Zlonamjerni programi na društvenim mrežama

Domagoj Klasić

CARNet

domagoj.klasic@carnet.hr

01 / 666 1729

Sažetak

Ovaj rad istražuje pojavu zlonamjernih programa na društvenim mrežama. Opisani su motivi autora zlonamjernih programa. Svim korisnicima društvenih mreža predložene su smjernice za zaštitu i sigurnu komunikaciju s drugim korisnicma. Na temelju kratke analize Koobfacea (zlonamjernog programa koji se širi društvenim mrežama) razvijen je model automatske zaštite svih korisnika društvene mreže Facebook.

1. Uvod

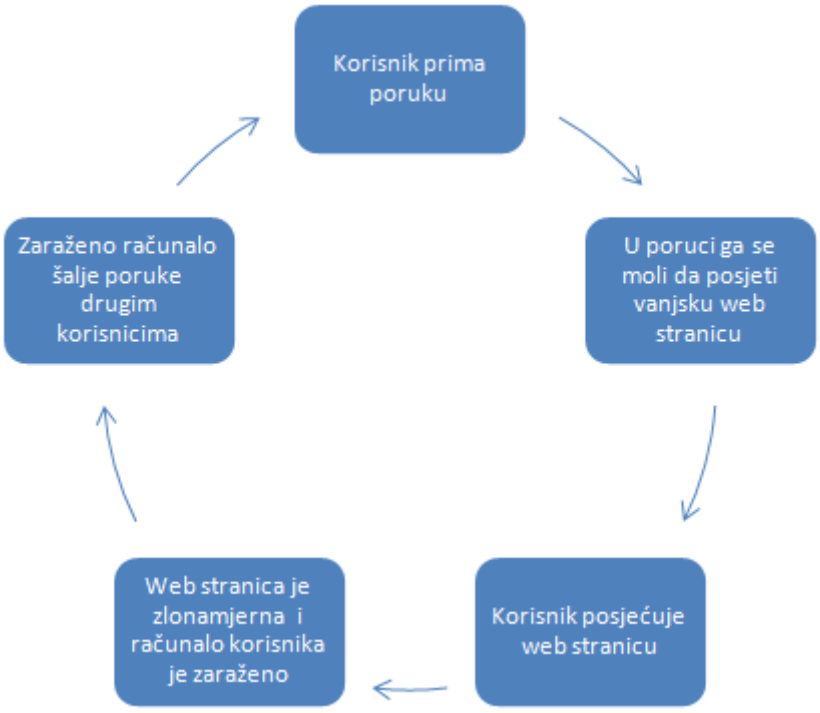
Društvene mreže korisnicima omogućuju komunikaciju i dijeljenje različitih multimedijskih sadržaja (fotografije, video zapisi…). Koristi od njih imaju i poslovni korisnici. Promidžbene poruke na društvenim mrežama donose veliku zaradu, a poslovne organizacije mogu izraditi vlastiti profil te se približiti svojim klijentima.

Nažalost, s sve većim rastom društvenih mreža raste i broj kriminalaca koji u njima vide priliku za brzu zaradu. Zbog toga, danas je svaki korisnik društvenih mreža moguća žrtva zlonamjenih programa koji se šire putem mreže. Takvi zlonamjerni programi kradu sve osobne podatke do kojih mogu doći. Korisnik zbog toga može pretrpjeti krađu indentiteta ili financijsku štetu.

2. Način širenja zlonamjernih programa

U izvještaju koji je objavila poznata antivirusna tvrtka Sophos navodi se kako je 36% korisnika društvenih mreža 2010. godine imalo problema s zlonamjernim programima. Posebno je zabrinjavajuće da je to porast od 69.8% u odnosu na prethodnu godinu.

Zlonamjerni kod se putem društvenih mreža najčešće širi tehnikama socijalnog inžinjerniga. Začarani krug na društvenoj mreži počinje kada zlonamjerni program korisniku pošalje poruku. Na sljedećem dijagramu je prikazan cijeli proces širenja zlonamjernog koda.



Slika 2.1 – Način širenja zlonamjernih programa na društvenim mrežama

Nakon što zloznamjerni program zarazi računalo korisnika, on će ukrasti njegove lozinke za sve društvene mreže koje korisnik posjećuje. Na tim društvenim mrežama će u ime korisnika, ali bez njegova znanja slati poruke svim njegovim kontaktima.

Kako bi održao visoki postotak zaraze, zlonamjerni program šalje veliki broj neželjenih poruka. Gotovo 70% korisnika društvenih mreža susreću se s takvim porukama .

3. Zaštita

Teško je očekivati da će društvene mreže, zaokupljene velikim rastom broja korisnika, uložiti značajna sredstva u suzbijanje zlonamjernih programa. No, za zaštitu dovoljno je slijediti nekoliko sigurnosnih preporuka:

- Koristiti antivirusni alat.
- Ažurirati sav softver na računalu, posebno web preglednik.
- Ne vjerovati sumnjivim porukama na društvenim mrežama. Čak ukoliko poruku pošalje osobni prijatelj. Postoji mogućnost da je njegovo računalo zaraženo zlonamjernim programom koji je poslao poruku. Uvijek je potrebno provjeriti njihovu vjerodostojnost.

Nažalost, većina korisnika društvenih mreža ne slijedi ove preporuke. Rezultat toga su porazne statistike koje govore o širenju zlonamjernih programa.

