Paula Segalà Ribé

ESTUDI SOBRE EL RANSOMWARE I TÈCNIQUES PER MITIGAR-NE L'IMPACTE

TREBALL DE FI DE GRAU

Co-dirigit pel Dr. Jordi Castellà Roca

Co-dirigit per Cristòfol Daudén Esmel

Grau d'Enginyeria de Sistemes i Serveis de Telecomunicacions

UNIVERSITAT ROVIRA I VIRGILI

Tarragona

2024

Agraïments

Vull expressar el meu sincer agraïment als meus directors del Treball de Fi de Grau, el professor Jordi Castellà i Cristòfol Daudén per la seva dedicació, paciència i compromís, que han estat fonamentals per a la realització d'aquest treball. Han invertit moltes hores del seu temps per oferir-me orientació i suport en cada pas del procés, i han mostrat un gran interès perquè aquest projecte esdevingués un treball ben fet i interessant.

Gràcies per les vostres aportacions i per la motivació constant, sense la vostra ajuda no hauria estat possible.

Resum

Les Tecnologies de la Informació i la Comunicació (TIC) són essencials en moltes empreses. Al mateix temps les fa susceptibles a atacs cibernètics. Un dels que més es produeix és el ransomware, on els atacants xifren les dades i exigeixen un rescat per recuperar-les. En aquest treball s'ha estudiat l'evolució del ransomware, identificant els factors que han permès el seu creixement i fent-lo un negoci lucratiu. Entre els factors a destacar hi ha les criptomonedes, els mètodes de xifratge robustos, i les infraestructures al núvol. Finalment, s'han descrit mesures de protecció per reduir el risc d'atac i recuperar-se el més aviat possible.

Resumen

Las Tecnologías de la Información y la Comunicación (TIC) son esenciales en muchas empresas. Al mismo tiempo las hace susceptibles a ataques cibernéticos. Uno de los que más se produce es lo ransomware, donde los atacantes cifran los datos y exigen un rescate para recuperarlas. En este trabajo se ha estudiado la evolución del ransomware, identificando los factores que han permitido su crecimiento y haciéndolo un negocio lucrativo. Entre los factores a destacar hay las criptomonedas, los métodos de cifrado robustos, y las infraestructuras a la nube. Finalmente, se han descrito medidas de protección para reducir el riesgo de ataque y recuperarse lo más bien posible.

Abstract

Information and Communication Technologies (ICT) are essential in many companies. At the same time, it makes them susceptible to cyber attacks. One of the most successful is ransomware, where attackers chiffen the data and demand a rescue to recover them. In this work, the evolution of ransomware has been studied, identifying the factors that have allowed its growth and making it a lucrative business. Among the factors to be highlighted are cryptocurrencies, robust encryption methods, and cloud infrastructures. Finally, protective measures have been described to reduce the risk of attack and recover as soon as possible.

Índex

Índex de Figures

Índex de Taules

1. Introducció

“Les Tecnologies de la Informàtica i la Comunicació (TIC) són les tècniques i els processos que utilitzem per crear, transferir o administrar informació mitjançant l'electrònica i la informàtica” [1]. En les últimes dècades, hem estat veient un increment continu d’aquestes tecnologies [2], les quals ens aporten avantatges significatius en molts sectors, transformant la manera com interactuem, treballem i ens entretenim.

Als anys noranta es va començar a expandir internet, i el correu electrònic es va convertir en una forma habitual de comunicació personal i professional. A la dècada dels 2000 es van popularitzar els telèfons intel·ligents i les xarxes socials. En els següents anys, les criptomonedes es van convertir en una nova forma de transferir valor de forma segura, i els pagaments mòbils cada vegada es van fer més populars [3]. El 2020 les tecnologies continuaven expandint-se i gairebé sense avís, ens vam trobar en una pandèmia, forçant milions de persones a adaptar-se per treballar i estudiar des de casa. Això va ser possible gràcies a l'avenç tecnològic dels darrers anys.

Avui en dia, en qualsevol àmbit depenem d’alguna manera de les tecnologies. En l’àmbit personal, si volem fer una reserva, demanar una cita o comprar entrades ho fem per internet. En l’àmbit de la salut, els hospitals guarden els registres dels pacients en sistemes electrònics, aportant accessibilitat al gran volum de dades que gestionen. En l’educació, gràcies a la quantitat d'informació que podem trobar a internet, com llibres electrònics i enciclopèdies, es pot obtenir un aprenentatge més personalitzat segons les necessitats de cada usuari, amb infinits recursos multimèdia per a fer més visual l'aprenentatge. A més, l’aula virtual és una eina que millora el seguiment dels alumnes i l’administració i avaluació de proves i tasques en línia. En l’àmbit laboral tothom disposa d’un correu electrònic, o una pàgina web. Per empreses repartides arreu del món, milloren en la comunicació a distància, gràcies a poder fer remotament entrevistes o videoconferències.

Totes les comoditats que ens aporten les tecnologies, també ens exposen a vulnerabilitats i riscos significatius, especialment en l’àmbit de la privadesa i la seguretat de les nostres dades. Una mostra és el nombre d’atacs cibernètics que es produeixen cada vegada en més mesura, i entre aquest s’ha de destacar el creixement dels atacs de ransomware en els últims anys [4], com es pot veure a la *Figura 1* [5]. Aquest aprofita el desconeixement dels usuaris per intentar segrestar les seves dades. Els ciberdelinqüents veuen una oportunitat de negoci en aquests atacs, que poden afectar tant a usuaris individuals com a grans organitzacions. Per afrontar aquest desafiament és essencial tant comprendre el funcionament del ransomware com implementar estratègies de protecció i recuperació.

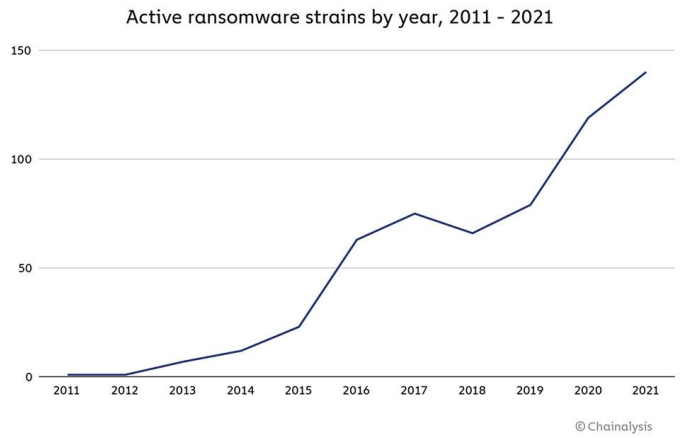

Figura 1. Varietats actives de ransomware per any, 2011 – 2021

1.1. Objectius

Donada la importància de l'impacte dels atacs de ransomware, els objectius d'aquest treball són:

- Descriure què és el ransomware i quin és el seu funcionament, des de l'estudi de la víctima fins a les conseqüències finals de l'atac.
- Fer un estudi de la seva evolució, els orígens i els elements claus que han contribuït a la seva expansió.
- Estudiar l'impacte econòmic d'aquests atacs.
- Conèixer les mesures de protecció i recuperació davant d'aquest tipus de programa maliciós.

1.2. Motivació i justificació

Els atacs de ransomware representen una amenaça greu a nivell econòmic, social i de gestió, ja que poden paralitzar operacions, causar pèrdues financeres importants i danyar la reputació de les organitzacions afectades. Amb l'augment d'aquests atacs en els darrers anys, és imprescindible entendre la gravetat del problema i la necessitat d'adoptar mesures de protecció. Per això, aquest treball s'ha realitzat amb la finalitat de comprendre millor aquest risc i explorar estratègies efectives per prevenir i mitigar els atacs de ransomware.

1.3. Organització de la memòria

La *Secció 2* conté una breu descripció del *malware* i dels diferents tipus que existeixen. S'aprofundeix amb el ransomware i s'expliquen conceptes previs que aniran apareixent al llarg del treball, per facilitar-ne una millor comprensió. A continuació es presenta un estudi del ransomware a la *Secció 3.* Aquest va des del seu origen fins als atacs més recents. Al final, es mostra una taula concisa amb un resum de cadascun d'aquests atacs, on s'explica el vector d'atac, el mètode de xifratge i el pagament. A més, s'inclou una línia cronològica que situa tots els atacs analitzats. L'impacte econòmic dels atacs es descriu a la *Secció 4*. S'analitza com el ransomware ha arribat a ser de lucratiu i els imports que s'han arribat a pagar per recuperar-se dels atacs. També s'estudien els sectors més atacats i vulnerables, així com els atacs no reportats. Per tal de protegir-nos, s'aborda el cicle de la seguretat a la *Secció 5*, exposant les mesures que s'han de prendre abans, durant i després dels atacs de ransomware. Finalment, a la *Secció 6* es presenten les conclusions del treball i se suggereixen les línies de treball futur que es podrien desenvolupar.

2. Conceptes previs

El *malware* (programari maliciós) és un programa o codi creat per danyar ordinadors, xarxes i servidors. Els ciberdelinqüents el desenvolupen per infiltrar-se a sistemes informàtics de manera discreta per restringir l'accés a les dades, filtrar informació confidencial o comprometre involuntàriament la seguretat informàtica i la privadesa de l'usuari [6].

El malware constitueix la major part del panorama d'amenaces en línia [7]. Depenent de qui és el receptor i l'objectiu de l'atac, podem separar-ne diferents tipus. A la *Taula 1* podem veure alguns dels més coneguts [6]:

Tipus de malware	Objectiu
Spyware	Fa un seguiment de les dades dels usuaris, que pot incloure pulsacions de tecles o hàbits de navegació, per recopilar informació de les activitats de la seva víctima o extreure altres dades, sense el seu coneixement.
Adware	Fer un seguiment de l'activitat en línia dels usuaris per determinar quins anuncis mostrar.
Trojan	Enganyar els usuaris perquè descarreguin o instal·lin un programa que conté malware per capturar dades, obtenir accés no autoritzat a les xarxes, suprimir, modificar o capturar dades, de forma il·lícita sense que la víctima se n'adoni.
Worms	Modificar i eliminar fitxers, injectar programari maliciós o fer còpies de si mateix per esgotar recursos del sistema. Es propaga fent còpies de si mateix d'un ordinador a un altre, sense interacció humana. Es poden transmetre a través de vulnerabilitats.
Rootkits	Facilitar l'accés no autoritzat, permeten als ciberdelinqüents prendre el control del sistema compromès. Poden manipular les funcions i els processos del sistema.
Ransomware	Xifrar els fitxers d'un usuari i extorsionar-los exigint un rescat per recuperar les dades, per no vendre-les o publicar-les.

Taula 1. Tipus de Malware

Dels tipus de *malware* descrits, el ransomware és l'amenaça més predominant [4].

El ransomware és un tipus de codi maliciós que impedeix l'ús dels equips o sistemes que infecta. El ciberdelinqüent aconsegueix el control d'un sistema informàtic i el "segresta" encriptant la informació (ransomware crypto) o bloquejant la pantalla (ransomware locker). L'usuari és víctima d'una extorsió, on se li exigeix un pagament a canvi de recuperar els fitxers xifrats [7]. Aquest atac pot comportar conseqüències irreparables en termes de privadesa i seguretat de dades, ja que poden posar-les a la venda o fer-les públiques; i fins i tot podria ser impossible tornar a accedir-hi a causa d'un mal xifratge.

