ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ransomware com a servei (RaaS), evolució del model de negoci

TLP: WHITE

FEBRER 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	09/03/2026	12/03/2026

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA 4
2. INTRODUCCIÓ 5
3. PANORAMA MUNDIAL DEL PROGRAMARI DE SEGREST 6
3.1. Grups de ransomware més actius 6
3.2. Països més afectats 8
3.3. Nombre de víctimes per mes en els darrers 3 any 11
4. ANÀLISI DE GRUPS RANSOMWARE-AS-A-SERVICE (RAAS) MÉS ACTIUS 13
4.1. Qilin 13
4.1.1 Sectors i països objectiu 14
4.1.2 Capacitats tècniques i eines 14
4.1.3 Indicadors de compromís (COI) 15
4.2. Akira 16
4.2.1 Sectors i països objectiu 18
4.2.2 Capacitats tècniques i eines 18
4.2.3 Indicadors de compromís (COI) 19
4.3. Cl0p 21
4.3.1 Sectors i països objectiu 22
4.3.2 Capacitats tècniques i eines 22
4.3.3 Indicadors de compromís (COI) 23
5. MODELS D'AFILIACIÓ 25
5.1. Model d'afiliació/participació en beneficis 25
5.2. Model basat en subscripció 25
5.3. Model de col·laboració per nivells 26
5.4. Models híbrids o amb serveis prèmium 26
6. NEGOCIACIONS DE RESCAT 27
7. ESTRATÈGIES DE PREVENCIÓ I RECUPERACIÓ 31
7.1. Estratègies de prevenció 31
7.2. Estratègies de recuperació 32
8. CLÀUSULA DE CONFIDENCIALITAT 33

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

El programari de segrest (*ransomware*) s'ha posicionat com una de les amenaces més crítiques i lucratives al panorama de ciberamenaces actual, tot representant el 20 % de tots els ciberdelictes. Com tothom sap, el programari de segrest té com a objectiu xifrar informació delicada i exfiltrar-la o, directament, bloquejar l'accés a sistemes, per exigir el pagament d'un rescat per recuperar-los.

L'aparició del model Ransomware-as-a-Service (RaaS) ha fet que el programari de segrest evolucioni a un tipus de cibercrim més industrialitzat amb l'adopció d'esquemes de negoci de programari legítim, que imiten el model del Software-as-a-Service (SaaS). En aquest tipus de model, els desenvolupadors proporcionen el codi maliciós (*malware*), la infraestructura i el suport tècnic als seus clients, que es coneixen com a afiliats, que són els que en última instància executen els atacs a canvi d'una part dels beneficis que obtinguin de cada víctima.

Aquesta mena de serveis fa que es redueixi la barrera d'entrada al cibercrim, fent que actors d'amenaça que estan començant o amb coneixements limitats puguin executar atacs o campanyes molt sofisticades.

El programari de segrest ha passat de ser una amenaça tècnica per convertir-se en un risc molt seriós per a organitzacions públiques i privades i infraestructures crítiques. En aquest informe es presentarà una anàlisi del panorama del programari de segrest a nivell mundial, que segueix creixent amb més de 120 grups de programari de segrest en actiu.

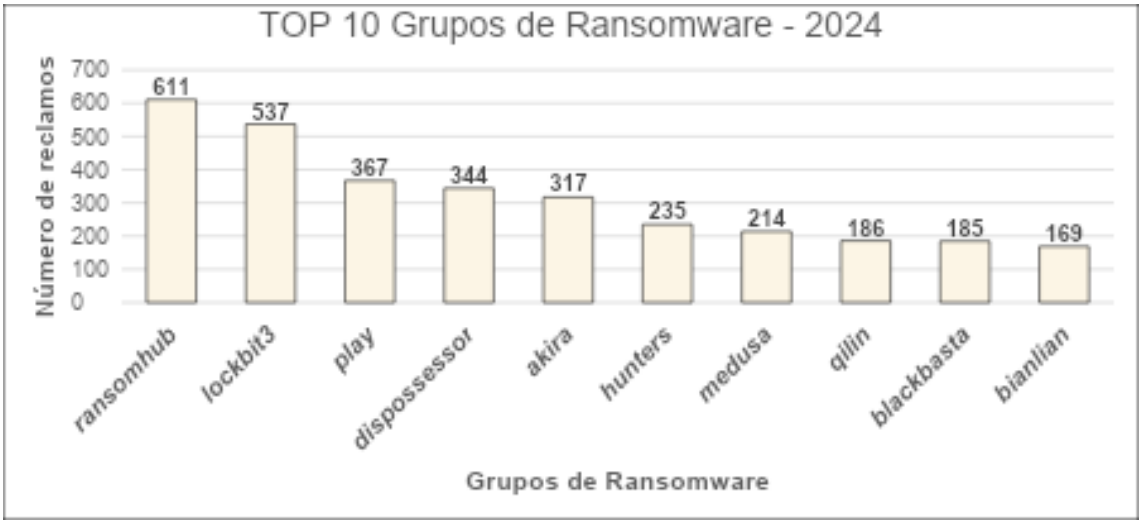
Aprofundirem en diversos els grups de Ransomware-as-a-Service (RaaS) més rellevants pel seu impacte. Identifiquem quins són els sectors més afectats, entendrem com funciona per dins l'ecosistema de Ransomware-as-a-Service (RaaS) i, per finalitzar, abordarem les dinàmiques de negociació de rescats i detalls.

3. PANORAMA MUNDIAL DEL PROGRAMARI DE SEGREST

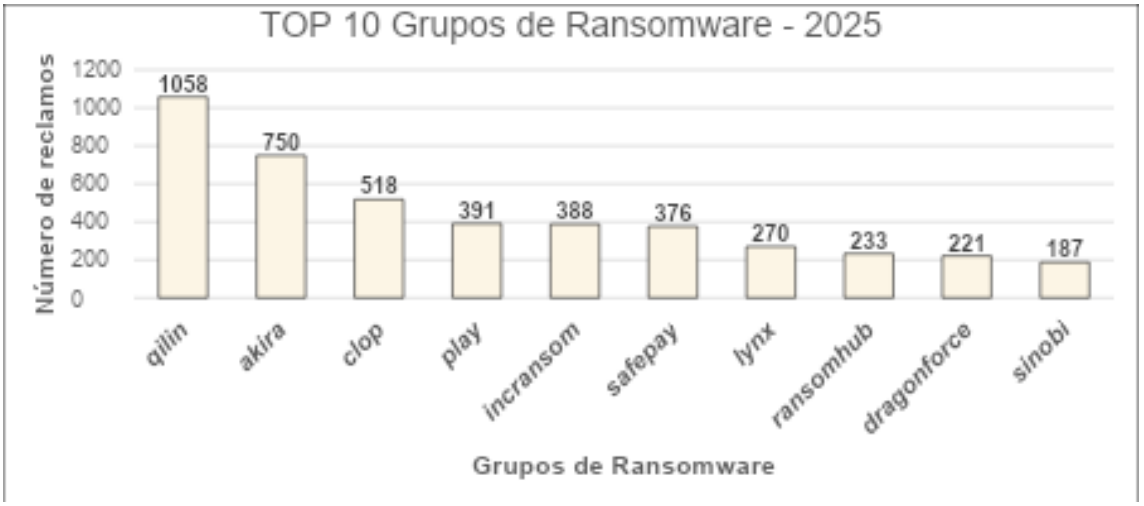
A l'apartat següent, s'analitzaran els grups de programari de segrest més actius dels darrers anys, els països més afectats pels seus atacs, el nombre de víctimes que han patit aquest tipus d'incidents per mes durant els darrers 3 anys, com també els sectors més afectats.

