UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Università degli Studi di Brescia
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE
Corso di Laurea Magistrale in Ingegneria Informatica

Descrizione, Analisi e Mitigazione Delle Più Comuni Minacce Nei Videogiochi MMORPG

Axel Mastroianni
Prof. Federico Cerutti

Contents

Chapter 1

Introduzione

In questo capitolo verrà illustrato il motivo per cui si è deciso di intraprendere il lavoro presentato, qual è il suo scopo e come si è deciso di conseguirlo.
Come emerge da un paper recente, datato 2019, i videogiocatori online risultano scarsamente consapevoli dei rischi in cui vanno ad incorrere mentre giocano ai popolari MMORPGs (Massive Multiplayer Online Role Play Game). Il recente avvento della pandemia ha inoltre contribuito ad aumentare il numero di queste persone, come emerge da questa fonte, e, di conseguenza, ha aumentato anche il numero di malintenzionati e le possibilità che le loro azioni vadano a buon fine. A concludere la panoramica rientra la nutrita percenutale di pubblico giovane che, stando a questo report di un anno fa, risulta per il 51% sotto i 34 anni di cui quasi la metà sono minorenni.

Tutto questo background rende quindi necessaria una maggiore sensibilizzazione dei giocatori online rendendoli consapevoli di quali siano i rischi in cui possono incorrere mentre giocano.

Saranno quindi fornite delle possibili mitigazioni che possono aiutare ad evitare di essere vittima di un malintenzionato per quanto riguarda le minacce più insidiose come il Phishing o la costruzione di relazioni fasulle che puntano ad estorcere informazioni personali dal giocatore o a compiere azioni che vadano a beneficio di colui che le perpetra.

Il lavoro presentato si propone di raggiungere questo scopo presentando in prima istanza un elenco di 14 minacce in cui si può incorrere giocando online in modo da instillare un primo livello di consapevolezza nel lettore.

Procederà poi in una più attenta analisi di 3 minacce valutate come le più insidiose tra le 14 presentate.
Infine, sarà possibile consultare le due appendici in cui è presentato il motivo per cui le 3 minacce sono state valutate come più insidiose rispetto alle altre.

Chapter 2

Minacce

Di seguito vengono riportate 14 minacce in cui si può incorrere giocando agli MMORPG. Queste ultime sono corredate da una breve descrizione e sono reperibili in forma più completa al sito web del Mitre Att&ck per quanto riguarda la sicurezza in ambito aziendale. In questo documento verrà presentata una loro applicazione in ambito videoludico.
Di ogni minaccia sarà inoltre riportato il relativo score CWSS (Common Weakness Scoring System), che indica con che priorità una minaccia vada tenuta in considerazione, con una breve spiegazione volta a motivarlo.

2.1 Lista Minacce

1. **Raccogliere Informazioni Riguardo l'Identità della Vittima**: questa minaccia è utilizzata per costruire un profilo della vittima da sfruttare, ad esempio, per attacchi di Spearphishing. Queste informazioni si possono ottenere attraverso email di Phising, data breaches o instaurando una relazione con la vittima (ad esempio creando un personaggio per costruire una relazione di fiducia con la vittima). **Lo score CWSS** di questo attacco è pari a 72.3 per via della facilità con cui l'attaccante può provare a compierlo, del moderato livello di Social Engineering richiesta, della facilità con cui un malintenzionato può scoprirne l'esistenza e della sua diffusione. Lo score si abbassa per via della presenza di altri mezzi più diffusi con cui ottenere queste informazioni come **Creare un Account**.

2. **Creare un Account**: l'avversario crea un account sul videogioco e lo usa per trarre in inganno la vittima, ad esempio proponendo falsi scambi di oggetti rari o instaurando una vera e propria relazione di "amicizia" con la vittima al fine di ottenerne le credenziali di accesso. **Lo score CWSS** di questa minaccia è pari a 86.5 per via dell'estrema facilità con cui è possibile iniziarlo, è sufficiente, infatti, avere una connessione a internet e creare un account. Di conseguenza questa minaccia è anche molto diffusa. L'unico contro è che richiede un alto livello di Social Engineering in quanto l'attaccante deve interagire con la vittima per conoscerne i bisogni.

3. **Compromettere un account**: l'avversario in questo caso entra in possesso di un account già esistente che ha già costruito relazioni con altri personaggi e lo utilizza per trarre in inganno altri giocatori o per rovinare la reputazione del possessore dell'account. Può richiedere che l'avversario studi in prima istanza il comportamento del possessore di quell'account. **Lo score CWSS** di questa minaccia è pari a 69.0 per via della media difficoltà che richiede all'inizio, ossia entrare in possesso delle credenziali dell'account. Contribuiscono ad alzare lo score la sua efficacia nel caso lo si riesca a portare a termine e la possibilità di consultare data breaches o sfruttare il phishing per ottenere le informazioni necessarie a compromettere l'account.

