Scientific and Practical Cyber Security Journal (SPCSJ) 4(4): 15-23 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

OPEN-SOURCE INTELLIGENCE.

ინფორმაციის ღია წყაროებში მოპოვება.

გიორგი იაშვილი - კავკასიის უნივერსიტეტი
Giorgi Iashvili – Caucasus University
რეზიკო ჩალაძე (N20-ე საჯარო სკოლა)
Reziko Chaladze (N20 public school)
დავით ბეგაშვილი (N87-ე საჯარო სკოლა)
Davit Begashvili (N87 public school)
ვიქტორია საგრადიანი (N157 საჯარო სკოლა)
Viktoria Sagradian (N157 public school)
ლუკა სანარსკი (N199 საჯარო სკოლა)
Luka Sanarski (N199 public school)

ABSTRACT: In the following article you will learn about the usage of open-source intelligence. How dangerous it could be to leak wrong information or how it could be used in ethical hacking. In addition, known attacks using similar techniques will be discussed. Finally you will see recommendations to better protect our identity.

აბსტრაქტი: მოცემულ სტატიაში თქვენ გაეცნობით ინფორმაციის ღია წყაროებიდან მოპოვებას და მათ გამოყენებას. თუ რა საფრთხის შემცველი შეიძლება გახდეს არასწორი ინფორმაციის გაჟონვა ან როგორ შეიძლება ის გამოვიყენოთ ეთიკურ ჰაკინგში. ამასთანავე განხილული იქნება მსგავსი ტექნიკით განხორციელებული ცნობილი შეტევები. საბოლოოდ კი შეხვდებით რეკომენდაციებს საკუთარი იდენტობის უკეთესად დასაცავად.

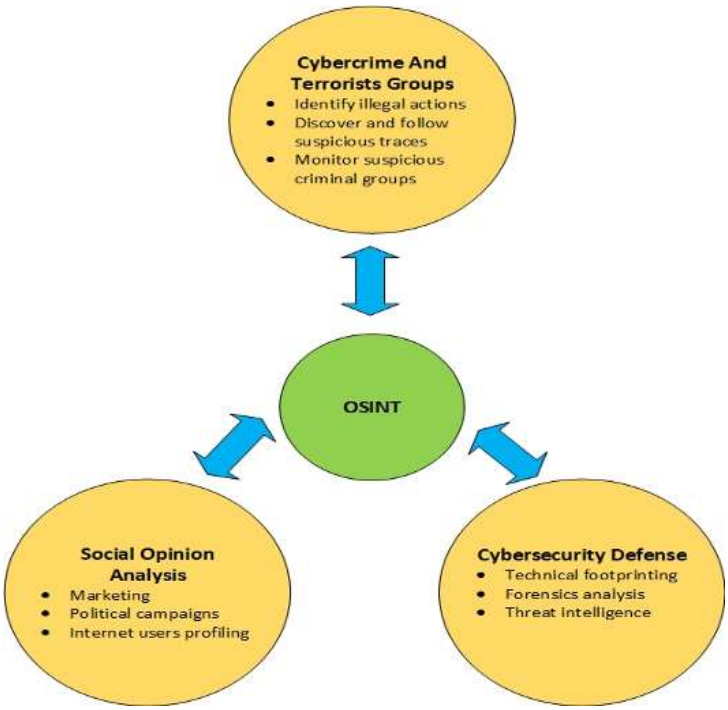
KEYWORDS: *open-source intelligence, social engineering, OSINT, informational leaks*

საკვანძო სიტყვები: *ღია წყაროებში ინფორმაციის მოპოვება, სოც. ინჟინერია, OSINT, ინფორმაციის გაჟონვა*

