

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky



Phishing v hernom priemysle

BAKALÁRSKA PRÁCA

Študijný program: Aplikovaná informatika

Študijný obor: Aplikovaná informatika

Autor: Adrián Heldes

Vedúci práce: Ing. Ladislav Luc

Praha, Apríl 2019

Prehlásenie

Prehlasujem, že som bakalársku prácu *Phishing v hernom priemysle* vypracoval samostatne za použitia v práci uvedených prameňov a literatúry.

V Prahe dňa 2019

.....

Podpis študenta

Podakovanie

Tímto by som chcel poďakovať Ing. Ladislavovi Lucovi za cenné rady, pripomienky a za pomoc pri spracovaní tejto bakalárskej práce.

Abstrakt

Táto bakalárska práca sa zaoberá témou phishingu, a to v hernom priemysle, v dnešnej dobe veľmi závažným problémom.

Prvý cieľ práce je zoznámiť čitateľa s phishingom obecne a v hernom priemysle. Pre dosiahnutie tohoto cieľu je vypracovaná teoretická časť, ktorá sa skladá z informácií o phishingu a o jeho typoch. Potom je podrobne popísaný herný priemysel, online obchod s hernými produktmi/hernými menami, vývojové trendy v online obchodovaní a riziká, ktoré s online obchodovaním súvisia.

Druhým cieľom práce je poskytnúť užívateľom platformy Steam informácie o phishingových útokoch a ako sa proti nim brániť. Pre tento cieľ je vybraná platforma Steam a rôzne externé webové stránky, ktoré sa používajú na obchod alebo hazard. V praktickej časti sú rozobrané phishingové útoky a opatrenia, ktoré vybraná spoločnosť urobila, aby sa tieto útoky neopakovali. Následne je porovnávaná bezpečnosť vybranej platformy s inými veľkými platformami. K vybraným útokom sú vypracované analýzy a možné opatrenia voči daným útokom. Práca je zakončená súhrnom o útokoch a možných protiopatreniach.

Kľúčové slová

phishing, Steam, herný priemysel, bezpečnosť, trendy

Abstract

This bachelor thesis deals with the topic of phishing in the gaming industry, a very serious problem in today's world.

The first goal of the work is to familiarize readers with phishing in general and in the gaming industry. To achieve this goal, the theoretical part is created, which consists of information about phishing and types of phishing. Then the gaming, the online gaming product/game currency market, the online trading trends and the risks associated with online trading are described in detail.

The second goal is to provide Steam users with information about phishing attacks and how to defend themselves against them. Steam platform and various external websites that are used for trading or gambling are selected to achieve this goal. In the practical part, phishing attacks and the measures that chosen platform has taken to prevent these attacks are discussed. Subsequently, the safety of chosen platform is compared with other large platforms. Selected attacks are analyzed and possible measures against the attacks are mentioned. The work is concluded with a summary of attacks and possible countermeasures.

Keywords

phishing, Steam, gaming industry, security, trends

Obsah

Úvod	17
1 Rešerš	19
1.1 Príprava rešerše	19
1.2 Samotná rešerš	19
2 Phishing	21
2.1 Definícia pojmu	21
2.2 Pharming	21
2.3 Kybernetická bezpečnosť	21
2.4 Kybernetický zločin	22
2.5 Anthem útok	22
2.6 Anti phishing act	22
3 Typy phishingu	25
3.1 Spear phishing	25
3.2 Clone phishing	25
3.3 Whaling	25
3.4 Manipulácia s odkazmi	25
3.5 Vyhnutie sa filtru	26
3.6 Faľšovanie webových stránok	26
3.7 Telefonovanie phishingom	26
3.8 Tabnabbing	27
3.9 Spoločné vlastnosti phishingových e-mailov	27
4 Anti-Phishing	29
4.1 E-mail	29
4.2 Overenie transakcie	29
5 Herný priemysel	31
5.1 Definícia slova „Video hra“	31
5.2 História herného priemyslu	31
5.2.1 Začiatky herného priemyslu	31
5.2.2 Zlatá éra	32
5.2.3 Prvé herné konzoly	33
5.2.4 Prvá konzolová „vojna“	33
5.2.5 Začiatok éry 3D hier	34
5.2.6 Moderný vek video hier	35
5.3 Rozdelenie hier	36
5.3.1 ESRB hodnotenie hier	36
5.3.2 Žánre video hier	38

5.3.3	Business modely video hier	40
5.4	Online obchod	40
5.4.1	Online obchod s hrami	40
5.4.2	Online obchod s hernými produktmi/menami	41
5.5	Trendy v hrách a na trhu herného priemyslu	41
5.6	Esports a sponzori	44
5.6.1	Esports	44
5.6.2	Sponzori	47
6	Steam	49
6.1	Zabezpečenie platformy Steam	49
7	Porovnávanie s inými platformami	53
7.1	Platforma Battle.net	53
7.2	Platforma GOG	53
7.3	Platforma Origin	54
7.4	Platforma Epic Games	54
7.5	Výsledné porovnanie	55
8	Obchodovanie na platforme Steam a externé stránky	57
9	Phishingové a iné útoky na platforme Steam	59
9.1	Útok pomocou phishingovej stránky	59
9.1.1	Postup útoku	59
9.1.2	Opatrenia	60
9.2	Falošna chyba v aplikácii Teamspeak	61
9.2.1	Postup útoku	61
9.2.2	Opatrenia	62
9.3	ESEA crack	62
9.3.1	Postup útoku	62
9.3.2	Opatrenia	62
9.4	SSFN podvod	63
9.4.1	Postup útoku	63
9.4.2	Opatrenia	63
9.5	Útok pomocou krádeže identity	63
9.5.1	Postup útoku	64
9.5.2	Opatrenia	64
9.6	Rýchla výmena tovaru	64
9.6.1	Postup útoku	64
9.6.2	Opatrenia	64
9.7	Vrátenie peňazí	65
9.7.1	Postup útoku	65
9.7.2	Opatrenia	65
9.8	Darčeková poukážka	65
9.8.1	Postup útoku	65

9.8.2	Opatrenia	65
9.9	Darčekový podvod	66
9.9.1	Postup útoku	66
9.9.2	Opatrenia	66
9.10	Faktúrový podvod	67
9.10.1	Postup útoku	67
9.10.2	Opatrenia	67
9.11	Zhrnutie o útokoch	67
9.12	Zhrnutie o opatreniach	67
9.13	Bezpečné zabezpečenie účtu	68
Závěr		69

Zoznam obrázkov

5.1	ESRB hodnotenie "E" (25)	36
5.2	ESRB hodnotenie "E10" (25)	36
5.3	ESRB hodnotenie "T" (25)	36
5.4	ESRB hodnotenie "M" (25)	37
5.5	ESRB hodnotenie "A" (25)	37
5.6	ESRB hodnotenie "RP" (25)	37
5.7	Bez ESRP hodnotenia (26)	38
5.8	ESRP hodnotenie pre hru Total war: Three kingdoms (27)	38
5.9	Vývoj a predpokladaný vývoj Čínskeho trhu hier (34)	42
5.10	Vývoj a predpokladaný vývoj Amerického trhu hier (34)	43
5.11	Globálne tržby z hier (34)	43
5.12	Vývoj a predpokladaný vývoj globálneho trhu hier (34)	44
5.13	Vývoj a predpokladaný vývoj počtu sledujúcich Esports (34)	45
5.14	Turanje a "Prize Pool" pre daný turnaj (38)	46
5.15	Vývoj a predpokladaný vývoj globálnych tržieb z Esports (34)	47
7.1	Výsledné hodnotenie bezpečnosti platforiem, Zdroj: Autor	56
9.1	Príklad 1 kontaktovania obete útočníkom (66)	59
9.2	Príklad 2 kontaktovania obete útočníkom (67)	59
9.3	Príklad 3 kontaktovania obete útočníkom (68)	59
9.4	Zoznam príkladov modifikovaných linkov (68)	60
9.5	Správne certifikáty spoločnosti Valve Corp., Zdroj: Autor	60
9.6	Detailný správny certifikát spoločnosti Valve Corp., Zdroj: Autor	61
9.7	Falošná chybná správa 1 (69)	61
9.8	Falošná chybná správa 2 (69)	62
9.9	Nahratie SSFN súboru (70)	63
9.10	Podvod pomocou darčekovej poukážky (71)	66

Zoznam tabuliek

5.1	Najpredávanejšie arkádové hry	32
7.1	Porovnanie platforiem	55
7.2	Porovnanie platforiem (dodatok)	55

Zoznam použitých skratiek

URL Uniform Resource Locator

IP Internet Protocol

DNS Domain Name Servers

NIC The National Information Center

SMS Short Message Service

IBM International Business Machines

NES Nintendo Entertainment System

CD Compact disk

ESRB The Entertainment Software Rating
Board

RPG Role Playing Game

RTS Real Time Strategy

MOBA Multiplayer online battle arena

LoL League of Legends

DotA Defense of the Ancient

CMS Construction and management
simulation

FIFA The Fédération Internationale de

Football Association

NHL National Hockey League

NBA National Basketball League

FPS First Person Shooter

PUBG PlayerUnknown's BattleGrounds

F2P Free to Play

B2P Buy to Play

P2P Pay to Play

MMORPG Massively Multiplayer Online
Role Playing Game

SA Severná Amerika

EU Európa

AP Ázia a Pacifik

API Application Programming Interface

DDoS Distributed Denial of Service

USB Universal Serial Bus

2FA Dvoj faktorová autentifikácie

ESEA E-Sports Entertainment Association

Úvod

Túto tému bakalárskej práce som si vybral z dôvodu, že sa v tomto priemysle už niekoľko rokov pohybujem a mám skúsenosti s podobnými útokmi. Herný priemysel je veľmi rýchlo rastúci priemysel a s rastom popularity rastie aj počet ľudí či organizácií, ktorí tento priemysel chcú zneužiť vo svoj prospech, čo môže odradiť veľkých investorov alebo aj nových hráčov. Práve kvôli novým hráčom som si vybral platformu Steam, ktorá je jedna z najviac používaných platforiem pre nákup hier, hranie hier, s možnosťou hrania hier s inými ľuďmi, vytváranie vlastného obsahu do hier a mnoho iných funkcií. Prvým cieľom tejto práce je zoznámiť čitateľa s phishingom a herným priemyslom. Druhým cieľom je poskytnúť užívateľovi platformy Steam informácie o phishingových útokoch a ako sa proti nim môže brániť.

Práca je delená do viacerých častí. Na začiatku je teoretická časť, ktorá je zameraná na vysvetlenie phishingu, kybernetickej bezpečnosti, opísanie typov phishingu a následne jednoduché doporučenie na obranu proti podobným phishingovým útokom. Keďže témou mojej práce je phishing v hernom priemysle, tak v nasledujúcich kapitolách opisujem históriu, rôzne rozdelenia, online obchod a trendy vo video hrách. Túto kapitolu uzatváram Esports a sponzormi. Informácie v tejto časti som čerpal najmä z internetu a to z dôvodu, že tieto témy sú relatívne nové a je veľmi málo publikovaných kníh, ktoré sa zaoberajú touto problematikou. V ďalšej časti popisujem platformu Steam, jej problémy so zabezpečením v minulosti a vysvetlím opatrenia, ktoré táto platforma učinila, aby sa tieto problémy neopakovali. Potom platformu Steam porovnávam s inými známymi platformami, s ktorými konkuruje. Po analýze bezpečnostných prvkov každej platformy je vypracované výsledné porovnanie, v ktorom je vyhodnotené zabezpečenie daných platforiem. V predposlednej časti je rozobrané obchodovanie na platforme Steam a iné externé stránky, ktoré využívajú platformu Steam na obchodovanie s tovarom. Posledná časť je zameraná na phishingové a iné útoky na platforme Steam. V tejto časti je rozobraných 10 rôznych útokov, s ktorými sa môže užívateľ platformy veľmi jednoducho stretnúť, ak nebude opatrný. Každý útok je podrobne rozobraný, vysvetlený jeho postup a sú navrhnuté opatrenia, ktoré môže užívateľ platformy Steam využiť, aby zabránil podobným útokom.

1. Rešerš

V tejto časti bude vypísaný prehľad relevantných publikácií, ktoré sa zaoberajú Phishingom v hernom priemysle. Sú tu uvedené zdroje a ich následné zhodnotenie.

1.1 Príprava rešerše

Pred prípravou rešerše si musíme stanoviť kľúčové slová a ako tieto práce budeme hľadať. Články budeme hľadať na internete pomocou vyhľadávača Google (www.google.com) a jazyk, ktorý budeme používať pri vyhľadávaní, je slovenský, český a anglický jazyk. Kľúčové slová, podľa ktorých budeme vyhľadávať sú: Phishing v hernom priemysle, diplomová práca.

1.2 Samotná rešerš

Nguyen Van, Bc. Thanh. *Phishing v herním průmyslu*. Praha, 2016. Bakalárska práca. Vysoká škola ekonomická v Praze. Fakulta informatiky a statistiky.

Autor bakalárskej práce v teoretickej časti čitateľovi opíše phishing a herný priemysel. V hernom priemysle rozoberá históriu počítačových hier, rozdelenie počítačových hier, herné platformy a jednoducho opíše trh herného priemyslu. Následne v ďalšej časti opíše podvody a čierny trh vo video hrách. V ďalšej časti opíše 4 typy útokov pomocou phishu a následne opíše možnosť ochrany. Potom analyzuje platformu Steam, kde opisuje platformu, pôsobisku na trhu a SWOT analýzu rôznych marketov. V ďalšej časti opíše 8 útokov na Steame a následne určí nebezpečnosť útoku. V poslednej časti opíše zabezpečenie na platforme Steam.

Na rozdiel od spomínanej práce, táto práca viac popisuje rôzne typy phishingu, vysvetľuje históriu konzolových hier, hlbšie rozoberá trendy v hernom priemysle, Esports, rozoberá aj iné rozdelenia video hier, obchodovanie na platforme, obchodovanie pomocou externých stránok a porovnávam platformu Steam aj s inými platformami. Následne praktická časť sa zameria na opatrenia proti útokom a na konci praktickej časti odporučím bezpečné nastavenie Steam účtu.

2. Phishing

V tejto kapitole je bližšie priblížené téma phishingu a kybernetickej kriminality. Následne je rozobraný jeden z najväčších phishingových útokov v histórii a je opísaný zákon zo Spojených štátov amerických, ktorý dopodrobna opisuje protizákonnosť phishingu.

2.1 Definícia pojmu

Phishing je pokus o získanie osobných informácií ako sú heslá, používateľské mená alebo informácie o kreditných kartách. Phisher sa zvyčajne snaží maskovať svoju identitu. Buď sa vydáva za fiktívnu osobu alebo za osobu, ktorou nie je. Slovo „phishing“ pochádza zo slov „password“ čo znamená heslo a „fishing“ čo znamená rybolov. (1) Takto pomenovaný je preto, lebo phisher používa návnadu na chytenie obetí. Vo väčšine prípadov sa phishing uskutočňuje prostredníctvom e-mailovej správy alebo akéhokoľvek iného typu správy. Kliknutím na odkaz je obeť presmerovaná na webovú stránku, ktorá pôsobí dôveryhodne, avšak nie je. Požiada obeť, aby vyplnila svoje osobné údaje, ktorých odcudzenie je po vyplnení triviálne. Jediný rozdiel medzi falošnou stránkou a pôvodnou stránkou je adresa URL, ktorých zámena je pre človeka triviálna. Zároveň môžu phishingové emaily obsahovať prepojenia na webové stránky, ktoré sú infikované vírusmi alebo malwarimi. Phishing využíva nepozornosť obetí.

2.2 Pharming

Pharming sa zameriava predovšetkým na zmenu IP adres v systéme. Presmerovanie takejto adresy môže útočník uskutočniť buď napadnutím servera DNS alebo zmenou súboru hosts priamo na počítači používateľa. (2) Ak používateľ zadá mennú adresu do internetového prehliadača, miesto stránky sa zobrazí jej dokonalá napodobenina. Používateľ teda nezistí, že sa nachádza na inej stránke.

2.3 Kybernetická bezpečnosť

Kybernetická bezpečnosť pozostáva z technológií, procesov a ovládacích prvkov, ktoré sú určené na ochranu systémov, sietí a údajov pred počítačovými útokmi. (3) Efektívna kybernetická bezpečnosť znižuje riziko kybernetických útokov a chráni organizácie a jednotlivcov pred neoprávneným využívaním systémov, sietí a technológií.

Implementácia účinných opatrení v oblasti kybernetickej bezpečnosti je dnes obzvlášť náročná, pretože existuje viac zariadení ako ľudí a útočníci sa stávajú inovatívnejšími.