4. **Relazione Di Fiducia**: l'avversario instaura una relazione di fiducia con la vittima o una persona che la conosce per avere più informazioni da sfruttare contro di essa o avere più indizi su quali potrebbero essere le sue credenziali di accesso o, ancora, per ottenere dei favori all'interno del videogioco che gli portano considervoli vantaggi (es. costruire una finta relazione amorosa online). **Lo score CWSS** di questa minaccia è pari a 72.7 per via della facilità con cui è possibile creare un account e iniziare così a costruire una relazione con la vittima. Contribuisce a diminuire lo score la necessità per l'attaccante di un'elevata operazione di social engineering e quindi una minor propensione alla scelta di questa strada oltre al fatto di essere un sottoinsieme sia di **Compromettere un Account** in quanto si può usare un account già esistente per creare la relazione di fiducia, sia di **Creare un Account**.

5. **Utilizzo di Account Validi**: molto simile a **Creare un Account** questa minaccia consiste nella possibilità dell'avversario di utilizzare

l'account di un Game Master o un Game Sage per avere maggiori privilegi all'interno del videogioco compresa la possibilità di richiedere consulenze a pagamento ad altri giocatori sfruttando l'autorità dell'account. **Lo score CWSS** di questa minaccia è pari a 86.5 per gli stessi motivi di **Creare un Account** con l'unica difficoltà di riuscire a spacciarsi per un Game Master invece che puntare a instaurare relazioni con la vittima.

6. **Utilizzare Metodi Alternativi di Autenticazione**: l'avversario può accedere al videogioco online non solo con i classici username e password ma anche rubando i cookie di sessione della vittima che gli consentirebbero di bypassare l'inserimento delle credenziali. I cookie di sessione possono essere rubati, ad esempio, attraverso delle email di Phishing. Si consulti la pagina relativa a questa minaccia per una più ampia conoscenza di altri metodi. **Lo score CWSS** di questa minaccia è pari a 20.0 per via dei controlli di sicurezza nell'ambito dei token di sessione e dei cookie (SOP, CSP e CORS) e anche della scarsa possibilità con cui un attaccante potrebbe optare per questa opzione. Come si può evincere consultando la bibliografia i metodi prediletti sono altri.

7. **Ottenere Credenziali Dai Password Storage**: l'avversario può entrare in possesso delle credenziali della vittima prendendole da un applicativo di gestione delle password dopo che ha trovato un metodo per accedervi. Una possibilità può essere quella che utlizzi un'email di Phising con un PDF malevolo che installa una backdoor sul sistema della vittima consentendo all'attaccante di accedere al Password Manager. Per altre modalità consultare la pagina di questa minaccia. **Lo score CWSS** di questa minaccia è pari a 4.20 per via della necessità di dover accedere al password storage della vittima. Come espresso anche nella precedente minaccia è inoltre molto improbabile che un attaccante possa optare per questa strada.

8. **Input Capture**: l'avversario può usare sistemi di keylogging per tenere traccia dei tasti che la vittima preme sulla tastiera potendo così capire quali sono le credenziali di accesso. Un modalità con cui un keylogger può installarsi sul sistema della vittima è ancora attraverso un'email di Phishing oppure attraverso un Trojan. Per altre modalità di Input Capture si consulti la pagina di questa minaccia. **Lo score CWSS** di questa minaccia è pari a 4.84 per via della difficoltà di installare

un programma di keylogging sul dispositivo della vittima. Questo tipo minaccia rientra nelle Advance Persistent Threats (APTs) che richiedono, per definizione, una conoscenza di tecniche avanzate da parte dell'attaccante per riuscire a nascondere il software nel dispositivo della vittima. Di conseguenza è improbabile che un malintenzionato in ambito MMORPG opti per questa strada.

9. **Generazione di Una Richiesta Multi Factor Authentication (MFA)**: l'avversario può inviare alla vittima una richiesta di conferma autenticazione per consentirgli di accedere all'account di quest'ultima. Ad esempio l'avversario può spacciarsi per un amico che gioca allo stesso videogioco della vittima e a cui si sono passate le credenziali. **Lo score CWSS** di questa minaccia è pari a 20.0 per la necessità dell'attaccante di passare per due layer costituiti dal reperimento delle credenziali della vittima e lo spacciarsi per un entità che la vittima ritiene affidabile (un amico o il videogioco stesso).

10. **Rimozione Accesso al Proprio Account**: l'avversario può cambiare le credenziali di accesso della vittima per impedirgli temporaneamente di accedere oppure può eliminare l'account della vittima. Questa minaccia può essere una conseguenza di **Compromissione di un Account** o di **Creazione di un Account** nel caso in cui la vittima ceda le credenziali all'avversario fidandosi di lui. **Lo score CWSS** di questa minaccia è pari a 62.1 siccome in questo caso si parte dal presupposto che l'attaccante sia già in possesso delle credenziali della vittima. In questo caso se il gioco dovesse utilizzare la Multi Factor Authentication l'attaccante dovrebbe generare una richiesta MFA che ha uno score CWSS basso. Un'altra difficoltà sta nella modalità di cambio password: questa avviene tramite email e se l'attaccante non ha accesso alla posta della vittima dovrà trovare un modo di convincerla ad aprire l'email e a cambiare la password. Tuttavia le conseguenze di sfruttare questo tipo di attacco e il fatto che alcuni videogiochi non utilizzino la MFA contribuiscono ad alzare questo score.