შესავალი

ტექნოლოგიურმა განვითარებამ შეცვალა ადამიანის ცხოვრების სტილი და ინტერესები. გააუმჯობესა კომუნიკაციის საშუალებები და ინტერნეტთან წვდომა. მეცნიერების აზრით 2030 წლისთვის ადამიანთა 90% გამოიყენებს ინტერნეტს(დაწყებული 6 წლიდან და ზევით). ინტერნეტმა უკვე ფართო დანიშნულება მიიღო, რომელიც ადამიანის ცხოვრებას დღითი-დღე ამარტივებს. პოპულარული გახდა სოციალური ქსელები სადაც ადამიანები წერენ საკუთარი თავის შესახებ, უზიარებენ ერთმანეთს ფოტოებს, ვიდეოებს, სიახლეებს და ა.შ. მომხმარებლები პირად ინფორმაციას საჯაროდ დებენ: სახელი, გვარი, საკონტაქტო ნომერი, საკონტაქტო მეილი, მიღებული განათლება, სამუშაო ადგილი და ა.შ. მაგრამ ამ ინფორმაციის გაზიარებისას ადამიანთა უმრავლესობა ვერ აანალიზებს მისგან გამოწვეულ შესაძლო პრობლემებს. თუ როგორ შეიძლება იყოს ეს ინფორმაცია მათ საზიანოდ გამოყენებული. ხოლო სანამ ამ თემაზე გადავალთ საჭიროა კარგად გავაანალიზოთ რა არის **ღია წყაროებში არსებული ინფორმაცია(OSINT)**.

ღია წყაროებში არსებული ინფორმაცია(OSINT) ეს არის საჯაროდ ხელმისაწვდომი ინფორმაციის მოპოვება, ანალიზი და ექსპლუატაცია მრავალმხრივი მეთოდების გამოყენებით. ის შეიძლება მოძიებული იყოს ინტერნეტშიც და მის გარეთაც(ტელევიზია, რადიო, გაზეთები, ჟურნალები, სტატიები და ა.შ).



როგორც ამერიკის შეერთებული შტატების თავდაცვის სამინისტრო ამბობს:

„ღია წყაროში არსებული ინფორმაცია(OSINT) არის ინფორმაცია, რომელიც წარმოებულია საჯაროდ ხელმისაწვდომი ინფორმაციისგან და არის შეგროვებული, ექსპლუატირებული და გავრცელებული შესაბამის აუდიტორიებში კონკრეტული ინფორმაციული მოთხოვნის გადასაჭრელად.“

ამასთანავე ინფორმაციის გაჟონვის ერთ-ერთი წყარო შეიძლება იყოს სოციალური ინჟინერია. სოც. ინჟინერიაარის ფსიქოლოგიური მანიპულაცია და შეტევა , რომლის დროსაც გარეშე პირი სისტემაზე ან ქსელზე მონოპოლირების მოპოვების მიზნით ანხორციელებს მოტყუების სხვადასხვა გზით მომხმარებლის გამოკითხვას და შემდეგ მიღებული ინფორმაციის გამოყენებას.

OSINT – ი შეგვიძლია დავყოთ რამოდენიმე პირობით ეტაპზე:

- იმის გარკვევა, რომ ინფორმაცია არის ღია წვდომაში
- ინფორმაციის მოგროვება
- ინფორმაციის ანალიზი ან/და გამოძიება

ინფორმაციის მოგროვების რამდენიმე ხერხი არსებობს

- პასიური მოგროვება

ეს არის OSINT – ში ყველაზე გამოყენებადი ინფორმაციის მოგროვების მეთოდი. რეალურად, მონაცემთა მოგროვების ნებისმიერი სქემა უნდა იყენებდეს პასიურ მეთოდს, რადგან OSINT – ის ერთ-ერთი მთავარი დანიშნულებაა ინფორმაციის მხოლოდ ღია წყაროებიდან მოგროვება.

- საშუალოდ პასიური მოგროვება

ტექნიკური თვალსაზრისით, ინფორმაციის მოგროვების ამ ხერხში ზოგადი ინფორმაციის მისაღებად, სამიზნე სერვერთან იგზავნება შეზღუდული ოდენობის ტრაფისი. გაგზავნილი ტრაფიკი მაქსიმალურად ცდილობს დაემსგავსოს ჩვეულებრივ ინტერნეტ ტრაფიქს. ეს კეთდება იმისათვის, რომ სისტემამ სერვერზე ინფორმაციის მოგროვების აქტივობა ვერ აღმოაჩინოს. ამ შემთხვევაში არ ხდება სამიზნის სიღრმისეული შესწავლა, ყველა ქმედება ტარდება ზედაპირულად.

