# 2024an identifikatutako ransomware-jarduerak.

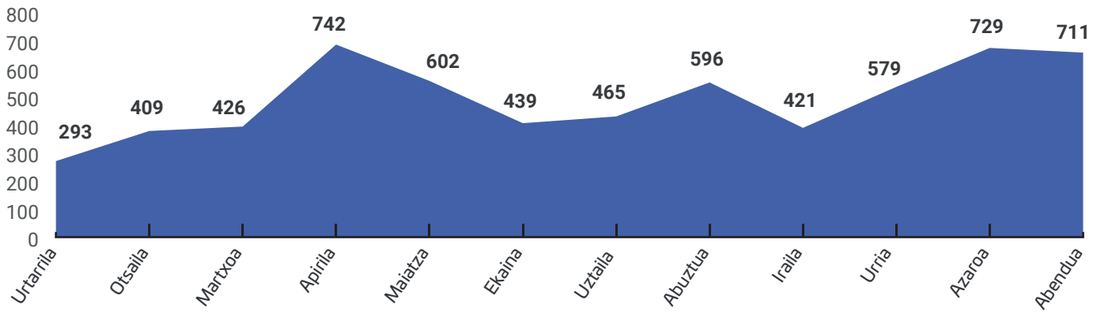
Ondoren, 2024an identifikatutako ransomwarearen jardueren datu kuantitatiboak eta kualitatiboak ageri dira, eta, horri esker, egungo egoera ebaluatu eta 2025erako aurreikuspenak egin ditzakegu. Jarraian, Mitre ATT & CKren framework-a oinarri hartuta, egindako azterketetatik ateratako informazioa jasotzen da, erakundeek erresilientzia-gaitasuna eta, ondorioz, zibersegurtasuneko heldutasun-maila handitzen lagunduko duten ekimenak lehenesteko eta abian jartzeko.

## Ransomware-erasoek kaltetutako biktimak

| Biktimak guztira | Hazkundea 2023arekin alderatuta |
|---|---|
| 6.413 | %16,73 |

## Biktimen hilabeteko bilakaera

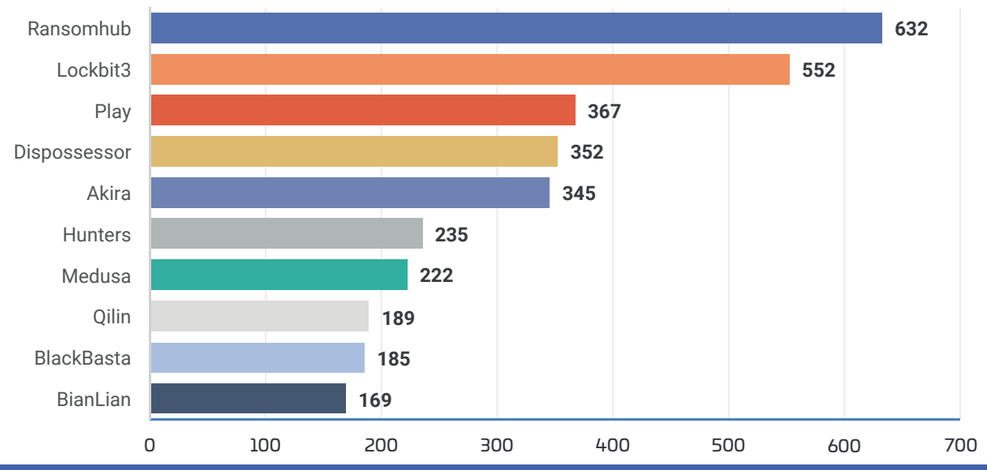
Biktimen kopurua aldakorra izan da urtean zehar eta gorakada esanguratsuak izan dira apirilean eta azaroan. Gorakada horiek mehatxu-eragileek zuzendutako balizko kanpaina espezifikoak adieraz ditzakete. Horrek erakusten du beharrezkoa dela etengabe zelatan egotea.




## Biktimen kopuruaren arabera aktiboen dauden ransomwareen taldeak

| Talde aktibo guztiak |
|---|
| 101 |

## Talderik aktiboenen Top 10a, biktima guztien kopurua aintzat hartuta




## Urte horretako ransomware familiarik aktiboenek ustiatutako kalteberatasunak

### Ransomhub: 632 biktima

- CVE-2020-1472 – (10.0 kritikoa) Microsoft

### Lockbit3: 552 biktima

- CVE-2021-22986 – (9.8 kritikoa) F5
- CVE-2023-27350: (9.8 kritikoa)- Papercut
- CVE-2023-4966 (Citrix Bleed) – (9.4 kritikoa) Citrix
- CVE 2023-4966: (9.4 kritikoa)- Citrix
- CVE-2023-27351: (8.2 handia)- PaperCut
- CVE-2023-0669: (7.2 handia)- Fortra GoAnywhere MFT

### Play: 367 biktima

- CVE-2020-12812 – (9.8 kritikoa) Fortinet
- CVE-2018-13379 – (9.1 kritikoa) Fortinet
- CVE-2022-41040 (8.8 handia) Microsoft
- CVE-2022-41080 – (8.8 handia) Microsoft
- CVE-2022-41082 -(8.0 handia) Microsoft

### Dispossessor: 352 biktima

- Ez da kalteberatasunik ustiatu eraso-bektore gisa.

