CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Napadi na servise za mrežno igranje

NCERT-PUBDOC-2011-05-326

Nacionalni CERT

Nacionalni CERT

Sadržaj

1 UVOD 2

2 SERVISI ZA MREŽNO IGRANJE 3

2.1 STEAM 3
2.2 BATTLE.NET 4
2.3 OSTALI SERVISI 6

3 VRSTE NAPADA 8

3.1 PHISHING 8
3.1.1 Primjeri phishing poruka 8
3.2 KEYLOGGERI I TROJANSKI KONJI 12

4 SAVJETI ZA ZAŠTITU 14

5 ZAKLJUČAK 16

6 LITERATURA 17

1 Uvod

Računalne igre, kao glavna zabava na računalima, uz nas su od samih početaka razvoja informatike, a upravo je svjetska industrija igara ta koja je godinama nametala sve brži i brži razvoj hardvera koji može pratiti zahtjeve sve složenijih igara. Prve igre mogli su igrati samo igrači na lokalnom računalu, ali ubrzo razvojem komunikacijskih mreža, nastaju i mrežne (multiplayer) igre u kojima istodobno sudjeluje više igrača sa svojih udaljenih računala.

Paralelno s razvojem Interneta i njegovih servisa, izdavači računalnih igara prepoznali su novo tržište za plasman svojih proizvoda. Naime, počeli su distribuirati igre putem web stranica koje su registriranim korisnicima dopuštali preuzimanje igara, dok su se aktivacijski ključevi (tzv. cd keyevi) koji su bili potrebni za pokretanja igara (ili obično samo mrežnog dijela) naplaćivali. Time su proizvođačima, odnosno distributerima smanjeni troškovi jer više nisu morali proizvoditi medije i ambalažu za pohranu igara pa su igre mogli ponuditi po znatno manjim cijenama. Nakon prvih web stranica, koje su po prirodi zapravo bile obične web trgovine, razvile su se platforme za digitalnu distribuciju igara. One korisnicima nude mnogo više mogućnosti od spomenutih klasičnih web stranica za prodaju. Te mogućnosti uključuju: automatsko preuzimanje nadogradnji za igre, društvenu interakciju, spremanje korisničkih postavki i dr.

Spomenuti sustavi za digitalnu distribuciju računalnih igara (putem Interneta), od kojih je najpopularniji Steam, posljednjih nekoliko godina su privukli desetke milijuna korisnika. Osim što predstavljaju servise za kupnju igara, u koraku s trendom su postali i društvene mreže koje okupljaju milijune igrača („gamera“) diljem svijeta. Svojim korisnicima nude povezivanje putem zajedničkih igara, prijateljstava i grupa baš kao i na klasičnim društvenim mrežama. Obično svoju publiku nalaze u ljudima koji se vole natjecati i nude im rangiranje po različitih ljestvicama, ligama itd. Nažalost, skupa s velikim mogućnostima i brojem korisnika, dolaze i sigurnosni rizici koji su vrlo slični onima na društvenim mrežama. Zlonamjerni korisnici, odnosno napadači pokušavaju doći do financijske koristi obično krađom korisničkih računa od spomenutih servisa za mrežno igranje. Ti korisnički računi mogu imati popriličnu novčanu vrijednost, posebno kada se uzme u obzir da na njih mogu biti vezani deseci različitih igara. Napadače privlači i činjenica da ukradene korisničke račune mogu vrlo jednostavno prodati putem web oglasa, odnosno bez ikakve potrebe za izlaganjem svojeg identiteta.

2 Servisi za mrežno igranje

2.1 Steam

Steam tvrtke Valve Corporation[1] najpopularniji je servis za mrežno igranje koji uključuje distribuciju igara te platformu za povezivanje i komunikaciju između korisnika (nazvan *Steam Community*, a predstavljen 2007.). U listopadu 2010. objavljeno je [1] kako ima više od 30 milijuna aktivnih korisnika kojima nudi ukupno 1200 računalnih igara različitih žanrova. Procjenjuje se da Steam drži oko 80% tržišta digitalne distribucije igara [2]. U ponudi su igre velikih proizvođača kao što su Electronic Arts, Activision i Ubisoft, ali i onih malih nezavisnih. Popularnosti Steama uvelike su pridonijele stalne vikend-akcije, odnosno velika sniženja izabranih igara tijekom vikenda. Cijene su istaknute u američkim dolarima za SAD-e, a za ostatak svijeta u eurima. Dio prihoda, Steam ostvaruje i kroz oglase, odnosno tzv. bannere unutar grafičkog sučelja, pa čak i u samim igrama (nalijepljene teksture na zidove i sl.). Također, Steam je lokaliziran na 21 jeziku.