3.1. Grups de *ransomware* més actius

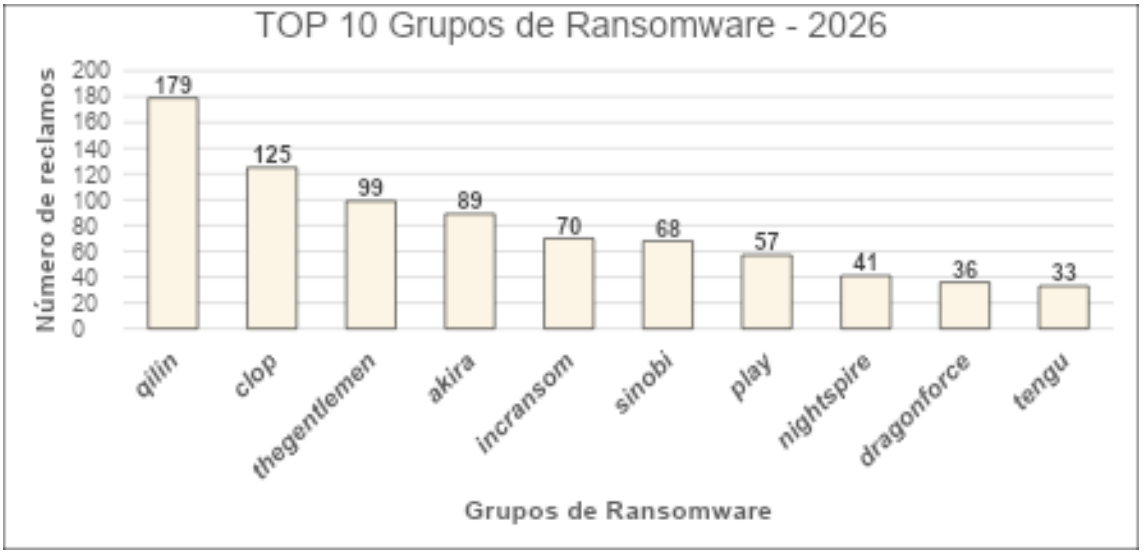
L'ecosistema del Ransomware-as-a-Service (RaaS) mostra una evolució clara: una alta fragmentació amb més de 120 grups actius, el tancament de RansomHub, la caiguda de LockBit i la consolidació de Qilin. A continuació, mostrarem el TOP10 per any basat en víctimes publicades als Data Leak Site (DLS) dels diferents grups durant els anys 2024, 2025 i el que portem de 2026.



Gràfic 1 – Top10 grups de ransomware amb més atacs el 2024



Gràfic 2 – Top10 grups de ransomware amb més atacs el 2025



Gràfic 3 – Top10 grups de ransomware amb més atacs el 2026 en data de febrer

Conclusions generals de l'evolució dels atacs de grups de programari de segrest (2024-2026):

- **Consolidació de Qilin**: passa de 186 víctimes en 2024 a 1058 en 2025, cosa que representa una pujada de 469 % en només un any. En data de febrer de 2026, se segueix apreciant Qilin com a líder indiscutible i el més probable és que, en acabar l'any, torni a acabar al TOP1 de nou.

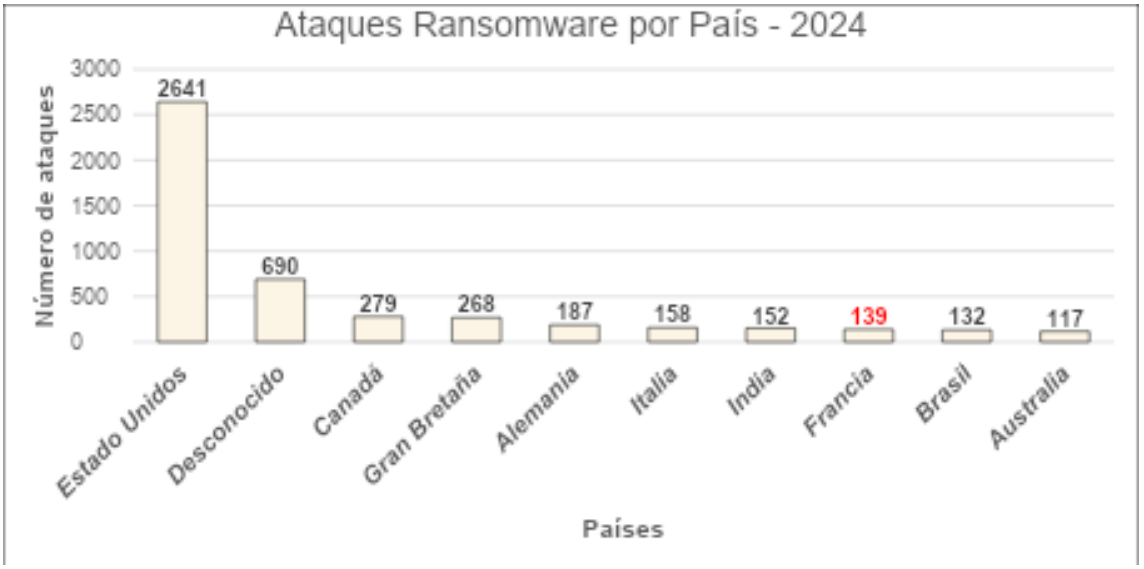
- **Migració d'afiliats**: l'any 2024 va ser dominat per grups com ara RansomHub i LockBit3.0, grups que van caure de forma abrupta el 2025. Això va provocar una migració d'afiliats massiva cap a grups com Qilin i Akira, que han sabut aprofitar la situació i s'han consolidat al TOP del panorama global.

- **Estabilitat de grups més clàssics i nous grups emergents**: Akira se segueix mantenint entre el TOP2-4 per la seva consistència en atacs i els alts pagaments que ha rebut per rescats. Altres grups, com ara Cl0p i Play, sobreviuen executant campanyes de *supply chain*. D'altra banda, hi ha nous grups emergents com ara SafePay, Sinobi, DragonForce i The Gentlemen, que han començat a guanyar certa reputació al sector.

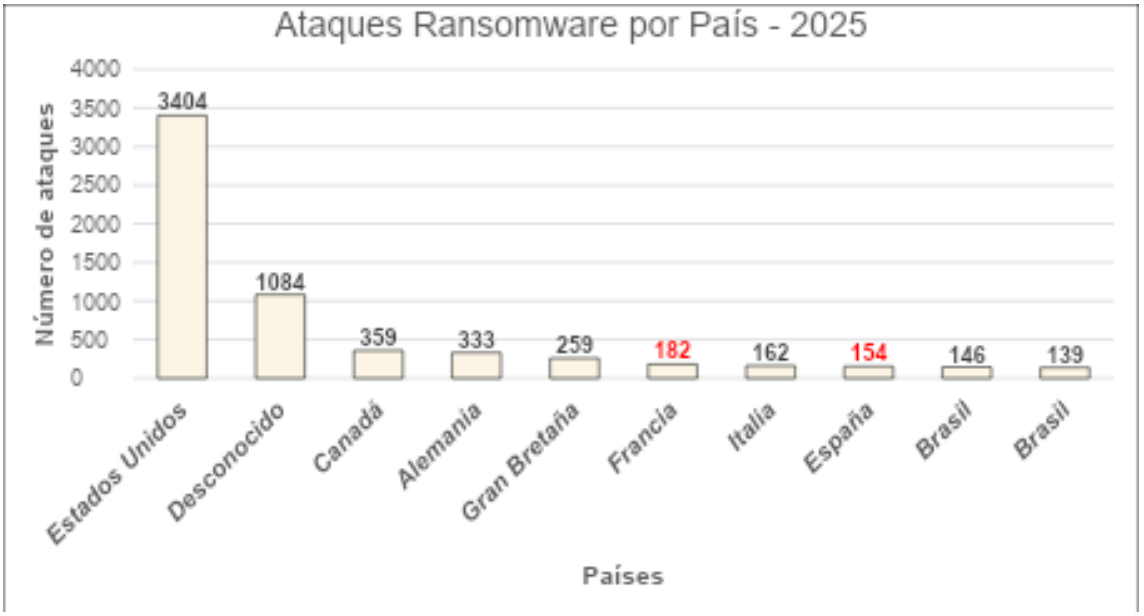
3.2. Països més afectats

Els grups de programari de segrest mantenen una concentració geogràfica als països amb economies més desenvolupades, a causa del valor dels objectius i d'una probabilitat més gran de pagament.

