ANDORRA DIGITAL

ANDORRA DIGITAL CIBERSEGURETAT

Informe de Ciberintel·ligència

Ransomware M3rx: anàlisi d'un incident en una pime i lliçons apreses

TLP: WHITE

JUNY 2026

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	29/06/2026	01/07/2026

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA **4**

2. INTRODUCCIÓ **5**

3. CRONOLOGIA DE L'INCIDENT **6**

4. EL GRUP M3rx: PERFIL DE L'ACTOR **8**
4.1. Com operen? 9
4.2. A qui ataquen? 9
4.3. Per què aquest perfil d'organització encaixa al seu patró 10

5. ANATOMIA DE L'ATAC **11**

6. IMPACTE I CAUSES **12**
6.1. L'impacte de l'incident 12
6.2. Causes: per què va ser possible 12

7. COM PROTEGIR-SE: RECOMANACIONS **13**
7.1. Mesures que hauria de prendre l'organització 13
7.2. Mesures que hauria de prendre cada empleat 13

8. CONCLUSIONS **14**

9. CLÀUSULA DE CONFIDENCIALITAT **15**

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 dia 3 de maig del 2026, una pime del sector assegurador/financer va patir un incident de ciberseguretat de gravetat molt alta. Un atacant va aconseguir accedir a uns dels seus servidors a través d'un accés remot exposat a Internet, va robar una quantitat significativa d'informació i finalment va xifrar els sistemes per impedir-ne l'ús i exigir un rescat. L'incident va afectar els serveis crítics de l'organització i la va obligar a operar de manera parcial durant uns quants dies.

Darrere de l'incident hi ha M3rx, un grup de programari de segrest (*ransomware*) d'aparició molt recent que opera sota el model de doble extorsió, primer robant les dades de la víctima i després xifrant aquestes dades de manera que pot pressionar la víctima per una doble via, la pèrdua d'accés a la informació i l'amenaça de publicar-la.

Aquest informe explica qui és l'atacant, com actua, a quin tipus d'organitzacions se sol dirigir i, sobretot, què es pot aprendre de l'incident.

Des de l'inici és important destacar una idea: la seguretat d'una organització no depèn únicament de les eines tecnològiques ni de l'equip tècnic. Depèn, en gran manera, de les decisions quotidianes de totes les persones que en formen part. Per això aquest informe s'adreça també a tots els empleats, amb independència del lloc o els coneixements informàtics.

Tot seguit, mostrarem una taula sobre què cobrirà l'informe i què no:

Què cobreix aquest informe
L'incident del 3 de maig del 2026 i la seva cronologia. *Què va passar, quan i com va evolucionar, des del primer accés fins a la recuperació.*
El perfil del grup atacant M3rx. *Com opera, a quins sectors i països es dirigeix i per què aquest tipus d'organització encaixa en el patró de víctimes.*
L'anatomia de l'atac i les causes. *Els passos que va seguir l'atacant i les febleses que ho van fer possible.*
Les mesures recomanades. *Quines mesures són les recomanades i què pot fer cada persona al seu dia a dia.*
Què no cobreix aquest informe
Dades identificatives reals. *La informació delicada es presenta de manera anonimitzada.*
Detall tècnic ofensiu. *Els indicadors i tècniques concretes de l'atac es tracten únicament a nivell conceptual, sense convertir-se en una guia operativa.*