11. **Screen Capture**: l'avversario può effettuare degli screenshot al sistema della vittima cercando di ottenere il momento in cui questa accede ad un qualsiasi applicativo che richiede le credenziali di accesso (trovando la lunghezza della password) o quando consulta il proprio password manager. Questi programmi possono installarsi sul sistema della vittima

come conseguenza di apertura di email di phising o tramite Trojan. **Lo score CWSS** di questa minaccia è pari a 4.84 per le stesse motivazioni di **Input Capture**.

12. **Video Capture**: simile al precedente ma l'attaccante registra un video dello schermo della vittima o la vittima stessa tramite la webcam. **Lo score CWSS** di questa minaccia è pari a 4.84 per le stesse motivazioni di **Input Capture** e **Screen Capture**.

13. **Forza Bruta**: l'avversario può provare ad accedere all'account della vittima cercando di indovinarne la password. Il fatto di indovinare la password può non essere un tentativo manuale ma l'avversario può utilizzare dei bot che tentano combinazioni random di caratteri o che accedono a delle liste di password comunemente usate. Più l'avversario ha informazioni sulla vittima maggiore è la probabilità che sia in grado di indovinare la password. Per altri metodi di Brute Forcing si consulti la pagina di questa minaccia. **Lo score CWSS** di questa minaccia è pari a 7.84 per via del fatto che risulta piuttosto dispendioso per un attaccante provare ad indovinare la password dell'utente nonostante possa fare affidamento su programmi in grado di automatizzare questo processo che devono però essere da lui scritti o cercati in rete. Contribuisce ad abbassare lo score la possibilità che il videogioco controlli il numero di tentativi di login e quindi blocchi l'IP che sta utilizzando l'attaccante per un certo periodo. L'attaccante dovrebbe a questo punto trovare un modo di mascherare il proprio IP ogni x richieste in modo da poter continuare a fare richieste senza essere scoperto ma risulterebbe più conveniente in termini temporali cercare di entrare in possesso delle credenziali della vittima oppure creare un account e instaurarvi una relazione.

14. **Phishing**: forma di frode in cui l'avversario si finge una certa entità (es. lo staff del videogioco) o una persona che ha un qualche legame con la vittima mandando un'email o utilizzando altre forme di comunicazione (SMS, Telefonata, ecc.) per spingerla a rivelare informazioni sensibili (come le sue credenziali) o per installare del software malevolo sul suo dispositivo. Un messaggio di Phising può essere generico, come ad esempio un avviso di manutenzione dei server del videogioco che richiedono il reinserimento delle credenziali, o mirato alla vittima (Spearphishing), come la proposta di un'offerta su un equipaggiamento molto costoso

che richiede il pagamento di pochi euro. **Lo score CWSS** è pari a 87.3 per la facilità con cui viene tentato negli MMORPG, come si vedrà dalle numerose sfumature che può assumere, e per via dei danni che può causare alla vittima. Nel caso non si voglia passare dal canale email sarà necessario per l'attaccante compiere un moderato lavoro di social engineering e questo contribuisce ad abbassarne leggermente lo score.

Chapter 3

Le Tre Minacce Più Insidiose

Di seguito vengono riportate le 3 minacce più insidiose tra le 14 elencate nel capitolo precedente.
Nello specifico saranno analizzate in modo più approfondito:

1. Compromissione di un Account
2. Phishing
3. Creazione di un Account

3.1 Compromissione Di Un Account

In questa minaccia l'attaccante si serve di un account esistente e finge di essere quella persona. Così facendo può, ad esempio, sfruttare la fiducia che la vittima ha nei confronti della persona di cui l'avversario ha l'account per portare a termine una operazione di social engineering oppure può compromettere la reputazione della persona con quell'account.
Per portare a termine con successo un attacco di questo tipo il malintenzionato deve:

1. Raccogliere informazioni sulla persona di cui intende compromettere l'account in modo che la vittima non si insopettisca troppo
2. Entrare in possesso delle credenziali della persona di cui intende compromettere l'account. Questo può essere portato a termine attraverso operazioni di Phishing, comprando le credenziali di interesse sul dark

web (se presenti), provando attacchi di Brute Forcing (se l'attaccante ha il nome utente della persona può provare a indovinare la password).

3.1.1 Esempi di Attacco

Per capire come quanto appena descritto si possa applicare al mondo dei videogiochi MMORPG saranno riportati alcuni casi reali:

1. Stuffing Server di Gaming: in questo caso gli attaccanti utilizzavano un account di cui avevano ottenuto le credenziali da un data breach per accedere ad altri servizi online utilizzati dalla vittima confidando che utilizzasse le stesse credenziali anche per diversi servizi.

2. BloodyStealer: Malware in grado di rubare password, dati su carte di credito, account bancari, cookies, ecc. Può essere acquistato sul dark web per 40$ e possiede una serie di tool in grado di bypassare i controlli di sicurezza. I dati rubati sono inviati ad un server sotto forma di ZIP e da qui gli attaccanti possono accedervi per ottenere delle credenziali a loro piacimento. Questo malware viene utilizzato dai cybercriminali per colpire molti attacchi contro account di videogiocatori, come si può leggere anche nell'articolo riportato in bibliografia relativo a BloodyStealer.

