SocioBrains

ISSN 2367-5721 (online), JOURNAL HOMEPAGE: WWW.SOCIOBRAINS.COM
Publisher: SMART IDEAS – WISE DECISIONS, Ltd., Sofia, Bulgaria

ISSUE 82, JUNE 2021

OPPORTUNITIES FOR TRANSMISSION OF STEGANOGRAPHIC MESSAGES TROUGH ONLINE SOCIAL NETWORKS (OSN) AND INSTANT MESSAGING APPS ON MOBILE DEVICES

Abstract: The paper presents the results of experiments of hiding documents with trade secrets of business organizations through the program OurSecret in file containers of graphic type. The possibilities for hidden transmission by insiders of secret documents of business organizations through the e-mail platforms abv.bg, yahoo.com and google.com and transmission of graphic stegofiles through some of OSN and the mobile instant messaging applications VIBER and WhatsApp are shown. Insiders would prefer to use the capabilities of the VIBER messenger to transmit information instead via e-mails. The results can be used in organizing steganological protection of information of business organizations.

Author information:

Kristina Sandeva
graduating student i
n Department of Computer Systems and Technologies,
Faculty of Mathematics and Informatics
at Konstantin Preslavsky – University of Shumen
✉ kristina19_85@abv.bg
Bulgaria

Luchezar Hristov
PhD student
in Department of Management of Security Systems
at Konstantin Preslavky - University of Shumen
✉ luchano@abv.bg
Bulgaria

Stanimir Stanev
hon. Prof. PhD
in Department of Management of Security Systems
at Konstantin Preslavky - University of Shumen
✉ stanimstanev@gmail.com
Bulgaria

Keywords:
steganography,trade secrets, insiders,mobile instant messaging, steganological protection

Увод

В процесите на изследвания и иновации в стопанските организации се създава информация, която не попада в обхвата на защитата, предоставена от традиционните права на интелектуална собственост като патенти или авторски права. Независимо от това, тази информация е ценна за бизнес иновациите и конкурентоспособността. Поради това е важно да се запази такава информация като „поверителна“. Информацията, която се пази като поверителна, за да се запазят конкурентните печалби, се нарича „търговска тайна“ [1]. Търговските тайни са една от ценностите на днешната икономика на знанието, поради което са изложени на повишен риск.

Един от подходите за информационна сигурност е стеганографията, чрез която се цели конфиденциалността на тайна информация чрез скриване на нейното съществуване. Стеганографията (steganography) е научно-приложна област, съвкупност от технически умения и изкуство за начините за скриване на факта на предаване (наличие) на информация. В [2] е въведен терминът стегоинцидент. Това е криминална дейност по използване на стеганография за посегателство към чувствителна за дадена бизнес организация информация чрез образуване на секретен канал за изтичане или за несанкциониран достъп до нея. Стегоинцидентите са съзнателни, тайно извършвани противоправни обществени деяния, с които се нанасят вреди на интересите на атакуваната организация. Стеганологичната защита (стегозащита) е комплекс от организационни и апаратно-програмни мерки за предотвратяване на стегоинциденти. За да се организира такава защита е необходимо изследване на възможностите, които предоставят съвременните технологи за създаване на канали за изтичане на търговски тайни на бизнес организации, придобити незаконно от инсайдери [3].

Целта на настоящата работа е да покаже резултати от направени експерименти за проверка на такива възможности чрез услуги от он-лайн социалните мрежи и платформите за мигновени съобщения („месинджери“).

1. **Реализиране на стегоканали в он-лайн социални мрежи (ОСМ)**

За защита на търговските тайни на една бизнес организация, е целесъобразно ръководството на организацията да изготви списък на нейната чувствителната информация.

С цел изследване възможностите за защита на компютърните документи, от авторите са са определени документи, съдържащи търговски тайни за едно голямо търговско дружество от Шуменска област, имащо клонове у нас и чужбина. Като такива са определени следните категории търговска тайна:

- Финансова информация: в пълен обем с изключение на изисквани от държавата и задължително публикувани отчети, одити;
- Производствена информация: в пълен обем за технология, машинно оборудване, отчети и анализи по система за управление на качеството, ремонтна дейност, дейност в направление внедряване и развитие, договори с външни подизпълнители;
- Търговска информация: договори с клиенти, анализи продажби, финансови параметри по договори;
- Специфична информация: това са случаи на производство на продукция и компоненти по технология и параметри на външне клиент и под негова марка.