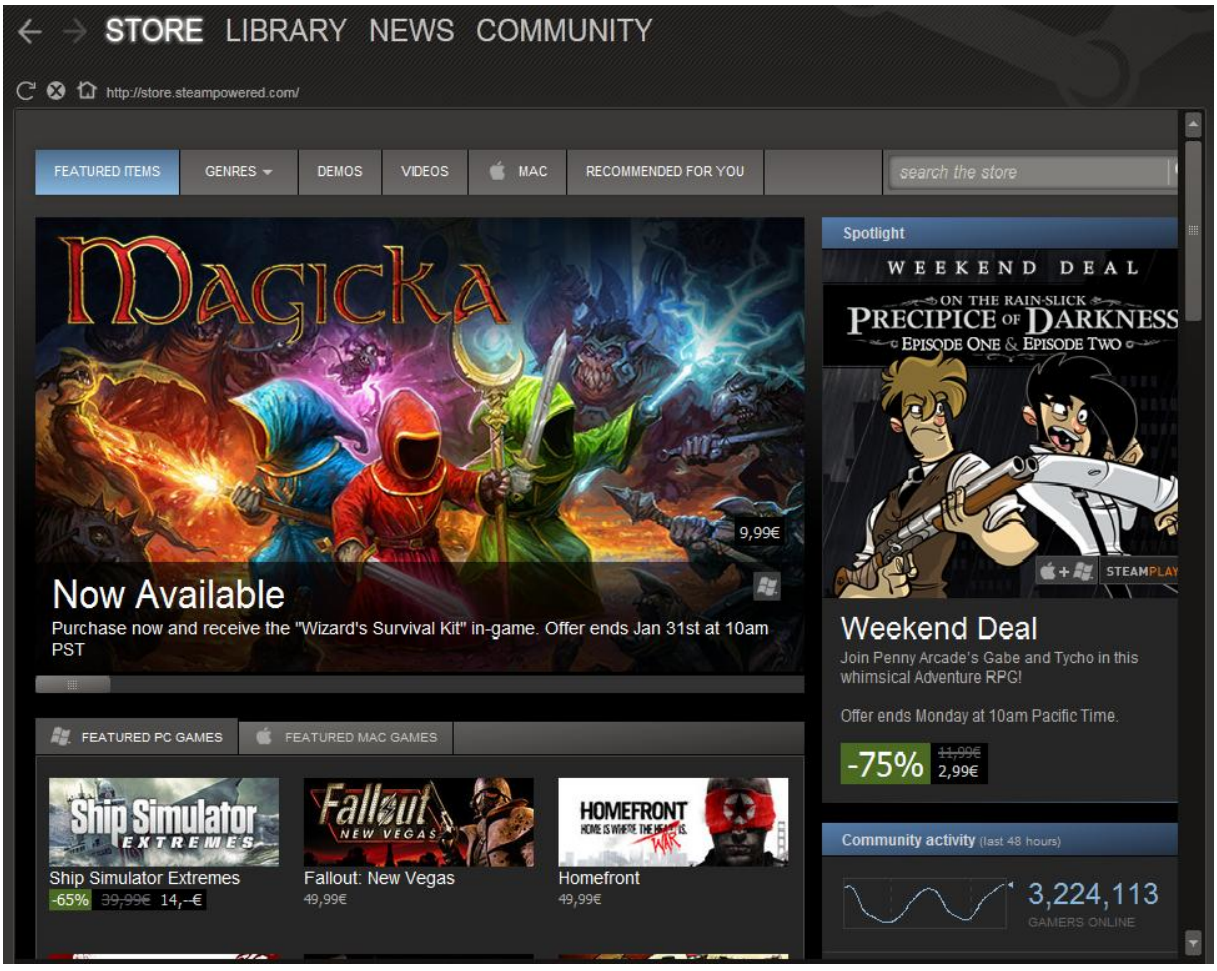
2.1: logotip Steama

Korisnici Steama mogu formirati prijateljstva (kao i na društvenim mrežama poput Facebooka), učlanjivati se u grupe, imati uvid u kojim igrama sudjeluju i koliko vremena u njima provode njihovi prijatelji, međusobno razmjenjivati poruke (chat) ili glasovno komunicirati. Svaki korisnik može urediti svoj profil i na njega dodati svoj avatar (sliku profila) te ostale informacije kao što su nacionalnost, mjesto prebivališta itd. Može i odrediti je li mu profil javan ili mu smiju pristupiti samo prijatelji. Na slici 2.2. prikazano je sučelje Steama.
Osim prijatelja, korisnici na svoj korisnički račun dodaju igre koje kupuju. Na svaki račun može biti vezano vlasništvo nad više igara. Sustav automatski nadograđuje sve igre (instalacijom tzv. patcheva). Korisnik tako može svojim igrama pristupiti sa bilo kojeg računala na kojem je instaliran Steam klijent, a kako bi igrao dovoljno mu je preuzeti igru putem sustava i potom je instalirati na računalo na kojem se trenutno nalazi. Postoji i ugrađena programska zaštita od varanja u igrama, tzv. *Valve Anti-Cheat* (VAC), koji se redovito nadograđuje skupa s platformom i samim igrama.

[1] Valve je tvrtka koja je 1998. stajala iza igre Half-Life, jedne od najpopularnije računalne igre u povijesti. Krajem 2003. Valve je predstavio Steam zajedno s novom inačicom Half-Lifea, što se pokazao kao odličan potez za tvrtku.

2.2 Battle.net

Battle.net je servis za mrežno igranje tvrtke Blizzard Entertainment, koja stoji iza naslova kao što su Warcraft, Starcraft i World of Warcraft. Servis je predstavljen još davne 1997. godine uz igru Diablo i bio je jedan od prvih servisa te namjene koji je bio integriran unutar neke računalne igre. Jednostavno sučelje i nepostojanje članarine, uz naravno ogromnu popularnost samih Blizzardovih igara, bili su glavni razlozi zašto je servis brzo postao vrlo popularan. Do studenog 1997., servis je već okupio 1,25 milijuna korisnika [3], a do kraja 2002. ta brojka je iznosila već 12 milijuna. Blizzard je 2009. predstavio novu inačicu Battle.net servisa, dok je stariju preimenovao u „*Battle.net classic*".



Slika 2.2: sučelje Steama

Novi servis odmah je povezan i sa igrom World of Warcraft (WoW), što ranije nije bio slučaj. WoW uvodi igrače u svijet fantazije u kojem upravljaju svojim likom ili više njih. Navedena igra donosi Blizzardu najveću zaradu zbog činjenice da igrači plaćaju mjesečnu pretplatu kako bi igrali, ali plaćaju i za virtualne predmete, magije, vještine i zlato unutar same igre. Kako lik kojeg igrač vodi, napreduje, raste i njegova razina („level"), a za to su potrebni sati i sati igranja, ali i prilična svota novca. Battle.net računi sa WoW likovima na oglasima se prodaju po cijenama od čak nekoliko tisuća kuna. Ta vrijednost naravno privlači zlouporabu, odnosno napadače (prevarante) koji u neprekidnom lovu na financijsku korist, kradu korisničke račune te ih prodaju putem web oglasa.

