Centre universitari adscrit a la

Universitat Pompeu Fabra Barcelona

Doble Grau en Informàtica de Gestió i Sistemes d'Informació/ Grau en Disseny i Producció de Vídeojocs

Seguretat Cibernètica en els Videojocs: Amenaces i Defenses del sector

Memòria

MARC BADAL BATLLORI

PROFESSOR: JAUME TEODORO SADURNÍ

TecnoCampus

Agraïments

Vull agrair al meu professor Jaume Teodoro per el seu coneixement i guiatge durant totes les etapes del treball.

Agrair a la meva família per la seva paciència i confiança amb mi.

Abstract

This thesis examines the cybersecurity landscape in the video game industry, focusing on attack trends and corresponding defense mechanisms. Analyzes various cyber threats, such as DDoS attacks, phishing and ransomware, among others. The research aims to provide a concise overview of the current state of cybersecurity in this growing industry and provide developers with insight into existing defense resources.

Resum

Aquest treball examina el panorama de la ciberseguretat en la indústria dels videojocs, centrant-se en les tendències d'atacs i els mecanismes de defensa corresponents. Analitza diverses amenaces cibernètiques, com ara els atacs DDoS, phishing i ransomware, entre d'altres. La investigació pretén proporcionar una visió concisa de l'estat actual de la ciberseguretat en aquesta indústria en creixement i oferir coneixement als desenvolupadors sobre els recursos de defensa existents.

Resumen

Este trabajo examina el panorama de la ciberseguridad en la industria de los videojuegos, centrándose en las tendencias de ataques y los mecanismos de defensa correspondientes. Analiza diversas amenazas cibernéticas, como los ataques DDoS, phishing y ransomware, entre otros. La investigación pretende proporcionar una visión concisa del estado actual de la ciberseguridad en esta industria en crecimiento y ofrecer conocimiento a los desarrolladores sobre los recursos de defensa existentes.

Índex

Índex de figures

Índex de taules

Glossari de termes

WI-FI *Wireless Fidelity:* Tecnologia que permet la connexió sense fils d'ordinadors, telèfons i altres dispositius a internet. S'utilitza en àmbits domèstics, laborals i públics per proporcionar accés a la xarxa.

TLS *Transport Layer Security*: Protocol de seguretat que encripta les dades enviades sobre internet, garantint privacitat i integritat en les comunicacions entre dispositius.

HTTP *HyperText Transfer Protocol*: Protocol que Facilita la comunicació entre navegadors web i servidors web, permetent l'intercanvi i la visualització de pàgines web

HTTPS *HyperText Transfer Protocol Secure*: Extensió de HTTP que afegeix seguretat a les comunicacions mitjançant encriptació.

IoT *Internet of Things*: Xarxa de dispositius físics que disposen de sensors, programari i altres tecnologies amb l'objectiu de connectar i intercanviar dades amb altres dispositius i sistemes a través d'internet.

EULA *End User License Agreement*: Contracte legal entre el proveïdor d'un programari o aplicació i l'usuari final, que estableix els termes i condicions sota els quals l'usuari pot utilitzar el programari.

MMORPG *Massively Multiplayer Online Role-Playing Game*: Gènere de videojocs que permet a un gran nombre de jugadors interactuar dins d'un món virtual persistent combinant elements de rol.

SGSI *Sistema de Gestió de la Seguretat de la Informació:* Conjunt de polítiques, processos i sistemes per gestionar els riscos de seguretat de la informació d'una organització.

GDPR *General Data Protection Regulation*: Marc legal de la Unió Europea que estableix les directrius per a la recollida, el processament i la protecció de les dades personals dels individus dins de la UE.

EXPLOITS Ús d'errors en el sistema del videojoc per obtenir avantatges o inesperats.

1. Introducció

La indústria dels videojocs és un clar exemple de la innovació i l'auge del sector de l'entreteniment. No obstant això, amb el ràpid creixement del mercat, que ha assolit ingressos globals de 242.52 bilions de dòlars en l'any 2023 segons la firma Precedence Research (2023), la indústria s'ha convertit en un objectiu creixent per els ciberdelinqüents, una preocupació que aquest Treball Fi de Grau (TFG), pretén abordar.

La recerca s'endinsa en l'exploració de l'Estat de l'Art i les tendències predominants en ciberseguretat dins l'àmbit dels videojocs, incidint en la identificació de vectors d'atacs i vulnerabilitats emergents. Aquest estudi pretén proporcionar el coneixement sobre les pràctiques de seguretat utilitzades actualment, així com les tecnologies més avançades que estan sent implementades per protegir tant els jugadors com les plataformes de joc.

La selecció d'aquest tema deriva de la seva crucial rellevància i el seu profund impacte global. Les ciberamenaces en la indústria dels videojocs no solament afecten la privacitat de dades i la confiança del consumidor, sinó que també posen en risc la pròpia estabilitat financera de les empreses.

Amb aquesta investigació, es busca proporcionar coneixement sobre l'estat actual de la ciberseguretat en la indústria dels videojocs, així com conscienciar sobre la importància d'aquest aspecte.

Aquesta investigació es destina als professionals de la indústria, acadèmics i als propis jugadors de videojocs.

2. Objectius

L'objectiu principal d'aquest Treball de Fi de Grau (TFG) és estudiar les amenaces actuals que afecten a la indústria dels videojocs i analitzar els recursos de defensa disponibles per minimitzar-les. El TFG està estructurat per delimitar els objectius principals i secundaris, garantint que l'abast de la recerca estigui ben definit i centrat a contribuir a la comprensió acadèmica de la ciberseguretat en el context de la indústria.

2.1 Objectius Principals

- **Analitzar les tendències d'atac a la Indústria dels Videojocs:** Identificar i examinar les diferents tècniques i mètodes d'atac que estan sent utilitzats actualment per comprometre la seguretat de la indústria.

- **Exposar els mecanismes de defensa disponibles per minimitzar l'impacte:** Identificar i descriure les diferents estratègies i tecnologies de ciberseguretat que s'utilitzen actualment per protegir les empreses de la indústria, els seus jugadors i els videojocs.

2.2 Objectius Secundaris

- **Proposar un model per impulsar i adoptar una cultura de ciberseguretat en les empreses de la indústria**: Proposar un model que ajudi les empreses de videojocs a adoptar una mentalitat cibersegura en qualsevol procés que es desenvolupi a l'empresa.

- **Crear un model per ajudar a les empreses a gestionar les vulnerabilitats dels seus sistemes:** Proposar i desenvolupar una eina per ajudar a les empreses de videojocs a gestionar les seves vulnerabilitats de manera més eficient, personalitzada i proactiva.

- **Exposar incidents representatius de la indústria**: Identificar casos reals d'incidents de ciberseguretat dins de la indústria dels videojocs.

3. Antecedents de la recerca

La ciberseguretat a la indústria dels videojocs ha experimentat canvis significatius al llarg dels anys, degut als avenços tecnològics de la indústria i la dinàmica d'un mercat amb canvis constants. A principis dels anys 2000, tal com van observar Jianxin i Hyun-Jin a l'estudi titulat Security issues in online games (2002) comenten que van estar marcats per el naixement de les necessitats de ciberseguretat a les empreses de desenvolupament de videojocs. Tot i que en l'estudi emfatitzen que l'enfocament predominant seguia en la producció sistemàtica i en el desenvolupament continu de videojocs, respecte l'adopció de mesures de seguretat sòlides. Aquesta tendència, neix del ràpid creixement i la competència de la indústria, que va causar que la seguretat acabés sent una necessitat secundaria, eclipsada per la urgència de llançar nous títols.

Els autors comenten que aquesta visió centrada en la producció, va propiciar l'augment d'atacs i va fer que les amenaces no només acabessin afectant a les empreses, sinó que també tinguessin un impacte directe en els usuaris finals: els jugadors. Les repercussions d'aquest enfocament s'han fet cada cop més evidents amb el temps. Les empreses que abans ignoraven la ciberseguretat ara s'enfronten a amenaces cibernètiques sofisticades que es dirigeixen tant a la seva infraestructura operativa com a la seva base d'usuaris.

Més enllà d'aquestes tendències, Davis i Price en l'article d'investigació de Computer Law & Security Review (2008) van emfatitzar la importància d'integrar estratègies de seguretat proactives en el procés de desenvolupament de videojocs. Comenten el concepte "d'enfocament per capes", on les consideracions de seguretat estan establertes des de l'inici del cicle de vida del desenvolupament. Tanmateix, com indiquen a la seva investigació, aquest enfocament no es va adoptar àmpliament a la indústria. Moltes empreses van continuar prioritzant la velocitat i la innovació per sobre de la seguretat, sovint a causa dels recursos limitats, la manca de competència en ciberseguretat o la simple reticència.

Shaofang, Mazaher i Stewart en la seva investigació (2019) assenyalen els riscos associats a prioritzar la velocitat sobre la seguretat, i afirmen que aquest enfocament pot provocar vulnerabilitats, fent els videojocs susceptibles a atacs.

La indústria, coneguda per la seva creativitat i innovació, de vegades veu els projectes més com a art que com a negoci. Aquesta perspectiva, tot i que fomenta la creativitat, de vegades pot limitar l'atenció a aspectes com la seguretat. Shaofang, Mazaher i Stewart suggereixen que perquè una indústria avanci de manera segura, cal que hi hagi un canvi de mentalitat on la seguretat es consideri com una part integral del procés creatiu i de desenvolupament, no com un obstacle o una idea poc important.

En l'estudi de Politowski, Petrillo, Ullmann i Guéhéneuc (2021) expliquen com els estudis de desenvolupament perceben, reaccionen i gestionen els riscs de ciberseguretat. Aquest estudi destaca que, tot i que els jugadors sovint són les víctimes visibles dels atacs, els mateixos estudis de desenvolupament s'enfronten a una infinitat de problemes per implementar mesures efectives de ciberseguretat.

4. Marc Teòric

4.1 Fonaments de la ciberseguretat

La ciberseguretat recau en la protecció del anomenat ciberespai, que s'utilitza no només per a la comunicació a Internet, sinó també per donar suport als diferents sistemes d'informació de les nostres infraestructura i serveis.

El ciberespai es pot conceptualitzar com un model multicapa. La capa física com cables, satèl·lits i encaminadors. La capa lògica, que inclou el programari com ara aplicacions per mòbils, sistemes operatius i navegadors web, que permeten el funcionament i la interacció de la xarxa física i La capa social que està formada per les persones que dissenyen, manipulen i interactuen amb aquests components digitals. Aquestes capes formen col·lectivament el ciberespai en què depèn cada cop més la societat, especialment per a sectors d'infraestructures crítiques com l'energia, el transport, l'alimentació, la salut, finances i els videojocs. (Upson, 2023)

La connectivitat, evidenciada pel fet que gairebé el 66,2% de la població mundial està connectada a Internet, crea un efecte que amplifica el valor i la utilitat de les connexions digitals que s'estenen més enllà dels dispositius personals, com sensors integrats en diversos entorns, des de cotxes fins a edificis (Fraguela, 2024).

Aquesta complexa xarxa de connectivitat fa que el món modern depengui molt de les tecnologies digitals. Des de facilitar la majoria de les comunicacions digitals fins a recolzar sectors d'infraestructures crítiques, Internet s'ha convertit en el sistema nerviós central del món. Tanmateix, aquesta dependència també obre vies per a les amenaces, fent de la ciberseguretat una preocupació primordial per als qui prenen decisions.

La ciberseguretat té com a objectiu protegir la confidencialitat, la integritat i la disponibilitat de la informació, una tasca difícil que les indústries han de comprendre.

4.1.1 Evolució de les normatives de ciberseguretat

L'evolució de les normatives de ciberseguretat s'han caracteritzat per diverses fases, cadascuna marcada per diferents tendències i desenvolupaments. Aquesta

evolució explorada en l'estudi de B. Madnick, Huang i S.Madnick (2023) es destaquen en tres fases principals:

Fase 1: Fase Inicial (2005-2012)

En la fase inicial, les normatives de ciberseguretat encara es trobaven en una etapa inicial, amb implementacions experimentals. Aquest període va establir el to de la futura implementació de normes de ciberseguretat. El GGE (Grup d'experts governamentals de les Nacions Unides) va tenir un paper fonamental durant aquest temps, guanyant protagonisme en els debats internacionals sobre normes de ciberseguretat. Les normes discutides eren genèriques, posant les bases per a futurs diàlegs més concrets.

Aquesta fase destaca per l'aparició de les primeres normatives de ciberseguretat i les discussions d'establir principis bàsics i responsabilitats al ciberespai.

Fase 2: Fase d'Expansió (2013-2016)

Aquest període va veure un augment significatiu de les discussions de normatives, amb el discurs global ampliant-se per abastar temes més específics i variats. Les normatives es van definir més i la participació de la comunitat internacional en les discussions sobre ciberseguretat van augmentar considerablement. Les característiques d'aquesta fase inclouen:

- La definició i discussió de noves normes de ciberseguretat.
- Discussió d'accions i responsabilitats més específiques.
- Més atenció a l'intercanvi d'informació, les infraestructures i la cooperació.

Fase 3: Declivi (2017-2020)

La fase final va observar un descens en el desenvolupament de noves normatives. Aquest descens s'atribueix a diversos factors com la reducció de l'activitat d'organitzacions influents del GGE de les Nacions Unides i esdeveniments globals com la pandèmia de COVID-19.

4.2 Marc Legal i Normatiu

L'establiment i el compliment dels estàndards són fonamentals per garantir la seguretat, la privadesa i la integritat de les dades i la informació.

Aquests estàndards, desenvolupats a través del consens entre organitzacions i altres parts interessades, proporcionen un marc per a la implementació de pràctiques de ciberseguretat, estratègies de gestió de riscs i la protecció de dades dels usuaris. L'aplicació d'aquests estàndards son fonamentals per mitigar la infinitat d'amenaces cibernètiques a què s'enfronten les industries i especialment la industria dels videojocs, fomentant així un ecosistema segur i sostenible.

A continuació s'exemplifiquen diferents normatives de seguretat aplicables a la indústria dels videojocs:

ISO/IEC 27001: Aquesta norma internacional descriu un marc per els sistemes de gestió de la seguretat de la informació (SGSI), que ofereix una guia completa sobre les polítiques, els procediments i els controls necessaris per assegurar els actius d'informació de l'organització. Dins de la indústria dels videojocs, la norma ISO/IEC 27001 serveix com a referència per a l'establiment de bones pràctiques de seguretat com la gestió d'actius, el control d'accés o la gestió d'incidents de seguretat (Sharron, 2024). El compliment d'aquesta norma demostra el compromís d'una empresa de mantenir alts nivells de seguretat de la informació, augmentant així la confiança entre els seus jugadors.

Marc de ciberseguretat NIST: Desenvolupat per l'Institut Nacional d'Estàndards i Tecnologia, aquest marc proporciona un marc polític d'orientació de seguretat sobre com les organitzacions del sector privat dels Estats Units poden avaluar i millorar la seva capacitat per prevenir, detectar i respondre als ciberatacs. Està format per estàndards, directrius i bones pràctiques per gestionar el risc relacionat amb la ciberseguretat. Permet a les empreses de videojocs aplicar els seus principis al context específic de les seves operacions, facilitant la identificació, protecció, detecció i resposta dels incidents de ciberseguretat (NIST, 2024)

COPPA (Children's Online Privacy Protection Act): COPPA imposa requisits específics als propietaris de llocs web o serveis en línia que estan dirigits o que recopilen informació de menors de 13 anys. A la indústria dels videojocs, això requereix la implementació de mesures que garanteixin la privacitat i la seguretat dels jugadors menors, com els mecanismes de consentiment dels pares, avisos de privadesa i la protecció de la informació personal. (FTC, s.f.).

GDPR (Reglament general de protecció de dades): Per a les empreses que operen a la Unió Europea, el GDPR estableix requisits de protecció de dades i privadesa. Aquesta normativa posa èmfasi en els principis de minimització de dades, consentiment i els drets de les persones sobre les seves dades. Les empreses de videojocs han de garantir el compliment del GDPR implementant la protecció de dades des del disseny, realitzant avaluacions periòdiques i proporcionant els usuaris control sobre les seves dades personals (Strebeck, s.f.)

4.3 Trampes

Incorporant les aportacions de la tesi de Samuli Lehtonen (2020), les trampes es poden classificar segons els comportaments en dos grups principals: trampes lleus i trampes severes. Aquesta classificació ajuda a entendre les diverses estratègies que utilitzen els jugadors per obtenir avantatges, empitjorant l'experiència del videojoc.

El gènere del videojoc té un paper crucial a l'hora de determinar la importància i l'impacte del tipus de trampes. Per exemple, en gèneres d'acció com ara els *shooters* en primera persona, l'ús d'eines d'automatització afecten significativament la integritat del videojoc, en canvi, aquestes estratègies poden ser menys efectives en gèneres com els d'estratègia per torns, on el ritme més lent i el disseny del videojoc limiten la utilitat de les automatitzacions d'accions ràpides.

Les trampes afecten tant el mon competitiu dels jugadors com l'ecosistema general i indirectament dels desenvolupadors afectant en conseqüència la confiança i la satisfacció dels jugadors envers aquests, provocant potencials pèrdues financeres i danys reputacionals (Lehtonen, 2020). Un exemple d'això és en el videojoc Call of Duty Modern Warfare 3 on l'ús de trampes que proporcionen avantatges visuals, com ara veure a través de les parets, provoquen el desgast generalitzat dels jugadors lícits ja que els hi aporta una gran desavantatge, afectant negativament l'èxit comercial del videojoc i la posició del desenvolupador al mercat.

Figura 4-1. Trampa visual del videojoc Call of Duty MW3. Font: Font: CheatSeller, 2024.

4.3.1 Trampes lleus

Lehtonen (2020) esmenta que les trampes lleus representen una categoria de trampes que s'aprofiten de les mecàniques d'un videojoc per obtenir un avantatge sobre altres jugadors, essencialment modificant les regles de l'entorn del videojoc sense trencar-les del tot.

Els marcs legals que envolten els videojocs, generalment encapsulats en els acords de llicència d'usuari final (EULA), sovint inclouen clàusules que prohibeixen explícitament l'ús injust de mecàniques de joc. Aquestes clàusules són àmplies, dissenyades per cobrir diferents tipus d'explotacions potencials, reconeixent la impossibilitat d'enumerar totes les trampes o *exploits* possibles. Tanmateix, malgrat aquestes barreres legals, les trampes lleus suposen la principal mesura a combatre per les mesures anti-trampes, i sovint difícils de mitigar perquè principalment no alteren el codi del videojoc ni es basen en programari extern, sinó que fan un mal ús dels sistemes existents.

Un escenari clàssic podria implicar que un jugador compri i vengui articles dins d'un videojoc de forma il·limitada per generar riquesa desproporcionada, aprofitant un error en l'economia del videojoc que els desenvolupadors van passar per alt.