Elementy kybernetickej bezpečnosti sú: bezpečnosť aplikácií, informácií, sietí, operácií, plánovanie kontinuity biznisu, záväzky vedenia a vzdelávanie koncového užívateľa. (4)

2.4 Kybernetický zločin

Je veľmi rýchlo rastúca časť kriminality. Čoraz viac a viac zločincov využíva rýchlosť, vymoženost a anonymitu internetu pre spáchanie veľkého množstva zločinov, či už fyzických alebo virtuálnych, a tým spôsobujú veľké škody a teda sú obrovským rizikom obete. Všeobecná definícia počítačovej kriminality neexistuje, avšak zákony rozdeľujú túto kriminalitu na dve skupiny: „pokročilá počítačová kriminalita“ a „počítačovo umožnená kriminalita“. Pokročilá počítačová kriminalita je sofistikovaný útok na hardware a software počítača. Naopak počítačovo umožnená kriminalita je taká, ktorá iba využíva technológiu na spáchanie „tradičných“ zločinov ako finančné zločiny alebo terorizmus. (5)

2.5 Anthem útok

Tento útok sa stal Anthem Inc dňa 6.2.2015. Anthem je druhou najväčšou zdravotnou poisťovňou v USA. Konečný počet obetí dosahuje približne 80 miliónov. Tento útok bol vykonaný prostredníctvom e-mailov, ktoré boli poslané členom tejto spoločnosti. Mená, adresy, číslo sociálneho poistenia, dátum narodenia a história zamestnania súčasných a bývalých zákazníkov. Všetky tieto údaje boli od spoločnosti odcudzené. NIC dospela k záveru, že zahraničná vláda pravdepodobne prijala 2 hackerov, ktorí vykonali jedno z najväčších narušení údajov v histórii. Všetko to začalo rok pred útokom, keď jeden zo zamestnancov klikol na odkaz vo phishingovom e-maile. Celkové náklady Anthem ešte nie sú známe, ale môžu presiahnuť viac ako 100 miliónov amerických dolárov. Našťastie údaje neboli predané, zdieľané alebo použité podvodne alebo o tom zatiaľ neexistujú žiadne dôkazy. (6)

2.6 Anti phishing act

Phishing ako každá iná trestná činnosť je protizákonná. Z tohto dôvodu vznikli zákony, ktoré sa zameriavajú priamo na túto kriminálnu činnosť. Jedným z nich je „Anti phishing act“. Je to americký zákon, ktorý zaisťuje, že phishing a pharming sú nezákonné a že štát má možnosť stíhať útočníkov. Tento zákon zároveň umožňuje súdne spory pre poskytovateľov internetových služieb a majiteľov webových stránok alebo ochranných známk, ktoré sa používajú bez ich povolenia. Zákon sa skladá z 10 častí. Prvá časť opisuje definície objektov a subjektov, na ktoré sa tento zákon vzťahuje. Druhá časť tohto zákona definuje kedy sa z niekoho stane viník z phishingu alebo pharmingu. Tretia časť je o imunitе poskytovateľa za zrušenie stránok, kvôli ktorým sú sprostredkované phishing alebo pharming útoky. Časť päť tohto zákona sa zaoberá porušením tohto zákona – kto môže podať žalobu a čo postihne obžalovaného, ak

bude odsúdený. V ďalších častiach sa rieši uplatniteľnosť zákona, zabezpečenie zákona, platnosť zákona, zrušenie starých zákonov podobného typu, ktoré boli nahradené týmto zákonom a posledná časť je o dátume, od ktorého tento zákon platí. (7) Podľa tohto zákona je možné, aby útočníci čelili pokute až 250 000 dolárov a zároveň mohli stráviť 5 rokov za mrežami. (7)

3. Typy phishingu

Keďže typov phishingových útokov je veľa a každý sa líši, tak v nasledujúcej časti sú tieto útoky popísané. Pri každom útoku sú popísané kroky ako daný útok prebieha. Táto časť je zakončená krátkym zhrnutím útokov a ako phishingový útok jednoducho rozoznať.

3.1 Spear phishing

Tento pokus o neoprávnené získavanie údajov je zameraný na konkrétnych jednotlivcov alebo spoločnosti. Tento typ sa nazýva „spear phishing“. Útočníci väčšinu času zhromažďujú mnoho informácií o svojich obetiach, čím pôsobia dôveryhodnejšie pre obeť, a preto je ich úspech vyšší ako pri iných typoch phishingov. Tieto útoky väčšinou nie sú robené jednotlivcami, ale organizovanou skupinou za účelom obohatenie alebo získania citlivých informácií. (8)

3.2 Clone phishing

Clone phishing používa predtým doručený e-mail obsahujúci prílohu alebo odkaz. Replikuje e-maily, ktorých príloha alebo odkaz je nahradený škodlivou verziou, ktorá je následne odoslaná z e-mailovej adresy, z ktorej bola odoslaná pôvodná klonovaná e-mailová adresa. Môže sa stať, že bude odoslaná pôvodná e-mailová správa alebo len aktualizovaná verzia originálu. (9)

3.3 Whaling

Typ phishingu nazývaný „whaling“ sa priamo odosiela vrcholovým manažérom alebo iným vysoko postaveným osobám. Tento typ je oveľa ťažšie vykonať. Obsah je vytvorený presne na jednu osobu s vysokým postavením a úlohou v spoločnosti. Väčšinou obsahuje sťažnosť od zákazníka, naliehavý problém, ktorý treba ihneď vyriešiť a podobne. Takýto e-mail zvyčajne zahŕňa falošný problém alebo informáciu, ktorá sa týka celej spoločnosti. (10)

3.4 Manipulácia s odkazmi

Väčšina metód phishingu používa taký druh technického podvodu, ktorý je navrhnutý na vytvorenie odkazu v e-maile, ktorý vyzerá, že patrí ku konkrétnej organizácii. Nesprávne zadané adresy URL alebo použitie subdomény sú bežné triky, ktoré používajú phisher. (11) Ďalším trikom phisherov je zobrazenie textu odkazu ako spoľahlivú destináciu, aj keď sa jedná o web phisherov. Mnoho desktopových e-mailových klientov a webových prehliadačov zobrazí

cieľový URL odkaz v stavovom riadku, zatiaľ čo nad ním bude ukazovať myš. Ďalší problém s adresami URL bol nájdený pri manipulácii s internacionalizovanými názvami domén vo webových prehliadačoch, ktoré by mohli umožniť, aby vizuálne identické webové adresy viedli k rôznym, možno škodlivým webovým stránkam. (11)

3.5 Vyhnutie sa filtru

Phishery začali dokonca používať obrázky namiesto textu, aby bolo pre filtre proti neoprávnenému získavaniu údajov obtiažnejšie odhaliť text, ktorý sa bežne používa vo phishingových e-mailoch. To však viedlo k vývoju filtrov proti phishingu. Pokročilosť takýchto filtrov je taká, že dokážu skenovať skrytý text na obrázkoch, aby dokázali rozpoznať aj skryté texty. Pre obrazové filtre sa používa optické rozpoznávanie znakov na optické naskenovanie obrazu a jeho filtrovanie. Navyše, niektoré filtre používajú inteligentné rozpoznávanie slov, ktoré dokážu zistiť kurzívu, ručne písaný alebo otočený text, ako aj text na farebnom pozadí. (12)

3.6 Falšovanie webových stránok

Akonáhle obeť navštívi webovú stránku phisherov, podvod ešte nekončí. Mnohé podvody phishingu používajú na úpravu panela s adresou príkazy JavaScript. Môžete to urobiť buď umiestnením obrázka legítimnej adresy URL na panel s adresou, alebo zatvorením pôvodného panela a otvorením nového s legítimnou adresou URL. (13) Aby sa zabránilo technikám proti phishingu, ktoré skenujú webové stránky s textom súvisiacim s phishingom, phishery začali používať webové stránky založené na flashi. Vyzerajú podobne ako skutočné webové stránky, ale skrývajú text v multimediálnom objekte.

3.7 Telefonovanie phishingom

Phishing nepotrebuje falošné webové stránky. Správy, v ktorých útočníci tvrdili, že sú z banky a následne obetiam bolo povedané, že majú nejaký problém s bankovým účtom alebo kreditnou kartou, sú taktiež časté. Keď obeť zavolajú na dané telefónne číslo, tak sa útočníci pokúsia získať ich osobné informácie o účte, ako je číslo karty alebo PIN. Útočníci, ktorí sa snažia o telefonické phishing alebo Vishing („Voice phishing“ = hlasový phishing) používajú falošné dáta identity, aby vyzerali, že hovory pochádzajú od dôveryhodnej organizácie. (14) K dispozícii je aj SMS phishing, ktorý používa textové správy.

3.8 Tabnabbing

Tento útok využíva dôveru používateľov a nepozornosť k podrobnostiam týkajúcich sa otvorených prehliadačových kariet a schopnosti moderných webových stránok prepísať karty a ich obsah dlho po načítaní stránky. Táto technika funguje opačne ako väčšina ostatných phishingových techník a to tak, že obeť priamo nepresmeruje na podvodnú stránku, ale namiesto toho načíta falošnú stránku do jednej z otvorených kariet prehliadača. Príkladom tejto metódy je internet banking. (15) Niektoré banky majú automatické odhlásenie po 15 minútach. Toto využije útočník a otvorí identicky vyzerajúcu stránku, ale URL adresa je rôzna. V dnešnej dobe už táto metóda nefunguje, keďže väčšina prehliadačov automaticky zabráňuje samovoľnému otváraniu kariet/okien.

3.9 Spoločné vlastnosti phishingových e-mailov

"Príliš dobré, aby to bola pravda naozaj lukratívne ponuky, ktoré sú tak dobré, aby boli pravdivé, ale niektorí naivní ľudia im veria. Tieto správy sú zamerané na prilákanie pozornosti ľudí.

Obmedzené časové ponuky - väčšina ľudí nedokáže myslieť pod časovým tlakom a práve to útočníci využívajú. Útočníci posielajú "ponuku s obmedzeným časovým limitom a obeť začne o tom premýšľať. Niektorí útočníci píšú, že musíte napísať svoje osobné informácie, ak nechcete, aby bol váš účet pozastavený.

Hyperlinky - odkaz, ktorý nemusí byť taký, ako sa zdá. Každý hypertextový odkaz, môže mať meno zmenené na čokoľvek. Správny odkaz je viditeľný len vtedy, keď sa prejde kurzorom nad hypertextový odkaz. Môže to byť úplne iný názov alebo len chybné napísané pôvodné webové stránky.

Prílohy - jediná príloha, ktorá je vždy bezpečná, je súbor .txt. Mnohokrát sa stane, že ľudia otvárajú .exe alebo iný typ súborov, ktoré môžu obsahovať škodlivý softvér alebo vírusy.

4. Anti-Phishing

Existuje veľa anti-phishing webových stránok, ktoré publikujú správy, ktoré nedávno cirkulovali na internete. Napríklad „FraudWatch international“. V súčasnosti existuje mnoho rôznych techník na boj proti phishingu. Existujú právne predpisy a technológie vytvorené špeciálne na boj a ochranu proti phishingu. Všetky tieto ochranné prostriedky môžu byť prijaté spoločnosťami alebo jednotlivcami. Webové stránky, telefonické alebo e-mailové phishingové správy môžu byť hlásené zodpovedným orgánom.

4.1 E-mail

Každý poskytovateľ e-mailu bojuje denne s phishingom. Väčšina z nich zaviedla spamové filtre, ktoré znižujú počet phishingových e-mailov, ktoré sa dostanú do doručenej pošty. Ďalším spôsobom boja je sanácia po ukončení dodávky, analýza a odstránenie útoku proti kopírovaniu pri doručovaní prostredníctvom doručovania na úrovni poskytovateľa elektronickej pošty. Všetky prístupy sa opierajú o strojové učenie a spracovanie prirodzeného jazyka na klasifikáciu phishingových e-mailov.

4.2 Overenie transakcie

Existujú aj riešenia pre bankové transakcie. Jedným z nich je dvojstupňová autentifikácia. Táto metóda vyžaduje ďalšiu vrstvu overenia, či už telefonicky alebo pomocou textovej správy. Táto správa sa automaticky pošle po tom, ako užívateľ zadá svoje prihlasovacie meno a heslo. Bez tohto údaju z textovej správy alebo z telefonátu sa užívateľ nedokáže prihlásiť.

5. Herný priemysel

Aby čitateľ jednoduchšie pochopil túto prácu, tak je v tejto časti vysvetlený herný priemysel. Vysvetlenie začína definíciou, históriou a rozdelením hier. Následne je popísaný online obchod s hrami a s hernými produktami/menami. Kvôli veľkej neinformovanosti nezainteresovaných ľudí bola vypracovaná aj časť týkajúca sa trendov v hrách a na trhu herného priemyslu. Táto časť priblíži čitateľovi veľkosť herného priemyslu a množstvo peňazí z tohto priemyslu. Kapitola je ukončená popisom Esports a sponzormi.

5.1 Definícia slova „Video hra“

Pojem videohra sa postupne vyvíjal od čisto technickej definície pre celkový koncept, ktorý definuje novú triedu interaktívnej zábavy. Z technického hľadiska, aby bol výrobok videohra, musí byť prenášaný obrazový signál na katódovú trubicu, ktorá vytvára rastrový obraz na obrazovke. (16) Táto definícia by vylučovala skoré počítačové hry, ktoré tlačili výsledky pomocou tlačiarne skôr ako na displej, akúkoľvek hru vykreslenú na monitore vektorového snímania alebo akúkoľvek hru prehrávanú na modernom displeji s vysokým rozlíšením. Z technického hľadiska by sa skôr mali nazývať elektronické hry alebo "počítačové hry".

Dnes sa však termín "videohra" úplne zbavil svojej čisto technickej definície a zahŕňa širšiu škálu technológií. Aj keď je stále termín „videohra“ dosť neurčitý, tak v súčasnosti vo všeobecnosti zahŕňa akúkoľvek hru prehrávanú na hardvéri vybudovanom s elektronickými logickými obvody, ktorý obsahuje prvok interaktívnosti a výstupy výsledkov činností hráča na displeji.

5.2 História herného priemyslu

5.2.1 Začiatky herného priemyslu

Ako každé technické odvetvie, tak aj herný priemysel bol zo začiatku veľmi technicky náročný. Jediné počítače, Colossus a ENIAC, ktoré po 2. svetovej vojne existovali boli tie, ktoré pomáhali spojencom vo vojne. (17) Následne, po 2. svetovej vojne, v skorých 60 rokoch sa začali počítače viac a viac komercializovať vďaka firmám ako IBM. To následne viedlo k väčšiemu využívaniu počítačov na univerzitách, veľkých firmách a vo vládnych organizáciách.

Jedna z prvých hier bola vytvorená v roku 1952 študentom PhD titulu na Cambridgeskej univerzite ako jeho dizertačná práca. Boli to piškvorky. Táto hra bola hraná človekom proti počítaču, pričom si človek mohol vybrať kto začína prvý. Po začatí hry si človek vybral kde chce položiť krížik alebo krúžok pomocou mechanického telefónneho dialeru. Táto hra bola naprogramovaná na počítači EDSAC, ktorý bol postavený v roku 1949. (18)

Prvá hra, ktorá aktualizovala obraz v reálnom čase bola hra biliardu naprogramovaná Williamom Brownom a Tedom Lewisom na univerzite v Michigane v roku 1954. (19)

Ďalšia z hier vytvorených v 60 rokoch minulého storočia je „Tennis pre dvoch“. Vytvorená v roku 1958 v národnej laboratórii v Brookhavenne. Nadizajnoval ju William Higinbotham a postavil ju Robert Dvorak. Táto hra bola postavená čisto pre zábavu verejnosti. Hra fungovala na analógovom počítači a obraz sa zobrazoval na osciloskope. (20) Táto hra nikdy nemala nádeje, aby sa dostala na trh, keďže v tej dobe počítače zaberali veľa miesta a boli drahé, čiže si ich domácnosti nemohli dovoliť.

5.2.2 Zlatá éra

Ako zlatá éra sa určuje doba kedy sa arkádové video hry stali súčasťou pop kultúry. Presný rok, kedy táto éra začala je sporný, ale kľúčové momenty boli v roku 1978 a 1978 vypustením na trh arkádových hier „Space Invaders“ respektíve „Asteroids“. (21)

Arkádové videohry sa hrávali na automatoch a mali zásadný vplyv na popularizáciu hier. Keďže herné automaty boli verejne a cenovo prípustné, začalo sa hranie video hier viac popularizovať a zároveň prišlo na scénu aj súťaženie o ceny v arkádových hrách .

S príchodom arkádových automatov taktiež nastala zmena v hernom priemysle. Vznikli prvé špecializovaná štúdiá, ako dnes už legendárny Atari (hry Pong / Asteroids / Pac-man) a Taito (hry Space Invaders / Polaris / Colony 7). (22) V tejto dobe sa hracie automaty bežne nachádzali v reštauráciách, baroch, herniach a boli postupne inštalované prakticky vo všetkých verejne prístupných objektoch a centrách rodinnej zábavy.