A continuació, es definiran conceptes que apareixeran al llarg del treball, per una millor comprensió:

- **Autoexec.bat** - Els arxius .bat són arxius de text que executen seqüències de comandes, amb l'objectiu d'automatitzar feines que requereixen un llarg nombre d'instruccions. Autoexec.bat és el responsable de regular la seqüència d'inici del sistema operatiu MS-DOS abans que aquest executi Windows [9].

- **RSA** - El xifratge RSA és una manera segura d'enviar missatges secrets i verificar la seva autenticitat utilitzant un parell de claus, una pública i una privada. Per a una explicació més àmplia, consulteu [12].

- **AES** - L'Advanced Encryption Standard (AES) és un estàndard de xifratge simètric desenvolupat pel National Institute of Standards and Technology (NIST) per protegir dades crítiques. AES utilitza claus de 128, 192 o 256 bits per xifrar i desxifrar informació en blocs de 128 bits, proporcionant un alt nivell de seguretat i eficiència, i és àmpliament utilitzat a tot el món per garantir la confidencialitat de la informació [14].

- **BlackHole** - BlackHole és un kit d'explotació utilitzat en campanyes de correu brossa per infectar sistemes vulnerables amb malware [18].

- **Phishing** - El phishing és una tècnica fraudulenta que utilitza correus electrònics o altres missatges convincents per enganyar les persones perquè obrin enllaços perjudicials o descarreguin programari maliciós [21].

- **Botnet** - Una botnet és una xarxa d'ordinadors infectats amb programari maliciós que són controlats per un atacant. Aquests ordinadors es poden utilitzar per llançar atacs coordinats, com ara robatori de comptes, atacs distribuïts de denegació de servei (DDoS) i campanyes de *phishing*, així com per robar informació confidencial [29].

- **Macro** - Les macros són esquemes predefinits que automatitzen processos, i poden ser creades o modificades pels usuaris, sempre que tinguin coneixements bàsics de programació [30].

- **Tor** - The Onion Router (TOR) és una *darknet* amb l'objectiu de crear una xarxa de comunicacions distribuïda i superposada a Internet convencional [31].

- **MS17-010** - EternalBlue és un *exploit* de Microsoft, identificat com MS17-010, que permetia a la NSA accedir de manera il·legal a dispositius amb sistemes operatius Windows [36].

- **Payload** - Un payload és la càrrega útil que s'executa una vegada que s'ha aprofitat una vulnerabilitat mitjançant un *exploit* [37].

- **Dark Web** - La Dark Web és una part de la Deep Web que està intencionadament oculta als motors de cerca. Aquesta secció de la web utilitza adreces IP emmascarades i només és accessible mitjançant navegadors especials, com el navegador Tor [52].

3. Història del ransomware

En aquesta secció analitzarem els orígens i l'evolució del ransomware, destacant els factors clau del vector d'atac, els mètodes de xifratge i les formes de pagament dels diferents ransomware.

3.1. Origen i antecedents

AIDS Trojan o *PC Cyborg* es considera el primer atac de ransomware. Va ser distribuït pel Dr. Joseph Popp el desembre de 1989. La companyia PC Cyborg va enviar uns 26.000 disquets infectats per correu postal, etiquetats com a *AIDS Information Introductory Diskette* [8], a usuaris subscrits a revistes relacionades amb la ciència i membres de l'OMS. Quan el disquet estava inserit al sistema, segrestava l'arxiu *AUTOEXEC.BAT* i l'alterava per comptar el nombre de reinicis del sistema. Quan el comptador arribava a 90, el programa s'activava i xifrava els noms dels fitxers del disc dur mitjançant un xifratge de substitució simètric senzill. A continuació, mostrava un missatge per renovar la llicència per tal de desxifrar i recuperar els arxius, juntament amb la direcció a un apartat postal a Panamà per fer el pagament [10]. Popp no va rebre diners, però l'atac va causar pànic, algunes pèrdues, i va posar de manifest la necessitat de mesures de seguretat de les dades.

Durant quinze anys els atacs de ransomware van estar aturats. Tot i això, amb el boom d'internet, el correu electrònic com a mètode de comunicació i l'arribada de les monedes digitals, aquests atacs es van reprendre.

3.2. Evolució i tècniques actuals

El desembre del 2004, a Rússia, es van rebre notícies d'usuaris que els seus fitxers havien estat xifrats i no sabien quin programa s'havia utilitzat. Aquest ransomware el van anomenar *GPcode*. Va afectar generalment bancs, agències de publicitat, immobiliàries i altres organitzacions que feien servir un gran nombre de documents. Es va usar un algorisme de xifratge simètric propi que es va poder desxifrar. L'autor de *GPcode* estava interessat en el volum d'atacs, ja que si demanava imports petits, les víctimes pagarien el rescat. Els usuaris afectats rebien instruccions per correu electrònic per fer el pagament i posteriorment desxifrar els fitxers. Es demanaven 1000 rubles, tot i que estaven disposat a acceptar-ne 500 (uns 20 dòlars). L'èxit d'aquest atac va fer que continuessin cometent-ne.

El juny del 2005 hi va haver una segona onada de *GPcode*. Aquest cop l'algorisme era més complex però també desxifrable, ja que llavors els experts ja havien vist més de 25 variants. El 26 de gener del 2006 es va detectar *GPcode.ac*, primera variant de *GPcode* en utilitzar algorisme de xifratge RSA de 56 bits. Era un gran salt de les tècniques de xifratge, així i tot, també el van poder desxifrar. A l'abril hi va haver una altra variant que feia servir parcialment l'algorisme RSA, igual que les anteriors, però aquesta vegada la clau de xifratge era de 67 bits [11].

A principis de juny de 2006 es van utilitzar noves variants per llançar un atac massiu. Van aparèixer 3 variants de *GPcode* en cinc dies. Cada variant utilitzava una clau de xifratge més llarga: *GPcode.ae* tenia una clau RSA de 260 bits, *GPcode.af* de 330 bits i *GPcode.ag* de 660 bits. Les persones que havien deixat la seva informació de contacte a un dels principals llocs web de contractació de Rússia van rebre un correu electrònic que semblava ser d'una empresa important. El correu brossa contenia *malware*, i quan els usuaris obrien el fitxer adjunt, s'instal·lava un troià que descarregava *GPcode*, encriptant més de 80 tipus de fitxers. Això va dificultar molt la determinació del vector d'infecció original, ja que no es va connectar el correu electrònic de contractació amb els fitxers xifrats dels usuaris. Després d'instal·lar-se, s'autodestruïen i deixaven un fitxer anomenat *readme.txt* on es comunicava que els fitxers havien estat xifrats amb RSA i per comprar el descodificador havien d'enviar un correu a k47674@mail.ru. En aquests atacs demanaven uns 70 dòlars. Els diners s'havien de dipositar en un compte Yandex (similar a PayPal). Tots els mètodes de xifratge contenien errors, així que va poder trencar l'algoritme utilitzat [11].

Al principi de juny del 2008 es va detectar *GPcode.ak*, que utilitzava el xifratge RSA amb una clau de 1024 bits, i que no repetia els errors trobats en versions anteriors del malware. Un cop els fitxers estaven xifrats, deixaven un missatge de text comunicant que si volien recuperar-los, s'havien de posar en contacte amb ells (********@yahoo.com) [13].

L'autor va estar parat del 2008 al 2010. L'any 2010 va canviar de mètode. No eliminava els fitxers després del xifratge sinó que sobreescrivia les dades dels fitxers, cosa que feia impossible utilitzar programari de recuperació de dades. Al novembre va aparèixer *Gpcode.ax* que utilitzava RSA-1024 i AES-256 [15]. Més tard va aparèixer *GPcode.bn*, que demanava el pagament mitjançant targetes de prepagament Ukash [16].

El gener del 2009 va aparèixer el bitcoin. La primera criptomoneda realment descentralitzada [17]. Això va fer que tot l'escenari dels atacs de ransomware canviés. A mesura que va començar a guanyar més atractiu, els desenvolupadors de ransomware el van reconèixer com el mètode d'extracció monetària que estaven buscant.

3.2.1. Atacs després del bitcoin

A finals del 2011 es va detectar el ransomware *Reveton*. Aquest va diferenciar-se dels ransowmare anteriors pels seus mètodes d'intimidació. S'instal·lava a través del kit d'explotació BlackHole, que utilitzava vulnerabilitats en navegadors i *plugins* com Java, Flash i Adobe Reader. Quan la víctima navegava a un lloc web compromès es redirigia a un lloc especialment dissenyat que allotjava aquest kit. Si BlackHole detectava una vulnerabilitat, l'explotava i instal·lava un troià al sistema, i al mateix moment el ransomware *Reveteon* [19]. Aquest malware bloquejava a l'usuari deixant-lo fora del sistema, el que es coneix com el ransomware de tipus locker. Mostrava un missatge que ocupava tota la pantalla i es personalitzava segons la ubicació de la víctima, per fer creure que era la policia local, amb logotips oficials. Acusava l'usuari d'haver comès un delicte. Els atacants feien pagar a la víctima una multa d'entre 100 i 200 euros, mitjançant un servei com Ukash, Paysafe, MoneyPak [20]. Es coneixen al voltant de 20 variants de *Reveton* [19].

El setembre del 2013 es va identificar *CryptoLocker*. S'enviava amb un fitxer adjunt a través d'un correu de *phishing*, que imitava l'aspecte d'empreses legítimes. Quan la víctima obria el fitxer, un ZIP presentat com a PDF, es descarregava el programari maliciós i s'executava automàticament, xifrant diversos tipus de fitxers. *CryptoLocker* utilitzava una clau RSA de 2048 bits per xifrar els fitxers i els afegia una extensió, per exemple *.encrypted*, *.cryptolocker* o *.[7 caràcters aleatoris]*, segons la variant. Finalment, el malware creava un fitxer a cada directori afectat que enllaçava a una pàgina web amb instruccions de desxifrat, que requerien que l'usuari fes un pagament. Es demanaven 300 dòlars en bitcoin, amb un límit de temps per pagar. Si no es pagava dins d'aquest interval, la clau de desxifratge s'eliminava, fent pràcticament impossible recuperar-la. L'única manera de desxifrar les dades era fent el pagament [22].

CryptoLocker va tenir diverses versions, però els autors a més van convertir el codi en un nou tipus de ransomware anomenat *CryptoWall*, que va ser identificat per primer cop l'any 2014. Hi va haver quatre versions diferents, cada nova versió es va crear per evitar les defenses de seguretat [23].

3.2.2. Millora en el mètode de xifratge

El febrer del 2014 es va identificar *TorrentLocker*. Combinava elements de *CryptoLocker* i *CryptoWall*. Tot i això, *TorrentLocker* era completament diferent d'aquests dos tipus de ransomware. Utilitzava un xifratge de blocs simètric AES per xifrar els fitxers de la víctima i un xifratge asimètric RSA per xifrar la clau AES [24]. Es propagava mitjançant *phishing*, correus electrònics que deien que la víctima havia de pagar una factura, un paquet per correu o una multa per excés de velocitat. Les primeres versions van ser fàcils de trencar, ja que tenien una debilitat (van usar el mateix flux de claus repetidament) [25]. Al desembre es va llançar una nova versió arreglant els errors, cosa que va fer impossible desxifrar els fitxers sense pagar el rescat. Les primeres versions demanaven enviar un correu per demanar la clau de desxifrat pel pagament. A les següents versions es feia tot a través de la pantalla de bloqueig de la víctima on es proporcionava tota la informació sobre com fer el pagament amb bitcoin [26].