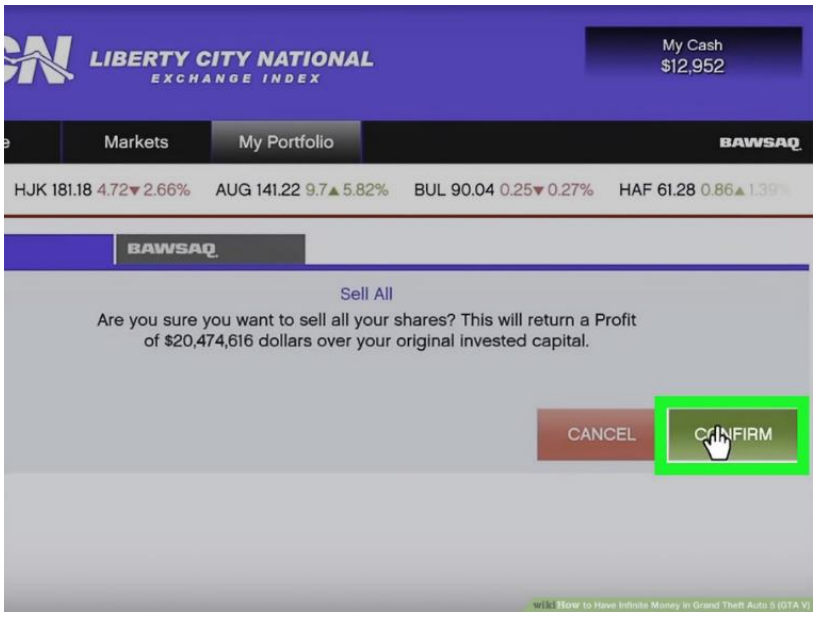

Figura 4-2. Trampa lleu pel videojoc Grand Theft Auto V, s'obté una quantitat desproporcionada de diners fent unes operacions en la borça. Font: Wikihw, 2024.

Una altra forma de trampa lleu implica transaccions amb diners reals per intercanviar-los per recursos del joc, que, tret que les regles del joc ho permetin explícitament, pertorben l'economia del videojoc i ofereixen un avantatge injust. Aquest tipus de trampa és difícil de controlar i demostrar, ja que les transaccions financeres es produeixen fora de la plataforma del videojoc. No obstant això, els desenvolupadors poden utilitzar anàlisi estadístics i registres de les accions dels jugadors per identificar i abordar activitats sospitoses indicatives d'activitats fraudulentes (Lehtonen, 2020).

4.3.2 Trampes severes

Lehtonen (2020) defineix les trampes severes com aquelles que afecten significativament la integritat del videojoc. Aquestes tècniques són el focus principal dels sistemes anti-trampes a causa del seu potencial per impactar dràsticament en el videojoc i en el seu equilibri. Les trampes severes inclouen qualsevol estratègia que modifiqui les funcionalitats o dades bàsiques del videojoc mitjançant intervencions externes, cosa que els converteix en una preocupació crítica tant per els desenvolupadors com per els jugadors.

Una forma comuna d'aquest tipus de trampes implica l'ús de programes externs o mètodes com les injeccions de codi per alterar el videojoc. Aquestes modificacions no només poden afectar la mecànica sinó també l'aspecte visual, com ara permetre els jugadors poder veure a través de superfícies. Una altre tècnica inclou la injecció en memòria, on aquest tipus de trampa interactua directament amb l'espai de memòria del videojoc per introduir noves funcionalitats o explotar-ne les existents, obviant les regles i mecàniques previstes.

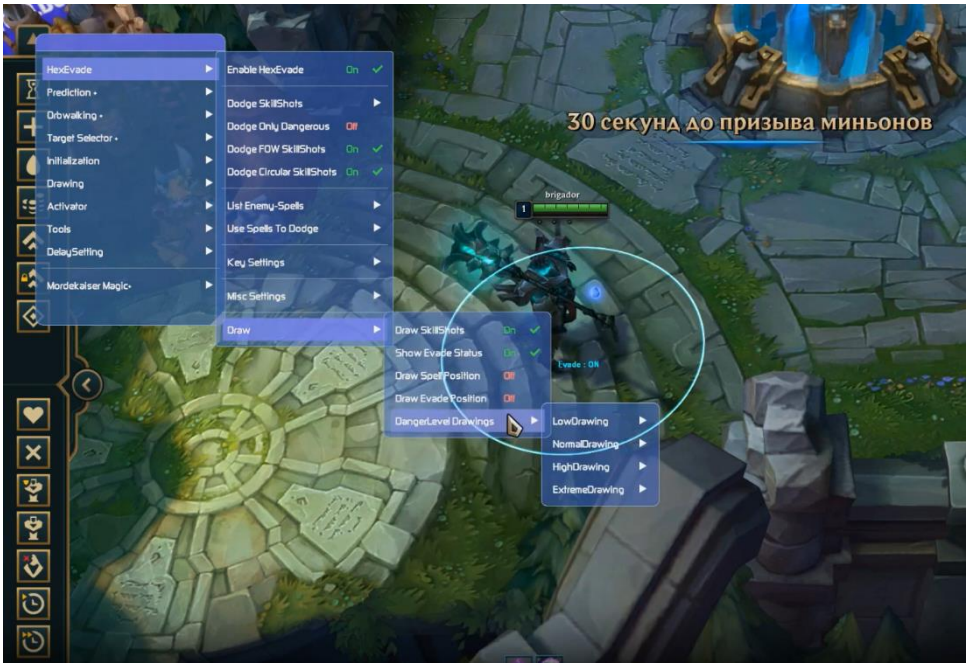

Figura 4-3. Trampa severa pel videojoc League of Legends, mitjançant un programa extern s'obté noves funcionalitats que aporten avantatges. Font: CheatSeller, 2024.

Les eines externes i els bots automatitzats representen unes de les trampes severes més utilitzades. Aquestes eines externes solen automatitzar el videojoc, executant tasques que normalment requereixen l'aportació humana, com ara moure personatges o executar accions. Els bots varien en la seva complexitat i mètodes, des d'aquells que simplement simulen entrades del teclat i el ratolí fins a versions més avançades que interactuen directament amb el client del videojoc o les comunicacions de xarxa per automatitzar funcionalitats. Tot i que alguns bots imiten les aportacions dels jugadors, la seva classificació com a trampes severes prové de la seva dependència de programes externs per obtenir aquest avantatge (Lehtonen, 2020).

Figura 4-4. Trampa severa pel videojoc World of Warcraft. Trampa que permet l'automatització de recursos. Font: CheatSeller, 2024.

La modificació de dades és una altra tàctica molt utilitzada. Aquesta metodologia implica accedir a informació oculta a simple vista pel jugador, com ara les ubicacions d'altres jugadors. Evitar aquest tipus de trampes requereix un disseny que inclogui consideracions sobre quines dades s'emmagatzemen amb memòria i com protegir-les de l'accés no autoritzat (Lehtonen, 2020).

Figura 4-5. Trampa severa pel videojoc Fortnite. Trampa de modificació de dades, jugador pot veure la localització de recursos no visibles a simple vista. Font: CheatSeller, 2024.

La modificació de paquets són tècniques on els paquets de dades enviats entre el client del videojoc i el servidor s'intercepten i es manipulen. Els atacants poden alterar les dades dels paquets per enganyar el servidor, per exemple, falsificant els moviments o les accions dels jugadors. Els atacs de repetició impliquen tornar a enviar paquets modificats al servidor per replicar un resultat desitjat, com ara executar una acció diverses vegades per obtenir avantatge.

4.4 Mètodes Anti-Trampes

La integritat dels videojocs en línia es veu contínuament afectada per la presència de trampes, un dilema que perjudica la indústria des de l'arribada dels videojocs multijugador. La recerca d'una experiència justa i atractiva requereix el desenvolupament de sistemes sofisticats dissenyats per eliminar aquestes pràctiques deshonestes. Aquests sistemes, coneguts com a mecanismes anti-trampes, estan en constant canvi degut a la naturalesa evolutiva de les trampes, que es perfeccionen per eludir la detecció. L'essència de la tecnologia anti-trampa rau en la seva capacitat d'adaptació i identificació de nous mètodes emergents, absorbint metodologies pròpies dels programaris antivirus.

La implementació de mesures anti-trampes no és només una qüestió de mantenir la integritat del videojoc, sinó també de salvaguardar la viabilitat econòmica de les empreses desenvolupadores.

L'ecosistema de trampes s'estén a l'explotació comercial de trampes i exploits, oferint una via lucrativa per obtenir guanys financers.

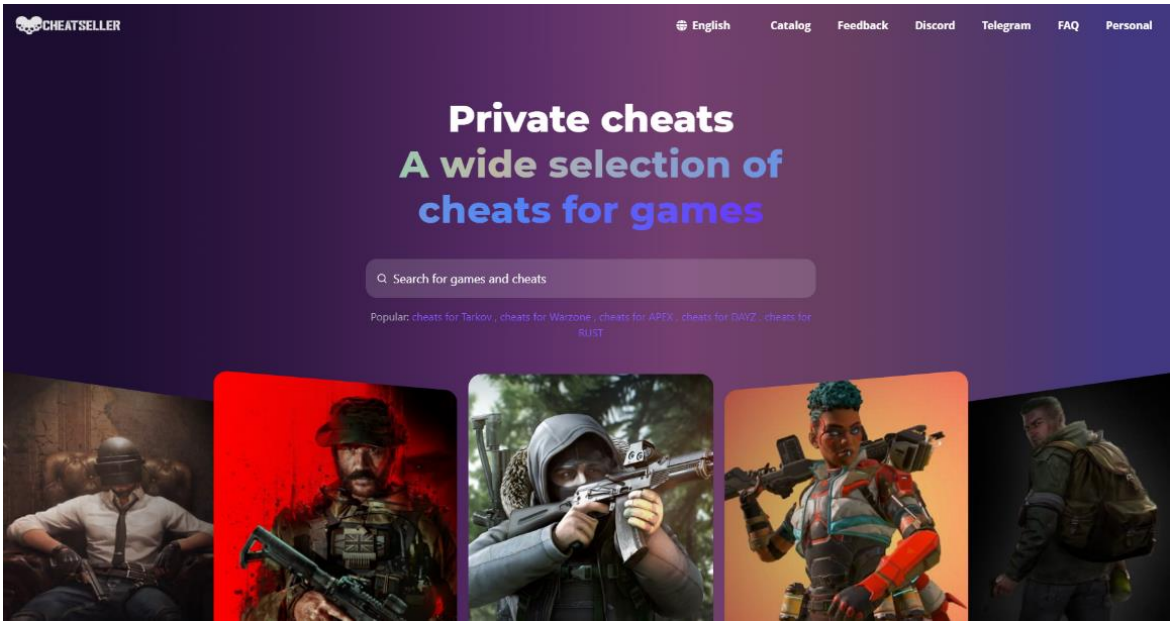

Figura 4-6. Web de venta de trampes. Font: CheatSeller, 2024.

4.4.1 Mètodes anti-trampa al costat del client

Lehtonen (2020) en la seva tesis relaciona l'anti-trampa del costat del client com aquelles metodologies i tecnologies implementades a l'entorn del client (és a dir, a l'ordinador o consola) per protegir-lo. Funciona supervisant l'execució del videojoc, el comportament del sistema i la integritat dels fitxers per identificar i contrarestar els intents de fer trampes. Aquests mètodes són crucials per experiències multijugador en línia on la integritat del videojoc i l'experiència és primordial per a tots els jugadors implicats. Els sistemes anti-trampes del costat del client poden variar àmpliament en la seva complexitat i enfocament, que van des de la simple detecció basada en signatures de programes maliciosos fins a tècniques més sofisticades com l'ofuscament de memòria i el xifratge de codi. A continuació es descriuen algunes de les metodologies emprades:

Xifratge de codi

El xifratge de codi consisteix a la transformació de seccions de codi d'un videojoc en un format il·legible sense la clau de desxifrat correcta. Aquest procés es pot implementar de diverses maneres, com ara xifrar completament l'executable del videojoc o utilitzant un xifratge parcial, on parts específiques de l'executable es desxifren segons sigui necessari i es tornen a xifrar després. Aquest mètode garanteix que la lògica interna del videojoc estigui oculta pels tramposos, protegint així contra possibles manipulacions. No obstant això, com que el videojoc ha de ser capaç de desxifrar el seu codi durant l'execució, les claus de desxifrat s'han d'emmagatzemar en algun lloc ocult de la memòria, significant que no es una mesura completament impenetrable (Lehtonen, 2020).

Verificació dels fitxers mitjançant hash

El hash de fitxers s'utilitza per verificar la integritat dels fitxers del videojoc, assegurant-se que no s'han alterat. En generar un valor hash únic basat en el contingut d'un fitxer, qualsevol modificació d'aquest donarà lloc a un valor hash diferent, que indica manipulació.

Tanmateix, la robustesa del hash de fitxers com a mecanisme anti-trampa depèn de la seguretat del procés de generació i verificació del hash. Els atacants poden interceptar i modificar els valors hash comunicats al servidor o alterant el mecanisme del videojoc per generar aquests valors hash. Per tant, tot i que el hash és una eina factible per garantir la integritat dels fitxers, hauria de formar part d'una estratègia anti-trampa en capes, complementada amb altres mètodes per protegir-se de la manipulació (Lehtonen, 2020).

Detecció de programes de trampes coneguts

La detecció de programes de trampes coneguts implica escanejar el dispositiu de l'usuari per buscar programari de trampes basat en diverses signatures, com ara noms de processos, noms de tasques o el propi hash de fitxers executables. Aquest mètode, tot i que és senzill, es fàcil d'evadir. Els tramposos poden manipular els mètodes d'escaneig per falsejar o utilitzar programes que canvien dinàmicament els seus identificadors, fent que les bases de dades de signatures siguin ineficaces. Malgrat aquestes vulnerabilitats, quan es combina amb altres mesures anti-trampes com el xifratge de codi i l'ofuscament de memòria poden millorar considerablement l'estratègia de protecció integral. Aquest enfocament es beneficia de mantenir una base de dades de signatures actualitzada, amb nous identificadors coneguts (Lehtonen, 2020).

Ofuscació de memòria

L'ofuscament de memòria té com a objectiu dificultar la visualització de dades crítiques del videojoc emmagatzemades en memòria, com ara les coordenades del jugador o els diferents estats del videojoc.

Tot i que és eficaç per dificultar activitats malicioses, l'ofuscació de memòria pot implicar l'ús de més recursos degut a passos addicionals necessaris per desxifrar i reubicar dades. Malgrat això, es tracte d'un element dissuasiu contra la manipulació, funcionant com una capa addicional per protegir la integritat del videojoc (Lehtonen, 2020).

Controladors anti-trampa basats en el nucli

Els controladors anti-trampa basats en el nucli operen al nivell del nucli del sistema operatiu, donant accés total als recursos del sistema i permetent un seguiment complet de les interaccions entre el videojoc i el sistema operatiu. Aquest enfocament millora significativament la capacitat de detectar i bloquejar els intents de trampes supervisant les peticions del sistema i els patrons d'accés a la memòria. Les solucions basades en el nucli poden interceptar els intents de manipulació en

memòria del joc o els processos, oferint una defensa contra les trampes més sofisticades. Tanmateix, la implementació d'anti-trampes a nivell del nucli requereix un disseny tècnic avançat i comporta riscs potencials, com vulnerabilitats que podrien ser explotades per malware. Malgrat aquestes consideracions, els mecanismes anti-trampes basats en el nucli son un dels mètodes més efectius del costat del client, especialment quan es combinen amb altres tècniques anti-trampa (Lehtonen, 2020).

4.4.2 Mètodes anti-trampes del costat del servidor

Els mètodes anti-trampes del costat del servidor són estratègies i tecnologies implementades al servidor, en lloc del client. Aquests mètodes es centren en el principi que el servidor no hauria de confiar en cap dada rebuda del client sense verificació. Les tècniques anti-trampes del costat del servidor estan dissenyades per garantir que totes les accions dels jugadors, estats i intercanvis de dades s'adhereixen a les regles i mecàniques definides.

No confiar en el client

Aquest enfocament es basa en que el servidor ha de verificar totes les dades rebudes del client per assegurar-se que no estan manipulades. Per exemple, si un jugador intenta fer una acció de vendre un article, el servidor comprova si realment el jugador té l'article i si la transacció és factible segons la lògica del videojoc. Aquest mètode evita que els jugadors explotin vulnerabilitats que podrien sorgir de confiar en les dades del costat del client (Lehtonen, 2020).

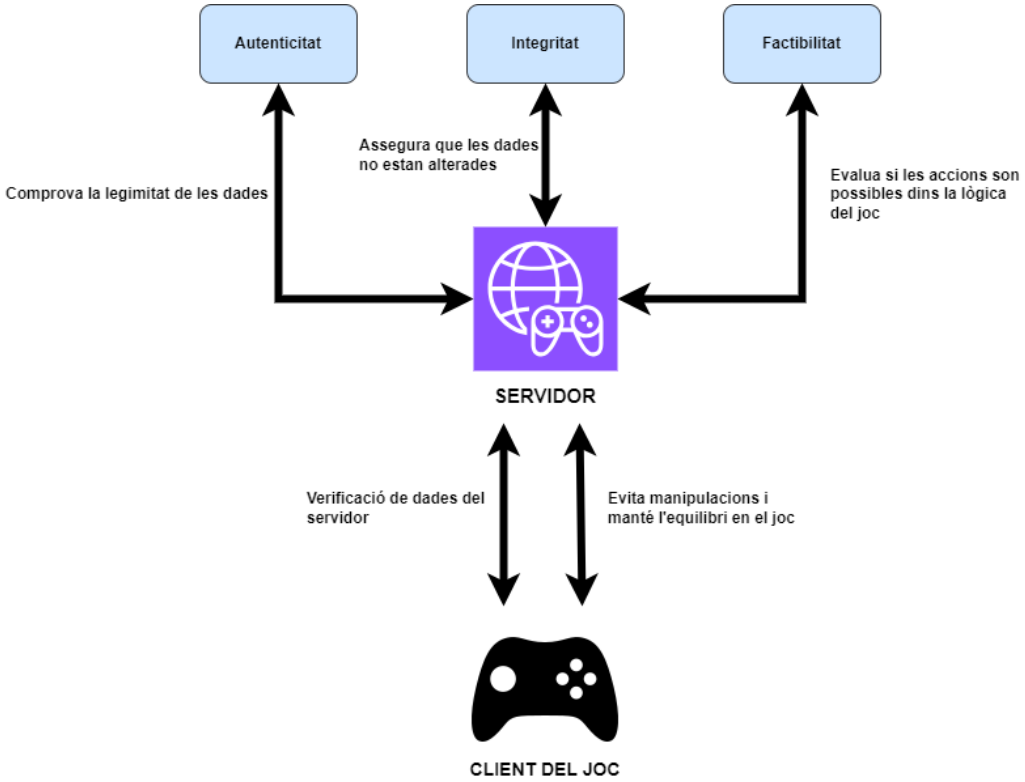

Figura 4-7. Cicle de la metodologia de No confiar amb el client. Font: Elaboració pròpia.

Ofuscament del trànsit de xarxa

L'ofuscament del trànsit de xarxa implica xifrar o ofuscar les dades enviades entre el client i el servidor per evitar la intercepció i l'anàlisi per part de possibles atacants. Tot i que no és infal·lible, l'ofuscament del trànsit de xarxa complica el procés de manipulació de paquets. Un exemple comú és la modificació de paquets de dades capturats per xarxa. El xifratge fa que sigui molt més difícil per els atacants desxifrar i comprendre les dades, tot i que no és una solució 100% eficaç (Lehtonen, 2020).

