Steganografska analiza jednog javnog WEB sajta

Julijana Mirčevski, Nikola Popović,

Sadržaj — **Rad se bavi steganografskom analizom jednog javnog Web sajta. Korišćeni su steganografski programski alati koji su raspoloživi u domaćim istraživačkim uslovima kao i freeware software. Prikazani su rezultati analize i ukazaano je na nedostatke sistemskog obezbedjivanja steganografskog i bezbednosnog software-a za naše institucije.**

Ključne reči **— Open source, steganografija, steganoanaliza, steganografski alati**

I. UVOD

Istraživanje opisano u ovom radu obuhvata višestruku analizu Web sajta www.psy-help-energy.com sa aspekta sadržaja steganografskih elemenata. Do sada, koliko je autorima poznato, nije identifikovan ni jedan domaći sajt sa steganografskim elementima. Moguće je da su takve analize obavljane za račun privatnih agencija i drugih nevladinih tela ali njihovi rezultati nisu javno objavljivani. Ovaj rad iskazuje i interes autora za zaštitu od steganografske zloupotrebe domaćih sajtova.

Definicija pojma steganografije sreće se u velikom broju članaka i radova, počevši od popularnih napisa preko tehničke dokumentacije za softverske proizvode iz domena steganografije pa do rezultata velikih istraživačkih projekata, naučnih instituta i fakulteta ali i vladinih vojnih i policijskih službi i organizacija. Referenca [1] detaljnije ukazuje na formiranje ovog pojma. Ovde će biti istaknuto da steganografija nije kriptografija, detaljnije o tome u [2]. Kriptografija podrazumeva transformaciju poruke tako da slučajni presretač takve poruke ne može da razume njen sadržaj bez poznavanja kriptografskog ključa. Steganografija se koristi da se sakrije originalna, razumljiva poruka bez transformacije same poruke u neki izmenjeni sadržaj ali da pritom ostane nevidljiva. Svaki presretač opremljen odgovarajućim softverskim alatom i znanjem može da odkrije takvu poruku, da je izdvoji iz nosača informacije i da je pročita. Ove dve tehnologije se često koriste suplementarno; kriptovani fajl se steganografskom aplikacijom upisuje u sliku i tako bezbednije prenosi. Potrebno je bitno razlikovati dve glavne grupe [3] primene staganografije: kada je okruženje koje nosi skrivenu informaciju značajno za prikazivanje u neizmenjenom obliku i sa potpunim kvalitetom i kada je skrivena poruka značajnija od medija koji služi samo kao koverat za poruku. Prva grupa primena je zaštita digitalnih kolekcija ili copyright protection (pomoću vodenog žiga, na primer) a druga je ciljano zaobilaženje neidentifikovanih presretača/primaoca poruke.

Julijana Mirčevski, (telefon: 381-64-4244--754; e-mail: julijana@afrodita.rcub.bg.ac.rs).

Nikola Popović, Ministrstvo inostranih poslova, Kneza Miloša 24-26, 11000 Beograd, Srbija; (e-mail: nipopo@afrodita.rcub.bg.ac.rs).

II. ANALIZA SAJTA

Web sajt koji je analiziran za potrebe ovog rada je tronivoski, profesionalno uradjen, informativnog karaktera realizovan poznatim softverskim alatima. Sigurno se zna da je sajt uspostavljen i bio aktivan tokom 2008 i delom 2007. godine. Sajt sadrži pretežno tekst koji se odnosi na osnovne postavke alternativne medicine i slike koje taj sadržaj vizuelno podržavaju. Slike nisu tipične za do sada poznate medijske nosače steganografskih informacija. Ukupno ima oko 50 slika od kojih su većina u *gif* formatu a samo 3 u *jpeg* formatu.

Sadržina sajta zauzima 1.37 MB u formi teksta i slika. Sastoji se od 10 html dokumenata, CSS (Cascading Style Sheets) dokumenta, 45 slika u GIF formatu, 3 slike u JPG formatu, i jednog dokumenta u PDF formatu obima 15 stranica. Ukljucen je i jedan SlideShow od 5 slika.