За експериментите са използвани следните образци от търговското дружество (Табл.1)

Таблица 1

Иденти-фикатор	**Образец документ**	**Компютърен формат**	**Страници (брой)**	**Обем в байтове**
st	Шаблон за трудов договор	**.docx**	3	158 084
dk	Декларация за конфиденционалност	**.docx**	3	43 520
dk1	Декларация за конфиденционалност	**.docx**	2	149 590
dd	Договор дестрибуция	**.pdf**	8	1 310 513
zo	Заявка за обучение	**.pdf**	1	173 409
rt	Разписание транспорт	**.pdf**	1	168 294
so	Справка отпуски	**.xlsx**	4-5	44 775

Тестовете са направени с избраната на базата на експертни препоръки, популярната в Интернет стегопрограма „OursSecret, която има предимството пред други подобни заради много удобния за потребителите интерфейс, цел определяне на възможността за стегоканали с електронна поща, ОСМ,VIBER и WHATSAPP, за коректен пренос на формирани с програмата стегофайлове със скрити съобщения.

За сравняване на използваемостта на контейнера от гледна точка на практиката е предложена характеристика – индекс на използваемост,

$$I_и = V_k / V_s,$$ където:

V_k - размер на контейнера в KB

V_s - размер на стегофайла в KB.

За сравняване на резултатите от гледна точка на практиката е избрана една важна характеристика - ефективността на вграждане,

$$E_e = V_m / V_s,$$ където:

V_m - размер на скритото съобщение в KB

V_s - размер на стегофайла в KB

Първата група тестове установи, че OurSecter е програма с добавяне, и с нея може да обработва информация, представена чрез файлове с формати от таблица 1.

Резултати от експерименти с използване на електронна поща за прехвърляне на прикачени .pdf файлове, обработени с програмата OurSecret между abv.bg и yahoo.com.ca дадени в табл.2.

Таблица 2

Контейнер	Съобщение	Стегофайл	E_e	$I_и$
zo.pdf : 173 409 Bytes	rt.pdf: 168 294 Bytes	zoS.pdf : 295 757 Bytes	**0,57**	**0,59**
.Jpg:962 445 Bytes	1 528 123 Bytes	2 087 929 Bytes	**0,73**	**0,46**

Чрез широко разпространените платформи за електронна поща – gmail, yahoo, abv и т.п. е възможна безпрепятствена стеганографска комуникация посредством прикачени към писмата мултимедийни обекти с вградени в тях съобщения.

От първите он-лайн социални мрежи - ОСМ, стартирани в Интернет през 1999 г., досега в киберпространството са известни над няколко стотин такива мрежи, най- популярни са Facebook, Twitter, Linkedin, Pinterest,Google Plus+, VK, и др. Разкриване на скритите канали в ОСМ изисква изучаването и тестването на различни стегано техники и софтуер в условията на платформите, предоставяни от операторите на мрежите. През 2011 год. са били направени изследвания в три социални мрежи – Facebook, Badoo и Google+[4]. От трите ОСМ, Facebook е сравнително най- добре защитена срещу използването й за стегокомуникации. Съвместни тестове на екипи от лаборатория „Компютърна сигурност“ на Шуменския университет и Дагестанския Унивеситет за народно стопанство, с участието на студенти от Русия и България, се проведоха за ОСМ - Facebook, Google+, Одноклассники, Вконтакте (VK), Мой Мир, Instagram, Tumblr и Linkedin [4]. Проведените експерименти потвърдиха,че не е възможно използването на безпрепятствена стеганография в албуми във Facebook и VK. При споделяне на снимки чрез Google+ е реализиран успешно целият цикъл на стеганографска комуникация от вграждане до извличане на скрити съобщения със формати JPEG, PNG, BMP и GIF [5].

