

Iiro Koistinen

Elektronisen urheilun kasvu ja kilpapelaamiseen liittyvät tietoturva- haasteet

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

26.10.2015

Tekijä(t) Otsikko	Iiro Koistinen Elektronisen urheilun kasvu ja kilpapelamiseen liittyvät tietoturvaasteet
Sivumäärä Aika	34 sivua 26.10.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Lehtori Tapio Wikström
<p>Työssä tutkittiin elektronisen urheilun historiaa ja kasvua käyttämällä mittareina ammattilaispelaajien ja turnausten lukumääriä, alalla liikkuvia rahamääriä sekä katsojalukujen kehitystä. Tämän lisäksi työssä perehdyttiin yleisimpiin tietoturvaasteisiin kuten turnauksia tai yksittäisiä pelaajia kohtaan suoritettaviin palvelunestohyökkäyksiin, selvitettiin niiden yleisimpiä toteutustapoja sekä luotiin käytäntöjä, joilla pyritään estämään ja vähentämään niiden vaikutusta.</p> <p>Elektronisen urheilun kasvussa keskityttiin vuosien 2000 ja 2015 välille. Kaikilla mittareilla mitattuna voidaan nähdä samantyyppistä kehitystä. Vuodesta 2000 vuoteen 2010 kehitys on ollut nousujohteista ja tasaista. Vuodesta 2010 eteenpäin kasvu on ollut selvästi nopeampaa, ja ala on moninkertaistunut viimeisen viiden vuoden aikana.</p> <p>Palvelunestohyökkäyksiä suorittaminen on nykyään yksinkertaista eikä vaadi erityistä ammattitaitoa eikä resursseja. Mitigaatio ja preventaatio on mahdollista, mutta vaatii yksittäisten pelaajien tasolta ymmärrystä ja toimia. Tämän lisäksi turnauksissa pelattavat pelit ovat suunnittelultaan alttiita yksittäistä peliä kohtaan suoritettaville hyökkäyksille, joiden preventaatio vaatii toimenpiteitä myös pelikehittäjiltä.</p> <p>Toisena tietoturvaasteena työssä käsiteltiin erilaisia huijausmetodeja ja näiden vaikutusten vähentämistä. Huijausohjelmia käytetään erityisesti Counter-Strike: Global Offensive -pelissä. Työssä käsiteltiin laitepohjaista ratkaisua vaikeasti havaittavien huijausohjelmien seuraamiseen sekä datan hallintaan perustuvaa mallia, jolla voidaan vähentää huijausyrityksiä LAN-ympäristöissä.</p>	
Avainsanat	eSports, DDoS, tietoturva, kilpapelaminen

Author(s) Title	Iiro Koistinen Growth of eSports and Security Concerns Regarding Competitive Gaming
Number of Pages Date	34 pages 26 October 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Information Networks
Instructor(s)	Tapio Wikström, Principal Lecturer
<p>The goal of this thesis was to study the history and growth of eSports through the growth of both tournament prize pool sizes and the number of active professional players in the field, as well as the increase in spectator numbers for the largest events. In addition, the thesis takes a look at the most common challenges in information security regarding eSports, such as denial-of-service attacks, and seeks to find methods to mitigate and prevent such attacks.</p> <p>The study focused on a time frame between years 2000 and 2015. From year 2000 to 2010 prize pool sizes, numbers in spectators and the number of active professional players have increased steadily. Since the 2010 the growth has accelerated significantly, and the numbers in all studied subjects have multiplied during the last five years.</p> <p>Performing a denial-of-service attack nowadays is simple and does not require any special skills or resources. Mitigation and prevention of such attacks is possible, but requires constant actions from individual players as well as tournament organizers. Additionally, some of the games played in popular eSports are susceptible to attacks, and the prevention of such weaknesses require measures from the game developers.</p> <p>The thesis also studies common cheating methods in popular eSports and finds ways to prevent cheating in tournaments, focusing on the game Counter-Strike: Global offensive. Presented preventive measures include a hardware based system to help detect cheating programs, as well as a data handling model that can help mitigate cheating attempts in LAN environments.</p>	
Keywords	eSports, DDoS, information security, competitive gaming

Sisällys

Lyhenteet

1	Johdanto	1
2	Elektronisen urheilun kasvu	2
2.1	Kilpapelamisen synty	2
2.2	Internet ja online-pelaamisen yleistyminen	2
2.3	Ammattillinen pelaaminen	3
2.3.1	Elektroninen urheilu Etelä-Koreassa	5
2.3.2	Turnausten määrät ja kasvavat palkintopotit	6
2.3.3	Elektroninen urheilu perinteisten urheilulajien rinnalla	11
3	Tietoturvaasteet kilpapelamisessa	13
3.1	DDoS ja kilpapelaminen	14
3.1.1	Motiivit	14
3.1.2	Yleisimmät metodit palvelunestohyökkäyksen toteuttamiseen	15
3.1.3	Uhrin IP-osoitteen selvittäminen yleisesti käytetyillä ohjelmilla	17
3.1.4	Palvelunestohyökkäysten ennaltaehkäisy online-kilpapelamisessa	21
3.1.5	Mitigaatio ja preventaatio LAN-ympäristöissä	22
3.2	Ohjelmistopohjaiset huijausohjelmat ja niiden vaikutusten vähentäminen	25
3.2.1	Epärehellisten metodien vaikutusten vähentäminen ja estäminen	26
3.2.2	Pelaajakohtaisen datan hallinta	28
4	Yhteenveto	29
	Lähteet	32

Lyhenteet

LAN	Local Area Network. Rajatulla alueella toimiva tietoliikenneverkko.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys. Palvelunestohyökkäys on verkkohyökkäys, jolla pyritään estämään verkkoliikenne hyökkäyksen kohteessa.
FPS	First Person Shooter. Videopelien kategoria, jossa pelaaminen tapahtuu pelihahmon näkökulmasta.
RTS	Real Time Strategy. Strategiapelit ovat pelejä, joissa kaksi tai useampi osapuolta pyrkivät voittoon suunnittelun ja taktiikan avulla. RTS on strategiapelien muoto, jossa pelaaminen tapahtuu reaaliajassa.
MOBA	Multiplayer Online Battle Arena. Videopelien kategoria, jossa pelaaminen muistuttaa RTS-genreä, mutta RTS-peleistä poiketen pelaajat kontrolloivat vain yhtä hahmoa eikä pelikenttä yleensä muutu pelien välissä.
IRC	Internet Relay Chat. Vuonna 1988 kehitetty tekstipohjainen internetin yli toimiva pikaviestintäpalvelu.
Botnet	Bottiverkko. Ohjelmista tai laitteista koostuva internetin kautta yhdistetty verkko, jonka avulla voidaan suorittaa hajautettuja palvelunestohyökkäyksiä.
Booter	Booter-palvelut ovat palvelunestohyökkäyksiä varten tarjolla olevia palveluita, joissa hyökkääjä voi maksua vastaan saada käyttöönsä bottiverkon, joka kykenee suorittamaan hyökkäyksiä.
P2P	Peer to Peer. Vertaisverkko, jossa yhteyteen ei käytetä erillisiä palvelimia, vaan jokainen verkkoon kytketty laite toimii sekä palvelimena että asiakkaana.
IP	Internet Protocol. Protokolla, joka huolehtii IP-tietoliikennepakettien toimittamisesta perille pakettikytkentäisessä Internet-verkossa.

VoIP	Voice over IP. Lyhenne tekniikalle, jossa puhetta siirretään reaaliaikaisesti IP-protokollaa käyttäjän verkon välityksellä.
HTTP	Hypertext Transfer Protocol. Protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
VPN	Virtual Private Network. Virtuaalinen verkko, jolla eri lokaatioissa sijaitsevia laitteita voidaan julkisen verkon välityksellä liittää samaan yksityiseen verkkoon.
NAT	Network Address Translation. Osoitteenmuunnos on Internet-tekniikka, jonka avulla pystytään piilottamaan ja säästämään IP-osoitteita.
ASA	Adaptive Security Appliance. Cisco Systemsin laite joka yhdistää palomuurin, viruksentorjunnan sekä hyökkäyksenestotoiminnot.

1 Johdanto

Elektroninen urheilu eli eSports on voimakkaasti kasvava kilpaurheilun ala, joka pyrkii vakiinnuttamaan asemaansa perinteisten urheilulajien rinnalla. Sekä katsojamäärät että kilpailuissa liikkuvat rahamäärät ovat kasvaneet huomattavalla tahdilla viimeisen kymmenen vuoden aikana, erityisesti viimeisen viiden vuoden sisällä. Viimeisimmät kilpapeliturnaukset kilpailevat jopa perinteisten urheilulajien kanssa niin palkintopottien koossa kuin katsojamäärissä.

Nopea kasvu tuo samalla myös erittäin nopeasti muuttuvan ympäristön kisajärjestäjille, sekä paljon uusia mahdollisuuksia väärinkäytöille. Perinteisestä urheilusta poiketen elektroninen urheilu on lujasti sidottu niin tietokoneisiin ja pelikonsoleihin sekä internetiin, joka mahdollistaa myös väärinkäytökset täysin uudella tasolla. Vaikka eSportsin historia on vielä varsin lyhyt, on jo nyt ehditty näkemään useita väärinkäyttöjä ammatillisissa turnauksissa. Tämän lisäksi myös peleihin liittyvä vedonlyönti on luonut kiinnostusta vaikuttaa pelien lopputulokseen. Alalla liikkuvat nopeasti kasvavat rahamäärät luovat tarpeen järjestelmällisille ja luotettaville tietoturvakäytännöille, jotta yleisö ja sponsorit säilyttävät mielenkiintonsa ja eSports kykenee vakiinnuttamaan asemansa perinteisten urheilujen rinnalla.

Tämän työn tarkoituksena on käsitellä elektronisen urheilun historiaa sekä tarkastella eSportsia ilmiönä ja mitata sen kasvua käyttämällä mittarina katsojamääriä sekä alalla liikkuvia rahamääriä. Tämä lisäksi työ tulee käsittelemään elektroniseen urheiluun liittyviä yleisimpiä sisäisiä ja ulkoisia tietoturva-uhkia LAN-ympäristöissä. Ulkoisena uhkana DDoS on selvästi suurin riski. Sisäisinä uhkina voidaan nähdä erilaiset ohjelmalliset tai inhimilliset tavat luoda epäreilua etua kilpailutilanteessa.

Työ tulee keskittymään Valve Corporationin peleihin Dota 2 sekä Counter-Strike: Global Offensive. Tällä hetkellä eSportsin suosituimpiin peleihin kuuluu näiden pelien lisäksi myös League of Legends sekä Starcraft 2. Vaikka työ keskittyy Valven tuotteisiin, voidaan tietoturvakäytäntöjä soveltaa useimmissa tapauksissa melkein suoraan myös muihin peleihin.

2 Elektronisen urheilun kasvu

Vaikka maailmassa on tänä vuonna jo yli kahdeksan tuhatta ammattilaispelaajaa, on videopelit ammattina edelleen kovin uusi käsite. Kaksikymmentä vuotta sitten vastaava luku oli nolla. Vauhti, jolla ala on kasvanut 1970-luvun alusta tähän päivään, on ollut huima.

2.1 Kilpapelaamisen synty

Kilpapelaaminen johtaa juurensa vuoteen 1972, jolloin Stanfordin yliopiston kampuksella järjestettiin Intergalactic Spacewar Olympics. Pelattavana pelinä oli nimen mukaisesti Spacewar. Osallistujat pelasivat vuorotellen yhdellä PDP-10-mallin tietokoneella, joka sijaitsi kampuksen laboratoriossa. Ensimmäisenä palkintona oli vuoden tilaus Rolling Stone -lehteä.

Spacewar oli avaruustaistelupeli, jossa pelaajat kontrolloivat kilpailevia avaruusaluksia. Pelin taustana toimi oikea tähtikartta, ja se sisälsi ominaisuuksia kuten painovoiman ja inertian. Nopeasti reagoivat alukset vaativat nopeita refleksejä, ja pelissä oli hämäävän paljon syvyyttä. Spacewar onkin varmasti yksi kaikkien aikojen tärkeimpiä videopelejä sen tuoman moninpelikokemuksen sekä kilpailullisuuden takia. Se toimi tienviittana kaikille sen jälkeen tulleille peleille niistä asioista, jotka saivat ihmiset palaamaan pelien ääreen ja ottamaan toisistaan mittaa pelien parissa. [1.]

Kilpapelaaminen kasvatti suosiotaan läpi 1970- ja 1980-luvun, ja jo vuonna 1980 järjestetyssä Space Invaders Championship -turnauksessa oli yli kymmenentuhatta osallistujaa. Kilpapelaaminen alkoi vakiinnuttaa itseään yleisesti hyväksyttynä harrastuksena. [2.]

2.2 Internet ja online-pelaamisen yleistyminen

1990-luku toi internetin ja todellisen online-pelaamisen. Tietokonepeleillä oli jo vakiintunut harrastajakunta. Mahdollisuus pelata moninpelejä maailmanlaajuisesti toi pelaamiseen täysin uuden ulottuvuuden. Vuonna 1993 julkaistu Doom oli ainutlaatuinen peli monilla tavoilla. Peli oli grafiikaltaan teknologisesti jotain täysin

uutta. Ensimmäisestä perspektiivistä kuvattu peli oli nopeatempoinen ja hyvin väkivaltainen. Tärkeintä kuitenkin oli, että peliin oli sisällytetty LAN-tuki moninpelaamista varten. Doom loi online death-match-pelimuodon, joka mahdollisti kokonaan uuden ulottuvuuden kilpapelamiseen. [3.]

Vuonna 1996 saapui Quake, joka kuten Doom, oli id Softwaren kehittämä FPS-peli. Quake nosti samanaikaisten pelaajien määrää verkkopelissä Doomista neljästä kuuteentoista, mutta muuten peli vaikutti hyvin paljon edeltäjältään. Quaken perusteet oli erittäin helppo oppia, mutta pelissä oli silti erittäin paljon syvyyttä. Yksinkertaiset taisteluareenat mahdollistivat monia vivahteiltaan erilaisia strategioita ja taktiikoita kohti voittoa, ja pelin nopeatempoisuus pakotti pelaajan jatkuvasti keskittymään. Quake oli erinomainen alusta kilpapelamiselle ja toi mukanaan ensimmäiset kilpapelamiseen keskittyneet joukkueet tai klaanit.