Analiza je izvedena upotrebom više različitih steganografskih programskih alata a u ovom radu biće izloženi rezultati rada ***StegSpy***, ***Stegdetect, Invisible Ink i StegAlyzer*** programima. Naime, ovi programi su raspoloživi na internetu kao *free ware* software sa izuzetkom StegAlyzer-a i bilo je moguće izvesti korektan download proces bez tehničkih i administrativnih problema u našim uslovima poslovanja.

Link prema CHAT segmentu u prvom trenutku nije skinut a nije ni bio aktivan (link je vracao na osnovnu stranicu) a kada je ponovo skidan Web sajt, CHAT segment je bio aktiviran.

Grafički, po strukturi i sadržaju Web sajt ne odudara od standarda za sajtove ovog tipa. Sa aspekta steganoanalize situacija je složena, pored osnovnog problema slika i teksta prisutan je i dokument u PDF formatu koji zahteva posebnu proceduru analize pošto kombinuje karakteristike tekstualnog dokumenta i slike. Na osnovu dosadašnjeg ispitivanja, posmatrani PDF dokument ne sadrži slike. Pored toga, potrebno je ukazati na nedostatak CHAT segmenta koji, ukoliko je funkcionisao moguće da je sadržao dinamičke podatke potencijalno od interesa za analizu celine Web sajta odnosno celinu njegove funkcionalnosti.

Steganografski programski alati posebno se brzo razvijaju posle 11. septembra 2001. godine. Uočeno je da su poboljšane njihove performanse u pogledu sve manjih

memorijskih zahteva, povećana portabilnost kao i sve nezavisnije funkcionisanje u odnosu na operativni sistem računara [4].

Metodi ovog istraživanja su zasnovani na primeni sledećih alata za skrivanje i/ili detekciju poruka u slici:

Naziv	Licenca
StegSpy v2.1	Free
Stegdetect v0.4	Open source
Digital Invisble Ink Toolkit v1.5	Open source
StegaAlyzer AS, SS v3.1	Licenciran

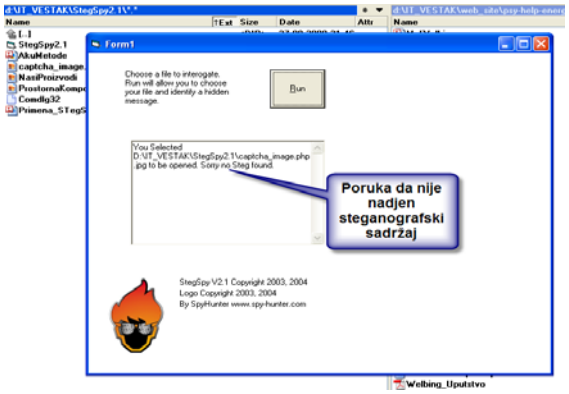
Pored toga korišćeni su i sledeći pomoćni forenzički alati:

Naziv	Licenca	Namena
Disk investigator v1.3	Free	Hex Editor
GetLeft v1.2	Open source	Skidanje Web sajtova
Teleport 1.55	Licenciran	Skidanje Web sajtova

Licencirani softveri, za ovu priliku, korišćeni su u institucijama koje imaju licencu.

III. SPECIFIČNOSTI DETEKTOVANJA STEGANOGRAFSKOG SADRŽAJA PROGRAMIMA *STEGSPY, STEGDETECT* I *DIGITAL INVISIBLE INKTOOLKIT*

Autor ***StegSpy*** programa je Michael T. Raggo. Program detektuje sledeće software: Hiderman, JPHideandSeek, Masker, JPegX i Invisible Secrets. Raspoloživ je za slobodno preuzimanje samo u izvršnoj verziji na www.spy-hunter.com/stegspydownload.htm.Tekuća verzija 2.1 pisana je u MS Visual Basic-u. Raspolaže grafičkim interfejsom koji korisniku omogućava izbor fajla koji će se ispitivati. U skladu sa opisom [5] StegSpy vrši steganoanalizu na osnovu signature, ali o tačnom načinu rada može da se samo pretpostavlja, što nas u istraživanju uopšte i usmerava na korišćenje Open source softvera.