Tabuľka 5.1: Najpredávanejšie arkádové hry

Názov	Rok vydania	Počet predaných kusov (v tisícoch)	Odhadovaný hrubý výnos (s infláciou v mil \$)
Pac-Man	1980	400	7,700
Space Invaders	1978	360	6,600
Street Fighter II	1997	200	3,600
Ms. Pac-Man	1981	125	2,560
NBA Jam	1993	20	1,700
Asteroids	1979	100	1,470
Defender	1981	60	1,390
Mortal Kombat II	1993	27	788
Donkey Kong	1981	132	686
Mortal Kombat	1992	24	478

Zdroj: (23)

5.2.3 Prvé herné konzoly

V roku 1967, vývojári vo firme Sanders Associates vedení Ralphom Baerom vytvorili prototyp multiplayer-multiprogramového herného systému, ktorý sa dal napojiť na televíziu. Jeho meno bolo „The Brown Box“. Následne túto konzolu predali firme Magnavox, ktorá konzolu predávala od roku 1972 pod názvom Odyssey, prvá herná konzola. V následných rokoch táto primitívna konzola nedokázala súperiť s konkurenciou a prestala sa predávať. (24)

Jedna z 28 hier, ktoré sa dali hrať na tejto konzole, bola inšpirovaná arkádovou hrou „Pong“ od firmy Atari, ktorá bola ich prvá vydaná arkádová hra v roku 1972. V roku 1975 firma Atari vydala na trh domácu verziu hry „Pong“, ktorá bola úspešná ako jej arkádová verzia. Firma Magnavox sa následne súdila s Atari za kopírovanie a nakoniec sa Atari stala koncesionárom na ďalších 20 rokov. Magnavox taktiež získala viac ako 100 miliónov dolárov v súdnych sporoch týkajúcich sa Odyssey a jej patentov na videohry. (24)

V roku 1977 Atari vydala vlastnú konzolu pod menom Atari 2600. Konzola obsahovala joystick a vymeniteľné herné kazety, ktoré dokázali prenášať farebný obraz. Táto konzola naštartovala druhú generáciu herných konzol. (24)

Následne v roku 1983 prišla herná kríza. Zapríčinilo to veľa faktorov vrátane trhu s prehnanými hernými konzolami, konkurencii v oblasti počítačových hier a veľké množstvo „overhype“ hier, nekvalitných hier, ako je neslávna hra „ET“, ktorú Atari založila na filme a je často považovaná za najhoršiu hru, ktorá bola kedy vytvorená. Táto kríza v nasledujúcich rokoch spôsobila skrachovanie množstva firiem, ktoré sa špecializovali na herné konzoly a počítače. (24)

Od roku 1985 začala kríza ustupovať a to najmä vďaka spoločnosti „Nintendo Entertainment System“, ktorá prišla v tomto roku na americký trh. Nintendo prinieslo na trh vylepšenú 8-bitovú grafiku, farby, zvuk a tak isto aj hrateľnosť. Vytvorila hry ako „Super Mario Bros.“, „The Legend of Zelda“ a „Metroid“. Tieto legendárne hry existujú do dnes, keďže stále vychádzajú nové diely hier. Najnovšie vyšlo pokračovanie hry „Metroid: Samus Returns“ v 2017 (to by som ešte overila, že či je naozaj posledná). Nintendo sa poučilo z chýb svojich predchodcov, takže zaviedlo množstvo pravidiel, ktoré museli spoločnosti splniť aby mohli vydať hru na ich konzolu. Toto zabránilo vydaniu nízko kvalitných hier. Ďalší prelomový rok bol 1989, kedy spoločnosť Nintendo opäť spopulárnili ručné konzoly vydaním 8-bitového game boy-a a sním aj veľmi populárnu hru tetris. Do súčasnosti táto spoločnosť vydávala populárne ručné konzoly ako napríklad Game boy color v roku 1998, Nintendo DS v roku 2004, Nintendo 3DS v roku 2011 a najnovšie Nintendo switch v roku 2017. (24)

5.2.4 Prvá konzolová „vojna“

Spoločnosť Sega v roku 1989 vydala svoju 16-bitovú konzolu Genesis v Severnej Amerike ako nástupcu svojho systému Sega Master z roku 1986, ktorá nedokázala dostatočne konkurovať

NES. So svojou technologickou nadradenosťou voči NES, šikovnému marketingu a uvoľneniu hry Sonic the Hedgehog v roku 1991 urobil Genesis významný pokrok proti svojmu súperovi. V roku 1991 vydalo Nintendo svoju 16-bitovú konzolu Super NES v Severnej Amerike a spustila prvú skutočnú "konzolovú vojnu". (24)

Od začiatku do polovice deväťdesiatych rokov minulého storočia sa objavilo množstvo populárnych hier na oboch konzolách vrátane nových hier, ako sú Street Fighter II a Mortal Kombat. Aj keď hra Mortal Kombat je veľmi brutálna a obsahuje veľa krvi, stala sa veľmi populárnou. Najnovšia verzia, ktorá pre túto hru vyšla v roku 2016, je 10 verzia. (24)

Ako odpoveď na násilné hry, Sega vytvorila „Videogame Rating Council“ v roku 1993, aby poskytla opisné označenie pre každú hru predávanú na domácej konzole spoločnosti Sega. Rada neskôr dala podnet celosvetovej rade pre „Entertainment Software Rating Board“, ktorá sa používa dodnes na hodnotenie videohier podľa ich obsahu. (24)

V polovici deväťdesiatych rokov minulého storočia sa videohry dostali do popredia vďaka uverejnenia akčného filmu Super Mario Bros. v roku 1993. Po ňom nasledovali Street Fighter a Mortal Kombat počas nasledujúcich dvoch rokov. Následne bolo vydané množstvo filmov založených na video hre. (24) Vďaka väčšiemu počtu hier, nižšej cene a úspešnému marketingu sa konzola Genesis dostala do popredia na americkom trhu a nechala za sebou konkurenciu ako napríklad SNES. (24)

5.2.5 Začiatok éry 3D hier

So skokom v oblasti počítačovej technológie priniesla piata generácia videohier trojrozmernú éru hrania hier.

V roku 1995 spoločnosť Sega vydala v Severnej Amerike svoj systém Saturn, prvú 32-bitovú konzolu, ktorá namiesto kaziet využívala CD, o päť mesiacov v predstihu. Tento krok bol uskutočnený kvôli tomu, že spoločnosť Sony sa chystala predávať neskôr v ten istý rok svoju prvú konzolu, Playstation, ktorá bola o 100 dolárov lacnejšia ako konzola Saturn. Nasledujúci rok spoločnosť Nintendo vydala svoj 64-bitový systém založený na kazetách, Nintendo 64. (24)

Aj napriek tomu, že Sega a Nintendo zverejnili svoj spravodlivý podiel vysoko hodnotených 3D titulov, ako napríklad „Virtua Fighter“ na Saturn a Super Mario 64 na Nintendo 64, tieto dve spoločnosti v oblasti videohier nemohli konkurovať spoločnostiam Sony, ktoré vyrábali hry pre Sony a Playstation. Tieto spoločnosti vydávali hry s exkluzívnymi titulmi, čo sa na ine konzoly nemohlo. Následne spoločnosť Sony dominovala trhu po niekoľko rokov. Veľmi tomu pomohlo aj vydanie Playstation 2, ktoré bolo uvedené v roku 2000. Konzola bola schopná hrať originálne hry Playstation a zároveň to bola aj prvá konzola, ktorá používala disky DVD. Vďaka tomuto a aj iným faktorom sa stala najpredávanejšou konzolou všetkých čias aj napriek početnej konkurencii ako Sega Dreamcaster (1999), Nintendo Gamecube (2001) alebo Microsoft Xbox (2001). (24)

Dreamcast bol považovaný mnohými za naddobový a zároveň za jednu z najlepších konzol, ktoré sa kedy vyrobili a to z niekoľkých dôvodov, vrátane schopnosti pre online hry. Bol to obchodný zámer firmy Sega, ktorý v minulosti doplatili na to, že nedovoľovali iným firmám vyrábať hry na ich konzoly. To sa zmenilo v roku 2001, kedy bol zákaz zrušený. (24)

5.2.6 Moderný vek video hier

V roku 2005 a 2006 vďaka Microsoft Xbox 360, Sony Playstation 3 a Ninto Wii začal nový moderný vek video hier s vysokým rozšírením. Aj napriek tomu, že Playstation 3 ako jediná konzola podporovala Blu-ray disky, tak Sony po prvýkrát pocítovala obrovský tlak zo strany konkurencie. Xbox 360, ktorý mal podobnú grafiku ako Playstation 3, bol chválený pre svoj online herný ekosystém a získal oveľa viac ocenení „Game Critics Awards“ ako ostatné platformy v roku 2007. Taktiež predstavil Microsoft Kinect, najmodernejší systém snímania pohybu, ktorý ponúkal iný spôsob, ako hrať videohry. (24)

A napriek tomu, že je technologicky horší ako ostatné dva systémy, Wii prekonala svoju konkurenciu v oblasti predaja. Jeho diaľkové ovládače citlivé na pohyb robili hranie hier aktívnejšími než kedykoľvek predtým a pomohli osloviť oveľa väčšiu časť širokej verejnosti vrátane ľudí v domovoch dôchodcov. (24)

Ku koncu desaťročia a začiatku ďalšieho sa videohry rozšírili na platformy sociálnych médií, ako je Facebook a na mobilné zariadenia, čím sa zapojilo do hrania video hier aj viac „casual“ publikum. (24)

8. generácia konzolí sa začala predajom Nintendo Wii U v roku 2012, po ktorom nasledovali Playstation 4 a Xbox One v roku 2013. Napriek tomu, že Wii U obsahovala diaľkové ovládanie dotykovej obrazovky, ktoré umožňovalo hrať hry na televízii a aj mimo nej, Wii U bol veľký neúspech oproti predchodcovi Wii a následne bol jeho predaj prerušený v roku 2017. (24)

V roku 2016 spoločnosť Sony vydala výkonnejšiu verziu svojej konzoly, ktorá sa nazýva Playstation 4 Pro, prvá konzola schopná 4k video výstupu. Následne v roku 2017 vydalo Nintendo svojho nástupcu Wii U, Nintendo Switch, opäť jediný systém, ktorý dokázal tú istú hru premietiť na TV a aj na prenosnom displeji ovládača. Spoločnosť Microsoft uvoľnila svoju konzolu 4K-ready, Xbox One X, koncom roka 2017. (24)

So svojimi novými upravenými konzolami majú spoločnosť Sony a Microsoft momentálne svoje priority nastavené na virtuálnu realitu, na technológiu, ktorá má potenciál zmeniť spôsob, akým hráči hrajú videohry. (24)

5.3 Rozdelenie hier

5.3.1 ESRB hodnotenie hier

ESRB (The Entertainment Software Rating Board) poskytuje stručné a objektívne informácie o obsahu videohry, aby spotrebiteľ, najmä rodič, mohol činiť informované rozhodnutia. ESRB hodnotenie má 3 časti – veková vhodnosť, opis obsahu a interaktívne elementy.



Obr. 5.1: ESRB hodnotenie "E" (25)

Obsah hry je všeobecne vhodný pre všetky vekové kategórie. Môže obsahovať minimum rozprávok, fantasy a/alebo zriedkavé násilie či použitie mierne nevhodného jazyku.



Obr. 5.2: ESRB hodnotenie "E10" (25)

Obsah je všeobecne vhodný pre vekovú skupinu od 10 rokov. Môže obsahovať viac rozprávok, fantasy, zriedkavé násilie, použitie mierne nevhodného jazyku a/alebo minimum nevhodných tém.



Obr. 5.3: ESRB hodnotenie "T" (25)

Obsah je všeobecne vhodný pre vekovú skupinu od 13 rokov. Môže obsahovať násilie, nevhodné témy, krutý humor, minimum krvi, simulované hazardné hry a/alebo zriedkavé použitie nevhodného jazyku.



Obr. 5.4: ESRB hodnotenie "M" (25)

Obsah je všeobecne vhodný pre vekovú skupinu od 17 rokov. Môže obsahovať intenzívne násilie, krv, sexuálny obsah a/alebo nevhodný jazyk.



Obr. 5.5: ESRB hodnotenie "AO" (25)

Obsah je všeobecne vhodný pre vekovú skupinu od 18 rokov. Môže obsahovať dlhé scény intenzívneho násillia, grafický sexuálny obsah a/alebo hazard s reálnou menou.



Obr. 5.6: ESRB hodnotenie "RP" (25)

Ešte nie je priradený konečný rating ESRB. Vyskytuje sa iba v reklamných, marketingových a propagačných materiáloch súvisiacich s fyzickou (napr. zabalenou) videohrou, pri ktorej sa očakáva, že bude mať hodnotenie ESRB, a malo by byť nahradené iným hodnotením po jeho priradení.

Opis obsahu má veľké množstvo kategórií: Odkazovanie na alkohol, animovaná krv, krv alebo zmrazenie časti tela, kreslené násilie, komické zlo, krutý humor, odkazovanie na drogy, fantasy násilie, intenzívne násilie, použitie nevhodného jazyku, referencie na nevhodné témy, dospelý humor, čiastočná nudita, nudita, reálny hazard, sexuálny obsah, sexuálne témy, sexuálne násilie, simulovaný hazard, nevhodný jazyk, časté referencie na nevhodné témy, silný sexuálny obsah, nevhodné témy, odkazovanie na tabak, užívanie alkoholu, užívanie drog, užívanie tabaku, násilie a odkazovanie na násilie. (25)

Interaktívne elementy sú 4. Prvým z nich je nákup v hre. Znamená to, že v hre je schopný užívateľ zakúpiť si digitálny tovar, prémiový účet a pod. pomocou reálnych peňazí. Ďalší element je interakcia medzi užívateľmi, čo označuje možné vystavenie nefiltrovaného / necenzurovaného obsahu vytvoreného používateľmi vrátane komunikácie medzi používateľmi a zdieľanie médií prostredníctvom sociálnych médií a sietí. Tretím elementom je zdieľanie polohy. Ob-

sahuje možnosť zobrazenie reálnej adresy iným užívateľom aplikácie. Posledný element je neobmedzený prístup k internetu. (25)

Príklad hra Total war: Three kingdoms. Pri odhalení tejto hry v lete 2018 ešte nemala táto hra žiaden ESRB rating.



Obr. 5.7: Bez ESRP hodnotenia (26)

Pri najnovšom hodnotení tejto hry už je hodnotenie ESRB priradené a to, že je vhodné pre vekovú skupinu od 13 rokov a obsahuje násilie.



Obr. 5.8: ESRP hodnotenie pre hru Total war: Three kingdoms (27)

Na oficiálnych stránkach ESRB si vy každý užívateľ vyhľadať hodnotenie hier, ktorým bolo toto hodnotenie priradené.

5.3.2 Žánre video hier

Herný priemysel, ako každý iný, sa rozdeľuje do veľkého množstva skupín. Tieto skupiny nazývame herné žánre, ktoré sa rozdeľujú podľa obsahu, cieľa, spôsobu hrania a ďalších iných faktorov. Keďže týchto žánrov je veľké množstvo, vybral som jedny z najpopulárnejších podľa obsahu.

Akčné hry – akčné hry sú zamerané na reakcie hráča a na koordináciu medzi zmyslami hráča. Veľká väčšina hier sa dá kvalifikovať ako akčná hra, ale väčšinou sa jedná o hry bojového typu. Či už sa jedná o bojové hry ako Tekken alebo Mortal Kombat, čo sú hry 1v1 v malej bojovej aréne alebo hry ako Call of Duty alebo Battlefield, kde už je svet o veľa väčší, tak ako aj počet hráčov.

Adventúra – tento žáner je jeden z najstarších žánrov založených na plnení misií, hernom

svete a príbehu. Pri adventúrach nie je treba koordinácia zmyslov, ale logické myslenie pri riešení hádanok. Na ich riešenie musí hráč napríklad komunikovať s hernými postavami alebo hľadať riešenie v hernom svete. Tieto hry sú väčšinou „singleplayer“ hry, čiže hráč hrá hru sám.

RPG – alebo „Role playing game“ je hra, v ktorej si hráč vytvorí svoju virtuálnu postavu a následne za ňu hrá. Následne môže hráč pomocou plnenia rôznych úloh túto postavu vylepšovať, zvyšovať jej úroveň a podobne. Najznámejší podžánre RPG je MMORPG alebo „Massively multiplayer role playing game“. V týchto hrách sa už pridáva aj možnosť hrania online s inými hráčmi v spoločnom svete. Tieto hry sa stali veľmi populárne uvedením hry World of Warcraft vydanéj v roku 2004. Avšak popularita týchto hier v posledných rokoch klesá, keďže vyžadujú obrovské množstvo času a dnešní hráči skôr preferujú hry, pri ktorých sa zabavia a nestrávia pri nich hodiny času.

Strategické hry – tieto hry vyžadujú taktické premýšľanie a znalosť danej hry. Dva najpopulárnejšie podžánre sú RTS („Real time strategy“) a MOBA („Multiplayer online battle arena“). RTS strategické hry vyžadujú kontinuálne strategické myslenie počas hrania hry. Väčšinou sú tieto hry zamerané na výstavbu budov, armády a následné porazenie nepriateľa. Postupom hry musí hráč svoju taktiku meniť na základe veľkého množstva faktorov, preto sa považujú tieto hry za jedny z najťažších. Najznámejšie hry tohto typu sú Starcraft séria, Warcraft séria alebo Age of Empires séria. Na rozdiel od RTS hráč pri MOBA hre ovláda iba jednu postavu. V najznámejších hrách ako „LoL“ (League of Legends) alebo „DotA 2“ (Defense of the Ancients 2) hrajú proti sebe 2 tímy po 5 členoch. Cieľom tejto hry je zničiť základňu nepriateľského tímu.

Simulácie – tieto hry sú dizajnované tak, aby presne simulovali aspekty reálnej alebo fiktívnej reality. Obsahujú 3 podžánre a to „CMS“ (Construction and management simulation), Life simulation a Vehicle simulation. Vehicle simulation sa zameriava na simuláciu vozidiel. Hráč je napríklad šofér vlaku a hra simuluje presný beh tohto vlaku (Train simulator). Life simulation alebo simulátor života simuluje život rodiny alebo jedinca, ktorého hráč ovláda. Najznámejším simulátorom života je séria SIMS. CMS sú typ simulačnej hry, kde má hráč za úlohu stavať, rozširovať alebo spravovať fiktívne komunity alebo projekty s obmedzenými zdrojmi. Jedny z najznámejších CMS simulátorov sú séria SIMCITY alebo hra Cities Skylines.

Športové hry – športové hry sú špeciálny typ simulácií, ktoré sa zameriavajú na šport. Tieto hry v reálnom čase simulujú fyziku reálneho športu. Hráč buď hrá proti počítačovo riadenému oponentovi alebo inému hráčovi či už offline alebo online. Najznámejšie hry sú série FIFA, NHL alebo NBA.

FPS – „First person shooter“ je podžánre akčných hier, kde hráč hrá hru z pohľadu prvej osoby. Tieto hry sú bojového typu, kde sa hráč snaží zneškodniť nepriateľov. Najznámejšou FPS sériou je „Counter-Strike“. Najnovšou hrou tejto série je „Counter-Strike: Global offensive“, ktorá vyšla v roku 2012 a je jednou z najpopulárnejších hier na platforme STEAM. (28)

Battle royal – tento typ hier sa stal populárnym v posledných rokoch. Jedná sa o hru, kde

hráči bojujú proti sebe na jednej mape a ten, ktorý prežije vyhráva. Tímy sa môžu skladať z jedného, dvoch, troch a aj to 4 hráčov. Každý hráč si zvolí miesto, kde chce hru začať a postupne po mape zbiera rôzne predmety (zbrane, vesty, granáty) a snaží sa prežiť a zároveň zabíjať čo najviac nepriateľov. Postupom času sa na mape zobrazí jedovatý dym, ktorý hernú plochu zmenšuje až na minimálne rozmery. Najzámennejšie Battle royal hry sú PUBG a Fortnite.