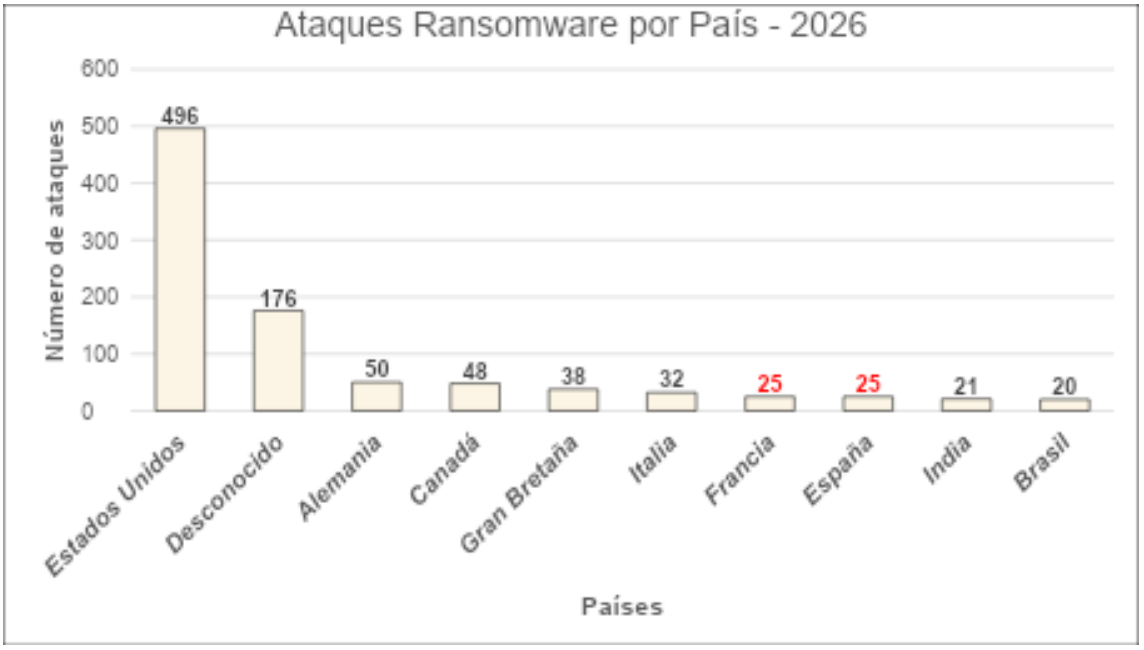
A continuació, mostrarem el TOP10 d'atacs de programari de segrest a països per any.



Gràfic 4 – Top10 països més atacats per ransomware l'any 2024



Gràfic 5 – Top10 països més atacats per ransomware l'any 2025



Gràfic 6 – Top10 països més atacats per ransomware en data de febrer de 2026

Conclusions generals de l'evolució dels atacs de programari de segrest a països des de l'any 2024 fins a l'actualitat:

- **Domini absolut dels Estats Units**: el 40-50 % de tots els atacs de programari de segrest ocorreguts entre els anys 2024 i el que ha transcorregut de 2026 van ser dirigits als Estats Units, a causa de ser una de les economies més potents i comptar amb les empreses més valuoses.

- **Atacs a Europa en ascens**: Alemanya es converteix en el país més atacat d'Europa, amb un creixement d'atacs del 78 % entre els anys 2024 i 2025. França passa de 139 víctimes el 2024 a 182 el 2025 i Espanya va entrar al TOP10 el 2025 i el 2026 tot sembla indicar que continuarà de la mateixa manera.

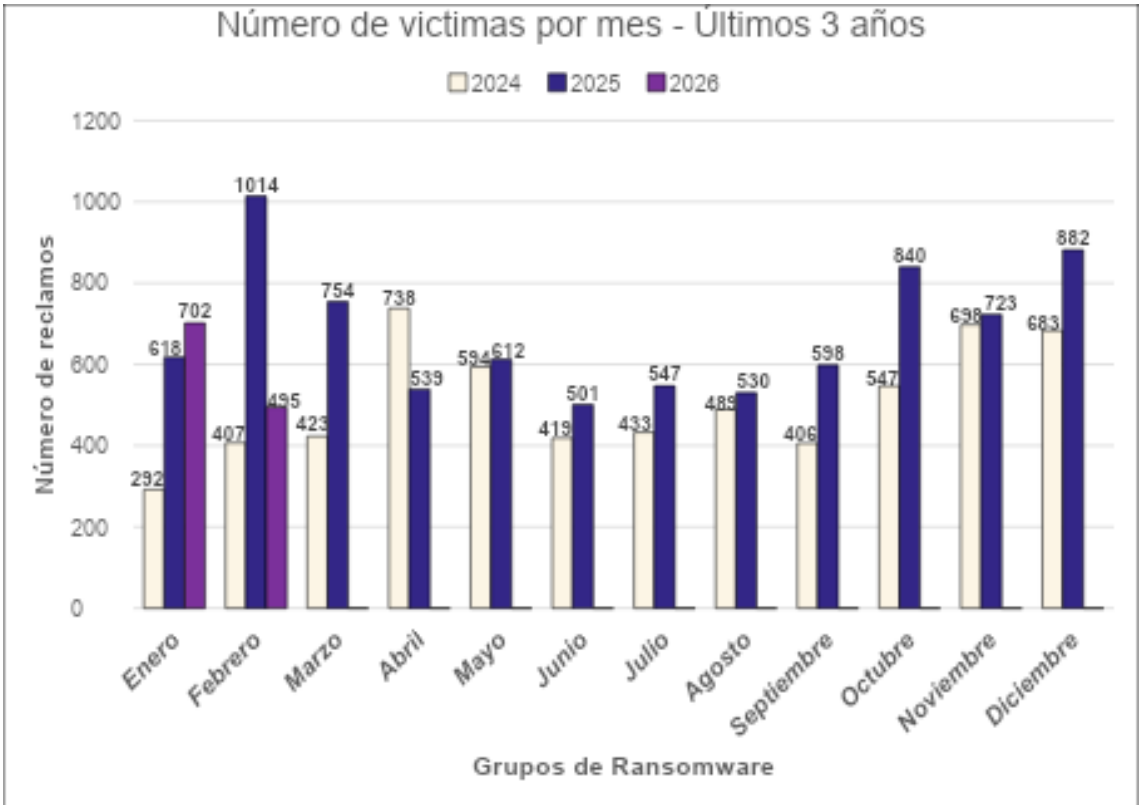
- **Implicacions estratègiques per a Andorra**: no apareix als top globals a causa de la seva grandària, però les seves relacions estructurals amb França i Espanya com a socis principals, com també condensar en un àmbit geogràfic molt reduït un pes econòmic i unes infraestructures crítiques importants, implica una exposició indirecta elevada.

3.3. Nombre de víctimes per mes en els darrers 3 any

El nombre de víctimes reclamades mostra una tendència alcista clara. Es passa d'una mitjana mensual de 477 atacs el 2024 a 630 atacs el 2025, una pujada del 32 %.

El 2026, els 2 primers mesos superen la mitjana del 2025, cosa que, si es manté aquesta tendència, indicaria que l'any 2026 podria superar els 8000-9000.