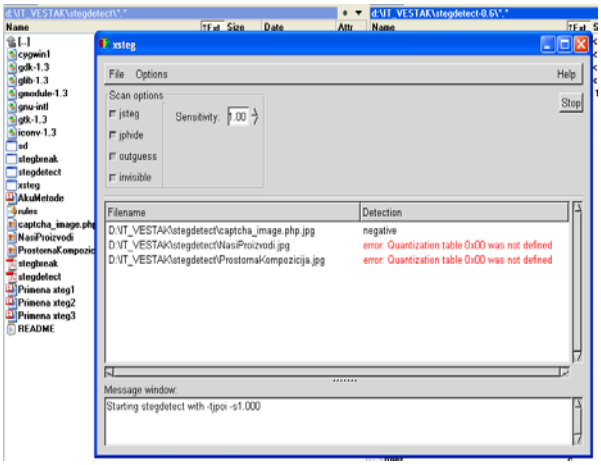


Sl. 1. Ilustracija rada programa StegSpy

Stegdetect program je raspoloživ u verziji 0.6 i 0.5. ***Stegdetect*** verzije 0.6 može da se download-uje samo u izvornom kodu pa mora da se iskompajlira kako bi se dobila izvršna verzija. ***Stegdetect 0.6*** podržava linearnu diskriminacionu analizu dajući kao rezultat set normalnih slika i set slika koje sadrže skrivene sadržaje ubačene steganografskim aplikacijama. Program može automatski da odredi linearnu funkciju detekcije koja može da se primeni na još neklasifikovane slike. Linearna diskriminaciona anliza odvaja u hyper ravni, „čiste“ slike od stego slika. „Naučena“ funkcija može biti sačuvana za kasnije korišćenje na novim slikama. ***Stegdetect*** podržava više različitih vektora osobina i automatski računa operativnu karakteristiku prijemnika što, takodje, može biti korišćeno za procenu kvaliteta automatski naučene funkcije detekcije. Korišćena je verzija open source ***Stegdetect v0.4,*** autora Niels Provos-a, raspoloživa na www.outguess.org/detection.php. Program detektuje sledeći softver: Jsteg, jphide, Invisible Secrets, Outguess 0.13b, F5, appendX and Camouflage

Stegdetect je pisan u C jeziku. Korišćena je verzija sa grafičkim interfejsom **-xsteg.** Grafički interfejs korisniku omogućava izbor fajla koji će se ispitivati kao i izbor programa sa kojim je potencijalno ugrađena skrivena poruka. U skladu sa opisom [6] Stegdetect vrši steganoanalizu samo slika u JPEG formatu.

Stegdetect je program koji analizira sliku na prisustvo steganografskog sadržaja. Obavlja statističke testove da bi odredio da li je prisutan steganografski sadržaj, a takođe pokušava da odredi koji je steganografski program bio korišćen. U ovoj verziji je prisutno dugme za izbor nivoa osetljivosti programa, mada u ovom istraživanju nije detaljnije ispitana ta funkcija.

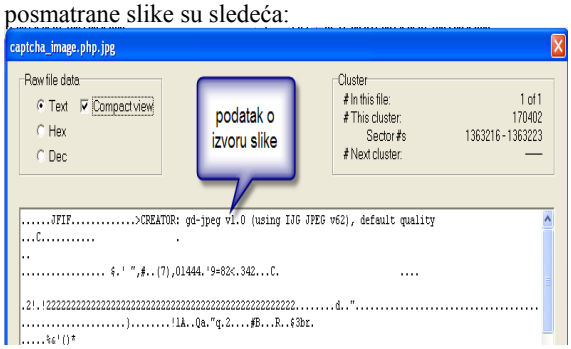


Sl. 2. Ekran tokom rada ***xsteg***-a

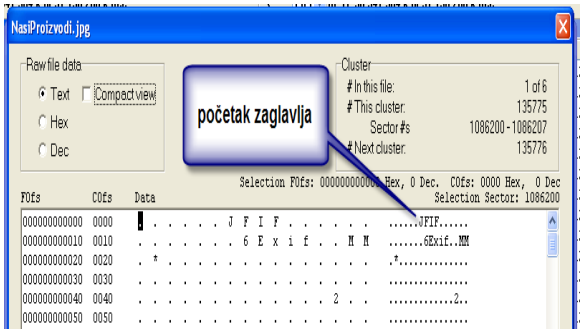
U slučaju prve slike vidi se da je slika nastala u okviru grafičkog programa. Druge dve slike imaju identičan početak zaglavlja (JFIF itd.) ali se tek posle više ugrađenih netekstualnih karaktera (uglavnom 0x00) pojavljuje podatak da su te dve slike urađene pomoću digitalnog fotoaparata. Navedena greška u tabeli kvantizacije DCT (Direct Cosinus Transformations) se verovatno može identifikovati detaljnim istraživanjem dokumentacije softvera kojim fotoaparat generiše JPEG slike odnosno respektivnom dokumentacijom za JPEG format.