2.3: sučelje servisa Battle.net classic

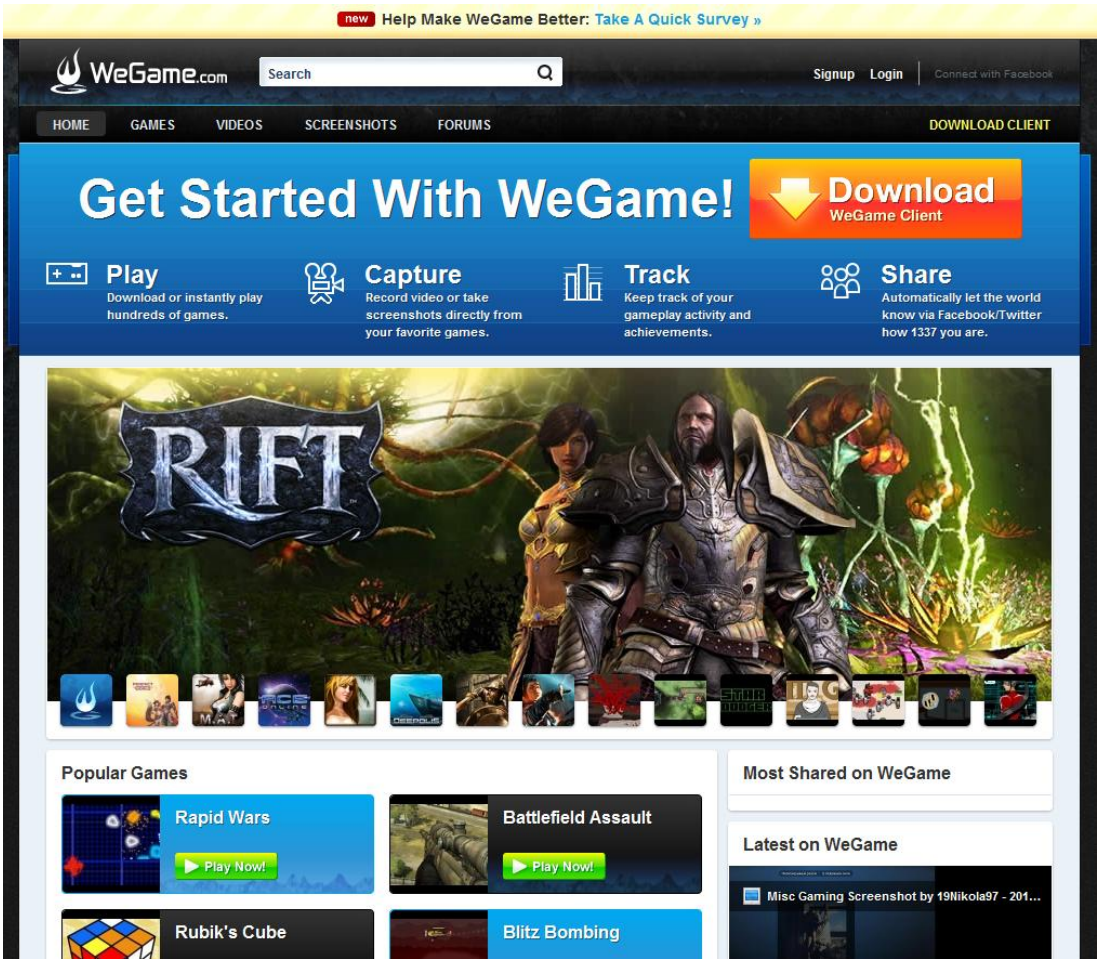
Novi Battle.net sastoji se od tri dijela. Prvi korisnicima omogućuje povezivanje više računa, WoW likova i prijatelja u jedan jedinstveni račun. Drugi je zadužen za natjecanje, odnosno omogućuje jednostavno organiziranje mečeva, ljestvica i liga između igrača sa sličnim vještinama. Treći dio služi za komuniciranje s prijateljima, a to uključuje direktnu razmjenu poruka (chat) između igrača koji igraju istu igru, koriste isti poslužitelj ili pak istu vrstu likova. Taj dio također uključuje i online tržnicu koja služi za kupnju i prodaju mapa za igru.

2.4: sučelje za "chat" na novom Battle.net-u

Početkom 2010., je procijenjeno [4] da WoW okuplja 11 i pol milijuna igrača diljem svijeta koji za pretplatu godišnje izdvajaju preko 2 milijarde američkih dolara. U 2009. u Hrvatskoj je bilo oko 12 tisuća aktivnih igrača [5].

2.3 Ostali servisi

Good Old Games (www.gog.com) nudi kupnju igara uz pristupačne cijene. Jednom kada se igra kupi, može se neograničen puta preuzeti i instalirati.
WeGame (www.wegame.com) je servis vrlo sličan Steamu sa također milijunskim brojem igrača. Korisnici preuzimaju WeGame softverski klijent i putem njega instaliraju igre i imaju ostale funkcionalnosti. Servis nudi i integraciju sa društvenim mrežama kao što su Facebook i Twitter.