Kilpapelamisen toinen suosittu genre, RTS, loi myös juuriaan 1990-luvun alussa. Pohjaa loivat pelistudio Westwoodin Dune 2, vuonna 1995 julkaistu Command & Conquer sekä Blizzardin tuottama Warcraft vakiinnuttivat strategiapelien suosion pelaajien keskuudessa. RTS-genren ainoa heikkous oli verkkopeli, joka korjaantui 1995 joulukuussa, kun Blizzard julkaisi jatko-osan Warcraftille, Warcraft 2: Tides of Darkness:in. Warcraft 2:n verkkopeli nousi FPS-pelejä vastaavaan suosioon, ja sen ympärille syntynyt yhteisö voidaan johtaa suoraan tämän päivän suosituimpiin kilpailullisten RTS-pelien yhteisöihin. [4.]

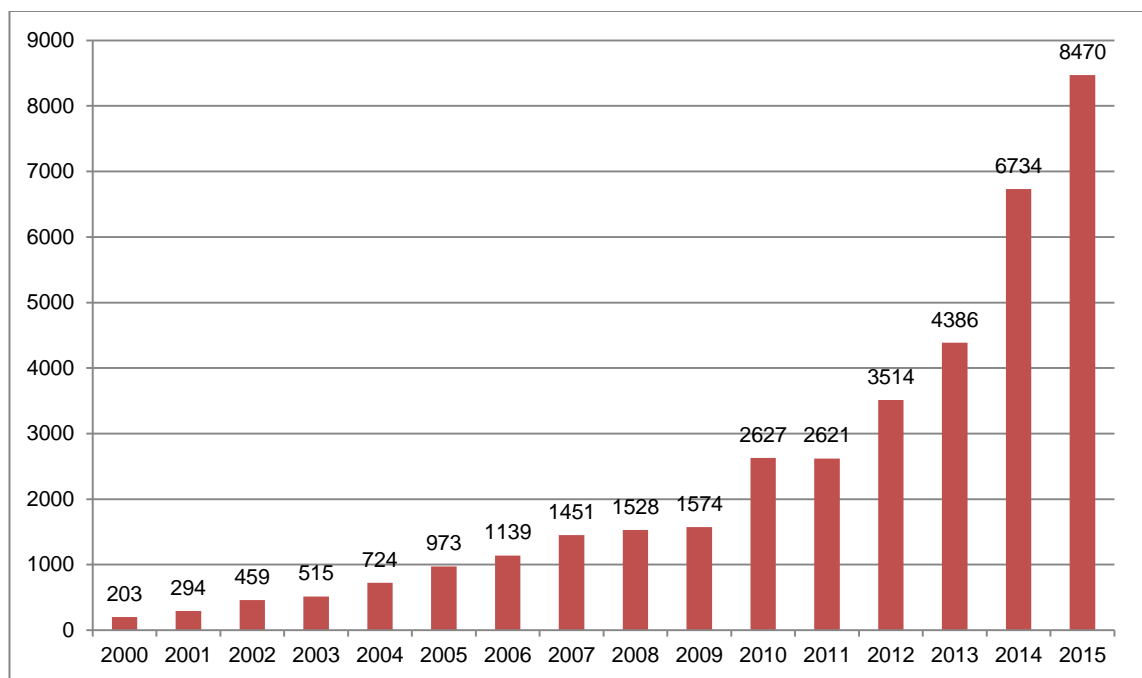
2.3 Ammattillinen pelaaminen

Vuonna 1999 Jonathan "Fatal1ty" Wendel osallistui Cyberathlete Professional Leaguen järjestämään Frag 3 -turnaukseen vain kahden kuukauden intensiivisen harjoittelun jälkeen. Pelinä oli Quake 3: Arena, joka oli suosion aloittaneen Quaken jatko-osa. Wendel sijoittui turnauksessa kolmanneksi voittaen neljä tuhatta dollaria. Samalla hänen ammattilaisuransa oli alkanut. Korkea sijoitus Frag 3 -turnauksessa ansaitsi Fatal1tylle kutsun Ruotsiin, turnaukseen maailman kahtatoista parasta pelaajaa vastaan. Wendel voitti turnauksen dominoivaan tyyliin voittaen 18 ottelua häviämättä yhtäkään. Ensimmäinen sija toi hänelle viisitoista tuhatta dollaria sekä varmuuden siitä, että hän pystyisi jatkamaan ammattilaisena. Wendelin suurin etu aikanaan oli mahdollisuus harjoitella. Koska pelaaminen oli hänelle ammatti, hän harjoitteli sitä joka

päivä noin kahdeksan tuntia päivässä, ja koordinoi omaa harjoitteluaan. Tämä antoi hänelle selvän edun vastustajiin, jotka pääsääntöisesti eivät kyenneet toimimaan ammattilaisena tai eivät olleet halukkaita noudattamaan säännöllistä ja aktiivista harjoitteluaiakataulua. Fatal1ty'n voitokas kulku jatkui vuoteen 2006 asti, ja hän tienasi yli 450 000 dollaria turnausvoitoina, jonka jälkeen hän on toiminut aktiivisena eSports-yhteisön jäsenenä ja työskennellyt ammatillisen pelaamisen puolesta. [4; 5; 6.]

2010-luvulta lähtien suosituimmiksi peleiksi ovat muodostuneet MOBA-genren kaksi suosituinta peliä: Dota 2 sekä League of Legends. Näiden lisäksi suosittuja pelejä ovat Counter-Strike: Global Offensive sekä StarCraft 2. Elektronisen urheilun maisema on kuitenkin alati vaihtuva, ja uusien pelien julkaisut sekä yleisön mielenkiinnon laantuminen vaikuttaa jatkuvasti suosituimpien pelien asemaan.

Taulukko 1. Aktiivisten kilpelaajien lukumäärien kasvu vuosien 2000-2015 välillä.



Aktiivisten kilpelaajien määrä on kasvanut vakaasti vuodesta 2000 eteenpäin (taulukko 1). Ammattilaisten tai puoliammattilaisten määrän voidaan olettaa kasvaneen samoissa määrin, mutta arviointi on haastavaa, koska saatavilla oleva data ei erittele amatöörejä tai ammattilaisia, ainoastaan pelaajan ja voitettujen palkintorahojen määrän. Vuosien 2000 ja 2009 välillä kasvu on ollut selkeästi rauhallisempaa, ja nopeasti kiihtynyt kasvu vuosien 2010 ja 2015 välillä kertoo myös koko alan

kiihtyneestä kasvusta tämän vuosikymmenen aikana. On todennäköistä, että myös ammattilaispelaajien prosentuaalinen osuus aktiivisten kilpapelaaajien määrästä on kasvanut varsinkin vuoden 2010 jälkeen kasvaneiden palkintopottien ja yleisömäärien johdosta.

2.3.1 Elektroninen urheilu Etelä-Koreassa

1990-luvun lopussa Etelä-Koreaa ravisteli Aasian finanssikriisi, johon vastauksena Etelä-Korean hallinto päätti keskittää voimavaroja telekommunikaation sekä Internet-infrastruktuurin kehittämiseen. Tämä kehitys toi internetin sekä online-pelaamisen laajasti saataville eteläkorealaisille, ja jo vuoteen 2000 mennessä maahan oli syntynyt voimakas pelaajayhteistö. Korean hallinto huomasi suosion kasvun ja otti osaa luomalla Koreaan ensimmäisen valtion tukeman eSports-yhteisön. Suosion kasvu mahdollisti myös monien uusien televisiokanavien synnyn, jotka keskittyivät lähes pelkästään elektronisen urheilun lähettämiseen. Televisiointi ja organisoidut turnaukset toivat eSportsin väestön tietoisuuteen, ja elektronisesta urheilusta tuli yhtä suosittua jossei jopa suosittumpaa kuin perinteisistä urheilulajeista. [7.]

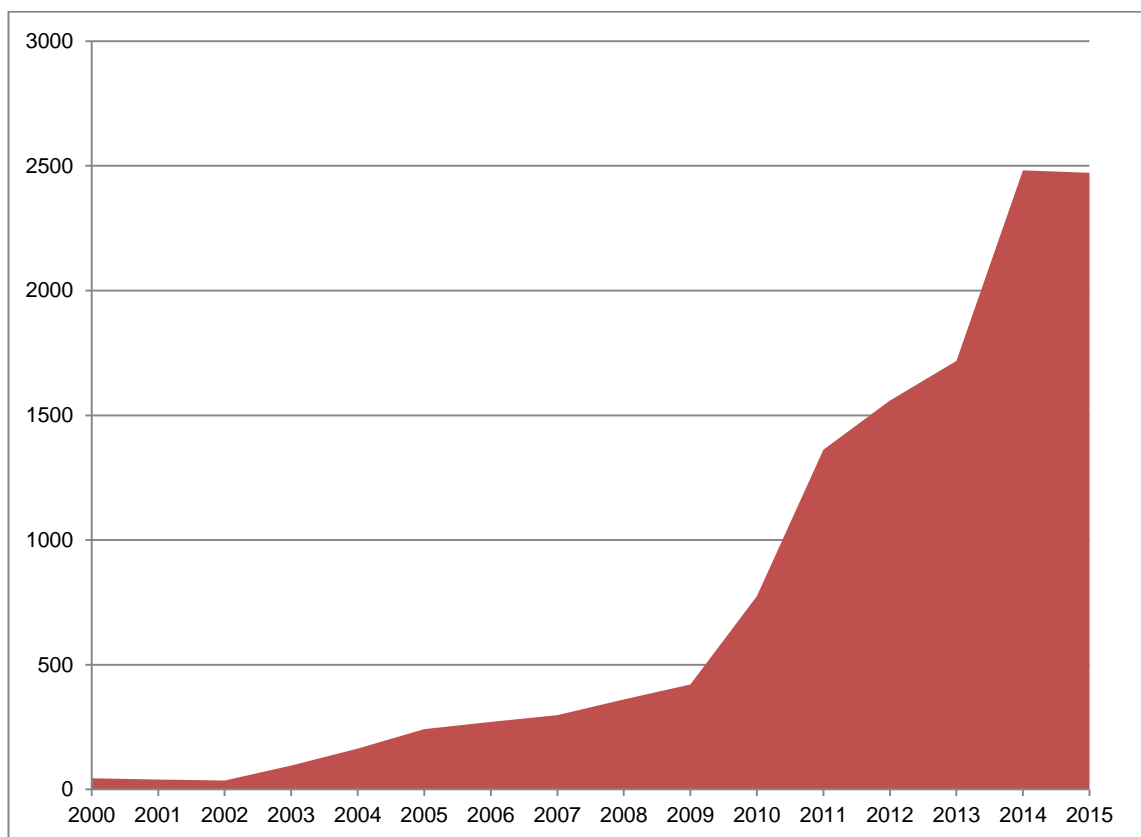
Valtakunnallinen sekä jopa maailmanlaajuinen suosio on tehnyt Etelä-Koreasta esimerkin muulle maailmalle elektronisen urheilun saralla. Siinä missä muualla maailmassa sponsorit ovat pääasiassa tietokone- ja oheislaitevalmistajia, ovat Etelä-Korean eSports-skenen suurimmat sponsorit Samsung, SK Telecom sekä Korea Telecom, jotka ovat samalla maan kolme suurinta yritystä. Tilanne on tosin alkanut muuttumaan varsinkin viimeisen viiden vuoden aikana, ja yritykset kuten Intel ja Coca-Cola ovat alkaneet ottamaan osaa eSports-turnauksiin Korean ulkopuolella.

Etelä-Koreassa elektroninen urheilu on osa nuorison kulttuuria eri tavalla kuin muualla maailmassa. Ammattilaispelaajat saivat jo 2000-luvulla julkisuutta ja olivat yhtä suosittuja kuin perinteisten urheilulajien tähdet. Vastaavat piirteet ovat alkaneet ilmaantumaan muualla maailmaan vasta viimeisen parin vuoden aikana. Ammattilaiseksi tuleminen on silti myös eteläkorealaisille hyvin haastavaa ja kuten muissa huippu-urheilijoissa, myös ammattilaisiksi tähtääville pelaajille tarjolla olevat paikat ovat erittäin harvassa. [8.]

2.3.2 Turnausten määrät ja kasvavat palkintopotit

Elektronisen urheilun kasvua voi mitata monella asteikolla. Turnauksien määrät sekä niihin liittyvät palkintorahat ovat vain yksi monista. Yksi merkittävä tekijä on yksittäisien pelaajien tai joukkueiden saamat sponsorirahat, joiden määrästä ei ole saatavilla tarkkaa dataa. Varsinkin perinteisissä urheilulajeissa sponsorirahat voivat muodostaa jopa valta-osan huippu-urheilijan palkasta. Esille tulevilla luvuilla tuleekin ottaa huomioon erillisten tulonlähteiden mahdollinen vääristävä vaikutus.