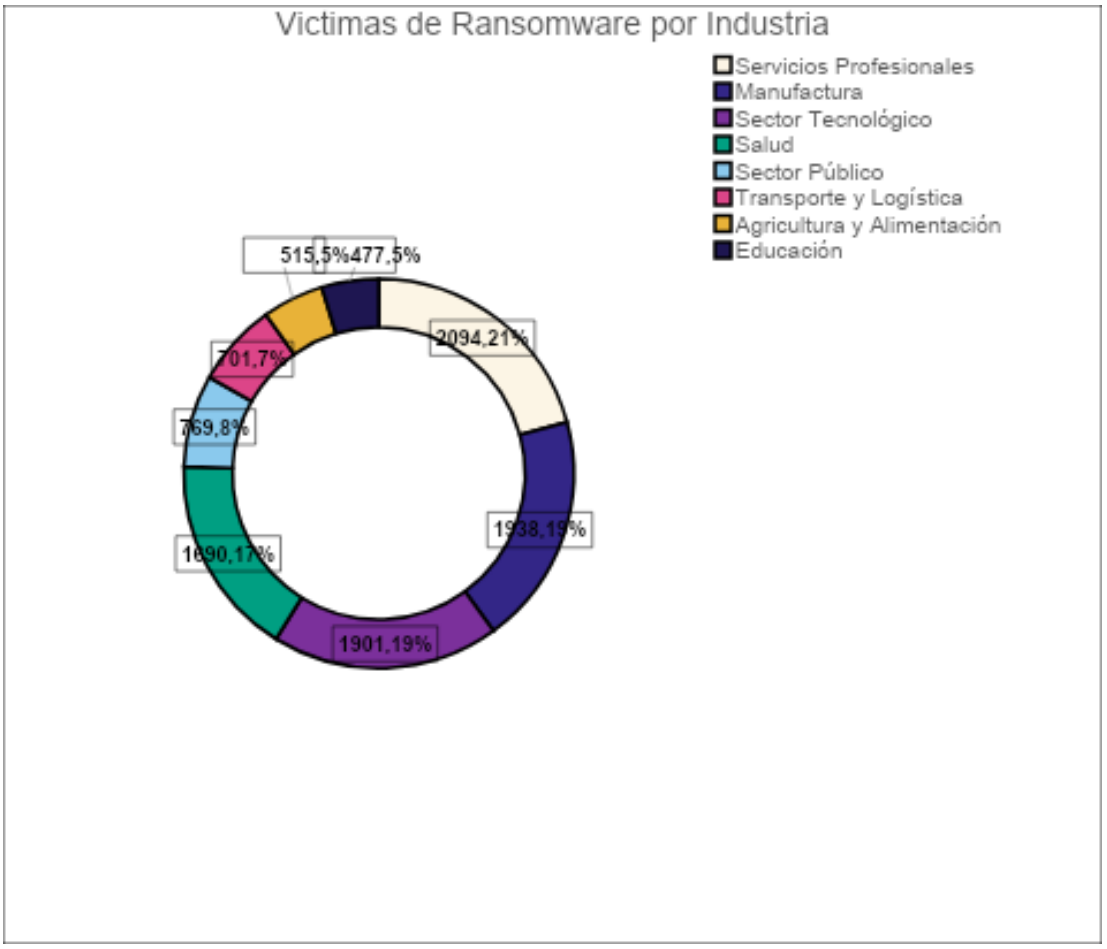
El gràfic següent exposa les víctimes reclamades mensuals dels darrers 3 anys (2024-actualitat):



Gràfic 7 – Nombre de víctimes per mes dels darrers 3 anys (2024-2026)

3.4. Sectors més afectats

Els grups de programari de segrest prioritzen els sectors amb més cost d'interrupció operativa, amb dades delicades i probabilitat elevada que les víctimes facin el pagament. Al gràfic següent veurem quins sectors són els més atacats pels grups de programari de segrest:



Gràfic 8 – Víctimes de ransomware per sector

Conclusions:

- El sector de manufactura i serveis professionals són objectius prioritaris per als grups de programari de segrest.
- El sector de salut ocupa el quart lloc amb 1.690 víctimes, i destaca pel risc dels pacients i la pressió regulatòria que genera pagaments ràpid.
- Els sectors públics, de transport i logística, agricultura i alimentació, i finalment educació, completen el TOP, cosa que reflecteix una diversificació cap a sectors regulats i essencials.

4. ANÀLISI DE GRUPS RANSOMWARE-AS-A-SERVICE (RAAS) MÉS ACTIUS

A continuació, analitzarem els 3 grups de Ransomware-as-a-Service (RaaS) més actius dels darrers 3 anys. Aprofundirem en el perfil dels grups, les seves capacitats tècniques i eines, els seus sectors i països objectiu i indicadors de compromís relacionats.

4.1. Qilin

Qilin, és un grup cibercriminal associat al model de Ransomware-as-a-Service (RaaS). Com hem pogut veure a l'apartat del panorama, és indiscutiblement el grup amb més ciberatacs el 2025 i també pel que fa al 2026 fins ara. El grup ataca múltiples sectors a nivell mundial, i exigeixen pagaments de rescat elevats en criptomonedes. Són coneguts per les tàctiques agressives i la capacitat d'adaptació a les mesures de seguretat. Aprofiten les vulnerabilitats del programari més utilitzat i fan servir tècniques avançades d'enginyeria social i pesca dirigida (*spear-phishing*).

Imatge 1 – DLS del grup ransomware Qilin

4.1.1 Sectors i països objectiu

Les dades més recents de Qilin indiquen que el grup està concentrant els seus atacs contra països occidentals desenvolupats, amb un clar enfocament als Estats Units. França i Espanya entren al top 5 països més afectats per Qilin.

	PAÏSOS	Nombre d'atacs
1	Estats Units	571
2	**França**	**66**
3	Canadà	64
4	Gran Bretanya	48
5	**Espanya**	**45**

Taula 1 – Països objectiu del grup de programari de segrest Qilin

Pel que fa als sectors, Qilin sembla tenir una preferència pel sector de manufactura, seguit per la tecnologia i la sanitat. Aquesta distribució de sectors indica que el grup prioritza indústries on la interrupció operativa és crítica com ara la sanitat, o on les dades robades tenen un alt valor com a empreses tecnològiques i financeres.

	SECTORS	Nombre d'atacs
1	Manufactura	175
2	Tecnologia	129
3	Assistència sanitària	123
4	Serveis empresarials	96
5	Serveis financers	69

Taula 2 – Sectors objectiu del grup de programari de segrest Qilin

4.1.2 Capacitats tècniques i eines

A continuació, es mostrarà un resum de les principals capacitats i eines del grup Qilin:

CATEGORIA	EINES I TÈCNIQUES PRINCIPALS
Descobriment (*Discovery*)	Nmap, Nping (escaneig de xarxa i serveis), enumeració d'usuaris/processos, scripts PowerShell.
Eines RMM (RMM *tools*)	NetSupport, ScreenConnect (abús d'eines legítimes per a persistència i control remot).
Evasió de defenses (*Defense evasion*)	BYOVD (Bring Your Own Device) amb controladors vulnerables (Toshiba TPwSav.sys, Zemana Anti-Rootkit, eskle.sys), EDRSandBlast, PCHunter, PowerTool, YDArk, actualitzador Carbon Black (upd.exe), eliminació de registres, autosupressió, mode segur.
Robatori de credencials (*Credential theft*)	Mimikatz (embegut per a dúmping LSASS, token theft, escalada de privilegis), stealers de Chrome i credencials guardades.
Seguretat ofensiva (OffSec)	Cobalt Strike (*beacons* i post-explotació), Evilginx (pesca AITM bypass MFA), NetExec (execució remota).
Xarxes (*Networking*)	Cadenes *proxy* (anonimat), PsExec, WinRM, fsutil (manipulació de volums), propagació lateral via SMB/RDP.
LOL	fsutil, bcdedit, vssadmin, wbadmin (dany a recuperació i backups), cipher.exe.
Exfiltració (*Exfiltration*)	EasyUpload.io (pujada ràpida de dades robades a serveis cloud/web), abans d'encriptació.

Taula 3 – Eines i tècniques principals del grup de programari de segrest Qilin

4.1.3 Indicadors de compromís (COI)

A continuació, es mostraran IdC representatius i comuns observats en anàlisis recentment relacionades amb Qilin.