- აქტიური მოგროვება

ამ შემთხვევაში საჭიროა უშუალო ურთიერთქმედება სისტემასთან. ამ პროცესის დროს მსხვერპლი ხვდება, რომ სისტემაში ხდება ინფორმაციის მოგროვება. აქტიური მოგროვების პროცესი მოიცავს ღია პორტების სკანირებას, ინფორმაციის მიღებას მსხვერპლის IT ინფრასტრუქტურის შესახებ, მოწყვლადობების სკანირებას, ისეთების როგორიცაა სისტემის გაუნახლებელი ვერსიები, ვებ სერვისის სკანირებას და ა.შ. ეს ტრაფიკი აისახება სისტემაში როგორც საეჭვო ან მავნე ქმედება და იქნება დაფიქსირებული მსხვერპლის IDS – ის ან IPS – ის მიერ. სოციალური ინჟინერიის თავდასხმაც შეიძლება ჩაითვალოს აქტიური ინფორმაციის მოგროვების მაგალითად.

- ამასთანავე სოციალურ ქსელებში ხშირად დიდი კვალი იტოვება ჩვენი პირადი ინფორმაციის შესახებ როგორიცაა: ტელეფონის ნომერი,მეილი,საცხოვრებელი ადგილი,ოჯახის წევრები და სხვა.

როდესაც ჩვენ კონკრეტული პიროვნება გვყავს სამიზნედ მისი პირადი ინფორმაცია შეიძლება ერთ კონკრეტულ რომელიმე სოც. ქსელში არ ჰქონდეს

და სხვა სოც. ქსელში დარჩენილი იყოს ის ინფორმაცია რაც ჩვენ გვჭირდება მის შესახებ ამისთვის გამოიყენება ხელსაწყო https://checkusernames.com/ რომლის საშუალებითაც

ჩვენ სახელი და გვარით ვეძებთ სხვადასხვა სოციალურ ქსელებში, თუ მაგალითად facebook ზე არაქვს დატოვებული კონკრეტული ინფორმაცია შეიძლება ეს ინფორმაცია სხვა რომელიმე სოც.ქსელში ქონდეს დატოვებული

და ამიტომ საჭიროა მისი სხვა სოციალური ქსელების დათვალიერება.

ღია წყაროში მოპოვებული ინფორმაციის გამოყენება

ღია წყაროში უამრავი ინფორმაციის მოპოვებაა შესაძლებელი მაგრამ მათი გამოყენება ორგვარად შეიძლება. ინფორმაციის გამზიარებლის სასიკეთოდ ან პირიქით მათსავე საზიანოდ.

რა იგულისხმება ინფორმაციის გამზიარებლის სასიკეთოდ გამოყენებაში?! ეს არის სოციალურ მედიაში მომხმარებლის მიერ საკუთარ თავზე გაზიარებული ინფორმაცია რომელიც შეიძლება შეიცავდეს განათლების დონეს, სამუშაო გამოცდილებას და ა.შ. ეს დიდ კომპანიებს კი ყავთ HR რომელიც ზუსტად ამ მეთოდის გამოყენებით ეძებს სამომავლოდ თანამშრომლებს ანდაც ამომავალ ტალანტებს.

მეორე მხრივ, OSINT შესაძლოა იყოს გამოყენებული ბოროტმოქმედების მიერ, რომლებიც აგროვებენ ინფორმაციას პოტენციური მსხვერპლის შესახებ და მიღებულ მონაცემებს შემდგომ სხვადასხვა ტიპის თავდასხმისთვის იყენებენ. მსგავსი ქმედების ერთ-ერთ მაგალითად შეიძლება ჩაითვალოს სოციალური ინჟინერია, რომლის გამოყენების დროსაც ბოროტმოქმედი ახდენს ფსიქოლოგიურ ზეწოლას პოტენციურ მსხვერპლზე, სასარგებლო ან სენსიტიური ინფორმაციის მისაღებად (მაგ. პაროლი ან საბანკო მონაცემები).

