UDC 355/359
SCOPUS CODE 3320
https://doi.org/10.36073/1512-0996-2022-3-186-198

კიბერშპიონაჟის მიზნები, ტაქტიკა და მისი საფრთხის მართვის საშუალებები საქართველოს საჯარო ადმინისტრირების სისტემაში

აკაკი შეყელაძე საწარმოო ინოვაციებისა და ოპერაციათა მენეჯმენტის დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: ashekeladze@gmail.com

რეცენზენტები:

კ. ხმალაძე, სტუ-ის ენერგეტიკის ფაკულტეტის პროფესორი
E-mail: khmaladzek@yahoo.com

მ. ტუღუში, თსუ-ის ეკონომიკისა და ბიზნესის ფაკულტეტის ასოცირებული პროფესორი
E-mail: miron.tugushi@tsu.ge

ანოტაცია. ბოლო წლებში განხორციელებულ კიბერშეტევებში ვხვდებით სამთავრობო ინფრასტრუქტურის წინააღმდეგ განხორციელებულ არაერთ შემთხვევას, როდესაც ადგილი ჰქონდა ქვეყნის დიპლომატიური საიდუმლოების, კონფიდენციალური და პერსონალური ინფორმაციის მოპარვას მოწინააღმდეგის მხრიდან სხვადასხვა მავნე მიზნით. ტექნოლოგიების განვითარებასთან ერთად, აღნიშნული ტიპის კიბერშეტევების არა მარტო სიხშირე, არამედ სიმძიმეც იმატებს, რაც სახელმწიფოებისთვის ქმნის განგაშის საფუძველს. ასეთი შეტევების მსხვერპლი არაერთხელ გამხდარან განვითარებული და განვითარებადი ქვეყნები, რომელთა შორის საქართველოცაა, რომელიც აღმოჩნდა ერთ-ერთი პირველი მსხვერპლთა შორის მსოფლიოში და მის წინააღმდეგ განხორციელებული მავნე ქმედების ძლიერი ტაქტიკაც მრავალი კიბერუსაფრთხოების ექსპერტის მიერ აღინიშნა.

მოცემულ სტატიაში განიხილება ინფორმაციული უსაფრთხოების კომპრომეტირების ერთ-ერთი მეთოდი – კიბერშპიონაჟი, რომელიც, როგორც ბოლო პერიოდის შემთხვევებმა ცხადყო, სახელმწიფოს წინაშე არსებული კიბერსაფრთხეებიდან უმთავრესია. ნაშრომში ყურადღება გამახვილებული იქნება კიბერშპიონაჟის მიზნებზე, ასევე იმ მეთოდებსა და საშუალებებზე, რომლებსაც ბოროტმოქმედები იყენებენ მავნე მიზნების მისაღწევად. მიზნების დე-

მონსტრირების პროცესში მკითხველი შეხვდება შესაბამის აქტუალურ სტატისტიკას და ინფორმაციას ბოროტმოქმედების ტაქტიკის შესახებ.

სტატიაში განხილულია კიბერშპიონაჟის ცნობილი მაგალითები და მათი შედეგები, ასევე – საქართველოს წინააღმდეგ განხორციელებული კიბერშპიონაჟის შემთხვევა, რომელიც ერთ-ერთი პირველი იყო მსოფლიოში. სწორედ ამგვარი მაგალითების განხილვით გავეცნობით იმ გამოცდილებას, რომელიც, ერთი მხრივ, იძლევა შიშის საფუძველს, ხოლო, მეორე მხრივ, გვაძლევს შესაძლებლობას, ვიფიქროთ და შევიმუშავოთ საფრთხესთან გამკლავების მეთოდოლოგია.

ბოლოს, საუბარი შეეხება იმ შესაძლო მეთოდებს, რითაც საჯარო სექტორში მსგავსი შემთხვევების თავიდან არიდება და მავნე შედეგების მინიმიზებაა შესაძლებელი.