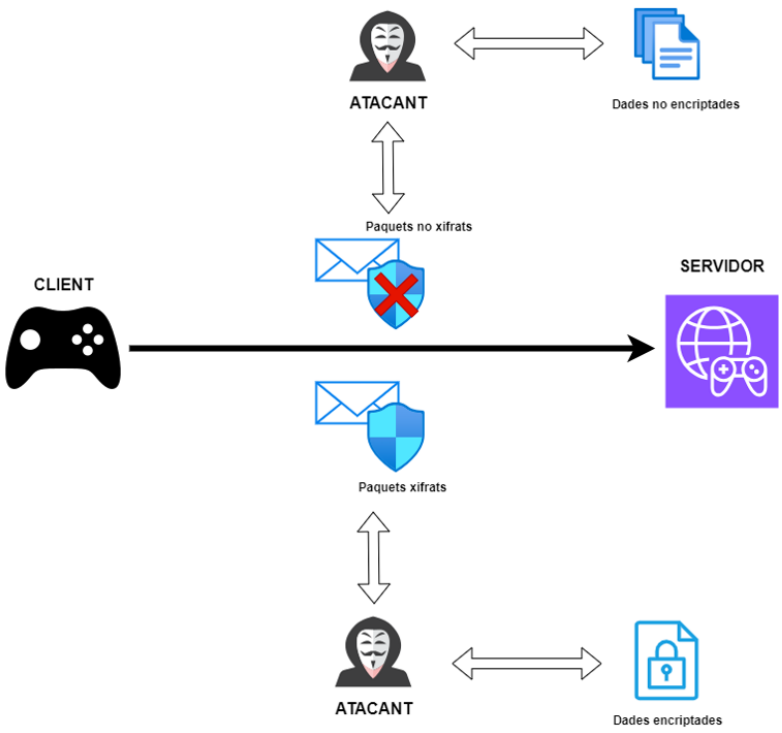

Figura 4-8. Cicle de la metodologia d'ofuscament del trànsit de xarxa. Font: Elaboració pròpia.

Ús de mètodes estadístics per descobrir els atacants

Els mètodes estadístics impliquen l'anàlisi de dades per identificar valors atípics o patrons que suggereixen l'ús de trampes. Per exemple, en un *shooter* la proporció de morts d'un jugador que es desvia significativament de la mitjana pot ser degut a un ús de trampes. Aquests mètodes són molt efectius, però requereixen un estudi de cada cas detallat per evitar falsos positius, com penalitzar els jugadors que simplement són més hàbils. Sistemes anti-trampes com FairFight utilitzen anàlisis estadístics del servidor sense dependre de les dades del client, oferint un mitjà sofisticat per detectar trampes basant-se en dades del videojoc.

La taula següent, adaptada de l'estudi comparatiu de Lehtonen (2020), il·lustra els punts forts i febles dels enfocaments d'anti-trampes del costat del servidor i del costat del client. Cada mètode s'avalua segons cinc criteris: resistència a manipulacions, facilitat d'implementació, falta de sobrecàrrega, no invasiu i idoneïtat per a una varietat de videojocs. Aquesta avaluació ofereix una visió de les

tècniques anti-trampes disponibles i la seva aplicació pràctica en el desenvolupament de videojocs.

Exemples de productes anti-trampa del mercat:

Sistema Anti-Trampes	Desenvolupador	Característiques	Costat Client/Servidor	Jocs que l'Utilitzen
Valve Anti-Cheat (VAC)	Valve Corporation	Busca signatures de fitxers maliciosos, caché DNS i memòria del videojoc	Costat client i servidor	Counter-Strike 2, Dota 2, Rust
PunkBuster	Even Balance, Inc.	Detecta trampes mitjançant l'exploració de memòria en temps real, comprovacions d'integritat dels fitxers, captures de pantalla	Costat client i servidor	Call of Duty: World at War, Battlefield 4, Crysis
BattlEye (BE)	Bastian Suter	Totalment automatitzat que supervisa les tendències i els patrons dels fitxers del videojoc.	Costat client i servidor	PUBG, ARK, DayZ
Easy Anti-Cheat (EAC)	Epic Games	Supervisió en temps real mitjançant l'exploració activa de la memòria del client per detectar i abordar ràpidament activitats sospitoses.Gratuit.	Costat client	Dead by Daylight, Elden Ring, Fall Guys
Xigncode3	Wellbia	Conegut per una alta tassa de falsos positius, suport cross-platform, ús de llistes negres.	Costat client	Eternal Return, Black Desert Online, Bless Online
EA Anti-Cheat	Electronic Arts	Integrat amb els jocs d'EA, enfocat en l'experiència d'usuari, es combina amb altres mesures de seguretat d'EA.	Costat client i servidor	Battlefield 2042, EA SPORTS FC 24
Fredaikis Anti-Cheat	Fredaikis AB	Pocs recursos, enfocat en exploits específics.	Costat client i servidor	Infestation: The new Z
EQU8 Anti-Cheat	EQU8 Technologies	Detecció en temps real, baix impacte en el rendiment, anàlisi basada en el núvol.	Costat client i servidor	Splitgate, Hide or Die
nProtect GameGuard	INCA Internet	Conegut per la protecció a nivell de kernel, efectiu contra diversos exploits, pot causar problemes de rendiment.	Costat client	Helldivers 2, Black Squad, Myth of Empires
BlackCipher	Nexon	Efectivitat moderada, mínim impacte en el rendiment.	Costat client i servidor	Counter Strike Nexon, LawBreakers, Vindictus
TenProtect	Tencent	Algoritmes d'aprenentatge automàtic, baixa tassa de falsos positius.	Costat client i servidor	Ring of Elysiumu, Metal Revolution
Ricochet	Activision	Orientat a nivell de Kernel, anàlisi al costat del servidor, dedicat a la franquícia de Call of Duty.	Costat client i servidor	Call of Duty: Warzone, Call of Duty: Vanguard
AnyBrain	AnyBrain SAS	Detecció basada en IA, adaptativa, mínim impacte en el rendiment.	Costat client i servidor	Lost Ark, Gray Zone Warfare

Taula 4.1. Mecanismes d'anti-trampes al mercat. Font: Elaboració pròpia.

4.5 Protecció de la Propietat Intel·lectual i DRM

Per ajudar a les empreses de videojocs a protegir eficaçment la seva propietat intel·lectual, es poden extreure coneixements de la tesi de Sadia Mosharrof (2020). Aquesta investigació descriu estratègies en el marc de la llei de drets d'autor i la seva aplicació pràctica a la indústria.

L'autora esmenta que la protecció de la propietat intel·lectual sorgeix com una necessitat fonamental per a les empreses que volen protegir els seus videojocs i garantir-ne un benefici. La llei de drets d'autor serveix com a mecanisme principal

per assegurar el contingut original dels videojocs, que inclou tant el programari, l'art, narracions, les peces musicals, etc.

Quan una empresa registra els drets d'autor, això actua com una prova preliminar de que l'empresa és la propietària legítima del videojoc i que és original. Així, el registre facilita l'acció legal contra les persones o empreses que infringeixen els drets d'autor i serveix com a advertència per dissuadir possibles infractors.

L'ús de mesures de protecció tecnològica (TPM) o la gestió dels drets digitals (DRM) son mesures que estan dissenyades per evitar la còpia i distribució no autoritzada, protegint així els drets de propietat intel·lectual dels desenvolupadors i editors.

Els DRM es poden classificar en diversos tipus, cadascun amb diferents mecanismes i implicacions:

DRM	Descripció	Jocs	Avantatges	Inconvenients
Clau	Proporciona un número de sèrie o codi únic amb la còpia física o digital del videojoc.	Atelier Sophie 2, Blue Reflection: Second Light, Angry Birds	Simple d'utilitzar e implementar.	Nombre d'instalacions per clau limitada
Activació en línia	Verifica la legitimitat de la còpia del videojoc via Internet durant la instal·lació i vincula el videojoc a un compte específic.	Atomic Heart, Age of Empires IV, BioShock 2	Simple d'utilitzar e implementar.	Pot causar inconvenients si no hi ha accés a Internet o els servidors estan fora de servei.
Basat en comptes	Vincula els videojocs a comptes de plataformes digitals com Steam.	Babylon's Fall, Apex Legends, Call of Duty: Modern Warfare III	Facilita l'accés multiplataforma i sincronització de dades entre dispositius.	Pot restringir el videojoc a un sol compte, limitant el seu ús compartit.
Límit d'activació	Limita el nombre de vegades que un videojoc pot instal·larse amb la mateixa clau.	Rayman Origins, The Sims 3, Mirror's Edge	Dissuadeix la instal·lació massiva i la distribució il·legal.	Afecta els usuaris amb múltiples dispositius.
Sempre en línia	Requereix connexió contínua a Internet mentre es juga.	Helldivers 2, Skull and Bones, The Crew 2	Ajuda a prevenir la pirateria	Fitxers del videojoc estaran constantment sent descarregats pel servidor per reduir intents de trampes

Taula 4.2. Categories de DRM utilitzades. Font: PCGamingWiki, 2024.

5. Disseny metodològic i cronograma

La metodologia que es desenvolupa en aquest treball es centra en la realització d'una revisió d'abast, o “scoping review”, seguint el marc PSALSAR. Aquest tipus de revisió sistemàtica està dissenyada per revisar la informació existent sobre un tema ampli.

PSALSAR és un acrònim que resumeix els passos d'aquest enfocament estructurat per fer revisions d'abast, facilitant l'exploració sistemàtica d'una àrea de recerca àmplia. Cada lletra de l'acrònim PSALSAR representa una etapa específica en el procés d’investigació:

	FASES	RESULTATS	METODOLOGIA
P S A L S A R	**Protocol**	Abast de la revisió	-
	Cerca	Estratègia de cerca	Identificació de paraules clau
		Cerca d'estudis	Cerca d'estudis, articles i base de dades
	Revisió	Selecció d'estudis	Criteri d'Inclusió i Exclusió
		Identificació de factors clau	
	Síntesis	Extracció de dades	Sintetitzar i analitzar les dades extretes de la cerca
		Categorització de dades	
	Resultats	Anàlisi de dades	Resultats i tendències.
		Resultats	
	Documentar	Redacció	Presentar els resultats
		Conclusió	

Taula 5.1. Metodologia PSALSAR.

Protocol:

La fase inicial d'aquesta metodologia PSALSAR implica la definició de l'abast i els objectius de l'estudi. Aquest pas ajuda a garantir que la revisió defineix l'abast dels aspectes a analitzar i a estudiar.

Cerca:

La fase de cerca d'aquest projecte està estructurada per incloure estudis, informes d'organitzacions, articles i literatura grisa, aquesta última per abastar un ventall més ampli d'informació i perspectives. L'estratègia de cerca es desenvolupa utilitzant una combinació de paraules clau específiques i bases de dades per garantir la inclusió de la literatura rellevant. La cerca de paraules clau es realitza amb els idiomes castellà i anglès.

Paraules Clau		**Base de dades**
Ciberseguretat i Videojocs	Jugadors, Videojocs, Ciberseguretat i Software	Google Schoolar, IEEE, ACM library.
Història i Cibersegurtat	Jugadors, Ciberseguretat i Bones pràctiques	
Normes i Ciberseguretat	Videojocs i Defenses	
Trampes i Videojocs	Indústria dels videojocs i Ciberatacs	
Anti-trampes i Videojocs	Jugadors i Ciberatacs	
Propietat Intelectual i Videojocs	Videojocs i Ciberatacs	
Cultura i Ciberseguretat	Malware i Videojocs	
Ciberseguretat i Empreses de videjocs	Ransomware i Videojocs	
Software, Ciberseguretat i Empreses de Videojocs	DDoS i Videojocs	
Hardware, Ciberseguretat i Empreses de Videojocs	Phishing i Videojocs	
Protecció i Empreses de Videojocs	Tècniques, Phishing i Videojocs	
Jugadors, Videojocs i Ciberseguretat	Empreses, Videojocs i Compromeses	

Taula 5.2. Procés de cerca emprant paraules clau, traduïdes al català. Font: Elaboració pròpia

Revisió:

Aquesta etapa es centra en la valoració i selecció de la recerca existent per garantir que els estudis inclosos en la revisió compleixen amb els criteris preestablerts. Aquí, es defineixen els criteris d'inclusió i d'exclusió, que guien l'avaluació i filtratge de les publicacions.

Tipus de Criteri	Criteris d'Inclusió	Criteris d'Exclusió
Data de Publicació	Recursos publicats en els últims 6 anys.	Recursos publicats fa més de 6 anys, excepte per aquells que siguin fonamentals.
Cobertura Geogràfica	Recursos globals o recerca centrada en regions específiques amb una presència significativa de la indústria dels videojocs.	Recerca amb rellevància limitada degut a un enfocament geogràfic no aplicable.
Idioma	Recursos publicats en català, castellà, anglès o altres idiomes (si la competència lingüística permet una anàlisi precisa).	Recerca en idiomes no entesos si això impedeix una interpretació precisa.
Presència de Paraules Clau	Recursos en els quals les paraules clau predefinides estiguin presents de forma significativa.	Recursos en els quals les paraules clau son innexistents o molt pobres.
Completesa dels Recursos	Recursos que estan complets	Recursos amb mancances de dades o incomplets.

Taula 5.3. Criteris d'inclusió-exclusió. Font: Elaboració pròpia

Síntesis:

L'etapa de Síntesi categoritza e integra la informació obtinguda dels recursos seleccionats durant la fase de Revisió. Aquest procés comporta l'extracció, l'organització i la combinació de dades per a poder extreure posteriorment els resultats.

L'organització de les dades es defineix de la següent manera:

Nº	Criteri	Categoria
1	**Any de publicació**	Ordenat per data de més recent a més antic
2	**Nom del recurs**	Títol del recurs
3	**Zona del recurs**	País o regió d'on està el recurs orientat
4	**Tipus de font del recurs**	Dades primàries, Dades secundàries o Dades mixtes
5	**Tipus del recurs**	Article, Estudi, Notícia, Revista, Llibre, Conferència, Publicació

Taula 5.4. Procés de síntesis de la metodologia PSALSAR. Font: Elaboració pròpia

Anàlisi i resultats:

Durant la fase d'anàlisi i resultats, es dona a terme l'estudi de les dades recopilades per extreure coneixements significatius de la recerca plantejada. El procés analític comporta l'avaluació de les dades amb els criteris preestablerts.

Documentació:

En aquesta fase es presenten els resultats de la revisió bibliogràfica i les seves conclusions mitjançant taules de resultats o documentació escrita.

6. Anàlisi i resultats

6.1 Cultura centrada en la ciberseguretat

A mesura que el sector dels videojocs s'expandeix i es diversifica, les potencials amenaces cibernètiques també ho fan, presentant un conjunt complex de reptes que exigeixen urgentment respostes estratègiques. Aquesta secció està elaborada amb la intenció de guiar a les empreses de videojocs, des de desenvolupadors independents en creixement fins a empreses mes grans, a adoptar un model cultural centrat en ciberseguretat que ajudi a protegir la integritat, confidencialitat i disponibilitat de totes les seves dades.

Aquesta cultura pretén ser integrada en les operacions d'una organització englobant els valors, creences i comportaments.

Adoptant el model de Huang i Pearlson (2019), es pretén que la indústria dels videojocs no només asseguri els seus actius digitals i la seva infraestructura, sinó que també alineï les seves operacions amb les millors pràctiques culturals que puguin reforçar les seves defenses contra les ciberamenaces, mantenint el compliment de les normatives i preservant la confiança dels seus usuaris. Aquesta cultura de ciberseguretat no és estàtica sinó dinàmica, evoluciona amb el creixement de la indústria i els canvis de l'entorn.

A continuació es mostren les característiques a adoptar per les empreses de videjocs segons el model adaptat:

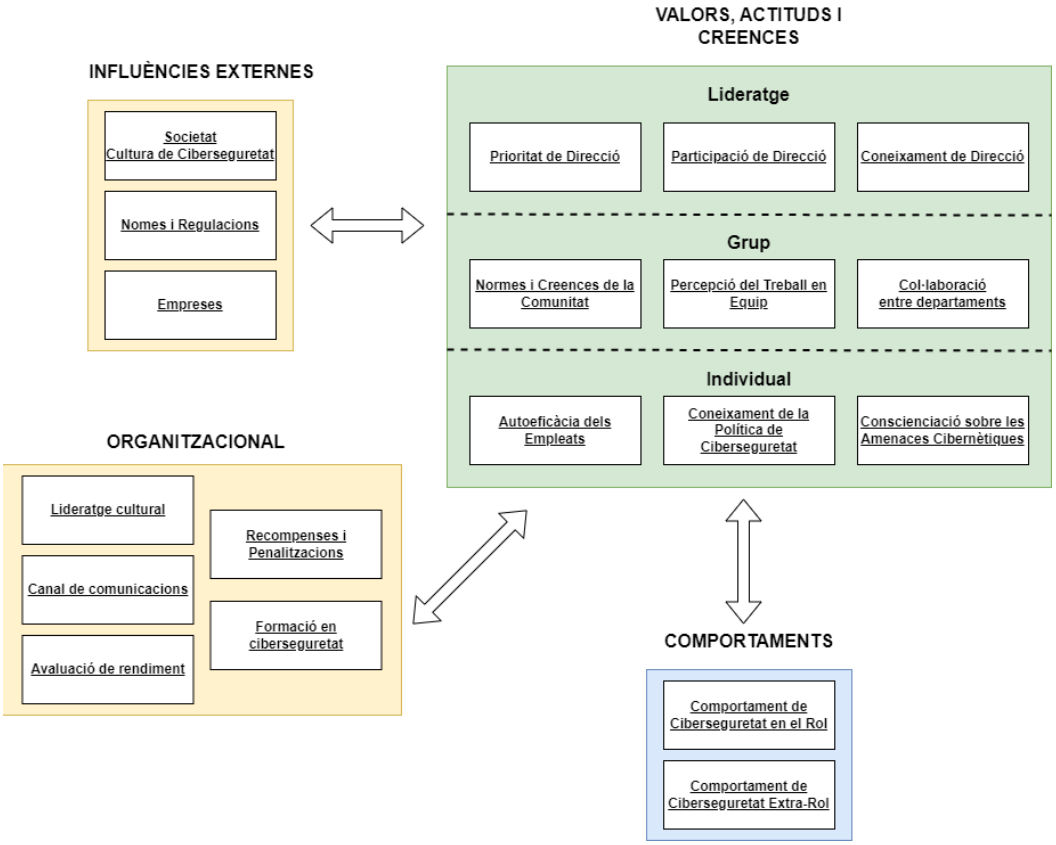

Figura 6-1. Mecanismes que formen la cultura de ciberseguretat. Font: Elaboració pròpia a partir de Huang i Pearlson, 2023.

Influències externes

- **Societat-Cultura de ciberseguretat**
  - Comparar regularment les pràctiques de seguretat de l'empresa amb les principals companyies de videojocs per estar al dia de les últimes tendències i estàndards de seguretat.
  - Participar en fòrums del sector, conferències e iniciatives de col·laboració per compartir i obtenir informació sobre les millors pràctiques de ciberseguretat.