TIPUS	COI
FTP	ftp://dataShare:nX4aJxu3rYUMiLjCMtuJYTKS@176.113.115.97
FTP	ftp://dataShare:2bTWYKNn7aK7Rqp9mnv3@176.113.115.209
IP	176.113.115.97
IP	176.113.115.209
IP	85.209.11.49
IP	31.41.244.100
IP	85.209.11.49
IP	176.113.115.209
IP	176.113.115.97
IP	188.119.66.189
MD5	d6e7547ad7dfd1fbc62e8282aebcc391
MD5	f588802958c35fe18eb87bc36651a3d1
MD5	2bb209ccfc5103eccab523c875050cfa
MD5	a7e7d00d531cb7ca27d0f3bee448573f
MD5	964c13b68dc6b6b918b66a9a10469d2a
MD5	3b10127e65fa3e215d21e0a2e7fd32be
MD5	d1c331c17ddd4abe0d53755461c1ec9a
MD5	417ad60624345ef85e648038e18902ab
MD5	b04e8ee43aba85fa5c585b9335c953c2
MD5	59d756280b06cf113ca43abc0050edd5
MD5	88bb86494cb9411a9692f9c8e67ed32c
MD5	37155f0bca29ccd6b6d4f5b2bc42eb4d
MD5	e01776ec67b9f1ae780c3e24ecc4bf06
MD5	417ad60624345ef85e648038e18902ab
MD5	11d795baafa44b73766e850d13b8e254
MD5	88630916b0c6633ca28c8896416a93ee
MD5	dd42c3e017889c107a81da78d87dc8af
MD5	1c4bea81c0da22badd9b7eab574c51cd

MD5	ab05a1925fee8334a2114811d5283364
MD5	64a590760fdbb84356544cc90ac3d50f
MD5	2020979e080d7ac9c0403172573c7de8

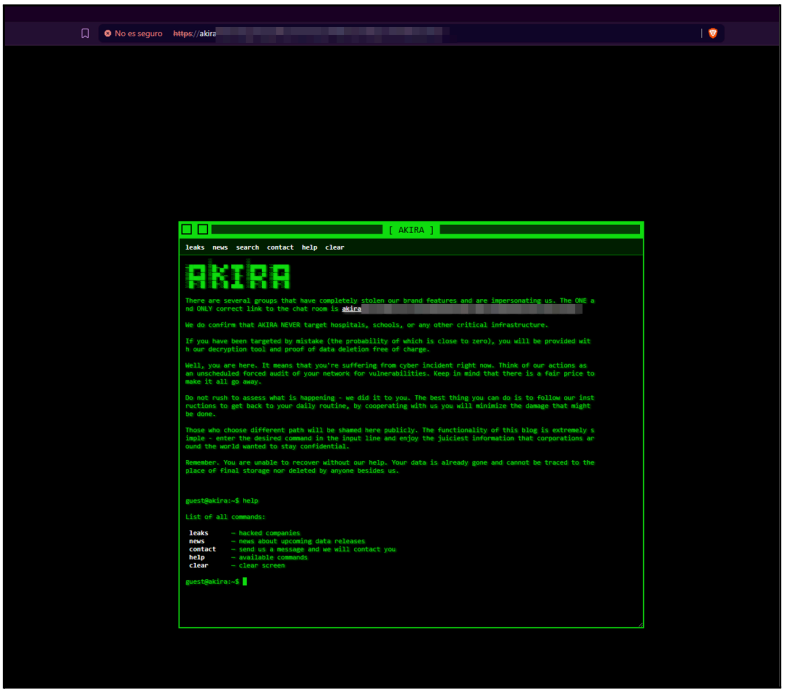
Taula 4 – Indicadors de compromís del grup de programari de segrest Qilin

4.2. Akira

Akira és un grup cibercriminal associat al model de Ransomware-as-a-Service (RaaS) que es manté actiu des del 2023. Opera mitjançant un programa d'afiliació que permet que altres grups facin servir el seu codi maliciós i la seva infraestructura a canvi d'un percentatge dels rescats.

Empra tàctiques d'extorsió en múltiples capes, que inclouen amenaces relacionades amb l'exfiltració i la publicació de dades, notificacions sobre problemàtiques associades a normatives i regulacions incomplertes per les víctimes i atacs DDoS.

La metodologia d'aquest grup és similar a la d'altres grups: xifra els fitxers amb l'extensió del seu nom, en aquest cas: «.akira», i deixa una nota de rescat anomenada «AKIRA_README.txt». I hi ha una clara similitud entre les operacions impulsades per Akira i les que duia a terme l'extint grup Conti, que es va dissoldre el 2022 després d'una filtració del codi font i comunicacions, cosa que indica que molts dels seus membres passessin de formar part de l'un a l'altre.



Imatge 2 – DLS del grup de programari de segrest Akira

4.2.1 Sectors i països objectiu

Els atacs d'Akira se centren exclusivament als Estats Units, ja que un 78 % de tots els atacs que duen a terme, s'hi concentren. Com es pot apreciar a la taula, Akira té una preferència per països que tenen un alt valor econòmic i amb una forta presència industrial.

	PAÏSOS	Nombre d'atacs
1	Estats Units	618
2	Canadà	64
3	Alemanya	48
4	Gran Bretanya	27
5	Itàlia	27

Taula 5 – Països objectiu del grup de programari de segrest Akira

Pel que fa als sectors, Akira colpeja amb força el sector manufacturer amb 224 atacs, líder destacat per la seva vulnerabilitat pel que fa a la cadena de subministrament, seguida del sector de serveis empresarials, amb 152 atacs, ja que sovint serveixen com a porta d'entrada a múltiples indústries.

	SECTORS	Nombre d'atacs
1	Manufactura	224
2	Serveis empresarials	152
3	Tecnologia	93
4	Construcció	69
5	Agricultura	59

Taula 6 – Sectors objectiu del grup de programari de segrest Akira

4.2.2 Capacitats tècniques i eines

A continuació, es mostrarà un resum de les principals capacitats i eines del grup Akira:

CATEGORIA	EINES I TÈCNIQUES PRINCIPALS
Descobriment (*Discovery*)	Advanced IP Scanner, SoftPerfect NetScan, Masscan, Bloodhound, SharpHound, ldapdomaindump, ReconFTW, SharpShares (escaneig de xarxa, ports, Active Directory, shares i enumeració de domini).

Eines RMM (RMM *Tools*)	AnyDesk, MeshAgent, MobaXterm, Radmin, RustDesk, TeamViewer (abús per a accés remot persistent, control i moviment lateral, sovint *rogue* o hijaquejat).
Evasió de defenses (*Defense evasion*)	PowerTool + Zemana Anti-Rootkit driver (BYOVD per *kernel-level*, terminació d'AV/EDR), POORTRY (*driver vulnerable signed*), eliminació de *shadow copies*, *uninstall EDR*, *disable* serveis de seguretat, *blending* amb *admin activity*.
Robatori de credencials (*Credential theft*)	Mimikatz (dumping LSASS, Kerberoasting), LaZagne, DonPAPI (extracció de credencials de processos, *browsers*, NTDS.dit, *password stores* com ara Veeam).
Seguretat ofensiva (OffSec)	CrackMapExec, Impacket (wmiexec.py per a execució remota), NetExec (moviment lateral i enumeració).
Xarxes (*Networking*)	Cloudflared (túnels), OpenSSH, Ngrok (túnels reversos i C2 anonimat), propagació via RDP/SSH/SMB.
LOL	net.exe, nltest, PowerShell (per a la descoberta, confiança de domini, supressió de còpies ombra), wmiexec, etc.
Exfiltració (*Exfiltration*)	FileZilla, WinSCP, RClone, MEGA, Temp.sh (pujada a cloud/storage extern o serveis temporals abans d'encriptar).

Taula 7 – Eines i tècniques principals del grup de programari de segrest Akira

4.2.3 Indicadors de compromís (COI)

A continuació, es mostraran IdC representatius i comuns observats en anàlisis recentment relacionades amb Akira.