სოციალური ინჟინერიის განხრები და მათი ანალიზი

- **სოციალური ინჟინერიის განხრებია:**

Phishing, Spear Phishing, Vishing , Pretexting, Baiting, Tailgating, Quid pro quo. აქ განვიხილავთ რამდენიმე მათგანს.

- **Vishing (Voice Phishing)**

სოციალური ინჟინრები შეიძლება ყველგან იყვნენ ინტერნეტში. Vishing-ის დროს იყენებენ ტელეფონს. ტელეფონის საშუალებით ფიშერები სათაღლითოდ იყენებენ IVR ტექნიკას (Interactive Voice Response). ისინი ხელახლა ქმნიან იმ ხმას, სატელეფონო საჟღერადო ტონს, რომლებიც განეკუთვნებიან ბანკებს ან სხვადასხვა კომპანიებს. თავდამსხმელი თხოვს მსხვერპლს შეიყვანოს პირადი ინფორმაცია, რის შემდეგაც იმახსოვრებენ პინ კოდებს, ანგარიშის პაროლებსა და სხვა და სხვა ინფორმაციას.

- **Baiting**

Baiting არის სოციალური ინჟინერიის ერთ-ერთი განხრა. ამ დროს თავდამსხმელი ტოვებს დაინფიცირებულ CD დისკებს ან USB-ებს, საჯარო ადგილებში იმ იმედით რომ რომელიმე გამვლელი აიღებს ცნობისმოყვარეობის გამო და გამოიყენებს თავის მოწყობილობაზე. მაგალითად ქმნიან დისკს რომელსაც ახატავენ რაიმე პოპულარული ბრენდის ლოგოს, წერენ იგივე საინსტალაციო ფაილს ოღონდ სინამდვილეში ვირუსებით სავსეს. შემდეგ, მათ ტოვებენ ბარებში, მეტროს, ავტობუსის ან ტაქსის სკამებზე. მსხვერპლი აერთებს ნაპოვნ მოწყობილობას თავის მანქანაზე და ჰგონია რომ 100$-იანი პროგრამა უფასოდ იშოვა მაგრამ სინამდვილეში ის საკუთარ მოწყობილობაზე წვდომას აძლევს ბოროტმოქმედს.

- **Tailgating**

ერთ-ერთი ფართოდ გავრცელებული სოციალური ინჟინერიის განხრაა Tailgating (piggybacking). Tailgating არის ფიზიკური უსაფრთხოების დარღვევა როდესაც ადამიანი რომელსაც არ აქვს შესვლის უფლება მიყვება ადამიანს რომელსაც აქვს საშვი დაცულ ადგილას

შესასვლელად. მაგალითად შეიძლება კარი დაუჭიროს თავდამსხმელს თანამშრომელმა და ასე შეუშვას. თუ ეს კომპანია დიდია დიდი ალბათობაა იმისა რომ შემოჭრილი ადამიანი გეგონება თანამშრომელი, სწორედ ამიტომ ასეთი თავდასხმები ხშირად წარმატებული არის.

- **Quid pro quo**

ერთ-ერთი სოციალური ინჟინერიის განხრაა Quid pro quo. ამ დროს ხალხს სთავაზობენ ტექნიკურ დახმარებას. ისინი შემთხვევითობის პრინციპით ურეკავენ რომელიმე კომპანიის თანამშრომელს და ეუბნებიან რომ რაღაც პრობლემის გამო უკავშირდებიან. ზოგჯერ ეძლევათ საშუალება მსხვერპლს გააკეთებინონ ის რაც მოუნდებათ. Quid pro quo ასევე შეიცავს რაღაც დახმარების გაწევას სამიზნისთვის რომ მიიღონ პირველ რიგში ნდობა ხოლო შემდეგ საჭირო ინფორმაცია. მაგალითად თავდამსხმელი ცდილობს მოაგვაროს მსხვერპლის რომელიმე პრობლემა. ასევე შეიძლება იყოს რაიმე მატერიალური შეთავაზება რომელიც გულისხმობს საჩუქარს ინფორმაციის სანაცვლოდ.

