Scientific and Practical Cyber Security Journal (SPCSJ) 4(1): 71 – 74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

„GozNym“-ი ტრანსნაციონალური კიბერდანაშაულისთვის”
“GozNym” for transnational cybercrime“

ნათია ფილაშვილი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი
მარიამ კიკლიაშვილი
ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.

Natia Pilashvili
Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
Mariam Kikliashvili
Ivane Javakhishvili Tbilisi State University, Sociology_Junior;

ანოტაცია: XXI საუკუნეში, სწრაფი ტექნოლოგიური პროგრესის პარალელურად, გამოუვლენელი და გაუხსნელი დანაშაულების ყველაზე მზარდი ტენდენცია კიბერდანაშაულის კუთხით აღინიშნება, რომელსაც ხშირად „მომავლის დანაშაულსაც“ უწოდებენ. მავნე პროგრამები, რომლებიც კიბერდანაშაულის ერთ-ერთი მთავარი მექანიზმია, თითოეულ ჩვენგანს მათ მსხვერპლად ადვილად გვაქცევს. მაშინ, როდესაც კიბერდანაშაული და ტანსნაციონალური დანაშაული ერთად მოქმედებს, საქმე გვაქვს მასშტაბურ, გლობალურ დანაშაულთან, რომელთან ბრძოლაც გაცილებით რთულია. სწორედ, ერთ-ერთი ასეთი ტრანსნაციონალური კიბერდანაშაულის იარაღს წარმოადგენდა „GozNym“-ის მავნე პროგრამა, რომლის საშუალებითაც 41 000 ათასზე მეტი ადამიანი ფინანსურად დაზარალდა.

Annotation: In the 21st century, in parallel with rapid technological progress, the increasing trend of unsolved and inexcusable crimes is marked by cybercrime, often referred to as "the crime of the future." Malicious software, one of the key mechanisms of cybercrime, makes it easy for us to be victims of it. While cybercrime and transnational crime work together, we are dealing with large-scale, global crime that is far more difficult to combat. One of these transnational cybercrime weapons was „GozNym’s” malicious program that has affected more than 41,000 people financially.

საკვანძო სიტყვები: კიბერდანაშაული, დისტანციური მართვის მექნიზმი(RAT), „ტროიანი“,

„GozNym”, „ტრანსნაციონალური დანაშაული“.

„GozNym“-ი ტრანსნაციონალური კიბერდანაშაულისთვის”

დღეს ტრანსნაციონალური დანაშაული მსოფლიოს წინაშე მდგარი უდიდესი გამოწვევაა. ის ორგანიზებული დანაშაულის ერთ-ერთ ფორმას წარმოადგენს, რაც თავის მხრივ გულისხმობს მართლსაწინააღმდეგო ქმედებას, რომელიც ადამიანთა ჯგუფის მიერ ხორციელდება არა ერთჯერადად, არამედ დროის გარკვეული პერიოდის განმავლობაში. დანაშაულის ჩადენა წარმოადგენს მუდმივ საერთო საქმეს ორგანიზებული სუბიექტებისთვის, რომელთა შორის თითოეულს გააჩნია საკუთარი ფუნქციონალური ვალდებულებები, „უფლებები და მოვალეობები“. ტრანსნაციონალურ დანაშაულს 4 ძირითადი თვისება ახასიათებს, რომელთაგან მეოთხე, სახელმწიფო საზღვრების იგნორირება, მას სხვა სახის ორგანიზებული დანაშაულებისგან გამოარჩევს. ეს თვისებებია:

1) ორგანიზაციის არსებობა ან მასში მონაწილეობა

2) უწყვეტობა

3) საქმიანობის მიზნად მოგების მიღების დასახვა

4) მისი მიღწევის ხერხები, რომლებიც ეყრდნობა სახელმწიფო საზღვრების იგნორირებას.

იმ დროს, როდესაც ხდება ტრანსნაციონალურ და კიბერდამნაშავეთა ურთიერთგადაკვეთა, საქმე გვაქვს გლობალურ მასშტაბზე გათვლილ დანაშაულებრივ სქემასთან.

სწორედ, ერთ-ერთი ასეთი კომპლექსური ტრანსნაციონალური კიბერდანაშაულის შემთხვევაა „GozNym“-ის მავნე პროგრამის გამოყენება აშშ-სა და მსოფლიოს სხვადასხვა ქვეყანაში მცხოვრები ადამიანებისთვის საბანკო ანგარიშებიდან 100 მლნ. აშშ დოლარის მოსაპარად. „GozNym“-ი მიეკუთვნება ეგრეთ წოდებული „ტროიანის“, იგივე „ტროას ცხენის“ მავნე პროგრამას. „ტროიანი“ ისეთი მავნე კომპიუტერული პროგრამაა, რომელიც ერთი შეხედვით უვნებლად გამოიყურება, ან თავს ინიღბავს ყველასთვის კარგად ცნობილ პროგრამად; რამდენადაც მომხმარებლები ცნობილი პროგრამების ინსტალირებას არ ერიდებიან, ისინი საკუთარი ნებით საშუალებას აძლევენ „ტროას ცხენს“ მათ კომპიუტერულ სისტემაში შესვლის. აღსანიშნავია, რომ მის მიზანი არაა საკუთარი თავის რეპლიკაცია, არამედ ჰაკერები მას იყენებენ, როგორც კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმს (RAT -Remote Administration Tool).