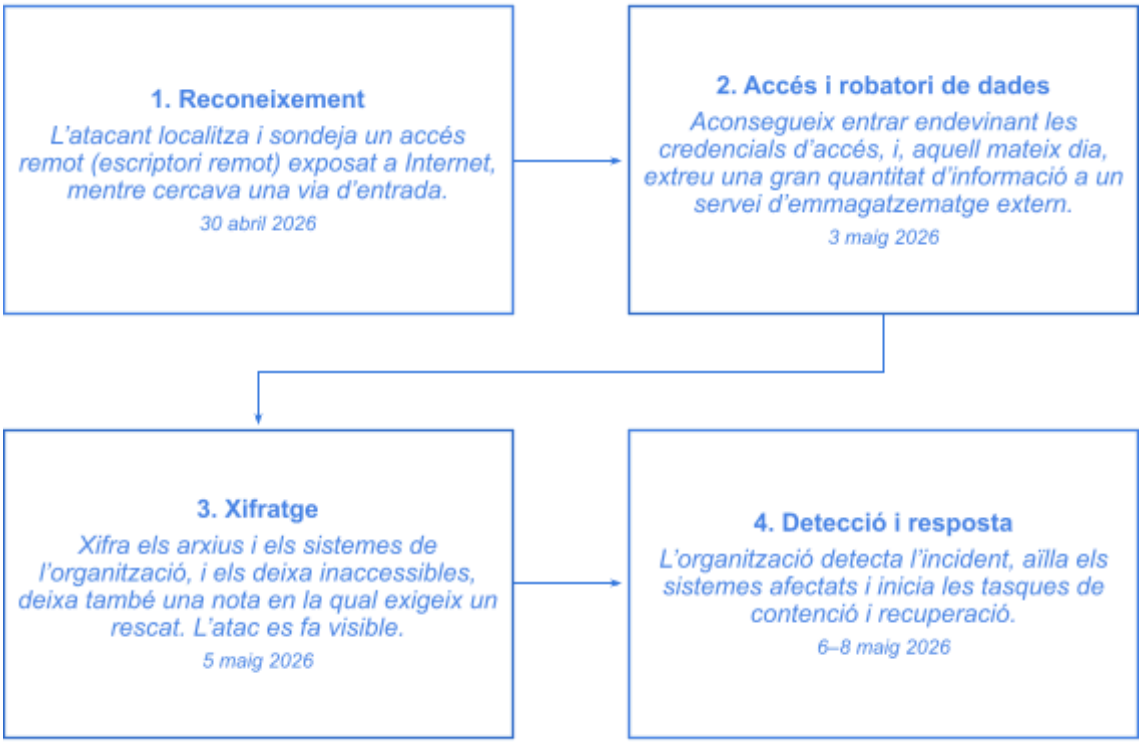
Taula 1 – Què cobreix aquest informe i què no

3. CRONOLOGIA DE L'INCIDENT

L'atac no va ser un succés que va passar de la nit al dia, sinó que va ser un procés que es va desenvolupar al llarg de diversos dies. Entendre les diferents fases de l'atac permet entendre com actuen aquest tipus d'atacants i en quin moment una organització té l'oportunitat de detectar-los i posar-hi remei.

A grans trets l'incident va comportar 4 fases diferents: la primera, la de reconeixement, en què l'atacant va escanejar els sistemes exposats a internet; la segona, l'accés i el robatori de dades, en què l'atacant va entrar al servidor i va extreure informació d'interès; la tercera, en la qual l'atacant va xifrar la informació i va deixar la nota de rescat; i, finalment, la de detecció i resposta, en què l'organització va identificar l'atac i va començar les tasques de contenció i recuperació.

El més interessant de tota la cronologia és el temps que l'atacant va aconseguir romandre dins dels sistemes sense ser detectat. Van passar diversos dies des del primer accés fins que l'atac es va fer visible amb el xifratge.