3.1.2 Mitigazioni

Purtroppo questo tipo di minaccia non è possibile da mitigare con controlli preventivi siccome è basata su comportamenti al di fuori del controllo della vittima.
Tuttavia è possibile mettere in atto una serie di azioni per evitare che le proprie credenziali finiscano in un data breach e che siano usate per accedere a tanti servizi diversi dall'MMORPG:

1. Utilizzare password sicure e cambiarle frequentemente oppure cambiare quelle di account precedenti man mano che si acquisisce una migliore consapevolezza in ambito della sicurezza informatica

2. Non utilizzare le stesse credenziali su diversi giochi o servizi online per evitare di essere vittima di stuffing con l'attaccante che utilizzerà le credenziali rubate o ottenute in un data leak per accedere al servizio di Home Banking della vittima

3.2 Phishing

In questa minaccia il malintenzionato manda un messaggio (come una email, un SMS, ecc.) alla vittima in cui è contenuto ad esempio un link o un file malevolo. Nel caso del link questo può contienere una form che si spaccia per veritiera e affidabile e chiede al malcapitato di inserire le proprie credenziali per poter sbloccare un pacco in posta. Un file malevolo invece, se aperto, può sfruttare una vulnerabilità del sistema operativo e installare una backdoor per l'attaccante.
Generalmente questi attacchi sono veicolati tramite email o SMS e spesso le persone riescono a riconoscerli come minacce.
Ma non finisce qui, infatti, i messaggi di phishing possono essere scritti apposta per la vittima, inserendo ad esempio un'intestazione con nome e cognome o proponendo un'offerta legata alle esigenze che la vittima può avere in quel momento. Questo tipo di Phishing è denominato Spearphishing.

Lo spearphishing e il phishing si possono presentare in 3 forme diverse:

1. Allegati: email che hanno in allegato un file malevolo che sfrutta le vulnerabilità del sistema operativo della vittima. Queste email possono contenere anche istruzioni su come bypassare i controlli di sistema dopo aver dato una valida ragione per cui la vittima dovrebbe aprire l'allegato

2. Link: possono evitare i controlli sugli allegati delle email e richiedono di essere cliccati oppure copiati e incollati nella barra di navigazione del browser. Il link può contenere un download di un file malevolo oppure reindirizzare ad un form molto simile ad un sito conosciuto dalla vittima in cui si chiede di inserire le credenziali per accedervi.

3. Tramite Servizio: il phishing viene portato a termine attraverso un altro sistema di messaggistica come i Direct Message di Instagram

3.2.1 Esempi Di Attacco

Per capire come quanto appena descritto si possa applicare al mondo dei videogiochi MMORPG saranno riportati alcuni esempi di phishing raccolti consultando diversi articoli. Se per la precedente minaccia sono stati riportati esempi reali per via della sua natura specifica qui il documento si limiterà a

riportare la descrizione delle varie sfumature che un attacco di phishing può assumere in un contesto MMORPG:

1. **Gateway To Trouble**: il malintenzionato induce la vittima a comprare per una cifra irrisoria (di solito 40$) un permesso per scaricare illimitati giochi per PC o console. Pagando la vittima ottiene l'accesso ad un sito di condivisione di file di dubbia legalità. Ciò che scaricherà potrà essere in effetti un gioco funzionante ma nella maggior parte dei casi sarà un malware.

2. **Online Casino Scams**: siccome gli enti possessori di carte di credito possono bloccare i pagamenti per siti di gioco d'azzardo online gli utenti possono appoggiarsi a terze parti per bypassare questo problema. Spesso queste terze parti sono dei malintenzionati con lo scopo di rubare il denaro della vittima o i suoi dati.

3. **Phshing per Email**: la vittima riceve un'email che richiede ad esempio la conferma di un cambio password e viene reindirizzata ad una pagina in cui gli vengono chieste le vecchie credenziali in modo da poter cambiare password correttamente. Queste vecchie credenziali entrano, però, in possesso dell'attaccante che avrà accesso all'account della vittima in quanto la sua password non è stata cambiata.

4. **Vendita di Asset Virtuali**: l'attaccante finge di vendere il proprio account o un oggetto molto raro su siti come eBay o simili. La vittima pagante nella maggior parte dei casi non riceverà mai ciò che ha chiesto e si vedrà i propri soldi rubati.

5. **Pagare per Testare**: l'attaccante propone alla vittima di testare il suo videogioco pagandola a partire da 100$. Durante il gameplay può essere richiesto il pagamento di oggetti o l'inserimento di credenziali proponendo un aumento della paga. Nella maggior parte dei casi la paga non ci sarà e la vittima avrà inutilmente speso soldi o rivelato delle credenziali di accesso a servizi che utilizza nel caso abbia l'abitudine ad utilizzare gli stessi username e password per servizi diversi.

6. **CellPhone Dialers**: la vittima scarica un gioco per cellulare che, in segreto, effettua delle chiamate verso posti improbabili, come l'Antardide. L'utente sarà ignaro di tutto ciò fino a che non arriverà il resoconto delle chiamate effettuate.