El 2016 *SamSam* va causar infeccions importants a hospitals dels Estats Units, tot i que es va detectar el 2015. Aquest ransomware s'utilitzava en atacs dirigits [27]. És a dir, atacaven organitzacions específiques que sabien que podien pagar grans quantitats de diners, com hospitals o institucions educacionals. A diferència dels anteriors ransomware, s'esperaven per atacar, espiaven un llarg temps després de la infecció inicial, sense ser detectat. Analitzaven on havien penetrat a la xarxa per si podien penetrar encara més en els sistemes per causar el màxim dany possible. Eliminava o sabotejava silenciosament les còpies de seguretat, després atacava i bloquejaven els fitxers [28]. Els atacs a objectius es van produir mitjançant servidors JBoss vulnerables. El 2018 *SamSam* va usar vulnerabilitats en sistemes RDP (Remote Desktop Protocol), servidors web desenvolupats en Java o servidors FTP (File Transfer Protocol) o va utilitzar atacs de força bruta contra contrasenyes febles per accedir a les xarxes. Els fitxers s'havien xifrat amb RSA-2048. La nota de rescat oferia desbloquejar un fitxer gratuïtament com a mostra de confiança. Els pagaments els demanaven mitjançant bitcoin [27].

Locky va ser identificat el febrer del 2016. Aquest ransomware combinava múltiples tècniques per atacar com *botnets, phishing*, enginyeria social i *malware*. La *botnet* de Necurs distribuïa milions de correus *spam* amb documents adjunts de Microsoft Word. Els correus especificaven que el document adjunt era una factura. Quan la víctima descarregava i obria el document, veia uns caràcters aleatoris i un text que deia que s'habilitarien les macros si la codificació de dades semblava incorrecta. Quan la víctima activava les macros, es descarregava i s'executava un troià. Aquest troià xifrava els fitxers de dades, com documents i fotos, amb les extensions predefinides mitjançant la clau AES de 128 bits i el xifratge de clau RSA de 2048 bits. Als fitxers xifrats els afegien l'extensió *.locky*. Finalment, la víctima trobava un missatge de text que explicava els passos a seguir per recuperar els fitxers. Els passos incloïen utilitzar el navegador Tor i pagar el rescat en criptomonedes. Els hackers proporcionaven a la víctima el seu identificador d'atac per utilitzar-lo després de pagar la clau de desxifrat. El ransomware Locky va tenir moltes variants i va donar origen a imitadors com *PowerLocky, Diablo, Zepto, Odin, Osiris, Thor* i *Lukitus* [32].

3.2.3. Nou model de negoci (RaaS)

El *Ransomware as a Service (RaaS)* és un model de negoci en què un grup de ransomware ven el seu codi del *malware* a altres *hackers*, que després el fan servir per realitzar els seus propis atacs de ransomware. Així, els *hackers* poden obtenir beneficis de l'extorsió sense haver de desenvolupar el seu propi *malware*, mentre que els desenvolupadors de ransomware poden augmentar els seus guanys sense haver de realitzar manualment els atacs a les xarxes. A partir del 2015 el ransomware va evolucionar cap al model *RaaS*. Aquesta estratègia s'ha anat perfeccionant i popularitzant fins a l'actualitat, contribuint a un augment significatiu dels atacs. Un informe de 2022 de Zscaler va trobar que 8 dels 11 ransomware més actius eren variants de RaaS [33].

El març del 2016 es va tenir coneixement per primer cop el *Ransomware as a Service (RaaS) Cerber*. Aquest es propagava amb correus de *phishing* que contenien un arxiu *.DOT* protegit amb contrasenya o un *Windows Script File (WSF)*. El correu contenia una contrasenya per obrir l'arxiu .DOT, que després executava una macro maliciosa. *Cerber* s'executava després que l'usuari hagués estat inactiu durant un temps. Mostrava alertes falses del sistema per obligar l'usuari a reiniciar el sistema. Amb el dispositiu reiniciat, *Cerber* iniciava el procés de xifratge. Concretament, xifrava 442 tipus de fitxers diferents amb AES-256 i RSA. L'usuari rebia instruccions per descarregar Tor per poder fer el pagament d'aproximadament 500 dòlars amb bitcoin [34]. Va estar parat fins al 2020 que va tenir un *peak* on va ser responsable del 58% dels intents d'atacs de l'àrea de la salut mundialment, coincidint amb la covid. Es creia que els atacs eren dirigits a petites empreses i particulars, ja que per cada transició movien pocs diners [35]. No atacava a dispositius de certs països, com Rússia [34].

La primera notícia del ransomware *Petya* va ser al 2016. Es propagava principalment a través de correus electrònics o vulnerabilitats. Els correus electrònics maliciosos seguien un patró sobre ofertes de feina o procediments legals perquè l'usuari hi confiés per executar els fitxers adjunts compromesos tipus *.zip, .exe, .pdf, .pif,* etc. o diversos enllaços a serveis en línia. També utilitzava la vulnerabilitat MS17-010 (EternalBlue) per propagar-se. Quan un ordinador s'infectava amb *Petya*, executava la càrrega útil (*payload*) que xifrava les dades dels sistemes del disc dur. *Petya*, a diferència d'altres ransomware, xifrava la Taula de Fitxers Mestre (MFT) del disc dur, que actua com una guia de referència ràpida per a tots els fitxers que es troben a la unitat. En no poder accedir a l'MFT, l'ordinador no trobava cap fitxer, de manera que no s'iniciava. Després d'instal·lar-se el ransomware a l'ordinador, s'infectava el Master Boot Record (MBR), la part de l'ordinador que carrega el sistema operatiu quan l'ordinador està encès. El procés era el següent: Petya obligava l'ordinador a reiniciar-se i després es mostrava la nota de rescat mentre s'estava xifrant l'MFT. L'ordinador infectat no podia accedir al contingut del seu disc dur, ni tan sols al seu sistema operatiu [38]. Petya utilitzava SALSA20 per xifrar parts essencials del disc [39]. Demanaven el pagament amb bitcoin [40].

Notpetya va ser una variant que es va conèixer el 2017. Va ser més perillós que *Petya* perquè encriptava permanentment qualsevol fitxer que es trobava. En un atac d'aquest ransomware, les víctimes no podien recuperar els fitxers ni pagant el rescat, per això es podria considerar un *wiper* disfressat de ransomware [38].

El ransomware *WannaCry* es va conèixer al maig del 2017. Aquest ransomware va destacar per la capacitat que va tenir de propagació utilitzant *worms* per difondre's a altres màquines dins d'una mateixa xarxa o fins i tot a través d'Internet; per aquesta raó va causar un impacte global molt ràpid. Igual que Petya, aprofitava la vulnerabilitat EternalBlue que afectava versions antigues i no actualitzades de Microsoft Windows [41]. Per xifrar els fitxers *WannaCry* generava una clau RSA-2048 única per a cada infecció i l'utilitzava per xifrar les claus AES-128 generades aleatòriament per cada fitxer. [42]. Exigien 300 dòlars en bitcoin, i un temportitzador a la pantalla d'infecció indicava quan doblarien el rescat si no el pagaven en tres dies. Entre les víctimes de *WannaCry* hi havia empreses i hospitals [41].

BitPaymer es va conèixer al juny del 2017 [43]. BitPaymer es propagava principalment a través de fitxers adjunts maliciosos en correus electrònics i actualitzacions de programari falses. També utilitzava troians que obrien portes posteriors al sistema. BitPaymer utilitzava una combinació d'algorismes de xifratge RC4 i RSA-1024 per xifrar els fitxers, afegint l'extensió .locked als noms de fitxer. Cada víctima rebia una clau única emmagatzemada en un servidor remot controlat pels atacants. Les demandes de rescat oscil·laven entre 500 i 1.500 dòlars, generalment pagats en criptomonedes. Els atacants solien proporcionar instruccions detallades per correu electrònic [44].

DoppelPaymer és una variant d'aquest ransomware que va començar a evolucionar el 2019 millorant la seva velocitat de xifrat. També va començar a amenaçar amb publicar les dades de les víctimes si no es pagava el rescat [44].

GandCrab es va descobrir a finals de gener del 2018 com un *RaaS* i es va convertir en el més conegut de l'any. Els seus autors van llançar com a mínim cinc versions, invertint temps en el manteniment i desenvolupament de cadascuna d'elles. *GandCrab* utilitzava el *Top Level Domain (TLD) .bit*, un *TLD* no sancionat per la ICANN, cosa que proporcionava un nivell addicional de secret als atacants. Aquest ransomware es distribuïa mitjançant correus brossa, kits d'explotació com GrandSoft i RIG, entre d'altres. Els correus de *spam* contenien arxius ZIP amb scripts que es descarregaven i executaven el ransomware. Aquest generava un parell de claus RSA de 2048 bits efímer a cada màquina, és a dir, la clau RSA es generava al moment, i es feia servir per xifrar la clau AES de 256 bits i el vector d'inicialització (IV) utilitzats per xifrar els fitxers. Als fitxers xifrats se'ls afegia l'extensió *.CRAB*. Per recuperar els fitxers, les víctimes havien de descarregar el navegador TOR i accedir a un URL on es trobaven les instruccions per al pagament del rescat. *GandCrab* va ser el primer ransomware a demanar el pagament amb la criptomoneda DASH, i oferia l'oportunitat de desxifrar un fitxer gratuïtament com a prova [45].

El ransomware *Ryuk* va ser detectat per primera vegada l'agost de 2018 i actuava com un *RaaS*. Utilitzava un enfocament específic per seleccionar i infectar les víctimes [46], buscava empreses i institucions que provoquessin interrupcions importants en els seus serveis com diaris, hospitals i serveis públics. El 91% dels atacs es cometien a través de correus de phishing [47], sovint combinats amb altres malwares com Trickbot i Emotet. A més, *Ryuk* explotava vulnerabilitats com la ZeroLogon en servidors de Windows. Per a l'encriptació dels fitxers, utilitzava l'algorisme AES-256 amb claus simètriques, que eren xifrades amb RSA-4096. Podia encriptar dades tant localment com remotament, incloent-hi accés a comparticions administratives remotes. A més, també era capaç d'eliminar les còpies de seguretat automàtiques, fent que la recuperació fos molt difícil sense còpies de seguretat externes [48]. El pagament del rescat se sol·licitava mitjançant bitcoin [46].

A l'abril del 2019 es va analitzar un nou *RaaS* anomenat *REvil/Sodinokibi*, que era altament evasiu i prenia moltes mesures per prevenir la seva detecció. Presentava similituds amb el ransomware *GrandCrab*. Per atacar, s'explotava vulnerabilitats en servidors, com la vulnerabilitat Oracle WebLogic (CVE-2019-2725). Més tard, també es va utilitzar kits d'explotació i correus de *phishing* amb enllaços maliciosos que contenien fitxers ZIP. *REvil* eliminava còpies de seguretat i comprovava l'idioma del sistema per evitar xifrar arxius en certs països. Utilitzava un xifratge RC4 [49] i s'afegia una extensió aleatòria a cada fitxer. A través del navegador Tor es mostrava una nota de rescat on es requeria el pagament en bitcoin. També s'oferia una prova de desxifrat per demostrar que la clau de desxifrat funcionava. REvil buscava víctimes d'alt valor, com empreses i proveïdors de serveis gestionats (MSPs), amb l'objectiu d'extorquir grans sumes de diners [50].