- **Normes i Regulacions**:
  - Complir amb les normatives i regulacions, com el GDPR per a la protecció de dades, la COPPA per a la protecció de dades de menors i altres lleis específiques del sector.

- Estar informats sobre els canvis en les lleis i les regulacions que afectin les pràctiques i polítiques de ciberseguretat.

- **Empreses**:
  - Relacionar-se amb altres empreses de videojocs per aprendre dels èxits, les noves adopcions i les noves amenaces emergents.
  - Adoptar les millors pràctiques d'institucions o empreses del sector per millorar la pròpia situació.

Organitzacional

- **Lideratge cultural**:
  - Crear una figura com un director de seguretat (CSO) o un equip dedicat responsable de preservar i millorar la cultura de ciberseguretat.
  - Proporcionar a l'equip els recursos i l'autoritat necessària per implementar mesures efectives.

- **Canal de comunicacions**
  - Assegurar-se que les comunicacions siguin segures i es reforci la importància de la ciberseguretat a tots els nivells de l'organització.

- **Formació en ciberseguretat**
  - Fomentar una cultura d'aprenentatge continu mitjançant seminaris, cursos i col·laboracions amb experts.
  - Fomentar l'intercanvi de coneixements i la col·laboració entre els departaments per construir un coneixement col·lectiu.

- **Avaluació de rendiment**
  - Integrar el compliment de la ciberseguretat i els comportaments proactius a les avaluacions de rendiment de tots els empleats.

- **Recompenses i penalitzacions**
    - Desenvolupar un sistema de recompenses per premiar les bones pràctiques de seguretat, i les conseqüències adequades per l'incompliment.

Creences, valors i actituds

- **Prioritat de direcció**
    - Fer de la ciberseguretat una prioritat estratègica, assegurant-se que forma part de la presa de decisions d'alt nivell.

- **Participació de direcció**
    - Fer que la direcció de l'empresa participin activament en iniciatives de ciberseguretat i siguin un exemple per a la resta de l'organització.

- **Coneixements de direcció**
    - Assegurar-se que la direcció estigui ben informada sobre les amenaces emergents i les estratègies de ciberseguretat implementades.

- **Normes i creences de la comunitat**
    - Desenvolupar una comprensió col·lectiva de la ciberseguretat.

- **Percepció del treball en equip**
    - Promoure un enfocament col·laboratiu en tots els processos.

- **Col·laboració entre departaments**
    - Fomentar la cooperació entre els diferents departaments de l'empresa de videojocs.

- **Autoeficàcia dels empleats**
    - Dotar els empleats del coneixement i eines per identificar les diferents amenaces de ciberseguretat.

- Assegurar que els empleats realitzin les actuacions adequades en el cas d'un incident de ciberseguretat.

- **Coneixement de la política de ciberseguretat**:
  - Assegurar-se que els empleats coneguin, entenguin i apliquin les polítiques de ciberseguretat de l'empresa i la seva importància.

- **Conscienciació sobre les amenaces cibernètiques**:
  - Mantenir informats els empleats sobre les amenaces i tendències de ciberseguretat emergents que afectin a la indústria.

Comportaments

- **Comportament de ciberseguretat en el rol**
  - Els empleats han de desenvolupar les seves funcions centrant-se en la seguretat i adherint-se en les polítiques de ciberseguretat.

- **Comportament de ciberseguretat extra-rol**
  - Animar els empleats a contribuir en el rol de ciberseguretat més enllà de les seves tasques habituals, funcions com informar d'activitats sospitoses i participar en fòrums de seguretat.
  - Reconèixer i premiar els empleats que prenen mesures proactives per millorar la ciberseguretat dins de l'organització.

6.2 Mecanismes de defensa en la indústria

En aquesta secció, es presenten taules de resultats que detallen els diferents mecanismes de defensa actuals existents en tres diferents àmbits de la indústria: Les empreses, els jugadors i els videojocs.

Les taules, estan dividides en les categories següents: el mecanisme, eines d'exemple (per il·lustrar com es pot aplicar el mecanisme a la pràctica), els sistemes o actius que protegeixen (per ajudar a identificar quines parts del sistema són vulnerables i necessiten protecció), l'amenaça a combatre (per comprendre l'efectivitat) i una descripció de cada mecanisme.

També s'utilitzen paràmetres mesurables com ara el rang de protecció (per saber l'abast), la facilitat d'implementació (per assegurar que els usuaris adoptin de manera efectiva la mesura), el cost (per mesurar l'accessibilitat) i l'eficàcia (per mesurar l'efectivitat del mecanisme).

Cada paràmetre es categoritza amb els valors d'ALT, MIG i BAIX per facilitar la comparació.

Els paràmetres estan definits segons:

Rang de protecció

- ALT: El mecanisme ofereix proteccions avançades i de gran complexitat.
- MIG: El mecanisme ofereix proteccions moderades i de complexitat mitjana.
- BAIX: El mecanisme ofereix proteccions bàsiques i de baixa complexitat.

Facilitat d'implementació

- ALT: El mecanisme és fàcil d'implementar i requereix uns coneixements tècnics o recursos mínims.
- MIG: El mecanisme requereix un esforç moderat per implementar-lo, possiblement necessitant alguns coneixements tècnics o recursos addicionals.
- BAIX: El mecanisme és difícil d'implementar i requereix una experiència tècnica, temps i recursos importants.

Cost

- ALT: El mecanisme és car i implica una inversió financera important per a la compra, la implementació o el manteniment.
- MIG: El mecanisme té un cost moderat per a la compra, la implementació o el manteniment.
- BAIX: El mecanisme és barat per a la compra, la implementació o el manteniment.

Eficàcia

- ALT: El mecanisme és altament eficaç, proporciona una protecció completa i redueix significativament el risc de l'amenaça.
- MIG: El mecanisme és moderadament efectiu, proporciona una protecció digna i redueix el risc de l'amenaça.
- BAIX: El mecanisme és menys efectiu, ofereix una protecció limitada i no sempre és efectiu contra l'amenaça.

COMPANYIA DE VIDEOJOCS										
CATEGORIA	**MECANISME**	**EINA**	**PROTEGEIX**	**AMENAÇA**	**DESCRIPCIÓ**	**RANG DE PROTECCIÓ**	**FACILITAT D'IMPLEMENTACIÓ**	**COST**	**EFICÀCIA**	**TOTAL**
Software	**Detector d'intrusions**	Snort, Suricata	Infraestructura de xarxa	Intrusions, Malware	Supervisa les activitats de la xarxa o del sistema per detectar activitats malicioses.	ALT	BAIX	ALT	ALT	**2.5**
	Prevenció d'intrusions	Cisco IPS, IBM Security IPS	Infraestructura de xarxa	Intrusions, Atacs de xarxa	Prevé i bloqueja activament les intrusions i atacs detectats a la xarxa.	ALT	BAIX	ALT	ALT	**2.5**
	Antivirus/Antimalware	McAfee, Norton	Servidors, Endpoints	Malware	Escaneja, detecta i elimina malware i protegeix contra possibles infeccions.	MIG	MIG	MIG	ALT	**3.5**
	Detecció i Resposta d'Endpoint	CrowdStrike, Carbon Black	Endpoints	Amenaces persistents avançades (APT)	Supervisa els esdeveniments d'endpoint, de xarxa i emmagatzema informació de manera centralitzada per a una anàlisi posterior.	ALT	BAIX	ALT	ALT	**2.5**
	Encriptació de dades	BitLocker, VeraCrypt	Dades	Robatori de dades	Xifra les dades per protegir-les de l'accés d'usuaris no autoritzats.	MIG	BAIX	BAIX	MIG	**2.75**
	Gestor d'Actualitzacions	WSUS, SCCM	Aplicacions i sistemes operatius	Vulnerabilitats i exploits	Assegura que el programari i els sistemes operatius estiguin actualitzats a la darrere versió per evitar vulnerabilitats.	BAIX	ALT	MIG	MIG	**2.75**
	Autenticació de Doble Factor (2FA)	Google Authenticator, Authy	Comptes de jocs	Intrusions	Segona forma d'autenticació, normalment un codi proporcionat per una aplicació mòbil.	MIG	ALT	BAIX	ALT	**4.5**
	Túnels VPN	Fortinet Forticlient, Cisco AnyConnect	Tràfic de xarxa	Man-in-the-middle	Crea una connexió segura a Internet entre el dispositiu de l'empleat i la xarxa de l'empresa.	ALT	BAIX	BAIX	ALT	**3.75**
	Anti-DDoS	Cloudflare, Akamai Kona	Xarxes i servidors	DDoS	Protegeix contra atacs DDoS filtrant i gestionant el trànsit.	ALT	BAIX	ALT	ALT	**2.5**
	Sistemes de còpies de seguretat	Acronis, Veeam	Integritat i disponibilitat de les dades	Robatori de dades, Ransomware	Solucions per crear còpies de seguretat de les dades	MIG	MIG	MIG	MIG	**3**
Hardware	**Firewall**	Fortinet FortiGate, SonicWall	Infraestructura de xarxa, Servidors	Intrusions, Malware, Robatori de dades	Supervisa i controla el trànsit de xarxa entrant i sortint en funció de regles de seguretat predeterminades.	ALT	BAIX	ALT	ALT	**2.5**
	Dispositius d'accés segur	YubiKey, RSA SecurID	Autenticació d'usuari	Phishing, Intrusions	Dispositius utilitzats per a l'autenticació multifactor	BAIX	ALT	BAIX	MIG	**3.25**
	Maquinari de backup	NAS, RAID	Integritat i disponibilitat de dades	Robatori de dades, Ransomware	Dispositius físics utilitzats per crear còpies de seguretat de les dades.	MIG	MIG	ALT	MIG	**2.25**
Organitzacional	**Polítiques de Seguretat**	ISO 27001, NIST Framework	Seguretat global de l'organització	Robatori de dades, Incompliments de seguretat	Conjunt de polítiques i procediments dissenyats per protegir els actius de l'empresa.	ALT	BAIX	ALT	ALT	**2.5**
	Formació de Seguretat	KnowBe4, SANS Security Awareness	Empleats i contractistes	Enginyeria social, Phishing	Programes de formació per educar el personal sobre les millors pràctiques de ciberseguretat i conscienciar de les amenaces.	MIG	MIG	MIG	MIG	**3**
	Pla de resposta a incidents	IBM Resilient, Splunk Phantom	Gestió d'incidents	Ciberatacs, Fugues de dades	Enfocament estructurat per gestionar les conseqüències d'un ciberatac	ALT	MIG	MIG	ALT	**4**
	Centre d'operacions de seguretat (SOC)	AlienVault USM, SolarWinds Security Event Manager	Seguiment i resposta contínua	Ciberamenaces, incidents	Unitat centralitzada que tracta i monitoritza temes de seguretat a nivell organitzatiu i tècnic.	ALT	BAIX	ALT	ALT	**2.5**
	Pla d'identificació de riscs	RiskWatch, RSA Archer	Risc organitzatiu global	Vulnerabilitats no identificades, amenaces	Processos i estratègies per a la identificació i avaluació de riscs.	ALT	MIG	MIG	ALT	**4**
	Proves de Penetració	Metasploit, Burp Suite	Xarxa, Aplicacions	Vulnerabilitats	Ciberatacs simulats per provar la seguretat dels sistemes i identificar vulnerabilitats.	ALT	BAIX	MIG	MIG	**2.75**
	Blue Team	Splunk, ArcSight	Infraestructura	Ciberamenaces, incidents	Grup encarregat de mantenir les defenses internes contra les amenaces cibernètiques.	ALT	BAIX	ALT	ALT	**2.5**
	Campanyes de Phishing	Cofense, PhishMe	Dades, Sistemes	Phishing	Atacs de phishing simulats per educar els empleats sobre com reconèixer i evitar els intents de phishing	MIG	MIG	BAIX	MIG	**3.5**
	Assegurança Cibernètica	AIG Cyber Insurance, Chubb Cyber Insurance	Actius financers	Pèrdues Financeres	Pòlissa d'assegurança per cobrir el cost dels ciberatacs, inclòs el robatori de dades i les possibles interrupcions operatives	ALT	MIG	ALT	ALT	**3.25**
	Cultura de Seguretat	Formació Continuada, Tallers de Sensibilització	Seguretat organitzacional	Enginyeria Social, Phishing	Cultivar una cultura de conscienciació en ciberseguretat entre els empleats per evitar possibles incidents	ALT	MIG	MIG	ALT	**4**

Taula 6-1. Mecanismes de defensa disponibles per les empreses de la indústria dels videojocs. Font: Elaboració pròpia.

JUGADORS PC										
CATEGORIA	**MECANISME**	**EINA**	**PROTEGEIX**	**AMENAÇA**	**DESCRIPCIÓ**	**RANG DE PROTECCIÓ**	**FACILITAT D'IMPLEMENTACIÓ**	**COST**	**EFICÀCIA**	**TOTAL**
Software	**Antivirus/Antimalware**	McAfee, Norton	Fitxers del videojoc, Dades personals, Integritat del PC	Malware	Escaneja, detecta, elimina malware i protegeix contra possibles infeccions.	MIG	MIG	MIG	ALT	**3.5**
	Gestor de contrasenyes	LastPass, 1Password	Comptes de videojocs	Phishing, robatori de credencials	Emmagatzema i gestiona les contrasenyes de manera segura.	MIG	MIG	BAIX	MIG	**3.5**
	Software de xifratge	VeraCrypt, BitLocker	Dades dels videojocs/ partides guardades, Dades sensibles	Robatori de dades	Xifra dades sensibles o dades guardades del videojoc.	ALT	BAIX	ALT	ALT	**2.5**
	VPN	NordVPN, ExpressVPN	Privacitat	MitM, Atacs DDoS	Amaga les adreces IP i xifra les connexions durant les partides en línia.	ALT	BAIX	ALT	ALT	**2.5**
	Autenticació de Doble Factor (2FA)	Google Authenticator, DUO	Comptes de videojocs	Robatori de comptes	Segona forma d'autenticació, normalment un codi proporcionat per una aplicació mòbil.	MIG	MIG	BAIX	ALT	**4**
	Eines anti-phishing	PhishTank, Norton Anti-Phishing	Comptes de videojocs	Phishing	Identifica i bloqueja intents de phishing, ajudant els jugadors a evitar estafes que busquen robar informació personal o credencials dels comptes.	ALT	MIG	ALT	ALT	**3.25**
Cultural	**Formació i conscienciació de seguretat**	KnowBe4, PhishMe	Coneixement del jugador	Phishing	Educa els jugadors sobre com reconèixer i evitar estafes de phishing.	MIG	ALT	BAIX	ALT	**4.5**
	Gestió d'accés	-	Comptes de videojocs	Intrusions	Utilitzar contrasenyes úniques i robustes per els diferents comptes de cada videojoc, habilitar l'autenticació doble factor i actualitzar regularment les contrasenyes.	MIG	ALT	BAIX	ALT	**4.5**
	Monitorització de l'activitat del compte	-	Comptes de videojocs	Intrusions	Comprovar l'activitat del compte i informar immediatament de qualsevol comportament sospitós.	MIG	ALT	BAIX	MIG	**4**
	Descarregar de pàgines legítimes	N/A	Integritat del PC, Dades personals	Malware	Només descarregar videojocs de pàgines oficials i legítimes.	MIG	ALT	BAIX	ALT	**4.5**
	Compartició d'informació	N/A	Privacitat, Dades personals	Robatori de dades, Phishing	Evitar compartir informació personal a través dels chats dels videojocs.	BAIX	ALT	BAIX	MIG	**3.25**
	Ús de gamertags	N/A	Privacitat	Robatori de dades	Utilitzar pseudònims en lloc de noms reals per protegir la identitat personal.	BAIX	ALT	BAIX	MIG	**3.25**
	Precaució amb mods i complements de tercers	N/A	Integritat del PC, Dades personals	Malware, Phishing	Només utilitzar mods i complements de pàgines oficials i legítimes.	MIG	ALT	BAIX	ALT	**4.5**

Taula 6-2. Mecanismes de defensa disponibles per els jugadors de PC. Font: Elaboració pròpia.

VIDEOJOC										
ATEGORIA	MECANISME	EINA	PROTEGEIX	AMENAÇA	DESCRIPCIÓ	RANG DE PROTECCIÓ	FACILITAT D'IMPLEMENTACIÓ	COST	EFICÀCIA	TOTAL
Software	**Antitrampes**	BattlEye, Easy Anti-Cheat	Integritat del videojoc,Experiència justa	Trampes, Exploits	Detecta i elimina les trampes i exploits.	ALT	BAIX	ALT	ALT	**2.5**
	Antimanipulació	Denuvo, Themida	Integritat del videojoc, Codi font	Modificació no autoritzada	Protegeix contra la manipulació del codi font del videojoc per evitar modificacions no autoritzades.	ALT	BAIX	ALT	ALT	**2.5**
	Ofuscació	ProGuard, Dotfuscator	Integritat del videojoc, Codi font	Enginyeria inversa, pirateria	Ofusca el codi font per dificultar la seva comprensió mitjançant enginyeria inversa.	ALT	MIG	MIG	MIG	**3.5**
	Xifrat de dades	AES, RSA	Dades sensibles del joc	Accés no autoritzat, robatori	Xifra dades del videojoc per dificultar la seva comprensió mitjançant enginyeria inversa.	ALT	MIG	MIG	MIG	**3.5**
	DRM	Denuvo, SecuROM	Contingut del videojoc	Pirateria	Protegeix els continguts dels videojocs de ser copiats o utilitzats de formes ilegals.	ALT	MIG	MIG	MIG	**3.5**
	Actualitzacions	Actualitzacions peròdiques	Integritat del videojoc	Explotacions, vulnerabilitats	Actualitzar regularment per solucionar vulnerabilitats i bugs.	MIG	ALT	BAIX	ALT	**4.5**
	Control d'accés	GameSparks, PlayFab	Integritat del videojoc	Intrusions	Controls d'accés al contingut i serveis del videojoc.	MIG	ALT	BAIX	ALT	**4.5**

Taula 6-3. Mecanismes de defensa disponibles per els videojocs. Font: Elaboració pròpia.

6.3 Tendències d'atacs actuals

En els darrers anys, el sector dels videojocs ha experimentat un ressorgiment notable en termes d'ingressos i nombre d'usuaris, impulsat principalment per les circumstàncies excepcionals derivades de la pandèmia del COVID-19. Segons el darrer informe de Newzoo (2024), el 2023, s'estima que hi ha més de tres mil milions de jugadors a nivell global, cosa que representa un augment del 6.3% en comparació a l'any anterior. Aquest vast conjunt d'usuaris ha contribuït a fer que els ingressos mundials del sector arribessin aproximadament a 242.39 mil milions de dòlars aquest any. (Kaspersky, 2023). Aquest increment en la popularitat i en la dependència dels videojocs com a forma d'entreteniment ha comportat l'augment d'atacs conduits cap aquesta indústria.