7. **Altre Minacce Da Cellulare**: durante il gameplay alla vittima vengono presentati dei pagamenti altissimi con la moneta del gioco al fine di poter proseguire. Si presenteranno così altri "giocatori" che proporranno alla vittima dei link, ovviamente malevoli, per ottenere monete gratuitamente in modo da poter proseguire. Questa minaccia risulta molto presente nei videogiochi di World Building ma è anche presente negli MMORPG, soprattutto quelli ad alta competizione.

La lista potrebbe continuare ancora e nel caso il lettore voglia saperne di più è invitato a consultare la bibliografia.

3.2.2 Mitigazioni

Alcune possibili azioni che l'utente può mettere in atto per proteggersi da queste minacce sono:

1. Utilizzare lo shop ufficiale del videogioco per acquistare, non farlo passando per siti di terze parti.

2. Non rispondere a email o messaggi che chiedono i dati bancari o personali anche se sembrano provenire dal videogioco.

3. Non diffondere informazioni personali o sensibili mentre si gioca.

4. Utilizzare una password forte e diversa da tutte le altre per servizi diversi.

5. Utilizzare la Two Factor Authentication nel caso il videogioco o la piattaforma di gaming che si sta utilizzando la metta a disposizione.

6. Non cliccare su alcun link che chieda di riconfermare la password cancellando o ignorando le email che invitano ad aggiornare le credenziali di accesso.

7. Non usare carte di debito per gli acquisti ma carte di credito siccome offrono maggior sicurezza.

3.3 Estabilish Accounts

In questa minaccia il malintenzionato crea un normale account e lo utilizza per costruire un personaggio che le persone possano spacciare per realmente esistente e affidabile.
Questo tipo di minaccia ha il vantaggio di non richiedere il possesso di un account già esistente ma ha come svantaggio un'onerosa operazione di social engineering. Un modo in cui l'attaccante può portare avanti questa minaccia è attraverso l'utilizzo delle armi della persuasione di Cialdini:

1. Riprova Sociale: ritenere validi i comportamenti adottati da un alto numero di persone (es. una gilda)
2. Commitment: promessa di fare qualcosa in futuro
3. Reciprocità: do ut des
4. Piacevolezza: secondo il bias che "bello è buono"
5. Scarsità: mettere un articolo disponibile per poco tempo e, a volte, in poche copie
6. Autorità: fingersi un'entità importante in un contesto. A volte basta che una persona indossi un camice per indurre le persone a pensare che abbia una qualche autorità nel campo di cui sta argomentando

Per maggiori informazioni sulle armi della persuasione di Cialdini si può fare riferimento alla bibliografia.

3.3.1 Esempi Di Attacco

Un modo con cui questa minaccia si manifesta negli MMORPG è attraverso il meccanismo dell'Impersonation in cui si crea un account valido all'interno del gioco e lo si utilizza per:

1. **Impersonare un Game Master**: il malintenzionato crea un account e rende il suo personaggio simile ad un Game Master copiandone l'equipaggiamento tipico e i modi di fare (variano a seconda del videogioco). A questo punto attenderà le richieste degli altri giocatori e li indurrà a compiere procedure come rivelare le credenziali di accesso di modo che lui possa passargli un oggetto raro

2. **Impersonare un conoscente**: il malintenzionato crea un account e si comporta come un'altra persona da lui osservata precedentemente. Quando gli amici gli chiedono i motivi del cambio di personaggio risponde semplicemente che vuole provarne uno nuovo e a quel punto inizierà a chiedere il prestito di oggetti rari o monete d'oro con la falsa promessa di restituirli

3. **Impersonare qualcuno di affidabile**: il malintenzionato crea un personaggio e si crea una buona reputazione da zero. Dopodiché inizierà a trarre in inganno gli altri giocatori in modi molto simili al caso del Game Master

4. **Impersonare una persona di un sesso diverso da quello reale**: nei casi più comuni un utente di sesso maschile impersona un personaggio femminile e induce gli altri giocaotri del sesso opposto a compiere azioni che volgono a loro vantaggio come farsi regalare oggetti rari con la promessa di sex chat o altro.

Infine, un altro modo con cui questa minaccia si può manifestare è attraverso il Cyberbullismo il cui obiettivo principale è quello di rovinare l'esperienza di gioco per mezzo di messaggi intimidatori o derisori o azioni che impediscono al giocatore di proseguire in tranquillità il gameplay. Il malintenzionato, o un gruppo di malintenzionati, può anche, ad esempio, minacciare il giocatore di rivelare qualcosa sul suo conto qualora non dovesse compiere una certa azione che volgerebbe a vantaggio del cyberbullo/i.