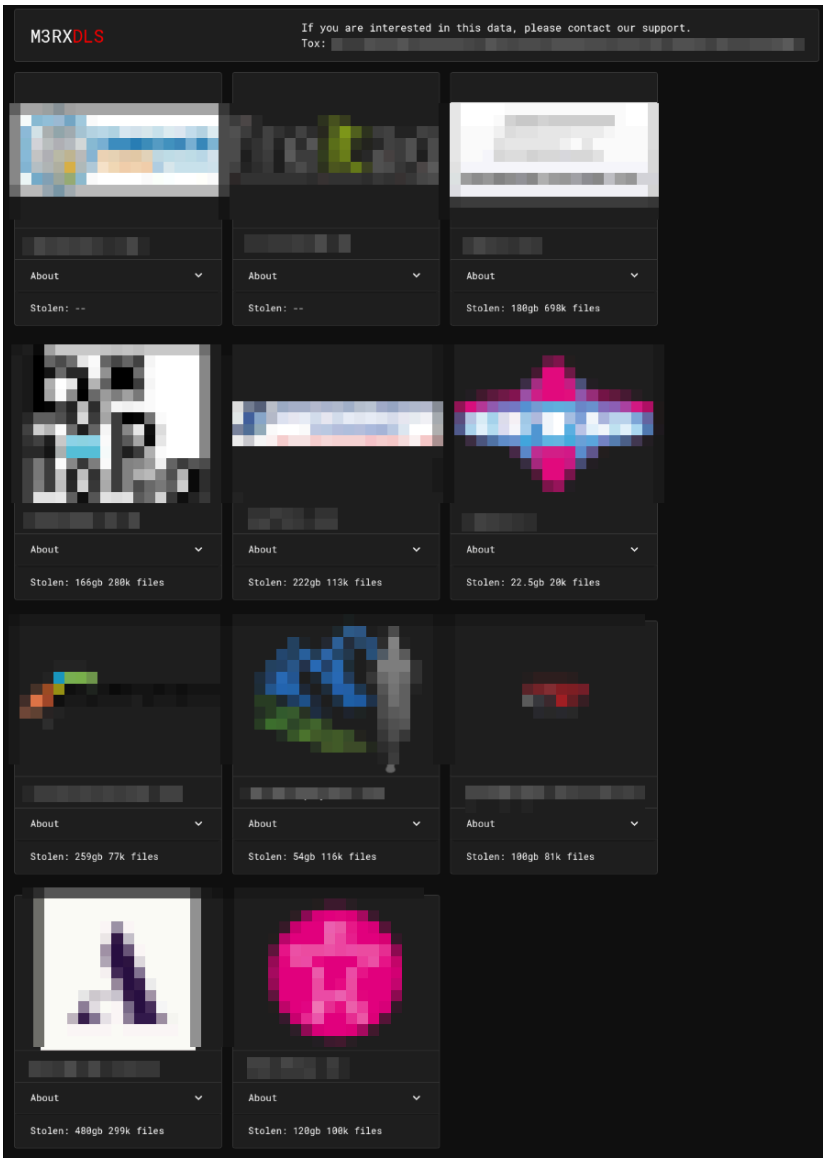


Il·lustració 1 - Línia temporal de l'incident

Un detall important que cal recordar és que l'atacant no va atacar a cegues ni a l'atzar, l'atacant va dedicar molt temps a estudiar prèviament els sistemes accessibles des d'Internet abans d'intentar accedir als sistemes. Això demostra que la víctima no va ser escollida a l'atzar, sinó que l'atac va ser el resultat d'una cerca activa d'organitzacions amb accessos vulnerables exposats.

4. EL GRUP M3rx: PERFIL DE L'ACTOR

Darrere de l'incident hi ha el grup M3rx, un grup de ciberdelinqüents especialitzat en programari de segrest (*ransomware*). Com ja hem indicat prèviament el grup és de creació molt recent, les seves primeres víctimes publicades al DLS són de l'abril del 2026. En data de la publicació d'aquest informe, han reivindicat unes 26 organitzacions de múltiples països.



Imatge 1 – DLS del grup M3rx

4.1. Com operen?

M3rx utilitza una tècnica coneguda com a doble extorsió, que s'ha convertit en l'estàndard dels grups de programari de segrest actuals. Com ja ho hem explicat a la introducció de manera molt resumida la tècnica emprada pel grup M3rx funciona en dos temps:

1. **Primer roben les dades**: abans de fer res visible i sospitós, el grup exfiltra una gran quantitat d'informació de la víctima.
2. **Després xifren els sistemes:** bloquegen els fitxers i l'equip perquè l'organització no pugui operar, i deixen una nota en la qual exigeixen un pagament per al rescat.

D'aquesta manera, M3rx pressiona per una doble via: l'organització no pot accedir a la seva informació i per altra s'amenaça de publicar les dades robades. Com s'ha pogut observar a la imatge 1, M3rx manté un lloc web al web fosc on van anunciant públicament les víctimes que no cedeixen, tot exhibint-les al que es coneix com el mur de la vergonya.

El pagament que exigeixen és a la criptomoneda bitcoin i sol negociar-se amb la mateixa víctima, en ser un grup nou el fet de pagar no garanteix recuperar la informació xifrada.

4.2. A qui ataquen?

M3rx no té un únic objectiu quant a sector o país, les víctimes es reparteixen per diversos continents i sectors, això sí, tenen un patró clar: busquen empreses sovint petites o mitjanes, amb alguna porta d'entrada mal protegida o configurada. Les taules següents resumeixen el seu perfil de víctimes conegut:

Sectors afectats
Tecnologia i serveis informàtics
Indústria i fabricació
Logística i transport
Serveis a empreses
Sector sanitari
Comerç i distribució
Sector immobiliari
Agricultura
Serveis financers i d'assegurances

Taula 2 – Perfil de víctimes del grup M3rx – Sectors

Països amb víctimes confirmades
Estats Units
Canadà
Regne Unit
Itàlia
Austràlia
Espanya
Alemanya
Suïssa
Dinamarca
Índia