საკვანძო სიტყვები: ინფორმაციული უსაფრთხოება; კიბერთავდაცვა; კიბერსაფრთხე; კიბერუსაფრთხოება; კიბერშპიონაჟი; სახელმწიფო ადმინისტრირება.

შესავალი

21-ე საუკუნის 20-იან წლებში უკვე საზოგადოდაა ცნობილი, რომ კიბერშეტევების სამიზნე ხშირად ხდება არა მარტო საბოლოო მომხმარებელი ან კომპანია, არამედ არაერთი სამთავრობო სტრუქტურა და სრულიად ქვეყნის კრიტიკული ინფორმაციული ინფრასტრუქტურა. სახელმწიფოს წინააღმდეგ კიბერშეტევებს ხშირად ყოფენ 2 ძირითად კატეგორიად: კიბერსაბოტაჟად და კიბერშპიონაჟად.

კიბერშპიონაჟი განეკუთნება ისეთი ტიპის კიბერშეტევას, როდესაც არაავტორიზებული მხარე, წარმატებით თუ წარუმატებლად, ცდილობს წვდომა მოიპოვოს შეზღუდული დაშვების ან, ზოგადად, სენსიტიურ ინფორმაციაზე ისეთი მიზნებით, როგორიცაა: ფინანსური, კონკურენტული უპირატესობის მოპოვება ან პოლიტიკური.

მნიშვნელოვანია აღინიშნოს, რომ კიბერომი და კიბერშპიონაჟი ერთმანეთის მსგავსი, მაგრამ არა ერთი და იგივეა. უმთავრესი განსხვავება მათ შორის არის მიზანი. კიბერომის მიზანი არის სახელმწიფოს ფუნქციონირების ხელის შეშლა, ხოლო კიბერშპიონაჟის მიზანი შემტევისთვის არის ინფორმაციის მოპარვა მალულად ყოფნის პირობებში [1].

კიბერშპიონაჟის სამიზნე ძირითადად ხდება მძლავრი კორპორაციები ან სახელმწიფოები. ყველაზე ხშირად აღნიშნული ტიპის შეტევის სამიზნე გამხდარა ისეთი ქვეყნები, როგორიცაა: აშშ, იაპონია, რუსეთი, დიდი ბრიტანეთი, სამხრეთ კორეა და ჩინეთი, ასევე საქართველო.

უკანასკნელი 20 წლის განმავლობაში კიბერშეტევის ყველაზე გავრცელებულ სახეს, რომლებიც მიმართული იყო სახელმწიფოების წინააღმდეგ, სწორედ კიბერშპიონაჟი წარმოადგენს.

ENISA-ს კიბერშპიონაჟის ანგარიშის მიხედვით, ინფორმაციული უსაფრთხოების ინციდენტების 20%-ის საფუძველი კიბერშპიონაჟია, ხოლო ინციდენტების 11% შპიონაჟის მიზნებით მომდინარეობდა (სურ. 1).

სურ. 1.

საყურადღებოა ის ფაქტი, რომ ამგვარი ტიპის შეტევა შეიძლება მიმდინარეობდეს ხანგრძლივი პერიოდის განმავლობაში და ბოროტმოქმედები ისე იპარავდნენ ინფორმაციას, რომ ორგანიზაციამ ან სახელმწიფომ არ იცოდეს ბოროტმოქმედის არსებობის შესახებ [2]. კიბერშეტევების, მათ შორის კიბერშპიონაჟის, შემთხვევების გამოძიება უკიდურესად რთულია, ხოლო შესაძლო დამნაშავეზე საჯაროდ გაცხადება კი – უკიდურესად კომპლექსური ხასიათის საკითხი.