3.3.2 Mitigazioni

Purtroppo per il caso dell'Impersonation non è stato possibile attingere da molte fonti oggettive, in quanto si parla di casi molto soggettivi che variano da giocatore a giocatore e da videogioco a videogioco in quanto le impersonation possono essere di svariate tipologie. Le uniche fonti riguardano il fatto che questo meccanismo esiste, come si potrà consultare nella bibliografia, e che i giocatori sono intimati a non attuarlo.
Si lascia quindi all'utente la responsabilità e il giudizio delle sue azioni giocando online documentetandosi ed essendo consapevole che queste minacce esistono. Nel frattempo, le case produttrici, come XBox, stiano cercando di muoversi per prevenire in modo automatico questa minaccia.

Nel caso del cyberbullismo il giocatore (o la sua famiglia nel caso si tratti di un soggetto minorenne) può:

1. Osservare come funziona il gioco e come i giocatori interagiscono tra loro normalmente
2. Controllare il tipo di community del videogioco
3. Comunicare con un Game Master o un Game Sage nel caso si abbia esperienza di cyberbullismo o si sospetti di esserne vittima
4. Selezionare con attenzione i giocatori con cui si decide di passare più tempo online
5. Evitare di rispondere a provocazioni
6. Evitare di compiere azioni che possano compromettere la reputazione del proprio personaggio (es. girare senza indumenti per la piazza della città principale)
7. Disconnettersi dal gioco nel caso ci si accorga di essere negativamente attivati durante una conversazione in quanto si rischierebbe di ricadere nel caso di compromettere la reputazione del proprio personaggio

Chapter 4

Conclusioni

Come emerge dagli score CWSS e dalle loro descrizioni, le minacce più insidiose risultano essere quelle del **Phishing**, della **Creazione di Account** (la cui sfumatura sta in **Utilizzo di Account Validi** e **Instaurare Relazioni di Fiducia**) e **Compromissione di un Account** accompagnate successivamente da **Instaurare Relazioni di Fiducia** che hanno la caratteristica comune di far leva sulla persona (social engineering) piuttosto che sulle tecnologie.
Le minacce che cercano invece di sfruttare le tecnologie senza passare da un'interazione con la persona, come **Input Capture**, **Video Capture** o **Generazione Di Una Richiesta Multi Factor Authentication**, non hanno infatti uno score molto elevato in quanto la protezione tecnologica ha raggiunto livelli tali da permettere ad un utente comune di giocare piuttosto al sicuro da queste minacce.
Quindi il rischio più grande che si corre risulta strettamente legato alle persone e, come emerge dalle mitigazioni proposte, uno dei modi per stare al sicuro da esse risulta non solo quello di essere consapevoli della loro esistenza ma anche essere consapevoli del loro funzionamento e delle loro conseguenze.
Uno degli sviluppi futuri che questo lavoro si propone è di conseguenza quello di portare avanti una campagna di sensibilizzazione per i videogiocatori (se minorenni, anche per i loro genitori) attraverso l'utilizzo di video sulla piattaforma di YouTube e tramite la realizzazione di un sito web in cui si andranno ad illustrare le minacce qui proposte sotto un profilo maggiormente adatto ad essere fruito da un'utenza variegata.
Questi progetti sono accomunati dall'obiettivo di voler instillare consapevolezza nell'utente che usufruisce dei videogiochi senza però minarne la possi-

bilità di divertimento che l'esperienza di gioco può offrire.

Chapter 5

Appendice A

Di seguito vengono riportate le ragioni dietro il calcolo degli score CWSS delle seguenti 3 minacce:

1. Compromissione di un Account
2. Creare un Account
3. Phishing

5.1 Compromissione di un Account

Lo score CWSS di questa minaccia è pari a 69.0 e qui ne verrà analizzato nel dettaglio il motivo.

5.1.1 Base Findings

1. **Technical Impact**: Non Applicabile siccome questa voce fa riferimento alla presenza di una vulnerabilità nel software.
2. **Acquired Privilege**: Non Applicabile siccome questa voce fa riferimento ai privilegi ottenuti dall'attaccante nel caso di un attacco ad un sistema (es. entrando nell'Active Directory di un'azienda con l'account di un dipendendente).
3. **Acquired Privilege Layer**: Non Applicabile per le ragioini del punto precedente

4. **Internal Control Effectiveness**: Moderato per via dei controlli che l'attaccante può incontrare quando cerca di entrare con le credenziali della vittima (es. Multi Factor Authentication). Non tutti gli MMORPG tuttavia implementano questi controlli.

5. **Finding Confidence**: Dimostrata Vera, in quanto tanti malintenzionati, come mostrato nel precedente capitolo, sono a conoscenza della possibilità di poter sfruttare questa minaccia.

5.1.2 Attack Surface

1. **Required Privilege**: Nessuno, l'attaccante può provare questo attacco navigando sul web alla ricerca, ad esempio, di data breaches e poi navigare alla pagina di login del videogioco

2. **Required Privilege Layer**: non applicabile in quanto l'attaccante è un semplice utente di internet.

3. **Access Vector**: internet, il videogioco o la sua pagine di login sono disponibili su internet.

4. **Authentication Strength**: Non Applicabile siccome alcuni giochi utilizzano sistemi con la Multi Factor Authentication e altri no. Per questa ragione si potrebbe optare per un livello Moderato, tuttavia si preferisce scegliere la strada del peggior scenario possibile.

