwareak **hazkunde esponenziala** izaten jarraitzen du 2025 osoan.

2. Zatiketaren sendotzea

- LockBit3 top-etik desagertzeak agerian uzten du **merkatua azkar zatikatzen dela**. Qilin, Clop eta Akira dira orain ekosistema lehiakorrago eta defenditzeko konplexuago baten buru.

3. Espezializazio sektorial egiaztatua

- Clop-ek azpiegitura kritikoetarako (**energia eta sektore publikoa**) oinarria finkatzen du.
- **Manufaktura eta Osasuna** zeharkako helburuak dira, zaugarritasun handikoak.

4. Ahultasun kritikoetan kontzentratzea

- Ustiapena **backup-eko softwarean** (Veeam), **fitxategien transferentzian** (MOVEit, Cleo, GoAnywhere) eta **urruneko kudeaketan** (Simple Help RMM) zentratzen da, 2023-2025eko CVE kritikoak bektore nagusi izanik.

Gomendioak

Lehentasunezko estrategiak:

- Aldizkako backup isolatuak.
- Faktore anitzeko autentifikazioa.
- Ahultasunak adabatzea.
- Sareen segmentazioa.
- Gutxieneko pribilegioaren legea.
- Zibersegurtasunari buruzko prestakuntza.
- Negozioarekin jarraitzeko planak, gorabeherei erantzuteko planak, etab.
- Mehatxuen monitorizazio sektoriala.

Eragin bereziko sektoreak:

- Manufaktura eta osasuna (kalteberatasun iraunkorra).
- Energia eta sektore publikoa (targeting gorakorra).
- Finantza-zerbitzuak (muturreko espezializazioa).