3.2.4. Doble extorsió de les dades

El ransomware *Maze* es va detectar el maig del 2019, inicialment conegut com a *ChaCha Ransomware* [51], i operava com un RaaS. Aquest atac era especialment perillós perquè, a més de xifrar les dades, els delinqüents amenaçaven de vendre o filtrar informació amb valor comercial si no es pagava el rescat, sovint a través de la *dark web* [52], o fins i tot utilitzar la informació robada per atacar clients i socis de les víctimes. *Maze* va crear una pàgina web on llistava les víctimes i publica mostres de dades robades com a prova. Típicament, es distribuïa mitjançant *phishing*, atacs de força bruta RDP i utilitzant kits d'explotació. Quan el malware aconseguia accés a una xarxa els operadors intentaven obtenir els màxims privilegis per poder implementar el xifratge de fitxers a totes les unitats [53]. El ransomware Maze utilitzava un esquema criptogràfic complex que incloïa el xifratge dels fitxers amb el xifratge ChaCha, i les claus generades es xifraven amb claus RSA-2048, garantint que el desxiframent fos difícil i només possible amb la clau privada dels atacants. A més, afegia extensions aleatòries als fitxers xifrats. Finalment, demanaven el pagament del rescat amb criptomonedes [51].

El ransomware *Clop*, o *Cl0p* es va observar per primera vegada a principis de 2019. Es propagava principalment mitjançant correus electrònics, webs o enllaços malicosos i explotava vulnerabilitats com Accellion FTA i ZeroLogon. *Cl0p* xifrava els fitxers utilitzant una combinació d'algoritmes AES, RSA, i RC4 amb les claus de xifratge emmagatzemades en un servidor remot, i afegia l'extensió *.clop* als fitxers. Després del xifratge, deixava notes amb instruccions per pagar el rescat, generalment en criptomonedes, i amenaçava de publicar les dades robades si no es feia el pagament [54]. *Clop* tenia la capacitat de propagar-se per la xarxa, eliminar els punts de restauració del sistema i evitar controls de seguretat mitjançant signatures digitals. També es va observar que no s'executava en sistemes configurats en rus [55]. A més, utilitzava la doble extorsió, amenaçant la víctima amb filtrar la informació si el rescat no es pagava dins del termini especificat. Podien també intimidar les víctimes dient que vendrien les dades robades a competidors o a la dark web, afegint més pressió [54].

NetWalker va ser descobert l'agost de 2019. Inicialment, es coneixia com a *Mailto*, que era l'extensió que s'afegia als fitxers encriptats [56]. El març de 2020 *NetWalker* es va convertir en un RaaS, i des de llavors va expandir el seu abast global. Pagava als seus afiliats fins a un 80% de cada rescat exitós. Aquest ransomware es distribuïa a través de correus de *phishing* que semblaven provenir de fonts legítimes, utilitzant dades relacionades amb la Covid-19. Quan els scripts del correu s'activaven, l'executable es guardava a la carpeta temporal de la víctima i l'atac s'iniciava. Les víctimes no eren conscients de la infecció, ja que el malware operava clandestinament, aprofitant processos legítims de Microsoft. Això s'aconseguia mitjançant una tècnica coneguda com a *process hollowing*, on el codi de l'executable de Microsoft es reemplaçava pel codi maliciós de *Netwalker* per accedir al sistema. A continuació, es realitzava una extracció massiva de totes les dades crítiques, que es xifraven amb l'algoritme AES [57]. Un cop completat l'atac, es publicaven mostres de les dades a la *dark web*, i es notificava a les víctimes amb una nota de rescat. Havien de pagar a través del navegador TOR, amb bitcoin, si no volien que es publiquessin més dades. Després del pagament, les víctimes rebien una eina de desencriptació específica per a la seva variant de *Netwalker* [58].

Els primers atacs de *LockBit van començar el s*etembre del 2019, que llavors es coneixia com el ransomware *ABCD* per l'extensió dels arxius xifrats. Era un *RaaS* i els atacants afiliats rebien fins a tres quarts dels fons del rescat. *Lockbit* era dirigit per processos predissenyats i automatitzats per buscar objectius valuosos, propagar la infecció i xifrar tots els sistemes informàtics accessibles a una xarxa [59]. Buscaven objectius que poguessin pagar el rescat, i que no poguessin prescindir dels fitxers xifrats, com el sector de la salut. Per infiltrar-se als sistemes utilitzava correus de *phishing*, amb fitxers maliciosos adjunts o links, que quan s'obrien, desplegaven el *payload* del ransomware; explotaven vulnerabilitats; o utilitzava atacs de força bruta RDP. Quan aconseguia l'accés inicial, per moure's lateralment dins de la xarxa, extreia les credencials del sistema per augmentar els privilegis i accedir a altres dispositius; escanejava la xarxa per identificar objectius addicionals i sistemes vulnerables; i utilitzava eines d'administració del sistema legítimes com PowerShell i PsExec per evitar la detecció. Utilitzava una combinació d'AES i RSA. A més, canviaven les extensions dels fitxers xifrats, al principi per *.abcd* i versions posteriors van optar per *.LockBit,* i també inserien un arxiu a cada carpeta amb una nota pel rescat. Abans de xifrar els fitxers, LockBit robava les dades i amenaçava en publicar-les si no es pagava el rescat [60], demanat amb bitcoin [61].

Conti, un altre *RaaS* [62], va estar actiu des del desembre del 2019 al maig del 2022. Va destacar per la velocitat amb què xifrava les dades i s'estenia a altres sistemes, i per pagar als afiliats amb un salari fix. Com a accés inicial utilitzava *phishing* per instal·lar TRickBot i BazarLoader Trojans, per aconseguir accés remot de les màquines infectades. Utilitzaven missatges que semblava que venien d'un remitent en el qual confiava la víctima. L'enganyava perquè descarregués un document maliciós de Google Drive. Un cop descarregat, també s'instal·lava un malware de la blackdoor de Bazaar (obtenir accés a un comte d'administrador de domini) per desactivar eines de seguretat. També utilitzava un mètode multithreading per estendre's ràpidament. Amenacen la víctima amb filtrar les dades a la *dark Web*. Normalment, revelava en un dark forum una petita quantitat de dades xifrades. També es podia propagar a través del Server Message Block (SMB). Després d'infectar el sistema, Conti robava les dades, eliminava còpies de seguretat i xifrava amb AES i RSA [63]. Demanaven el pagament amb bitcoin [64].

Darkside es va identificar com un *RaaS* l'agost de 2020, amb semblances amb REvil. Utilitzava principalment correus electrònics de *phishing* personalitzats i explotava comptes i sistemes accessibles remotament, com VDI (Virtual Desktop Infrastructure) i RDP (Remote Desktop Protocol). També podia aprofitar processos legítims de Microsoft mitjançant tècniques com el *process hollowing*. *DarkSide* utilitzava els algoritmes Salsa20 i RSA per xifrar dades crítiques. Demanava el pagament del rescat en bitcoins a través de TOR, amenaçant de fer públiques les dades robades si no es pagava, fins i tot si la víctima aconseguia recuperar les dades xifrades per altres mitjans. DarkSide es centrava en grans organitzacions que podien permetre's pagar grans rescats, evitant atacar hospitals, escoles, organitzacions sense ànim de lucre i institucions governamentals [drakside]. Van construir la seva pròpia xarxa de distribució de continguts (CDN) per emmagatzemar i lliurar les dades compromeses. *Darkside* va atacar al gasoducte Colonial Pipeline, que va causar una gran interrupció en la distribució de combustible als Estats Units, on es va pagar un rescat de 4,4 milions de dòlars [65]. Una variant és *BlackMatter*.

El setembre del 2020 van començar els atacs del ransomware *Egregor*, considerat una variant del ransomware *Sekhmet*. També es va observar que col·laboraven amb afiliats de *Maze* [66]. *Egregor* funcionava com un RaaS [67]. Els afiliats utilitzaven tècniques d'atac com *malspam* i l'explotació de vulnerabilitats del RDP, a més d'eines com Qbot, Cobalt Strike, Advanced IP Scanner, SharpHound i AdFind. Abans de xifrar les dades, *Egregor* utilitzava Rclone i 7zip per a l'extracció de dades. *Egregor* utilitzava l'algoritme ChaCha per xifrar fitxers i RSA-2048 per xifrar les claus ChaCha [66]. Els fitxers xifrats tenien extensions de fitxers modificades amb cadenes de caràcters aleatoris. El *payload* només es podia desxifrar si es proporcionava la clau correcta. El pagament del rescat es negociava mitjançant una funció xat especial a cada víctima, i es feia en bitcoin [68]. També robava les dades de la víctima i les emmagatzemava als servidors dels atacants abans de xifrar-les. Si no es pagava el rescat en un termini de 72 hores, les dades es publicaven a la web d'extorsió "Egregor News" [67].

Hive es va observar per primera vegada el juny de 2021, i operava com un *RaaS*. Es distribuïa mitjançant correus electrònics de *phishing* amb adjunts maliciosos, credencials VPN filtrades, i l'explotació de vulnerabilitats, com les de Microsoft Exchange (ProxyShell). Hive xifrava els fitxers amb els algoritmes Elliptic Curve Diffie-Hellman (ECDH) i XChaCha20-Poly1305. Durant el procés de xifratge, es creava una nota de rescat en text pla en cada carpeta amb fitxers xifrats. El rescat es demana amb bitcoin a través de la xarxa TOR, amb l'amenaça de publicar les dades robades a la web *HiveLeaks* si no es complien les condicions [69]. Els sectors més afectats eren sanitat i fabricació [70].

BlackCat, també conegut com ALPHV, va sorgir al desembre de 2021 com a *RaaS*. Atacava a través de correus de phishing. Un cop dins el sistema, xifrava els fitxers amb l'algorisme XChaCha20-Poly1305. Després de xifrar els sistemes, *BlackCat* exigia rescats en criptomonedes, amenaçant amb fer públics les dades si no es pagava. Abans de la seva desarticulació, *BlackCat* va afectar més de 1.000 organitzacions, causant danys significatius a sectors com l'energia, la construcció, i les finances [71].

Royal es va observar per primera vegada a principis del 2022. Els vectors d'atac incloïen l'ús de formularis de contacte de llocs web empresarials per enviar enllaços maliciosos, documents PDF maliciosos distribuïts com a nòmines, malvertising amb Google Ads, i alertes falses de caducitat de proves de programari per enganyar les víctimes a instal·lar malware. Xifrava els arxius utilitzant un mòdul conegut com Zeon que es basava en l'encriptació parcial per evadir la detecció, utilitzant XChaCha20-Poly1305. Els fitxers xifrats tenien extensions *.royal* o *.royal_w*. Royal també utilitzava tàctiques de doble extorsió, amenaçant de fer públiques les dades robades si no es pagava. Les demandes de rescat oscil·laven entre 250,000 i 2 milions de dòlars, demanats amb bitcoin. Royal no es venia com un RaaS. En lloc d'això, el grup Dev-0569, que operava Royal, comprava accés directe a les xarxes corporatives de IABs i gestionava internament les campanyes d'atac. Royal atacava principalment grans empreses. Les seves víctimes van incloure organitzacions com el Silverstone Circuit, el Travis Central Appraisal District i una important empresa de telecomunicacions dels Estats Units, que va rebre una demanda de rescat de 60 milions de dòlars [72]. Blacksuit en va ser una variant, i actuava com a *RaaS*.

Descripció del codi utilitzat a la *Taula 2*:

VECTOR D'ATAC:

D – Disquets.

E – Enginyeria social.

P – Phishing (exemples: emprenen el nom d'empreses legítimes per enganyar als usuaris amb un ZIP adjunt; simulen factures, paquets o multes falses; adjunten malwares com TrickBot i Emotet).

K – Kit d'explotació (exemplse: BlackHole que executa un troià; GrandSoft i RIG).

V – Vulnerabilitats (exemples: MS17-010 (EternalBlue); ZeroLogon; en servidors).