### Akira: 345 biktima

- CVE-2023-20269 – (9.1 kritikoa) Cisco
- CVE-2020-3259- (7.5 handia) Cisco
- CVE-2023-27532: (7.5 handia)- Veeam Backup & Replication

### Hunters: 235 biktima

- CVE-2021-34473 – (9.1 kritikoa) Microsoft
- CVE-2021-34523 – (9.0 kritikoa) Microsoft
- CVE-2021-34527 – (8.8 handia) Microsoft
- CVE-2019-7481 – (7.5 handia) SonicWall
- CVE-2021-31207 – (6.6 ertaina) Microsoft

### Medusa: 222 biktima

- CVE-2023-48788 – (9.8 kritikoa) Fortinet
- CVE-2018-13379 – (9.1 kritikoa) Fortinet
- CVE-2022-2294 – (8.8 handia) Google
- CVE-2022-2295 – (8.8 handia) Google
- CVE-2022-21999 – (7.8 handia) Microsoft

### Qlin: 189 biktima

- CVE-2023-27532 – (7.5 handia) Veeam Backup & Replication

### BlackBasta: 185 biktima

- CVE-2024-1709- (10.0 kritikoa) ConnectWise ScreenConnect
- CVE-2020-1472 – (10.0 kritikoa) Micosoft
- CVE-2021-34527 - (8.8 handia) Microsoft
- CVE-2024-1708 - (8.4 handia) ConnectWise ScreenConnect
- CVE-2024-26169 – (7.8 handia) Microsoft
- CVE-2022-30190 - (7.8 handia) Microsoft

### BianLian: 169 biktima

- CVE-2020-1472 – (10.0 kritikoa) Netlogon Remote Protocol

## Tekniken Top 10a (taktika bakoitzean gehien erabili duten teknika)

| | |
|---|---|
| **Initial Access** | Exploit Public-Facing Application - T1190 |
| **Execution** | Command and Scripting Interpreter - T1059 |
| **Persistence** | Registry Run Keys / Startup Folder File - T1547.001 |
| **Privilege Escalation** | Exploitation for Privilege Escalation - T1068 |
| **Defense Evasion** | Obfuscated Files or Information - T1027 |
| **Credential Access** | OS Credential Dumping - T1003 |
| **Discovery** | File and Directory Discovery - T1083 |
| **Lateral Movement** | SMB/Windows Admin Shares - T1021.002 |
| **Collection** | Data from Local System – T1005 |
| **Exfiltration** | Exfiltration Over C2 Channel - T1041 |
| **Impact** | Data Encrypted for Impact - T1468 |

## Arintze-neurrien top 10

**M1026 Privileged Account Management**

17,6%

Kontu pribilegiatuei lotutako sorkuntza, aldaketa, erabilera eta baimenak administratzea, SYSTEM eta root barne.

**M1047 Audit**

8,8%

Sistemen, baimenen, segurua ez den softwarearen, seguruak ez diren konfigurazioen eta abarren auditoretzak edo azterketak egitea balizko ahultasunak identifikatzeko.

**M1040 Behavior Prevention on Endpoint**

11,2%

Gaitasunak erabiltzea, amaierako puntuaren sistemetan jokabide-eredu susmagarriak gerta ez daitezen. Horrek prozesu susmagarri bat, artxiboa, APIra deitzea eta abar barne har ditzake.

**M1027 Password Policies**

8,8%

Pasahitzen politika zorrotzak ezartzea, gutxieneko luzeraren, konplexutasunaren eta aldizkako txandaketaren baldintzak barne.

**M1018 User Account Management**

10,4%

Erabiltzaile-kontuei lotutako sorkuntza, aldaketa, erabilera eta baimenak administratzea.

**M1026 Password Policies**

8%

Pasahitzen politiken konfigurazio aurreratuak ezartzea kontu kritikoak babesteko. Horren barruan sartzen da pasahitz berdingabeak eta konplexuak erabiltzea, faktore anitzeko autentifikazioa (MFA) gaitzea eta berrerabilitako pasahitzak edo konprometituak erabiltzea prebenitzea.