Taula 3 – Perfil de víctimes del grup M3rx - Països

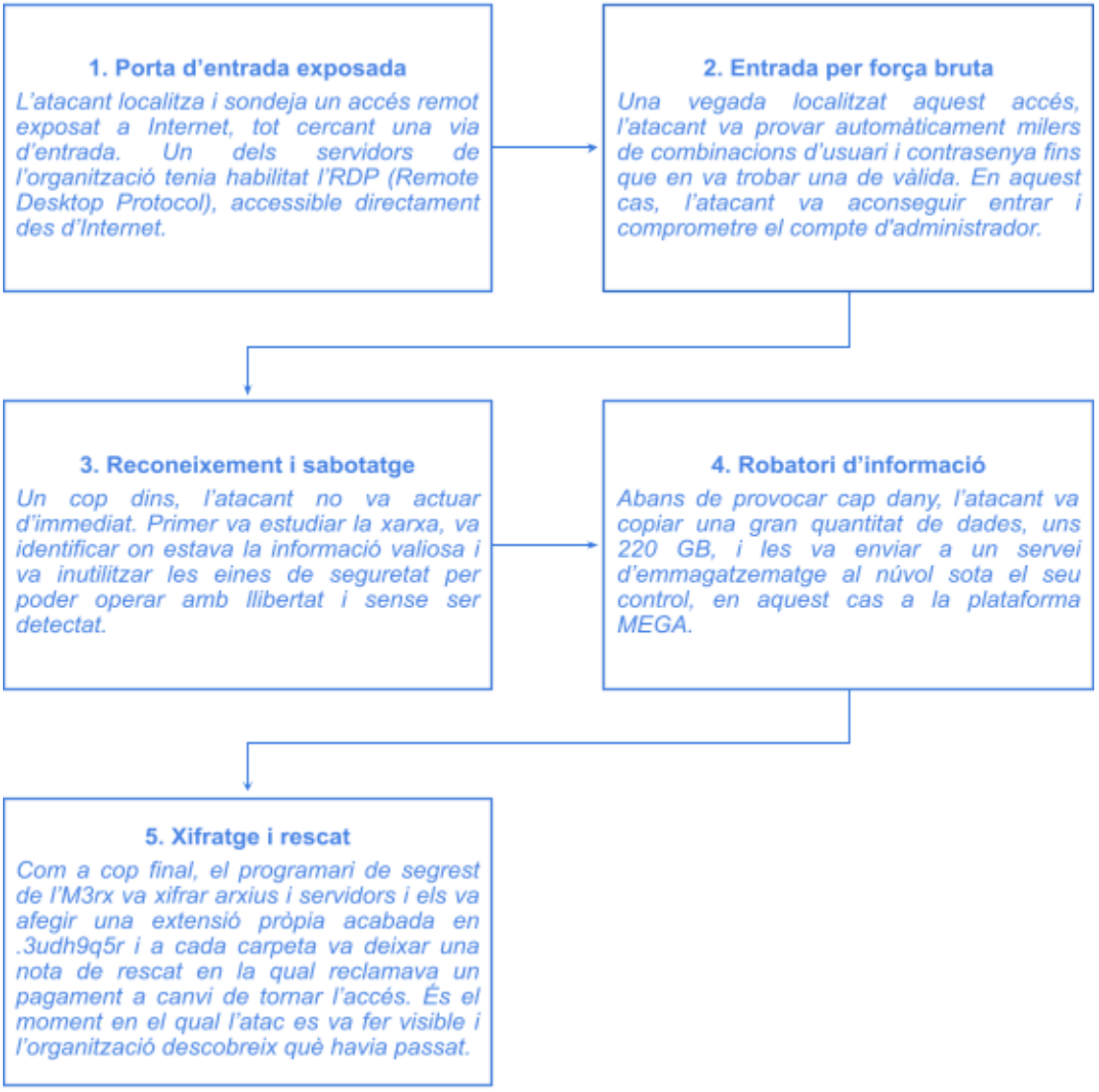
4.3. Per què aquest perfil d'organització encaixa al seu patró

Que entre les víctimes de l'M3rx hi hagi organitzacions de l'àmbit financer i assegurador no és casualitat, i explica perquè una pime d'aquest sector resulta un objectiu molt lucratiu per a grups de programari de segrest com ara l'M3rx. Tot seguit, s'exposaran els patrons clars:

- **Gestionen informació molt sensible i valuosa**: dades personals, financers i de pòlisses de molts clients, cosa que augmenta el valor de les dades robades i la pressió per pagar el rescat.
- **Estan subjectes a obligacions legals**: la possible filtració de dades personals comporta unes conseqüències legals i regulatòries, cosa que afegeix un incentiu més per poder fer xantatge a aquestes organitzacions.
- **Solen disposar de menys recursos de ciberseguretat**: com que són empreses petites o mitjanes, fan que es converteixin en un objectiu més accessible.