F – Força bruta (exemple: en RDP).

MÈTODE DE XIFRATGE:

S – Xifratge de substitució Simètric senzill.

SP – Algorisme de xifratge Simètric Propi.

SD – Sobre Digital.

L – Ransomware tipus Locker, bloqueja la pantalla, no xifra les dades.

SD + CE – Sobre digital + claus efimeres.

PAGAMENT:

AP – Apartat Postal.

Y – Compte Yandex.

TP – Targetes de Prepagament (exemples: Ukash, Paysafe, MoneyPak)

BC – Bitcoin.

C – Criptomonedes.

D – Criptomoneda DASH

A la taula següent es presenta de manera concisa un resum del vector d'atac, el mètode de xifratge i el mètode de pagament de cadascun dels ransowmare analitzats prèviament:

NOM	VECTOR D'ATAC	MÈTODE DE XIFRATGE	PAGAMENT
AIDS Trojan	D	S	AP
GPcode -GPcode.ac -GPcode.ae -GPcode.af -GPcode.ag -GPcode.ak -GPcode.ax -GPcode.bn	E, P -E, P -E, P -E, P -E, P -E, P -E, P -E, P	SP -RSA 56 i 67 bits -RSA 260 bits -RSA 330 bits -RSA 660 bits -RSA 1024 -SD -SD	Y -Y -Y -Y -Y -Y -Y -TP
Reveton	K, V	L	TP
CryptoLocker	P	RSA 2048	BC
TorrentLocker	P	SD	BC
SamSam	V, F	RSA 2048	BC
Locky	B, P, E	SD (AES 128 RSA 2048)	C
Cerber	P	SD (AES 256 i RSA)	BC
Petya	P, V	SALSA20	BC
WannaCry	V	SD (RSA-2048 AES-128)	BC
BitPaymer	P, E	RC4 i RSA-1024	C
GandCrab	P, K	SD (RSA 2048 i AES 256)	D
Ryuk	P, V	SD (AES 256 i RSA 4096)	BC
REvil	V, K, P	RC4	BC
Maze	P, F, K	ChaCha i RSA-2048	C
Clop	P, V	AES, RSA i RC4	C
Netwlaker	P	AES	BC
Lockbit	P, V, F	SD (AES i RSA)	BC
Conti	P	SD (AES i RSA)	BC
Darkside	P, K	Salsa20 i RSA	BC
Egregor	P, M	SD (ChaCha i RSA 2048)	BC
Hive	P, V	XChaCha20-Poly1305	BC
BlackCat	P	XChaCha20-Poly1305	C
Royal	P	XChaCha20-Poly1305	BC

Taula 2. Vector d'atac, mètode de xifratge i pagament dels ransomware analitzats

A continuació, a la *Figura 2* es presenta una línia cronològica dels atacs analitzats, amb un resum destacat de cadascun d'ells:

Figura 2. Línia cronològica dels atacs analitzats

4. Impacte econòmic dels atacs

El ransomware s'ha convertit en un negoci altament lucratiu, impulsat per l'anonimat que ofereixen els pagaments no traçables i els avenços tecnològics. Aquesta forma de ciberdelinqüència ha evolucionat, perfeccionant les tècniques d'extorsió per maximitzar els guanys. A la *Figura 3* [74] [75] es pot observar que el negoci del ransomware és extremadament rendible, amb un augment constant dels imports pagats per les víctimes. A la *Figura 4* [76] podem veure que s'han pagat rescats d'imports molts grans. Els cibercriminals ajusten les seves demandes segons la capacitat econòmica de la víctima, exigint sumes més elevades si saben que l'objectiu té recursos suficients. En molts casos, els imports exigits són tan elevats que poden posar en risc la continuïtat de l'empresa [73], fent que el ransomware sigui una amenaça crítica per a l'estabilitat econòmica de les organitzacions.

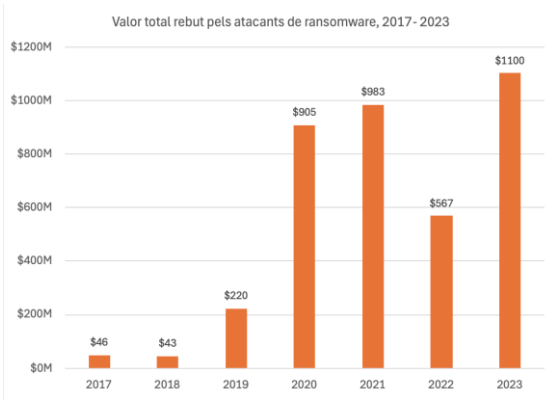

Figura 3. Valor total rebut pels atacants de ransomware, 2017-2023

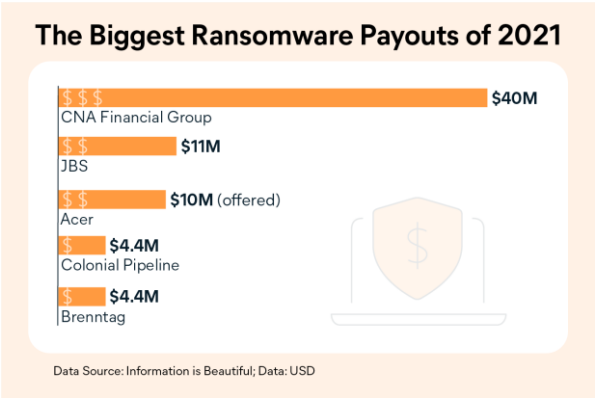

Figura 4. Els pagaments més grans de ransomware de 2021

Analitzant amb més detall la *Figura 3*, el 2020 es pot observar un augment significatiu en els pagaments, que podria apuntar a un efecte de la COVID-19, ja que moltes organitzacions haurien hagut de fer la transició ràpidament al teletreball, sovint sense la infraestructura de seguretat adequada. L'any 2022 es pot veure una disminució dels pagaments, segons *Chainalysis*, a causa del conflicte entre Rússia i Ucraïna, així com la infiltració del FBI al grup ransomware Hive, que hauria evitat pagaments significatius i reduït l'impacte global aquell any. El 2023, els pagaments dels rescats de ransomware van repuntar, continuant amb la tendència de creixement que ja es venia observant.

El ransomware ha evolucionat d'una amenaça menor a la indústria criminal lucrativa que coneixem avui en dia. Durant els primers 20 anys, aquests atacs sovint fracassaven en obtenir pagaments, ja que no es disposava de mètodes de pagament segurs. Tot i que es van intentar mètodes com les targetes de prepagament i les transferències bancàries, no va ser fins a l'aparició del bitcoin el 2009 que es va trobar una solució efectiva. La criptomoneda va oferir una manera segura i anònima de fer pagaments, la qual cosa va permetre als autors de ransomware augmentar l'amenaça i la seva eficàcia.

El 2013 C*ryptolocker*, uns dels primers ransomware a utilitzar bitcoin com a mètode de pagament, va atacar usuaris de Windows, aconseguint aproximadament 3 milions de dòlars en rescats [87]. A més, amb un sistema de xifratge robust com RSA de 2048 bits, *Cryptolocker* es va convertir en una amenaça seriosa. A diferència dels atacs anteriors, que sovint presentaven vulnerabilitats o es podien trencar amb força bruta, *Cryptolocker* va marcar un punt d'inflexió en la sofisticació del ransomware, utilitzant mètodes de xifratge que feien gairebé impossible la recuperació de dades sense la clau de desxifratge. El 2014, molts atacs ja utilitzaven un xifratge impenetrable sense el pagament del rescat, i això es va reflectir en un augment dels atacs, com es pot veure a la *Figura 5* [77].

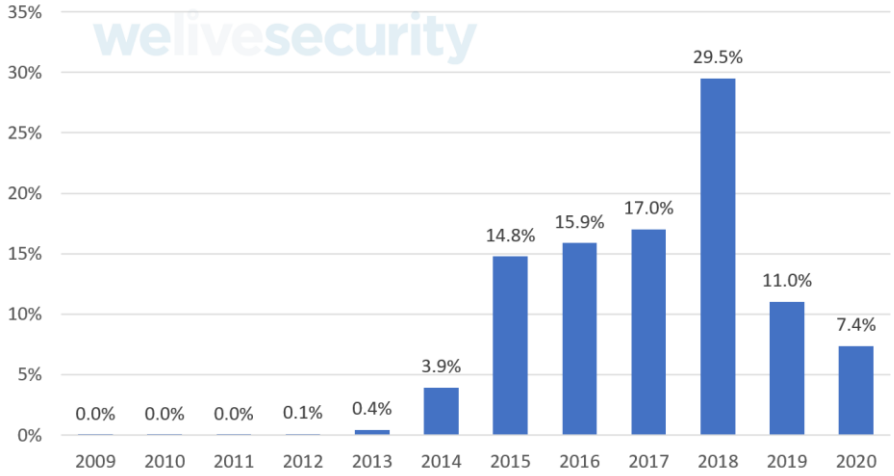

Figura 5. Deteccions de ransomware al món

A mesura que els mètodes de xifratge s'han anat sofisticant, també ho ha fet l'eficàcia del ransomware. Actualment, el xifratge és tan avançat que, en la majoria dels casos, l'única manera de recuperar les dades segrestades és pagant el rescat. Aquest èxit ha impulsat la creació de serveis de *Ransomware as a Service*, on ciberdelinqüents proporcionen les eines i serveis perquè altres delinqüents puguin dur a terme atacs de ransomware. *Cerber* és un dels primers exemples de *RaaS* i va ser responsable del 58% dels intents d'atac en l'àmbit de la salut durant la pandèmia de la COVID-19.

Els atacs s'han tornat més personalitzats i selectius. Això podria explicar la baixada d'atacs del 2019, ja que molts atacants prefereixen buscar grans víctimes i demanar rescats elevats enlloc de llançar atacs massius amb rescats petits. L'any 2018 *Ryuk* va atacar a organitzacions sanitàries, de fabricació i de tecnologies (EMCOR, hospitals UHS, SEPE) guanyant probablement 150 milions de dòlars a finals de 2020 [42]. *LockBit* buscava objectius valuosos, des del sector de la salut a les institucions financeres i del gener del 2022 fins al febrer del 2024 van aconseguir 144 milions de dòlars en rescats [lockbit3]. Conti va atacar a hospitals, escoles, serveis d'emergència, el Govern de Costa Rica i Peruvian [63], aconseguint 180 milions de dòlars el 2021 [63], i de gener a maig del 2022 més de 150 milions de dòlars [62].

El ransomware ha anat superant totes les dificultats que se li han presentat per aconseguir el seu objectiu: demanar rescats cada vegada més grans, fins al punt de ser selectius a l'hora de triar les víctimes. Els sectors més vulnerables a atcs de ransomware són aquells que treballen amb dades crítiques, que no poden permetre's interrupcions, com hospitals, sectors públics o empreses de fabricació.

Quan aquests atacs succeeixen, a més de voler recuperar les dades, les empreses volen evitar que aquestes es venguin o es difonguin. Les pèrdues econòmiques són considerables, tant pel cost de recuperar les dades com pels ingressos perduts durant el temps d'inactivitat. Moltes empreses prefereixen no fer públiques aquestes pèrdues, mentre que els sectors públics tenen l'obligació de comunicar-les, fet que podria fer semblar que són els més afectats, com es pot veure a la *Figura 6* [76].