A continuació s'exposen els atacs més comuns dirigits tant als jugadors com a les empreses:

6.3.1 Malware

El malware o programari maliciós definit com a software dissenyat per danyar, explotar o obtenir accés no autoritzat als sistemes informàtics s'ha convertit en una preocupació important a la indústria dels videojocs, ja que els atacants sovint utilitzen aquest mètode cada cop més sofisticat per explotar els sistemes de les empreses de videojocs i extorsionar-les. També afecta a la base de jugadors ja que els ciberdelinqüents solen utilitzar tàctiques com el phishing per enganyar els usuaris i fer-los descarregar programes nocius fent veure que es tracten de simples actualitzacions de videojocs o modificacions legítimes.

El món competitiu dels videojocs també porta els jugadors a instal·lar inadvertidament malware prometent falsos avantatges però que finalment acaben comprometen la seva seguretat.

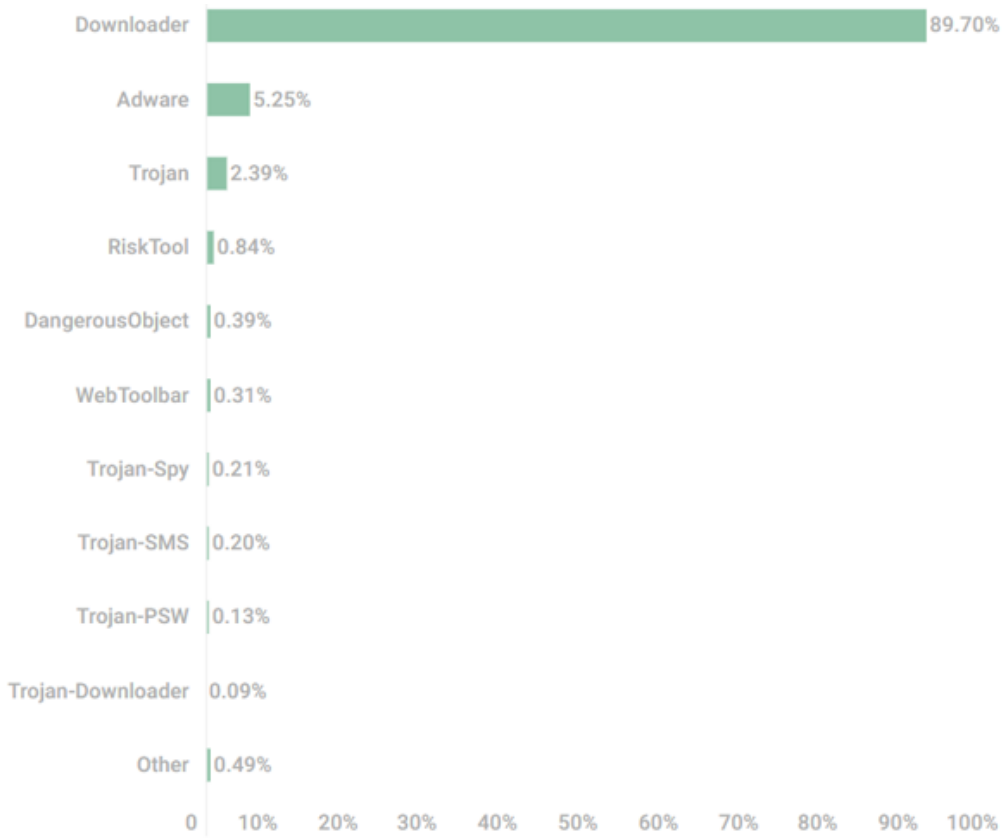

Figura 6-2. Tipus de malware utilitzats a la industria dels videojocs entre 2022 a 2023. Font: Kaspersky, 2023.

El gràfic extret de l'informe de Kaspersky (2023) mostra quin tipus de malware ha sigut el més utilitzat entre l'1 de juliol de 2022 i l'1 de juliol de 2023.

Segons les dades mostrades els Downloaders dominen amb molta diferència amb un 89,70%. Tot i que aquests no són inherentment perjudicials, representen un risc important, ja que poden descarregar automàticament altres programes en un dispositiu, inclòs malware més perillós. A més, les dades mostren que l'adware, que es tracte d'un tipus de malware que mostra anuncis no desitjats al dispositiu de l'usuari sense consentiment d'aquest, representa el 5,25% de les amenaces, mentre que els troians, que poden dur a terme accions com robar dades o provocar la instal·lació de més programari maliciós, constituïen el 2,39%.

Nom	Nombre de fitxers alients utilitzant el títol del videojoc
Minecraft	23239
FIFA	10776
Roblox	8903
Far Cry	8736
Call of Duty	8319
Need for Speed	7569
Grand Theft Auto	7125
Valorant	5426
The Sims	5005
CS:GO	4790

Taula 6-4. Nombre de fitxers suplantant el nom de videojocs. Font: Elaboració pròpia a partir de Kaspersky, 2023.

A l'informe de Kaspersky (2022), es documenta que entre juliol de 2021 i juny de 2022, la indústria dels videojocs va veure un total de 89.888 fitxers, que contenien malware, distribuïts sota l'aparença de videojocs legítims. Això va afectar un total de 384.224 usuaris a tot el món.

Durant aquest període, Minecraft va ser identificat com el més suplentat, amb un total de 23.239 fitxers utilitzats il·lícitament sota el seu nom, que van afectar un total de 131.005 usuaris. Malgrat aquestes xifres elevades, es va produir una reducció notable respecte a l'any anterior: la distribució de fitxers maliciosos va disminuir un 36% i el nombre d'usuaris afectats va disminuir gairebé un 30% (Kaspersky, 2022).

L'informe també destaca altres jocs importants com FIFA, Roblox, Far Cry i Call of Duty com a videojocs freqüentment suplantats.

Anàlisis de TLauncher

Aquesta secció presenta l'anàlisi de TLauncher, és tracte d'una plataforma no oficial per el popular videojoc Minecraft, que permet als usuaris jugar sense la necessitat de comprar el videojoc. Tot i que pot semblar una alternativa accessible per accedir a Minecraft, l'ús de TLauncher presenta diversos riscs de seguretat significatius.

En aquesta secció, s'analitza l'arxiu executable descarregat directament de la web de TLauncher i utilitzant la plataforma Triage, es disseccionа l'arxiu mitjançant la seva tecnologia de sandboxing. Aquest tipus d'eina facilita l'estudi de manera segura analitzant el comportament d'una mostra de software en un entorn controlat i aïllat:

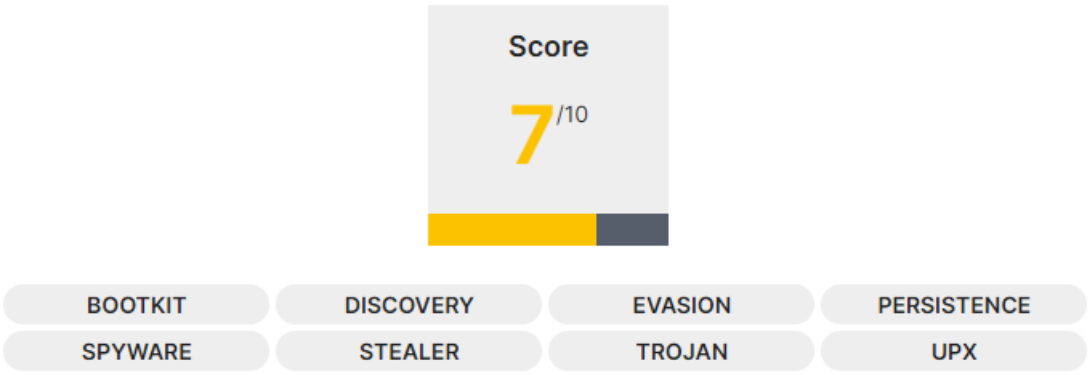

Figura 6-3. Veredicte de TLauncher realitzat pel sandbox Triage. Font: Elaboració Pròpia.

El veredicte del sandbox cataloga l'executable de TLauncher com a 7/10 de nivell de risc, i l'associa amb una sèrie de signatures:

Bootkit: Malware que s'inicia juntament amb el dispositiu per amagar-se eficaçment dels sistemes d'antivirus i obtenir persistència.

Spyware: Recopila informació sense el coneixement de l'usuari, espiant la seva activitat en línia.

Stealer: Realitza activitats com el robatori de dades sensibles, credencials i informació financera.

Trojan: Es fa passar per programari legítim per enganyar els usuaris i sistemes d'antivirus per permetre l'accés no autoritzat.

Evasion: Utilitza tècniques per evitar la detecció dels sistemes antivirus i antimalware.

Persistence: Capacitat del malware per mantenir-se actiu en el sistema inclús després de reiniciar o apagar el dispositiu.

UPX: Mecanisme utilitzat per comprimir executables i complicar-ne la identificació i l'anàlisi.

Discovery: Habilitat del malware per explorar i captar informació del sistema i l'usuari.

Processes: INSTALLER.EXE

description	ioc
Set value (str)	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{E19F9331-3110-11D4-991C-005004D3B3DB}\InprocServer32\ThreadingModel = "Apartment"
Key deleted	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{CAFEEFAC-0014-0002-0041-ABCDEFFEDCBA}\INPROCSERVER32
Set value (str)	\REGISTRY\USER\S-1-5-21-3845472200-3839195424-595303356-1000_CLASSES\CLSID\{CAFEEFAC-0015-0000-0002-ABCDEFFEDCBB}\InprocServer32\1
Set value (str)	\REGISTRY\USER\S-1-5-21-3845472200-3839195424-595303356-1000_CLASSES\CLSID\{CAFEEFAC-0016-0000-0044-ABCDEFFEDCBA}\InprocServer32\
Set value (str)	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{CAFEEFAC-0017-0000-0051-ABCDEFFEDCBA}\InprocServer32\ThreadingModel = "Apartment"
Set value (str)	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{CAFEEFAC-0013-0001-0058-ABCDEFFEDCBA}\InprocServer32\ThreadingModel = "Apartment"
Set value (str)	\REGISTRY\USER\S-1-5-21-3845472200-3839195424-595303356-1000_CLASSES\CLSID\{CAFEEFAC-0015-0000-0063-ABCDEFFEDCBC}\InprocServer32\
Key created	\REGISTRY\USER\S-1-5-21-3845472200-3839195424-595303356-1000_CLASSES\CLSID\{CAFEEFAC-0016-0000-0059-ABCDEFFEDCBC}\InprocServer32
Key deleted	\REGISTRY\MACHINE\SOFTWARE\Classes\CLSID\{CAFEEFAC-0017-0000-0075-ABCDEFFEDCBA}\INPROCSERVER32

Figura 6-4. Cambis al registre del dispositiu realitzat pel procés installer.exe de TLauncher. Font: Elaboració Pròpia.

El comportament mostrat en la captura del procés INSTALLER.EXE de TLauncher indica diverses operacions en el registre del sistema. Aquest executable realitza activitats com la creació, eliminació i modificació de valors i claus de registre. El fet que es creïn i després s'eliminin aquestes claus suggereix que TLauncher intenta modificar de forma dinàmica el comportament del sistema i posteriorment netejar possibles rastres després de realitzar certes accions per així no ser detectat o catalogat com a malware. Això és típic en el comportament de programes maliciosos que intenten amagar la seva presència i assegurar la seva persistència.

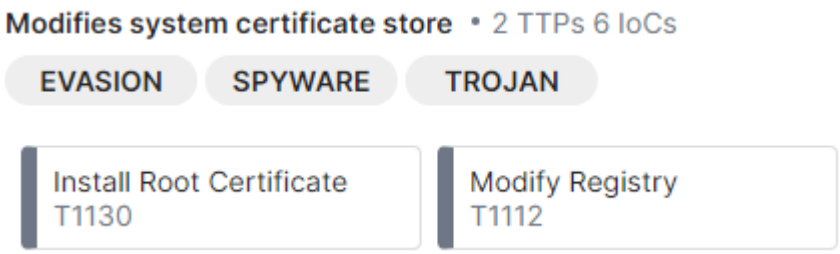

Figura 6.5. Detecció d'activitats pròpies d'evasió, spyware i troià en TLauncher. Font: Elaboració Pròpia.

El sandbox cataloga TLauncher com a possible Troià, ja que s'activen dues signatures basades amb el framework de seguretat MITRE:

- **Install Root Certificate (T1130)**: Aquest mètode els atacants intercepten o manipulen trànsit xifrat, facilitant atacs de man-in-the-middle sense ser detectats per l'usuari, ja que el trànsit apareix com a legítim (MITRE, 2024)

- **Modificar Registre (T1112)**: Consisteix en canvis al registre del sistema operatiu, utilitzats per alterar configuracions de seguretat (MITRE, 2023)

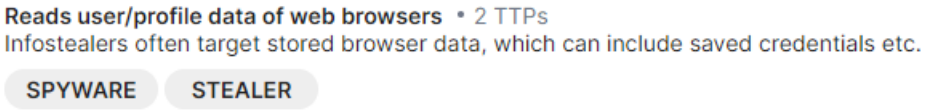

Figura 6.6. Detecció d'activitats pròpies de spyware i stealer en TLauncher. Font: Elaboració Pròpia.

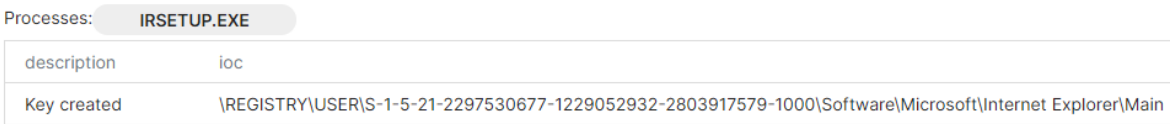

Figura 6-7. Modificació de registre en el navegador Internet Explorer per un executable de TLauncher. Font: Elaboració Pròpia.

El procés IRSETUP.EXE de TLauncher, està relacionat amb la creació d'una clau de registre sota un procés que pertany a Microsoft Internet Explorer. Aquest comportament juntament amb la signatura catalogada per Triage com a SPYWARE i STEALER indica que es realitzen activitats per modificar configuracions del navegador o implantar components addicionals que podrien obtenir les dades dels perfils d'usuaris del navegador web, l'extracció de possibles credencials guardades, dades de targetes de crèdit i altres dades personals.

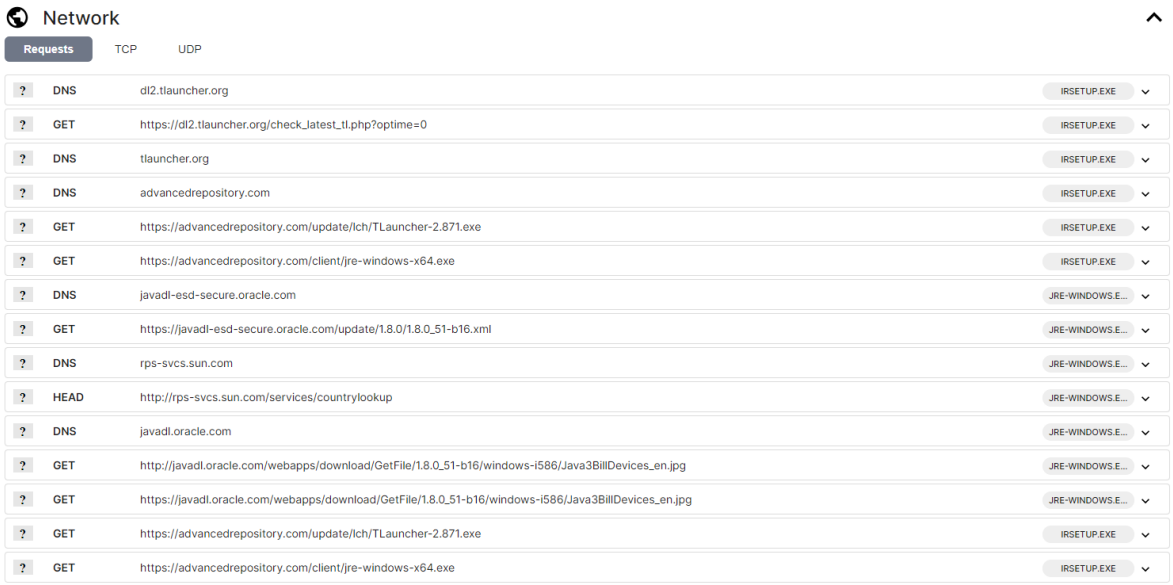

Figura 6-8. Activitats de xarxa de TLauncher. Font: Elaboració Pròpia.

TLauncher realitza sol·licituds DNS a diferents dominis relacionats com "tl.launcher.org" i "advancedrepository.com". Es poden veure múltiples sol·licituds GET per descarregar executables com TLauncher-2.871.exe i altres fitxers de configuració des d'una pàgina no reconeguda anomenada advancedrepository.com. Això indica que el programa està obtenint components addicionals, que podrien ser parts necessàries pel funcionament o per descarregar malware addicional.

6.3.2 Ransomware

La indústria dels videojocs, amb la gran quantitat de dades sensibles de clients i transaccions financeres que es realitzen diàriament, ha fet que es converteixi en un objectiu principal pels atacs de ransomware. Aquest fet destaca per les dades que mostren un augment del 37% en la freqüència d'atac respecte el 2022, amb un cost mitjà de cada incident d'uns 5,3 milions de dòlars, segons les conclusions de l'equip d'investigació d'amenaces de Zscaler (2023).

El ransomware, és un tipus de malware, que bloqueja l'accés als sistemes informàtics i xifra les seves dades per posteriorment demanar un rescat per restaurar l'accés. Els ciberdelinqüents també amenacen amb eliminar les dades de manera permanent o publicar-les públicament si no es paga el rescat.

El ransomware no només afecta a les empreses sinó que també als jugadors, es el cas de TeslaCrypt una variant que va apareixer al 2015, i que utilitzava la tecnologia de xifratge AES per encriptar dades de partides guardades i claus d'activació, afectant a milers de jugadors de videojocs com Call of Duty, Skyrim, entre d'altres. TeslaCrypt es propagava aprofitant vulnerabilitats d'Adobe Flash Player (el-brujo, 2015).

Figura 6-9. Interfície gràfica del ransomware Wannacry. Font: Elaboració Pròpia.

El cas d'Insomniac Games

L'any 2023, Insomniac Games, un estudi de PlayStation Studios conegut per les seves franquícies d'èxit com Spider-Man, va ser víctima d'un atac de ransomware. El grup criminal Rhysida responsable de l'atac, afirmaven haver robat 1,67 TB de dades, inclosa informació sensible sobre un videojoc no anunciat de la franquícia de Wolverine per a PS5, els llançaments estratègics previstos per Insomniac Games fins a l'any 2033 i dades personals dels empleats de l'estudi. Aquest incident posa en manifest els efectes tant perjudicials del ransomware i com ha afectat a la privadesa dels empleats, la propietat intel·lectual i a l'economia de l'empresa.

Rhysida va posar un termini de set dies per realitzar el pagament del rescat, amenaçant amb publicar les dades robades tret que Sony e Insomniac Games paguessin un rescat substancial de 50 BTC (més de 2 milions de dòlars).

De mentres el grup criminal va iniciar una subhasta per vendre la informació robada al millor postor (Erard, 2023).

