Opasnosti Facebooka

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalno središte za računalnu sigurnost
National Computer Emergency Response Team

Nacionalni CERT

Večernji list

Uvod

Osim što je uvelike promijenila način komuniciranja i povezivanja putem Interneta, društvena mreža Facebook utječe i na naš svakodnevni život. Mreža je donijela mogućnost da jednostavno pratimo čime se bave naši prijatelji, dopisujemo se s njima putem poruka ili chata, postavljamo albume fotografija, glazbu koju volimo, igramo igre u kojima možemo kupiti virtualne predmete, pretplaćujemo se na poznate osobe ili političke stranke, biramo koga želimo pratiti više, a koga manje itd. Time su mnoge aktivnosti koje obavljamo u stvarnom svijetu zamijenjene onim virtualnim. Facebook stalno uvodi nove mogućnosti, a nedavnim razvojem pametnih telefona, postale su nam dostupne i u pokretu.

Godine prisutnosti Facebooka i svega što dolazi uz njega, stvorili su kod korisnika rutinirani i automatizirani oblik korištenja mreže. Ako na to dodamo kombinaciju emocija i potrebe za društvenošću te povjerenje koje imamo prema sadržaju kojeg postavljaju naši prijatelji, ovo može biti ozbiljan problem ukoliko se pogleda druga strana medalje. Naime, Internet, uz sve svoje dobre strane, ima i one loše. Zlonamjerni korisnici su uvidjeli da im Facebook može poslužiti kao platforma za svoje zlonamjerne aktivnosti. Društvene mreže im omogućuju brzo širenje zlonamjernog sadržaja, a pritom osiguravaju određenu vjerodostojnost jer korisnici vjeruju svojim prijateljima. Na njima se također nalaze velike količine, često povjerljivih, privatnih korisničkih informacija koje se isto mogu zloupotrijebiti ili indirektno koristiti u napadima.

Krajem 2011. Facebook je objavio kako je svaka 24 sata čak 600,000 korisničkih računa pod napadom ili zloupotrebom! Također, Facebookov centar za sigurnost dnevno skenira 2 trilijuna linkova i pritom blokira 220 milijuna različitih poruka sa zlonamjernim linkovima!

Mnogi korisnici su tehnički neobučeni i nedovoljno upoznati s postojećim prijetnjama. Zbog svega toga je vrlo važno biti upoznat na koje sve načine djeluju napadači i u tome pomaže čitanje ove brošure.

Opasnosti

Opasnosti, odnosno sigurnosne prijetnje kojima je suočen korisnik na Facebooku uključuju cijeli spektar poznatih prijetnji s Interneta. To su: **„malware“** (zlonamjerni programi), **„phishing“** (npr. marketing lažnih proizvoda), a u novije vrijeme **„click-jacking“** te razni drugi oblici prijevara.

Napadači se za širenje zlonamjernog sadržaja koriste lažnim reklamama (uključujući i oglase koje napadači legalno kupe), promocijama, aplikacijama i personaliziranim porukama. Pritom putem **socijalnog inženjeringa**, pokušavaju manipulirati korisnicima koristeći njihove emocije te ih nastoje navesti na otvaranje zlonamjernog sadržaja. Prilikom korištenja Facebooka najvažnije je da korisnik bude svjestan da njegovi prijatelji **nisu nužno autori** svojih poruka, nego netko ili nešto (zlonamjerni program) u tom trenutku upravlja njihovim računalom, odnosno Facebook računom. Važno je prepoznati potencijalno rizičan sadržaj, posebno ako on vodi na URL-ove izvan Facebooka (izvan domene facebook.com). Napadači koriste sve moguće načine komunikacije na Facebooku kako bi potencijalnim žrtvama podvalili zlonamjerne URL-ove zadužene da zaraze računala korisnika. Korisnici Facebooka se tako najčešće mogu zaraziti putem:

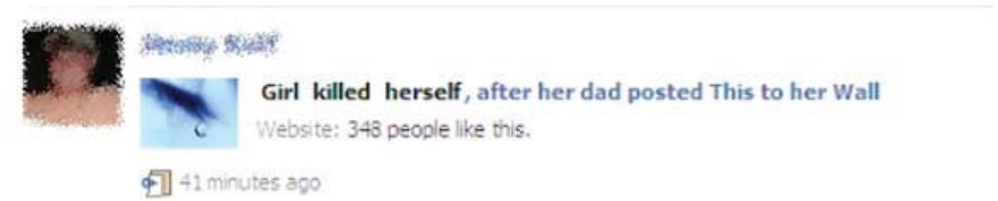
- „News Feeda“, odnosno linkova u statusima prijatelja
- privatnih poruka
- poruka na chatu
- zlonamjernih URL-ova na grupama, profilima poznatih ličnosti itd.