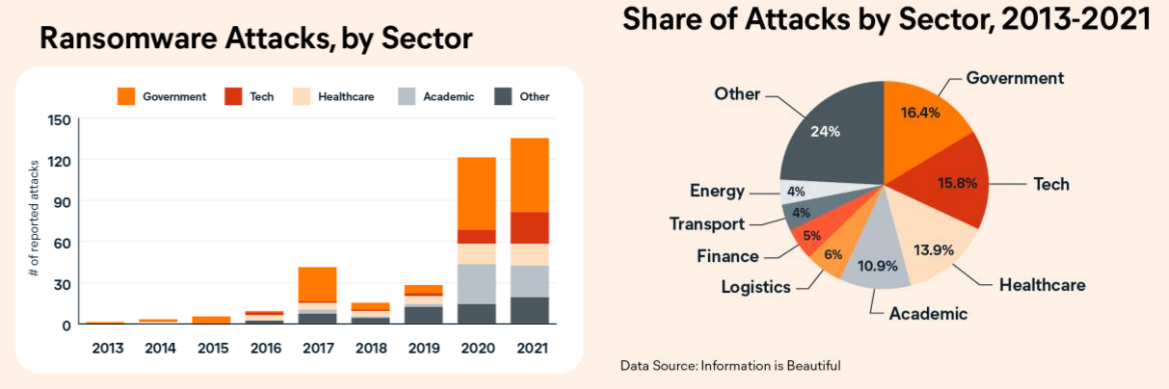

Figura 6. Atacs de ransomware per sector

A causa de l'impacte que suposa ser víctima d'un atac de ransomware, moltes empreses opten per no denunciar els fets. A la *Figura 7* [78] es pot observar un percentatge alt d'atacs no reportats. Tot i que el sector públic sembla ser el més afectat, això podria deure's a la seva obligació de reportar els atacs, mentre que en altres sectors no queda clar si es fa.

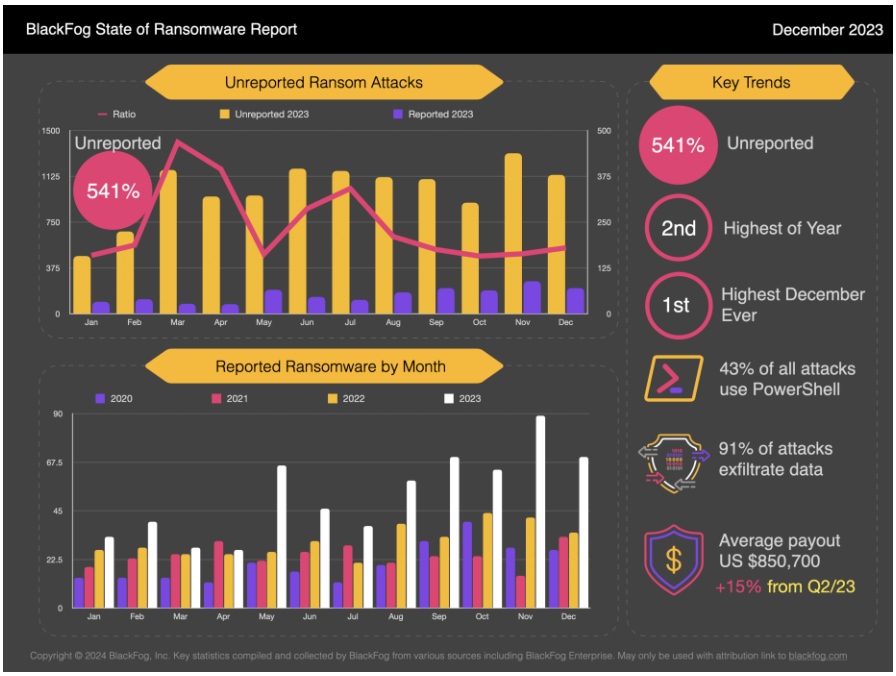

Figura 7. Informe de l'estat de ransomware

Donada la part oculta dels atacs, és difícil estimar quins són els sectors més afectats. Les assegurances i les empreses que gestionen aquestes incidències també tenen un paper important, però la manca de dades fiables dificulta una avaluació precisa. Els motius pels quals no es reporten els incidents poden incloure preocupacions sobre la reputació, possibles demandes legals, i altres factors. És crucial tenir en compte aquesta part oculta quan es fan estimacions o es presenten dades sobre els atacs.

5. Cicle de la seguretat

Per garantir la seguretat d'una empresa o entitat davant les creixents amenaces digitals, com el ransomware, és fonamental implantar el cicle de la seguretat. Aquest consta d'un conjunt de fases: i) estudi o avaluació de la seguretat; ii) prevenció/protecció; iii) monitoratge; iv) avaluació/verificació de les mesures implantades; v) resposta; vi) recuperació i; viii) estudi forense en cas d'atac.

5.1. Estudi o avaluació de seguretat

És essencial identificar i llistar tots els actius tecnològics, assignant-los valors o categories segons la seva importància, sensibilitat i criticitat per a l'empresa. Aquests actius poden incloure maquinari, programari, bases de dades, xarxes i qualsevol altre recurs tecnològic crític. Un cop identificats, cal dur a terme una avaluació detallada de les possibles amenaces i vulnerabilitats que poden afectar aquests actius. Aquesta avaluació ha d'incloure tant amenaces internes, com ara errors de configuració, negligència dels empleats o intents malintencionats des de dins de l'organització, com amenaces externes, com ara atacs de ransomware, *phishing* o robatoris.

5.2. Prevenció/Protecció

Per aconseguir una protecció eficaç, és essencial desenvolupar i implementar solucions per reduir l'abast als sitemes TI, garantint la confidencialitat, integritat, disponibilitat i audibilitat, i mantenint el rendiment de serveis informàtics essencials.

Entre les pràctiques recomanades per l'FBI per prevenir els atacs, s'inclouen la limitació dels privilegis d'usuari, la realització de còpies de seguretat regulars, la deshabilitació de macros i scripts de Java, l'establiment de polítiques de restricció de programari, i la formació dels empleats en la conscienciació sobre el ransomware [80]. Altres mesures de protecció inclouen l'ús de tallafocs, WAF, proxies, sistemes anti-spam, antivirus i el blindatge de xarxa.

És crucial mantenir les còpies offline per evitar que el ransomware les infecti. Els atacants xifren la informació, fent-la inaccessible. Per això, és essencial garantir que les còpies de seguretat no estiguin accessibles als atacants.

Per implementar aquesta protecció, es poden utilitzar dispositius físicament desconnectables, com ara discs durs externs. Les còpies de seguretat de dades crítiques s'han de fer regularment, i en entorns de treball dinàmics, és recomanable fer còpies diàries. A més, cal verificar regularment aquestes còpies per assegurar-se que es poden restaurar correctament i que no estan danyades. També és important fer còpies de seguretat completes del sistema, incloent-hi el sistema operatiu, aplicacions, configuració i scripts, per permetre una restauració ràpida en cas d'infecció.

La protecció d'aquests atacs també depèn del comportament dels usuaris, ja que molts no són conscients de les pràctiques segures a Internet. Segons CSO Online, els correus electrònics maliciosos són la principal via de propagació del ransomware, responsable del 92% de les infeccions [301]. Per exemple, el juny del 2019, Lake City va pagar 460.000 dòlars per un atac de Ryuk després que un treballador obrís un correu infectat [41].

5.3. Monitoratge

El monitoratge continu dels sistemes és essencial per detectar activitats sospitoses o no autoritzades que podrien indicar un intent d'incident de seguretat. Per garantir aquesta supervisió, és crucial instal·lar i configurar eines i sistemes específics com els sistemes de detecció d'intrusions (IDS) i els sistemes de prevenció d'intrusions (IPS).

Els IDS supervisen el trànsit de xarxa per identificar possibles activitats malicioses o vulneracions de polítiques de seguretat. Aquests sistemes analitzen el trànsit que es mou per la xarxa i emeten una alarma quan detecten un incident, ja sigui perquè reconeixen el patró d'un atac conegut o una anomalia en el comportament habitual de la xarxa. Així, els IDS permeten alertar els administradors de la xarxa en cas de qualsevol irregularitat.

Els IPS, en canvi, no només detecten activitats sospitoses, sinó que també prenen mesures immediates per bloquejar-les, prevenint automàticament la propagació d'una amenaça en bloquejar el trànsit maliciós. No obstant això, cal tenir en compte que, a vegades, els IPS poden intervenir en situacions que no són realment atacs, bloquejant trànsit legítim. Tot i aquest risc, els IPS són essencials per mantenir una vigilància constant i reaccionar ràpidament davant possibles amenaces.

5.4. Avaluació/Actualitzacions de seguretat de forma periòdica

Quan instal·les un programari, pot ser que amb el temps apareguin errors. Això és degut al fet que els sistemes evolucionen constantment, per la qual cosa és necessari mantenir-los actualitzats i tenir en compte les noves amenaces. El manteniment constant és essencial, així com assegurar-se que el monitoratge funcioni correctament.

Per protegir els usuaris d'atacs de ransomware, calen nous enfocaments de protecció que no només detectin el *malware*, sinó que també evitin que aquest causi danys des del principi. A mesura que sorgeixen noves amenaces, és crucial fer actualitzacions i correccions per garantir el bon funcionament de les mesures de seguretat. És important fer avaluacions periòdiques de seguretat [79] i implementar actualitzacions i pagats de seguretat regulars per als sistemes operatius i el programari, corregint així les vulnerabilitats que podrien ser explotades pels atacants.

Un exemple és el cas de *WannaCry*, que va afectar 230.000 ordinadors arreu del món. El Sistema Nacional de Salut del Regle Unit va ser greument afectat amb un cost estimat de 92 milions de lliures i 19.000 cites mèdiques cancel·lades. *WannaCry* va causar unes pèrdues globals de quatre mil milions de dòlars. Tot i que Microsoft va llançar un pedaç de seguretat abans de l'atac, molts usuaris no van actualitzar els seus sistemes, deixant-los vulnerables [77].

El recent atac de *Cl0p* ha posat de manifest la necessitat de control d'identitat i d'accés més estrictes en els sistemes empresarials i industrials per prevenir la propagació del *malware* [82]. L'ús d'eines de gestió de vulnerabilitats permet identificar i corregir forats de seguretat abans que puguin ser explotats, oferint una capa addicional de protecció. A més, és crucial dur a terme enquestes i investigacions actualitzades que aprofundeixin en la investigació existent sobre aquest tema, mantenir-se al dia amb les noves formes d'atacs i mesures de protecció efectives. Quan es produeix un atac, el CERT publica informació de les noves amenaces, que permet solucions de seguretat tan aviat com sigui possible.

5.5. Resposta

En cas d'un atac de ransomware, és crucial que les víctimes informin dels fets per estudiar les noves formes d'atac i proporcionar conscienciació a les persones de manera periòdica.

Com que la informació queda segrestada, una manera de recuperar-la es mitjançant còpies de seguretat. Una de les principals raons per les quals esdevens objectiu dels atacs de ransomware és la connexió de les còpies de seguretat als sistemes principals [8].

Quan es detecta un atac cal donar-hi una resposta immediata, la qual ha d'estar definida en un pla que permeti minimitzar els danys i resturar la seguretat. El primer pas és identificar l'atac i aïllar els sistemes afectats per evitar la propagació de la infecció. Després, és crucial identificar les dades compromeses i informar immediatament els usuaris afectats, proporcionant instruccions clares sobre les mesures a prendre. També és necessari informar a les autoritats pertinents sobre l'atac.

El procés de resposta ha de tenir en compte el cost versus el benefici de les accions preses, assegurant que es prenguin decisions que minimitzin l'impacte econòmic i operatiu per a l'organització. Una resposta ràpida i efectiva és crucial per restaurar la confiança i la funcionalitat dels sistemes de l'empresa després d'un incident de seguretat.