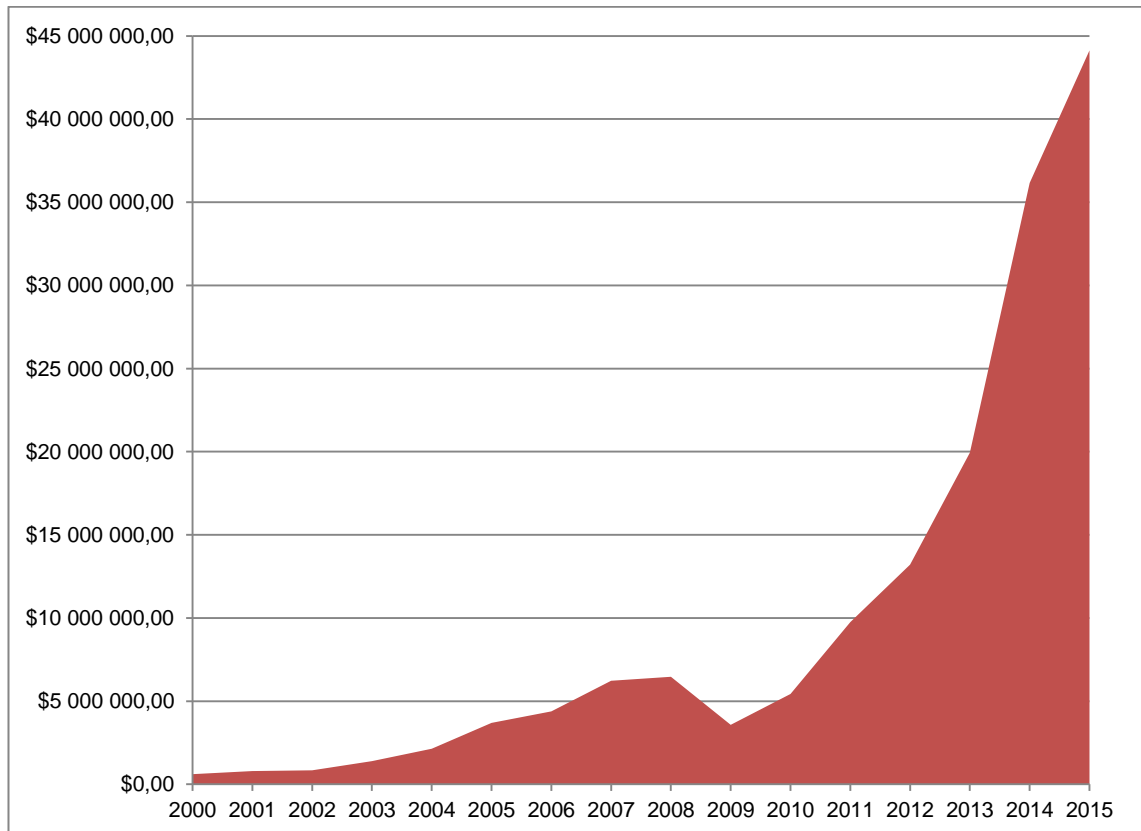
Taulukko 2. Turnausten kokonaislukumäärien kehitys vuosien 2000-2015 välillä.



Vuosina 2000-2002 rahaturnausten lukumäärä oli vielä suhteellisen alhainen, ja turnauksia oli keskimääräisesti vain neljäkymmentä vuodessa. Vakaa kasvu alkoi vuonna 2003, jonka jälkeen turnausten lukumäärä on kasvanut keskimääräisesti viidellä kymmenellä joka vuosi (taulukko 2). Vuonna 2009 turnauksia järjestettiin jo 421, joka on kymmenkertainen määrä kymmenen vuoden takaiseen. Kasvua tällä ajanjaksolla voidaan pitää vakaana. Huomattavasti nopeampi kasvu alkoi vuonna 2010, kun elektroninen urheilu alkoi saavuttaa maailmalaajuista huomiota palveluiden, kuten Twitch.tv, avustamana. Vuonna 2010 turnauksia oli jo 775, eli lähes

kaksinkertainen määrä vuoteen 2009 verrattuna. Nopea kasvu on jatkunut, ja vuonna 2015 turnauksia on syyskuuhun mennessä ollut 2472. [9.]

Taulukko 3. Turnauspalkintomäärien kehitys vuosien 2000-2015 välillä.



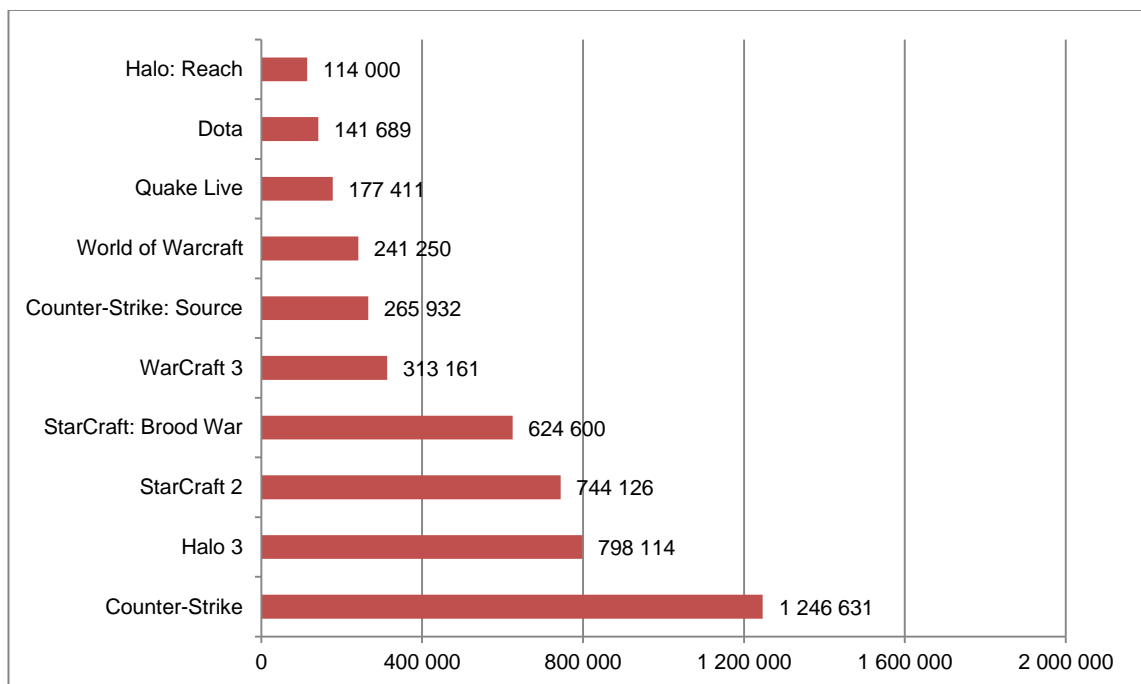
Vuosien 2000 ja 2010 välillä turnausten palkintomäärät ovat kasvaneet vakaalla tahdilla (taulukko 3). Ainoa poikkeus tähän on vuosi 2009, jolloin taluskriisi ajoi monet joukkueet ja turnausjärjestäjät ahdinkoon. Vuodesta 2010 eteenpäin kasvu on ollut erittäin nopeaa, ja vuoden 2015 syyskuuhun mennessä on kokonaismäärä jo 44 131 249 dollaria, kun vuoden 2010 kokonaispalkintomäärä oli 5 435 009 dollaria. Kasvu on ollut vain viiden vuoden välillä lähes kymmenkertaista. Turnausten lukumäärään verrattuna palkintopottien kasvu on myös huomattavasti nopeampaa. Vuodesta 2010 turnausten lukumäärä on kasvanut 319 prosenttia. Vastaavalla aikavälillä rahapalkintojen määrät ovat kasvaneet 811 prosenttia. [10.]

Suurelta osin tähän kasvuun on vaikuttanut Dota 2 ja sen suurimman turnauksen The Internationalin kasvaneet palkintomäärät. The International järjestettiin vuonna 2015 viidettä kertaa, ja vuodesta 2013 eteenpäin sen palkintopotti on määräytynyt osaltaan

yleisön tuen perusteella. Turnauksen yhteydessä myydään virtuaalista tuotetta, jonka ostamalla osa tuotteen hinnasta menee suoraan palkintopottiin. Turnaus on Valve Corporationin järjestämä, joka on samalla Dota 2:n kehityksen takana oleva yritys. Valven osuus palkintopotista on ollut joka vuosi sama, 1 600 000 dollaria, mutta yleisörahoituksen turvin The Internationalin palkintopotti on ollut huomattavasti muita turnauksia korkeampi viimeiset kaksi vuotta. Vuoden 2014 Internationalin kokonaispalkinnot olivat lähes 11 miljoonaa dollaria, ja vuoden 2015 turnauksessa potissa oli 18 416 970 dollaria.

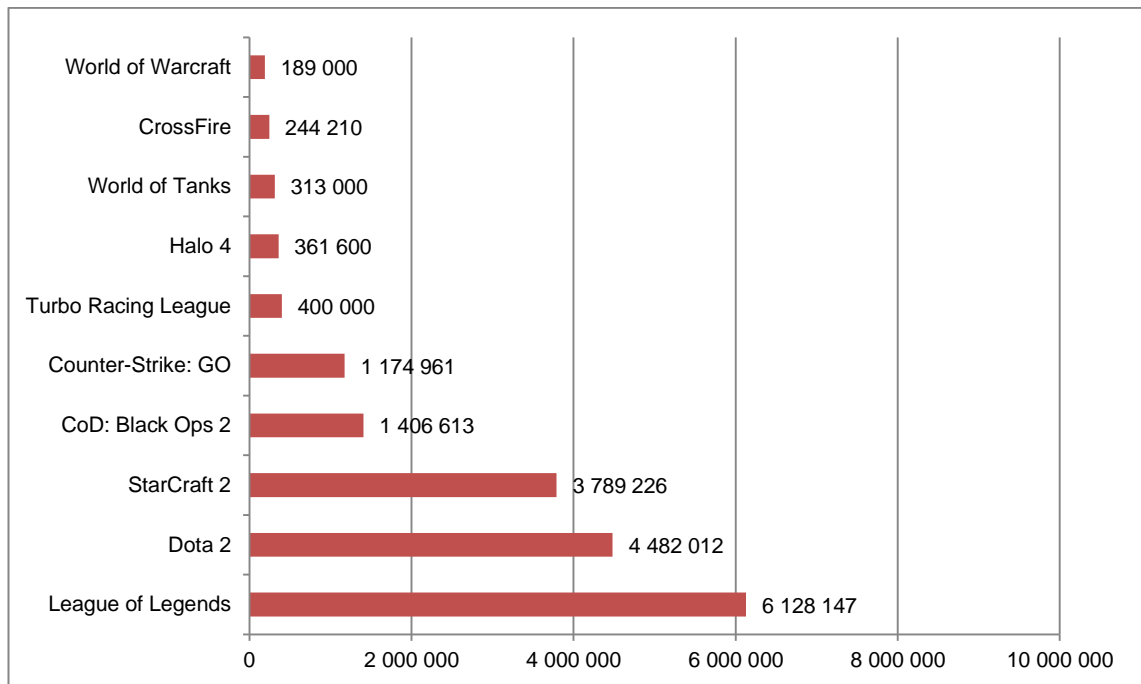
Yleisörahoitus ei kuitenkaan välttämättä ole vakaa rahoituksen muoto, eikä voida olettaa, että se jatkuu nousujohtoisena vuodesta toiseen. Pelaajien ja yleisön mielenkiinto lajiin vaihtuu pelien kehittyessä ja uusien pelien saapuessa markkinoille.

Taulukko 4. Turnauspalkintomäärät vuonna 2010 pelien mukaan jaoteltuina. Luvut on ilmaistu dollareina (\$).



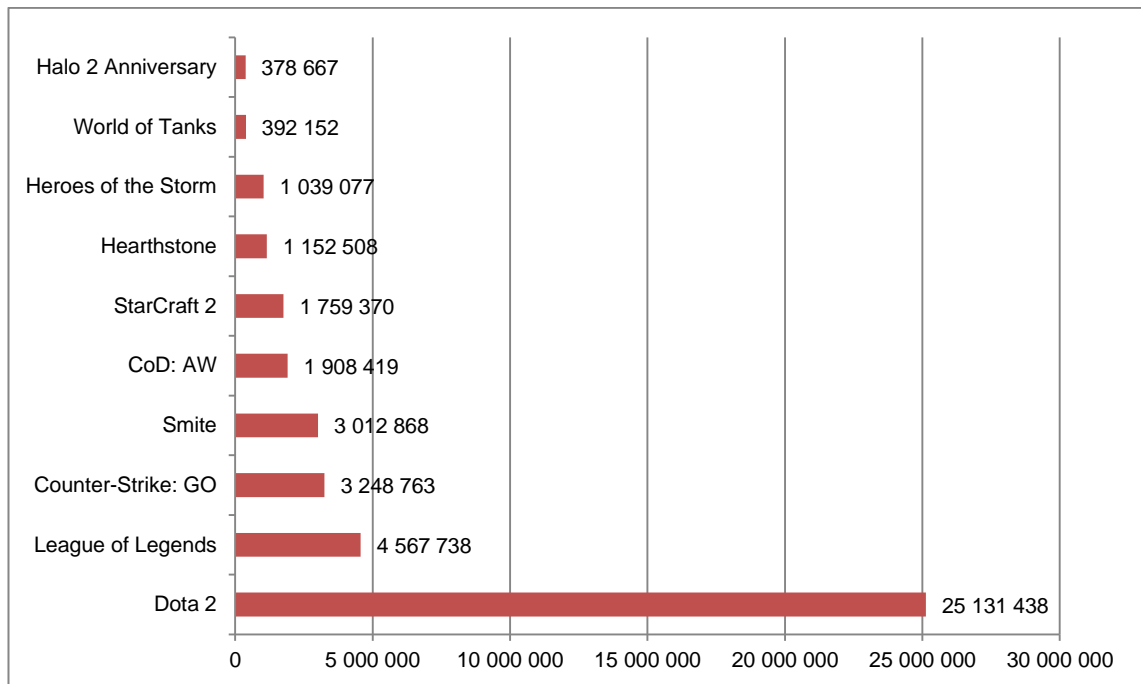
Vuonna 2010 ei Dota 2 ollut vielä edes markkinoilla, ja sen edeltäjä Dota oli vasta yhdeksänneksi rahakkain peli maailmalla (taulukko 4). Suosituimmat pelit tietokonepuolella olivat kyseisenä vuonna julkaistu StarCraft 2 sekä vanha suosikki Counter-Strike, joka aloitti kulkunsa hittipeli Half-Lifen erillisenä modifikaationa jo vuonna 1999.

Taulukko 5. Turnauspalkintomäärät vuonna 2013 pelien mukaan jaoteltuina. Luvut on ilmaistu dollareina (\$).



Vuoden 2013 luvuista nähdään, että eri pelien suosio voi vaihdella rajusti jo parin vuoden välillä (taulukko 5). Vuonna 2010 Counter-Strike oli listan kärjessä ja vuonna 2013 sen seuraaja, Counter-Strike: Global Offensive on vasta viidentenä, ja määrällisesti vertailtuna kokonaismäärä on vähentynyt. Tässä yksittäisessä tapauksessa uuden pelin saapuminen aiheuttaa aina siirtymisperiodin, kun osa pelaajista seuraa vielä vanhaa peliä ja osa uutta, joka osaltaan selittää Counter-Striken taantumista. Siirtymisperiodia kasvatti vielä CS: Source, pelisarjaan kuuluva, pelien välissä tehty vähemmälle suosiolle jäänyt peli.

Taulukko 6. Turnauspalkintomäärät vuonna 2015 pelien mukaan jaoteltuina. Luvut on ilmaistu dollareina (\$).