Zlonamjerni programi i prijevare sve više pogađaju i mobilne platforme, a ne samo klasična računala. Korisnik se zlonamjernim programom može zaraziti i izvan Facebooka (npr. putem elektroničke pošte), a program može njegov Facebook račun koristiti za svoje daljnje širenje

Najčešći oblici prijetnji

Sigurnosne prijetnje na Facebooku najčešće se pojavljuju u četiri oblika:

- **poruke s tekstom „Moraš vidjeti ovo“ i sl.**



- **besplatne stvari (promocije)**

- **nove aplikacije (funkcionalnosti)**

- **događaji koji uključuju poznate ličnosti**

Jasno je kako svi ovi oblici zapravo socijalni inženjering u svojem tipičnom obliku čija je funkcija navesti korisnika na određenu akciju.

Zlonamjerni programi

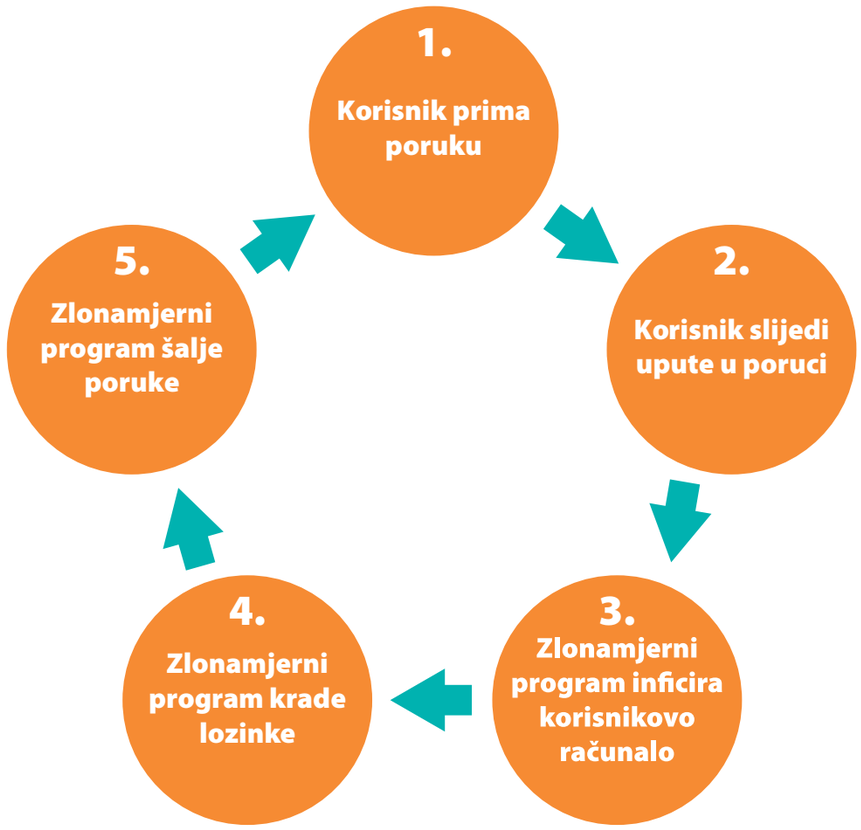
Zlonamjerni programi su s godinama postali sve složeniji i na sve maštovitije načine pokušavaju prevariti korisnike. Kako bi mogao prepoznati zarazu, korisnik treba biti upoznat s općenitim mogućnostima zlonamjernih programa. Procijenjeno je da se oko 20% korisnika Facebooka suočava s zlonamjernim programima dok su na toj društvenoj mreži. Današnji moderni zlonamjerni programi su u stanju:

- ukrasti povjerljive podatke (Facebook račun, brojeve kreditnih kartica i sl.)
- u potpunosti onemogućiti rad antivirusnog programa na računalu
- servirati prozore s oglasima za krivotvorene proizvode, pornografiju i sl.
- izmijeniti DNS postavke na zaraženom računalo što dovodi do toga da web preglednik umjesto originalnih web stranica prikazuje lažne, često „phishing“ stranice i one koje poslužuju druge zlonamjerne programe
- zaključati rad na računalu uz lažno upozorenje (i lažno predstavljanje) dok se ne plati određena suma novca
- iskoristiti računalo za napad na druga računala i web sjedišta na Internetu

Životni ciklus zlonamjernog programa najčešće izgleda ovako:

1. Korisnik prima poruku koja sadrži poveznicu na zlonamjerni program
2. Korisnik slijedi poveznicu i tamo obavlja akciju na koju je naveden
3. Zlonamjerni program se instalira na korisnikovo računalo zbog akcije korisnika

4. Zlonamjerni program krade korisničke podatke te tako dobiva i podatke Facebook računa
5. Zlonamjerni program šalje poruke kojima se dalje širi s Facebook računa zaraženog korisnika



životni ciklus zlonamjernog programa

Primjeri zlonamjernih programa

Računalni crv **Koobface** (ime izvrnuto od Facebook) je bio prvi specijalizirani zlonamjerni program koji je napadao društvene mreže. Crv se širio putem poruka poput jedne prikazane na slici. U poruci se tvrdi kako je korisnik snimljen i kako može pogledati navodni video sadržaj. Koobface je pravi primjer sofisticiranog zloćudnog programa koji se sastojao od nekoliko komponenti. Popis njegovih mogućnosti je nevjerojatan. Sa zaraženih računala je otimao povjerljive podatke različitih korisničkih računa, otimao je čak i licence za legalni softver, prisiljavao žrtve na

rješavanje CAPTCHA poruka, pretvarao zaraženo računalo u poslužitelj zlonamjernih web stranica, mijenjao DNS postavke kako bi žrtvu uputio na različite zlonamjerne stranice itd.

Facebook je u siječnju 2012. objavio kako je prošlo više od 9 mjeseci otkako su uočene posljednje poruke kojima se širio Koobface, međutim crv se i dalje širi drugim web servisima.

Nakon Koobfacea, mrežom je harao niz drugih crva. Na primjer, crv **Palevo** se širio chat porukama, a bio je u obliku Facebook aplikacije koja je korisnike upućivala na zlonamjerne web stranice. Kao što se vidi na slici, chat poruka koja stiže od prijatelja djeluje prilično uvjerljivo. Naravno računalo tog prijatelja je zaraženo crvom.

Zabilježeno je i kako su napadači koristili Facebook za širenje zloglasnog trojanskog konja Zeusa, specijaliziranog za krađu bankarskih podataka s zaraženom računala. Širio se preko otetih korisničkih Facebook računa pomoću kojih je slao poruke s linkovima za preuzimanje slika atraktivnih djevojaka.

„Clickjacking“

Clickjacking je vrsta napada, odnosno prijevare u kojem se korisnika navodi da klikne na skriveni link koji je prikriven nekim drugim linkom ili grafičkim elementom. Naime, manipulacijom HTML-a i skriptnim kodom (koristeći više slojeva grafičkog sučelja), napadač preko zlonamjernog linka stavlja link (gumb) za neku drugu akciju koju korisnik (žrtva) misli da će učiniti. Taj napad je moguć jer web preglednici dopuštaju da web stranice sadrže više prozirnih grafičkih elemenata naslaganih jedan na drugom.

klikom na gumb za pokretanje videa, zapravo "lajkamo" zlonamjerni sadržaj

Likejacking je oblik clickjackinga karakterističnog za Facebook. U tom napadu korisnika se navodi na poduzimanje akcije poput pokretanja nekog videa, što ustvari uzrokuje neželjeno „lajkanje" i dijeljenje tog sadržaja na profilu te se on dalje širi Facebookom. Tako će i neki prijatelji tog korisnika učiniti isto, a napadači će imati koristi od velikog broja posjeta svojoj web stranici (zarada od oglasa), a često i od daljnjeg preusmjeravanja korisnika putem podvaljenih linkova.