**M1038 Execution Prevention**

9,6%

Arerioek DLL berriak erabil ditzakete teknika hau exekutatzeko. Bilaketa-aginduak bahituz exekutatutako eta maltzurra izan daitekeen softwarea identifikatzea eta blokeatzea, software legitimoak kargatutako DLL fitxategiak blokeatzeko gai diren aplikazioak kontrolatzeko soluzioak erabiliz.

**M1018 Privileged Account Management**

8%

Kontu pribilegiatuak kudeatzeko neurri zorrotzak ezartzea, besteak beste, sarbidea mugatzea baimendutako erabiltzaileentzat soilik, erabiltzeko politikak ezartzea eta auditoretza erregularrak egitea.

**M1017 User Training**

9,6%

Erabiltzaileak trebatzea aurkari baten sarbide- edo manipulazio-saiakeren berri izan dezaten, spearphishing, gizarte-ingeniaritza eta erabiltzailearen interakzioa inplikatzen duten beste teknika batzuen arrakasta-arriskua murrizteko.

**M1027 Privileged Account Management**

8%

Kontu pribilegiatuen erabilera mugatzeko eta monitorizatzeko kontrol aurreratuak ezartzea.

# 2024ko ondorioak

2024an oso aktibo jarraitu du ransomwarearen mehatxuak.

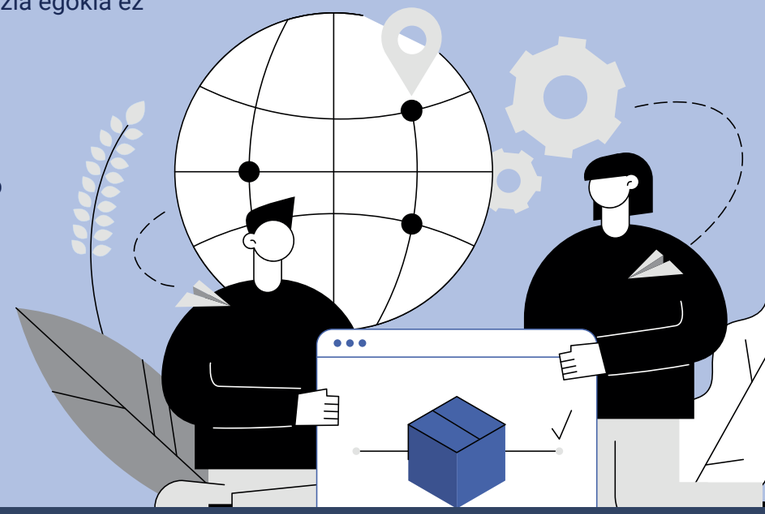
- Nabarmen igo da biktimen kopurua.
- Eragile gaiztoen teknikak geroz eta sofistikatuagoak dira.
- Hazkunde horrek agerian uzten du erasotzaileek kalteberatasun kritikoak aprobetxatzeko gaitasuna izateaz gain, inpaktu handiko kanpainak diseinatzeko eta exekutatzeko gaitasuna dutela.
- Familiarik aktiboenek, hala nola Ransomhub eta Lockbit3k, erakutsi dute eskala handian jarduteko gaitasuna dutela.
- Kalteberatasun kritikoen ustiapenak agerian utzi du adabakien eta eguneraketen kudeaketa indartzea beharrezkoa dela.

Ransomwarearen eredua zerbitzu gisa (RaaS) ustiatzen jarraitu dute, estortsio bikoitz eta hirukoitzeko eskemekin:

- Zifratutako informazioa berreskuratzeko ordainketa-eskaerak egiten.
- Informazio hori ransomwarearen taldeen orrialdeetan argitaratzen.
- Zerbitzua ukatzeko erasoak egiteko mehatxua egiten.
- Kontrol-autoritateei jakinarazteko mehatxua, biktimak zigor ditzaten segurtasunaren arloan diligentzia egokia ez egiteagatik.

Sektore batzuei zuzendutako eraso-patroiak daude:

- Manufaktura-sektoreari edo osasuneko sektoreari zuzendutako erasoak.
- Biktima gehien dituzten herrialdeak AEB, Kanada eta Erresuma Batua dira.
- Ohiko taktikak identifikatu dira, besteak beste, defentsei ihes egitea eta pribilegioetan gora egitea.



# 2025ko aurreikuspenak

- Erasoak geroz eta pertsonalizatuagoak izaten jarraitzea espero da, bai eta zerbitzu moduko operazioetan (RaaS) hazkundea izatea ere.
- Baliteke teknikak geroz eta berritzaileagoak izatea teknologia berriei esker, hala nola adimen artifizialari esker, eraso egiteko metodoak optimizatuko dituztelako.
- Prebentzio-jarrera ezartzen duten erakundeek posizio hobea izango dute mehatxu horien inpaktua arintzeko eta beren aktiboak babesteko.
- 2025era begira, ransomwareak eboluzionatzen jarraituko duela aurreikusten da.

2024an identifikatutako ransomware-jarduerak.