5.6. Recuperació (cas especial)

La recuperació després d'un incident de seguretat és una part fonamental per restaurar l'estat normal dels sistemes i assegurar la continuïtat del negoci. Aquest procés inclou la restauració dels serveis, la recuperació de les dades i la revisió dels sistemes per garantir que no quedin vulnerabilitats que puguin ser explotades novament.

En primer lloc, un cop l'incident ha estat contingut, és vital treballar per restablir els serveis essencials. Això pot implicar la reinstal·lació de sistemes operatius, aplicacions i la configuració de xarxes per assegurar-se que els sistemes afectats funcionin correctament sense el *malware*. L'entorn on es fa la restauració ha de ser net, només així s'hi pot restaurar la informació. En paral·lel, la recuperació de les dades és un aspecte crucial, especialment si aquestes han estat danyades o eliminades. Després de la recuperació, es duu a terme una revisió completa per identificar les vulnerabilitats explotades durant l'atac, amb l'objectiu d'actualitzar les mesures de seguretat i garantir que els sistemes estan protegits contra futurs incidents.

Quan es tracta d'un atac de ransomware, la recuperació és especialment complexa i requereix un enfocament específic. El ransomware utilitza xifratge avançat que, en molts casos, és considerat segur per les tecnologies actuals, cosa que fa molt difícil desxifrar les dades sense la clau proporcionada pels atacants. En aquesta situació, l'organització es troba davant de dues opcions principals.

5.6.1. Còpies de seguretat (i configuració del sistema)

La primera i millor opció és disposar de còpies de seguretat actualitzades. Si es tenen, la restauració de dades es pot fer a partir d'aquestes, evitant així altres mètodes.

En l'atac de ransomware SamSam a Hancock el 2018, les còpies de seguretat van jugar un paper crucial en la recuperació dels sistemes afectats. Després de l'atac, Hancock Health va decidir no pagar el rescat, ja que experts van determinar que els fitxers encriptats es podien recuperar a partir de les còpies de seguretat existents. Tot i això, els costos de recuperació es van estimar en 55.000 dòlars. De manera similar, en l'atac de ransomware *Clop* que va afectar a ExecuPharm el 2020, les còpies de seguretat també van ser essencials per la recuperació dels sistemes. Tot i que van decidir no pagar el rescat, això va resultar en retards en els enviaments per als clients fabricants de medicaments [8].

5.6.2. Pagament

Quan no es tenen còpies de seguretat hi ha una altra opció, si no ho volem perdre tot; pagar el rescat demanat pels atacants. Considerar el pagament del rescat és una decisió crítica que planteja dilemes legals i ètics. Per a sectors crítics com la salut, on l'accés a les dades és vital, pagar el rescat pot evitar la interrupció de serveis essencials. Tot i que pot ser la forma més ràpida de recuperar les dades i menys costosa que altres opcions [81] a curt termini, i potser l'única de recuperar la totalitat d'aquestes [79], també comporta diversos riscos i implicacions.

No obstant això, pagar el rescat incentiva els cibercriminals a continuar amb aquests atacs, ja que veuen que és una manera efectiva de guanyar diners. A més no hi ha garanties que es recuperin les dades un cop s'hagi pagat el rescat, i hi ha el risc de convertir-se en objectius més atractius per a futurs atacs, perquè els criminals saben que estan disposats a pagar [81].

La legalitat del pagament d'un rescat depèn del país i la legislació vigent. En alguns casos, pot ser il·legal, especialment si el pagament es fa a grups vinculats a activitats terroristes o sancionats per les autoritats. A més, l'ètica del pagament és un debat obert. Pagar el rescat pot semblar una solució ràpida, però pot tenir conseqüències negatives a llarg termini, com encoratjar futurs atacs i finançar activitats il·lícites [83].

Les asseguradores poden tenir un paper important en aquest context, ajudant a negociar el rescat, que sovint varia en funció de la víctima. Un cop més, entra el joc el tema legal d'aquesta acció [84].

Cadascú ha de prendre la decisió que consideri millor en funció de les circumstàncies, però és fonamental destacar la importància de la prevenció i les còpies de seguretat com a estratègies clau per evitar haver de considerar opcions tan comprometedores com el pagament del rescat.

5.7. Auditoria forense

L'objectiu principal de l'auditoria forense després d'un atac de ciberseguretat, especialment en casos de ransomware, és recuperar-se de l'incident, minimitzant les pèrdues econòmiques i de reputació. Aquesta auditoria esdevé un pas fonamental per comprendre l'abast de l'atac, identificar les vulnerabilitats explotades i implementar mesures per prevenir futurs incidents [86].

Durant l'auditoria forense, es reconstrueix la seqüència dels fets per descobrir com l'atacant va accedir al sistema, quines accions malicioses va dur a terme i quines dades o sistemes van ser compromesos. Aquest procés inclou una anàlisi detallada de l'atac, l'avaluació dels sistemes afectats i la detecció de qualsevol presència residual de malware, garantint així una recuperació completa i segura.

Les asseguradores juguen un paper clau en aquest procés. Donada la proliferació dels atacs cibernètics, moltes asseguradores ofereixen compensacions a les empreses afectades, però sovint requereixen una auditoria forense prèvia per avaluar l'estat de seguretat de l'empresa abans i després de l'atac. Això assegura que l'empresa compleixi amb els estàndards de seguretat necessaris per ser assegurada i per garantir una resposta efectiva en futurs incidents [85].

6. Conclusions

L'impacte del ransomware ha revelat un panorama en constant evolució, amb tècniques i estratègies que s'han perfeccionat al llarg dels anys. Inicialment, els ransomware eren rudimentaris i utilitzaven mètodes de xifratge simples. Amb el temps, però, han evolucionat cap a formes més sofisticades i perilloses. La introducció de criptomonedes com el bitcoin ha permès als atacants operar amb menys risc de ser rastrejats, mentre que els avanços en el xifratge, com els sistemes híbrids de xifratge simètric i asimètric (AES i RSA), han complicat la recuperació de les dades sense pagar el rescat.

Les tècniques d'extorsió també s'han sofisticat, amb la incorporació de mètodes com l'eliminació de còpies de seguretat i la doble extorsió. En aquest darrer cas, els atacants no només xifren les dades, sinó que també les roben i amenacen amb la seva divulgació si no es paga el rescat. A més, el model de negoci conegut com Ransomware-as-a-Service (RaaS) ha democratitzat l'accés a les eines de ransomware, permetent a atacants amb poc coneixement tècnic llançar atacs efectius utilitzant tècniques desenvolupades per grups més sofisticats.

Aquesta evolució en les tècniques de ransomware ha incrementat l'abast i l'eficàcia dels atacs, amb un enfocament particular en empreses grans i sectors crítics com la salut i els serveis públics, que són objectius freqüents a causa de la seva rellevància i les dades sensibles que gestionen. Els atacs a aquests sectors no només són més lucratius, sinó que també exerceixen una pressió addicional sobre les víctimes.

Per protegir-se contra aquests atacs, és essencial seguir un cicle de seguretat rigorós. Aquest cicle inclou la formació del personal i la realització de còpies de seguretat regulars. La formació ha de centrar-se en educar els empleats sobre els perills del ransomware i com identificar intents d'enginyeria social, establint polítiques clares sobre l'ús segur de la tecnologia.

En conclusió, el ransomware s'ha convertit en un negoci altament lucratiu i en constant evolució. Els avenços en tècniques de xifratge, mètodes de pagament anònims i estratègies d'extorsió han augmentat la seva efectivitat i impacte econòmic. La clau per afrontar aquesta amenaça radica en la preparació i la implementació de pràctiques de seguretat eficients, juntament amb una vigilància constant davant els nous mètodes d'atac.

6.1. Treball futur

Si hagués pogut dedicar més temps a aquest treball hagués aprofundit en aspectes que he anat veient fonamentals per al futur. En particular, hagués pogut realitzar una enquesta a diverses empreses per conèixer de primera mà les seves necessitats i expectatives en relació amb els serveis de *backup*. A més, m'hagués agradat analitzar amb més detall els diferents serveis de *backup* disponibles al mercat per identificar els més adequats segons diferents tipus d'empreses. Finalment, considero que un estudi econòmic més detallat hauria estat molt útil per comparar els costos i beneficis de cada opció, oferint així una visió més completa i informada per a la presa de decisions.

Referències

[1] Les tecnologies de l'aprenentatge i el coneixement (TAC), Institut Obert de Catalunya. https://ioc.xtec.cat/materials/FP/Recursos/fp_edi_m05_/web/fp_edi_m05_htmlindex/WebContent/u5/a1/continguts.html

[2] Internet of Things (IoT) security dataset evolution: Challenges and future directions. Barjinder Kaur,Sajjad Dadkhah, Farzaneh Shoeleh,Euclides Carlos Pinto Neto,Pulei Xiong,Shahrear Iqbal,Philippe Lamontagne, Suprio Ray,Ali A. Ghorbani. Internet of Things, Volume 22, July 2023, 100780. Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S2542660523001038

[3] Max Beckett, "History of the internet: A timeline throughout the years", Uswitch, gener 2024. https://www.uswitch.com/broadband/guides/broadband-history/

[4] Internet of things and ransomware: Evolution, mitigation and prevention. Mamoona Humayun,NZ Jhanjhi,Ahmed Alsayat, Vasaki Ponnusamy. Egyptian Informatics Journal, Volume 22, Issue 1, March 2021, Pages 105-117. Elsevier. https://www.sciencedirect.com/science/article/pii/S1110866520301304

[5] Mathew J. Schwartz, "9 Ransomware Trends: More Leaks, Higher Ransom Payments", Bank Info Security, febrer 2022) https://www.bankinfosecurity.com/9-ransomware-trends-more-leaks-higher-ransom-payments-a-18519

[6] A study of the relationship of malware detection mechanisms using Artificial Intelligence. Jihyeon Song, Sunoh Choi, Jungtae Kim, Kyungmin Park, Cheolhee Park, Jonghyun Kim, Ikkyun Kim. ICT Express, Volume 10, Issue 3, June 2024, Pages 632-649. Elsevier. https://www.sciencedirect.com/science/article/pii/S2405959524000298

[7] Kurt Baker, "What Is Malware", Crowdstrike, abril 2023. https://www.crowdstrike.com/cybersecurity-101/malware/

[8] Marlese Lessing, "Case Study: AIDS Trojan Ransomware", sdxcentral, març 2024. https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-aids-trojan-ransomware/

[9] Marcos Merina, "Qué es un archivo BAT y cómo (y para qué) puedes crear uno tú mismo en pocos pasos", Genbeta,setembre 2021. https://www.genbeta.com/windows/que-archivo-bat-como-puedes-crear-uno-tu-pocos-pasos

[10] "AIDS Trojan Ransomware", WatchGuard. https://www.watchguard.com/wgrd-ransomware/aids-trojan

[11] Aleks Gostev, "Blackmailer: The Story of GPCode", Securelist, juny 2006. https://securelist.com/blackmailer-the-story-of-gpcode/36089/

[12] R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (Feb. 1978), 120–126. https://doi.org/10.1145/359340.359342

[13] Aleks Gostev, "GPCode: The Return of the File Encryptor", Securelist, juny 2008. https://securelist.com/gpcode-the-return-of-the-file-encryptor/30423/

[14] (National Institute of Standards and Techonology (NIST), Advanced Encryption Standard (AES), FIPS Publication, 2001, FIPS PUB 197, 51 pàgines). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[15] Aleks Gostev, “GPCode-Like Ransomware Is Back”, Securelist, novembre 2010. https://securelist.com/gpcode-like-ransomware-is-back/29633/

[16] Aleks Gostev, “GPCode Strikes Back”, Securelist, març 2011. https://securelist.com/ransomware-gpcode-strikes-back/29784/

[17] Julie Pinkerton, “The History of Bitcoin”, U.S.News & World Report, març 2024 https://money.usnews.com/investing/articles/the-history-of-bitcoin

[18] Oliver, J., Cheng, S., Manly, L., Zhu, J., Paz, R. D., Sioting, S., & Leopando, J. (2012). Blackhole Exploit Kit: A Spam Campaign. *Not a Series of Individual Spam Runs*, *10*, 17.