На базата на получените резултати от направените опити може само да се предположи, че чрез някои от ОСМ може да се реализира стегоканал, но за това трябва да се правят експерименти за тяхното откриване.

2. Реализиране на стегоканали с приложения за мигновени съобщения

Разкритията на Едуард Сноудън изкараха много хора от заблудата им, че в Интернет пространството могат да се скрият от любопитните очи на хора, правителства, организации. Има обаче приложения и услуги, които гарантират сигурността на абонатите.

Популярни мобилни приложения за предаване на мигновени съобщения (т.н. „месинджъри“) са WhatsApp, Viber, Facebook Messenger, Snapchat, Instagram, Signal и Telegram. Общото между тях е предаването на изображения и видео информация и то в режим на мигновен трансфер. Съхраняването на тази информация в някои от приложенията е за кратък

период, което е предимство, поради факта че ако има наблюдател на скритата информация съществува вероятност, той да пропусне трансфера.

Всяко от посочените мобилни приложения има особености, които трябва да бъдат познавани, за да се използват за нуждите на конфиденциална комуникация [6].

От изследователски екип във Факултета АПВОКИС на НВУ“Васил Левски“- Шумен, са направени изследвания по възможностите чрез тези приложения да се създаде стегоканал за предаване на тайни съобщения.

След първоначално реализиране на сравнение е установено, че в различните приложни среди размерът на изображението се трансформира. WhatsApp коригира размерът на изображението до 1200 x 1600, Viber до 1024 x 1280, за Instagram тези автоматични корекции са до 3024 x 3780, а за Messenger-360 x 480. Чрез сравнение на статистическите характеристики на двойките изображения (контейнер и стегофайл) се установи, че Instagram запазва най-добри показатели на статистическите характеристики на изображенията, а тези на Viber водят до най-големи промени. Това би могло да подкрепи тезата, че Instagram би бил полезен за предаване на тайни съобщения чрез общодостъпни канали [6].

Тест1. WhatsApp канал Чужбина –Шумен- Чужбина (април 2021) чрез смартфони

Таблица 3

Име на оригиналния файл и размер (Bytes) (Москва)	**Размер на файла, получен в Шумен (Bytes)**	**Размер на файла, получен в чужбина след препращане от Шумен (Bytes)**	**Бележки**
konferencia.jpg 2 438 735	konferencia.jpg 275 274	konferencia.jpg 275 274	
mart.png 51 166	mart.jpg 184 650	mart.jpg 184 650	Смяна на формата **.png** в **.jpg**
kartaBG.bmp 350 518	kartaBG.jpg 77 540	kartaBG.jpg 77 540	Смяна на формата **.bmp** в **.jpg**

Тест 2.WhatsApp канал Чужбина –Шумен-Чужбина (април 2021) чрез инсталиран вариант на WhatsApp на компютри.

1. В контейнер konferencia.jpg с обем 275 274 Bytes е вложено текстово съобщение и е получен стегофайл konferenciaVS.jpg с размер 275 558 Bytes. Файлът е предаден чрез WhatsApp на компютъра по канал Шумен-Чужбина. В чужбина чрез инсталиран на компютър WhatsApp е получен файл с име konferenciaVS.jpg, но с размер 275 274 Bytes, съобщението липсва и не е открито там от програмата OurSecret (съобщение The file hides no data!).

2. В контейнер konferencia.jpg с обем 275 274 Bytes е вложено изображение stan.jpg с размер 792 939 Bytes и е получен стегофайл konferenciaS2.jpg с размер 1 065 006 Bytes. Файлът е изпратен чрез WhatsApp по канал Шумен-Чужбина. В Чужбина чрез инсталиран на компютър WhatsApp е получен файл с име konferenciaS2.jpg, но с размер 275 274 Bytes, съобщението липсва и не е открито там от програмата OurSecret (съобщение The file hides no data!).

Тест 3. Telegram канал Чужбина –Шумен- Чужбина на исталирани на компютри варианти на програмата. (април 2021г.)