5.3.3 Business modely video hier

Hry môžeme ešte deliť aj podľa ich business modelu. Sú 3 typy. „F2P“ (Free to play), „P2P“ (Pay to play) a „B2P“ (Buy to play). Prvý typ F2P je typ hry, ktorú môže hrať každý bez toho aby za ňu musel platiť. Avšak vo väčšine týchto hier je množstvo mikrotraskácií, ktoré môžu hráčov, ktorí do hry investujú reálne peniaze veľmi zvýhodniť (Séria FIFA). Avšak sú aj také hry, v ktorých si hráč môže dokúpiť iba vizuálny skin, či už na svoju postavu, alebo zbrane a vôbec nebude zvýhodnený oproti iným hráčom (League of Legends alebo Counter-strike). Ďalším typom je P2P, ktorá umožňuje hranie hry po zaplatení mesačného alebo iného predplatného (World of Warcraft). Posledným typom sú B2P hry, ktoré si stačí raz kúpiť a stanete sa ich vlastníkom. Hráč si ich môže kúpiť v kamennom obchode, kde dostane disk v obale alebo si ich môže kúpiť na internetovom obchode, kde dostane kľúč k odomknutiu hry alebo si hru môže priamo kúpiť na platforme (STEAM) a bude mu priradená k účtu.

Popularita rôznych žánrov sa líši od platformy, na ktorej sa tieto hry hrajú. Mobilné hry hrajú najviac hráči, ktorý nemajú veľa času, čiže sa zameriavajú na F2P hry, ktoré však majú veľké množstvo mikrotransakcií, ktoré zvýhodňujú hráčov, ktorí platia reálne peniaze (Candy Crush, Clash of Clans). Konzoly vďaka joysticku majú výhodu oproti počítačovým užívateľom v lepšom a presnejšom ovládaní pri závodných alebo športových hrách. Najpopulárnejšou hrou v roku 2018 na konzolách ako aj na počítači bola hra Fortnite s 200 miliónmi registrovaných hráčov. (29)

5.4 Online obchod

5.4.1 Online obchod s hrami

V minulosti sa počítačové hry dali kúpiť iba v kamenných obchodoch, ale v dnešnej dobe je väčšina hier zakúpená na internete. Hry na internete sa dajú kúpiť buď na veľkých internetových obchodoch (Amazon, Alza), kedy hráč dostane reálnu kópiu hry v obale alebo si ich môže kúpiť na online platforme (Steam, Origin), kedy hráč dostane virtuálnu kópiu hry, ktorá je pripísaná na jeho účet na danej platforme. Taktiež si môže kúpiť na internetových tržniciach (G2A) kľúč na hru, ktorý následne použije pri inštalácii hry. Prvé dva typy nakupovania hier sú najbezpečnejšie, keďže hráč kupuje originálnu kópiu hry priamo od predajcu.

Pri internetových tržniciach ako G2A je síce cena nižšia, ale s kúpou na takýchto platformách prichádza riziko, že kľúč nebude fungovať.

5.4.2 Online obchod s hernými produktmi/menami

Veľké množstvo hier, či už F2P, B2P alebo aj P2P, má možnosť kupovania si produktov priamo v hre, a to buď za reálne peniaze alebo za hernú menu. Kde je možnosť kúpy, tam je možnosť aj výmeny a v hernom priemysle je to presne tak. V niektorých hrách, najmä žánru MMORPG, je hráč schopný vymieňať herné produkty s inými hráčmi, či už za iný herný produkt, hernú menu alebo za reálne peniaze. Prvé dve metódy vždy musia potvrdiť obaja hráči, avšak pri výmene za reálne peniaze nastáva riziko, že jeden z hráčov podvedie toho druhého. Predávajúci hráč nemusí po prevode peňazí predmet vymeniť, alebo naopak, po výmene nemusí kupujúci hráč zaplatiť. Takmer všetky hry majú takéto výmeny zakázané, ale keďže sa na tieto obchody veľmi ťažko príde, tak sú veľmi časté, hlavne pri naivných hráčoch. Pre tieto nelegálne obchodovania vznikli aj rôzne internetové stránky, ktoré tieto obchody umožňujú. Na stránke <https://www.g2g.com/> si je schopný hráč kúpiť herné meny, kredity pre rôzne platformy, herné produkty, herné účty, vizuálne vylepšenia predmetov/postáv alebo si môže zaplatiť „boostera“ (človek, ktorý za finančnú odmenu hrá na účte iného hráča za účelom vylepšenia daného účtu). Keďže G2G funguje na rovnakom princípe ako G2A, čiže ako internetové trhovisko, s využívaním týchto služieb opäť prichádza veľké riziko.

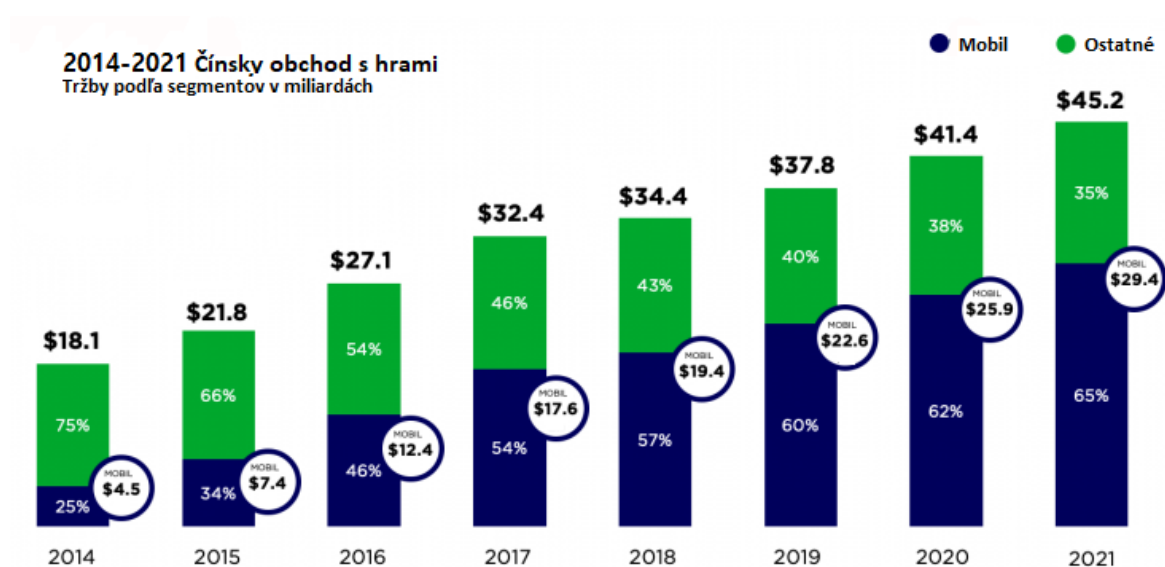
5.5 Trendy v hrách a na trhu herného priemyslu

Herný priemysel, ako každý iný, je vysoko založený na popularite a trendoch. Napríklad hra Pokemon GO, ktorá vyšla v lete 2016 na mobilné zariadenia. Po vypustení hry na trh si túto hru stiahlo viac ako 130 miliónov ľudí po celom svete. Vynikajúci nápad sa spojil s každému známou témou Pokemon a vznikol celosvetový fenomén. Bola to jedna z prvých veľmi úspešných hier na mobilné zariadenia, ale v roku 2017 a 2018 je táto, predtým populárna hra na vzostupe. Stereotypné vlastnosti hry, podvádžanie, skorá nutnosť platenia herného tovaru pomocou peňazí a aj rapídne sa zvyšujúca konkurencia na mobilnej platforme zapríčinili vzostup. (30)

Vývojové trendy v hrách sú rôzne pre každú platformu. Na počítačovej platforme dlhú dobu dominovali hry typu MMORPG (WoW, Runescape) následne MOBA (DotA 2, LoL) a za posledné dva roky sa k MOBA hrám pridali aj hry typu Battle royal (Fortnite, Pubg). Podľa štatistík hernej platformy STEAM sú 3 najviac hrané hry na ich platforme DotA 2, Pubg a Counter-strike: Global Offensive s 905 000, 810 000 a 636 000 denným počtom hráčov ku dňu 2.2.2019. (31) Avšak v porovnaní s League of Legends, ktorú denne hrá vyše 27 miliónov ľudí a mesačne cez 80 miliónov, sú tieto čísla veľmi nízke. (32) V decembri 2018 boli na PC 3 najpopulárnejšie hry v Európe a Severnej Amerike League of Legends, Counter-Strike: Global Offensive a Fortnite. (33)

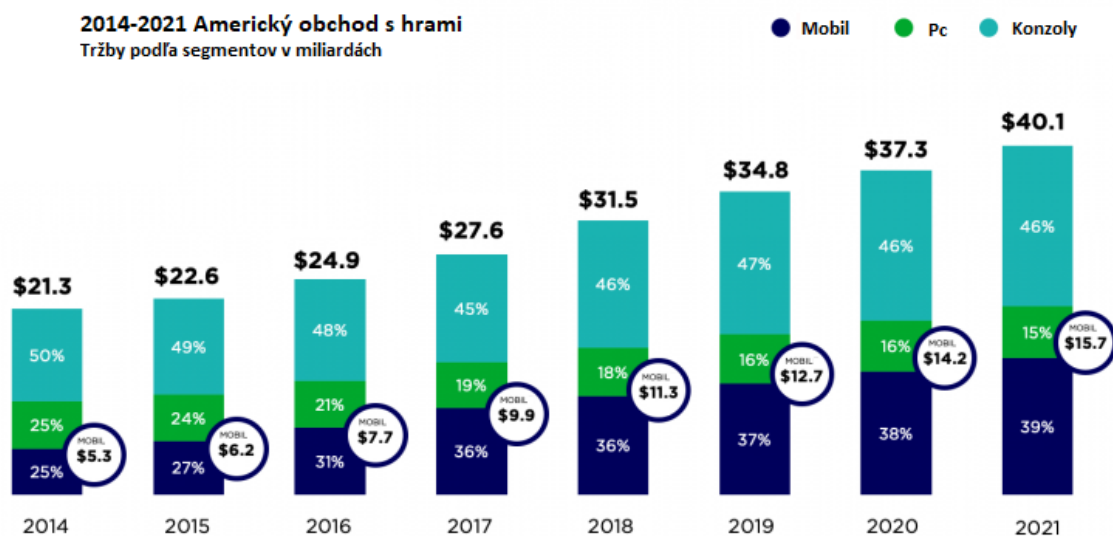
Na rozdiel, od už spomenutých hier, hra Fortnite je dostupná nielen na počítač, ale aj na Playstation, Xbox a Nintendo, čo je veľkou výhodou oproti ostatným hrám. Táto hra, vydaná v roku 2017, si získala hlavne hráčov nižšej vekovej kategórie a taktiež hráčov, ktorí viac vyhľadávajú jednoduchšie hry, ktoré si môžu zahrať s kamarátmi. Keďže je táto hra F2P a aj jej hardwarové požiadavky sú veľmi nízke, tak si ju môže stiahnuť skoro každý.

Trh herného priemyslu sa každým rokom mení a od roku 2017 s 36%, mu vládne trh s hrami mobilného priemyslu. Je to následkom veľkého množstva hier, do ktorých musí dať hráč nadmerné množstvo reálnych peňazí, aby mohol byť kompetitívny s inými hráčmi. Mobilnému a aj celému hernému marketu vládne Juhovýchodná Ázia na čele s Čínou, Japonskom a Južnou Kóreou. Z celkových príjmov z tohto odvetvia bolo v roku 2018 až 49,1% z Ázie, 25,1% zo Severnej Ameriky, 15,8% zo západnej Európy a iba 2,8% z východnej Európy.



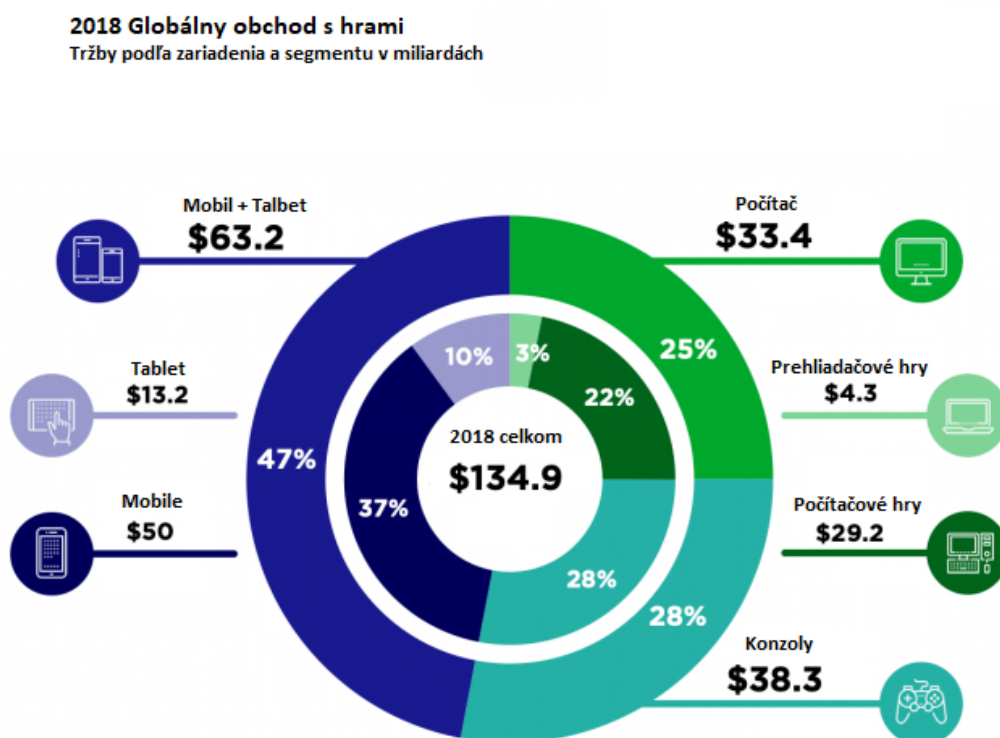
Obr. 5.9: Vývoj a predpokladaný vývoj Čínskeho trhu hier (34)

Na grafe vyššie je vidieť, ako trend mobilných hier v roku 2017 prekročil hranicu 50% v porovnaní s inými príjmami z tohto odvetvia. Najmä vďaka čínskemu marketu je v hernom odvetví najvyšší zisk práve z mobilných hier a tabletových hier. Dokopy činia okolo 47%. Následne druhou najväčšou skupinou sú konzole, ktoré majú približne 28%. Je to najmä vďaka trhu v Severnej Amerike, v ktorom konzole vedú v zisku a dosahujú až 46% celkového zisku.



Obr. 5.10: Vývoj a predpokladaný vývoj Amerického trhu hier (34)

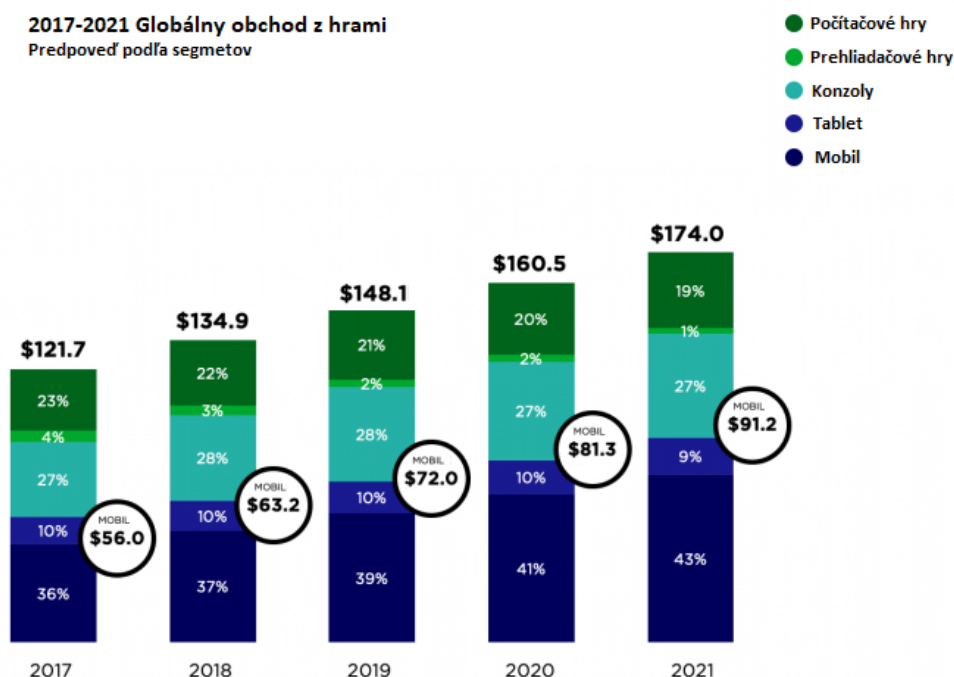
Následne poslednou skupinou je počítačová platforma s 25%. Z týchto 25% je 22% z predaja hier typu B2P a 3% sú z mikrotransakcií v prehliadačových hrách.



Obr. 5.11: Globálne tržby z hier (34)

Celkový zisk z herného priemyslu bol v roku 134,9 miliardy dolárov. Predpokladá sa, že zisk bude iba rásť, keďže herný priemysel sa stáva jedným z hlavných zábavných priemyslov na svete. Vývojový trend ukazuje, že aj po nasledujúce 3 roky by mal dominovať trhu mobilný

herný priemysel a to najmä na čínskom trhu. Pri konzoliach sa predpokladá, že budú stále v podobných pomeroch, okolo 28%, a pri počítačovom odvetví sa predpokladá pokles pomeru, následkom predpokladaného zvýšenia počtu hráčov v ostatných odvetviach.