5. ANATOMIA DE L'ATAC

Tot i que un atac de programari de segrest sembla un cop sobtat, en realitat és l'última peça d'una cadena de passos encadenats. Cada pas d'aquesta cadena representa un punt on l'atac podria haver estat evitat. A continuació, explicarem cada pas d'incident amb detall:



Il·lustració 2 - Anatomia de l'atac pas a pas

6. IMPACTE I CAUSES

Tot seguit explicarem l'impacte i les causes d'incident.

6.1. L'impacte de l'incident

Un atac de programari de segrest no causa un únic dany, sinó diversos alhora i en plans diferents, és per això que les conseqüències per a l'organització es van repartir en 4 àmbits diferents:

Àmbit	Impacte de l'incident
Operatiu	Servidors i fitxers xifrats i inaccessibles. L'organització va haver d'operar de manera parcial durant diversos dies, amb la pèrdua conseqüent de productivitat i de servei.
Informació i confidencialitat	Robatori d'una gran quantitat de dades, amb possible exposició d'informació personal, financera i de clients. Encara que es recuperin els sistemes, aquesta informació ja es va exfiltrar.
Recuperació	Les còpies de seguretat van quedar afectades, cosa que va dificultar la tornada a la normalitat.
Reputacional i legal	Risc que les dades robades es publiquin al lloc de M3rx, i obligacions derivades de la normativa de protecció de dades.

Taula 4 - Impacte de l'incident per àmbits

6.2. Causes: per què va ser possible

Tan important com saber que va passar és entendre per què va ser possible, no per apuntar culpables, sinó per corregir les vulnerabilitats concretes que l'atacant va saber aprofitar. Aquest incident no va passar per una tècnica sofisticada ni una fallada impossible de preveure, sinó per una combinació de vulnerabilitats bàsiques i conegudes que mostrarem a continuació:

- **Un accés remot (RDP) exposat a Internet**: el servei RDP accessible des de qualsevol punt de la xarxa és un risc conegut i un dels vectors més explotats en els atacs de programari de segrest.
- **Autenticació feble i sense doble factor**: l'atacant va poder entrar provant contrasenyes per força bruta sobre un compte d'administrador. L'absència d'un segon factor de verificació (MFA) ho va fer més fàcil.
- **Còpies de seguretat mal protegides**: en estar connectades de forma permanent i accessible, les còpies van quedar exposades al mateix xifrat que la resta dels sistemes.
- **Defenses que es van poder desactivar i una intrusió no detectada a temps**: l'atacant va aconseguir inutilitzar eines de seguretat i moure's durant dies sense ser descobert, cosa que indica que faltaven mecanismes de protecció.

L'atac va ser possible a causa de vulnerabilitats bàsiques, que també es podrien haver previngut amb mesures bàsiques, de fet, d'això tracta la secció següent.

7. COM PROTEGIR-SE: RECOMANACIONS

Un incident com aquest deixa una lliçó clara, perquè la seguretat és una responsabilitat compartida entre l'organització i els empleats. Aquesta secció es dividirà en dues parts, mesures a nivell d'organització i accions concretes que estan en mans de cada empleat.

7.1. Mesures que hauria de prendre l'organització

Cadascuna de les accions que van fer possible l'atac tenen una mesura recomanada. La taula següent relaciona les dues coses:

Debilitat aprofitada per l'atacant	Mesura recomanada
Accés remot (RDP) exposat a Internet	Eliminar l'exposició directa de l'accés remot i permetre l'accés només mitjançant una connexió segura i controlada.
Contrasenyes febles i sense doble factor	Implantar la verificació en dos passos MFA als accessos i aplicar una política de contrasenyes més robusta.
Còpies de seguretat desprotegides	Disposar de còpies de seguretat aïllades i a prova de xifratge, verificades de manera periòdica.
Defenses desactivables i intrusió no detectada	Reforçar les eines de seguretat amb protecció davant de manipulació i establir una vigilància contínua que detecti intrusions de forma primerenca.