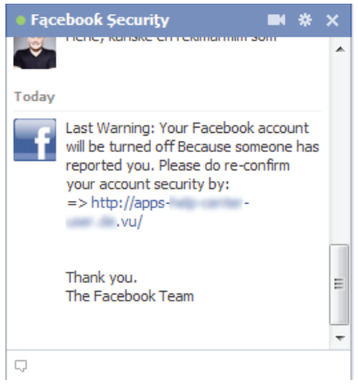
„Phishing"

„Phishing" je vrsta prijevare koja postoji na internetu već duže vrijeme. Korisnika se navodi da otkrije svoje povjerljive podatke (korisničko ime i lozinku) tako da ih upiše u krivotvorenu web stranicu odnosno login formu koja je izgledom jednaka originalnoj, ali ima drugačiju adresu tj. domenu.

Jedna od takvih stranica je prikazana na slici niže. Linkovi na krivotvorene stranice se šire putem elektroničke pošte ili privatnih poruka kao u slučaju Facebooka. Važno je upamtiti kako Facebook nikad neće tražiti da mu dostavimo naše podatke (putem elektroničke pošte ili poruka na samoj mreži). Također ukoliko smo već ulogirani u Facebook, neće nas na nekoj drugoj web stranici tražiti da ponovno upisujemo svoje podatke.

Napadači koji koriste phishing postaju sve domišljatiji. Jedan od takvih napada koristio je e-mail poruke u kojima je korisnika obavještavao kako mu je Facebook račun blokiran te ga je tražio potvrdu podataka. Napadači su se lažno predstavljali kao „Facebook Security". Phishing stranica je prikazana na slici iznad:

Još jedan od takvih phishing napada širio se putem kompromitiranih Facebook računa. Napadači su nakon što bi oteli neki račun, mijenjali ime profila u „Facebook Security" te putem chata (prikazano na slici) upozoravali prijatelje da će im se račun ugasiti ukoliko ne potvrde svoje podatke, odnosno identitet. Link je vodio na formu koja ja tražila ne samo podatke za pristup Facebooku, nego i elektroničkoj pošti te podatke o kreditnoj kartici.



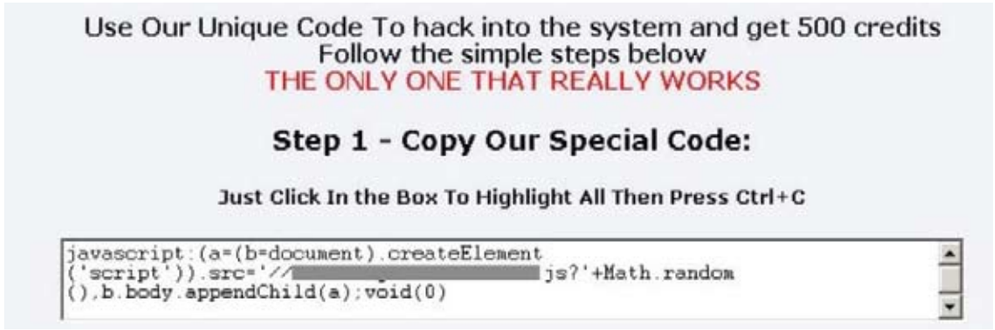
Kako bi se zaštitio od phishinga, za korisnika je najvažnije da razvije naviku provjere URL-a prije upisivanja svojih korisničkih podataka te naravno nikad ne ostavlja podatke na web stranici za koju nije siguran da je originalna.

Ostale prijevare

Zlonamjerni korisnici pokušavaju različitim prijevarama izvući neku korist od žrtvi na Facebooku.

Prijevare uključuju lažno skupljanje donacija (npr. za stradale u potresu, bolesne osobe i sl.), prodaju lažnih aplikacija (npr. da vidimo tko posjećuje naš Facebook profil) i predmeta (knjiga o nekakvim velikim tajnama i sl.). Važno je upamtiti kako će napadači uvijek primijenjivati tehnike socijalnog inženjeringa.

Zabilježeni su i primjeri u kojima napadači navode korisnike na upisivanje zlonamjernog skriptnog koda u svoj web preglednik (u adresnu traku). Ako nasjednu, žrtve napadaju (tj. kompromitiraju svoj profil) same sebe (slika dolje).