[19] “The Reveton ransomware, ”CERT-IST, febrer 2013. https://www.cert-ist.com/public/en/SO_detail?code=201301_article

[20] “Reveton Worm”, KnowBe4. https://www.knowbe4.com/reveton-worm

[21] National Institute of Standards and Technology. Phishing, Created October 22, 2021, Updated March 14, 2024. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

[22] Michael Buckbee, “CryptoLocker: Everything You Need to Know”, Varions, maig 2023. https://www.varonis.com/blog/cryptolocker

[23] “CryptoWall Ransomware”, Proofpoint. https://www.proofpoint.com/es/threat-reference/cryptowall-ransomware

[24] “TorrentLocker”, Kaspersky. https://www.kaspersky.com/resource-center/threats/torrentlocker-malware

[25] Marc-Etienne M.Léveillé, “TorrentLocker. Ransomware in a country near you”, Eset, desembre 2014. https://web-assets.esetstatic.com/wls/2014/12/torrent_locker.pdf

[26] “TorrentLocker”, KnowBe4. https://www.knowbe4.com/torrentlocker

[27] Sayaala, “All about SamSam Ransomware”, Infosec, juliol 2018. https://www.infosecinstitute.com/resources/threat-intelligence/all-about-samsam-ransomware/

[28] “What is SamSam Ransomware”, Nomios. https://www.nomios.com/resources/what-is-samsam-ransomware/

[29] “What is a Botnet?”, Akamai. https://www.akamai.com/es/glossary/what-is-a-botnet

[30] “¿Qué es una macro?”, Ingenio 2010, abril 2020. https://www.ingenio2010.es/que-es-una-macro/

[31] “Red Tor: qué es, cómo funciona y cómo se usa”, Xataka, juny 2021. https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

[32] Laura Klusaitė, “What is Locky ransomware, and hoy do you prevent it?”, NordVPN,maig 2023. https://nordvpn.com/blog/locky-ransomware/

[33] “Ransomware as a Service”, IBM, agost 2024. https://www.ibm.com/topics/ransomware-as-a-service

[34] “Cerber Ransomware”, Proofpoint. https://www.proofpoint.com/us/threat-reference/cerber-ransomware

[35] “Ransomware Cerber en el panorama de amenazas nacional”, Entel Digital, març 2021. https://portal.cci-entel.cl/Threat_Intelligence/Boletines/839/

[36] Malcolm Higgins, “EternalBlue: What it is and how it works”, NordVPN, abril 2023. https://nordvpn.com/blog/what-is-eternalblue/

[37] “Qué es un Payload”, OpenWebinars, octubre 2018. https://openwebinars.net/blog/que-es-payload/

[38] “Petya Ransomware: History, M.O., Targets”, Heimdal Security. https://heimdalsecurity.com/blog/petya-ransomware-history-m-o-targets/

[39] “Ransomware Petya: A Technical Review”, G DATA Software, març 2016. https://www.gdatasoftware.com/blog/2016/03/28226-ransomware-petya-a-technical-review

[40] “Petya Ransomware”, CISA, juliol 2017. https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

[41] “WannaCry Ransomware”, Kaspersky. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[42] “Wcry Ransomware Analysis”, Secureworks. https://www.secureworks.com/research/wcry-ransomware-analysis

[43] “Ransomware Variants: BitPaymer, DoppelPaymer”, Cyber NJ. https://www.cyber.nj.gov/threat-landscape/ransomware/ransomware-variants/bit-paymer-doppelpaymer

[44] “BitPaymer Ransomware Removal Guide”, PCRisk. https://www.pcrisk.com/removal-guides/12859-bitpaymer-ransomware

[45] Ravikant Tiwari, “Evolution of GandCrab Ransomware”, Acronis, agost 2018. https://www.acronis.com/en-us/blog/posts/gandcrab/

[46] Hardik Manocha, “Ryuk Ransomware Simulation: MITRE TTP", FourCore, agost 2022. ttps://fourcore.io/blogs/ryuk-ransomware-simulation-mitre-ttp

[47] “What is Ryuk Ransomware?”, Trend Micro. https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

[48] “Ryuk Ransomware”, SentinelOne. https://www.sentinelone.com/cybersecurity-101/ryuk-ransomware/

[49] “The Sodinokibi Ransomware Attack”, Cybereason. https://www.cybereason.com/blog/research/the-sodinokibi-ransomware-attack

[50] “REvil (Sodinokibi) Ransomware”, Secureworks. https://www.secureworks.com/research/revil-sodinokibi-ransomware

[51] “Maze Ransomware”, Securelist. https://securelist.com/maze-ransomware/99137/

[52] “Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella”, Xataka, maig 2024. https://www.xataka.com/basics/que-dark-web-que-se-diferencia-deep-web-como-puedes-navegar-ella

[53] “What is Maze Ransomware?”, Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

[54] Ahona Rudra, “Understanding Clop Ransomware”, PowerDMARC, abril 2024. https://powerdmarc.com/understanding-clop-ransomware/

[55] “Clop Ransomware”, SentinelOne https://www.sentinelone.com/anthology/clop/

[56] Omer Solomon, “Netwalker Ransomware Report”, Cynet. https://www.cynet.com/attack-techniques-hands-on/netwalker-ransomware-report/

[57] Alex Tray, “Netwalker Ransomware: Everything You Need to Know to Stay Safe”, HackerNoon, desembre 2022. https://hackernoon.com/netwalker-ransomware-everything-you-need-to-know-to-stay-safe

[58] Edward Kost, “What is Netwalker Ransomware?”, UpGuard, novembre 2023. https://www.upguard.com/blog/what-is-netwalker-ransomware

[59] “LockBit Ransomware”, Kaspersky. https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

[60] “Technical Analysis of LockBit Ransomware: Understanding the Mechanics”, Medium, maig 2024. https://medium.com/@iamautorobert/technical-analysis-of-lockbit-ransomware-understanding-the-mechanics-bb1efa928256

[61] “Reward for Information: LockBit Ransomware as a Service”, U.S. Department of State, febrer 2024. https://www.state.gov/reward-for-information-lockbit-ransomware-as-a-service/

[62] “Reward for Information: Owners, Operators, and Affiliates of the Conti Ransomware as a Service (RaaS)”, U.S. Department of State, maig 2022. https://www.state.gov/reward-for-information-owners-operators-affiliates-of-the-conti-ransomware-as-a-service-raas/

[63] “What is Conti Ransomware?”, Heimdal Security, març 2024. https://heimdalsecurity.com/blog/what-is-conti-ransomware/

[64] “Conti Ransomware Technical Breakdown”, StoneFly. https://stonefly.com/blog/conti-ransomware-technical-breakdown/

[65] “DarkSide Ransomware Analysis Report”, Brande Defense, gener 2023. https://brandefense.io/wp-content/uploads/2023/01/DarkSide-Ransomware-Analysis-Report.pdf

[66] “Egregor Ransomware”, Forescout, gener 2021. https://www.forescout.com/resources/egregor-ransomware/

[67] “Egregor Ransomware”, Heimdal Security, agost 2023. https://heimdalsecurity.com/blog/egregor-ransomware/

[68] “Cybereason vs. Egregor Ransomware”, Cybereason. https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware

[69] Nadav Ovadia, “Hive Ransomware Analysis”, Varonis, febrer 2023. https://www.varonis.com/blog/hive-ransomware-analysis

[70] “What is Hive Ransomware?”, Heimdal Security, octubre 2023. https://heimdalsecurity.com/blog/what-is-hive-ransomware/

[71] “La historia de BlackCat: el grupo de ciberatacantes que secuestraba datos en todo el mundo”, Infobae, desembre 2023. https://www.infobae.com/tecno/2023/12/20/la-historia-de-blackcat-el-grupo-de-ciberatacantes-que-secuestraba-datos-en-todo-el-mundo/

[72] “Royal Ransomware Protection”, BlackBerry. https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/royal-ransomware

[73] “The Hidden Costs of Ransomware Attacks”, SpyCloud. https://spycloud.com/blog/the-hidden-costs-of-ransomware-attacks/

[74] “Crypto Ransomware Revenue Down as Victims Refuse to Pay”, Chainalysis. https://www.chainalysis.com/blog/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[75] “Ransomware 2024”, Chainalysis. https://www.chainalysis.com/blog/ransomware-2024/

[76] “Biggest Ransomware Attacks in History”, Avast. https://www.avast.com/c-biggest-ransomware-attacks

[77] “WannaCry: Cómo evolucionó en la escena del ransomware”, WeLiveSecurity (ESET), maig 2021. https://www.welivesecurity.com/la-es/2021/05/12/wannacry-como-evoluciono-escena-ransomware/

[78] “The State of Ransomware in 2023”, BlackFog. https://www.blackfog.com/the-state-of-ransomware-in-2023/

[79] Bander Ali Saleh Al-Rimy, Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid, “Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions”, Computers & Security, Elsevier, maig 2018. https://www.sciencedirect.com/science/article/abs/pii/S016740481830004X

[80] Mamoona Humayun, NZ Jhanjhi, Ahmed Alsayat, Vasaki Ponnusamy, “Internet of Things and Ransomware: Evolution, Mitigation and Prevention”, Egyptian Informatics Journal, Elsevier, març 2021. https://www.sciencedirect.com/science/article/pii/S1110866520301304

[81] Cath Everett, “Ransomware: to pay or not to pay?”, Computer Fraud & Security, Elsevier, abril 2016. https://www.sciencedirect.com/science/article/abs/pii/S1361372316300367

[82] Mourad Benmalek, “Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges”, Internet of Things and Cyber-Physical Systems, Elsevier, 2024. https://www.sciencedirect.com/science/article/pii/S2667345223000561

[83] “What Are the Legal Implications of Paying Ransomware Demands?”, HackerNoon, octubre 2023. https://hackernoon.com/what-are-the-legal-implications-of-paying-ransomware-demands

[84] “¿Deben las aseguradoras pagar el rescate por los ataques de ransomware a sus clientes?”, Seguros News, setembre 2022 https://segurosnews.com/news/deben-las-aseguradoras-pagar-el-rescate-por-los-ataques-de-ransomware-a-sus-clientes

[85] “Pesadilla Ransomware: Análisis Forense y Estrategias de Mitigación”, CyberProtegidos. https://cyberprotegidos.info/analisis-forense/pesadilla-ransomware-analisis-forense-estrategias-mitigacion/

[86] Sergio Agruña Álvarez, “Análisis de la Evolución del Ransomware y su Impacto en las PYMES”, Dipòsit Digital de la Universitat de Barcelona. https://diposit.ub.edu/dspace/bitstream/2445/182840/2/tfg_sergio_agru%C3%B1a_alvarez.pdf

[87] “11 Biggest Ransomware Attacks in History”, Cobalt.io. https://www.cobalt.io/blog/11-biggest-ransomware-attacks-in-history