2.5: web stranica servisa WeGame

ImpulseDriven (http://www.impulsedriven.com/) još je jedan servis sličan Steamu, odnosno WeGameu.
Servis **OnLive** koristi novu paradigmu u mrežnom igranju, tzv. *cloud-gaming*, odnosno igranje „u oblaku“. To znači da servis svojim korisnicima omogućuje pokretanje igara putem web preglednika uz korištenje poslužitelja servisa, odnosno resursa. Time nije važno kakve hardverske karakteristike ima korisnikovo računalo, nego je dovoljno da on ima broadband pristup prema Internetu. Kao platforma za igranje podržani su i pametni telefoni. Potencijalni korisnici također mogu određeni kratki vremenski rok (obično 30

minuta) besplatno isprobati neku igru. Servis radi na principu plaćanja mjesečna pretplate koja iznosi 10 američkih dolara [6].

2.6: sučelje servisa OnLine

3 Vrste napada

Za sve napade karakteristična je upotreba socijalnog inženjeringa. Na taj način se od korisnika pokušavaju iznuditi korisnički podaci (phishing) ili ga se navodi na instalaciju malvera. To je nešto sofisticiraniji oblik prevare koji uključuje instalaciju trojanskog konja ili keyloggera koji onda tehnički način pokušavaju doći do istih podataka.

3.1 Phishing

Phishing je vrsta napada u kojoj napadač putem socijalnog inženjeringa i obično krivotvorene web stranice navodi potencijalnu žrtvu na izlaganje svojih povjerljivih podataka (obično korisničkih imena i lozinki). Krivotvorena web stranica u potpunosti ili gotovo u potpunosti imitira izgled legitimnog web servisa. U ovom slučaju to mogu biti Steam, Battle.net i drugi.

3.1: primjeri phishing (krivotvorenih) web stranica

3.1.1 Primjeri phishing poruka

U ovom dijelu, navest ćemo nekoliko primjera phishing poruka i analizirati način na koji napadači (prevaranti) nastoje prevariti žrtvu kako bi im ustupila svoje povjerljive podatke. Takve poruke su obični e-mail poruke ili poruke upućene putem chata koje žrtve navode na posjećivanje krivotvorenih web stranica kojima upravljaju napadači.

Primjer 1 - Steam phishing e-mail:

Hi there, this is Greg Coomer.
I'm the head of communications at Valve.
http://www.valvesoftware.com/people.html
We have recently been detecting more than 1 user IP connecting to your Steam account,

which is illegal.
This means that we are going to block all IP's from connecting to your Steam account.
We can however, if requested by the owner, allow his or her IP only to connect to the account.
If you are the owner of the account, and would like to be able to continue connecting to it, reply to this e-mail with the following information, in the following format:

Name:
Steam Account Name:
Steam Password:
E-Mail address:

NOTE: Ensure that the e-mail address you enter, is the e-mail address which you have registered your Steam account with.

Details will be automatically checked with our database, If the information that you've entered is correct, you are the proven owner of the account and your IP address will be allowed to connect.

If no reply is recieved, all IP connections to your account will be blocked as of Monday 9th April 2010.

Kao što vidimo, napadač se lažno predstavlja kao zaposlenik Valvea (voditelj odjela za komunikaciju) i lažno obavještava korisnika kako je više različitih IP adresa koristilo njegov korisnički račun, što je ilegalno. Korisnik se upozorava kako će sve IP adrese biti blokirane, osim one njegove ako odgovori na e-mail tako da pošalje svoje podatke - korisničko ime, lozinku te e-mail adresu kojom je registriran na Steam. Ako te ne učini do određenog roka, Steam račun će mu bit blokiran. Ovo je klasični primjer socijalnog inženjeringa u kojem napadač na vrlo jednostavan način navodi potencijalnu žrtvu da mu direktno, putem e-maila, u ruke preda svoj Steam račun. Važan je i način manipulacije u kojem napadač korisniku zadaje određen rok i računa da će to kod njega pobuditi strah od gubitka računa.

Primjer 2 - World of Warcraft (WoW) phishing e-mail:

From: "WoWAccountAdmin" <WoWAccountReview@blizzardadmins.net>

Greetings,

It has come to our attention that you are trying to sell or trade your personal World of Warcraft account. As you may or may not be aware of, these actions conflict with the EULA and Terms of Service (TOS) of Blizzard Entertainment and World of Warcraft. If upon further investigation you are indeed attempting to obtain monetary profit against the TOS agreement, your account can and will be disabled. Blizzard has the right to consider legal action if necessary, based on the severity of the action.

If you hope to avoid account suspension you should verify your personal possession of the account in question. We at Blizzard Entertainment take infractions of the TOS quite seriously and we must confirm the original ownership of the account. This is easily done by supplying your account information below.

Please use the following template below to verify your account and information via email.

- Account Email:
- Account Password:

If you ignore this communication your account can and will be closed permanently due to suspicions of alternative ownership. We ask that during the investigation you give approximately twenty-four hours of inactivity after sending a response email. This should provide enough time for Blizzard to confirm your identity and that the TOS are being followed as outlined.

Blizzard Entertainment Inc
Account Administration Team
P.O. Box 18979, Irvine, CA 92623

Regards,
Krondel
Account Recovery Team
Blizzard Entertainment Inc.

U ovoj poruci, korisnik je lažno optužen za pokušaj prodaje svojeg WoW računa što se navodno protivi Blizzardovim pravilima korištenja servisa te se zbog toga navedeni račun mora verificirati, odnosno utvrditi mu pravom korisnika. Naravno, dalje u poruci, napadač traži od korisnika da potvrdi svoje vlasništvo nad računom slanjem svoje e-mail adrese vezane uz račun i pripadajuće lozinke. Ukoliko to ne učini, račun će mu biti blokiran. Vrlo sličan primjer phishinga kao i prethodni.