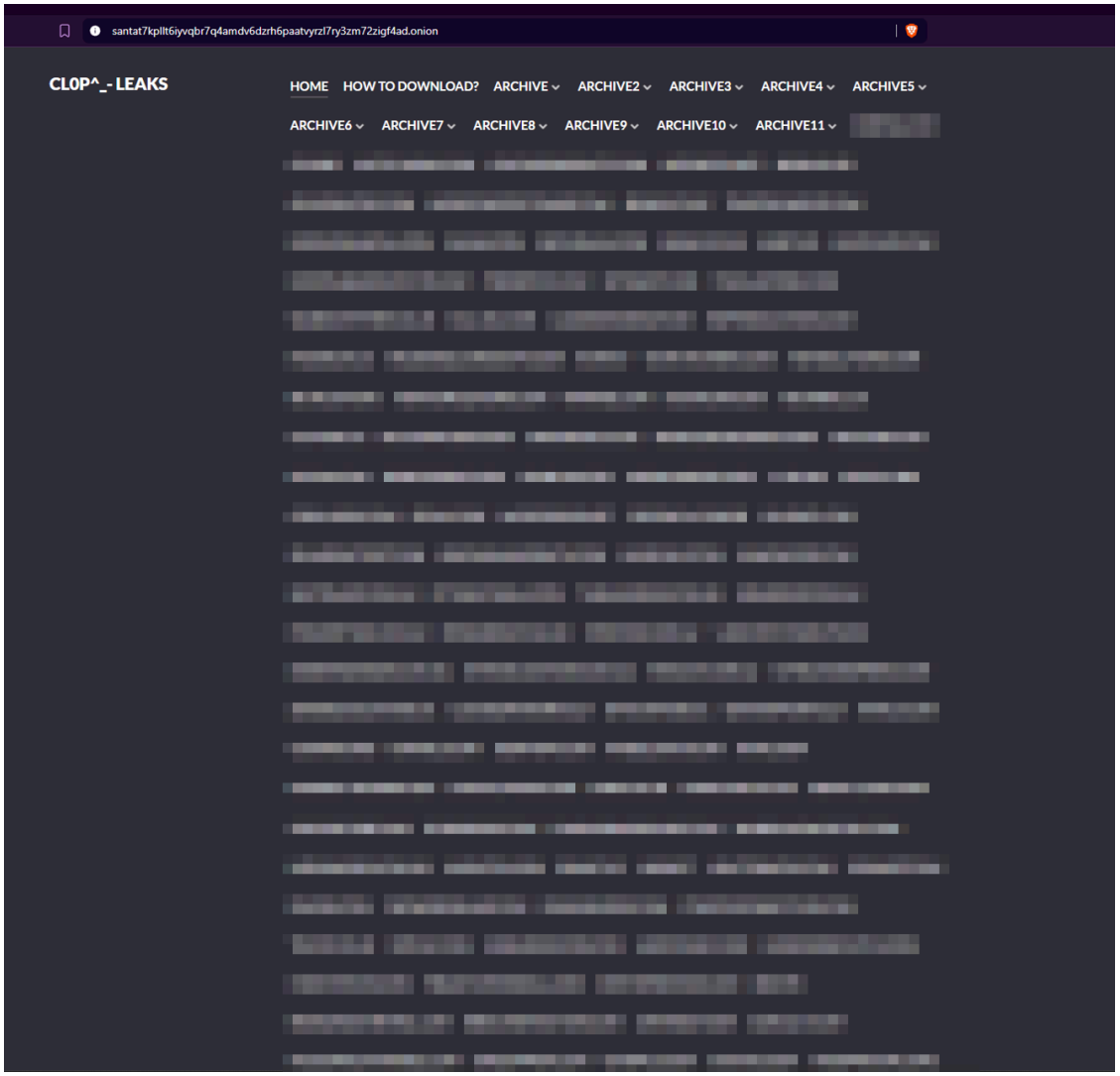
TIPUS	COI
Direcció BTC	bc1qr0txunr259we37wer7w6et33qyq0n6hv83pw24
Direcció BTC	bc1q6dqe4esmqejmxhpj95qadv0j4clsqcxxp4cd94
Direcció BTC	bc1qandfxc4knaf943njca77edl9mmegzs83tv8lpx
Direcció BTC	bc1qr0pqfghr9cksfc5arr2rak3lt2y50v03pc76nh
Direcció BTC	bc1qpwwtck0zhzrj56fxeayz6wz5546nlp607qzpvh
Direcció BTC	bc1qghj85gz0dkr9jeucana3z4xu50ujtllj50rvj0

Direcció BTC	bc1qcnw5v94y40ast06eatgalnjpluu2p067qewh46
MD5	083740c55d0a459674457b8551ed9c6a
MD5	1a7df536c3bb676a6f90af5b3bea5302
MD5	4d43e35962c8c7fdca5f64da8f561f5a
MD5	f17b6cdcbac9462f01da65bd4f8636db
MD5	27182f9017d8e4212fbc32e954e19d37
MD5	ab359be0ab33876eb32325706e43f0c1
MD5	1d895cf4391b817e54fb9ec9d8e65f7e
MD5	03b9887dee2c3c825b6a6c0df1d104ad
MD5	4d79fb750955ec8702cb79cfdb36e66b
MD5	c387b2eb96bb137cdd54220d920edce9
MD5	be1f993b1d26e6baa3c8f7dc0cb63472
MD5	28a72219951ce207601e120c9d590d47
MD5	39a14bfc65e6f5e13fc2817206a39cad
SHA256	78d75669390e4177597faf9271ce3ad3a16a3652e145913dbfa9a5951972fcb0
SHA256	2c7aeac07ce7f03b74952e0e243bd52f2bfa60fadc92dd71a6a1fee2d14cdd77
SHA256	88da2b1cee373d5f11949c1ade22af0badf16591a871978a9e02f70480e547b2
SHA256	566ef5484da0a93c87dd0cb0a950a7cff4ab013175289cd5fccf9dd7ea430739
SHA256	ccda8247360a85b6c076527e438a995757b6cdf5530f38e125915d31291c00d5
SHA256	87b4020bcd3fad1f5711e6801ca269ef5852256eeaf350f4dde2dc46c576262d
SHA256	988776358d0e45a4907dc1f4906a916f1b3595a31fa44d8e04e563a32557eb42
SHA256	3805f299d33ef43d17a5a1040149f0e5e2d5db57ec6f03c5687ac23db1f77a30
SHA256	abba655df92e99a15ddcde1d196ff4393a13dbff293e45f5375a2f61c84a2c7b
SHA256	a546ef13e8a71a8b5f0803075382eb0311d0d8dbae3f08bac0b2f4250af8add0
SHA256	6005dcbe15d60293c556f05e98ed9a46d398a82e5ca4d00c91ebec68a209ea84
SHA256	43c5a487329f5d6b4a6d02e2f8ef62744b850312c5cb87c0a414f3830767be72

Taula 8 – Indicadors de compromís del grup de programari de segrest Akira

4.3. Cl0p

El grup de programari de segrest Cl0p és una variant d'un cep prèviament conegut anomenat CryptoMix. La diferència principal d'aquest actor amb els altres actors RaaS és que combina campanyes massives amb atacs dirigits, tot mitjançant l'explotació de vulnerabilitats zero-day. Cl0p afegeix l'extensió «.clop» al final dels fitxers, o altres tipus d'extensions com ara «.CIIp, .Cllp» i «.C_L_O_P».



Imatge 3 – DLS del grup de programari de segrest Cl0p

4.3.1 Sectors i països objectiu

Els atacs de Cl0p se centren també als Estats Units, que representen al voltant d'un 70-80 % de tots els atacs que fan. Com es pot apreciar a la taula, Cl0p té una preferència per països anglosaxons on el potencial de pagament/impacte regulador són molt elevats.

	PAÏSOS	Nombre d'atacs
1	Estats Units	423
2	Canadà	53
3	Gran Bretanya	26
4	Austràlia	24
5	Alemanya	23

Taula 9 – Països objectiu del grup de programari de segrest Cl0p

En sectors, Cl0p prioritza el sector tecnològic a causa del rol que tenen en proveïdors de programari i serveis digitals, ja que aquests faciliten els atacs de *supply-chain*. La selecció d'aquests sectors reflecteix l'estratègia d'explotar plataformes compartides (*file transfer*), fent que la pressió d'extorsió sigui màxima a causa de les dades delicades que gestionen

	SECTORS	Nombre d'atacs
1	Tecnologia	146
2	Transport i logística	68
3	Serveis al consumidor	65
4	Manufactura	64
5	Serveis empresarials	34

Taula 10 – Sectors objectiu del grup de programari de segrest Cl0p

4.3.2 Capacitats tècniques i eines

A continuació, es mostrarà un resum de les principals vulnerabilitats explotades pel grup Cl0p:

FABRICANT	PRODUCTE	CVE
Accellion	Dispositiu de transferència de fitxers Accellion	CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104
Cleo	Cleo VLTrader, Harmony, LexiCom	CVE-2024-55956

Fortra	Transferència de fitxers gestionada de GoAnywhere	CVE-2023-0669
Oracle	Suite de negocis electrònics	CVE-2025-61882
Progress Software	Transferència MOVEit	CVE-2023-34362
PaperCut	Servidor d'aplicacions PaperCut	CVE-2023-27350, CVE-2023-27351
SolarWinds	FTP del servei SolarWinds Serv-U	CVE-2021-35211

Taula 11 – Eines i tècniques principals del grup de programari de segrest Cl0p

4.3.3 Indicadors de compromís (COI)

A continuació, es mostraran IdC representatius i comuns observats en anàlisis recentment relacionades amb Cl0p.