Na slici se istovremeno vide i rezultati ispitivanja tri slike sa Web sajta koje su bile u JPEG formatu. Detaljnijim istraživanjem poruke o grešci / detekciji

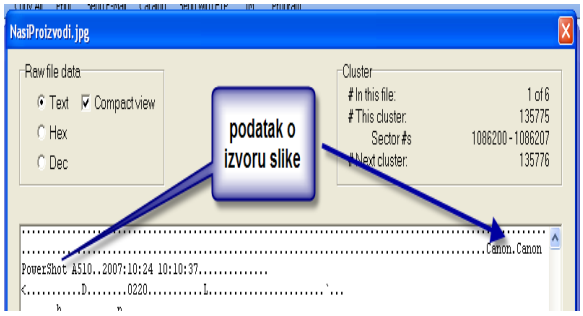
ustanovili smo da se ipak ne radi o steganografskom sadržaju već o razlikama koje se javljaju u procesu generisanja slika u JPEG formatu. Prikazana poruka pripada listi grešaka koje se javljaju pri čitanju JPEG formatu nastalim u različitim izvorima. Zaglavlja tri posmatrane slike su sledeća:



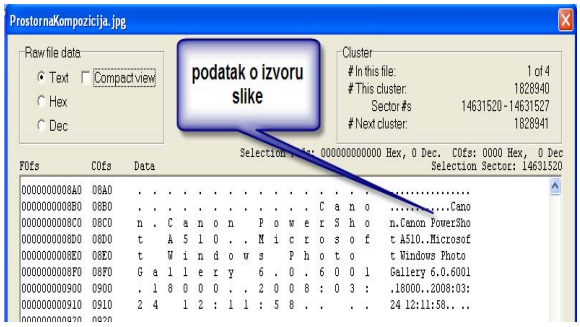
Sl. 3. Analiza prve slike u JPEG formatu



a)



b)

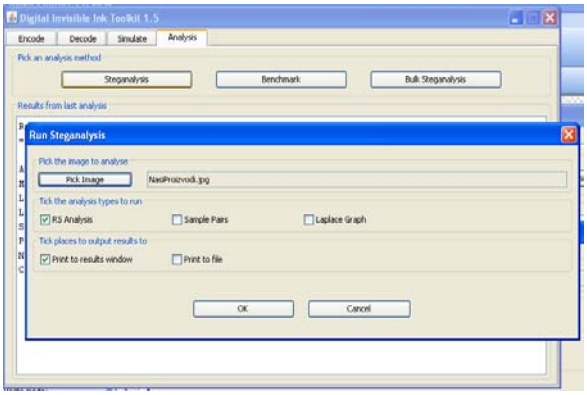


c)

Sl. 4. Izgled ekrana tokom ispitivanja slika u JPEG formatu

Digital Invisible InkToolkit je steganogafski alat pisan u Javi, koji može da „sakrije“ bilo koju vrstu fajla (pod pretpostavkom da fajl može da se po veličini uklopi u noseću sliku, i da je slika nosilac sa 24-bitnim kolorom). Program radi pod Windows i Linux operativnim sistemom pošto je pisan u ***javi*** i kao takav, nezavisan od platforme.

Opremljen je sa četiri delimično podesiva algoritma za skrivanje podataka kao i sa open-source implementacijom RS analize. Program ima dodatnu prednost za simulaciju „skrivanja“ slike tako da može da se dobije dovoljno tačna mapa područja gde je skrivena slika. Za analizu pojedinih slika sajta korišćen je upravo ovaj segment programa.