Primjer 3 - World of Warcraft (WoW) phishing e-mail 2:

Greetings,

An investigation of your World of Warcraft account has found strong evidence that you are eligible for an account upgrade. You are eligible for the Wrath of the Lich King Beta. To sign-up and get your download please visit our website at this special link: http://worldofwarcraft.com/login This process usually last's one week. Thank you for your time and attention to this matter, and your continued interest in World of Warcraft.

Sincerely,

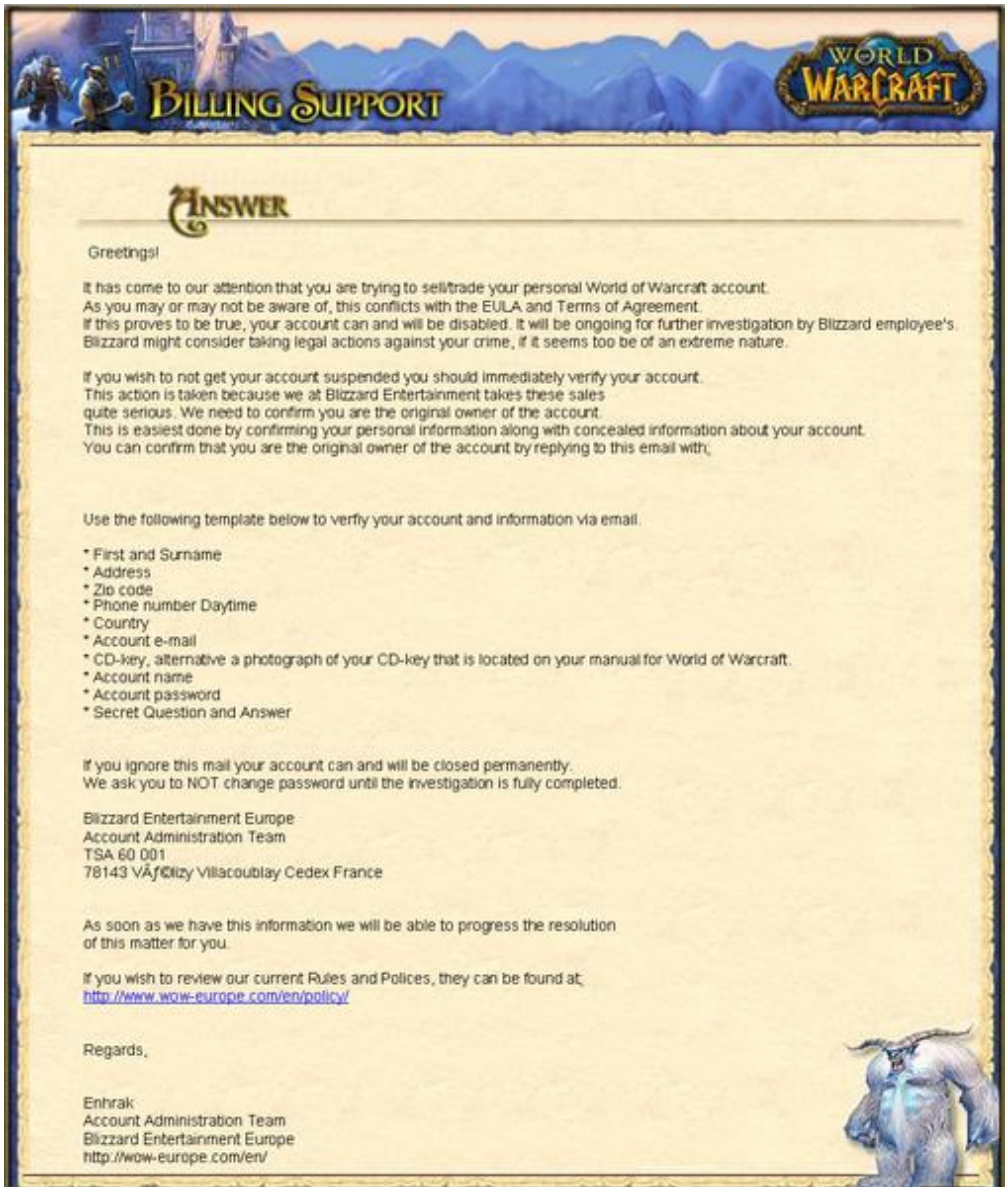
Account Administration
Blizzard Entertainment

Ovdje se korisnika se pokušava navesti na posjećivanje zlonamjernog URL-a i to tako što mu se nudi besplatna nadogradnja igre. Link vodi na drugačiji URL nego onaj što je naveden u tekstu.
Važno je još napomenuti da e-mail poruke obično dolaze uređene (HTML formatirane) u stilu korisnikovog servisa. Slika 3.2 prikazuje grafički izgled poruka.
Također, neke od otkrivenih domena koje su koristile phishing stranice su:

- steamcommuntity.com
- h1.ripway.com/steamedcommunity

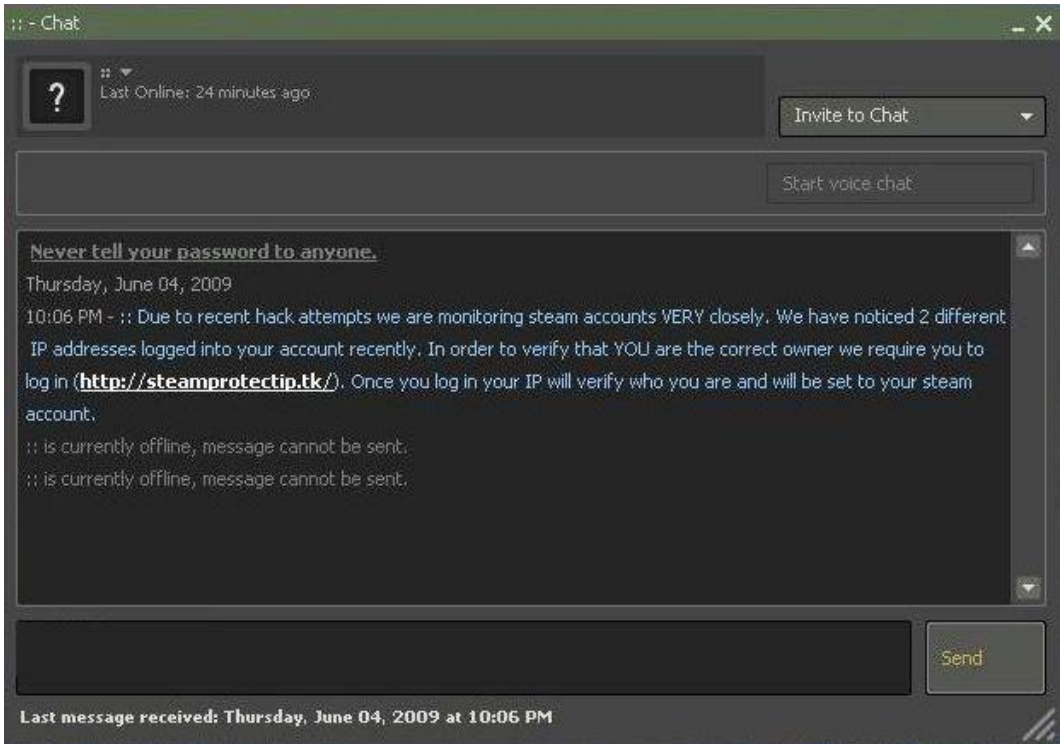
- blizzard-forums.com
- worldofnwarcraft.com
- wor1dofwrcraft.com
- wowaccount-surveyus.com
- restoreaccount.us

Vidimo da napadači uvijek pokušavaju da njihove domene budu što sličnije originalnim tako da se one znaju razlikovati u samo jednom jedinom slovu. Postoji i opasnost od **XSS napada**, odnosno korištenja ranjivosti legitimne web stranice koja u tom slučaju žrtvu preusmjerava na maliciozno web sjedište. Takav slučaj [7] je otkriven krajem 2009. kada se pod udarom našao Steam i njegova poddomena cafe.steampowered.com čija je ranjivost iskorištena za ubacivanje malicioznog HTML *iframe* elementa. Prilikom posjeta navedenog URL-a, originalna Steamova web stranica bi korisnika preusmjerila na potpuno identičnu krivotvorenu web stranicu.



3.2: izgled phishing e-mail poruke

Primjer 4 - Steam phishing putem Friends poruke:



3.3: phishing poruka na Steamu

Za izvođenje ovakvog napada, napadači koriste prethodno kompromitirane korisničke račune, koje su prikupili na isti ili sličan način. Naime, listi prijatelja sa ukradenog računa šalju se poruke koje navode potencijalne žrtve na posjećivanje malicioznih URL-ova. Na tim URL-ovima su ili phishing stranice (krivotvorine koje imitiraju izgled legitimnog servisa) ili one pak vode na malver zadužen za krađu korisničkih računa i daljnje širenje poruka.