„საუკეთესო თავდაცვა არის კარგი OSINT"

დღესდღეობით ხშირი გახდა საჯაროდ გაზიარება ამა თუ იმ პროგრამის სისუსტეების შესახებ. ალბათ ადამიანი იფიქრებს: „რა არის ამაში ცუდი, ისინი გვაჩვენებენ რომ ანახლებენ პროგრამას და ზრუნავენ მომხმარებლის დაცულობასა და კომფორტზე." მართალიც იქნება მაგრამ აქ არის ერთი დიდი მაგრამ. არსებობს ხალხის კატეგორიაც რომელიც ვერ ახერხებს ამ განახლების ინსტალაციას და არჩევს ძველ ვერსიაზე დარჩენას. სისუსტის გაზიარებით შეიძლება ითქვას რომ ჰაკერს ლანგრით ვართმევთ შეტევის გზას ან იდეას. თავდამსხმელი მარტივად გამოიყენებს ამ სისუსტეებს და შეძლებს ან მომხმარებლის კომპიუტერზე წვდომის მიღებას ან მომხმაებლის პირადი ინფორმაციის ნახვას ანდაც ყველაზე უარეს შემთხვევაში ამ პროგრამის მონაცემთა ბაზებზე წვდომას.

ამიტომ როდესაც ზოგიერთი კომპანია ხმარებაში უშვებეს განახლებას, აიძულებეს მომხმარებელს რომ მათ მხარესაც განახლდეს პროგრამა რათა არ მოხდეს მსგავსი ინციდენტები.

ყველა დროის 3 საუკეთესო შეტევა სოც. ინჟინერიით

1. **ტოიოტა, 2019**

2019 წელს ტოიოტა ბოშოკუ კორპორაციაზე მოხდა თავდასხმა სოც ინჟნერიის გამოყენებით. ჰაკერების მსხვერპლი გახდა აუტო ნაწილების მიმწოდებელი. მას გაუგზავნეს საქმიანი მეილი

რომლის დახმარებითაც მსხერპლი დარწმუნეს რომ ადრესატის საბანკო ანგარიშის ინფორმაცია შეეცვალა. საბოლოოდ კი ტოიოტამ 37მილიონი ამერიკული დოლარით იზარალა.

2. ამერიკის დემოკრატიული პარტია, 2016

ერთ-ერთი დასამახსოვრებელი სოც. ინჟინერიის შეტევა მოხდა 2016 წელს აშშ-ში საპრეზიდენტო არჩევნების წინ. რომელმაც არჩევნების შედეგზეც იმოქმედა და დონალდ ტრამპს დაეხმარა გამარჯვებაში.

ჰაკერებმა შექმნეს ტყუილი ანგარიშები რომლითაც დემოკრატიული პარტიის წევრებს გაუგზავნეს ლინკი უჩვეულო საქმიანობის გამო. ამის შემდეგ კი მათ მიიღეს წვდომა ასობით მაილზე და მათზე არსებულ მგრძნობიარე ინფორმაციაზე.

3. RSA, 2011

RSA არის საჯაროდ ცნობილი კრიპტოსისტემა რომელიც უზრუნველყოფს მონაცემების დაცულად მიმოცვლას. 2011 წელს მათ მოუწიათ 66 მილიონი დოლარის დახარჯვა დაცვის სისტემისათვის. ამის მიზეზი კი გახდა ერთ-ერთი თანამშრომლისათვის ექსელის ფაილის გაგზავნა სახელით ,,სამუშაო გეგმა“. რომელიც შეიცავდა ვირუსს და გზა გაუხსნა ჰაკერებს.