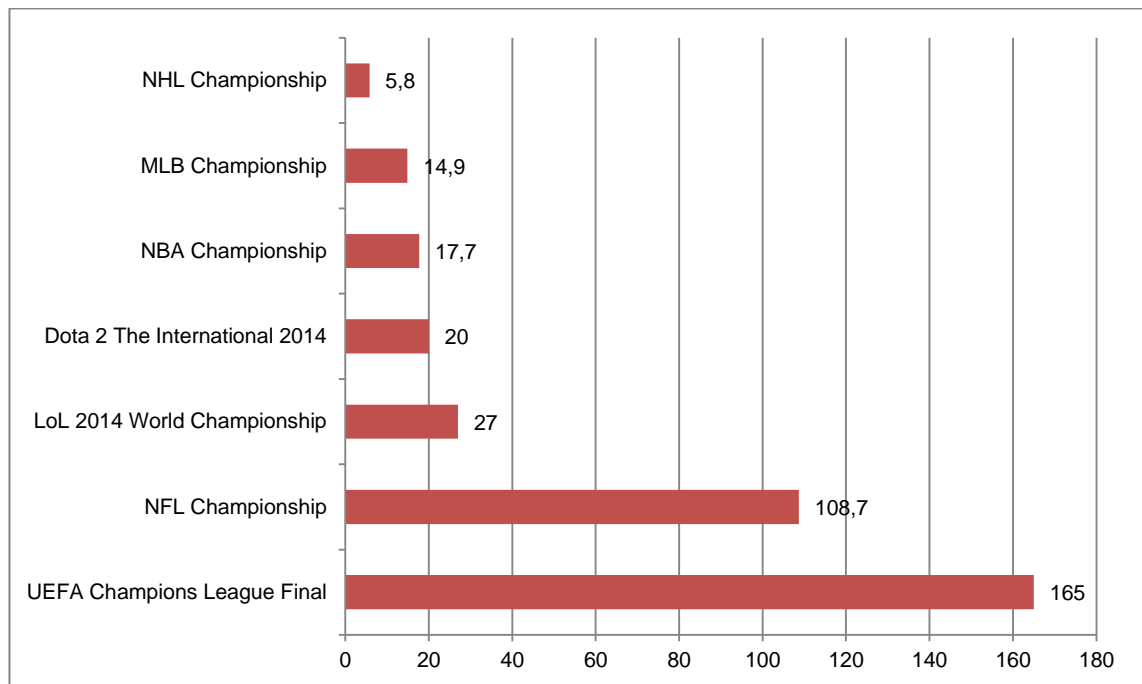


Vuoden 2015 luvuissa Dota 2 on täysin omassa luokassaan. Tämä johtuu pääasiassa aiemmin selvitetystä The International -turnauksen palkintostruktuurista. Jos Dota 2:n palkintomäärästä vähennettäisiin yleisörahoituksen osuus, olisi pelin kokonaismäärä vain 8 301 825 dollaria (taulukko 6). Tämäkin luku on selvästi korkeampi kuin seuraavana oleva League of Legends, mutta vuoteen 2013 verrattuna pelien voitaisiin melkein nähdä vain vaihtaneen paikkoja. Yleisörahoituksen korkeaa osuutta voidaan kuitenkin pitää merkinä siitä, että peliyhteisö on valmis tukemaan elektronisen urheilun kasvua. Tässä tapauksessa Dota 2 vakiinnuttaa paikkansa kilpailullisena lajina.

2.3.3 Elektroninen urheilu perinteisten urheilulajien rinnalla

Elektronisen urheilun suosion nopea kasvu on tuonut sen perinteisten urheilulajien rinnalle hieman jopa yllättäen. Nopea kasvu varsinkin palkintopoteissa viimeisen viiden vuoden aikana on nostanut suosituimmat eSports-pelit kuten Dota 2:n ja LoL:n suoraan suosituimpien urheilulajien rinnalle.

Taulukko 7. Dota 2:n ja LoL:n keskimääräiset katsomäärät vuonna 2014 verrattuna perinteisiin urheilulajeihin. Luvut on ilmaistu miljoonina. [14; 15; 16.]

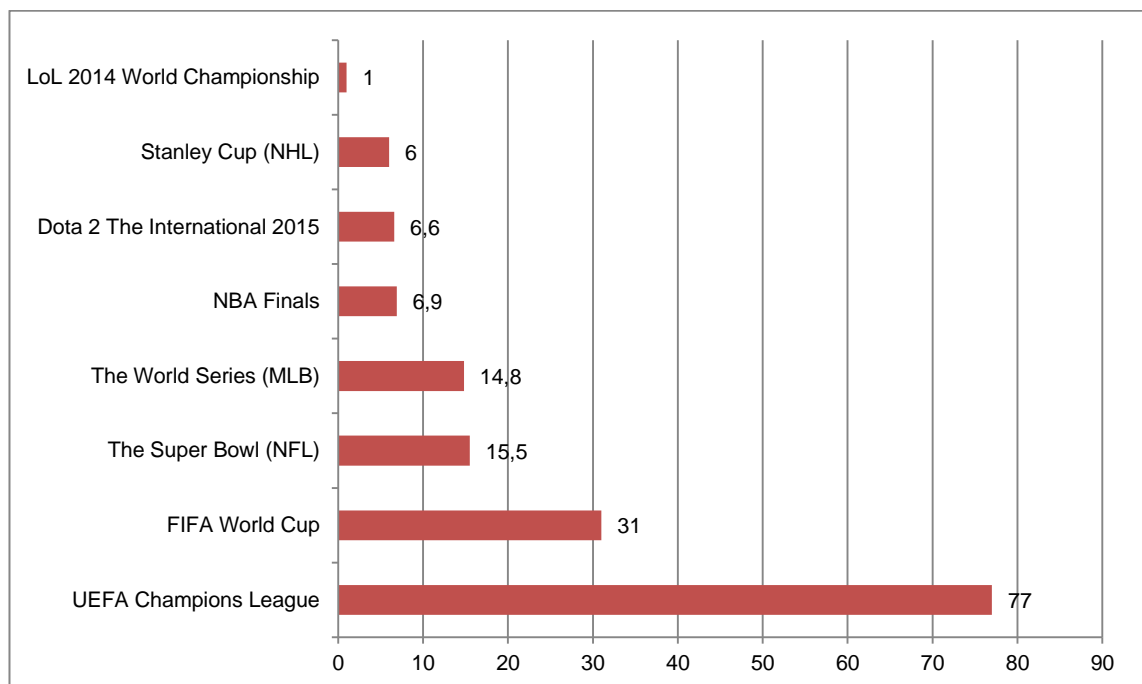


Maailman selvästi suosituin urheilutapahtuma on FIFA World Cup, joka keräsi vuonna 2006 715 miljoonaa katsojaa. Jalkapallo on maailman suosituin urheilulaji, ja sen saama maailmanlaajuinen huomio on vertaansa vailla. Yhdysvalloissa suosituista urheilulajeista jääkiekko (NHL), pesäpallo (MLB) sekä koripallo (NBA) jäävät Dota2:n sekä LoL:n perään vuoden 2014 katsojaluvuissa (taulukko 7).

Perinteisistä urheilulajeista poiketen eSportsin yleisö koostuu pääasiassa internetin kautta tapahtumia seuraavista katsojista. Perinteisten urheilulajien katsojat ovat valtamäärissä television kautta tapahtumia seuraavia katsojia. Internet on luonut valtavan potentiaalisen katsojakunnan kaikenlaisille yleisötapahtumille, ja elektronisen urheilun nopea kasvu katsojamäärien saralla voidaankin osaltaan selittää tällä helpolla saatavuudella.

Suosituin eSports turnaus League of Legendsin 2014 World Championship on yllättäen selvästi suositumpi kuin mikään näistä, ylittäen NBA:n mestaruusottelun 17,7 miljoonan katsojan yleisön melkein kymmenellä miljoonalla. The International Dota 2 -turnaus, joka on eSports-skenen rahakkain turnaus, on hieman League of Legendsin perässä, mutta ylittää silti myös nämä perinteiset urheilulajit 20 miljoonan katsojan yleisöllä. Amerikkalainen jalkapallo (NFL) on silti edelleen huomattavasti suositumpaa, ja Super Bowl on edelleen yksi maailman katsotuimmista tapahtumista yli 108 miljoonan katsojan yleisöllä. Jalkapallon suosiosta kertoo myös, että FIFA World Cupia rahakkaampi turnaus UEFA Champions Leaguen finaali on vielä selvästi katsotumpi 165 miljoonalla katsojalla. [11.]

Taulukko 8. Dota 2:n ja LoL:n suurimpien turnausten voitosta saatava palkinto verrattuna perinteisten urheilulajien vastaaviin tapahtumiin. Luvut on ilmaistu miljoonina dollareina (\$). [18.]



Palkintorahojen puolella UEFA Championships League on selvästi muiden yläpuolella 77 miljoonan dollarin palkintopotillaan (taulukko 8). Maailman suosituimman urheilutapahtuman FIFA World Cupin palkintopotti on myös yli 31 miljoonaa dollaria.

eSports-turnaukset ovat listan viimeisimpinä. League of Legendsin 2014 World Championshipin voittajajoukkue sai tasan miljoona dollaria, joka on huomattavasti

vähemmän kuin katsojamääriltään vähemmän suosittujen Stanley Cupin (NHL) tai The World Seriesin (MLB). The International 2015:n voittajat kuittasivat 6,6 miljoonaa dollaria, joka on samalla viivalla kuin lähes yhtä katsottu NBA finaali, mutta silti huomattavasti vähemmän kuin The World Series. Näistä luvuista tulee kuitenkin ottaa huomioon, että jokaisessa listatussa perinteisessä urheilulajissa voiton jakavan joukkueen koko on selvästi suurempi. Siinä missä Dota 2:n ja LoL:n joukkueen koko on viisi pelaajaa, on vastaava luku esimerkiksi jalkapallossa ja jääkiekossa noin kaksikymmentä. Täten yksittäisen urheilijan saama osuus on prosentuaalisesti pienempi. Lopulliseen summaan vaikuttaa myös organisaation ottama osuus sekä urheilijoiden sopimusten väliset erot.

Luvuista voidaan nähdä, kuinka elektronisen urheilun nopea kasvu on luonut perinteisistä urheilulajeista poikkeavaa eroa katsojamäärien ja palkintopottien suhteen. Internet on mahdollistanut eSportsille huomattavan yleisön, mutta turnausten ja pelien suhteellinen uutuus ja sitä kautta tietty epävakaus vaikuttaa varmasti alalla liikkuviin rahamääriin verrattuna perinteisiin urheilulajeihin.

3 Tietoturvaasteet kilpapelamisessa

Kilpapelamisen yleistyminen ja turnausten lukumäärän nopea lisääntyminen on johtanut ympäristöön, jossa keskitettyjen tietoturva- ja anticheat-käytäntöjen puute aiheuttaa epävarmuutta niin pelaajien, sponsoreiden kuin kisajärjestäjienkin keskuudessa. Nopea kasvu on tuonut paljon uusia turnausjärjestäjiä ja liigoja, jotka luovat omat tietoturvakäytäntönsä ennalta määritettyjen ja määrättyjen käytäntöjen puuttuessa. Ala on hitaasti alkanut vakiintumaan, ja suurimmat kisajärjestäjät ovat alkaneet saamaan statusta yhteisössä, mutta muuttuvat ja epäsystemaattiset käytännöt luovat edelleen ympäristön, joka mahdollistaa väärinkäytökset.

Kasvavat rahamäärät tuovat tarpeen systemaattisille ja luotettaville käytännöille sekä ympäristölle, jonka eheyteen sekä katsojat että sponsorit voivat luottaa. Jos ala ei kykene osoittamaan pystyvänsä kitkemään väärinkäytöksiä sekä esim. katsomiskokemuksia heikentäviä DDoS-ongelmia, on elektronisen urheilun vaikea vakiinnuttaa itseään vakavasti otettavana liiketoiminnan alana tai urheiluna. Hyvänä esimerkkinä voidaan pitää tämän vuoden The International Dota 2 -turnausta, joka on Valve Corporationin järjestämä ja suurimmalta osalta yhteisön rahoittama turnaus,

jonka palkintopotissa oli tänä vuonna 18 429 613 dollaria. Kyseisen turnauksen päätapahtuma jouduttiin useina päivinä keskeyttämään jatkuvien DDoS-hyökkäysten vuoksi. Pahimmillaan yli tunnin mittaiset katkokset heikentävät varmasti sekä katsojien että potentiaalisesti kiinnostuneiden sponsoreiden kiinnostusta peliä kohtaan. Asiaa pahensi myös se, että The International on koko Dota 2:n vuoden tärkein turnaus, ja Valven onnistumista kisajärjestäjänä voidaan varmasti pitää jonkinlaisena suunnannäyttäjänä myös muiden turnausten osalta. [12; 13.]

3.1 DDoS ja kilpapelaminen

Palvelunestohyökkäykset ovat olleet viimeisten vuosien aikana pinnalla monissa eri asiayhteyksissä. DDoS- tai DoS-hyökkäykset eivät ole itsessään uusi asia, ja aikaisin hyökkäys on tehty jo vuonna 1999 Minnesotan yliopiston IRC-palvelinta vastaan. Elektronisen urheilun suosion kasvu on tuonut palvelunestohyökkäykset myös kilpapelamiseen, ja niiden helppo toteutus sekä potentiaalinen hyöty tekevät niistä erittäin houkuttelevan vaihtoehdon verkkorikollisille. [19.]

3.1.1 Motiivit

Kuten lähes kaikissa urheilulajeissa, myös suurimpien eSports-tapahtumien yhteydessä on nykyään mahdollista lyödä vetoa oikeasta rahasta. Sivustot kuten Vulcun ja AlphaDraft sekä esimerkiksi Betsafe tarjoavat nykyään mahdollisuuden lyödä erityyppisiä vetoja joko pelaajiin tai otteluihin liittyen.

Koko alalla liikkuvat rahamäärät olivat vuonna 2014 194 miljoonaa dollaria. Ne voivat kasvaa vuoteen 2017 mennessä jopa miljardiin dollariin. Vedonlyönnin mahdollisuus sekä nopeasti kasvavat rahamäärät luovat väärinkäytölle motiivin niin yksittäiselle tekijälle kuin suuremmillekin toimijoille. [21.]