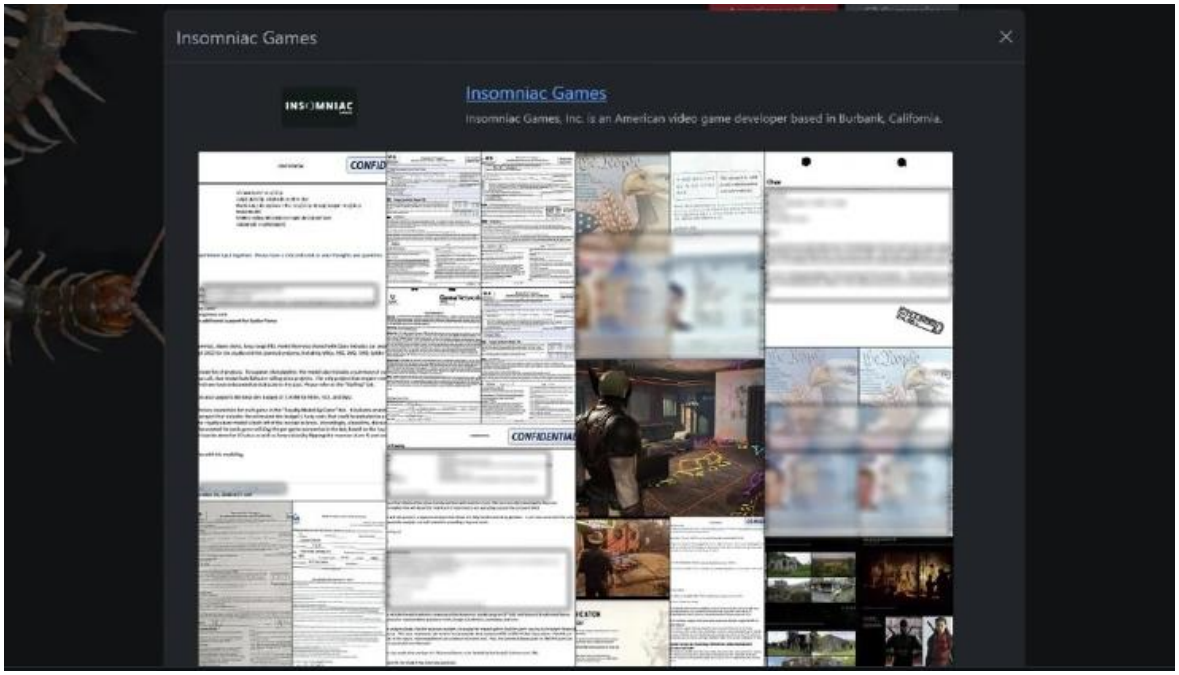

Figura 6-10. Anunci del grup criminal Rhysida anunciant la possessió de dades crítiques d'Insomniac Games. Font: (Hollingworth, 2023).

El cas de Gellyberry Studios

També al 2023, l'empresa desenvolupadora del MMORPG "Ethyrial: Echoes of Yore" va experimentar un atac de ransomware que va provocar l'eliminació de 17.000 comptes de jugadors, inclosa la pèrdua del progrés i dels objectes aconseguits en el videojoc pels seus usuaris. Gellyberry Studios, va anunciar els efectes pel seu canal oficial de Discord.

Ignorant l'opció de realitzar el pagament a favor dels atacants, Gellyberry Studios va decidir emprendre la difícil tasca de restaurar manualment els sistemes afectats. Tot i que l'atac va provocar una pèrdua important de dades, l'estudi es va comprometre a restaurar els comptes dels jugadors i el seu progres de la manera més completa possible.

A més, l'estudi va anunciar plans per reforçar les seves mesures de seguretat com còpies de seguretat offline de forma més freqüent, la implementació d'una VPN P2P per a un accés remot segur als servidors i restriccions a l'accés del servidor a intervals d'IP específics (Cluley, 2023).

Figura 6-11. Videojoc Ethyrial: Echoes of Yore. Font: Gellyberry Studios, 2023.

6.3.3 DDoS

A la indústria dels videojocs, els atacs de denegació de servei distribuït (DDoS) han mostrat una tendència ascendent tant en freqüència com en sofisticació. Segons l'informe tècnic d'Akamai (2023) aquest tipus d'atacs representen el 37% tràsit total DDoS observat a nivell global, cosa que és gairebé el doble en comparació del sector financer, el segon més afectat.

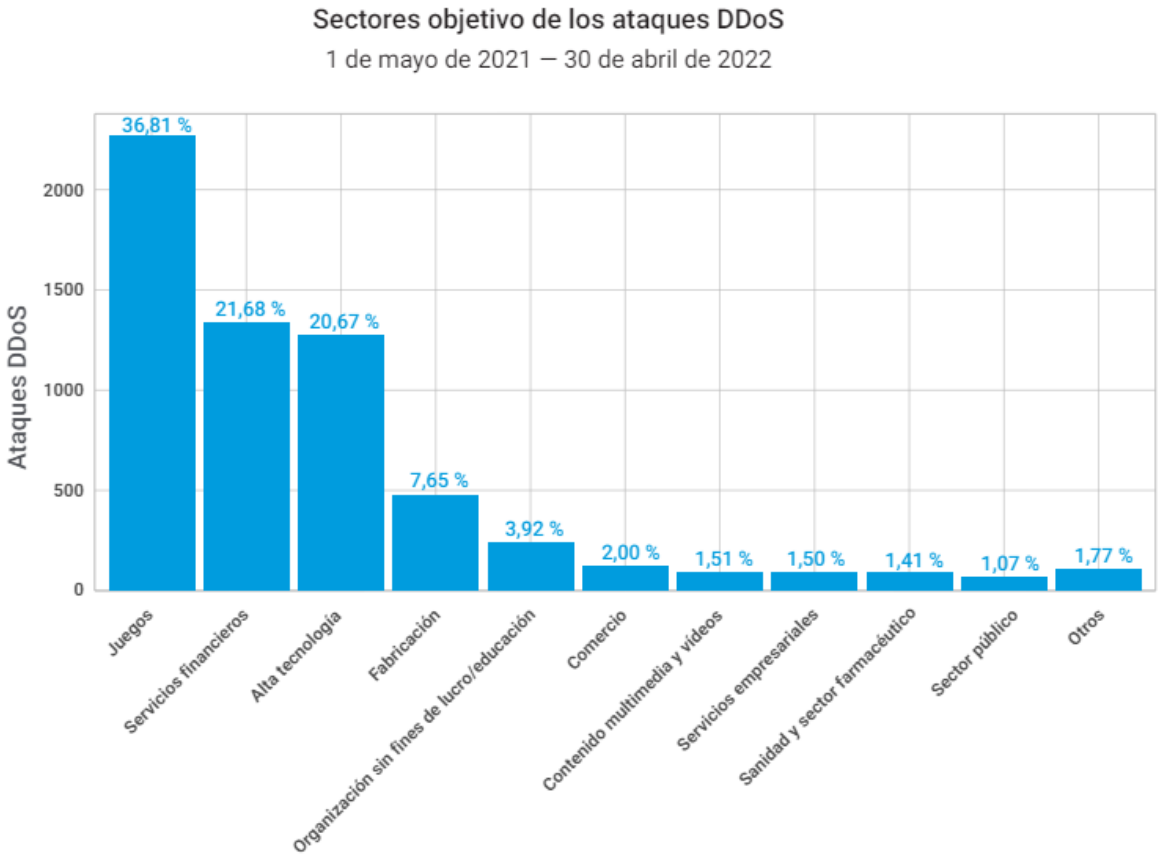

Figura 6-12. Atacs DDoS capturats del 2021 a 2022 per indústries. Font: Akamai, 2023.

Els atacs DDoS fan servir xarxes de bots (grup de dispositius infectats) i altres tècniques automatitzades per inundar els servidors de joc amb un gran nombre de sol·licituds. Aquestes tàctiques no només tenen el potencial d'empitjorar les connexions i els estats de les partides online, sinó també deixar inoperatius els serveis multijugador. Resultant en afectes molt perjudicials per el rendiment dels videojocs i les seves empreses, incrementant els costos i disminuint la satisfacció dels usuaris en veure l'experiència del videojoc frustrada.

Els atacs DDoS a la indústria dels videojocs han evolucionat en grandària i complexitat, afectant milers de jugadors en qüestió de segons o sent selectivament dirigits per augmentar la latència i atorgar avantatge a certs jugadors sobre altres. Segons l'informe d'Akamai (2023) la naturalesa d'aquests atacs es classifiquen principalment en tres tipus: volumètrics, de protocol i de capa d'aplicació. Cadascun té com a objectiu principal alentir o aturar completament el trànsit legítim per impedir que arribi als servidors finals, comprometent la disponibilitat dels recursos del viedeojoc i disminuint-ne el rendiment.

Hadji-Vasilev i Chapman (2024) esmenten que quan els atacs van dirigits a un jugador en específic, es busca que la seva experiència de joc sigui lenta i pràcticament injugable. Això succeeix quan l'atacant adquireix l'adreça IP del jugador, possiblement a través de malware que el jugador es descarrega de forma involuntària, i transmetent aquesta informació a l'atacant. Amb l'adreça IP, l'atacant utilitza una xarxa d'ordinadors infectats i bombardeja la xarxa del jugador amb peticions excessives. Actualment, és possible llogar aquestes xarxes mitjançant mercats negres.

El cas de Blizzard

Durant l'accés anticipat d'Overwatch 2 el dia 4 d'octubre de 2023, el videojoc va enfrontar-se a diversos problemes a causa d'un atac DDoS que va impedir als jugadors poder gaudir del títol uns dies abans del llançament global. Aquest incident va causar que nombrosos jugadors experimentessin llargues esperes en forma de cues virtuals per poder accedir al videojoc.

Els comentaris dels usuaris destaquen esperes molt significatives, amb alguns jugadors tenint fins a 40.000 persones a la cua davant d'ells. Però un cop superades aquestes cues, s'enfrontaven a freqüents desconnexions, obligant a molts a tornar a iniciar el procés de les cues virtuals.

El president de Blizzard, Mike Ybarra, va reconèixer que aquests problemes eren el resultat d'un "atac DDoS masiu". Va assegurar que els equips tècnics estaven enfocats en controlar i mitigar l'atac per a restablir el servei lo abans possible. (el-brujo, 2022).

6.3.4 Phising

L'ascens del phishing dins de la indústria dels videojoc no és un fenomen aïllat, sinó un reflex de l'evolució de les tècniques de ciberdelinqüència que busquen aprofitar-se de les plataformes amb gran afluència d'usuaris. Dins d'aquest àmbit, la interacció constant entre els jugadors i l'intercanvi freqüent de dades personals i financeres creen nombroses oportunitats per els atacants.

Les estafes de phishing en aquesta indústria sovint adopten diferents formes, des d'assegurar falses recompenses d'un videojoc fins a falses alertes de seguretat. Aquestes tàctiques són dissenyades per a enganyar els usuaris fent-los creure que estan interactuant amb serveis legítims, quan en realitat estan comprometent la seva seguretat i la dels seus comptes. Els atacants utilitzen l'aspecte visual i textual utilitzat per les comunicacions oficials, per aprofitant-se de la confiança i la expectativa dels jugadors.

El resultat d'aquestes estafes va més enllà de la pèrdua financera immediata o el robatori d'identitat. Els impactes psicològics i emocionals també són significatius, ja que els jugadors poden sentir-se traïts i vulnerables dins d'un espai que sovint consideren segur i acollidor. La repercussió sobre la reputació de les empreses de videojocs és considerable, ja que la confiança del consumidor és fonamental per a la retenció d'usuaris i la sostenibilitat econòmica a llarg termini.

L'objectiu principal d'aquests actors maliciosos és atraure els jugadors a fer clic en enllaços nocius o a introduir informació personal en llocs web falsificats que imiten plataformes de jocs autèntiques. Les webs solen demanar informació personal, credencials d'inici de sessió, dades de contacte i, de vegades, fins i tot la informació de pagament amb l'excusa de verificar la identitat del jugador o la propietat del compte.

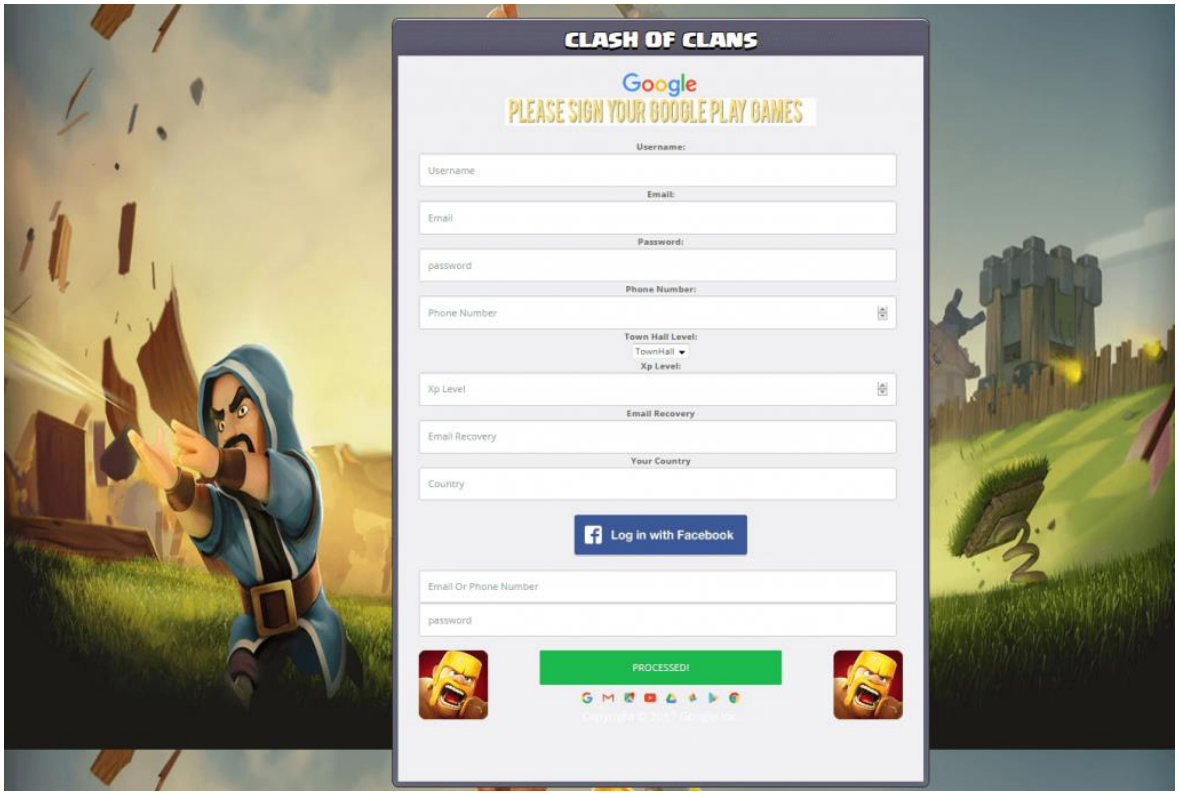

Figura 6-13. Web suplantant la web oficial del videojoc Clash of Clans. Font: Kostin, 2017.

Un cop enviada la informació, els ciberdelinqüents poden explotar-la de múltiples maneres. Les conseqüències directes poden anar des de l'accés no autoritzat al compte del jugador, que a conseqüència, condueix al robatori de recursos o fins a la venta del compte via mercats negres. A més, els enllaços maliciosos també poden servir com a vies per a la instal·lació de malware al dispositiu de la víctima, comprometent la integritat del sistema.

El cas de Roblox i la seva moneda Robux

El videojoc Roblox conegut per la seva gran base d'usuari de jugadors menors d'edat ha sigut el focus d'una gran quantitat d'atacs de phishing.

Una de les metodologies que més utilitzen els estafadors es l'enviament de missatges a través del propi xat del videojoc, dient que tenen una manera d'obtenir Robux (moneda del videojoc) de forma gratuïta. L'usuari rep un enllaç a una pàgina web amb temes e imatges relacionades amb Roblox on s'ofereixen Robux gratis i demana a l'usuari que introdueixi el seu nom d'usuari i contrasenya per rebre els Robux directament al seu compte. Després d'introduir les seves credencials, en lloc de rebre els Robux, l'estafador accedeix al compte de la víctima i roba tots els recursos de valor. Posteriorment el compte és utilitzat per difondre missatges per captar a més jugadors (Baker, 2024)

Figura 6-14. Ús de tècniques de phishing mitjançant bots en el xat del videojoc Roblox. Font: Roblox, 2006.

Un altre mètode d'estafa en línia son els que promouen ser generadors de Robux gratuïts. Aquests llocs web fraudulents atrauen els usuaris sol·licitant el seu nom d'usuari de Roblox i la quantitat desitjada de Robux que volen obtenir. Afirmen falsament connectar-se amb els servidors de Roblox per transferir Robux al compte de l'usuari, cosa que en realitat no passa. Després de simular la generació Robux, es demana als usuaris que completin un procés de verificació humà. Aquest pas

sovint implica veure vídeos de YouTube o fer clic a nombrosos anuncis. Completar aquestes accions només beneficia els estafadors, ja que generen ingressos publicitaris (Baker, 2024).

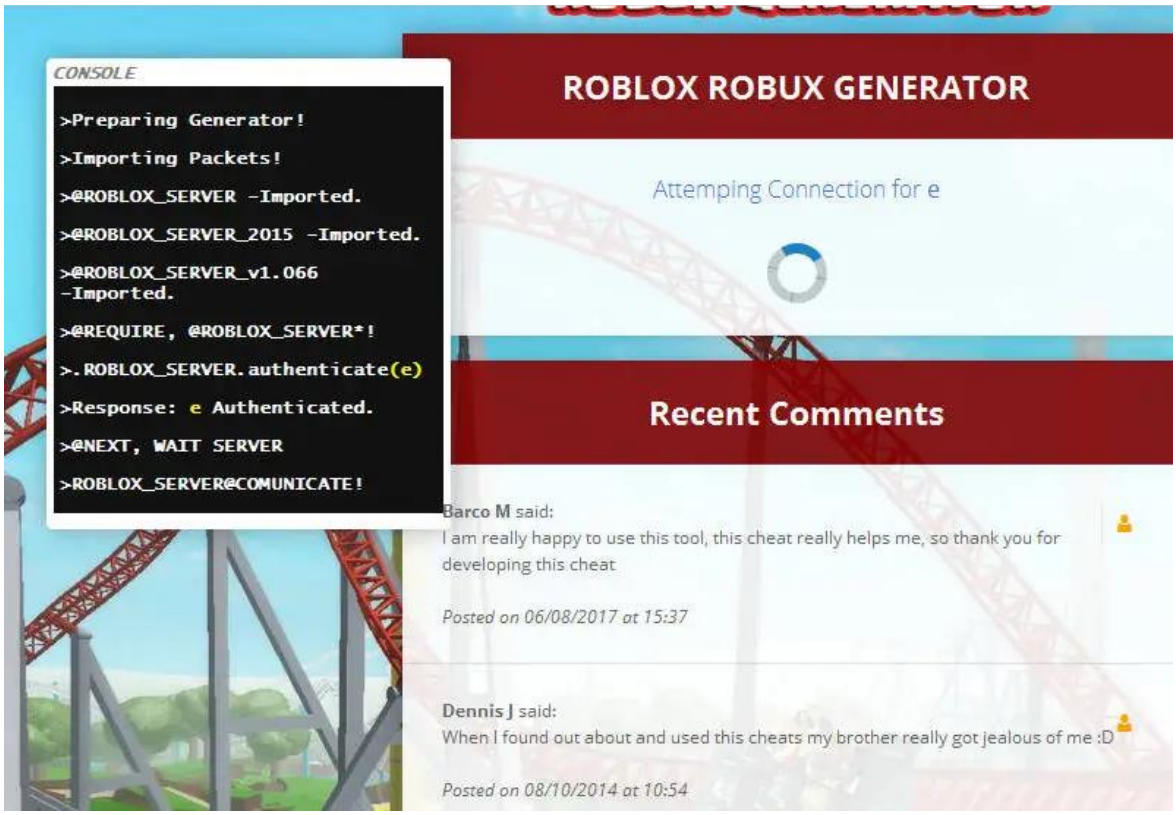

Figura 6-15. Web generadora de Robux. Font: Boyd, 2017.