Taula 5 – Debilitats i recomanacions a nivell organització

7.2. Mesures que hauria de prendre cada empleat

Encara que aquest no sigui el cas, la majoria dels atacs de programari de segrest comencen aprofitant la distracció d'un empleat. Tot seguit, mostrarem les accions més eficaces a adoptar:

Àmbit	Mesures que pot fer l'empleat
Contrasenyes	Fer servir contrasenyes llargues i úniques per a cada servei; mai no reutilitzar-les ni compartir-les. Disposar del suport d'un gestor de contrasenyes, és clau.
Verificació en dos passos (MFA)	Activar-lo sempre que estigui disponible. Sempre que es rebi una sol·licitud d'aprovació de MFA, no acceptar-la: ja que podria ser un intent d'accés extern.
Correu i pesca	Desconfiar de missatges inesperats que continguin enllaços, adjunts o un to d'urgència. Verificar el remitent i, davant del dubte, no fer clic a res que no coneguis.
Equips i sessions	Bloquejar la sessió quan l'usuari s'absenti, mantenir l'equip actualitzat i no instal·lar programes no autoritzats.
Report	Avisar immediatament davant de qualsevol cosa que sigui estranya o fora del comú. És preferible una falsa alarma a un avís que arriba tard.

Taula 6 – Recomanacions a nivell emprat

8. CONCLUSIONS

L'incident analitzat no va ser fruit d'un atac sofisticat ni d'un atacant amb grans habilitats, sinó el resultat d'unes poques debilitats bàsiques aprofitades per un grup expert a buscar-les. Aquesta és alhora la dolenta i la bona notícia: l'atac va ser possible, però també era evitable.

A continuació, mostrem les conclusions principals de l'informe:

- **L'atac no va començar amb el xifratge, sinó abans**: quan els sistemes van ser xifrats, l'atacant feia dies que estava a dins i ja havia exfiltrat la informació. El que era visible només va ser el final d'una cadena que va començar amb una porta exposada i una contrasenya feble.
- **El robatori i exfiltració de dades és un dany irreparable**: els sistemes es recuperen restaurant còpies, però la informació que surt de l'organització no es pot recuperar. Per això, la prevenció importa més que la capacitat de recuperació.
- **M3rx no va triar aquesta organització per qui és, sinó per encaixar en un perfil rendible**: una pime del sector financer/assegurador, amb dades valuoses i un accés exposat, és exactament el tipus d'objectiu que aquests grups busquen de forma activa.
- **Ser una pime no t'allunya de ser atacada**: aquests grups no descarten una organització per ser petita. Si troben l'oportunitat, l'aprofiten. Les empreses petites solen ser objectius més fàcils, precisament perquè tenen menys recursos en ciberseguretat.
- **Per a una pime, un atac així pot ser la seva fi**: el temps sense facturar, el cost de recuperació, les possibles sancions i el dany reputacional, tots sumats, poden arribar a comprometre la viabilitat del negoci.
- **Les debilitats eren bàsiques i, per tant, també ho són les solucions**: tancar els accessos remots exposats, activar la verificació en dos passos, protegir les còpies de seguretat i vigilar la xarxa són mesures conegudes i a l'abast de l'organització.
- **La seguretat és una responsabilitat compartida**: les eines i les mesures tècniques són imprescindibles, però la primera línia de defensa són els empleats, una contrasenya forta, un clic que no es fa i, sobretot, un avís a temps pot marcar la diferència.

En definitiva, aquest incident ha d'entendre's menys com un cop de mala sort i més com una crida d'atenció útil. Els atacs de programari de segrest com el de M3rx continuaran produint-se i buscant objectius vulnerables, però les organitzacions que aprenen de casos com aquest i reforcen el que és bàsic i consciencien la seva plantilla són precisament les que deixen de ser un blanc fàcil.

Per acabar, deixem aquesta cita de Robert Mueller, exdirector de l'FBI:

> *«Només hi ha dos tipus d'empreses: les que han estat atacades i les que ho seran.»*

Més enllà del to rotund, la frase conté una veritat útil: convé assumir que l'incident pot passar i cal preparar-se en conseqüència, en lloc de confiar que mai passarà.

9. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat d'Andorra Digital. 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 d'Andorra Digital.