კიბერშპიონაჟის მავნე შედეგები მოიცავს: ინფორმაციის განადგურებას, კონკურენტული უპირატესობის დაკარგვას, ინფრასტრუქტურის დაზიანებას, საიდუმლოების გაჟონვას, ადამიანთა სიცოცხლის მოსპობას. აქედან გამომდინარე, უმნიშვნელოვანესია, რომ ამ ტიპის შეტევის საფრთხეები, შესაძლო მავნე შედეგები და რისკების შემცირების საშუალებები სწორად და ჯეროვნად იყოს გააზრებული.

ძირითადი ნაწილი

1. კიბერშპიონაჟის მიზნები

კიბერშპიონაჟით ბოროტმოქმედები უტევენ მსხვილ კორპორაციებს, საგანმანათლებლო დაწესებულებებს და სამთავრობო სტრუქტურებს. ზოგჯერ, მიზნობრივი კამპანიები ტარდება ცნობილი ადამიანების, ბიზნესმენებისა და სახელმწიფო თანამდებობის პირების წინააღმდეგ.

ინფორმაციული აქტივები, რომლებიც ძირითადად ხდება შეტევის სამიზნე, შესაძლოა იყოს [3]:

- პერსონალური ინფორმაცია;
- სადაზვერვო ინფორმაცია;
- პოლიტიკური სტრატეგიები, კავშირები;
- ბიზნესმიზნები, სტრატეგიული გეგმები და მარკეტინგის ტაქტიკა;
- კვლევის მონაცემები;
- ორგანიზაციის ფინანსებთან და ხარჯებთან დაკავშირებული ინფორმაცია (ხელფასი, პრემია და სხვა სენსიტიური მონაცემები).

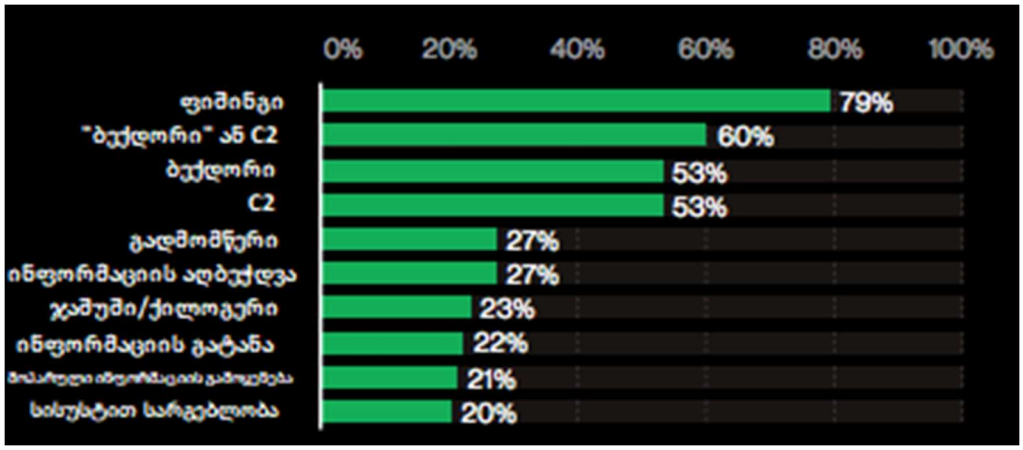
ძირითადად შემთხვევაში, ამგვარი შეტევით სურთ მოიპარონ შინასამსახურებრივი, კონფიდენციალური და საიდუმლო ინფორმაცია.

2. ძირითადი ტაქტიკა

კიბერშპიონაჟის შემთვევები, ძირითადად, კატეგორიზდება როგორც ე.წ. APT [Advanced Persistent Threat (მოიაზრებს მუდმივ, სერიოზული ხასიათის საფრთხეს)]. ასეთ დროს თავდამსხმელი შეაღწევს მსხვერპლის სისტემაში სენსიტიური ინფორმაციის მოპარვის მიზნით. APT შეტევების განხორციელება არ არის მარტივი და მოითხოვს დიდ ძალისხმევას, დროს, ადამიანურ და ფინანსურ რესურსებს.