4. Koobface

Koobface je naziv zlonamjernog programa otkrivenog u prosincu 2008. godine. U to vrijeme on je bio revolucionaran primjerak zlonamjernog koda. Naime, Koobface se širio isključivo putem društvenih mreža (Facebook, MySpace, Twitter …).

Kada zarazi računalo, Koobface se spaja u botnet mrežu s drugim zaraženim računalima. Putem te botnet mreže napadaču je omogućena udaljena kontrola nad svim zaraženim računalima. Osim što stvara *botnet* mreže, Koobface s zaraženog računala šalje poruke drugim korisnicima društvenih mreža kako bi na prije opisan način zarazio i njihova računala.

U porukama koje Koobface šalje obično stoji tekst *My home video :)* i poveznica na zlonamjernu stranicu koja imitira YouTube. Zlonamjerna stranica ima slično ime – YuoTube.

Na navedenoj stranici od korisnika se traži da preuzme i pokrene nepoznatu izvršnu datoteku kako bi mogao pogledati video. Ta izvršna datoteka je sam Koobface, ukoliko ju korisnik pokrene – njegovo računalo će biti zaraženo.

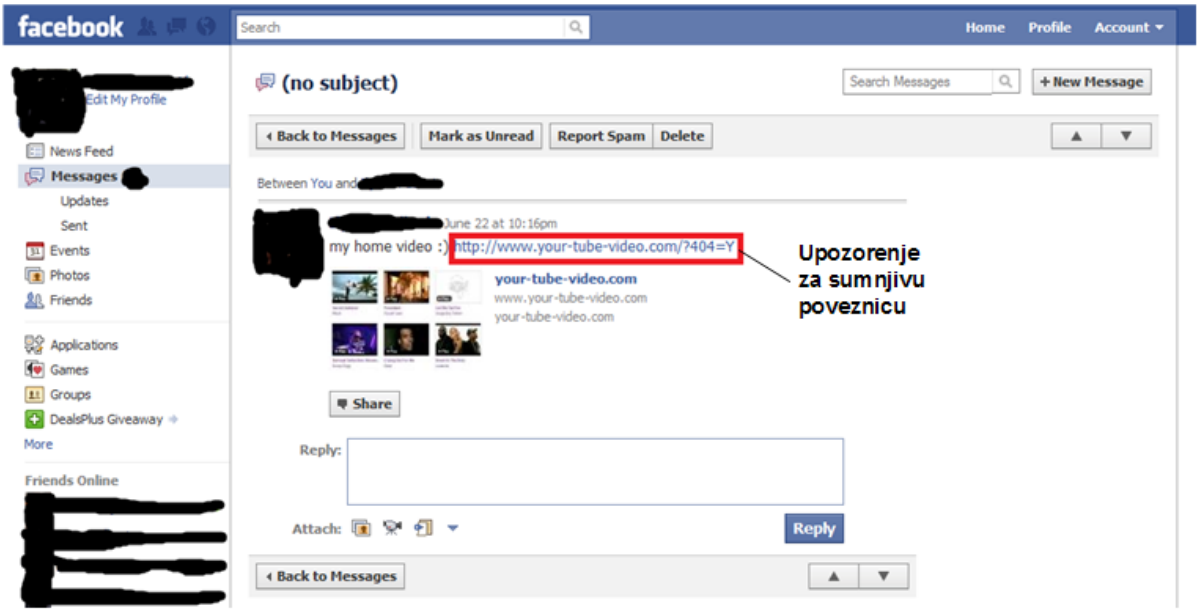
5. Zaštita od Koobfacea

Za zaštitu od Koobface i sličnih zlonamjernih programa predložen je program koji automatski provjerava sve poruke koje korisnik prima. U porukama program traži poveznice na druge stranice. Ako program otkrije da je riječ o sumnjivoj poveznici upozoriti će korisnika.

Program traži poveznice koje:

- Vode na stranice izvan društvene mreže na kojoj je poruka poslana
- Imaju slično ime kao i neki od popularnih web servisa

Ako poveznica zadovoljava oba kriterija program ju može označiti crvenom bojom i upozoriti korisnika o mogućoj opasnosti. Funkcionalnost je ilustrirana i sljedećom slikom.



Slika 5.1 – Predloženi softver upozorava korisnika na sumnjivu poveznicu

S obzirom na opisani način širenja zlonamjernog koda ovakav program mogao bi pomoći korisnicima da ne slijede zlonamjerne poveznice.

6. Literatura

Baltazar Jonell, Costoya Joey i Flores Ryan The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained [Izvješće]. - [s.l.] : TrendMicro, 2009.

Leggio Jenifer Facebook's (futile) malware exorcism - can social networks fight back? [Mrežno] // ZDNet. - ZDNet, 8. 8 2008. - 21. 6 2010. - http://www.zdnet.com/blog/feeds/facebooks-futile-malware-exorcism-can-social-networks-fight-back/176.

Sophos Security Threat Report: 2010 [Izvješće]. - [s.l.] : Sophos, 2010.

Whitney Lance Malware and social network attacks surge in '09 [Mrežno] // Cnet News. - CBS Interactive, 17. 2 2010. - 21. 6 2010. - http://news.cnet.com/8301-1009_3-10454870-83.html.