Sl. 5. Izgled ekrana tokom analiziranja fajla pomoću ***Digital Invisible InkToolkit*** programa

IV. REZULTATI ISPITIVANJA PROGRAMOM *STEGALYZER SS V3.1*

Familija proizvoda ***StegAlyzer*** kreirana je i implementirana u SARC - Steganography Analisys and Research Center, USA, sa ciljem da se obezbedi efikasan programski alat za potrebe forenzičara koji rade na pronalaženju i izdvajanju skrivenih informacija koje su ubačene primenom različitih steganografskih aplikacija. Dva najčešće korišćena programa iz navedene familije su: ***StegAlyzer AS (Artifact Scanner) i StegAlyzer SS (Signature Scanner). StegAlyzer AS*** je programski alat koji proširuje standardne kompjuterske metode forenzičkih preegleda skeniranjem sumnjivih medijskih nosača na artifakte nastale primenom steganografskih aplikacija pošto je predhodno. ***StegAlyzer SS*** je program visokih performansi sa sposobnošću da skenira celokupan fajl sistem, pojedinačne direktorije ili sumnjive medije na prisustvo steganografskih sadržaja. Pritom se detektovani skriveni sadržaj može automatski i izdvojiti u okviru izvršavanja samog ***Steg Alyzer***-a. Korišćene su trial licencirane verzije ***StegAlyzer AS v3.1 i StegAlyzer SS v3.1***. Nije eksplicitno odredjeno koji software detektuje jer istraživači SARC-a prema literaturi neprekidno prikupljaju podatke o svim raspoloživim steganografskim alatima u svetu i podešavaju respektivne baze podataka. Proizvodi su raspoloživi na www.backbonesecurity.com/detection.php.

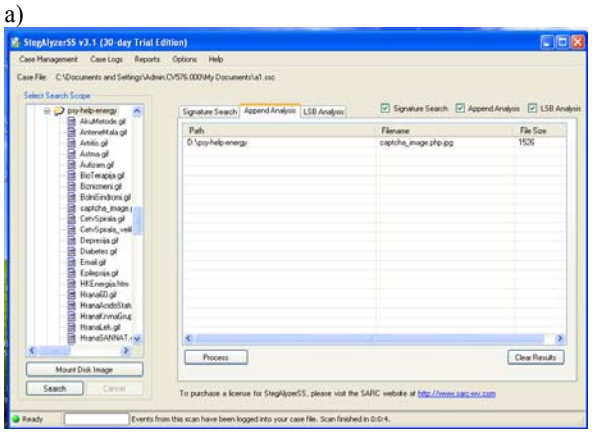
U ovom slučaju bili smo zainteresovani da testiramo softverska rešenja SARC instituta iz USA. Izvršena je parcijalna registracija i dobijen je uvid u trial verziju softvera. Problem se pojavio kod kritrijuma za konačno preuzimanje otvorenog segmenta baze podataka sa pattern-ima za identifikaciju steganografskih sadržaja. SARC institut održava biblioteku steganografskih alata, alata za „vodene žigove“ i drugih aplikacija za prikrivanje

podataka rutinski pretražujući internet za freeware, shareware i licencirane aplikacije (trenutno raspolažu sa oko 250 aplikacija). Na taj način je formiran fajl pod imenom SAFDB koji sadrži profile fajlova koji se koriste u pronadjenim i registrovanim aplikacijama (SAFDB - Steganography Application Fingerprint Database).
Konkretan problem je bio sledeći:

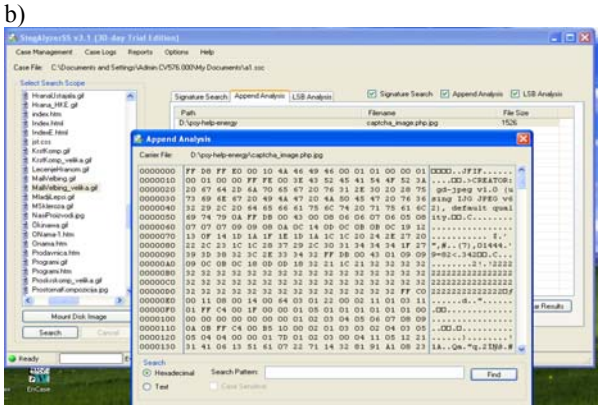
- Kako čuvati dobijenu bazu podataka SAFDB
- U kojem periodu važi obaveza čuvanja ovih podataka
- Softver SARC instituta je veoma složen kompleks čija čak i trial upotreba zahteva uspostavljanje interinstitucionalnih relacija.