კიბერშპიონაჟის ტიპის შეტევის შემდეგი წყარო არის სოციალური ინჟინერია, რომლის გამოყენებითაც, მსხვერპლზე გავლენის მოხდენის, მანიპულაციის ან მოტყუების მეთოდით, ხდება კომპიუტერულ სისტემაში შეღწევა, ინფორმაციის მოპარვა,

პერსონალური ან/და ფინანსური მონაცემების ჩათვლით [4]. სოციალური ინჟინერიის მეთოდებს განეკუთვნება ფიშინგწერილები მავნე ბმულით ან დანართით (შანტაჟის/გამოსასყიდი პროგრამული უზრუნველყოფა, ვირუსი, „შპიონი“ პროგრამა და სხვა).



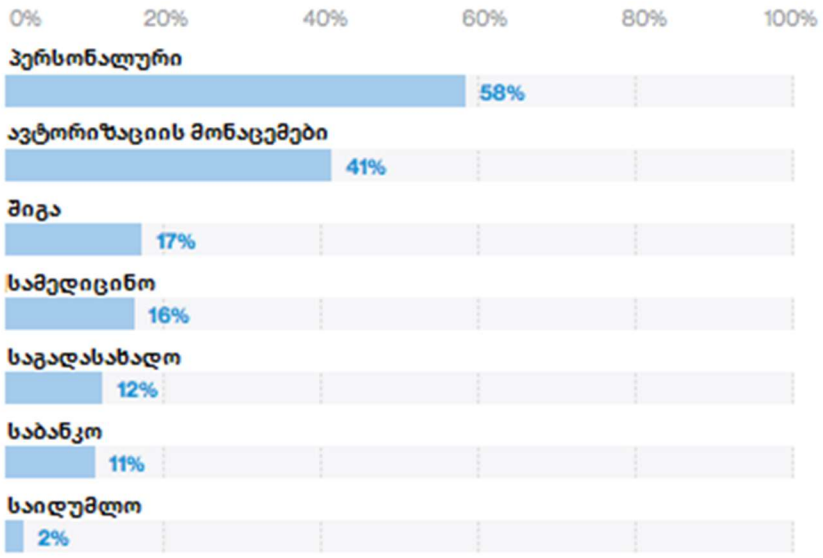
სურ. 2.

კომპანია Verizon-ის ანგარიშის თანახმად, კიბერშპიონაჟის შემთვევები ძირითადად ეფუძნებოდა: ფიშინგს და მავნე პროგრამა „ბექდორს“. ამ ორიდან ფიშინგზე მოდის შეტევების 79% (სურ.2).

სხვა ტექნიკური შესაძლებლობები მოიცავს:

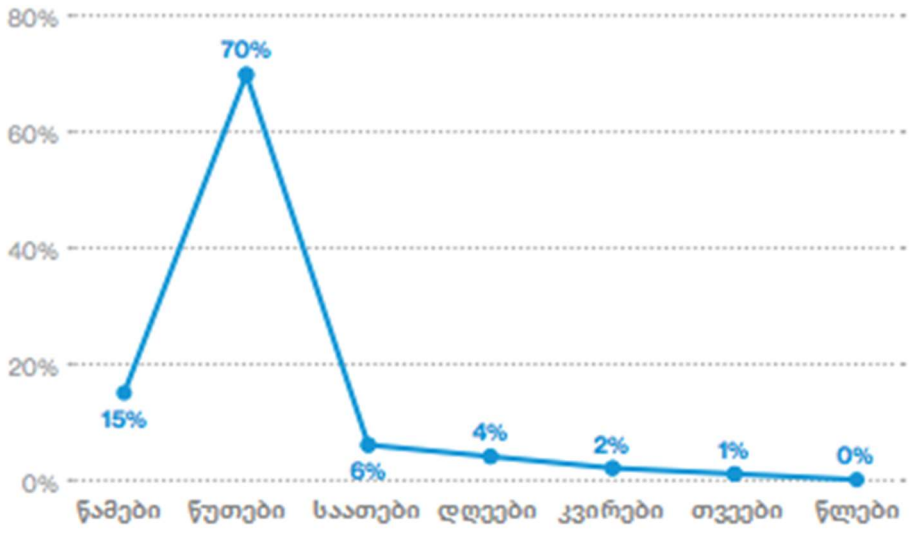
- Watering hole: ბოროტმოქმედები მავნე პროგრამებით აინფიცირებენ ვებგვერდებს, რომელსაც ხშირად მიმართავს მსხვერპლი;
- Spear ფიშინგი: ჰაკერი მიზნად ისახავს სენსიტიური ინფორმაციის (მათ შორის ანგარიშის სახელები და პაროლები) მოპარვას კონკრეტული პირებისგან ისეთი საშუალებებით, როგორიცაა: ყალბი წერილები, შეტყობინებები და სატელეფონო ზარები;
- Zero-Day ექსპლოიტი: კიბერკრიმინალები ნახულობენ და ბოროტად იყენებენ პროგრამული უზრუნველყოფის უსაფრთხოების სისუსტეს (მოწყვლადობას) მანამ, სანამ პროგრამის დეველოპერები ან IT სპეციალისტები მას გამოასწორებენ;
- შიგა საფრთხეები: ბოროტმოქმედები არწმუნებენ დასაქმებულს ან კონტრაქტორს, რომ მათ მიჰყიდონ ან გაუზიარონ ინფორმაცია, ან არაავტორიზებულ პირებს მისცენ სისტემაზე წვდომა.

ბოროტმოქმედები, ძირითად შემთხვევებში, იპარავენ პერსონალურ და შიგასამსახურებრივ ინფორმაციას, ვინაიდან სწორედ ამ ტიპის მონაცემები იძლევა ქსელურ სისტემებზე წვდომის შესაძლებლობას (სურ. 3).

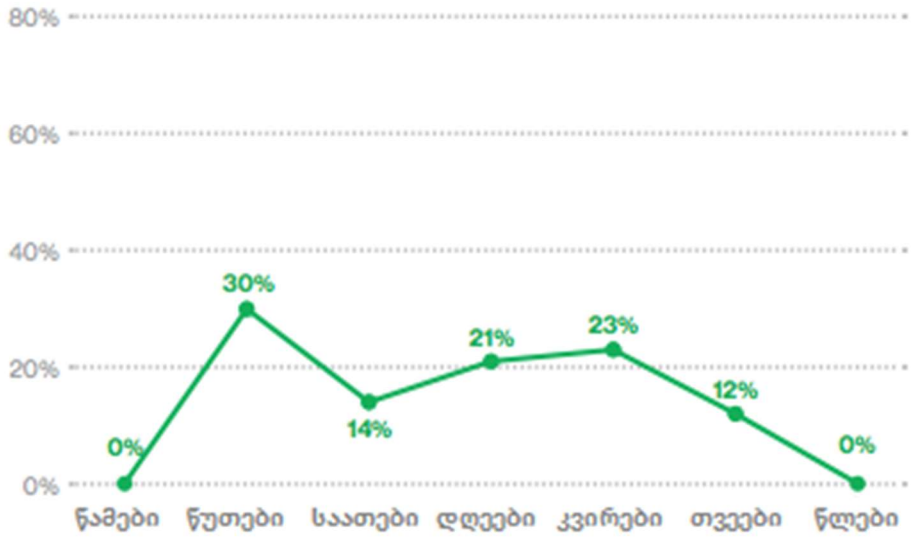


სურ. 3.