TIPUS	COI
IP	103.173.211.124
IP	106.75.139.199
IP	193.161.193.99
IP	193.24.211.240
IP	72.21.91.29
IP	98.159.37.224
IP	185.220.101.4
IP	192.42.116.191
IP	185.220.101.1
IP	185.220.101.5
SHA1	8c015d80b8a23f780bdd215dc842b0f5551f63bd
SHA256	bebe2853a3485d1c2e5c5be4249183e0ddaff9f87de71652371700a89d937128
MD5	5bfa51f3a417b98e7443eca90fc94703
SHA1	0bc9bf8ebf17941ba2750edd09e032d5f677351d
MD5	03c90fd77221e1b5b9d98e32ada70990
SHA256	a01e57611537699d85e9767023638dbd88a224075a866c17509dc17d7e5ddbde
SHA256	107e1e25b8872cbd2901af0b83a4f34c6fa0490768200d77993a0bda7bb8eaa4

SHA256	528c7bd0521391ba35ec8ab1baa8db2755c038bff849b748185d2a66482e5d61
SHA256	eb84f044322092ea87624ad1846465dc9472c1183e52e6e6207429266aad4b1e
SHA256	f3a939131ffaf473f8b1ffa0cd11d8cbce46f50dcc7e9fd2ff8404201ab5bc8e

Taula 12 – Indicadors de compromís del grup de programari de segrest Cl0p

5. MODELS D'AFILIACIÓ

Els models d'afiliació de Ransomware as a Service (RaaS) han transformat el panorama del ransomware en un negoci econòmic molt rendible per als cibercriminals, aquests models busquen copiar les plataformes de negoci legítimes de Software-as-a-Service (SaaS).

En aquest tipus de models els desenvolupadors del Ransomware as a Service (RaaS) creen i mantenen el codi maliciós (*malware*), la infraestructura de *Command and control* (C2), els *leak sites* i les eines de negociació. Així, els afiliats simplement han d'executar els atacs amb les eines proporcionades. Gràcies a aquest tipus de models es redueix significativament la barrera tècnica i financera d'entrada perquè es creïn o apareguin nous grups a l'ecosistema del programari de segrest.

A la data actual, el RaaS segueix apostant pel model d'afiliats, i és aquí on analitzarem les diferents tipologies que impulsen per competir entre grups, amb l'objectiu d'atreure i retenir talent.

5.1. Model d'afiliació/participació en beneficis

El model d'Affiliate/Profit Share o el model de programa d'afiliats amb repartiment de guanys, és el model més habitual al panorama actual, i el fan servir grups com ara Akira, Qilin, Play, etc.

Els punts clau del model serien:

- Els afiliats que s'uneixen a aquest model no paguen una quota d'entrada, en alguns casos paguen un dipòsit simbòlic, però no és habitual.
- Els desenvolupadors retenen un percentatge fix de cada rescat que es paga, que acostuma a oscil·lar entre el 20-40 %, mentre que els afiliats es queden amb el pagament restant del rescat.
- Quan l'afiliat té un nivell superior o és més rendible, el repartiment de beneficis es pot ampliar fins al 80-90 %, però només se sol donar en casos excepcionals.
- És un model *win-win* per a l'operador i l'afiliat, ja que l'operador té una escalabilitat molt gran sense costos, i l'afiliat té un risc inicial baix i un gran potencial de guany.

5.2. Model basat en subscripció

El model de Subscription-based o el model de subscripció és cada cop menys freqüent, ja que models com l'Affiliate/Profit Share són més atractius, però encara continua present en alguns programes.

Els punts clau del model serien:

- Els afiliats paguen una subscripció mensual per poder accedir al kit de *ransomware*, actualitzacions, suport tècnic i múltiples funcions més.
- De vegades, en aquest model també es produeixen repartiment de guanys, encara que no és habitual.
- El model ofereix més autonomia a l'operador, però com hem comentat, aquest model està perdent popularitat, perquè no pot fer front a models sense cost inicial com l'Affiliate/Profit Share.

5.3. Model de col·laboració per nivells

El model de Tiered o Partnership o model de *profit sharing* negociat és un model pràcticament similar a l'Affiliate/Profit Share però és usat en operacions més avançades.

Els punts clau del model serien:

- El repartiment de diners es negocia segons el valor que la víctima pugui tenir i segons l'historial que tingui l'afiliat en atacs previs.

- Els afiliats amb *track record* provat i d'alt rang poden arribar a obtenir beneficis tan alts com fins al 80 % o, fins i tot, més grans.

5.4. Models híbrids o amb serveis prèmium

El model híbrid i amb serveis prèmium neix de la competència que ha fet escalar aquest ecosistema, incorporant valor afegit als models de RaaS convencionals amb la finalitat de retenir o atraure afiliats.

Els punts clau d'aquest tipus de models serien:

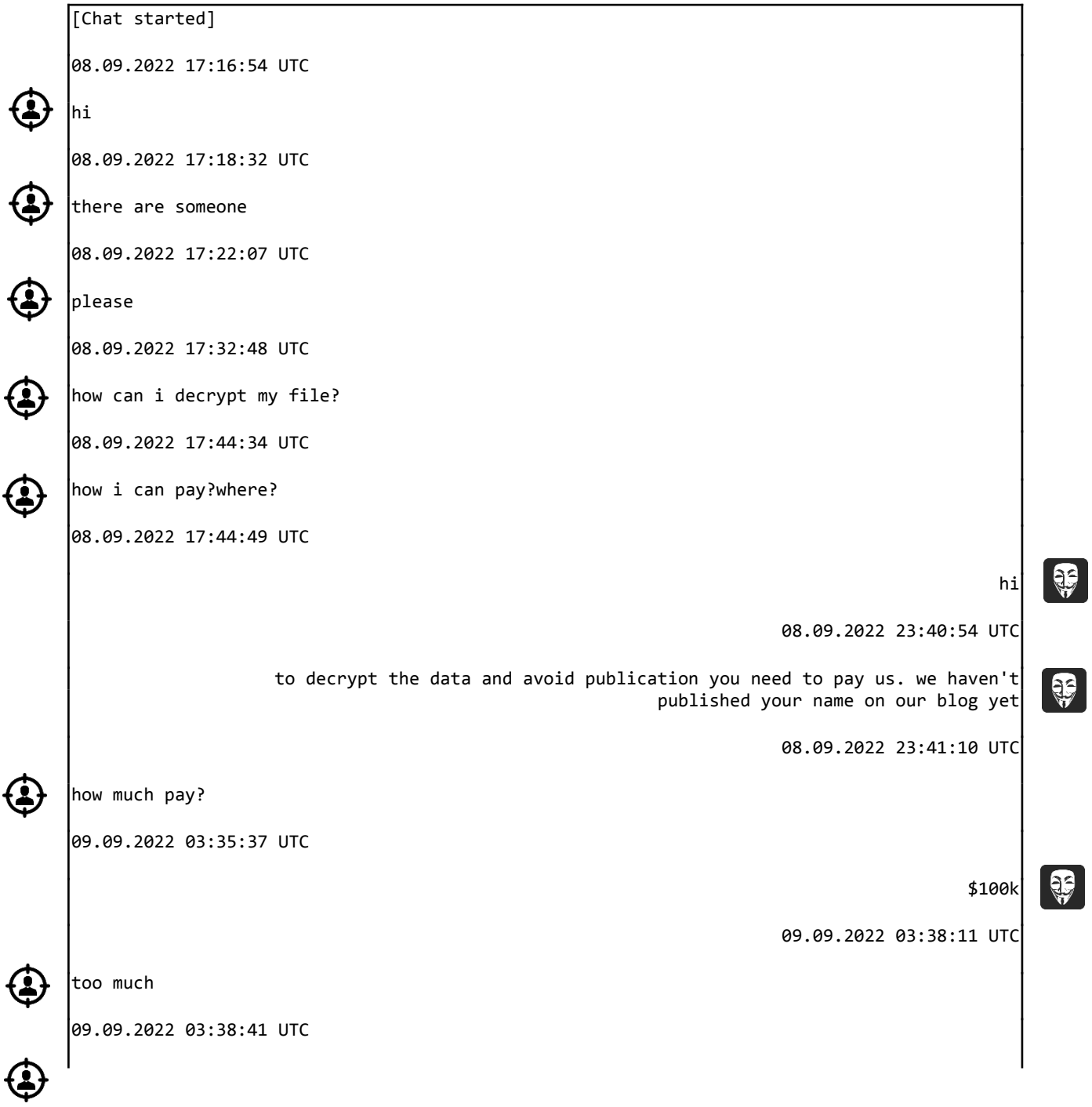
- La inclusió de ferramentes tipus DDos-as-a-Service.