Monet tämän hetken eSports-turnaukset noudattavat sääntöjä, jotka mahdollistavat väärinkäytökset palvelunestohyökkäysten avulla. Nykyään käytännössä kaikkien suurten eSports-turnauksien finaalit pelataan LAN-ympäristöissä, mutta finaaleihin pääsevät joukkueet päätetään online-karsinnoissa, joissa pelaajat pelaavat omilla tietokoneillaan joko kotonaan tai joukkueen tiloissa. Jos pelin aikana pelaajan internet-

yhteys ja tätä kautta yhteys peliin katkeaa, joutuu kyseisen pelaajan joukkue turnauksesta riippuen joko ottamaan sijaispelaajan tai luovuttamaan ottelun.

Havainnollistavana esimerkkinä voidaan käyttää vuoden 2015 elokuussa tapahtunutta hyökkäystä League of Legends -pelaaja Thomas "Kirei" Yuenia vastaan. Hänen joukkueensa oli pelaamassa European Challenger Seriesin karsintaottelua. Yuenin IP:tä kohtaan suoritettiin palvelunestohyökkäys, ja monista yrityksistä huolimatta hän ei kyennyt yhdistämään takaisin otteluun vaaditun kymmenen minuutin sisällä. Turnauksesta vastaavan Riot Gamesin sääntöjen perusteella hänen joukkueensa joutui luovuttamaan ottelun. [20.]

Vedonlyönnin kannalta kyky vaikuttaa ottelun lopputulokseen joko suoraan pakottamalla toinen joukkue antamaan luovutusvoitto, tai välillisesti heikentämällä heidän suorituskykyään sijaispelaajan avulla antaa vahvan motiivin suorittaa palvelunestohyökkäyksiä. Motiivia vahvistaa vielä se, että palvelunestohyökkäysten suorittaminen on nykyään erittäin helppoa.

Muina motiiveina hyökkäysten suorittamiseen voi olla halu saada ammatillinen urheilu vaikuttamaan amatöörimäiseltä, tai yksinkertaisesti ilkeältä. Ammattipelaaminen on pääasiassa nuorempien sukupolvien suosiossa, ja helppo toteutus sekä internetin näennäinen anonymiteetti saattaa pienentää kynnystä palvelunestohyökkäysten toteuttamiseen.

3.1.2 Yleisimmät menetöt palvelunestohyökkäyksen toteuttamiseen

Yksinkertaista palvelunestohyökkäystä toteutettaessa ainoa asia, jonka hyökkääjä tarvitsee, on kohteen IP-osoite. Erityyppisiä DDoS-palveluita on tarjolla monia ja yksittäisen IP:n estämiseen vaadittava sijoitus on erittäin matala. Niin sanotut Botter-palvelut antavat käytännössä kenelle tahansa mahdollisuuden suorittaa palvelunestohyökkäys yksittäistä IP-osoitetta vastaan (kuva 1). LAN-tapahtumia vastaan tämä metodia ei välttämättä volyymin pienuudesta johtuen toimisi, mutta yksittäistä kotitaloutta vastaan kyseiset palvelut ovat erittäin tehokkaita. Internetpalveluntarjoajien yleisin suhtautumistapa tilanteessa, jossa yksittäinen IP-osoite alkaa vastaanottamaan valtavia määriä dataa, on vain katkaista yhteys, jotta muiden yhteyksien toimivuus alueella ei vaarannu. Botter-palvelut luovat myös anonymiyyttä hyökkäysten suorittajille, sillä hyökkääjän tulee vain syöttää uhrin IP-

osoite ja suorittaa maksu, jonka jälkeen palvelunestohyökkäys suoritetaan palveluntarjoajan botnet-verkolla.



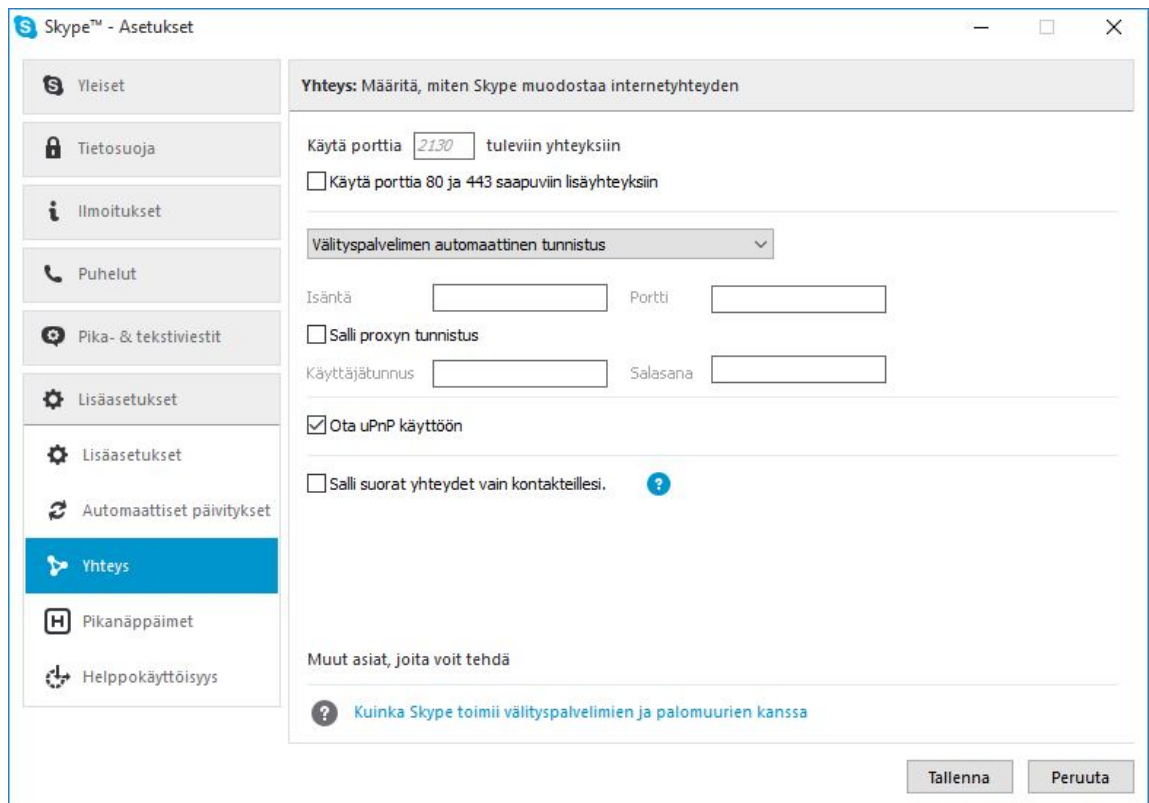
Kuva 1. Kuvankaappaus erilaisista kaupallisista Booter-palveluista.

Booter-palvelut antavat myös hyökkääjän valita monista erilaisista Layer 4- ja Layer 7 -tason hyökkäyksistä, joista osa on erittäin tehokkaita katkaisemaan yksittäisen henkilön internet yhteyden. Osalla näistä hyökkäyksistä voidaan jopa saada aikaan vain suurta viivettä pakettien vastaanottoon, jolloin pelaaja pystyy mahdollisesti yhdistämään takaisin peliin, mutta suuren yhteysviiveen takia hän ei kykene pelaamaan kilpailullisella tasolla.

3.1.3 Uhrin IP-osoitteen selvittäminen yleisesti käytetyillä ohjelmilla

Online-ympäristöissä ammattipelaajilla on kaksi ohjelmaa, jotka ovat lähes aina vaadittuja. Ensimmäisenä on luonnollisesti pelattava peli ja toisena kommunikaatioon käytettävä puheohjelma. Valven tuotteet kuten Dota 2 sekä Counter-Strike: Global Offensive toimivat Valven oman Steam-nimisen pelikirjaston ja kauppana toimivan alustan kautta.

Suosituin verkossa käytettävä puheohjelma on Skype, joka on erittäin helppokäyttöinen ja luotettava, mutta samalla myös kilpapelamisen kannalta hyvin haavoittuvainen. Skype muodostaa soiton aikana P2P-yhteyden, jolloin vastaajan IP-osoite saadaan helposti selville esimerkiksi Wireshark-ohjelmalla yksinkertaisesti saapuvia ja lähteviä paketteja tarkastelemalla.

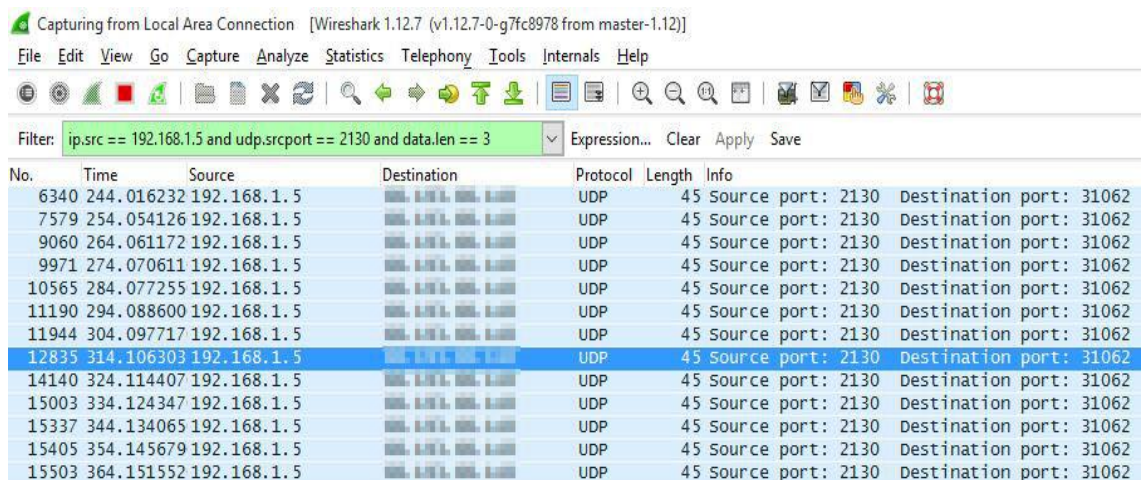


Kuva 2. Skype-asetukset, Yhteys-välilehti.

Wiresharkin konfiguraatiota varten hyökkääjän tulee asettaa Skypen asetuksista tulevien yhteyksien portti halutuksi, sekä poistaa valinta "Käytä porttia 80 ja 443 saapuviin lisäyhteyksiin". Tällöin kaikki liikenne kulkee valitun portin (tässä

tapauksessa portti 2130) kautta. Lisäksi hyökkääjän tulee tuntea oma IP-osoitteen, jonka saa Windows-ympäristössä helpoiten selville avaamalla komentokehötteen ja syöttämällä komennon "ipconfig".

Wireshark konfiguroidaan valitsemalla käytössä oleva adapteri, jonka kautta internetyhteys kulkee sekä filteröimällä paketit hyökkääjän omalla lähde IP:llä (tässä tapauksessa 192.168.1.5) sekä Skypeen käyttämällä portilla. Pakettien dataosuuden pituuden rajoittaminen on valinnaista, mutta auttaa erottelmaan paketteja tehokkaammin.



Capturing from Local Area Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.src == 192.168.1.5 and udp.srcport == 2130 and data.len == 3` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6340	244.016232	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
7579	254.054126	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
9060	264.061172	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
9971	274.070611	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
10565	284.077255	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
11190	294.088600	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
11944	304.097717	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
12835	314.106303	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
14140	324.114407	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
15003	334.124347	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
15337	344.134065	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
15405	354.145679	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062
15503	364.151552	192.168.1.5	192.168.1.5	UDP	45	Source port: 2130 Destination port: 31062

Kuva 3. Wireshark-kaappaus Skype-soitosta uhrille. Filteri on asetettu määrittäksillään "ip.src == 192.168.1.5 and udp.srcport == 2130 and data.len == 3". Uhrin IP-osoite on sensuroitu tietoturvasyistä.

Konfiguraatioiden jälkeen tulee hyökkääjän enää soittaa uhrilla Skype välityksellä. Riippumatta siitä, vastaako uhri vai ei, tulee uhrin IP-osoite näkyviin Wiresharkin Destination kohtaan. Hyökkäyksen helppoutta korostaa se, että uhrin ei tarvitse millään tavalla vuorovaikuttaa hyökkääjän kanssa jotta IP-osoite saadaan selville. Useimmat muut palvelut vaativat myös uhrilta vuorovaikutusta, kuten esimerkiksi Steam palvelun kautta tehdyissä IP-osoitteen selvityksissä.