Obr. 5.12: Vývoj a predpokladaný vývoj globálneho trhu hier (34)

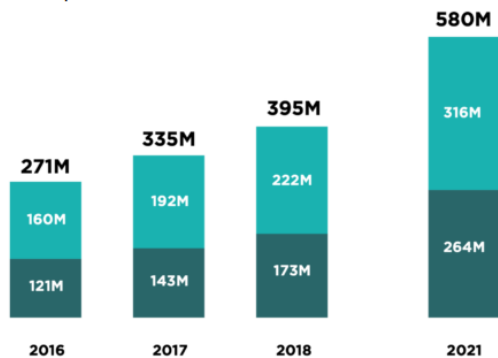
5.6 Esports a sponzori

5.6.1 Esports

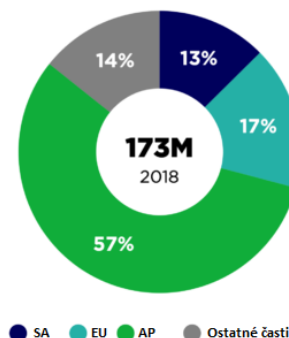
Esports alebo elektronický šport šplhá na popredné miesta v sledovanosti. Sledovanosť finálnych zápasov v počítačových hrách predbieha sledovanosť sledovanosti finálnych zápasov iných športov. Sledovanosť finálnych zápasov NHL bolo v priemere 4,8 milióna , NBA 17,7 milióna a NFL 103,4 milióna ľudí. (35) (36) (37) Finále majstrovstiev sveta v hre League of Legends, ktoré sa konalo 3.11.2018 v Busane (Južná Kórea) pozeralo 205,3 miliónov ľudí po celom svete. Ďalší turnaj tejto hry, ktorý sa odohral v máji 2018, mal 127,5 milióna sledovateľov a finále v roku 2017 malo 106,2 miliónov sledovateľov. (38) Na platformách ako YouTube alebo Twitch si každý deň môžu hráči pozrieť videá alebo živé prenosy iných hráčov. Najviac sledovaná hra na YouTube a aj na Twitch v januári 2019 bola hra Fornite s 35 respektíve 124,8 miliónmi napozieraných hodín. Na platforme Twitch bola druhá najsledovanejšia hra League of Legends s 98,2 miliónmi a na platforme YouTube to bola hra PUBG s 20,5 miliónmi hodín. Fortnite je už od marca 2018 každý mesiac najviac sledovaná hra na platforme Twitch a predbehla dlhodobo najpopulárnejšiu hru League of Legends. Na platforme YouTube mala taktiež veľký úspech, keďže minulý rok bola najsledovanejšou hrou 8 mesiacov. Toto miesto si striedala s League of Legends a PUBG. (39)

Rast sledujúcich Esports
Vývoj a prognóza

Príležitostný sledujúci
Nadšenci Esports



Nadšenci Esports za rok 2018



Obr. 5.13: Vývoj a predpokladaný vývoj počtu sledujúcich Esports (34)

Najviac sledovateľov je z ázijských krajín (%), a to najmä z Číny. Následne z Európy 17% a Severnej Ameriky 13%. Sledovateľov je spolu skoro 400 miliónov. Okolo 56% sú príležitostní diváci a 44% sú nadšenci Esportu.

Esport turnaje majú čím ďalej väčšiu popularitu, keďže sa zvyšuje aj množstvo peňazí, ktoré môže víťaz vyhrať. Hranie hier sa už berie ako šport, keďže sa možno po prvýkrát ukáže aj na olympijských hrách v roku 2024 v Paríži, a vrcholní športovci dokážu vydať výkony, ktoré si obyčajní hráči nevedia predstaviť. (40)

Ceny, o ktoré tímy bojujú v týchto turnajoch, sa šplhajú už do astronomických výšin. Najznámejšie hry s vysokým „Prize Pool“ sú Dota 2 a League of Legends. Zatiaľ najvyšším price poolom bol turnaj „The International 2018“ hry Dota 2, a to 25,5 milióna dolárov. Víťaz si odviezol vyše 11 miliónov, strieborný tím 4 milióny a bronzový tím 2,6 milióna amerických dolárov. Základný price pool tohto turnaja bol 1,6 milióna dolárov. Avšak spoločnosť VALVE, ktorá je výrobcom tejto hry umožňuje hráčom kupovať rôzne položky v hre. Následne pridáva do cien pre tímy časť zo zisku z predaja, presnejšie v roku 2018 to bolo 23,9 milióna dolárov, čo zvýšilo celkový price pool skoro o 1500%. (41)

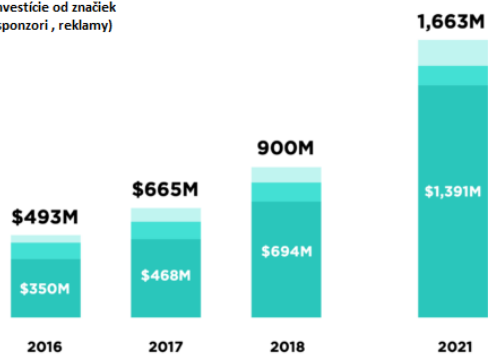
	TITLE	PRIZE POOL ▼
	The International 2018 Dota2, The International, Valve	\$25 532 177
	The International 2017 Dota2, The International, Valve	\$24 787 916
	Fortnite Fall Skirmish Fortnite, Epic Games	\$6 018 000
	2016 World Championship LoL, LoL Worlds, Riot Games	\$5 070 000
	2017 World Championship LoL, LoL Worlds, Riot Games	\$4 170 000
	The Boston Major 2016 Dota2, Dota Major Championships, PGL	\$3 000 000
	PUBG Global Invitational 2018 PUBG, PGI 2018, PUBG Corporation	\$3 000 000
	Fortnite Celebrity Pro-Am Fortnite, Epic Games	\$3 000 000
	The Kiev Major 2017 Dota2, Dota Major Championships, PGL	\$3 000 000

Obr. 5.14: Turanje a "Prize Pool"pre daný turnaj (38)

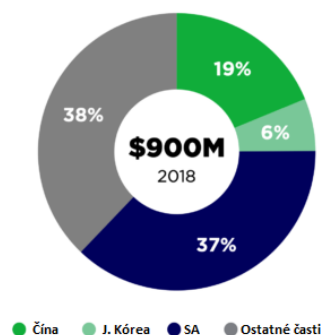
Výnosy z Esport sa rok dostali na hranicu 900 miliónov amerických dolárov, pričom 50,6% je od sponzorov, 20% za mediálne práva, 18% reklamy, 13% poplatky vydavateľov hier a 10% za lístky a za iný tovar spojený z Esports. Predpokladá sa, že v roku 2021 bude výnos skoro dvojnásobne vyšší a to 1 miliarda a 663 miliónov amerických dolárov (z čoho 1,391 miliardy bude od sponzorov, reklám a mediálnych práv). (34)

Rast tržieb z Esports
Vývoj a prognóza

● Tovar a lístky
● Poplatky pre tvorcu hry
● Investície od značiek (sponzori, reklamy)



Tržby z Esport za rok 2018



Obr. 5.15: Vývoj a predpokladaný vývoj globálnych tržieb z Esports (34)

Profesionálni hráči sa berú ako športovci. Majú veľké množstvo sledovateľov na sociálnych sieťach, vlastných sponzorov a sú súčasťou tímu, s ktorým sú viazaní zmluvami. Profesionálni hráči nie sú vekovo obmedzovaní, avšak ak chcú hrať na turnajoch danej hry, musia spĺňať minimálnu vekovú hranicu danej hry, ESRB rating.

5.6.2 Sponzori

Takmer každý profesionálny tím má sponzorov. Či už od značiek, ktoré im dodávajú príslušenstvo ako počítače, klávesnice, slúchadlá, herné stoličky alebo aj značky, ktoré vôbec s herným priemyslom nesúvisia, ako napríklad Gillete alebo Redbull. Títo sponzori sponzorujú tímy a turnaje finančne, produktami, ale aj cenami, ktoré sa môžu vyhrať.

6. Steam

V tejto časti je čitateľovi priblížená platforma steam a jej zabezpečenie.

Steam je platforma od firmy Valve, vydaná 12. septembra 2003, kde sa digitálne distribuujú, predávajú a kupujú video hry. Táto platforma vznikla z dôvodu problému s aktualizáciou hier, keď mali hráči problémy s prihlásením sa do hry a kvôli implementácií silnejších proti pirátskych a hackerských opatrení. Steam ponúka manažment digitálnych práv, matchmakingové servisy, živé vysielanie videa a služby sociálnych sietí. Steam taktiež hráčovi ponúka inštaláciu a automatickú aktualizáciu hier, ukladanie na cloud a komunitné funkcie ako zoznam priateľov, skupiny hráčov a hlasový rozhovor alebo chatovanie v hre. (42)

Steam taktiež ponúka voľne dostupnú API nazývanú „Steamworks“, ktorú môžu vývojári použiť na integrovanie rôznych funkcií Steamu, ako napríklad networking, matchmaking, úspechy v hre, mikrotransakcie a taktiež podporu pre hráčmi vytvorený obsah pomocou „Steam Workshop“.

Steam je dostupný na všetky veľké platformy ako Microsoft Windows, macOS, Linux, iOS, Android a Windows Phone, a to v 29 jazykoch. Napríklad český Steam je preložený na 99%. (43)

6.1 Zabezpečenie platformy Steam

Oblúbenosť spoločnosti Steam viedla k tomu, že v minulosti bola platforma terčom rôznych útokov hackerov a phisherov. Jeden pokus sa vyskytol v novembri 2011, keď spoločnosť Valve dočasne zatvorila komunitné fóra, pričom uviedla, že služba mohla byť ohrozená hackerským útokom. (44) O niekoľko dní neskôr spoločnosť Valve oznámila, že hackeri napadli jednu z ich zákazníckych databáz a že potenciálne umožnila páchatelom prístup k informáciám o zákazníkoch - vrátane zašifrovaných hesiel a údajoch o kreditných kartách. V tom čase spoločnosť Valve nevedela, či útočníci skutočne získali prístup k týmto informáciám alebo objavili metódu šifrovania, avšak napriek tomu upozornili používateľov, aby boli obozretní. (45)

Spoločnosť Valve, v marci 2011 pridala na svoju platformu funkciu Steam Guard z dôvodu ochrany pred kradnutím účtov prostredníctvom phishingových útokov, čo bol jeden z najväčších problémov platformy Steam v danom období. (46) Steam Guard využil ochranu identity poskytovanú druhými generáciami procesorov Core Intel a kompatibilným hardvérom základnej dosky, ktorá umožňuje používateľom zamknúť svoj účet do konkrétneho počítača. Po uzamknutí musí byť aktivita daného účtu v iných počítačoch najskôr schválená používateľom z uzamknutého počítača. Support API pre Steam Guard sú k dispozícii vývojárom tretích strán prostredníctvom Steamworks. (47) Steam Guard tiež ponúka dvojfaktorovú autentifikáciu, ktorá používa jednorazový overovací kód zaslaný na overenú e-mailovú adresu

priradenú k Steam účtu. Táto metóda bola neskôr rozšírená o autentifikáciu pomocou aplikácie Steam, respektíve pomocou Steam Guard Mobile Authenticator. (48) V prípade, že je táto funkcia zapnutá, pri každom prihlásení sa musí zadať kód, ktorý sa zobrazí v Steam mobilnej aplikácii.

V roku 2015, spoločnosť Valve uviedla, že kvôli vysokej cene inventárov hráčov na ich platforme, či už hier alebo iných virtuálnych tovarov, sa hackery a phishery snažia dostať do účtov hráčov pre finančný prospech a neustále odporúča, aby hráči využívali zabezpečenie Steam Guard. Tí, ktorí službu Steam Guard nepoužívali, mali spomalené vymieňanie a predávanie tovaru. Akonáhle si nejaký produkt daný hráč kúpil, následne ho nemohol predat alebo vymeniť nasledujúcich 15 dní. (49)

Napriek tomu, že služba Steam Guard pomáha pri ochrane účtov, je možné ju pri phishingovom útoku jednoducho obísť. Keďže tento kód sa negeneruje na vyžiadanie užívateľa, ako napríklad SMS kód, ale každých 30 sekúnd sa generuje nový, útočníkom stačí rýchlo prepísať prihlasovacie meno, heslo a následne, keď užívateľ vyplní aj svoj Steam Guard kód, tak sa dokážu jednoducho prihlásiť.

Spoločnosť Valve oznámila, že v decembri 2015 bolo odcudzených približne 77 000 účtov každý mesiac, čo umožnilo únosom vyprázdniť inventár používateľov prostredníctvom obchodovania a vymieňania tovaru. Akonáhle v roku 2011 Steam uviedol novú možnosť vymieňania a predávania tovaru, odcudzovanie účtov narástlo viac ako 2000%. (50)

Platforma Steam má v sebe zabudovaný aj prehliadač, ktorý umožňuje hráčom využívať internet stlačením klávesovej skratky a hráč nemusí preklikávať z hry do iného prehliadača. Síce je to pre pohodlné, avšak s používaním tohto prehliadača nastáva veľké množstvo bezpečnostných rizík, na ktoré spoločnosť ReVuln zverejnila v októbri 2012 štúdiu. V nej uvádza, že protokol prehliadača Steam predstavuje bezpečnostné riziko tým, že umožňuje jednoduché klikanie na vytvorenú steam:// URL v prehliadači. (51)

V júli 2015 chyba softvéru umožnila komukoľvek obnoviť heslo na akýkoľvek účet pomocou funkcie "zabudnuté heslo", čím profesionálni hráči a streameri stratili prístup k svojim účtom. (52) A decembri 2015, po reakcii na útok DDoS bola sieť spoločnosti Steam nesprávne nakonfigurovaná, čo spôsobilo dočasné vystavenie stránok obsahujúcich osobné údaje 34 000 používateľom. Spoločnosť Valve uviedla, že dáta, ktoré boli zverejnené boli dodacia adresa, história transakcií, posledné 4 číslice mobilného čísla, emailové adresy a posledné 2 číslice kreditnej karty. (53)

V apríli 2018 spoločnosť Valve pridala nové nastavenia ochrany osobných údajov pre používateľov Steam, pomocou ktorých sú schopní nastaviť svoj účet tak, aby ich aktuálny stav činnosti bol súkromný, viditeľný len pre priateľov alebo viditeľný pre všetkých. Podobným spôsobom môžu taktiež skryť svoje zoznamy hier, inventár a iné prvky profilu. Na jednej strane tieto zmeny priniesli možnosť väčšieho zabezpečenia účtov a súkromia hráčov, avšak na strane druhej negatívne ovplyvnili niektoré stránky, ktoré čerpali dáta z verejných informácií pomocou tejto platformy (odhad počtov predaja daných hier, množstvo hráčov, ktorý

hru hrajú a podobne).

7. Porovnávanie s inými platformami

Pri porovnávaní platforiem sa zameriava na chatovanie medzi hráčmi, žiadosti o priateľstvo, možnosť prihlásenia cez iné sociálne siete a viacfaktorové zabezpečenie. Na konci tejto kapitoly je vyhotovené výsledné porovnanie, ktoré určuje bezpečnosť danej platformy.

7.1 Platforma Battle.net

Platforma Battle.net od spoločnosti Blizzard, cez ktorú hráči hrajú hry ako World of Warcraft, Hearthstone, StarCraft, Overwatch a podobne, funguje na podobnom princípe ako Steam s jedným rozdielom a to, že táto platforma slúži výhradne len na hry od spoločnosti Blizzard. Podobne ako pri platforme Steam, má táto platforma obchod, kde si hráč môže kupovať hry alebo iné produkty využiteľné v hre. Taktiež obsahuje možnosť pridávania priateľov alebo pridávania so do rôznych skupín, kde môže hráč následne komunikovať s inými hráčmi. Na tejto platforme sa nedá obchodovať s tovarom, iba priamo v hrách.

Zabezpečenie na tejto platforme funguje na podobnom systéme ako na platforme Steam. Pri registrácii musí užívateľ zadať heslo, ktoré musí spĺňať vyžadované podmienky a musí vybrať jednu „Security question“, pomocou ktorej sa následne môže užívateľ prihlasovať na iných zariadeniach. Užívateľ si taktiež môže nastaviť dvojfaktorovú autentifikáciu pomocou emailu, SMS, mobilnej aplikácie, už zmienenej „Security question“ alebo pomocou fyzického autentifikátora (USB), ktorý si môže užívateľ zaobstaráť za 6,5 dolára. Spoločnosť Blizzard si nebezpečie, ktoré nastáva pri nevyužití dvojfaktorovej autentifikácie udeľuje a preto hráčov, ktorí si svoj účet zabezpečia, odmenia unikátnym predmetom v hre. (54)

Čo sa týka chatovania medzi hráčmi a žiadosťami o priateľstvo, je na užívateľovi ako si to nastaví. Pridávanie priateľov slúži pomocou mena a kódu hráča, ktorý nie je verejne dostupný, čiže si ľudí nemožno pridávať náhodne. Užívateľ sa taktiež môže prihlásiť pomocou Facebooku alebo Google účtu, čo môže byť pohodlné. Takéto prihlasovanie nesie riziko, že v prípade ak bude odcudzený Facebook účet, phisher sa dokáže dostať aj do účtu Battle.net.

7.2 Platforma GOG

GOG, od spoločnosti CD Projekt, vznikla v roku 2008 a je veľmi podobná platforme Steam. Na tejto platforme si môžu hráči kupovať väčšinou staršie hry, ako napríklad Heroes Might and Magic III alebo Mafia I či II. Za posledné roky sa na tejto platforme začali predávať aj nové hry, ako napríklad Mafia III alebo Witcher III. Čo sa týka obchodu, veľmi sa podobná Steamu. Hru si môže hráč kúpiť buď cez webové stránky alebo priamo cez platformu. Obchodovanie medzi hráčmi na tejto platforme nie je možné.

Zabezpečenie na tejto stránke síce obsahuje dvojfaktorovú autentifikáciu, ale iba pomocou emailu. Užívatelia môžu využívať chatovanie medzi hráčmi, lenže toto chatovanie je možné iba po pridaní do zoznamu priateľ. Do tejto platformy sa dá prihlásiť aj pomocou Facebooku.

7.3 Platforma Origin

Táto platforma, od spoločnosti Electronic Arts, prišla na trh v roku 2011. Hry, ktoré sú na tejto platforme, podobne ako u Battle.net, sú len hry od spoločnosti Electronic Arts (napr. Battlefield, Fifa, Sims alebo Need for Speed). Nie je tu možné obchodovanie medzi hráčmi.

Na tejto platforme je možnosť dvojfaktorovej autentifikácie, a to buď pomocou SMS, mobilnej aplikácie alebo emailu. Síce platforma nemá vlastnú aplikáciu, avšak používa Google Authenticator. Na rozdiel od iných platforiem, musí hráč, ktorý chce hrať FIFA Ultimate Team, čo je jeden z módov FIFA, využiť dvojfaktorové prihlásenie, inak nebude môcť tento mód hrať. (55) Chatovanie medzi hráčmi je možné iba po pridaní do zoznamu priateľov.