А) Файл контейнер madara1.jpg с размер 1 921 076 Bytes е изпратен без вложено съобщение в режим на програмата Telegram „без компресия“. В Чужбина е получен файл madara1.jpg с размер 146 647 Bytes.

Б) Същият файл madara1.jpg с размер 1 921 076 Bytes без вложено съобщение е изпратен в режим „с компресия“. В Чужбина е получен файл madara1.jpg с размер 146 647 Bytes.

В) В контейнер madara1.jpg с размер 1 921 076 Bytes е вложено съобщение с размер 613 886 Bytes, и е изпратен стегофайл madaraRus.jpg с размер 1 921 076 Bytes в режим „без компресия“. В Чужбина е получен файл madaraRus.jpg с размер 146 647 Bytes.

Тест 4. С инсталирани на компютър програми Viber са проведени следните експерименти (Табл. 4).

В режим „инстант"

Таблица 4

Оригинален файл - подател	**Файл при получателя**	**Върнат файл при подателя**
madara1.jpg 1 921 076 Bytes	madara1p.jpg 218 897 Bytes (1200 X 1600)	madara1p.jpg 218 897 Bytes (1200 X 1600)
stan1.jpg 1 357 728 Bytes	stan1p.jpg 164 860 Bytes (1200 X 1600)	stan1p.jpg 164 860 Bytes (1200 X 1600)

1. **Контейнер:** madara1p.jpg - 218 897 Bytes, **съобщение**: stan1p.jpg-164 860 Bytes

Стегофайл (с „OurSecret“): madara1s.jpg – 382 287 Bytes, предаден в режим „Instant delivery“

Получен: madara1s.jpg – 232 483 Bytes , съобщение The file hides no data!.

2. **Контейнер:** madara1p.jpg - 218 897 Bytes, **съобщение**: stan1p.jpg-164 860 Bytes

Стегофайл (с „OurSecret“): madara1s.jpg – 382 287 Bytes, предаден в режим „Origial size”

Получен: madara1s.jpg – 382 287 Bytes ; Успешно извличане на съобщението (с „OurSecret“) - 164 860 Bytes.

Тест 5. От компютър в режим „Origial size” при предаване към смартфона Viber се осигурява стегоканал с използване на графични файлове, **предварително пропуснати** през Viber.

Табл. 5

Оригинален файл - подател	**Файл при получателя**	**Върнат файл при подателя**
brothers.jpg 6 096 697 Bytes	brothers.jpg 6 096 697 Bytes	brothers.jpg 6 096 697 Bytes
dog1.png 30 124 Bytes	dog1.png 30 124 Bytes	dog1.png 30 124 Bytes
zo.pdf 173 409 Bytes	zo.pdf 173 409 Bytes	zo.pdf 173 409 Bytes
st.docx 158 084 Bytes	st.docx 158 084 Bytes	т
so.xlsx 44 775 Bytes	so.xlsx 44 775 Bytes	so.xlsx 44 775 Bytes
rt.pdf 168 294	rt.pdf 168 294	rt.pdf 168 294

Тест 6. В режим „Origial size” е извършено предаване на стего файл от подател А към получател Б, той го декодира за да види коректността на извличането, след това Б връща същото стего към А. Резултатите са дадени в таблица 6.

Табл. 6

Контейнер подател А	**Съобщение Подател А**	**Стего от Подател А**	**Стего при Получател Б**	**Съобщ.След извличане**	**Обратно Изпратено Стего от Б**	**Получено Стего при А**	**Съобщ.След Извличане при А**
.png 30124	so.xlsx 44775	69672	69672	.xlsx 44775 коректно	69672	69672	44775 коректно
.jpg	so.xlsx 44775	3 045702	3 045702	44775	3 045702	3 045702	so.xlsx 44 775

При предаване в режим INSTANT не се осъществява стегоканал, изображенията се променят.

1.Експеримент за проверка на канала в режим „Origial size" дали има изкривяване на изображението след преминаване по канала.Изпратен от А файл **bbq1.jpg** с размер 3 006 162, получен при Б файл с размер 3 006 162. Б изпраща към А полученият файл с размер 3 006 162, този файл е получен при А със същия размер 3 006 162.