Taxonomia de Phising orientat als jugadors

La taula següent ofereix una categorització detallada dels diferents tipus de phishing que afecten a la indústria dels videojocs:

Categoria	Mètode	Descripció
Plataforma	**Discord**	Missatges directes fraudulents, invitacions a servidors fraudulents no oficials.
	YouTube	Tutorials falsos, obtenció gratuïta d'objectes i recursos, enllaços de phishing.
	Twitter	Promocions falses, missatges directes, comptes de desenvolupadors falsos
	Reddit	Fils de phshing, comptes de desenvolupadors falsos
	Email	Promocions falses, sol·licituds de verificació de comptes falses, estafes de renovació de subscripcions, alertes de seguretat falses
	Facebook	Pàgines falses, publicacions amb links fraudulents, invitacions a grups maliciosos
	Instagram	Missatges directes amb links fraudulents, publicacions fraudulentes, comptes falsos
	Chat In-Game	Enllaços fraudulents, Suplantació de moderadors/equip de suport
	Marketplace	Articles falsos, suplantació de venedors oficials
	Webs	Webs generadores de recursos falsos, webs de descàrrega de videojocs gratuits, webs de registre de tornejos falsos, marketplace de recursos falsos
	Apps Mòvils	Anuncis amb links fraudulents, aplicacions fetes per tercers amb intencions malicioses, modificacions del videojoc, guies falses
	WhatsApp	Bots amb links maliciosos, comptes de suport falsos, grups fraudulents
	Telegram	Bots amb links maliciosos, grups fraudulents, comptes de suport falsos
	SMS	Codis de verificació falsos, codis promocionals falsos, links fraudulents
	Twitch	Enllaços fraudulents al xat, suplantació de streamer
	Mixer	Enllaços fraudulents al xat, suplantació de streamer

Metodologia	**Suplantació**	Representants de moderadors/equip de suport, Amics/companys d'equip, Desenvolupadors, Influencers o Streamers
	Ofertes	Monedes/recursos gratuïts, codis de descompte, invitacions a proves beta falses, ofertes d'accés anticipat falses, codis promocionals falsos
	Robatori de credencials	Pàgines d'inici de sessió falses, correus electrònics "Verifiqueu el vostre compte", sol·licituds falses d'autenticació de dos factors (2FA), formularis de recuperació de comptes falsos
	Malware	Enllaços maliciosos, descàrregues de videojocs gratuits, modificacions de videojocs, actualitzacions del videojoc per tercers, recursos gratuits del videojoc per tercers
Vectors d'atac	**Links**	Enllaços en xats/publicacions, enllaços en xarxes socials, enllaços de descàrrega, enllaços en les ressenyes
	Adjunts	Fitxers infectats per correu electrònic/missatge directe per xarxes socials, fitxers adjunts a fòrums, modificacions infectades, actualitzacions de tercers infectades, recursos de tercers infectats
	Enquestes	Registres d'accés a proves beta, formularis falsos d'opinions sobre videojocs, formularis de reclamació de premis falsos, formularis de recuperació de comptes
Phishing dirigit	**Streamers e Influencers**	Ofertes de patrocini falses, enllaços maliciosos, bots fent se passar per espectadors, avís del compte ha sigut compromès
	Jugadors amb gran quantitat de recursos de joc	Enllaços maliciosos, avís del compte ha sigut compromès, ofertes de recursos falses

Taula 6-5 Taxonomia de phishing orientada als jugadors de videojocs. Font: Elaboració pròpia.

6.3.5 Atacs a aplicacions web

A la indústria dels videojocs, els atacs a aplicacions web han augmentat degut a l'auge de les tecnologies cloud gaming, que permeten els usuaris jugar de manera remota a través d'internet, en lloc de fer-ho localment des d'un dispositiu com una consola o un ordinador personal. Amb el cloud gaming, els videojocs són executats en servidors remots i transmesos en temps real als dispositius dels jugadors. Segons Akamai (2022) ha hagut un augment del 167% entre maig de 2021 i abril de 2022 en comparació amb l'any anterior i 821 milions d'atacs durant aquest període.

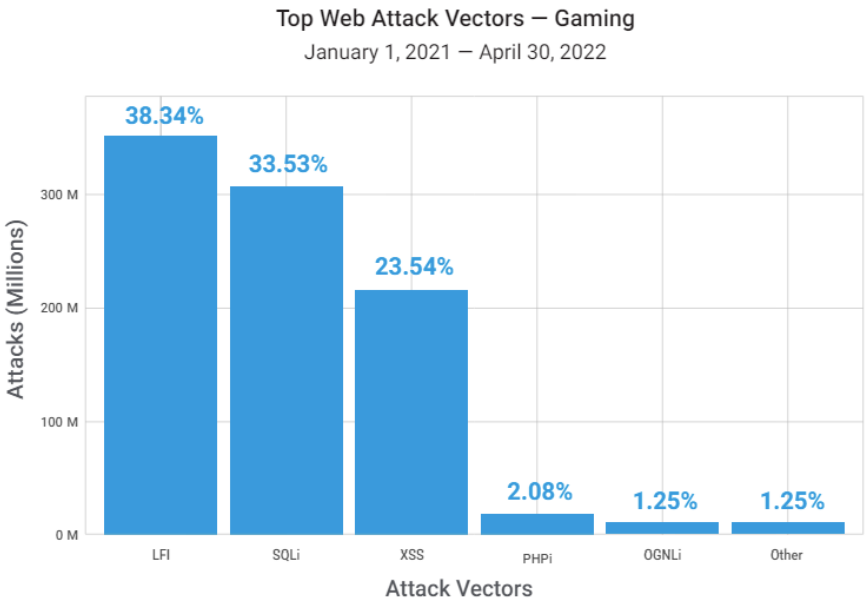

Figura 6-15. Tipus d'atac web registrats demtre el 2021-2022 a la indústria dels videojocs. Font: Akamai, 2022.

El gràfic extret de l'article d'Akamai (2022) exposa els atacs web més comuns on LFI (inclusió de fitxers locals) és el més utilitzat amb un 38,34%, aquests atacs busquen enganyar les aplicacions web perquè executin o exposin fitxers en els servidors. Aquesta vulnerabilitat permet els atacants introduir fitxers maliciosos als sistemes web (Didzar, 2021).

SQLi (injecció SQL) amb un 33,53%, suposa pels atacants interferir i modificar les accions que l'aplicació web fa a la seva base de dades. En manipular els camps d'entrada, els atacants poden veure, editar o suprimir dades només accessibles pels administradors de l'aplicatiu web (PortSwigger , s.d).

Els atacs XSS (Cross-Site Scripting) amb un 23,54% es donen quan es carreguen scripts amb funcionalitats malicioses cap els aplicatius web (Kirsten, s.d)

El cas de PHPi (injecció PHP) , OGNLi (injecció OGNL) entre d'altres resulten més minoritaris .

6.4 Empreses públicament afectades

En la següent taula s'exposen les empreses que han sigut víctimes d'atacs cibernètics i la tipologia d'atac que van patir, indiferentment de la seva mida o facturació:

Nom de l'empresa	Data de l'atac	Tipus d'atac	Detalls de l'atac
Sony (PlayStation Network)	Maig 2011	Exfiltració de dades	Intrusió externa que va comprometre les dades personals de 77 milions de comptes i va impedir l'accés als serveis als usuaris de PlayStation 3 i PlayStation Portable durant 23 dies
Bethesda (ZeniMax Media)	Juny 2011	Exfiltració de dades	La web va ser compromesa resultant amb el robatori de dades d'usuaris tot i que van assegurar que no es van comprometre dades financeres però els atacants van accedir a noms d'usuari, adreces de correu electrònic i contrasenyes.
Konami	Juliol 2013	Força Bruta	El portal Konami ID va ser compromès i més de 35,000 usuaris van ser afectats. L'atac es va dur a terme mitjançant intents d'inici de sessió per força bruta realitzats durant diverses setmanes, es van realitzar 3,945,927 intents, aconseguint-ho 35,252 vegades.
Digital Extremes	Novembre 2014	SQL exploit	Es van comprometre 775,749 adreces de correu electrònic a través d'un exploit SQL
Chucklefish	Desembre 2015	Exfiltració de dades	Els fòrums de l'empresa van ser objectiu dels atacants. Es van exposar noms d'usuari i correus electrònics. Els atacants també van eliminar dues grans seccions del fòrum: la secció 'Social', i la secció de discussió d'administradors/moderadors. Afortunadament, vam poder posar els fòrums fora de línia abans que poguessin eliminar-ho tot. La còpia de seguretat més recent era del març, cosa que va significar que tot el que hi havia entre aquelles dates es perdés.
Hello Games	Juliol 2016	Phishing	Els atacants van comprometre els comptes de X i correu elctrònic de la desenvolupadora penjant a les xarxes posts ofensius.
Supercell	Gener 2017	Exfiltració de dades	Els atacants van robar les credencials d'un milió de comptes d'usuari registrats al seu fòrum. Es van exposar noms d'usuari, correus electrònics i contrasenyes.
Zynga	Setembre 2019	Exfiltració de dades	El hacker conegut com Gnosticplayers va explotar una vulnerabilitat en els sistemes de Zynga, accedint a la base de dades dels jugadors que van instal·lar Words With Friends. L'atac va exposar detalls d'inici de sessió, adreces de correu electrònic, noms d'usuari i contrasenyes.
Ubisoft	Gener 2020	DDoS	Es van llançar diferents atacs DDoS orientats cap els servidors del videojoc Rainbow Six Siege
Nintendo	Maig 2020	Exfiltració de dades	Codi font de les consoles de Nintendo i videojocs van ser publicats als fòrums de 4chan
Innersloth	Setembre 2020	Phishing	Les lobbies del videojoc Among Us s'omplien de bots que enviaven missatges de manera continuada. La majoria dels missatges intentaven coaccionar els usuaris perquè es subscrivissin a canals de YouTube sota l'amenaça de destruir el seu dispositiu. Els enllaços també redirigien a Discord i Twitter.

Capcom	Novembre 2020	Ransomware	L'atac de ransomware Ragnar Locker va comprometre la informació personal dels empleats i clients.
CD Projekt Red	Febrer 2021	Ransomware	Els hackers van robar el codi font de Cyberpunk 2077 i The Witcher 3, van exigir un rescat i van filtrar les dades en línia.
Electronic Arts (EA)	Juny 2021	Exfiltració de dades	Els hackers van accedir a la xarxa d'EA mitjançant una vulnerabilitat relacionada amb les cookies d'autenticació, robant el codi font de FIFA 21 i el motor Frostbite.
Roblox Corporation	Juliol 2021	Exfiltració de dades	L'atac va afectar principalment els assistents a conferències de desenvolupadors de Roblox entre 2017 i 2020. Aproximadament 3.943 comptes van ser compromesos. Les dades exposades eren noms, noms d'usuari, números de telèfon, correus electrònics, adreces IP, adreces, dates de naixement i talles de samarretes.
Blizzard	Maig 2022	DDoS	L'atac va ser dirigit a la plataforma Battle.net. Aquest incident va provocar que alguns jugadors experimentessin alta latència i desconnexions en jocs com Call of Duty, Overwatch, Starcraft, World of Warcraft, Diablo i Hearthstone.
Bandai Namco	Juliol 2022	Ransomware	L'atac de ransomware BlackCat va permetre l'accés no autoritzat a sistemes interns i l'exfiltració de dades de diverses empreses del grup asiàtic.
Square Enix	Setembre 2022	Suplantació	Es va intentar accedir als comptes de Square Enix utilitzant una combinació de credencials d'altres serveis en línia d'altres companyies.
Rockstar Games	Setembre 2022	Phishing/Exfiltració de dades	El codi font i vídeos del GTA VI es van filtrar per un atacant del grup Lapsus$ utilitzant tècniques de phishing.
2K Games	Setembre 2022	Phishing	Els atacants van obtenir il·legalment credencials d'un dels seus proveïdors, utilitzant la seva plataforma de suport per enviar comunicacions malicioses a alguns jugadors.
Riot Games	Gener 2023	Phishing	Els empleats van ser enganyats per proporcionar accés, resultant en el robatori del codi font del videojoc League of Legends, TFT i de la plataforma anti trampes utilitzada
Valve Corporation	Setembre 2023	Phishing/Malware	Es van comprometre comptes de Steam de diversos desenvolupadors de videeojocs i es va oferir malware en comptes dels videojocs
Gellyberry Studios	Novembre 2023	Ransomware	Els sistemes interns de l'estudi van ser encriptats per un ransomware, provocant que el progrés de més de 17.000 usuaris es perdés

Ubisoft	Desembre 2023	Exfiltració de dades	L'atacant va realitzar un intent de filtració de 900 GB de dades relacionades amb el videojoc Rainbow Six Siege, va estar en els sistemes durant 48h
Obsidian Entertainment	Desembre 2023	Exfiltració de dades	Va ocòrrer a la web Obsidian.net, la plataforma en línia d'Obsidian Entertainment. Es van comprometre dades emmagatzemades i incloïen principalment correus electrònics.
Insomniac Games	Desembre 2023	Ransomware	El grup criminal Rhysida va comprometre l'empresa amb un ransomware, van aconseguir captar 1'67TB de dades i 1'3 milions de fitxers de desenvolupament, documents de disseny i centenars d'empleats van tenir les seves dades exposades.
Activision Blizzard	Març 2024	Phishing/Malware	Els atacants van aconseguir prendre el control del compte de X i van publicar un missatge per promoure una suposada criptomoneda juntament amb una imatge de Crash Bandicoot.
Grinding Gear Games	Maig 2024	Phishing	Es va comprometre la pàgina de Steam de Path of Exile. Es va publicar un link amb continguts maliciosos

Taula 6-5 Llistat d'empreses que han tingut atacs cibernètics. Font: Elaboració pròpia.

6.5 Model Web per a la Gestió de Vulnerabilitats

Moltes de les amenaces de ciberseguretat i tipus d'atac, com l'exfiltració de dades o el ransomware, es duen a terme a causa d'una gestió inadequada dels sistemes i programes informàtics ja que presenten diverses vulnerabilitats. Per abordar aquesta problemàtica, es proposa la creació d'un model a replicar en forma de base de dades que ajudi les empreses a gestionar les vulnerabilitats dels seus sistemes de manera eficient i centralitzada.

Aquest model d'exemple està publicat en format web a l'adreça URL: https://mbadal.pythonanywhere.com/

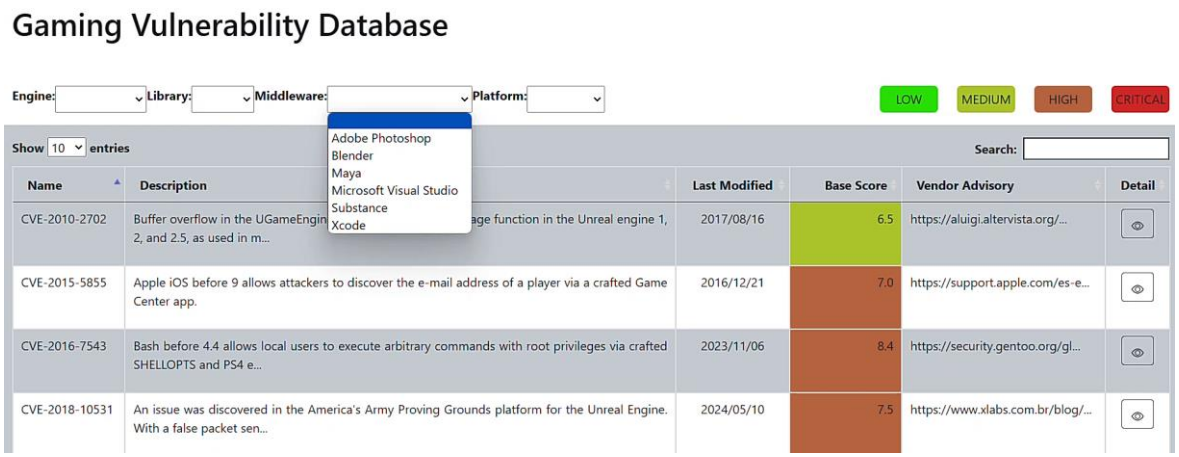

Figura 6-16. Model proposat per gestionar les vulnerabilitats de les empreses de videojocs. Font: Elaboració pròpia.

El model funciona com una base de dades de vulnerabilitats que afecten específicament a l'empresa, permetent identificar-les i gestionar-les.

Aquesta eina està basada en les vulnerabilitats tipus CVE (Common Vulnerabilities and Exposures), un estàndard àmpliament utilitzat a la indústria de la ciberseguretat per facilitar el seguiment d'aquestes entre diferents organitzacions.

Una de les funcionalitats principals d'aquesta base de dades son els filtres que estan dissenyats per ajudar a personalitzar segons els sistemes i tecnologies específiques que utilitza cada empresa, cosa que facilita una gestió més enfocada de les vulnerabilitats.

En el cas de la web d'exemple s'ha simulat una empresa que utilitza els següents sistemes: Motor de Joc (Engine), Llibreries (Libraries), Middleware i Plataforma (Platform).

Per cada filtre hi ha un desplegable, en el cas de Middleware s'ha simulat una empresa que utilitza Adobe Photoshop, Blender, Maya, Microsoft Visual Studio, Substance i Xcode.

La web mostra les vulnerabilitats trobades per el programari seleccionat.