7.4 Platforma Epic Games

Platforma Epic Games od spoločnosti Epic games, slúži najmä ako launcher jednej z najviac populárnej hry súčasnosti – Fortnite, aj keď si na tejto platforme môže hráč kúpiť hry aj od iných spoločností. Ani na tejto platforme nie je možnosť obchodovania priamo cez platformu.

Čo sa týka zabezpečenia, tak na tejto platforme je veľké množstvo dvojfaktorových autentifikácií, či už pomocou emailu alebo pomocou autentifikátorov od Google-u, LastPass-u, Microsoft-u a od spoločnosti Authy. Podobne ako spoločnosť Blizzard, tak aj Epic Games ponúka bonus pre hráča, ktorý si nastaví túto autentifikáciu. Tým bonusom je zväčšený priestor v hernom inventári a jeden bonusový predmet. Platí to iba pre platenú časť hry Fortnite. (56) Keďže hra Fortnite sa môže hrať na viacero konzolách ako Xbox, PlayStation a podobne, tak užívateľ má možnosť prihlásiť sa pomocou emailu, Facebooku, Google účtu, Xbox účtu, PlayStation účtu alebo pomocou Nintendo účtu. Tak ako aj na iných platformách, tak aj na tejto je chatovanie možné iba po pridaní do zoznamu priateľov.

7.5 Výsledné porovnanie

Výsledné porovnanie porovnáva vybrané platformy a možnosti zabezpečenia účtu na danej platforme. V tabuľke 6.1 a 6.2 sú platformy porovnané na základe 6 parametrov. Ak daná platforma ponúka danú možnosť, tak je jej priradená 1 a ak možnosť neponúka, tak je jej priradená 0.

Tabuľka 7.1: Porovnanie platforiem

Platforma	Chat	Zoznam priateľov	2FA - email	2FA - SMS	2FA - aplikácia	2FA - autentifikátor
Steam	1	1	1	0	1	0
Battle.net	1	1	1	1	1	1
GOG	1	1	0	0	0	0
Origin	1	1	1	1	1	0
Epic Games	1	1	1	0	0	1

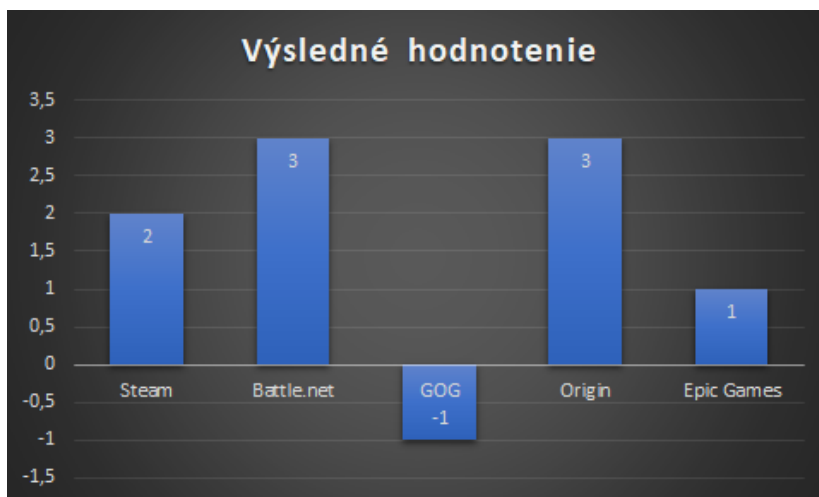
1=ponúka možnosť, 0=neponúka možnosť, Zdroj: Autor

Tabuľka 7.2: Porovnanie platforiem (dodatok)

Platforma	Prihlasovanie pomocou sociálnych sietí
Steam	0
Battle.net	1
GOG	1
Origin	0
Epic Games	1

1=ponúka možnosť, 0=neponúka možnosť, Zdroj: Autor

Keďže všetky porovnávané platformy ponúkajú funkciu Chatu a Zoznamu priateľov, tak v následnom grafe 6.1 sa tieto funkcie nebrali do úvahy. Za každú možnú funkciu autentifikácie je platforme priradený 1 bod (max. 4) a za funkciu prihlásenia pomocou sociálnych sietí je platforme 1 bod odobraný.



Obr. 7.1: Výsledné hodnotenie bezpečnosti platforiem, Zdroj: Autor

Platforma Battle.net a platforma Origin sú najviac zabezpečené platformy. Síce platforma Battle.net obsahuje všetky štyri dvojfaktorové autentifikácie, ale obsahuje aj možnosť prihlásenia cez sociálne siete a to môže ohroziť účet, keďže sa útočník môže prihlásiť do účtu, aj keď pozná prihlasovacie údaje do sociálnej siete obete. Platforma Steam so skóre 2, je síce zabezpečená iba pomocou dvojfaktorovej autentifikácie pomocou emailu a aplikácie, ale keďže neobsahuje funkciu prihlasovania pomocou sociálnych sietí, tak je bezpečnejšia ako platforma Epic Games, ktorá má skóre 1. Najmenej zabezpečená platforma je platforma GOG, ktorá má skóre -1. Na tejto platforme nie je možnosť dvojfaktorovej autentifikácie a obsahuje funkciu prihlásenia pomocou sociálnych sietí, čiže je pre útočníka jednoduchšie odcudziť účet obete.

8. Obchodovanie na platforme Steam a externé stránky

V nasledujúcej kapitole je čitateľovi priblížená téma obchodovania na platforme Steam a na externých stránkach, ktoré ako tovar používajú tovar na platforme Steam.

Keďže na Steame sa dá obchodovať s tovarom aj priamo cez platformu pomocou Steam marketplace, vzniklo veľké množstvo externých stránok, či už na hazard alebo na výmenu herného tovaru za reálne peniaze. Tieto stránky vznikli po aktualizácii „Arms Deal“ v hre Counter-Strike: Global offensive, ktorá pridala do hry vizuálne „skiny“ na zbrane. Tieto skiny si môže hráč zaobstaráť hraním, aj keď šanca, že hráč dostane hodnotný predmet, je veľmi nízka, alebo si môže kúpiť „bedňu“, ktorá obsahuje 17 skinov rôznych kvalít a rôzneho poškodenia. Hráč môže túto bedňu otvoriť pomocou kľúča a dostane jeden náhodný skin. Hodnoty týchto skinov závisia od kvality, poškodenia a od typu zbrane, na ktorý je konkrétny skin určený. Pôvodný zámer týchto skinov bol podľa spoločnosti Valve: „experience all the illicit thrills of black market weapons trafficking without any of the hanging around in darkened warehouses getting knifed to death“. (57) Čiže chcela hráčom sprístupniť skúsenosť s obchodovaním na čiernom trhu, bez toho, aby hráča niekto v tmavom sklادisku dobodol do smrti. Túto skúsenosť chceli hráčom sprostredkovať pomocou možnosti vymieňania a predaja tovaru na trhovisku. Tým priniesli hráčom veľa možností získať skiny, ktoré chcú bez investovania peňazí, ale veľmi ťažko. Taktiež aj pri otváraní bední bola veľmi malá šanca, že hráč dostane hodnotný predmet.

Keďže tieto obchody a výmeny prebiehali priamo na platforme a nie v hre, veľa externých stránok využilo verejne dostupnú API a vytvorili si stránku buď na hazard, výmenu tovaru alebo predaj tovaru za reálne peniaze. Prvé stránky boli na vsádzanie na profesionálne tímy v zápasoch a stránky na výmenu tovaru. Keďže v tom čase bol Counter-Strike: Global offensive jedna z najpopulárnejších hier, tak aj počet divákov na jednotlivých zápasoch a turnajoch bol veľmi vysoký a možnosť zarobenia na výhre svojho obľúbeného tímu nalákala veľké množstvo hráčov na tieto stránky. Jedna z najznámejších stránok je <https://csgolounge.com/>, ktorá funguje doteraz. Tieto stránky fungujú nasledovne - hráč sa prihlási pomocou svojho účtu na dané stránky a následne vloží predmety, s ktorými chce vsádzať alebo ktoré chce vymieňať. Následne mu príde na jeho Steam účet ponuka k vymeneniu tovaru od jedného z botov danej stránky. Po úspešnej výmene tovaru sa peňažná hodnota skinu, väčšinou menšia ako reálna hodnota na platforme, pripísala na účet na stránke. Následne hráč mohol vsadiť na tím, ktorý si vybral. Následne ak vyhral, tak sa mu pripočítala výhra a ak prehral, tak odpočítal vklad. Výhru si mohol hráč vybrať pomocou predmetov, ktoré si zvolil a potom mu bot stránky poslal ponuku na výmenu tovaru s jeho vybranými predmetmi. Postupom času začali vznikať aj stránky čisto na hazard, ktoré sprevádzkovali online kasíno, kde mohli hráči hrať ruletu, blackjack, hráčom vytvorené bedne a podobne. V roku 2016 bol výnos zo skinov 5 miliárd dolárov a približne 40% z nich bolo následne využitých na vsádzanie na zápasy. (58) Spoločnosť

Valve tieto externé stránky nijako neregulovala a tým pádom vznikol čierny market. Taktiež nevyžadovali žiadnu vekovú autentifikáciu užívateľa, čiže mohli vsádzať aj neplnoletí, čo je vo veľa krajinách protizákonné a kvôli tomuto faktu 5. októbra 2016 podala Washingtonská štátna komisia pre hazard príkaz na zastavenie prenosu skinov z ich platform pod hrozbou trestného oznámenia. (59) Spoločnosť Valve odpovedala, že nemá s týmito stránkami nič spoločné a že neporušili žiaden zákon. Keďže tieto stránky nepatrili Valve, tak nemali možnosť ako ich vypnúť bez toho, aby postihli hráčov, ktorí používali tieto služby zákonne, ale aj uviedla, že bude plno spolupracovať so štátom a bude im pomáhať zatvárať účty, ktoré využívali tieto služby protizákonne a nespĺňali ich podmienky používania licenčnej zmluvy pre koncového používateľa. (60)

Kvôli všetkým reguláciám a problémom, ktoré vznikli pre tieto externé stránky v roku 2016, sa niektoré stránky rozhodli prejsť do kryptomeny s názvom „Skincoin“, ktorá vznikla v 2017. (61) Pomocou tejto kryptomeny mohli hráči svoje skiny jednoducho za ňu vymeniť a následne ju mohli využiť na hazard alebo nákup iných skinov. (62)

V tom istom roku vzniklo aj veľké množstvo stránok, ktoré ponúkali skiny „zadarmo“ v prípade ak hráč pozeral reklamy, vyplňoval dotazníky alebo pomocou pozývania iných užívateľov na tieto stránky. Tento biznis model sa nazýva „Get paid to“ alebo „GPT“. (63)

V septembri 2018, na konferencii Európskeho fóra regulátorov hazardných hier, zástupci 15 Európskych krajín spolu so štátom Washington oznámili spoločne spoluprácu zameranú na riešenie "rizík spôsobených vymazaním hraníc medzi hraním hier a hazardnými hrami", ktoré sa zameriavajú predovšetkým na webové stránky tretích strán, ktoré ponúkajú funkcie hazardných hier pomocou skinov. (64)

Všetky stránky sú vždy vo výhode, keďže sa jedná o hazard, takže sa všeobecne neodporúča tieto stránky využívať, avšak niektoré stránky sú vyslovene podvodné a okrádajú hráčov o ich peniaze vo forme skinov. Užívatelia platformy Steam preto vytvorili zoznam stránok, ktoré okrádajú hráčov. (65)

9. Phishingové a iné útoky na platforme Steam

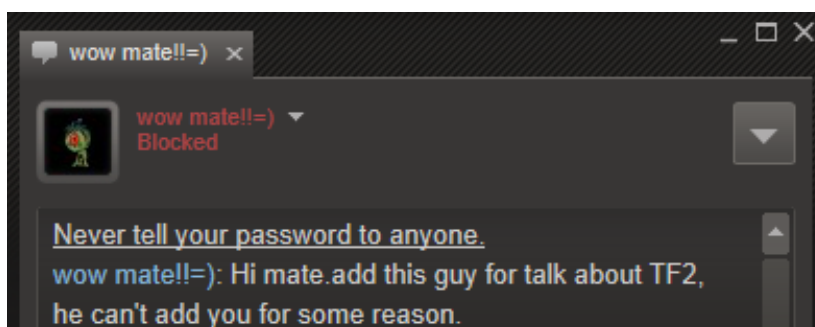
Táto kapitola sa zaoberá analýzou útokov. Každý útok je popísaný, je vysvetlený postup a obsahuje odporúčané opatrenia, ktoré môžu danému typu útoku zabrániť. Na konci kapitoly sú všetky útoky a opatrenia zhrnuté a následne je odporúčené nastavenie svojho Steam účtu.

9.1 Útok pomocou phishingovej stránky

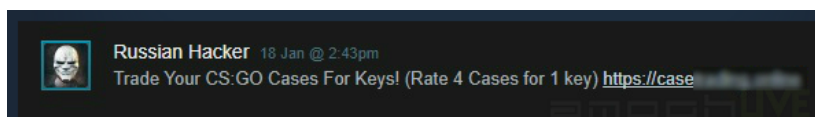
Tento typ phishingu je jeden z najtypickejších útokov a skoro každý užívateľ sa s týmto útokom raz v živote stretol. Funguje na jednoduchšej schéme a spolieha sa na nepozornosť užívateľa.

9.1.1 Postup útoku

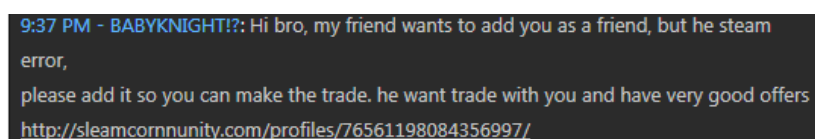
Schéma zo 4 krokov. Útočník si pridá obeť do zoznamu priateľov a pokúsi sa ju kontaktovať alebo uverejní príspevok v skupine alebo fóre.



Obr. 9.1: Príklad 1 kontaktovania obete útočníkom (66)



Obr. 9.2: Príklad 2 kontaktovania obete útočníkom (67)



Obr. 9.3: Príklad 3 kontaktovania obete útočníkom (68)

Správa obsahuje link na phishingovú stránku útočníka, ktorá obsahuje prihlásenie do platformy. Pôvodný link môže obsahovať odkaz na externú stránku slúžiacou na výmenu/predaj skinov alebo na iný účel. Následne pri prihlasovaní bude url adresa nesprávna a prihlasovacie meno a heslo získa útočník.

steamcommunitay.com	sleamccommunily.com	steamcornunity.com
steamcommunitay.com	sleamcommunity.com	steamcorrurity.com
steamcommuniti.com	sleamcommunuty.com	steamcoummunuty.com
steamcommunitly.net	sleamcommunity.com	steamcoummunuty.com
steamcommunitriy.com	sleamcommunity.com	steamcowwunity.com
steamcommunity.cm	sleamcommunity.com	steamcummunuty.com
steamcommunity.com.ru	staemcommnuity.com	steamcuommunity.com

Obr. 9.4: Zoznam príkladov modifikovaných linkov (68)

Toto prihlásenie nie je do platformy a pomocou tohto prihlásenia získa útočník prihlasovacie údaje do Steam-u.

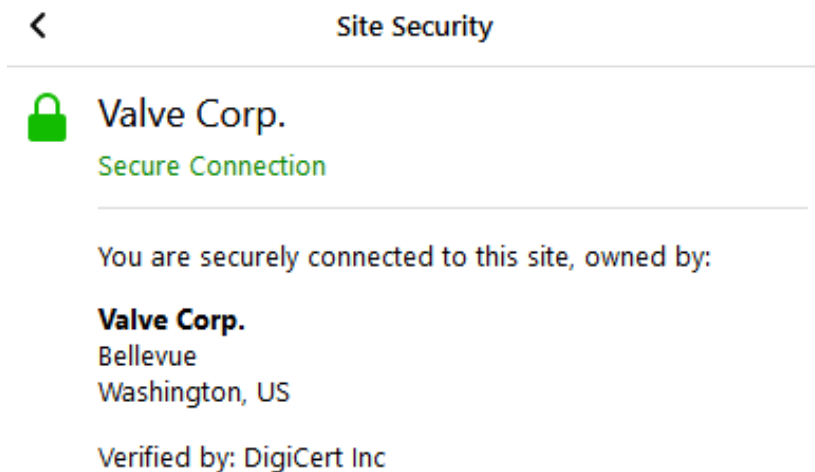
9.1.2 Opatrenia

Užívateľ sa môže proti tomuto útoku obhraňovať jednoducho. Neprijímaním požiadavky o priateľstvo od užívateľov, ktorých nepozná a neklikáť na odkazy, ktoré sú z neznámych zdrojov. Oficiálne stránky Steam majú vždy doménu buď steampowered.com, steamcommunity.com, store.steampowered.com alebo help.steampowered.com a obsahujú certifikát s menom „Valve Corporation [US]“ alebo „Valve Corp. [US]“.



Obr. 9.5: Správne certifikáty spoločnosti Valve Corp., Zdroj: Autor

Po otvorení certifikátu si taktiež môže užívateľ overiť vlastníka stránky, ktorý musí obsahovať „Valve Corp. Bellevue Washington, US“.



Obr. 9.6: Detailný správny certifikát spoločnosti Valve Corp., Zdroj: Autor

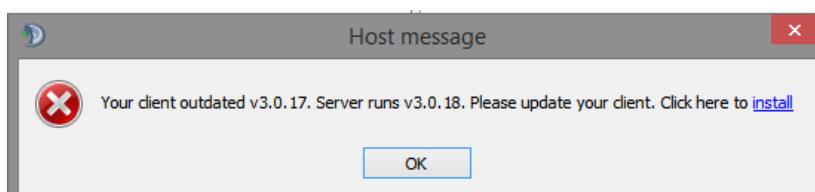
Poslednou záchranou užívateľa je dvojfaktorová autentifikácia, ktorú je ťažké obísť.