2.Експеримент за проверка на канала в режим „instant" на Viber дали има изкривяване на изображението след преминаване по канала.Изпратен от А файл **bbq1.jpg** с размер 3 006 162, получен при Б файл с размер 240292. Б изпраща към А полученият файл с размер 240292, този файл е получен при А със същия размер 240292.

3. Експеримент с предаване на стегофайл в режим „instant" на Viber.(табл. 7**)**

Табл. 7

Контейнер подател А	**Съобщение Подател А**	**Стего от Подател А**	**Стего при Получател Б**	**Съобщ.След извличане**
.jpg 240292	so.xlsx 44775	279832	240233	.не се извлича **The file hides no date**

4. Експеримент с предаване на стегофайл в режим „Origial size" на Viber. (табл.8)

Табл. 8

Контейнер подател А	**Съобщение Подател А**	**Стего от Подател А**	**Стего при Получател Б**	**Съобщ.След извличане**
.jpg 240292	so.xlsx 44775	.jpg 279832	.jpg 279832	so.xlsx 44775

5.Изпращане на документи на БО в режим „Origial size" на Viber. Резултатите са дадени в табл. 9.

Табл. 9

Контейнер подател А	**Съобщение Подател А**	**Стего от Подател А**	**Стего при Получател Б**	**Съобщ.След извличане**
.jpg 3 909 956	so.xlsx 44775	3 949 496	3 949 496	so.xlsx 44775
.jpg 3 909 956	zo.pdf 173 409	4 040 304	4 040 304	zo.pdf 173 409

Заключение

Направените експегименти доказват възможността за формиране на стегоканали чрез използване на платформите за електронна поща abv.bg, yahoo.com и google.com. Експерименти чрез предаване на стегофайлове - изображения с няколко приложения за мигновени съобщения показват възможността за предаване на скрити съобщения. Приложението WhatsApp не

позволява предаване на стегофайлове. За предпочитане е при предаване на информация – търговска тайна за БО по електронен път да се използват възможностите на месинджера VIBER, вместо чрез електронна поща. Резултатите от работата могат да се използват при организиране на стеганологична защита на информацията на бизнес организациите.

Стеганографията ще се развива в съответствие със степента на изучаването на средата, в която се предават секретните съобщения. Като се има предвид динамично променяща се среда за сигурност, анализът в бъдеще на възможните стеганографски атаки към чувствителна икономическа информация ще даде възможности за организирането на нейната ефективна защита.

References:

1. **Fact Sheet Trade secrets: An efficient tool for competitiveness, 2017**. European IPR Helpdesk. June .
2. **Stanev,S., 2013:** Steganologichna zashtita na informatsiyata.Universitetsko izdatelstvo "Episkop KonstantinPreslavski",Shumen. ISBN 978-954-577-825-4. 320 pages.
3. **Hristov,L., S.Stanev i H.Hristov,2018:**Sredstva za zashtita na chuvstvitelnata informaciya na fermata ot vutreshni zlozhelateli (insajderi). In: Sbornik nauchni trudove na mezhdunarodna nauchna konferenciya MATTEH 2018.Tom2,Part1.Shumen. pp.109-115. ISBN 1314-3921.
4. **Galyaev,V.,2014:** O nekotoryh eksperimentah po peredache stegosoobshtenij cherez socialnye seti. In: Sbornik nauchni trudove na mezhdunarodna nauchna konferenciya MATTEH 2014.Tom1,Shumen. pp.119-122. ISBN 1314-3921.
5. **Emiov,D, S. Hasanova and D.Tonchev,2014**: Steganografiya v on-lajn socialnite mrezhi. In: Sbornik nauchni trudove na mezhdunarodna nauchna konferenciya MATTEH 2014.Tom1,Shumen. pp. 173-178. ISBN 1314-3921.
6. **Stoyanova,V.,2017:** Vuzmozhnosti za poluchavane na konfidencialna informaciya chrez mobilni ustrojsytva. https://cio.bg/digitalizacia/2017/07/25/3434757_vuzmojnosti_za_poluchavane_na_konfidencialna/