როგორ უნდა დავიცვათ თავი

- **წესი #1:** დავაყენოთ ძლიერი პაროლები და უმჯობესი იქნება თუ 3 თვეში ერთხელ შევცვლით პაროლებს.
- **წესი #2:** Facebook - ზე თქვენი კონფიდენციალურობის პარამეტრების არჩევისას გახადეთ თქვენი პოსტები ხილვადი მხოლოდ თქვენი მეგობრებისათვის. დარწმუნდით, რომ თქვენი დასტურის გარეშე თქვენს გვერდზე არ გამოჩნდება პოსტები, რომლებზეც მონიშნული ხართ.
- **წესი #3:** კარგი იქნება თუ დამალავთ თქვენს საცხოვრებელ მისამართს, ტელეფონის ნომერს, ელექტრონული ფოსტის მისამართს და სხვა მონაცემებს (ან არასდროს შეიყვანოთ ისინი რადგან Facebook ხშირად მას მესამე პირებს ჰყიდის).
- **წესი #4:** შეზღუდეთ თქვენი პროფილის მოძებნის შესაძლებლობა და მონიშნეთ ,,მხოლოდ მეგობრები“. ყოველთვიურად წაშალეთ თქვენი Facebook მიმოწერის კონტენტი. იმ შემთხვევაში, თუ პროფილს მოგპარავენ, ვერ შეძლებენ სენსიტიური ინფორმაციის მოპოვებას თქვენი პირადი მიმოწერიდან.

- **წესი #5:** გამორთეთ პერსონალიზებული რეკლამები (Personalized ads).
- **წესი #6:** თქვენი სმარტფონით გადაღებული ფოტოები ბევრ სენსიტიურ მონაცემს შეიცავს მათი გადაღების დროისა და ადგილის შესახებ. თუ შესაძლებელია, არ გააზიაროთ ისინი პირდაპირ სოციალურ მედიაში ან გამორთეთ თქვენი ფოტოების ადგილმდებარეობა. გარდა ამისა, შეამცირეთ ფოტოს ზომა და დაარედაქტირეთ ის (რაც დააზიანებს ფოტოს მეტამონაცემებს).
- **წესი #7:** LinkedIn ხშირად გამოიყენება პერსონალური მონაცემების შესაგროვებლად. თუ თქვენთვის საჭიროა აღნიშნული ქსელის გამოყენება, განათავსეთ მხოლოდ საჯაროდ არსებული ინფორმაცია. გადაამოწმეთ რა ინფორმაცია გაქვთ აქამდე გაზიარებული LinkedIn-ზე.
- **წესი #8:** გაითვალისწინეთ, რომ ყველაფერი, რასაც სოციალურ მედიაში აქვეყნებთ, „ვირტუალურად წაუშლელ“ ინფორმაციად იქცევა, რომელიც თქვენს მოწინააღმდეგეებს გამოადგებათ გამოქვეყნებიდან წლების შემდეგ. შესაბამისად, არ გამოაქვეყნოთ თქვენი სახლის, თქვენი შვილებისა და ახლო მეგობრების ან ნათესავების ფოტოები. გირჩევთ, რომ გადახედოთ ყველა თქვენს ფოტოს Facebook-ზე, Twitter-ზე და Instagram-ზე და წაშალოთ ისეთები, რომლებიც გამოავლენენ იმ ადგილების ან ადამიანების იდენტობას, რომლების გსურთ, რომ დაიცვათ.
- **წესი #9:** დაუთმეთ რამდენიმე საათი თქვენს შესახებ იმ ინფორმაციის ამოსარჩევად, რომელიც, თქვენი აზრით, პირადი ან სენსიტიურია და მოძებნეთ ის Google-ის მეშვეობით, რათა დარწმუნდეთ, რომ სადმე არ გამოჩნდება. ამგვარი მოქმედებით ასევე გაიგებთ, თუ რა ინფორმაციაა საჯაროდ ხელმისაწვდომი ღია წყაროებში თქვენს შესახებ.
- **წესი #10:** გააქტიურეთ Google Alerts შეტყობინების ფუნქცია, რომელიც ელ-ფოსტაზე გამოგიგზავნით შეტყობინებებს, თუ თქვენი სახელი (ან თქვენი სახელის, თანამდებობის, ან თქვენი თანამშრომლის კომბინაცია) რომელიმე ვებსაიტზე ჩნდება. შედეგები არ მოიცავს სოციალურ მედიას.

Acknowledgement

The work was conducted as a part of SPG-19-133 financed by Shota Rustaveli National Science Foundation of Georgia.

ბიბლიოგრაფია

1. R. Layton P. Watters - Automating Open Source Intelligence – 2015
2. N. A. Hassan, R. Hijazi - Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, 2018
3. A., Babak, B., P. Saskia, S., Fraser - Open Source Intelligence Investigation, 2016