- Reclutament d'*insiders* dins de l'empresa o l'explotació dels coneguts com a *gig workers*, és a dir, empleats temporals o de serveis específics.

- Eines White-label, cosa que permet als afiliats personalitzar la infraestructura i el programari maliciós base com si fos seu.

6. NEGOCIACIONS DE RESCAT

A continuació, analitzarem una negociació de rescat real d'un xat del grup Lockbit3.0 que va tenir lloc el setembre de 2022. Aquest cas mostra de manera molt clara les tàctiques que fa servir un grup cibercriminal en les negociacions.



and i m not sure that you decrypt my file

09.09.2022 03:39:06 UTC

we have a test decryptor, you can try. just use it correctly

09.09.2022 03:40:33 UTC

max 50kb my file are more big

09.09.2022 03:41:05 UTC

then use another file

09.09.2022 03:42:50 UTC

100k$is too much my company is small

09.09.2022 03:43:08 UTC

you'll have to look for money. not that small a company. we know who you are

09.09.2022 03:45:22 UTC

I'll give you advice right away. we don't like whiners and negotiators. we are serious people and we have a reputation and we came here not to play and not to joke. so pay and be free

09.09.2022 03:47:11 UTC

for us is too much if i pay 100k if i pay i can close my company,

i know you are serious

09.09.2022 03:55:11 UTC

i can pay max 10000$

09.09.2022 03:55:38 UTC

how i can pay?

09.09.2022 04:11:20 UTC

ok! i speak with ceo and we pay 100K but how pay?thanks

09.09.2022 04:15:51 UTC

we accept payment only in BTC

09.09.2022 09:11:57 UTC

wich address?

09.09.2022 09:19:18 UTC

bc1qpgggs7j546rfavshtckq4v8x4fh87zztaqw5zz

09.09.2022 09:52:35 UTC

sorry i open account on exchange but i can't buy 100k in btc,

i can only send you 10k in btc otherwise financial company control

me and block my company

09.09.2022 14:10:15 UTC

if you want i send you 10k in btc otherwhise i prefer lost and close my company

09.09.2022 14:11:06 UTC

use brokers. we will not accept 10k

09.09.2022 14:14:25 UTC

you're funny

09.09.2022 14:14:54 UTC

will you pay? or should I publish a post about you?

12.09.2022 14:45:32 UTC

El xat mostrat data de setembre de 2022 entre una petita empresa víctima i el grup LockBit3.0.

Aquest xat és un exemple perfecte de com se solen desenvolupar generalment les negociacions de rescat: Lockbit3.0 arrenca de manera molt forta i fent-se respectar sol·licitant uns 100.000 dòlars a Bitcoin.

En cap moment rebaixen aquest preu, malgrat les contraofertes de la companyia víctima, oferint fins a 10.000 dòlars.

Es pot apreciar com la companyia víctima està nerviosa des del principi, i es va movent pels riscos associats a no pagar el rescat, com ara el possible tancament de l'empresa i, fins i tot, les limitacions que té per moure diners a Bitcoin. Lockbit3.0, així i tot, no es mou del primer preu, amb l'objectiu de mantenir la seva reputació intacta.

D'aquest xat no hi ha resolució coneguda, però el patró és similar en la majoria dels casos: LockBit3.0 buscar intimidar de pressa, no negocia i fa servir l'amenaça de *leak* com a arma principal.

7. ESTRATÈGIES DE PREVENCIÓ I RECUPERACIÓ

A continuació, es detallaran enfocaments clau per millorar les estratègies de prevenció i recuperació davant d'atacs de programari de segrest.

7.1. Estratègies de prevenció

L'estratègia de prevenció és fonamental per evitar els riscos associats al Ransomware-as-a-Service (RaaS). Reduir la superfície d'atac, l'educació dels empleats i enfortir les defenses són mesures clau que ara aprofundirem:

- **Implementació de còpies de seguretat regulars i segures**: és important fer les còpies de seguretat periòdicament, seguint la regla d'1-2-3, que significa tres còpies de dades en dos tipus de mitjans diferents com pot ser en local o al núvol, això fa que les dades que són encriptades puguin ser recuperades sense haver de dependre de la negociació amb els grups de programari de segrest. És vital protegir les còpies de seguretat d'infeccions d'aquest tipus, perquè els grups de programari de segrest els busquen per poder tenir més control en la negociació, i no quedi més remei que dependre'n.

- **Educació dels empleats**: és una de les millors inversions que es poden fer, perquè això fa que es redueixi la superfície del vector d'entrada més utilitzada per aquests grups. Programes de conscienciació, identificació de pesques i tàctiques d'enginyeria social, tot això és el que cal que aprenguin els empleats per crear un entorn corporatiu més segur.

- **Actualitzacions i gestió de vulnerabilitats**: tots els sistemes, programari i microprogramari sempre han d'estar actualitzats i amb els pedaços de seguretat. La gestió de vulnerabilitats també ha de ser una cosa que cal tenir en compte, per resoldre les vulnerabilitats que puguin ser explotades per grups de programari de segrest.

- **Autenticació i control d'accés**: l'ús del MFA o el 2FA a, com a mínim, tots els accessos crítics, però cal tenir en compte que s'ha de fer recomanablement extensible a qualsevol punt d'accés. Adoptar un model Zero Trust també pot marcar la diferència per poder verificar sempre la identitat i limitar certs privilegis.

- **Eines de detecció i defensa**: la implementació de diversos antivirus, sistemes de detecció i resposta, XDRs, SIEMs i tallafocs, és de vital importància per poder monitorar el trànsit que passa a l'organització i d'aquesta manera poder detectar anomalies primerenques per tenir la capacitat d'aïllar dispositius infectats amb la intenció d'evitar una propagació del programari de segrest.

7.2. Estratègies de recuperació

En cas que hagi estat víctima d'un atac de programari de segrest, la recuperació ha de ser ràpida i és important poder minimitzar l'impacte operatiu. Tenir un pla de resposta davant d'incidents és molt beneficiós, sobretot per no haver de pagar rescats. A continuació, aprofundirem en les estratègies de recuperació:

- **Activació del pla de resposta davant d'incidents**: l'equip de resposta davant d'incidents s'ha d'activar immediatament després d'un incident de programari de segrest. Un equip de resposta ha de tenir experts en ciberseguretat, legal i comunicacions. Cal que hi hagi implementats protocols per a la contenció, eliminació i recuperació, sobretot per donar prioritat a la continuïtat del negoci.

- **Aïllament i eliminació del codi maliciós (*malware*)**: s'han d'aïllar els equips infectats per prevenir la propagació del programari de segrest. Tot això, amb eines especialitzades que ajudin a escanejar equips i erradicar el programari de segrest assegurant-nos que no quedi cap rastre.

- **Restauració des de les còpies de seguretat**: mitjançant les còpies de seguretat que estiguin verificades i, el més important, sense infectar. És molt important revisar la integritat de les còpies de seguretat abans de restaurar res, perquè així es podrien produir reinfeccions.

- **Anàlisi després de l'incident i millores dels punts febles**: fer una anàlisi forense de com va succeir l'atac ajuda a actualitzar polítiques i metodologies de seguretat, com també impulsar campanyes de conscienciació i, fins i tot, entrenaments d'equips, basats en lliçons apreses. Identificar la causa ajudarà a no cometre els mateixos errors que han fet que un atac hagi tingut èxit.

8. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.