9.2 Falošna chyba v aplikácií Teamspeak

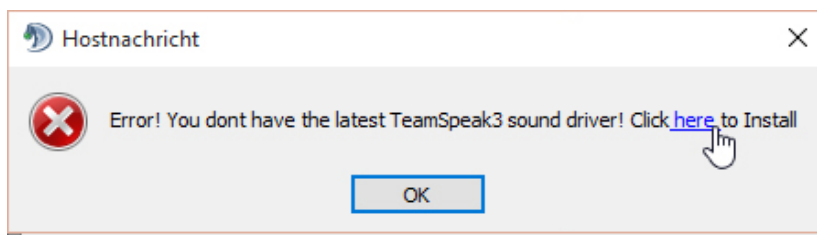
Tento útok sa spolieha na dôverčivosť človeka a na aplikáciu Teamspeak, ktorá sa často používa medzi hráčmi na komunikáciu.

9.2.1 Postup útoku

Útočník si pridá obeť po hre do zoznamu priateľov a niekedy si spolu s obeťou zahrá aj niekoľko hier, aby získal dôveru. Následne sa ho spýta, či sa nechce pridať na jeho Teamspeak server, aby mohli jednoduchšie komunikovať. Obeť sa pripojí na server, ale namiesto pripojenia na server sa mu objaví chyba, ako napríklad, že aplikácia/ovládač zvuku/hlasu sú neaktuálne a potrebuje aktualizáciu. Následne tento link stiahne vírus do počítača obete.



Obr. 9.7: Falošná chybná správa 1 (69)



Obr. 9.8: Falošná chybná správa 2 (69)

9.2.2 Opatrenia

Taktiež aj tomuto útoku sa dá predísť nepridávaním neznámych ľudí do zoznamu priateľov. Tak isto aplikácia Teamspeak pri hocijakej aktualizácii vyhodí chybu hneď po spustení aplikácie a nie po pripojení na server. Keďže tento útok sa na platforme Steam odohráva iba čiastočne, tak dvojfaktorová autentifikácia nepomôže. V tomto prípade pomôže antivírový program.

9.3 ESEA crack

Pri tomto útoku útočník využíva naivitu obete a externú platformu ESEA, ktorá slúži na ligy v hre Counter-Strike: Global offensive.

9.3.1 Postup útoku

Podobne ako pri útoku pomocou aplikácie TeamSpeak, tak aj pri tomto útoku si pri hraní pridá útočník obeť do svojho zoznamu priateľov a snaží sa získať dôveru obete. Následne sa obete opýta, že či niečo vie o platforme ESEA, či niekedy hrala a či vlastní licenciu na túto platformu. Ak obeť túto licenciu nemá, tak jej ponúkne licenciu zdarma. V prípade, že obeť súhlasí, útočník pošle súbor, ktorý obsahuje vírus.

9.3.2 Opatrenia

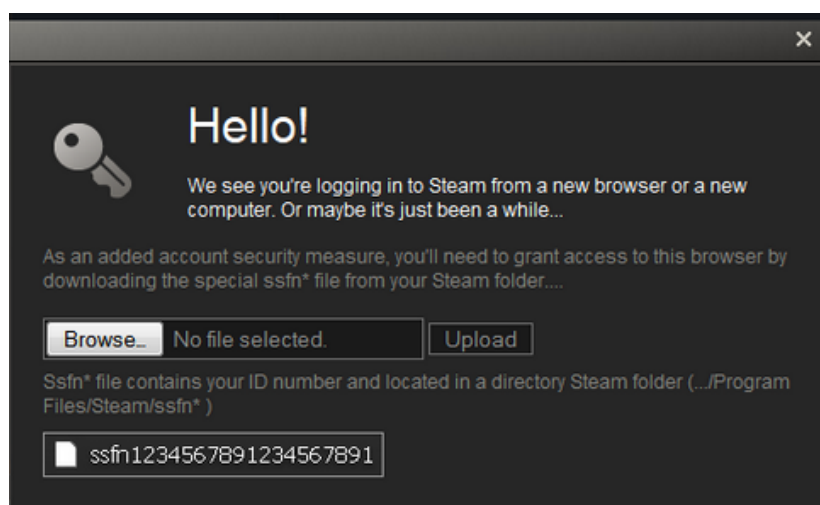
Základným pravidlom aj pri tomto útoku je nepridávať si neznámych ľudí do zoznamu priateľov. Takéto útoky, typu „Too good to be true“ alebo príliš dobré, aby to bola pravda, sú väčšinou podvody a treba byť na pozore aj keď útočník ponúka zľavu z plnej ceny. Ani pri tomto útoku nepomôže dvojfaktorová autentifikácia, ale aj tu pomôže antivírový program.

9.4 SSFN podvod

Tento podvod je prepracovanejší typ pomocou phishingovej stránky. Používa SSFN súbor, pomocou ktorého sa užívateľ prihlasuje do platformy Steam bez použitia autentifikácie.

9.4.1 Postup útoku

Postup útoku je rovnaký ako postup pri útoku pomocou phishingovej stránky, lenže po prihlásení požiada obeť, aby nahral svoj SSFN súbor, ktorý je uložený v Steam zložke.



Obr. 9.9: Nahratie SSFN súboru (70)

Následne sa pomocou tohto súboru dokáže prihlásiť do aplikácie Steam bez dvojfaktorovej autentifikácie.

9.4.2 Opatrenia

Opatrenia sú rovnaké, ako pri iných útokoch pomocou phishingovej stránky, lenže akonáhle obeť nahrá svoj SSFN súbor, tak už mu nepomôže dvojfaktorová autentifikácia. Tento súbor nikdy nebude Steam od užívateľa vyžadovať.

9.5 Útok pomocou krádeže identity

Pri tomto útoku útočník vystupuje ako zamestnanec Valve a kontaktuje obeť buď emailom alebo pomocou pridania do zoznamu priateľov.

9.5.1 Postup útoku

Útočník kontaktuje obeť pomocou správy s tým, že jeho účet bol nahlásený kvôli podvodu a podobne. Následne útočník povie, že musí skenovať jeho položky v inventári, či nie sú ukradnuté. Akonáhle obeť tieto predmety vymení, tak si útočník obeť zablokuje a predmety mu nevráti. Pri kontaktovaní emailom útočník pošle email buď od Valve alebo Steam podpory. V prílohe bude priložený súbor, ktorý obsahuje vírus.

9.5.2 Opatrenia

Aj tomuto útoku sa dá ľahko predísť nepridávaním si neznámych ľudí do zoznamu priateľov. Taktiež zoznam pracovníkov, ktorí užívateľa môžu kontaktovať je na stránke: <https://steamcommunity.com/discussions/moderators>. Akonáhle užívateľ nebude na tomto zozname, tak nie je pracovníkom. Čo sa týka emailu, tak pracovník Valve nikdy nepošle v emaile žiadnu prílohu. Po stiahnutí súboru je posledná záchrana antivírusový program.

9.6 Rýchla výmena tovaru

Tento podvod je pri výmene tovarov na platforme veľmi častý a je založený na nepozornosti obete.

9.6.1 Postup útoku

Tento podvod začína buď na externých stránkach zameraných na výmenu tovaru alebo v hre. Na výmenu tovaru nemusia byť hráči priatelia v hre, čiže ponuku na výmenu tovaru môže poslať hocikto. Následne pri výmene tovaru najskôr podvodník vloží správny tovar a následne sa snaží obeť zmiasť otázkami alebo sa snaží naviazať konverzáciu, aby sa nesústredil na výmenu tovaru. Pred potvrdením výmeny podvodník vymení tovar za rovnaký tovar horšej kvality alebo bez nálepiek alebo iných prídavkov na tovare.

9.6.2 Opatrenia

Jediné opatrenie pri tomto podvode je skontrolovanie si predmetov pred potvrdením výmeny. Keďže predmet horšej kvality môže byť aj o stovky eur lacnejší.

9.7 Vrátenie peňazí

Tento podvod používa spolu s výmenou tovaru aj iné externé platformy, ktoré umožňujú vrátenie peňazí, ak predajca nedodá tovar. Keďže pri virtuálnej výmene tovaru je ťažké zistiť, či ten tovar bol alebo nebol doručený, dá sa tento systém veľmi ľahko zneužiť. Používa sa napríklad PayPal platforma.

9.7.1 Postup útoku

Útočník si pridá obeť do zoznamu priateľov alebo ho kontaktuje cez inú externú stránku. Následne obeť informuje, že by mal záujem kúpiť predmet obeť, ale že chce zaplatiť cez PayPal alebo inú externú platformu. Útočník pošle peniaze vopred, aby mu obeť verila a vymenila tovar. Následne po pár dňoch útočník požiada o vrátenie peňazí, keďže žiaden tovar nebol dodaný.

9.7.2 Opatrenia

Neprijímať žiadosti od neznámych hráčov a keďže sa pre to tento útok používajú externé platformy na platbu a vymenia za virtuálny tovar, tak opatrenie je už iba jedno a to nepoužívať na platbu externé platformy, ktoré majú funkciu vrátenia peňazí, ak tovar nebude doručený.

9.8 Darčeková poukážka

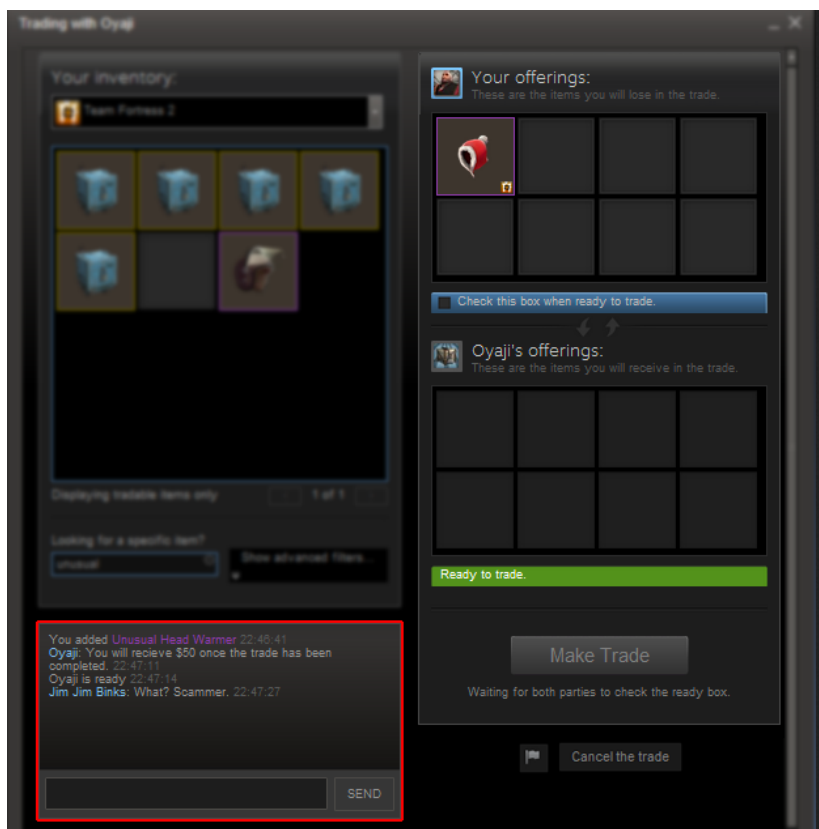
Útočník pri tomto podvode používa naivitu obeť a snaží sa získať tovar obeť za následné poslanie darčekovej poukážky.

9.8.1 Postup útoku

Útočník si obeť pridá do zoznamu priateľov alebo napíše správu na externej stránke slúžiacej na výmenu tovaru. Po krátkej konverzácii mu ponúkne výmenu tovaru obeť za darčekovú poukážku na platformu Steam. Následne obeť vymení tovar za nič, daruje ho, a útočník si danú osobu zablokuje, bez toho, aby poslal kód darčekovej poukážky.

9.8.2 Opatrenia

Nepridávať si cudzích hráčov do zoznamu priateľov a nevymieňať tovar s tým, že druhý hráč pošle túto poukážku neskôr.



Obr. 9.10: Podvod pomocou darčekovej poukážky (71)

9.9 Darčekový podvod

Tento podvod je postavený na výmene kradnutého tovaru a na využití 2 účtov.

9.9.1 Postup útoku

Útočník si pridá do zoznamu priateľov obeť a ponúkne mu obchod, ktorý sa viac oplatí obeti a tak isto ponúkne zaplatiť prvý. Následne požiada obeť, aby si pridala do priateľov útočníkov druhý účet a následne z tohto účtu vymení tovar kúpený ukradnutou kreditnou kartou. Akonáhle tento produkt obeť dostala, tak vymení tovar na útočníkov prvý účet, ktorý neobsahuje žiadne predmety zakúpené ukradnutou kartou. Hneď ako vlastník ukradnutej karty zistí, že mu z účtu zmizli financie, tak to nahlási a Steam zablokuje všetky predmety kúpené touto kartou a môže aj zablokovať účet, ktorý tieto predmety vlastní.

9.9.2 Opatrenia

Aj pri tomto podvode platí pravidlo nepridávať si neznámych ľudí do zoznamu priateľov a tak isto neprijímať darčeky od týchto osôb. Vždy treba predmety vymieňať za iný predmet a nie prijať dar a následne predmet darovať.

9.10 Faktúrový podvod

Pri tomto podvode útočník využíva externú platformu PayPal a jej funkciu pre predajcu poslať faktúru kupujúcemu.

9.10.1 Postup útoku

Útočník si aj pri tomto podvode pridá obeť do zoznamu priateľov alebo ju kontaktuje pomocou externej stránky. Po dohode ponúkne zaslanie peňazí vopred, čo v obeti vyvolá pocit dôvery. Následne útočník pošle faktúru obeti, malo by to byť však naopak a obeť by mala posilať faktúru útočníkovi, ktorú vytvorí ako PayPal darček. Potom útočník túto faktúru označí ako zaplatenú a keďže v podmienkach tejto faktúry je, že táto transakcia sa nedá vrátiť, tak sa obeť nebude obávať, že sa stane obeťou podvodu vrátenia peňazí. Obeť myslí, že útočník už peniaze poslal, aj keď jeho zostatok na účte je stále rovnaký, keďže táto transakcia môže trvať až 24 hodín, tak mu tovar vymení. Akonáhle takto učiní, tak útočník obdrží tovar a obeť nedostane žiadne peniaze.

9.10.2 Opatrenia

Nepridávať si neznámych ľudí do zoznamu priateľov je prvé opatrenie. Ďalším opatrením je počkať 24 hodín, po ktorých by mali byť tieto peniaze pripísané na účet. Taktiež by mal hráč vedieť, že faktúru má posilať predávajúci a nie kupujúci. Ďalšie opatrenie je nevyužívať externé stránky na výmenu alebo predaj tovarov.

9.11 Zhrnutie o útokoch

Všetky útoky sú zamerané buď na naivitu obete alebo na jej nepozornosť. Všetky popísané útoky sú nebezpečné, ale najviac nebezpečné útoky sú pomocou phishingu, keďže je najťažšie sa proti ním brániť. Platforma Steam je veľmi dobre zabezpečená proti týmto útokom, lenže útočníci sa postupom času zlepšujú a hľadajú cesty ako tieto zabezpečenia obísť. Ako už bolo spomenuté v časti 2.9, tak niektoré príliš dobré alebo časovo obmedzené ponuky, hyperlinky alebo prílohy v emailoch môžu byť veľmi škodlivé. To isté platí aj na platforme Steam.

9.12 Zhrnutie o opatreniach

Skoro všetkým útokom sa dalo predísť nepridaním útočníka do zoznamu priateľov. Následne veľkému množstvu útokov sa tak isto dalo predísť pozornosťou a vždy si pred výmenou tovar skontrolovať. Taktiež pri phishingových útokoch na platforme sa dá predísť dvojfaktorou

autentifikáciou. Ďalšie opatrenia sú nebyť moc naivný a tak isto nevymieňať tovar s tým, že následne druhá osoba pošle peniaze pomocou externej stránky/prevodu na účet/výmenou za darčkovú poukážku alebo iný darček. Pri výmene tovaru treba zásadne používať iba možnosti platformy Steam a nepoužívať externé stránky, ktoré môžu byť iba nebezpečím. Posledné opatrenie je, nenahrávať žiadne súbory zo Steam zložky a neotvárať žiadne súbory čo vám niekto pošle. Administrátor a ani moderátor nikdy nebude od užívateľa žiadať nahranie alebo stiahnutie súboru,.

9.13 Bezpečné zabezpečenie účtu

Keďže platforma Steam obsahuje dvojfaktorovú autentifikáciu pomocou emailu, aj aplikácie, odporúča sa túto možnosť zapnúť. Vďaka dvojfaktorovej autentifikácii je veľmi ťažké odcudziť účet alebo predmety na účte. Taktiež si môže užívateľ nastaviť súkromný profil, vďaka ktorému ostatní užívatelia platformy Steam nevidia aktivitu, hry a ani inventár užívateľa. Ďalšie veľmi dobré doporučenie je nepridávať si cudzích ľudí do zoznamu priateľov. Veľkému množstvu útokov sa dá predísť tým, že si obeť útočníka nepridá do zoznamu priateľov. Posledný a veľmi dôležitý krok je silné heslo. Najviac bezpečné heslo by malo obsahovať malé aj veľké písmená, čísla a znaky. Písmená by nemali dávať zmysel, respektíve nemali by byť v slovníku. Čísla by taktiež nemali dávať zmysel, nemal by to byť rok narodenia/dátum narodenia a podobne.

Záver

Prvým cieľom mojej práce bolo zoznámiť čitateľa s phishingom obecné a v hernom priemysle. Tento cieľ som splnil v teoretickej časti, kde som postupne opísal phishing, typy phishingov, podrobne rozobral herný priemysel a trendy v tomto priemysle.

K dosiahnutiu druhého cieľa mojej práce, ktorý bol poskytnúť užívateľom platformy Steam informácie o phishingových útokoch a ako sa proti nim brániť, som vypracoval analytickú a praktickú časť. Rozobral som postupne bezpečnosť platformy Steam, následne som ju porovnal s ďalšími platformami a opísal som obchodovanie na tejto platforme. V praktickej časti som popísal desať útokov, ktoré využívajú phish alebo iné prostriedky. Praktickú časť som zakončil zhrnutím o útokoch, opatreniach a následným doporučením zabezpečenia svojho Steam účtu.