კიდევ ერთი მნიშვნელოვანი სტატისტიკური მონაცემი, რომელიც აღნიშვნის ღირსია, არის შეტევის მიმდინარეობის ხანგრძლივობა. 2014–2020 წლების შეტევების ანალიზის შედეგად დადგინდა, რომ „შეტევის განხორციელებისთვის საჭირო დრო ვარირებს წამებიდან დღეებამდე (სურ. 4), ხოლო შეტევისგან აღმოფხვრის დრო – წუთებიდან კვირებამდე (სურ. 5)“ [5].



სურ. 4



სურ. 5

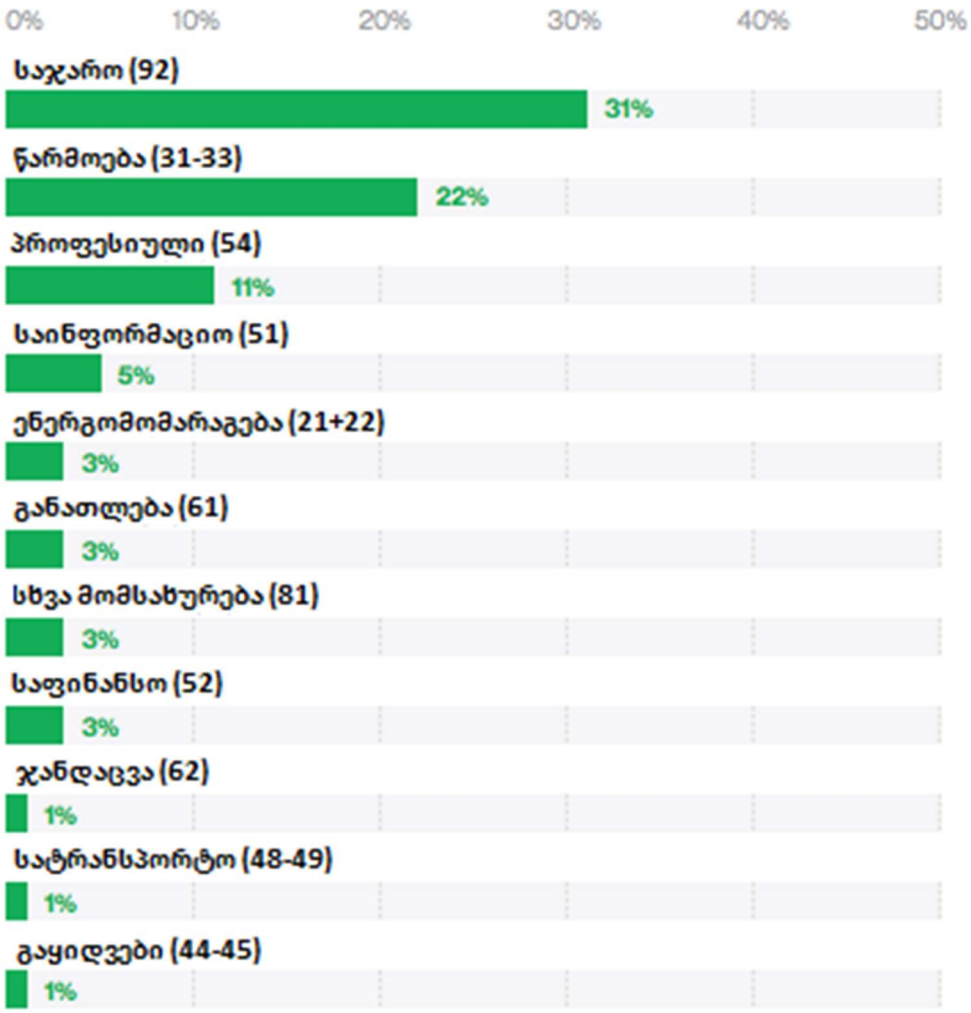
აღნიშნული შეტევის საშუალებებითაა განპირობებული ის, რომ პრობლემების აღმოჩენა ხდება ძალიან გვიან. კვლევების თანახმად, შეტევების აღმოჩენას სჭირდება წამებიდან წლებამდე დრო. კვლევის ფარგლებში განხილული 2918 შემთხვევიდან 38%-ის აღმოჩენას თვეზე მეტი დასჭირდა.