5. **Level Of Interation**: Limitato, non sempre è necessario per l'attaccante interagire con la vittima per avere la possibilità di comprometterne l'account.

6. **Deployment Scope**: Ovunque, questa minaccia è presente in qualsiasi MMORPG.

5.1.3 Environmental

1. **Business Impact**: Non Applicabile siccome non si è in un contesto di Enterprise.

2. **Likelyhood Of Discovery**: Alta, l'attaccante è facile che scopra la possibilità di sfruttare questa minaccia come mostrato negli articoli riportati nella trattazione approfondita di questa minaccia.

3. **Likelyhood Of Exploit**: Alta, è facile che l'attaccante provi a sfruttare questa minaccia con successo. Anche in questo caso su alcuni MMORPG può essere più facile che in altri e quindi si opta per lo scenario peggiore.

4. **External Control Effectiveness**: Nessuno, per via della possibilità di registrarsi con i soli nome utente e password l'attaccante può accedere alla pagina di login e poi semplicemente inserire i dati di cui è in possesso.

5. **Prevalence**: Ampiamente Diffuso, come mostrato negli articoli riportati nella trattazione di questa minaccia.

5.2 Creazione Di Un Account

Lo score CWSS di questa minaccia è pari a 86.5 e qui ne verrà analizzato nel dettaglio il motivo.

5.2.1 Base Findings

1. **Technical Impact**: Non Applicabile siccome questa voce fa riferimento alla presenza di una vulnerabilità nel software.

2. **Acquired Privilege**: Non Applicabile siccome questa voce fa riferimento ai privilegi ottenuti dall'attaccante nel caso di un attacco ad un sistema (es. entrando nell'Active Directory di un'azienda con l'account di un dipendendente).

3. **Acquired Privilege Layer**: Non Applicabile per le ragioini del punto precedente

4. **Internal Control Effectiveness**: Nessuno, l'attaccante sta infatti creando un normalissimo account e lo sta utilizzando secondo le regole del videogioco.

5. **Finding Confidence**: Dimostrata Vera, chiunque giochi online è a conoscenza della possibilità di creare un account regolare da utilizzare per "ingannare" gli altri giocatori.

5.2.2 Attack Surface

1. **Required Privilege**: Nessuno, è possibile creare un account avendo accesso a internet e utilizzando il browser per collegarsi alla pagina del videogioco.

2. **Required Privilege Layer**: Non applicabile, l'attaccante è un semplice utente di Internet e non di un'azienda.

3. **Access Vector**: Internet, l'attaccante si collega alla pagina di creazione di un account e utilizza il videogioco tramite Internet.

4. **Authentication Strength**: Non applicabile, l'attaccante crea un account valido con le proprie credenziali.

5. **Level Of Interaction**: Alto, è richiesto che l'attaccante interagisca con la vittima da un minimo di una richiesta di scambio (es. un oggetto raro che ha disponibile per pochi minuti e che ha deciso di dare alla vittima) fino ad una costruzione di un vero e proprio rapporto di amicizia con la vittima.

6. **Deployment Scope**: Ovunque, qualsiasi MMORPG può essere utilizzato per portare avanti questo attacco.

5.2.3 Environmental

1. **Business Impact**: Non Applicabile siccome non si è in un contesto di Enterprise.

2. **Likelyhood Of Discovery**: Alta, per il fatto che ha un **Deployment Scope** di Ovunque.

3. **Likelyhood Of Exploit**: Alta, siccome è molto facile da provare tanti giocatori hanno la possibilità di metterla in atto.

4. **External Control Effectiveness**: Nessuno, come già ribadito, l'attaccante non sta facendo nulla di male per cui potrebbe essere bloccato da un sistema di controllo di sicurezza.

5. **Prevalence**: Ampiamente Diffuso, come già evidenziato da **Deployment Scope** e le due **Likelyhood**.

5.3 Phishing

Lo score CWSS di questa minaccia è pari a 87.3 e qui ne verrà analizzato nel dettaglio il motivo.

5.3.1 Base Findings

1. **Technical Impact**: Non Applicabile siccome questa voce fa riferimento alla presenza di una vulnerabilità nel software.
2. **Acquired Privilege**: Non Applicabile siccome questa voce fa riferimento ai privilegi ottenuti dall'attaccante nel caso di un attacco ad un sistema (es. entrando nell'Active Directory di un'azienda con l'account di un dipendendente).
3. **Acquired Privilege Layer**: Non Applicabile per le ragioini del punto precedente
4. **Internal Control Effectiveness**: Nessuno, all'interno degli MMORPG non c'è nessun meccanismo in grado di bloccare messaggi di Phishing ad eccezione dei Game Master che, però, sono persone e non sistemi automatici.
5. **Finding Confidence**: Dimostrata Vera, come si può evicere dall'elevato numero di possibili sfumature con cui un attacco di Phishing si può presentare.

5.3.2 Attack Surface

1. **Required Privilege**: Nessuno, l'attaccante utilizza il proprio browser per giocare e ingannare la vittima o inviargli delle email di Phishing.
2. **Required Privilege Layer**: Non applicabile, l'attaccante è un semplice utente di Internet e non di un'azienda.
3. **Access Vector**: Internet, l'attaccante utilizza Internet per inviare le email di Phishing o collegarsi al videogioco.
4. **Authentication Strength**: Non applicabile, non entra mai in gioco il tentativo dell'attaccante di autenticarsi in questi casi in quanto è uno step successivo.