Trendy v hernom priemysle ukazujú, že aj v budúcich pár rokoch bude dominovať čínsky a severoamerický trh. Na čínskom trhu dominujú hry na mobilných zariadeniach a tabletoch, pričom na severoamerickom trhu dominujú konzoly. Postupom času počet hráčov na počítači, v pomere ku hráčom na konzoliach/mobiloch ubúda. Hlavným dôvodom je zvyšovanie počtu príležitostných hráčov a hráčov, ktorí nechcú investovať veľa peňazí do drahého počítača, ale radšej si kúpia lacnejšiu konzolu. Čo sa týka trendov v Esports, tak podobne ako sa zvyšuje počet hráčov, ktorí hrajú hry, rovnako sa zvyšuje aj počet ľudí, ktorí sledujú profesionálne zápasy v hrách. Najväčší počet nadšencov pre Esports je v Ázii a v Tichomorí. To je najmä vďaka čínskemu a juhokórejskému trhu, kde sa profesionálne hranie na počítači berie ako šport. Rastúcim počtom sledujúcich Esports sa zvyšuje aj počet sponzorov, ktorí do tohoto odvetvia začali investovať. Predpokladom je, že množstvo peňazí, ktoré sú generované Esports sa bude len zvyšovať.

Bezpečnosť platforiem som porovnal a najbezpečnejšia platforma z môjho výberu bola platforma Battle.net, ktorá umožňovala najviac dvojfaktorových autentifikácií a platforma Origin, ktorá síce neumožňuje užívateľovi používať autentifikátor, ale n rozdiel od platformy Battle.net neobsahuje prihlásenie pomocou sociálnych sietí. Platforma Steam skončila v porovnaní na treťom mieste, keďže obsahuje iba dve dvojfaktorové autentifikácie. Síce vybraná platforma skončila na treťom mieste, ale aj tak je veľmi dobre zabezpečená proti phishingovým útokom, keďže funkcia Steam guard je veľmi dobre premyslená.

Veľmi rizikové útoky sú útoky, či už pomocou phishu, alebo použitím iných externých stránok. Platforma Steam urobila veľa opatrení, aby sa mohol užívateľ čo najviac zabezpečiť proti útokom pomocou phishu, ale aj napriek tomu sa pri útokoch, ktoré používajú externé stránky s prostriedkami na platforme Steam, obraňovať nedá, ale ak je užívateľ dostatočne informovaný a ohľaduplný, tak aj tieto útoky sa dajú veľmi ľahko odhaliť.

Oba ciele mojej práce boli splnené a jedným z hlavných prínosov mojej práce považujem, že užívateľ môže použiť moju prácu ako návod na bezpečné užívanie platformy Steam, na čo

najlepšie zabezpečenie účtu na tejto platforme a na čo najbezpečnejšie online obchodovanie pomocou tejto platformy. Ďalším prínosom mojej práce je, že čitateľ, ktorý sa nikdy nestretol s herným priemyslom, získa veľa nových informácií o reálnej veľkosti jedného z najrýchlejšie rastúceho zábavného priemyslu súčasnosti, o trendoch, Esports a o sponzoroch.

Práca môže slúžiť na ďalšie spracovanie. Buď na použitie daných útokov a testovaním na užívateľoch s použitím spomínaných protiopatrení alebo môže byť použitá na hlbšiu analýzu trendov v hernom priemysle a Esports.

Bibliografia

- (1) JAMES, Lance. Phishing bez záhad. Praha: Grada, 2007. str. 281. ISBN 9788024717661.
- (2) What is Pharming? Definition from Techopedia. (n.d.). [online]. [cit. 2019-04-14]. Dostupné z: <https://www.techopedia.com/definition/4048/pharming>
- (3) What Is Cybersecurity?. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>
- (4) What is Cyber Security? | IT Governance UK. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.itgovernance.co.uk/what-is-cybersecurity>
- (5) Cybercrime. [online]. [cit. 2019-01-12]. Dostupné z: <https://webcache.googleusercontent.com/search?q=cache:6oxIrYwmyqAJ:https://www.interpol.int/en/Crimes/Cybercrime+&cd=1&hl=sk&ct=clnk&gl=cz&client=firefox-b-d>
- (6) Anti-Phishing Act American Legislative Exchange Council. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.alec.org/model-policy/anti-phishing-act/>
- (7) Will the the Anti-Phishing Act make a difference? | Network World. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.networkworld.com/article/2356547/will-the-the-anti-phishing-act-make-a-difference-.html>
- (8) What is spear phishing? Definition from WhatIs.com. [online]. [cit. 2019-01-12]. Dostupné z: <https://searchsecurity.techtarget.com/definition/spear-phishing>
- (9) What is Clone Phishing? Pentest People. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.pentestpeople.com/clone-phishing/>
- (10) What is whaling attack (whaling phishing)? Definition from WhatIs.com. [online]. [cit. 2019-01-12]. Dostupné z: <https://searchsecurity.techtarget.com/definition/whaling>
- (11) Hidden JavaScript Redirect Makes Phishing Pages Harder to Detect. [online]. [cit. 2019-01-12]. Dostupné z: <https://news.softpedia.com/news/hidden-javascript-redirect-makes-phishing-pages-harder-to-detect-505295.shtml>
- (12) Fraudsters seek to make phishing sites undetectable by content filters | Netcraft. [online]. [cit. 2019-01-12]. Dostupné z: https://news.netcraft.com/archives/2005/05/12/fraudsters_seek_to_make_phishing_sites_undetectable_by_content_filters.html
- (13) WebCite query result. [online]. [cit. 2019-01-12]. Dostupné z: <https://www.webcitation.org/5w9Z2iACi?url=http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/>

- (14) Crooks Net Millions in Coordinated ATM Heists — Krebs on Security. [online]. [cit. 2019-01-12]. Dostupné z: <https://krebsonsecurity.com/2013/02/crooks-net-millions-in-coordinated-atm-heists/>
- (15) New Type of Phishing Attack Goes After Your Browser Tabs. [online]. [cit. 2019-01-12]. Dostupné z: <https://mashable.com/2010/05/25/tabnabbing-phishing/?europe=true>
- (16) WOLF, Mark J. P. The video game explosion: a history from PONG to Playstation and beyond. Westport, Conn.: Greenwood Press, 2008. str. 3-7. ISBN 978-0313338687.
- (17) CAMPBELL-KELLY, Martin, William ASPRAY, Nathan ENSMINGER, Jeffrey R. YOST a William ASPRAY. Computer: a history of the information machine. Third edition. Boulder, CO: Westview Press, A Member of the Perseus Books Group, [2014]. str. 12-13. ISBN 978-0813345901.
- (18) Pong-Story : A.S.Douglas' 1952 Noughts and Crosses game. [online]. [cit. 2019-01-16]. Dostupné z: <http://www.pong-story.com/1952.htm>
- (19) The Priesthood at Play: Computer Games in the 1950s | They Create Worlds. [online]. [cit. 2019-01-16]. Dostupné z: <https://videogamehistorian.wordpress.com/2014/01/22/the-priesthood-at-play-computer-games-in-the-1950s/>
- (20) Tennis Anyone? | They Create Worlds. [online]. [cit. 2019-04-14]. Dostupné z: <https://videogamehistorian.wordpress.com/2014/01/28/tennis-anyone/>
- (21) WHITTAKER, Jason. Cyberspace handbook. London: Routledge, 2004. str. 122. ISBN 0-415-16835-x.
- (22) Historie firmy Atari kapitola 1. [online]. [cit. 2019-01-16]. Dostupné z: <http://historie.atari.sweb.cz/>
- (23) Top 10 Highest-Grossing Arcade Games of All Time | USgamer. [online]. [cit. 2019-01-16]. Dostupné z: <https://www.usgamer.net/articles/top-10-biggest-grossing-arcade-games-of-all-time>
- (24) Video Game History HISTORY. [online]. [cit. 2019-01-21]. Dostupné z: <https://www.history.com/topics/inventions/history-of-video-games>
- (25) Rating categories, content descriptors, and interactive elements from ESRB. [online]. [cit. 2019-01-26]. Dostupné z: https://www.esrb.org/ratings/ratings_guide.aspx
- (26) Total War: THREE KINGDOMS – E3 Gameplay Reveal YouTube. [online]. [cit. 2019-01-26]. Dostupné z: <https://www.youtube.com/watch?v=jQX6qBiCu9E>
- (27) Total War: THREE KINGDOMS Heroes Guanxi Let's Play YouTube. [online]. [cit. 2019-01-26]. Dostupné z: <https://www.youtube.com/watch?v=hRy5KGxpQew>
- (28) Counter-Strike: Global Offensive on Steam. [online]. [cit. 2019-01-28]. Dostupné z: https://store.steampowered.com/app/730/CounterStrike_Global_Offensive/

- (29) "Fortnite"now has nearly 250 million players Business Insider. [online]. [cit. 2019-01-28]. Dostupné z: <https://www.businessinsider.com/how-many-people-play-fortnite-2018-11>
- (30) Pokemon GO Active Player Base Highest Since 2016 – Game Rant. [online]. [cit. 2019-02-02]. Dostupné z: <https://gamerant.com/pokemon-go-player-count-2018/>
- (31) Steam: Game and Player Statistics. [online]. [cit. 2019-02-02]. Dostupné z: <https://store.steampowered.com/stats/Steam-Game-and-Player-Statistics?l=english>
- (32) You'll Never Guess How Many People Play League of Legends 2019. [online]. [cit. 2019-02-02]. Dostupné z: <https://www.unrankedsmurfs.com/blog/players-2017>
- (33) Most Popular Core PC Games | Global | Newzoo. [online]. [cit. 2019-02-02]. Dostupné z: <https://newzoo.com/insights/rankings/top-20-core-pc-games/>
- (34) Newzoo's Key Numbers | Games, Esports, Mobile. [online]. [cit. 2019-02-02]. Dostupné z: <https://newzoo.com/key-numbers/>
- (35) • NBA Finals average US TV viewership 2002-2018 | Statista. [online]. [cit. 2019-02-06]. Dostupné z: <https://www.statista.com/statistics/240377/nba-finals-tv-viewership-in-the-united-states/>
- (36) • NHL Stanley Cup games average TV viewership 2008-2018 | Statista. [online]. [cit. 2019-02-06]. Dostupné z: <https://www.statista.com/statistics/305801/average-tv-viewership-nhl-stanley-cup-games/>
- (37) • Number of Super Bowl viewers (TV) 2018 | Statista. [online]. [cit. 2019-02-06]. Dostupné z: <https://www.statista.com/statistics/216526/super-bowl-us-tv-viewership/>
- (38) Esports Tournaments: Statistics Top and Upcoming Games Tournaments | Esports Charts. [online]. [cit. 2019-02-06]. Dostupné z: <https://esc.watch/tournaments>
- (39) Most Watched Games on Twitch | Esports Content and Total. [online]. [cit. 2019-02-06]. Dostupné z: <https://newzoo.com/insights/rankings/top-games-twitch-youtube/>
- (40) What Olympic Recognition Could Mean For Esports, And Vice Versa. [online]. [cit. 2019-02-06]. Dostupné z: <https://www.forbes.com/sites/dbloom/2018/10/18/esports-olympics-recognition-ioc-esl-advertising-sponsors/#1a01ff6a3b05>
- (41) The International 2018 Dota 2 Prize Pool Tracker. [online]. [cit. 2019-02-06]. Dostupné z: <http://dota2.prizetrac.kr/international2018>
- (42) The 15-year evolution of Steam | PC Gamer. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.pcgamer.com/steam-versions/>
- (43) Steam Translation Server Welcome. [online]. [cit. 2019-02-15]. Dostupné z: <https://translation.steampowered.com/>

- (44) Steam games forum down amid hack fears • The Register. [online]. [cit. 2019-02-15]. Dostupné z: https://www.theregister.co.uk/2011/11/09/steam_forum_hack/
- (45) Valve confirms Steam hack: credit cards, personal info may be stolen | Ars Technica. [online]. [cit. 2019-02-15]. Dostupné z: <https://arstechnica.com/gaming/2011/11/valve-confirms-steam-hack-credit-cards-personal-info-may-be-stolen/>
- (46) Valve introduces Steam Guard to fight account phishing and hijacking | Joystiq. [online]. [cit. 2019-02-15]. Dostupné z: <https://web.archive.org/web/20141028181533/http://www.joystiq.com/2011/03/03/valve-introduces-steam-guard-to-fight-account-phishing-and-hijack/>
- (47) Gamasutra Valve Unveils Steam Guard For Account Security. [online]. [cit. 2019-02-15]. Dostupné z: http://www.gamasutra.com/view/news/33347/Valve_Unveils_Steam_Guard_For_Account_Security.php
- (48) Valve adds two-factor login authentication to Steam mobile app Polygon. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.polygon.com/2015/4/15/8424587/steam-mobile-app-two-factor-login-steam-guard>
- (49) New Steam Security Updates Coming Next Week GameSpot. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.gamespot.com/articles/new-steam-security-updates-coming-next-week/1100-6435256/>
- (50) 77,000 Steam Accounts Hijacked Each Month For Items | Rock Paper Shotgun. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.rockpapershotgun.com/2015/12/10/steam-account-hijacked-items/>
- (51) ReVuln_Steam_Browser_Protocol_Insecurity.pdf. [online]. [cit. 2019-02-15]. Dostupné z: http://revuln.com/files/ReVuln_Steam_Browser_Protocol_Insecurity.pdf
- (52) Valve patches huge password reset hole that allowed anyone to hijack Steam accounts | Computerworld. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.computerworld.com/article/2953016/valve-patches-huge-password-reset-hole-that-allowed-anyone-to-hijack-steam-accounts.html>
- (53) Valve apologizes for Christmas breach, citing denial-of-service attack - The Verge. [online]. [cit. 2019-02-15]. Dostupné z: <https://www.theverge.com/2015/12/30/10690446/valve-christmas-breach-denial-of-service-attack-apology>
- (54) Blizzard Authenticator - Blizzard Support. [online]. [cit. 2019-02-16]. Dostupné z: <https://us.battle.net/support/en/article/24520>
- (55) Origin - Use Login Verification for extra account security. [online]. [cit. 2019-02-17]. Dostupné z: <https://help.ea.com/en-us/help/account/origin-login-verification-information/>

- (56) Protect your Account! Enable 2FA. [online]. [cit. 2019-02-17]. Dostupné z: <https://www.epicgames.com/fortnite/en-US/news/2fa>
- (57) Counter-Strike: Global Offensive » 8/13 – The Arms Deal Update. [online]. [cit. 2019-02-18]. Dostupné z: <https://blog.counter-strike.net/index.php/2013/08/7425/>
- (58) How Counter-Strike turned a teenager into a compulsive gambler. [online]. [cit. 2019-02-19]. Dostupné z: http://www.espn.com/espn/feature/story/_/id/18510975/how-counter-strike-turned-teenager-compulsive-gambler
- (59) Gamasutra - Washington state authority orders Valve to stop allowing CS:GO skin gambling. [online]. [cit. 2019-02-19]. Dostupné z: http://www.gamasutra.com/view/news/282773/Washington_state_authority_orders_Valve_to_stop_allowing_CSGO_skin_gambling.php
- (60) Valve denies wrongdoing in skin gambling legal rumblings: "no factual or legal support for these accusations PC Gamer. [online]. [cit. 2019-02-19]. Dostupné z: <https://www.pcgamer.com/valve-misses-deadline-to-respond-to-washington-state-gambling-regulator-but-says-its->
- (61) What Do ICO's and Cryptocurrencies Have to Do with Esports? - The Esports Observer. [online]. [cit. 2019-02-19]. Dostupné z: <https://esportsobserver.com/esports-ico-cryptocurrencies/>
- (62) Skincoin Aims to Become an Irreplaceable Crypto in Online Gaming | NewsBTC. [online]. [cit. 2019-02-19]. Dostupné z: <https://www.newsbtc.com/2017/06/16/skincoin-aims-become-irreplaceable-cryptocurrency-online-gaming-market/>
- (63) The 'Free' CS:GO Skin Industry Is Booming, Following Gambling Crackdown. [online]. [cit. 2019-02-19]. Dostupné z: <https://kotaku.com/the-free-cs-go-skin-industry-is-booming-following-gamb-1820410636>
- (64) 15 European gambling regulators unite to tackle loot box threat • Eurogamer.net. [online]. [cit. 2019-02-19]. Dostupné z: <https://www.eurogamer.net/articles/2018-09-17-15-european-gambling-regulators-unite-to-tackle-loot-box-threat>
- (65) List of CS:GO gambling and scam sites · GitHub. [online]. [cit. 2019-02-23]. Dostupné z: <https://gist.github.com/MRuy/a3a64bc870a320864557>
- (66) Steam Community :: Guide :: Dealing with phishers. Updated 3/15. [online]. [cit. 2019-02-23]. Dostupné z: <https://steamcommunity.com/sharedfiles/filedetails/?id=234954013>
- (67) Steam Community :: Guide :: Steam Phishing Scams - Fake Steam Login. [online]. [cit. 2019-02-23]. Dostupné z: <https://steamcommunity.com/sharedfiles/filedetails/?id=1274465459>
- (68) Steam phishing attacks exploiting look-alike domain names | Netcraft. [online]. [cit. 2019-02-23]. Dostupné z: <https://news.netcraft.com/archives/2014/06/25/steam-phishing-attacks-exploiting-look-alike-domain-names.html>

- (69) reddit: the front page of the internet. [online]. [cit. 2019-02-23]. Dostupné z: https://www.reddit.com/r/Steam/wiki/scamtypes#wiki_variation.3A_third_person_scam_.2F_chatroom_scam
- (70) [PSA] New phishing/scam technique on fake Steam phishing sites: "As an added account security measure, you'll need to grant access to this browser by downloading the special ssfn* file from your Steam folder": Steam. [online]. [cit. 2019-03-01]. Dostupné z: https://www.reddit.com/r/Steam/comments/1yw25k/psa_new_phishingscam_technique_on_fake_steam/
- (71) de7ROlp.png (PNG Image, 620 × 681 pixels). [online]. [cit. 2019-03-01]. Dostupné z: <https://i.imgur.com/de7ROlp.png>