Capturing from Local Area Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

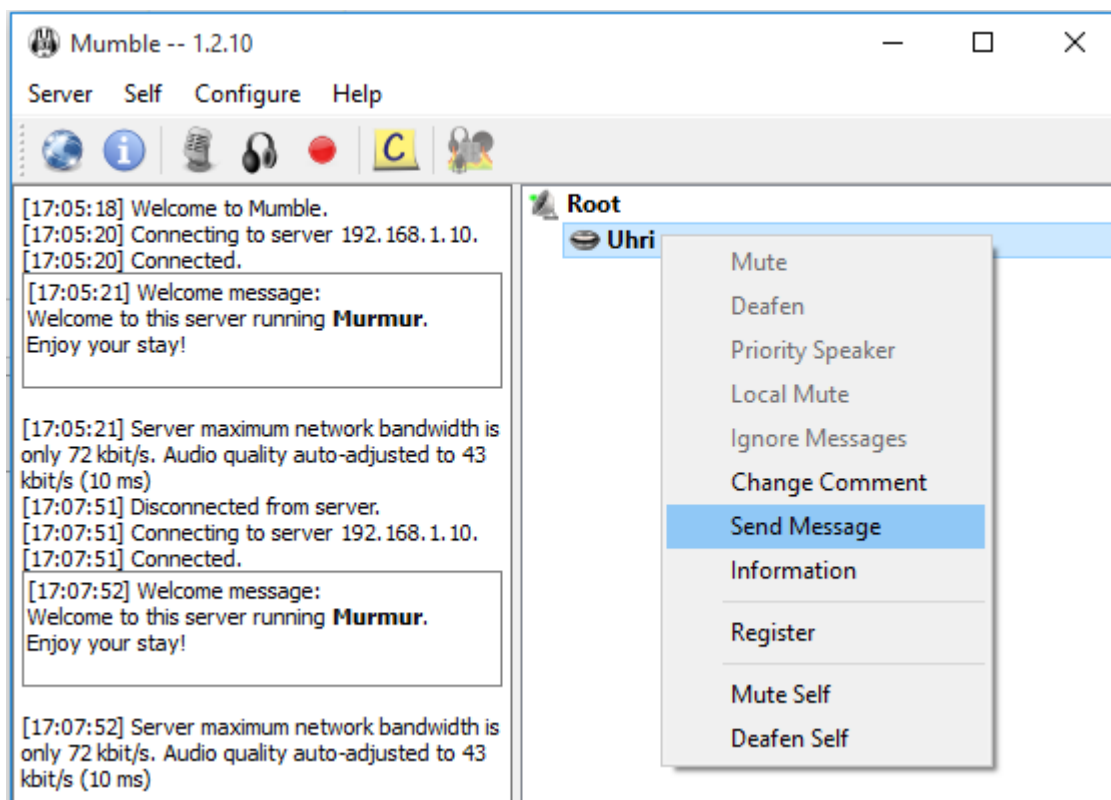
Filter: classicstun Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1673	28.8242370	192.168.1.5	192.254.196.41	CLASSIC	62	Message: Binding Request
1674	28.8650650	192.254.196.41	192.168.1.5	CLASSIC	98	Message: Binding Response
1682	30.0255660	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1686	30.0875280	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1688	30.1099480	192.254.196.41	192.168.1.5	CLASSIC	110	Message: Binding Response
1689	30.1140520	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1690	30.1141220	192.168.1.5	192.254.196.41	CLASSIC	110	Message: Binding Response
1705	31.1194550	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1706	31.1420100	192.254.196.41	192.168.1.5	CLASSIC	110	Message: Binding Response
1708	31.1540680	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1709	31.1541980	192.168.1.5	192.254.196.41	CLASSIC	110	Message: Binding Response
1718	31.6114870	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1728	32.0988620	192.168.1.5	192.254.196.41	CLASSIC	98	Message: Binding Request
1729	32.1140920	192.254.196.41	192.168.1.5	CLASSIC	98	Message: Binding Request
1730	32.1141870	192.168.1.5	192.254.196.41	CLASSIC	110	Message: Binding Response

Kuva 4. Wireshark-kaappaus Steam-puhelusta. Filteri on asetettu määrittäksill "classicstun". Uhrin IP-osoite on sensuroitu tietoturvasyistä. Ylimmät kaksi riviä esittävät steamien palvelimen ja hyökkääjän välistä keskustelua. Loput riveistä hyökkääjän ja uhrin välistä pakettien vaihtoa.

Steamin kautta tehtävässä hyökkäyksessä Wireshark konfiguroidaan muuten samoin kuin Skypeen kautta, mutta filteri asetetaan ainoastaan määrittäksellä "classicstun", joka suodattaa paketit vastaamaan perinteistä VoIP-puheluissa käytettävää protokollaa (kuva 4). Skypestä poiketen Steamin kautta IP-osoitetta selvitetäessä uhrin tulee itse mahdollistaa osoitteensa saatavuus. Jotta IP-osoite on mahdollista lukea, tulee uhrin ensin joko olla hyökkääjän kaverilistalla tai hyväksyä hyökkääjän tekemä kaveripyynnö. Tämän jälkeen uhrin tulee vielä vastata hyökkääjän tekemään puheluun Steamin sisällä. Puheluyhteyden muodostuessa näkee hyökkääjä uhrin IP-osoitteen suoraan Wiresharkin syötteestä Source sekä Destination kohdista, jotka vaihtelevat uhrin sekä hyökkääjän oman IP-osoitteen välillä.

Toinen pelaajien keskuudessa suosittu puheohjelma on avoimen lähdekoodin ilmaisohjelma Mumble. Jos uhri käyttää yleisesti tunnettua Mumble-palvelinta tai hyökkääjä jollain tapaa vuotaa tiedot käytettyyn palvelimeen, voi hyökkääjä tämän jälkeen hyödyntää Mumblesta löytyvää Html-pohjaista heikkoutta. Edellisistä tavoista poiketen tämän heikkouden hyödyntäminen vaatii hyökkääjältä myös pääsyä selvityksessä käytettävän HTTP-palvelimen access-lokeihin.



Kuva 5. Mumblen kautta tehdyssä IP-osoitteen selvityksessä hyökkääjä lähettää uhrille yksityisviestin, jonka sisältö on hyökkääjän hallussa olevan HTTP-palvelimen materiaalia.

Hyökkääjä lähettää uhrille yksityisviestin, joka voi olla mikä tahansa kuvatiedosto, joka löytyy hyökkääjän hallitsemalta HTTP-palvelimelta. Oletusasetuksilla Mumble lukee tämän tiedoston, ja uhrin IP-osoite ilmestyy automaattisesti HTTP-palvelimen access-lokeihin. Työssä tehdyssä esimerkkitapauksessa käytetty HTTP-palvelin oli Linux-pohjainen Apache, jonka access-lokit löytyvät oletusarvoisesti polusta `/var/log/apache2/access.log`, ja uhrin tekemä käynti näkyy tiedoston viimeisellä rivillä varustettuna uhrin omalla IP-osoitteella ja aikaleimalla.

Vastaavia metodeja IP-osoitteen selvittämiseen on monia muitakin kuten esimerkiksi Facebookin chat-palvelun kautta tehty vastaava selvitys, mutta kuten Steamien kautta tehty selvitys, vaativat ne aina uhrilta itseltään vuorovaikutusta hyökkääjän kanssa. Muita tapoja selvitykseen on esimerkiksi IP-logger-palvelut, joiden avulla hyökkääjä voi naamioida yksinkertaisen verkkosivun esimerkiksi Googlen URL-lyhentäjän avulla uskottavan näköiseksi. Jos uhri klikkaa kyseistä linkkiä, saa hyökkääjä tämän IP-osoitteen selville HTTP Request -paketissa ilmenevän IP-osoitteen kautta hyvin samaan tapaan kuin Mumblen kautta tehdyssä selvityksessä.

Edellä mainittujen tapojen lisäksi IP-osoitteen selvittäminen on joissain tilanteissa mahdollista myös suoraan pelattavasta pelistä, jos kyseisessä pelissä on tietoturvaavoittuvuuksia. Näiden löytäminen ja hyödyntäminen on kuitenkin huomattavasti monimutkaisempaa, ja pelejä kehittävät yhtiöt tekevät jatkuvasti työtä heikkouksien paikkaamiseksi. Vuoden 2014 lopulla Valven Dota 2 -pelissä oli tietoturvaavoittuvuus, joka mahdollisti kenen tahansa pelaajan IP-osoitteen hankkimisen suoraan peliohjelman kautta riippumatta uhrin vuorovaikutuksesta. Vuoden 2015 toukokuuhun mennessä kyseinen haavoittuvuus oli paikattu, eikä yleisesti tunnettuja haavoittuvuuksia tällä hetkellä ole.

3.1.4 Palvelunestohyökkäysten ennaltaehkäisy online-kilpapelamisessa

Yksittäisten käyttäjien ja IP-osoitteiden tapauksissa tärkein tekijä palvelunestohyökkäysten ennaltaehkäisyssä on saada käyttäjä itse ymmärtämään, mitkä tekijät vaikuttavat IP-osoitteen vaarantumiseen. Kuten kohdassa 3.1.3. todettiin, vaativat useimmat IP-osoitteen selvitysmetodit jonkinlaista vuorovaikutusta uhrilta itseltään. Jos käyttäjä ymmärtää nämä riskit ja osaa välttää toimia, jotka vaarantavat IP-osoitteen, on palvelunestohyökkäyksen toteuttaminen selvästi vaikeampaa keskivertohyökkäjälle.

Samalla myös pelattavalla koneella olevat muut ohjelmat tulee valita hyvin tarkasti, ja niiden kokonaismäärä tulee pitää minimissä. Puheohjelmien tapauksessa käytettävään ohjelmaan ja siitä löytyviin heikkouksiin tulee perehtyä. Kohdassa 3.1.3 esitetyistä esimerkeistä Skype ja Mumble voidaan konfiguroida siten, että esiintyneet heikkoudet saadaan estettyä.

Näiden toimenpiteiden lisäksi jokaisen ammattilaispelaajan tulisi siirtyä käyttämään kaupallisia VPN-palveluita. Nykyään löytyviä, jopa suoraan pelaajille suunnattuja ja palvelunestohyökkäyksiä silmälläpitäen suunniteltuja VPN-palveluita löytyy noin kymmenen euron kuukausihinnoilla. VPN-tunnelin käyttö luo käyttäjälle anonyymiyden kerroksen, jolloin käyttäjän omaa IP-osoitetta on selvästi vaikeampaa saada selville perinteisin menetelmin. Yleisistä palveluntarjoajista poiketen VPN-verkot on myös suunniteltu kestämaan palvelunestohyökkäyksiä, eivätkä ne myöskään poista käyttäjää hyökkäyksen tapahtuessa automaattisesti verkosta kuten yleisimmät internetpalveluntarjoajat. Huonona puolena VPN:n käytössä on joissain tapauksissa

latenssin kasvu, jonka pysyminen matalana on kilpapelaaamisen kannalta erittäin vitaalia. Tämän takia VPN ei välttämättä aina ole käytännöllinen vaihtoehto. [20; 22.]

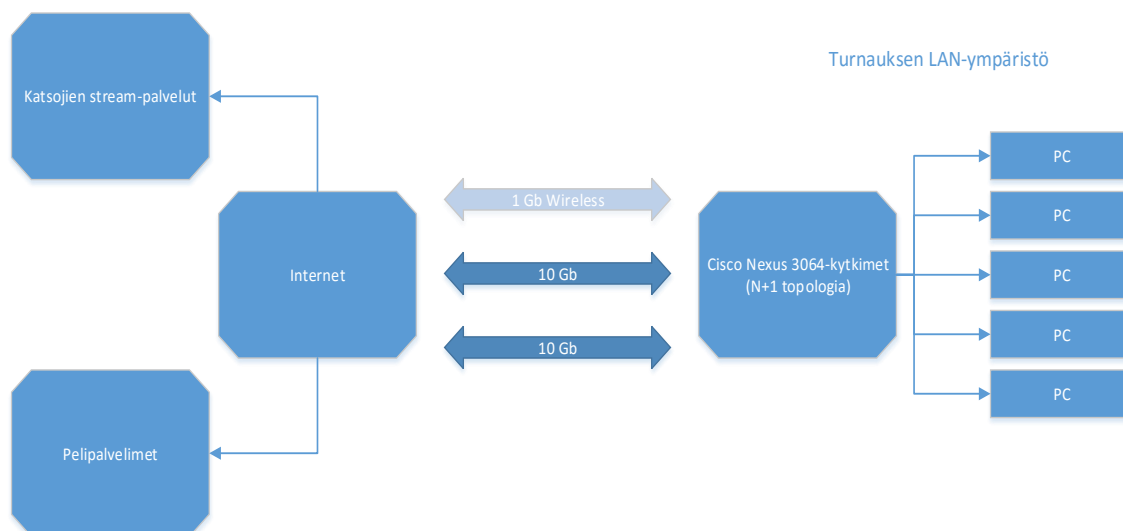
Näiden tekijöiden lisäksi jokaisella pelaajalla tulisi olla mahdollisuuksien mukaan myös toinen, varalla oleva internetyhteys. Tätä optiota ei ole kaikissa maissa saatavilla, mutta esimerkiksi Suomessa kaupunkialueilla yleistyneet nopeat 4G-yhteydet täyttävät pelaamiseen tarvittavat nopeus- ja latenssikriteerit, ja tarpeen mukaan pelaaja voi nopeasti vaihtaa yhteytensä täysin erilliseen internetyhteyteen, jonka IP-osoitteen selvittäminen tulee toteuttaa erikseen.

3.1.5 Mitigaatio ja preventaatio LAN-ympäristöissä

LAN-ympäristöissä palvelunestohyökkäysten estäminen on osaltaan yksiulotteisempaa ja toisaalta selvästi haastavampaa kuin online-tilanteissa. Yksittäisen pelaajan tietokone on selvästi paremmin suojattu, sillä NAT-konfiguraatiot mahdollistavat ympäristön, jossa vain koko LAN-tapahtuman ulkoverkkoon käytettävä IP-osoitteimisto näkyy ulkopuolisille, ja yksittäisen pelaajan IP-osoite on maskeerattu sisäverkossa. Täten kohdassa 3.1.3. esitetyt menetelmät palauttaisivat ainoastaan LAN-ympäristön ulkoverkon IP-osoitteen, ja koko tapahtuman verkon kaataminen palvelunestohyökkäyksellä vaatii moninkertaisesti suurempaa kapasiteettiä kuin yksittäisen henkilön estäminen. Koska hyökkäykset kohdistuisivat koko LAN-ympäristöön eikä ainoastaan yksittäisen pelaajan yhteyteen, vie tämä samalla motivaatiota yksittäisiltä tekijöiltä suorittaa hyökkäyksiä, sillä henkilökohtaista hyötyä vedonlyönnin tai muun vastaavan rahallisen edun muodossa on huomattavasti vaikeampaa, ellei mahdotonta, saavuttaa.

Tämä jättää jäljelle hyökkäykset, joita suoritetaan joko ilkeiden takia tai halusta vaikuttaa koko elektronisen urheilun tai yksittäisen pelin maineeseen ammattimaisena urheiluna negatiivisesti. Ongelmat turnausten järjestämisessä ja sujuvassa toteuttamisessa antaa nopeasti katsojille kuvan amatöörimäisyydestä, joka heikentää niin katsojien kuin sponsoreidenkin luottoa lajiin.

Vuoden 2015 The International -turnausta varten turnauksen järjestäjä Valve oli palkannut OptaNet-nimisen yrityksen toteuttamaan turnauksen verkkoympäristön ja varmistamaan että verkko kestäisi sekä palvelunestohyökkäyksiä kuin mahdolliset laiteongelmat ilman, että turnauksen kulku keskeytyisi.



Kuva 6. The International 2015 Dota 2 -turnauksen verkkoympäristö.