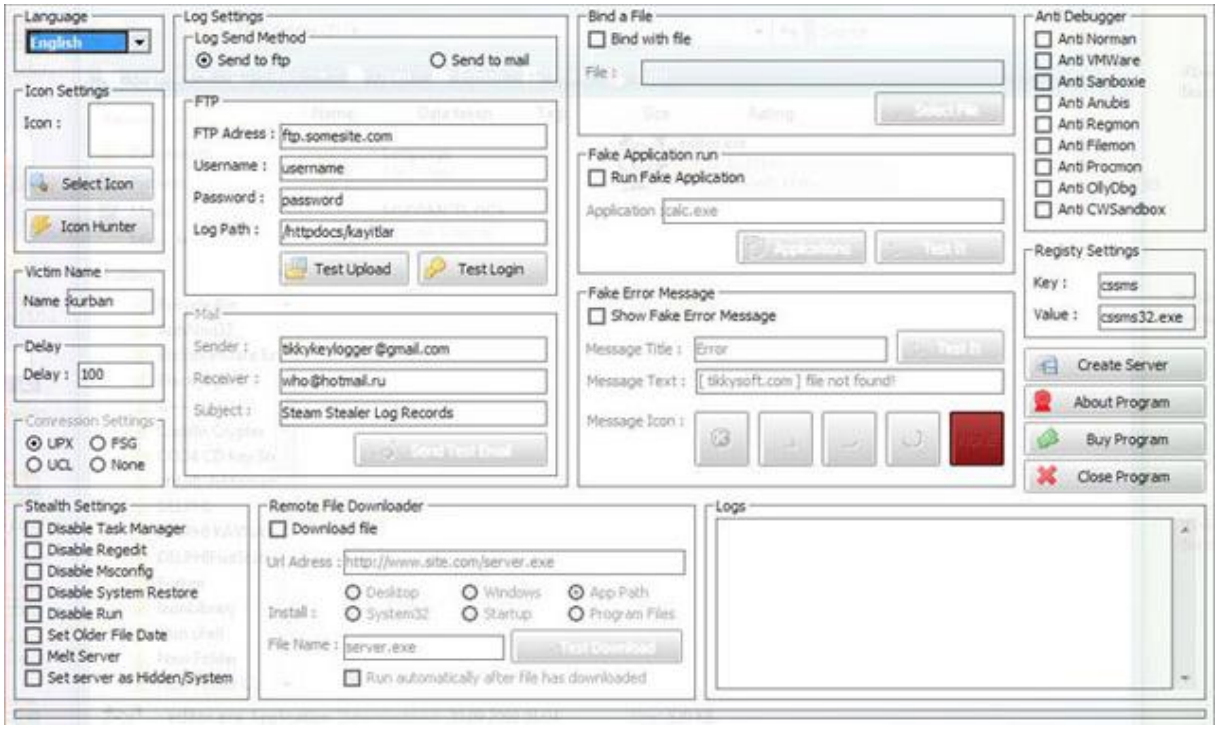
3.2 Keyloggeri i trojanski konji

Osim krađe korisničkih podataka isključivo putem socijalnog inženjeringa, odnosno prevare, napadači u tu svrhu koriste i malver kao što su keyloggeri i trojanski konji.
Keylogger je softver namijenjen tajnom praćenju i snimanju pritisnutih tipki na računalu. U ovom slučaju, napadači koriste specijalizirane keyloggere zadužene za krađu specifičnih podataka, kao što su korisničko ime (e-mail adresa) i lozinka za pristup Steamu ili nekom drugom servisu slične namjene.
Ovakav malver se obično širi putem spam poruka na servisima za igranje, poslanih sa kompromitiranih računa od prijatelja, odnosno računala zaraženim nekim oblikom spomenutog malvera.
Trojanski konj je oblik malvera koji se korisniku lažno predstavlja kao neki korisni softver kako bi ga korisnik izvršio, odnosno dozvolio mu instalaciju. Takav malver može omogućiti napadaču potpunu kontrolu nad zaraženim računalom. Time napadač, u ovom slučaju, može:

- koristiti zaraženo računalo kao dio svoje „botnet“ mreže za daljnje širenje spam poruka, odnosno malvera

- ukrasti povjerljive informacije (trojanski konj može u sebi zadržavati i drugi malver poput keyloggera)
- koristiti resurse zaraženog računala za svoje zlonamjerne radnje

Oblik u kojem se trojanski konji pojavljuju povezan je sa njihovom namjenom. Na primjer, u slučaju servisa Steam, malver može bit lažno predstavljen kao nadogradnja platforme koja omogućuje besplatne igre onome koji je instalira [7], dok u slučaju igre World of Warcraft malver može biti predstavljen kao dodatak koji igraču daje besplatno zlato u igri. Socijalni inženjering napadačima je potreban i u ovakvim slučajevima. Druga metoda može biti zastrašivanje korisnika kako bi ga naveli na instalaciju malvera. Takva vrsta malvera naziva se „***scareware***".



3.4: sučelje programa za izradu keyloggera

Posebno je zabrinjavajuća činjenica da kriminalne grupe izrađuju besplatni softver koji običnim zlonamjernim korisnicima omogućuje izradu malvera kao što su različiti keyloggeri. Takvi programi se distribuiraju po različitim („*underground*") forumima na Internetu te često i sami sadrže trojanskog konja. Time zlonamjerni korisnici istovremeno postaju i napadači i žrtve. Grafičko sučelje jednog takvog programa za izradu keyloggera, prikazano je na slici 3.3.
Glavni način širenje malvera su spam poruke koje se šalju putem samog servisa za mrežno igranje ili elektroničkom poštom te sadrže maliciozne URL-ove. Korisnik koji se tako zarazi obično toga i nije svjestan što je i cilj napadača.

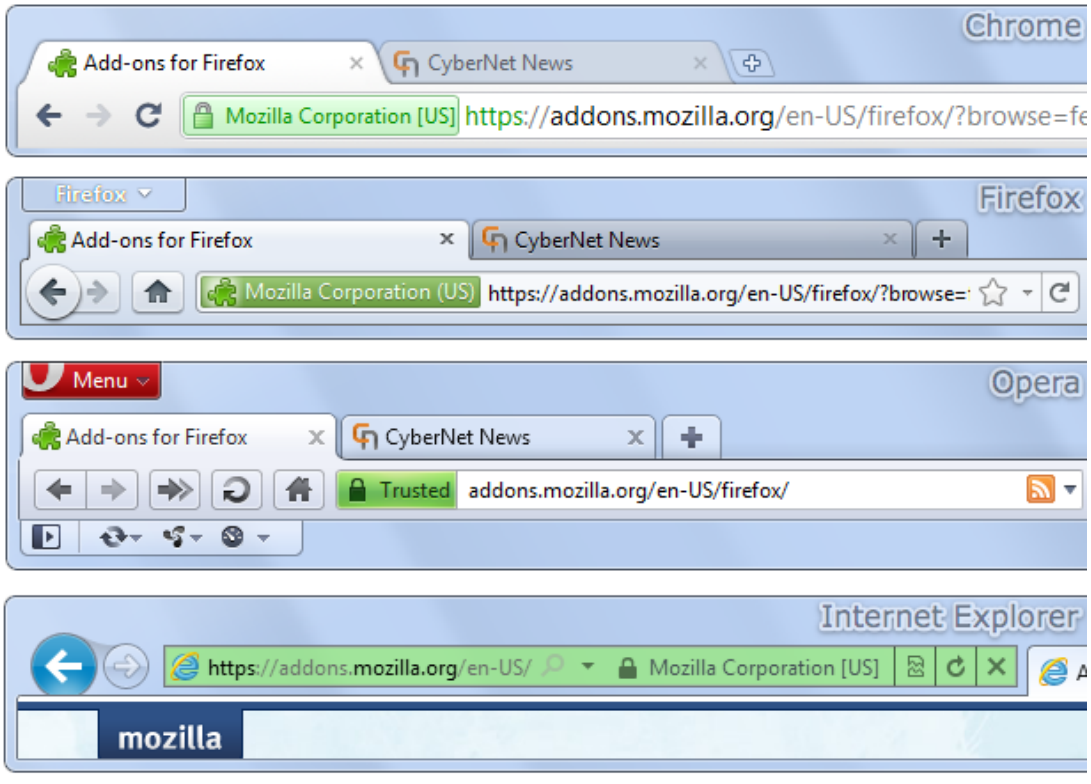
4 Savjeti za zaštitu

U ovom poglavlju, dajemo praktične savjete kako se zaštiti, odnosno prepoznati potencijalnu zlouporabu. Savjeti su podijeljeni prema „mjestu“ napada. Također preporučujemo uvid u službene web stranice samih servisa za mrežno igranje posvećene istoj temi.