Napadači se koriste i lažnim Facebook računima i šalju zahtjeve za prijateljstvom kako bi time dobili pristup (često osobnim pa čak i povjerljivim) informacijama koje korisnici stavljaju na svoj profil. Stoga je preporučeno ne prihvaćati zahtjeve za prijateljstvo od nepoznatih osoba. Zabilježeno je kako napadači koriste alate s kojima uzimaju imena i slike profila pravih prijatelja (ukoliko žrtva ima podešen profil da je to moguće) prije nego što zatraže prijateljstvo, zbog toga je potrebno dobro (s prijateljem) provjeriti tko stoji iza zahtjeva čak i ako je naizgled riječ o prijatelju.

Savjeti za zaštitu

Oprez prije svega!

Prije svega valja istaknuti kako je najbolja zaštita od zlonamjernog sadržaja na Facebooku – oprez. Važno je dobro promisliti prije klikanja na linkove u porukama od prijatelja, linkove za instalaciju aplikacija itd. Sumnjivom sadržaju ne vjerovati čak i ako dolazi od prijatelja jer upravo se zlonamjerni sadržaj tako i širi! Razne ponude poput besplatnih kupona i slično gotovo uvijek su prijevare.

Nije svaka lozinka ista

Korištenje sigurne lozinke (od barem 8 znakova koji uključuju velika i mala slova, znakove i brojeve) osnovni je uvjet sigurnosti korisničkih podataka. Također je važno da lozinka ne bude vezana uz privatne podatke (ime, datum rođenja i sl.) čak i ako je „iskrivljena“ umetanjem brojeva umjesto slova i sl. Razlog tome je što napadači koriste alate koji isprobavaju sve moguće kombinacije znakova u lozinkama uz pomoć baze osobnih podataka (ključnih riječi).

Što možemo učiniti na samom Facebooku?

Uključiti korištenje kriptiranog HTTPS protokola pod **Naslovnica -> Postavke korisničkog računa -> Sigurnost** uključiti opciju **„Sigurno pretraživanje“** („Secure Browsing“). Na istom mjestu je preporučeno uključiti i i „Obavijesti o pristupu“ što znači da će nas Facebook obavijestititi elektroničkom poštom svaki put kad netko pristupi Facebooku s računala kojeg nismo prethodno za to koristili ili smo na njemu izbrisali „cookie“ datoteku .

Redovite nadogradnje

Jedna od osnovnih mjera zaštite je redovito održavanje antivirusnog softvera, vatrozida, web preglednika itd. Ovo je posebno važno ukoliko društvenoj mreži pristupate putem pametnog telefona, koristeći Facebookovu **mobilnu aplikaciju.** Naime, pošto je riječ o relativno novoj tehnologiji, često se otkrivaju sigurnosni propusti u navedenoj aplikaciji te ju je stoga potrebno redovito osvježavati novim inačicama.

Alati

Uz antivirusno rješenje, dobro je koristiti alat za filtriranje URL-ova, na primjer u obliku dodatka (addon) za web preglednik. Jedan od poznatijih dodataka preglednicima je „Web of Trust“ (WoT). Takvi alati mogu upozoriti korisnika prilikom posjeta zlonamjernoj web stranici jer su povezani s globalnom bazom zloćudnih web stranica.

Tu su još i dodaci NoScript za Firefox preglednik te inačica za Chrome vrlo sličnog imena, NotScripts. Ti dodaci blokiraju izvršavanje JavaScript koda sa svih domena kojima to nismo eksplicitno dopustili i time mogu spriječiti učitavanje zlonamjernog sadržaja.

Informiranje

Općenito, za očuvanje računalne sigurnosti, važno je biti pravovremeno informiran, stoga je dobro pretplatiti se na službene Facebookove grupe (stranice) namijenjene tome – „Facebook Security“ i „Facebook Safety“. Postoje i specijalizirane Facebook aplikacije za sigurnost, no ovdje je potrebno biti vrlo oprezan jer, kao što je navedeno, postoji veliki broj malicioznih aplikacija.

Impressum

Izdavač
Hrvatska akademska i istraživačka mreža CARNet,

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Josipa Marohnića 5, Zagreb
tel: 01 6661 616, fax: 01 6661 615
http://www.carnet.hr