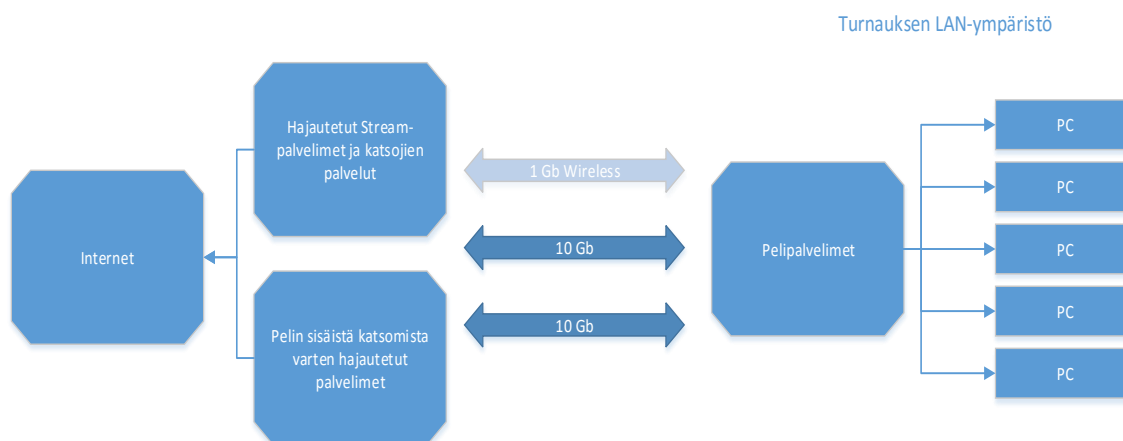
Turnauksen verkko oli toteutettu Ciscon Nexus 3064 layer 3 -kytkimillä sekä Ciscon ASA-laitteilla. Verkko luotiin N+1-mallilla, joka tarkoittaa, että verkon jokaisessa yhteyspisteessä yksi laite voi kaatua ilman, että verkko menettää toimintakykyään (kuva 6). Ulkoverkkoon yhteys muodostettiin kahden 10 Gbit nopean linjan avulla. Niistä toinen oli varattu ainoastaan pelaajien ja pelipalvelinten väliseen liikenteeseen. Toinen linja oli ylläpitäjien ja streamaus-palveluiden datan välittämiseen. Linjat oli myös konfiguroitu siten, että yhden linjan pettäessä kaikki liikenne siirtyisi saumattomasti toiselle linjalle. Näiden lisäksi käytössä oli vielä kolmas, 1 Gbit nopea langaton yhteys, jota pidettiin varalinjana sen varalle, että molemmat päälinjat jostain syystä katkeaisivat. OptaNet valvoi jatkuvasti verkkoa ja sen suorituskykyä, jotta verkon suorituskyky pysyisi vaaditulla tasolla tapahtumassa, jota seurasi yli kaksikymmentä miljoonaa ihmistä. [23.]

The International 2015 -verkkosuunnittelu oli järkevästi toteutettu, ja palvelunestohyökkäysten toteuttaminen LAN-ympäristöä tai yksittäistä konetta vastaan oli erittäin haastavaa. Silti turnaus kärsi useampana päivänä DDoS-ongelmista, ja pelit jouduttiin keskeyttämään jopa tunneiksi kerrallaan, kun teknikot kamppailivat saadakseen pelaamiseen vaadittavat yhteydet takaisin kuntoon. OptaNet oli tähän ongelmaan syytön, ja heikkous verkkosuunnittelusta löytyi tällä kertaa pelin kehittäjän ja turnausjärjestäjän Valven puolelta. Dota 2 on verkkopeli, jossa yksittäinen peli toimii sille varatun yksittäisen palvelimen kautta, ja Valven keskitetyt palvelimet sijaitsevat luonnollisesti eri paikassa kuin missä turnaus järjestettiin. Tämä loi verkkoon

heikkouden, jota hyökkääjät pääsivät hyödyntämään suorittamalla hyökkäykset palvelimia kohtaan.

Perinteisesti suosituista eSports-peleistä on löytynyt lokaali pelimuoto, joka mahdollistaa pelin hostaamisen samasta fyysisestä lokaatiosta kuin missä pelaaminen tapahtuu. Pelien kasvanut interaktiivisuus sekä mahdollisuus seurata ammattilaispelejä suoraan pelin sisältä on kuitenkin tehnyt tästä mahdotonta ja oletusarvoisesti host-koneiden tulee sijaita esimerkiksi Dotan tapauksessa Valven omissa palvelinsaleissa. Mahdollisuus seurata pelejä suoraan pelin sisältä tuo uusia ulottuvuuksia pelien seuraamiseen, ja katsoja voi esimerkiksi seurata suosikkipelaajansa pelaamista suoraan kuin katsoisi tämän ruutua, nähdessä jokaisen hiiren napsautuksen ja liikkeen. Turnauspelaamisessa tärkeintä on kuitenkin pelin sujuva kulku, ja varsinkin nyt kun host-koneiden erillisen sijainnin on todettu mahdollistavan palvelunestohyökkäykset peliä kohtaan, tulisi pelinkehittäjien reagoida ongelmaan.

Yksi mahdollinen ratkaisu tähän heikkouteen olisi luoda pelistä lokaali versio, joka tukisi palvelinten sijoittamista samaan fyysiseen tilaan kuin missä pelaaminen tapahtuu.



Kuva 7. Parannusehdotus The International 2015 -verkkoympäristöstä.

Jos pelipalvelimet olisivat samassa fyysisessä lokaatiossa turnauksen kanssa, voitaisiin ulkoverkkoon menevät linjat valjastaa pelidatan välittämiseen. Ulkoverkon välityslokaatiossa voisi olla hajautettuja palvelimia sekä streamaus-palveluiden kautta seuraaville katsojille kuin pelin sisäisille katsojille (kuva 7). Tämä eristäisi turnauksen sisäverkon internetistä, eikä itse tapahtumassa tapahtuva pelaaminen vaatisi

minkäänlaista yhteyttä ulkoverkkoon. Lisäksi itse tapahtumaa vastaan suoritettava palvelunestohyökkäys olisi selvästi vaikeampaa toteuttaa turnauspaikalla olevan verkon ollessa sitä silmällä pitäen konfiguroitu ja suunniteltu.

Tämä ei kuitenkaan poistaisi koko palvelunestohyökkäyksen ongelmaa, jos hyökkääjän motiivina on ilkeä tai halu luoda amatöörimäistä ilmapiiriä lajin ympärille. Vaikkei hyökkäys voisi kohdistua itse pelaajia tai peliä kohtaan, voi hyökkääjä saavuttaa motiivinsa mukaisen tavoitteen vaikeuttamalla katsojien kokemusta turnauksesta. Hyökkäyksen suorittaminen ja efektiivisyyden saavuttaminen olisi kuitenkin hajautettuja palvelimia vastaan selvästi vaikeampaa, ja vastaavanlainen efektiivisyys vaatisi moninkertaiset resurssit verrattuna tämänhetkiseen ratkaisuun.

Lokaalin version luominen pelistä vaatisi suunnitelmallista panostusta pelinkehittäjien puolelta. Rahallisesta näkökulmasta on helppo ymmärtää, miksi tällaisia ratkaisuja ei peleihin ole luotu oletusarvoisesti, mutta lajin suosio sekä turnauksissa liikkuvien rahamäärien kasvu luovat perustellun tarpeen turnausversioille peleistä. 2015 The Internationalin palkintopotti oli yli 18 miljoonaa dollaria. Alan muiden turnausten infrastruktuurin sekä itse pelien suunnittelu pitäisi olla rahamäärän mukaisia.

3.2 Ohjelmistopohjaiset huijausohjelmat ja niiden vaikutusten vähentäminen

Huijaaminen ja epäreilun edun saavuttaminen on tuttua jo perinteisen urheilun puolelta, jossa dopingskandaalit ovat värittäneet useita eri ammattilaislajeja vuosien varrella. Myös tietokonepelaamisen puolella erilaisia huijausohjelmia on ollut olemassa jo useita vuosikymmeniä, ja varmasti jokainen, joka on pelannut FPS-pelejä internetissä on joskus törmännyt pelaajaan joka, käyttää apuohjelmaa moninaisten epäreilujen etujen saavuttamiseen pelissä.

Yleisimmät huijaustyökalut parantavat joko pelaajan tarkkuutta ja hallintaa joko hiirellä (ns. aimbotit) tai näppäimistöllä (skriptit). Näiden lisäksi myös ohjelmat, jotka antavat pelaajalle kyvyn saada informaatiota, jota pelaajan olisi muuten mahdotonta nähdä tai kuulla, ovat suosittuja (ns. wallhackit). Vaikka perinteisesti tällaiset ohjelmat ovat suhteellisen helppo havaita, ja niiden käyttö on rajoittunut satunnaiseen online-pelaamiseen, ovat myös huijausohjelmat parantuneet vuosien varrella, eikä niiden huomaaminen ole lainkaan niin yksiselitteistä kuin aikaisemmin. Tämä on tuonut

huijausohjelmia myös ammattimaiseen pelaamiseen ja varsinkin Counter-Strike: Global Offensive -pelin yhteisöä ovat ravistelleet useat huijauskandaalit viimeisten vuosien aikana. [24.]

3.2.1 Epärehellisten metodien vaikutusten vähentäminen ja estäminen

CS:GO ja muut FPS-pelit ovat muita pelejä alttiimpia ympäristöä hyödyntäville huijausohjelmille kuten wallhackeille, koska ne toimivat kolmiulotteisessa ympäristössä. Muut nykyään suosittu pelit kuten Dota 2, League of Legends tai Starcraft 2 saattavat vaikuttaa kolmiulotteisilta, mutta todellisuudessa peliareena on kaksiulotteinen lukuunottamatta korkeuseroja. Kolmiulotteisuus tarkoittaa, että pelaajan ja palvelimen väliseen datanvaihtoon tulee sisällyttää enemmän dataa, jotta pelikokemus ja latenssi pysyvät kilpailullisella tasolla. Samalla se avaa enemmän ovia huijausohjelmille saada selville esimerkiksi wallhack-tapauksissa, jossa vastustavat pelaajat liikkuvat. Kaksiulotteisten pelien tapauksessa suurin osa datasta, jota pelaajan ei tule nähdä tai kuulla, voidaan pitää täysin poissa pelaajan ja palvelimen välisestä tietoliikenteestä. Täten huijausohjelmien toteuttaminen on selvästi vaikeampaa.

Wallhackejä pyritään estämään pääasiassa anticheat-ohjelmilla, jotka valvovat jatkuvasti pelaajan eli clientin sekä palvelimen eli hostin välistä liikennettä ja pyrkivät päättämään mahdollisia huijausohjelmia näistä saaduista tiedoista. Anticheat-ohjelmat kuten muutkin tietoturvaohjelmistot vaativat jatkuvaa päivittämistä ja ovat jatkuvaa kilpajuoksua ohjelmien kehittäjien välillä. Wallhackit ovat edelleen myös suhteellisen helppo havaita, ja niiden piilottaminen varsinkin LAN-ympäristöissä on hyvin vaikeaa, sillä seinien läpi näkyvät hahmot erottuvat selvästi normaalista pelinäköymästä (kuva 8).



Kuva 8. Kuvankaappaus CS:GO-pelistä Wallhack-huijausohjelman ollessa käynnissä. Ohjelma näyttää sekä vastustavan (punaiset) että oman (siniset) joukkueen pelaajat kartalla, vaikka perinteisesti tätä tietoa ei pelaajalla ole saatavilla, jos suoraa näköyhteyttä vastustajaan ei ole.

Haastavampia tämän hetkisten pelien kannalta ovat FPS-peleissä käytettävät ns. triggerbotit, jotka parantavat pelaajan tarkkuutta ja reaktionopeutta. Triggerbot on yksinkertainen ohjelma joka, FPS-pelissä ampuu automaattisesti, kun pelaajan tähtäin liikkuu vastustavan pelaajan yli. Ammattilaispelaajat ovat luonnostaan erittäin nopeita ja tarkkoja, joten ylimääräisen edun huomaaminen voi joskus olla haastavaa.

Kuten wallhackkien tapauksessa, myös aimbotteja sekä triggerbotteja pyritään havaitsemaan anticheat-ohjelmilla. Koska triggerbot ei kuitenkaan vaadi minkäänlaista dataa, jota pelaajalla ei olisi jo saatavilla, on niiden havaitseminen ohjelmiston kannalta vaikeampaa. Vastausta onkin lähetty viime aikoina hakemaan laitteiston puolelta, ja yksi lupaava vaihtoehto on David Titarencon kehittämä Arduino-alustaan perustuva piiri. Kaksi USB-porttia sisältävä yksinkertainen piiri kytketään pelaajan tietokoneen ja hiiren väliin, ja laite kaappaa kaiken hiiren tekemän liikkeen ja painallukset. Tämän jälkeen kaapattua liikettä verrataan ruudulla tapahtuvaan liikkeeseen. Tätä kautta pystytään päättämään, käyttääkö pelaaja esimerkiksi triggerbottia. Alusta sisältää tämän lisäksi ethernet- ja wifi-yhteydet, ja laitteen on tarkoitus olla jatkuvasti yhteydessä palvelimeen, joka varmistaa, ettei laitteen ohjelmointia muuteta kesken sen käytön. [25.]

Titarencon kehittämä konsepti on teoriassa erittäin hyvä, mutta mahdolliseksi ongelmaksi voi muodostua hiiren ja tietokoneen välisen latenssin kasvu. Pelaamisessa ja varsinkin ammattimaisessa pelaamisessa on erittäin kriittistä, että hiiren liikkeestä tietokoneen rekisteröintiin ei ole huomattavaa eroa. Alusta on kuitenkin vielä kehitysasteella ja sen lopullinen potentiaali tulee selviämään vasta tuotteen valmistuessa. Ratkaisu ei myöskään vaikuta online-pelaamisessa esiintyviin ongelmiin, vaan ratkaisee ainoastaan LAN-ympäristöissä tapahtuvat huijaukset.

3.2.2 Pelaajakohtaisen datan hallinta

Toinen tapa hallita huijausyrityksiä LAN-ympäristöissä on hallita pelaajien pääsyä laitteistoon. Jos pelaajan pääsy sekä käyttöoikeudet pelikoneelle voidaan minimoida, pystytään riskejä hallitsemaan selvästi tehokkaammin. Yleisesti turnauksissa on käytössä päälava, jolla on pelistä riippuen kahdesta kymmeneen tietokonetta. Jokaisen pelin välissä seuraavaksi pelaava joukkue pääsee omille tietokoneilleen tekemään tarvitsemansa konfiguraatiot, jotta tietokone on omien tottumusten mukainen. Tämä antaa pelaajille mahdollisuuden asentaa samalla mahdollisia huijausohjelmia ja konfiguroida ne tarvittavalla tavalla.