5. **Level Of Interaction**: Moderato, l'attaccante può mandare email di Phishing dopo aver osservato la vittima e seza interagirvi ma, in alcuni casi come il fatto di indurla a testare il proprio videogioco, è necessario che vi interagisca per rendere più probabile la riuscita dell'attacco.

6. **Deployment Scope**: Ovunque, l'attaccante può provare questo attacco su qualsiasi MMORPG.

5.3.3 Environmental

1. **Business Impact**: Non Applicabile siccome non si è in un contesto di Enterprise.

2. **Likelyhood Of Discovery**: Alta, l'attaccante può venire a conoscenza di questa minaccia semplicemente cercando su Internet quali sono le minacce in cui si incorre giocando online e cliccare sul primo link.

3. **Likelyhood Of Exploitation**: Alta, l'attaccante può provare quasi senza sforzo, come ad esempio inserirsi tra gli utenti che inducono la vittima a pagare nel videogioco da testare con la promessa di una paga più alta o mettere un annuncio di vendita di un personaggio su eBay, queste minacce dopo aver compiuto una ricerca. In alcuni casi provare questi attacchi può richiedere conoscenze informatiche più approfondite, come la creazione di un sito che vende asset fasulli che sono in realtà malware. Tuttavia si preferisce considerare sempre il caso peggiore e quindi la probabilità viene mantenuta alta.

4. **External Control Effectiveness**: Limitata, alcuni siti di e-commerce, come eBay, si stanno muovendo verso l'impedire la vendita di personaggi o asset di videogiochi. I siti che vendono asset fasulli possono essere in http e quindi possono essere bloccati dai browser utilizzando politiche HTTP strict. Tuttavia si naviga ancora nel mare del buon senso dell'utente che non dovrebbe visitare siti non https o aprire link di email di dubbia provenienza o accettare richieste di beta testing retribuito su videogiochi anonimi.

5. **Prevalence**: Ampiamente diffuso, come mostrato dall'elevato numero di casistiche con cui può essere portato avanti.

Chapter 6

Appendice B

In questa appendice viene discussa la motivazione dietro la scelta del far rientrare le 3 minacce approfondite come meritevoli di approfondimento.
Il motivo principale è quello dell'alto score CWSS rispetto alle altre 11 minacce:

1. Compromissione di un Account: 69.0
2. Creazione di un Account: 86.5
3. Phishing: 87.3

In reltà alcune delle minacce scartate avevano score non trascurabili:

1. Raccogliere informazioni sulla vittima: 72.3
2. Relazione di Fiducia: 72.7
3. Utilizzo di Account Validi: 86.5

Quindi il lettore potrebbe essersi chiesto come mai siano stati scartati in favore delle 3 analizzate.

6.1 Raccogliere Informazioni Sulla Vittima

Nonostante questa minaccia abbia uno score CWSS superiore a quello di **Compromissione di un Account** è stata scartata per via dell'inclusione nella minaccia del **Phishing**.

6.2 Relazione Di Fiducia

Nonostante questa minaccia abbia uno score CWSS superiore a quello di **Compromissione di un Account** è stata scartata per via dell'inclusione nella minaccia **Creazione di un Account**.

6.3 Utilizzo di Account Validi

Nonostante questa minaccia abbia uno score CWSS superiore a quello di **Compromissione di un Account** è stata scartata per via dell'inclusione nella minaccia **Creazione di un Account** e **Compromissione di un Account**.

Chapter 7

Bibliografia

1. Testimonianze Compromissione Account: https://www.verdict.co.uk/hackers-online-gaming-accounts
2. BloodyStealer: https://www.techradar.com/news/thousands-of-online-gaming-accounts-hit-in-major-cyberattack
3. Mitigazioni Compromissione Account: https://nordvpn.com/blog/online-gaming-security-threats/
4. Casistiche Phishing: https://scambusters.org/onlinegamesscam.html
5. Video minacce MMORPG e giochi online: https://www.youtube.com/watch?v=U8CcCq8uyO0
6. Cyberbullismo: https://www.stopbullying.gov/cyberbullying/cyberbullying-online-gaming
7. Difendersi dal Phishing: https://www.verywellfamily.com/teach-kids-about-phishing-and-online-scams-5248479
8. Esistenza Della Minaccia Impersonation: https://www.epicgames.com/site/en-US/community-rules
9. Testimonianza Impersonation: http://forums.xgenstudios.com/t/in-game-staff-impersonation/7254
10. Contromisure Impersonation da parte di XBOX: https://support.xbox.com/en-US/help/family-online-safety/enforcement/protecting-players-from-account-related-offenses

11. Tabella MitreAtt&ck: https://attack.mitre.org/

12. Calcolatore Score CWSS: https://www.cwss-score.info/

13. Armi della persuasione nel marketing: https://blog.xtribe.com/le-7-armi-della-persuasione-applicate-al-marketing/