Visualitzar Detalls:

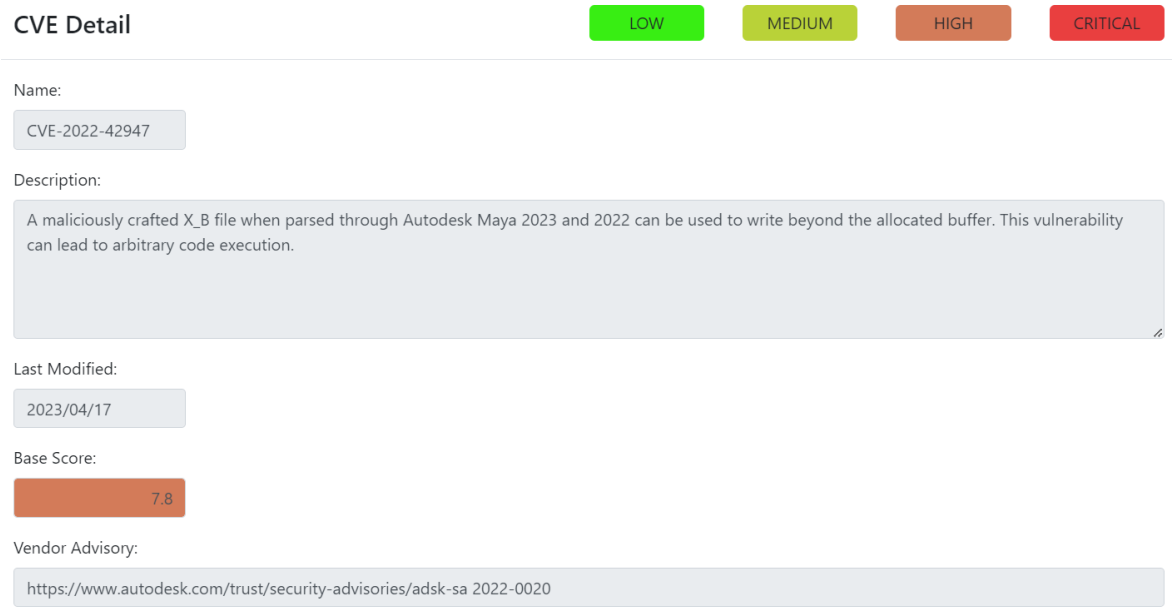

Figura 6-17. Detalls de la vulnerabilitats amb identificador CVE-2022-42947 del programa Maya. Font: Elaboració pròpia.

La imatge proporcionada mostra un exemple de com es presenta el detall d'una vulnerabilitat:

Nom (Name): Cada vulnerabilitat té un identificador únic, en aquest cas, CVE-2022-42947. Aquest identificador segueix l'estàndard CVE (Common Vulnerabilities and Exposures), cosa que permet una referència i gestió eficient de la vulnerabilitat.

Descripció (Description): Es proporciona una descripció detallada de la vulnerabilitat.

Última Modificació (Last Modified): Indica la data de la darrera modificació de la vulnerabilitat. Això ajuda els usuaris a saber com de recent és la informació i si hi ha hagut actualitzacions recents.

Puntuació Base (Base Score): Mostra la severitat de la vulnerabilitat utilitzant el sistema Common Vulnerability Scoring System (CVSS).

Assessoria del Proveïdor (Vendor Advisory): Es proporciona un enllaç a la pàgina d'assessorament del proveïdor o d'un tercer, que ofereix detalls addicionals i possibles solucions per a la vulnerabilitat.

Cada vulnerabilitat i els seus detalls han sigut exportades del repositori de CVE.MITRE, organització que crea, cataloga i gestiona les vulnerabilitats.

7. Conclusions i línies de futur

Aquest treball ha nascut de la necessitat d'abordar una temàtica que actualment cada cop més està tenint més impacte, un sector que anualment s'enfronta a milers d'atacs afectant tant a les empreses com els seus usuaris més fidels.

7.1 Conclusions

Un dels objectius principals del treball ha estat l'anàlisi i documentació dels principals mecanismes de defensa que hi ha en la indústria dels videojocs. Per fer-ho, s'ha realitzat una revisió de la documentació existent, analitzant diferents estudis e informes tant del sector dels videojocs com d'altres indústries. Aquesta anàlisi ha permès identificar i comprendre les diverses estratègies disponibles per combatre les amenaces cibernètiques que afecten a la indústria.

Tot i que actualment hi ha una gran quantitat de mesures de defensa implementades en la indústria dels videojocs, és evident que aquestes no són suficients per garantir una protecció total. Malgrat les inversions substancials en ciberseguretat de les empreses triple A, avui en dia continuen sent compromeses per atacs cibernètics. Aquest fet posa en manifest la necessitat d'una millora contínua i l'adopció de noves estratègies de defensa. A més, les dades indiquen que la situació només empitjora, ressaltant encara més aquesta problemàtica. Els atacs cibernètics afecten tant a les grans empreses triple A com a les petites empreses indies, significant que la ciberseguretat és una preocupació universal independentment de la mida o el tipus d'empresa.

Les empreses han de reconèixer que la ciberseguretat és un procés continu i dinàmic. Les amenaces evolucionen constantment, i els atacants desenvolupen noves tècniques per superar les defenses existents. Per tant, és crucial que les empreses no només implementin mesures de seguretat, sinó que també mantinguin una cultura de ciberseguretat proactiva.

En el treball s'ha proposat un mètode que subratlla la importància de la cultura de ciberseguretat com una mesura imprescindible per reduir la probabilitat de ser vulnerats. La cultura de ciberseguretat no només implica la implementació de

tecnologies avançades, sinó també la formació contínua i la conscienciació dels empleats sobre les amenaces cibernètiques. Com s'ha exposat en la taula d'empreses compromeses, moltes d'elles podrien haver evitat incidents greus si haguessin adoptat aquesta mesura cultural. Un exemple notable és el cas de Riot Games, que va patir un atac de phishing i enginyeria social dirigit als seus empleats. Aquest incident podria haver estat evitat amb una formació adequada i una cultura de seguretat robusta. Així, el treball posa de manifest que, per aconseguir una protecció efectiva contra les ciberamenaces, les empreses han de fomentar una cultura de seguretat integral que involucri tots els nivells de l'organització.

Pel que fa a les tendències d'atac, s'ha observat que el nombre de casos relacionats amb malware està augmentant considerablement. En particular, la tendència actual mostra un increment del tipus Downloader. Aquest tipus de malware té com a objectiu evadir els sistemes antivirus dels jugadors i que el jugador executi el programa maliciós instal·lat fent-se passar per benigne. Això permet als atacants instal·lar altres tipus de malware o spyware amb més facilitat, posant en risc tant les dades personals dels jugadors com la integritat dels sistemes de les empreses.

Aquest tipus de malware sovint es presenta com un arxiu legítim o una modificació, fent que els usuaris siguin més propensos a executar-lo sense sospitar.

Un exemple clar d'aquesta situació és el cas de la plataforma no oficial TLauncher, que, un cop analitzat, s'ha observat que a part de permetre jugar al videojoc Minecraft de forma gratuïta, té un propòsit maliciós. Milers d'usuaris s'han descarregat TLauncher sense saber que inclou funcions com l'espionatge o la descàrrega d'arxius troians. Això demostra com els atacants utilitzen programes aparentment inofensius per infectar els sistemes dels usuaris.

Un altre tipus de malware en auge és el ransomware, que afecta molt notablement a les empreses. Segons els casos públics de l'últim any 2023, hi ha hagut diversos incidents notables, com es el cas de les empreses Insomniac Games i Gellyberry Studios. Aquest tipus de malware encripta les dades i exigeix un rescat per alliberar-les, causant grans pèrdues econòmiques i operatives. Els atacs de ransomware demostren la necessitat urgent de sistemes de còpies de seguretat, plans de resposta a incidents ben definits per mitigar els danys o assegurances cibernètiques per cobrir l'impacte econòmic.

Els atacs DDoS (Denegació de Servei Distribuït) s'han observat amb gran freqüència en la indústria dels videojocs, fet que segons les dades observades es tracte de la indústria amb més casos registrats superant la indústria de serveis financers amb un 15,13% més de casos. Un exemple notable és el cas d'Activision Blizzard amb el seu videojoc Overwatch 2, on el dia d'accés anticipat, els jugadors van experimentar una qualitat de servei molt pobre o pràcticament nul·la a causa d'un atac DDoS. Els efectes d'aquests atacs poden ser devastadors, ja que no només afecten l'experiència del jugador, sinó que també poden danyen la reputació de l'empresa, provocar pèrdues econòmiques significatives entre d'altres. Això remarca la importància de tenir mesures anti DDoS efectives per protegir-se contra aquests atacs.

El phishing, tal com es coneix, consisteix a enganyar els usuaris perquè revelin informació sensible, com les credencials dels seus comptes de joc o dades financeres, mitjançant diferents metodologies com l'enviament de missatges falsos que semblen provenir de fonts fiables. La importància que les empreses es preocupin pels seus jugadors és especialment rellevant en casos com el de Roblox, on la base d'usuaris majoritària és de menors d'edat. Aquest grup és particularment vulnerable als atacs de phishing i altres formes de manipulació. Per això, és fonamental que les empreses implementin mesures educatives i tecnològiques per protegir aquests usuaris joves, incloent programes de conscienciació sobre ciberseguretat i millorar les seves tecnologies per desenvolupar filtres avançats per detectar i bloquejar qualsevol intent de phishing. Mitjançant aquest treball s'ha pogut exposat les diverses plataformes i metodologies emprades per dur a terme atacs de phishing dirigits als jugadors.

A través de la recopilació d'incidents públics que han afectat la indústria dels videojocs, es pot observar una tendència creixent en l'ús de l'extorsió per part dels atacants. L'extorsió es defineix com l'acte d'obtenir alguna cosa, especialment diners, mitjançant l'ús de la força o amenaces. En el context de la ciberseguretat, això sovint implica l'exfiltració de dades, on els atacants s'infiltren als sistemes per robar materials sensibles de l'empresa i després exigir un rescat per no fer públiques aquestes dades o per retornar-les.

Un exemple destacat d'aquesta tendència és el cas del molt esperat videojoc Grand Theft Auto VI. Els atacants van robar informació i materials de desenvolupament, posant en risc la seguretat i la reputació de l'empresa. Aquest incident il·lustra clarament com els ciberdelinqüents utilitzen l'extorsió per treure profit de les empreses de videojocs, destacant la necessitat urgent de millorar les mesures de seguretat cibernètica en aquesta indústria. La majoria de casos d'infiltració a les empreses es deuen a atacs de phishing o a l'explotació de vulnerabilitats en els sistemes, com en es cas de Bethesda, on els atacants es van aprofitar de vulnerabilitats web i van accedir a informació confidencial. És per això que un dels propòsits d'aquest treball ha sigut desenvolupar un model a replicar que ajudi a les empreses a controlar les vulnerabilitats dels aplicatius i sistemes que utilitzen.

Aquest model permet a les empreses la capacitat de tenir el coneixement centralitzat de les vulnerabilitats que van sorgint, únicament dels sistemes que posseeixen, per tal de poder realitzar contramesures més ràpidament. Això millora la capacitat de resposta davant de possibles atacs, minimitzant els riscs i protegir millor la informació sensible de l'empresa.

7.2 Línies de futur

Un cop realitzada aquesta investigació s'han detectat diversos camins a seguir per ampliar la temàtica d'aquest estudi, que a continuació s'exposen:

- **Estudi Comparatiu entre Sectors**: Comparació de les pràctiques de ciberseguretat en la indústria dels videojocs amb altres sectors per identificar oportunitats de millora i adopció de millors pràctiques.

- **Formació i Conscienciació dels Usuaris:** Investigació de l'efectivitat dels programes de formació en ciberseguretat per els empleats i jugadors.

- **Col·laboració Internacional**: Estudiar la col·laboració entre els diferents països i les diverses empreses de videojocs per millorar la resposta global a les ciberamenaces.

8. Referències

Akamai (s.d.) *Gaming Respawned. Cyberattacks on Players and Gaming*

Baker. K (2024). *ROBLOX SCAMS: WHAT PARENTS NEED TO KNOW*. IdentityIQ. Recuperat de: https://www.identityiq.com/scams-and-fraud/roblox-scams-what-parents-need-to-know/

Boyd. C (2017) *The Roblox Robux generator is too good to be true*. MalwareBytes. Recuperat de: https://www.malwarebytes.com/blog/news/2017/06/the-roblox-robux-generator-is-too-good-to-be-true

CVE Recuperat de: https://cve.mitre.org/

Chapman. S, Hadji-Vasilev. A (2024). *What Is DDoS in Gaming? Cyber Attacks on Gamers in 2024*. Cloudwars. Recuperat de: https://www.cloudwards.net/what-is-ddos-in-gaming/

Companies Rise Again. Recuperat de: https://www.akamai.com/resources/state-of-the-internet/soti-security-gaming-respawned

Cluley. G (2023). *Ethyrial: Echoes of Yore hacked! 17,000 game accounts "lost"*. Bitdefender. Recuperat de: https://www.bitdefender.com/blog/hotforsecurity/ethyrial-echoes-of-yore-hacked-17-000-game-accounts-lost/

Cheatseller. (s.d.) Recuperat de: https://cheatseller.com/

Davis, S. B., & Price, W. J. (2008). *Security issues for third party games : Technical , business and legal perspectives*. 24, 163–168. . https://doi.org/10.1016/j.clsr.2008.01.004

Digital rights management (DRM). PCGamingWiki. Recuperat de: https://www.pcgamingwiki.com/wiki/Digital_rights_management_(DRM)

El-brujo (2015). *TeslaCrypt, una variante del ransomware CryptoLocker que si puede ser descifrado*. Elhacker.net. Recuperat de: https://blog.elhacker.net/2015/05/teslacrypt-una-variante-del-ransomware-cryptolocker-que-si-puede-ser-decifrado.html

El-brujo (2022). *El videojuego OverWatch 2 sufre un ataque DDoS el día de su estreno*. Elhacker.net. Recuperat de: https://blog.elhacker.net/2022/10/el-videojuego-overwatch-2-sufre-un-ataque-ddos-blizzard.html

Erard. G (2023). *Insomniac Games habría sido hackeado: amenazan con filtrar detalles de 'Wolverine' y datos de los empleades.* Hipertextual. Recuperat de: https://hipertextual.com/2023/12/insomniac-games-hackeo-filtracion-wolverine

Didzar. A (2021). *Atac LFI: atacs de la vida real i exemples d'atac*. Bright. Recuperat de: https://brightsec.com/blog/lfi-attack-real-life-attacks-and-attack-examples/

Fraguela, N (2024, gener). *El número de usuarios de internet en el mundo crece un 1,8% y alcanza los 5.350 millones (2024).* Marketing4eCommerce. Recuperat de: https://marketing4ecommerce.net/usuarios-de-internet-mundo/

Henry.J (2023, Novembre) *Ethyrial: Echoes of Yore' MMORPG Ransomware Attack Deletes 17,000 Player Accounts, In-Game Items.* TechTimes. Recuperat de: https://www.techtimes.com/articles/299178/20231128/ethyrial-echoes-yore-mmorpg-ransomware-attack-deletes-17-000-player.htm

Hollingworth. D (2023). *Spider-Man 2 developer Insomniac Games hit by Rhysida ransomware attack*. Cyberdaily.au. Recuperat de: https://www.cyberdaily.au/culture/9931-spider-man-2-developer-insomniac-games-hit-by-rhysida-ransomware-attack

Huang. K, Pearlson. K (2019). *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture*. Massachusetts Institute of Technology. Recuperat de: https://web.mit.edu/smadnick/www/wp/2019-02.pdf

Jeff Yan, J. and Choi, H. (2002), *Security issues in online games*, The Electronic Library, Vol. 20 No. 2, pp. 125-133. https://doi.org/10.1108/02640470210424455

Kaspersky (2023). *Gaming-related cyberthreats in 2023: Minecrafters targeted the most*. Securelist. Recuperat de: https://securelist.com/game-related-threat-report-2023/110960/

Kaspersky (2022). *Good game, well played: an overview of gaming-related cyberthreats in 2022*. Securelist. Recuperat de: https://securelist.com/gaming-related-cyberthreats-2021-2022/107346/

Kirsten. S (s.d) *Cross Site Scripting (XSS).* Owasp. Recuperat de: https://owasp.org/www-community/attacks/xss/

Kostin. A (2017). *Clash of Greed*. Securelist. Recuperat de: https://securelist.com/clash-of-greed/78271/

Lehtonen, S. J. (2020). *Comparative Study of Anti-cheat Methods in Video Games.* (Treball fi de Màster). Universitat de Helsinki. Finlàndia.

Madnick, B., Huang, K., & Madnick, S. (2023). *The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process*. Information Security Journal: A Global Perspective, 1-22. https://doi.org/10.1080/19393555.2023.2201482

MITRE (2017). *Modify Registry*. Attack.Mitre. Recuperat de: https://attack.mitre.org/techniques/T1112/

MITRE (2020). *Subvert Trust Controls: Install Root Certificate*. Attack.Mitre. Recuperat de: https://attack.mitre.org/techniques/T1553/004/

Mosharrof. S (2020). *Intellectual Property Rights and the Game Industry.* (Treball fi de Màster). Universitat d'Uppsala. Suècia.

National Archives (2013). *PART 312—CHILDREN'S ONLINE PRIVACY PROTECTION RULE.* National Archives Recuperat de: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

Newzoo (2024) Newzoo's Global Games Market Report 2023 | May 2024 Update. Recuperat de: https://newzoo.com/resources/trend-reports/newzoo-global-games-market-report-2023-free-version

NIST (2024, Febrer). *The NIST Cybersecurity Framework (CSF) 2.0* . NIST. https://doi.org/10.6028/NIST.CSWP.29

Olivo,S (2020, Maig). *Ni siquiera los menores se libran del phishing: ¡Cuidado con el anzuelo de Fortnite!*. Escudo Digital. Recuperat de: https://www.escudodigital.com/ciberseguridad/ni-siquiera-los-menores-se-libran-del-phishing-cuidado-con-el-anzuelo-de-fortnite_11732_102.html

Pereira. T. *Attackers use JavaScript URLs, API forms and more to scam users in popular online game "Roblox."* (2023, Novembre). Cisco Talos Blog. Recuperat de: https://blog.talosintelligence.com/roblox-scam-overview/

Politowski, C., Petrillo, F., Ullmann, G. C., & Guéhéneuc, Y. G. (2021). *Game industry problems: An extensive analysis of the gray literature*. Information and Software Technology, 134, 106538. https://doi.org/10.1016/j.infsof.2021.106538

PortSwigger (s.d.) *SQL injection* Recuperat de: https://portswigger.net/web-security/sql-injection

Steam (2023) *Ethyrial: Echoes of Yore*. Recuperat de: https://store.steampowered.com/app/1277920/Ethyrial_Echoes_of_Yore/?l=latam

Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). *AVARCIBER: a framework for assessing cybersecurity risks*. Cluster Computing, 23, 1827-1843. Doi: 10.1007/s10586-019-03034-9

Sharron, M (2024, Maig). *Introduction to ISO 27001 in the Gaming Industry.* Recuperat de: https://www.isms.online/sectors/iso-27001-for-the-gaming-industry/

Strebeck, Z (s. d.) *GDPR Compliance for Game Companies.* Zachary Strebeck Recuperat de https://strebecklaw.com/gdpr-compliance/

Video Game Market. (Agost 2023). Precedence Research. Recuperat de https://www.precedenceresearch.com/video-game-market

Vang, P. Upson, Kelvin (2023) 3 Layers of Cyberspace Domain. Course Sidekick. Recuperat de: https://www.coursesidekick.com/computer-science/3277837

Wen, S., Kianpour, M., & Kowalski, S. (2019). *An Empirical Study of Security Culture in Open Source Software Communities*. 863–870. https://doi.org/10.1145/3341161.3343520

Zscaler (2023). *Ransomware Attacks on the Gaming Industry*. Recuperat de: https://www.zscaler.com/resources/solution-briefs/ransomware-attacks-gaming-industry.pdf