Tätä riskiä voidaan hallita luomalla jokaisella pelaajalle henkilökohtainen kovalevy, ja vaatia jokaista pelaajaa toimittamaan tarvittavat konfiguraatiot sekä ajurit tiettyyn aikarajaan mennessä ennen turnauksen alkua. Nämä konfiguraatiot ja asennukset tehdään sitten pelaajalle valmiiksi kovalevylle kolmannen osapuolen toimesta, oletettavasti turnausjärjestäjien toimesta. Pelaajien saapuessa turnaukseen heille annetaan tietty aikamääre valvotussa ympäristössä, jossa he voivat tarkistaa konfiguraatioiden oikeudet ja esittää tarvittavat korjaustarpeet. Kaikki konfiguraatiomuutokset tässä vaiheessa tehdään myös kolmannen osapuolen toimesta tai tämän tarkassa valvonnassa.

Tämän jälkeen kovalevyt sijoitetaan valvottuun ympäristöön. Turnauksessa käytettäviin tietokoneisiin asennetaan esimerkiksi tietokoneen etupaneeliin hotswap-kovalevykehikko, jotta pelaajien kovalevyjä voidaan vaihtaa otteluiden välissä nopeasti ja tehokkaasti. Jos pelaajilla tulee turnauksen aikana laitteiston tai konfiguraatioiden kanssa ongelmia, tulee heidän joka tilanteessa pyytää turnausjärjestäjää tekemään kaikki tarvittavat muutokset.

Yleisesti turnauskoneet toimivat Windows-käyttöjärjestelmillä, koska suosituimmat pelit ovat parhaiten yhteensopivia tällä alustalla. Turnauksissa käytettävät käyttäjätunnukset tulisi konfiguroida siten, että pelaajien käyttämällä tunnuksilla on mahdollisimman rajattu pääsy ohjelmiin ja asetuksiin. Käytännössä ainoastaan puheohjelman ja käytettävän pelin suorittaminen tulisi olla sallittua. Tämä voidaan toteuttaa esimerkiksi Active Directory -pohjaisella konfiguraatiolla, jossa ryhmäjäsenyyksillä voidaan estää kaikkien muiden kuin valittujen ohjelmistojen suorittaminen käyttäjältä.

Turnauksen jälkeen pelaajien kovalevyt säilytetään vielä tietty aikamääre, jotta jos epäilyjä epärehellisistä toimista nousee, voidaan pelaajien henkilökohtaiset asetukset ja asennetut ohjelmat vielä tarkastaa.

Henkilökohtaiset kovalevyt sekä Active Directory -pohjaiset ratkaisut asettavat selvästi enemmän rasiusta turnausjärjestäjille ja lisäävät henkilökunnan tarvetta. Tämä osaltaan voi vaikuttaa turnauksen rahalliseen kannattavuuteen ja vaikeuttaa aikataulutusta. Vastaavanlaisia toteutuksia on jo käytössä joissain isoissa turnauksissa, mutta varsinkin pienemmät ja uudemmat turnausjärjestäjät ovat valittavan usein jättäneet datanhallintaan ja riskien minimointiin liittyvät seikat vähemmälle huomiolle.

Yhtenäiset ja tarkkaan sovitut tietoturvakäytännöt ja huijauksenestokäytännöt auttavat kilpapelaaamista vakiinnuttamaan itseään vakavasti otettavana lajina, ja huijaustapausten vähentyminen lisää luottamusta niin katsojien kuin sponsoreidenkin silmissä.

4 Yhteenveto

Elektroninen urheilu on vakiintuva kilpaurheilun ala, joka hakee paikkaansa niin katsojien kuin alan rahoittajienkin silmissä. Vaikka tietokone- ja konsolipelaaminen on ollut olemassa jo pitkään, on alalla liikkuvat rahamäärät ja katsojaluvut alkaneet kasvamaan vasta viimeisellä vuosikymmenellä räjähdysmäisesti.

Työssä tutkittiin elektronisen urheilun kasvua sen suhteellisen lyhyen historian aikana käyttäen mittareina katsojamääriä ja turnausten palkintorahoja. Niin katsojamäärät kuin rahamäärätkin ovat kasvaneet vuosien 2000 ja 2010 välillä tasaisesti, mutta vuodesta 2010 eteenpäin molemmat ovat alkaneet kasvaa huomattavasti nopeammalla tahdilla

moninkertaistuen vain parin vuoden välein. Katsojamäärien kasvun nopeutumista voidaan selittää internetin kautta toimivien streamaus-palveluiden kuten Twitch.tv:n suosion lisääntymisellä, joka on tuonut kilpaturnaukset suuremman yleisön saataville. Palkintorahojen kehitykseen on vaikuttanut huomattavasti muutos turnausten palkintorahojen lähteissä. Perinteisen sponsori- tai laitevalmistajarahoitteisen turnausformaatin sijasta alan rahakkaimmat turnaukset ovat nykyään valtaosaltaan yleisörahoitteisia. Yleisörahoitus on kuitenkin suhteellisen riskialtis ja vaihteleva rahoituksen muoto, ja tulevat vuodet tulevatkin näyttämään, pystyvätkö rahamäärät pysymään kasvussa.

Jotta kilpaurheilu kykenee vakiinnuttamaan paikkansa, tulee sen luoda vakaa ympäristö pelaamiselle, jotta sponsorit ja katsojat säilyttävät mielenkiintonsa. Tällä hetkellä alaa häiritsevät vaihtelevat katsojakokemukset, jotka johtuvat turnauksia ja yksittäisiä pelaajia vastaan suoritettavista palvelunestohyökkäyksistä. Palvelunestohyökkäyksiä voidaan estää tai mitigoida valitsemalla pelikoneella käytettävät ohjelmat huolella ja estämällä hyökkääjiä saamasta yksittäisen pelaajan IP-osoitetta haltuunsa. Useat yleisesti käytetyt puheohjelmat sekä pelaamiseen käytettävät ohjelmat ovat alttiita IP-osoitteen selvitykseen tehtäville hyökkäyksille, ja ammattipelaajien tuleekin tiedostaa nämä heikkoudet ja varmistaa, että käytettävät ohjelmat on konfiguroitu vaaditulla tavalla. Lisäksi pelaajien tulisi panostaa joko VPN-palveluun tai varalla olevaan internet-yhteyteen, esimerkiksi 4G-yhteyteen, jos tällainen on saatavilla.

LAN-tapahtumissa yksittäisen pelaajan tietokonetta vastaan on huomattavasti vaikeampi suorittaa palvelunestohyökkäystä, ja tämän takia turnausten tuleekin keskittyä verkkosuunnitteluun. Lisäksi pelinkehittäjien tulisi reagoida viimeaikaisiin tapauksiin, jossa palvelunestohyökkäyksiä on turnauspaikan sijasta suoritettu pelin verkkopalvelimia vastaan. Yksi tapa kiertää tämä ongelma on luoda peleistä lokaali versio, joka ei itse pelaamisen osalta vaadi yhteyttä turnauspaikan ulkopuoliseen verkkoon.

Toinen alaa häiritsevä tekijä on varsinkin Counter-Strike: Global Offensive -peliä ympäröivät huijaustapaukset. Yleisimmät huijausohjelmat parantavat pelaajan reaktioita tai antavat hänelle informaatiota pelikentältä, jota hänelle ei muuten olisi saatavilla. Näiden mitigointiin pyritään pääasiassa anticheat-ohjelmilla, joiden pysyminen ajan tasalla vaatii jatkuvaa panostamista. LAN-tapahtumissa

huijauksenestoa voidaan suorittaa hallitsemalla pelaajien fyysistä pääsyä tietokoneille, sekä suunnittelemalla laitteiden ja datan hallinta siten, että yksittäiselle pelaajalle ei tule mahdollisuuksia asentaa ja konfiguroida huijausohjelmia turnauksessa käytettäville tietokoneille.

Elektronisen urheilun nopea kasvu on tehnyt siitä varteenotettavan tekijän perinteisten urheilulajien rinnalla sekä katsojamäärissä että alalla liikkuvissa rahamäärissä. Vaikka käsite kilpapelaamisesta kuulostaa ehkä vielä oudolta, on videopelaamisesta tullut maailmanlaajuinen ilmiö eikä suosiolla näy loppua. Jos kasvu jatkuu vastaavalla tahdilla, on kilpapelaamisella potentiaalia nousta jopa suosituimman urheilulajin jalkapallon rinnalle.

Lähteet

- 1 Today is the 40th Anniversary of the world's first known video gaming tournament. 2012 Verkkodokumentti. Kotaku. <<http://kotaku.com/5953371/today-is-the-40th-anniversary-of-the-worlds-first-known-video-gaming-tournament>>. Luettu 4.9.2015.
- 2 Gaming like a Pro: An overview of the eSports scene. 2012 Verkkodokumentti. Digital Spy. <<http://www.digitalspy.co.uk/gaming/news/a363769/gaming-like-a-pro-an-overview-of-the-esports-scene.html>>. Luettu 4.9.2015.
- 3 History of eSports. 2015 Verkkodokumentti. Zengaming. <<http://blog.zengaming.co/article/history-of-esports/>>. Luettu 4.9.2015.
- 4 A History of Esports. 2012 Verkkodokumentti. Teamliquid. <<http://www.teamliquid.net/forum/starcraft-2/324077-a-history-of-esports>>. Luettu 7.9.2015.
- 5 About Fatal1ty. 2015 Verkkodokumentti. Fatal1ty Brand. <<http://fatal1ty.com/about-fatal1ty/>>. Luettu 7.9.2015.
- 6 Jonathan "Fatal1ty" Wendel. 2015 Verkkodokumentti. E-Sports Earnings. <<http://www.esportsearnings.com/players/1139-fatal1ty-johnathan-wendel>>. Luettu 7.9.2015.
- 7 For South Korea, E-Sports Is National Pastime. 2014 Verkkodokumentti. The New York Times. <http://www.nytimes.com/2014/10/20/technology/league-of-legends-south-korea-epicenter-esports.html?_r=1>. Luettu 7.9.2015.
- 8 The Surprising Esports Culture of Korea. 2010 Verkkodokumentti. LoL Esports. <<http://euw.lolesports.com/articles/surprising-esports-culture-korea>>. Luettu 9.9.2015.
- 9 Field of streams: how Twitch made video games a spectator sport. 2013 Verkkodokumentti. The Verge. <<http://www.theverge.com/2013/9/30/4719766/twitch-raises-20-million-esports-market-booming>>. Luettu 16.9.2015.
- 10 E-Sports Earnings, History. 2015 Verkkodokumentti. E-Sports Earnings. <http://www.esportsearnings.com/history/2015/list_events>. Luettu 10.9.2015.
- 11 Fifa World Cup. 2015 Verkkodokumentti. FIFA. <<http://www.fifa.com/aboutfifa/worldcup/>>. Luettu 15.9.2015.

- 12 The International Dota 2 tournament. 2015 Verkkodokumentti. Valve Corporation. <<http://www.dota2.com/international/compendium/>>. Luettu 1.9.2015.
- 13 DDOS attack temporarily shuts down International 'Dota 2' tournament. 2015 Verkkodokumentti. Forbes. <<http://www.forbes.com/sites/davidthier/2015/08/04/ddos-attack-temporarily-shuts-down-international-dota-2-tournament/>>. Luettu 1.9.2015.
- 14 Number of TV viewers of major sporting events in United States as of June 2014. 2014 Verkkodokumentti. Statista. <<http://www.statista.com/statistics/311949/number-tv-viewers-sporting-events-usa/>>. Luettu 25.9.2015.
- 15 Valve News. 2015 Verkkodokumentti. Valve Corporation. <<http://www.valvesoftware.com/news/?id=17568/>>. Luettu 25.9.2015.
- 16 League of Legends 2014 World Championship viewer numbers. 2014 Verkkodokumentti. onGamers. <<http://www.ongamers.com/articles/league-of-legends-2014-world-championship-viewer-n/1100-2365/>>. Luettu 25.9.2015.
- 17 Worldwide reach of the Lisbon Final. 2014 Verkkodokumentti. Uefa.com. <<http://www.uefa.com/uefachampionsleague/news/newsid=2111684.html>>. Luettu 25.9.2015.
- 18 The ten richest sporting events in the world. 2012 Verkkodokumentti. Forbes.com. <<http://www.forbes.com/sites/monteburke/2012/05/24/the-ten-richest-sporting-events-in-the-world/>>. Luettu 25.9.2015.
- 19 DDoS: A Brief History. 2013 Verkkodokumentti. Fortinet. <<https://blog.fortinet.com/post/ddos-a-brief-history>>. Luettu 25.9.2015.
- 20 eSports has a DDoS problem. 2015 Verkkodokumentti. Vice Media LLC. <<http://motherboard.vice.com/read/esports-has-a-ddos-problem>>. Luettu 25.9.2015.
- 21 The Esports economy will generate at least \$465 million in 2017. 2015 Verkkodokumentti. Newzoo BV. <<http://www.newzoo.com/insights/esports-economy-will-generate-least-465-million-2017/>>. Luettu 25.9.2015.
- 22 VyprVPN. 2015 Verkkodokumentti. Golfen Frog, GmbH. <<https://www.goldenfrog.com/vyprvpn/gaming-vpn>>. Luettu 30.9.2015.
- 23 OptaNet deliver core network at the world's largest eSports tournament. 2015 Verkkodokumentti. OptaNet Ltd. <<http://www.optanet.com/optanet-deliver-core-network-at-the-worlds-largest-esports-tournament/>>. Luettu 14.10.2015.

- 24 CS:GO eSports community shaken following revelation of cheating. 2014 Verkkodokumentti. IGN US. <<http://www.ign.com/articles/2014/11/25/csgo-esports-community-shaken-following-revelation-of-cheating>>. Luettu 19.10.2015.
- 25 Can this little device fix cheating in eSports?. 2015 Verkkodokumentti. Vice Media LLC. <<http://motherboard.vice.com/read/can-this-little-device-fix-cheating-in-esports>>. Luettu 22.10.2015.