To su razlozi zbog kojih smo u ovom trenutku odustali od daljeg sprovodjenja ovog testa. Međutim, postoje racionalni razlozi da se realizuje dalja saradnja sa SARC Institutom naravno u okviru većeg definisanog dugoročnog projekta.

a)



b)



Sl. 6. Ilustracija testiranja programom StegAlyzer SS v3.1

V. ZAKLJUČAK

Steganografska analiza sajta www.psy-helpenergy.com rezultira zaključcima u više domena od interesa za ovu oblast primene software-a. Ovde će biti navedene samo najbitnije stavke:

- Nema eksplicitnih dokaza da je sajt korišćen za steganografsko slanje poruka mada ima indikacija za takve namere,
- Programi raspoloživi za korišćenje u uslovima izvan institucija su nedovoljni za sigurno utvrdjivanje postojanja skrivene poruke u sadržaju sajta,
- Nema sistemskog rešenja za opremanje sajtova naučnoistraživačkih institucija, državnih organa ili provajdera programskim alatima za relevantnu steganografsku analizu sadržaja sajtova,
- Ne vrši se zvanična redovna, periodična steganografska analiza ni jednog domaćeg sajta.
- Free ware software raspoloživ na internetu potpunije obuhvata domen skrivanja, upisivanja tajnih poruka u sliku a mnogo redje domen steganoanalize slika prisutnih na sajtovima odnosno detektovanje skrivenih poruka što podkrepljuje navode u [9] [10].

I u svojim ranijim radovima [1], [4], autori su ukazivali na neophodnost redovne kontrole sadržaja domaćih sajtova i preporučivali ovu proceduru. U sadašnjem stepenu neuredjenosti tržišta softverske opreme nije moguće sprovoditi česte i kompetentne redovne procedure detektovanja skrivenih poruka u sadržajima sajtova ali gruba periodičnost na polugodišnjem ili godišnjem nivou, učinila bi mnoge pokušaje skrivanja proskribovanih poruka besmislenim.

Literatura

[1] Julijana Mirčevski, Biljana Djokić, Nikola Popović, Moderne softverske tehnike u prepoznavanju proskribovanih kompjuterskih sadržaja, II Konferencija ZITEH, Tara, novembar 2006.

[2] Jeremy Callinan, Donald Kemick, Detecting Steganographic Content in Images found on the Internet, Department of Business Management, University of Pitsburgh at Bradford, aug. 2001, http://www.chromesplash.com/jcallinan.com/publications/steg.pdf

[3] Niels Provos, Peter Honeyman, Detecting Steganographic Content on the Internet, Center for Information technology Intergration, University of Michigan, ISOC NDSS'02, San Diego, CA, February 2002.

[4] Julijana Mirčevski, Biljana Djokić, Milesa Srećković, Nikola Popović, Software Tools and Technologies in Steganography, International Conference ICEST 2007. June 24-27 2007, Ohrid, Macedonia, Procedings of Papers, Volume 2, pp. 543-546

[5] Source of software URL: http://sourceforge.net/projects/AnyFile2Image/

[6] K. Hempstalk, Digital Invisible Ink Toolkit – How To, University of Waikato, 2005, http://diit.sourceforge.net/howtos.html

[7] Steganography Detection with Stegdetect, http://www.outguess.org/detection.php

[8] An Analytical Approach to Steganalysis, http://www.sarc-wv.com

[9] H.B. Bahar, Ali Aboutalebi, Image Steganography, a New Approach for Transfering Security Information, july 2008 http://arxiv.org/ e-print service Cornell University Library.

[10] Sathiamoorthy Manohan, An Empirical Analysis of RS Steganalysis, third International Conference on Internet Monitoring and Protection, 2008 IEEE, DOI 10.1109/ICIMP.2008.15

ABSTRACT

The steganography analysis of one public web site is subject of this paper. The steganography program tools available under domestic investigation conditions were used as a freeware software. The analysis results are presented and point out on deficiency of system providing the security, more exactly steganography software for our institutions.

STEGANOGRAPHY ANALYSIS OF ONE PUBLIC WEB SITE

Julijana Mirčevski, Nikola Popović