„GozNym“-ი ორი მავნე პროგრამის ერთობლიობაა: „Gozi ISFB“ (ასევე ცნობილია, როგორც Ursnif) და „Nymaim“. „GozNym“–ს ჰაკერები იყენებენ ბანკების, ელექტრონული კომერციის პლატფორმების, საკრედიტო კავშირებისა და სხვა ბიზნეს ანგარიშებიდან ფულის მოსაპარად. ეს მავნე პროგრამა განსაკუთრებით საშიშია, რადგან მას შეუძლია თავიდან აიცილოს ანტივირუსული პროგრამების ეფექტი. უამრავი ადამიანი იყენებს ერთი და იგივე პაროლს მრავალი ანგარიშისთვის. ამიტომ, საბანკო ანგარიშის გატაცებისა და მთელი პროფილის

შემოწმების შემდეგ, კიბერ დამნაშავეებმა შესაძლოა ასევე მიიღონ წვდომა მსხვერპლთა ელ. ფოსტის მისამართებზე და საბოლოოდ, სხვა პირად ანგარიშებზე.

აღნიშნული დანაშაულებრივი ქსელი და მისი ლიდერი, ზედმეტსახელად „None"-ი, რომელიც პროკურატურის ცნობით ეროვნებით ქართველია, ახორციელებდა ათასამდე კომპანიის კომპიუტერულ სისტემაში უნებართვო შეღწევას, კომპიუტერული სისტემიდან კომპიუტერული მონაცემების უნებართვოდ მოპოვებასა და მათი უკანონოდ შენახვა-გავრცელებას, კომპიუტერული მონაცემისა და კომპიუტერული სისტემის უკანონოდ გამოყენებას. აღნიშნული გლობალური დანაშაულებრივი ქსელის მსხვერპლი 41 000-ზე მეტი კომპანია გახდა.

დაჯგუფებამ მომხმარებლების კომპიუტერი „GozNym"-ის ვირუსით დააინფიცირა, რითაც მათ წვდომა მოიპოვეს ინტერნეტ ბანკის მონაცემებზე, შემდეგ კი მოპარული თანხების ლეგალიზებას უცხოურ ბენეფიციარ ბანკებში არსებული ანგარიშების საშუალებით ახორციელებდნენ. დანაშაულებრივი ქსელის ფორმირება იატაკქვეშა რუსულენოვან ინტერნეტ ფორუმებზე მოხდა, სადაც ჰაკერებმა ჯგუფში მოსახვედრად საკუთარი ტექნიკური შესაძლებლობები გამოიყენეს. დაზარალებულები ფიქრობდნენ, რომ ინტერნეტში მარტივ ოპერაციას ახორციელებდნენ, რა დროსაც კიბერ დამნაშავეები მათ სენსიტიურ და პირად ინფორმაციაზე წვდომას იღებდნენ. დაზარალებულთა შორის სხვადასხვა ქვეყნის არაერთი იურიდიული თუ საქველმოქმედო ორგანიზაციაა.

შეერთებული შტატების ხელმძღვანელობით ჩატარებულ საერთაშორისო ოპერაციაში საქართველოს, უკრაინის, მოლდოვის, გერმანიისა და ბულგარეთის პროკურატურები მონაწილეობდნენ. საქმეში აქტიურად ჩაერთნენ საერთაშორისო ორგანიზაციები - „ევროჯასტი" და „ევროპოლი", რომელთა ინიციატივით არაერთი შეხვედრა დაიგეგმა და შედგა ჰააგაში. საერთაშორისო გამოძიების ფარგლებში ბრალი 10 პიროვნებას წარედგინა. საქმის გამოძიება 2 წლის განმავლობაში მიმდინარეობდა და მხოლოდ 2019 წლის მაისში გაიხსნა. პირი, რომელმაც ვირუსი ისე დაშიფრა, რომ ის ქსელში შესამჩნევი არ ყოფილიყო, მართლმსაჯულების წინაშე მოლდოვაში წარდგა. თუმცა დღემდე ქსელის რამდენიმე წევრი კვლავ ძებნაშია.

ნებისმიერი კიბერდანაშაულის შემთხვევა განსაკუთრებით კი გლობალური, ტრანსნაციონალური კიბერდანაშაულები, კარგად გვიჩვენებს, თუ როგორი საფრთხის წინაშე დგას ნებისმიერი ჩვენგანი ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან გადაჯაჭვული ცხოვრების გამო, რაც დღევანდელობის განუყოფელი ნაწილია. ყოველი ახალი შემთხვევა საჭიროა იყოს ჩვენთვის მაგალითი იმისთვის, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე ინტერნეტ სივრცეში ყოფნის დროს, რათა არ გავხდეთ უნებლიედ თუ „ჩვენივე ნებით" ჰაკერებისა და მავნე პროგრამების მორიგი მსხვერპლი.

ბიბლიოგრაფია

1. „GozNym virus removal guide“ Written by Tomas Meskauskas on 03 September 2019
2. „GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION“ 16 MAY 2019
3. „Cybercrime Gang Behind GozNym Banking Malware Dismantled“ May 16, 2019
4. “კრიმინოლოგია და სამართლებრივი სისტემა საქართველოში” მთავარი რედაქტორი: გიორგი ღლონტი; თინათინ წერეთლის სახელმწიფოსა და სამართლის ინსტიტუტი 2008წ.