Web stranice

Prilikom posjete web stranicama (prvenstveno onim namijenjenim za prijavu na sustav) potrebno je pripaziti na sljedeće:

- **ime domene** - phishing stranice imitiraju ime domene, lažne domene imaju obično grešku u jednom slovu ili sl.
- **certifikat i protokol HTTPS** - treba obratiti pozornost je li web stranica namijenjena autentikaciji koristi protokol HTTPS („**https:“** na početku URL-a), odnosno vjerodostojan certifikat tvrtke koja stoji iza servisa. Takav URL je unutar web preglednika obično posebno označen sa lokotom, zelenom bojom ili sl. Poznatiji servisi koriste HTTPS i ovo je vrlo dobar način razlikovanja legitimnog od lažnog web sjedišta. Slika 4.1. prikazuje kako web preglednici prezentiraju adresu prilikom posjeta web stranici koja koristi protokol HTTPS, odnosno SSL certifikat.



4.1: izgled adresne trake u popularnim web preglednicima prilikom pristupa HTTPS stranicama [8]

- unošenje **bilo kakve** kombinacije korisničkog imena i lozinke nas svejedno prebacuje na sljedeću stranicu - ovo je očiti znak da je riječ o phishing stranici

Elektronička pošta

- legitimni servis nikad neće tražiti vašu **lozinku** putem elektroničke pošte i stoga je najsigurnije zanemariti poruke u kojima se to od vas traži
- phishing poruke obično su loše gramatički napisane
- ako ipak niste sigurno u identitet pošiljatelja, uvijek možete (putem elektroničke pošte) kontaktirati servis koji koristite
- ne pokrećite izvršne datoteke (EXE) i ne otvarajte dokumente (PDF, DOC i dr.) iz privitaka e-mail poruka koje **ne očekujete**

Maliciozne poruke na servisima

- ne prihvaćajte zahtjeve za prijateljstva od nepoznatih ljudi
- ne slijedite sumnjive URL-ove koje vam šalju prijatelji jer je lako moguće da je njihov račun kompromitiran i širi maliciozne URL-ove listi prijatelja

Upravljanje lozinkama

- koristiti jaku lozinku, odnosno lozinku koja se sastoji od minimalno **8 znakova** i koja sadrži kombinaciju **malih i velikih slova, znakova i brojeva**. Izbjegavajte jednostavnu izmjenu riječi iz rječnika brojevima „4“ umjesto „A“, „0“ umjesto „O“ i sl.
- ne koristite istu lozinku na servisima i na različitim forumima za igrače i sl.
- ne dijelite račun s drugim igračima pa čak i ako ih poznate jer je moguće da se oni neće pridržavati svih sigurnosnih mjera

Dodaci za igre iz neprovjerenih izvora

Izbjegavajte nadogradnje i dodatke za igre koje stižu iz neprovjerenih izvora jer je obično riječ o malveru zaduženom za krađu vaših računa.

Redovite softverske nadogradnje

Vršite redovite nadogradnje vašeg antivirusnog softvera, vatrozida, web preglednika i čitača dokumenata. To su najvažnije kategorije alata koji su vam potrebne za veću sigurnost ili su nužni za rad na računalu. Također je poželjno redovito skenirati tvrdi disk koristeći antivirusni ili sličan alat.

5 Zaključak

Razvojem globalne mreže, razvijaju se i njezini servisi koji uključuju i one namijenjene zabavi. Ovaj dokument se fokusirao na one servise koji uključuju instalaciju, odnosno pristup klasičnim računalnim igrama. Takvi servisi imaju na desetke milijuna korisnika, a većinom je riječ o mlađoj populaciji, koja se nužno mora informirati o opasnostima koje im prijete. U tome je vrlo važna i uloga roditelja. Zlouporabe, odnosno napadi na servise za mrežno igranje ne razlikuju se od napada na druge servise. Uz to, napadi postaju sve sofisticiraniji, a u tome im pomaže sve veća društvena interakcija između korisnika. Kao i kod drugih aspekata korištenja Interneta, pokazalo se da veći broj korisnika automatski povlači i veću zlouporabu te je glavni način njene prevencije edukacija i pravodobno informiranje.

6 Literatura

1. http://store.steampowered.com/news/4502/, službena stranica Steama, 18.10.2010.
2. Steam ubija PC tržište, http://www.bug.hr/master/vijesti/steam-ubija-pc-trziste/104847.aspx, 11.11.2010.
3. Battle.net Defines Its Success: Interview With Paul Sams, http://www.gamasutra.com/view/feature/3240/battlenet_defines_its_success_.php, studeni 1997.
4. World of Warcraft statistic in 2010, http://www.mmorpgrealm.com/world-of-warcraft-statistic-in-2010/ , 25.2.2010.
5. http://www.slobodnadalmacija.hr/Mozaik/tabid/80/articleType/ArticleView/articleId/61528/Default.aspx , 11.7.2009.
6. OnLive, službena web stranica, http://www.onlive.com/support/getstarted
7. New Trojan Distributed as Steam Game Hack, http://techbuzzblog.com/gadgets/2010/12/new-trojan-distributed-as-steam-game-hack.html , 5.12.2010.
8. A Closer Look at the Next Generation Address Bars, http://cybernetnews.com/browser-address-bar/ , 19.11.2010.