უნდა აღინიშნოს ისიც, რომ სამართალდამცავ ორგანოებს არ აქვს ისეთი ქმედითი ბერკეტები, რომლითაც შეძლებენ კიბერკრიმინალების დევნასა და დასჯას, ვინაიდან ისინი მალავენ საკუთარ იდენტობას, შლიან კვალს და, უმრავლეს შემთხვევაში, ოპერირებენ ძალიან დიდი ფიზიკური დისტანციიდან.

მიუხედავად აღნიშნულისა, ვინაიდან ჩვენ ვიცით ზოგადი ტაქტიკა ამ ტიპის შეტევებისთვის, ასევე ცნობილია არაერთი შპიონაჟის შემთხვევა, უნდა შევძლოთ დასკვნების გაკეთება იმასთან დაკავშირებით, თუ როგორ ავირიდოთ მავნე შედეგები და როგორ დავიცვათ მომხმარებლები და ინფრასტრუქტურა ბოროტმოქმედებისგან.

3. საყურადღებო შემთხვევები

მიუხედავად იმისა, რომ ინფორმაციული უსაფრთხოების ინციდენტები ხორციელდება ნებისმიერი ტიპის ინფრასტუქტურის წინააღმდეგ, კიბერშპიონაჟი, ძირითადად, მიმართულია სახელმწიფო სექტორზე. ცნობილი შემთხვევები გვიჩვენებს, რომ შეტევის უმრავლესობა იმართება სახელმწიფო ან სახელმწიფოს მიერ დაფინანსებული დაჯგუფებების მხრიდან. Verizon-ის კვლევამ აგრეთვე აჩვენა, რომ 2014–2020 წლებში განხორციელებული კიბერშპიონაჟის შემთხვევების 31% (სულ 1580 შემთხვევა) განხორციელდა სახელმწიფო სექტორში (სურ. 6).



სურ. 6.

ENISA-ს ანგარიშის თანახმად, 2019–2020 წლებში კიბერშპიონაჟის შემთხვევებიდან 23-ზე მეტი შეიძლება შეფასდეს როგორც მსხვილმასშტაბიანი [11].

კიბერშპიონაჟის ცნობილ შემთხვევებს განეკუთვნება ერთ-ერთი პირველი Aurora-ს შეტევა, რომელიც 2009 წლით თარიღდება. ჩინელი აქტივისტები, რომლებიც ადამიანის უფლებებს აპროტესტებდნენ, უტევდნენ Google-ის საფოსტო ანგარიშების მფლობელებს. მოგვიანებით აღმოჩნდა, რომ შეტევებმა მოიცვა სხვა მსხვილი კორპორაციებიც, როგორიცაა Adobe და Yahoo. შეტევას საფუძვლად ედო Internet Explorer-ის მოწყვლადობა.

სახელმწიფოს მიერ დაფინანსებული კიბერდაჯგუფებები მსოფლიოში უკვე მრავლადაა ცნობილი. ერთ-ერთი მათგანია Fancy Bear (იგივე Sofacy ან APT29). აღნიშნული დაჯგუფება იყენებს ფიშინგწერილებს იმისთვის, რომ მიიღონ წვდომა კომპიუტერულ და მობილურ მოწყობილობებზე და მოიპარონ მონაცემები. ევროპული, ასევე ამერიკული, სამხედრო ორგანიზაციები არაერთხელ აღმოჩნდნენ

ამ დაჯგუფების იერიშის მსხვერპლი. ინფორმაციული უსაფრთხოების ექსპერტები ამტკიცებენ, რომ ჯგუფი იმართება რუსეთიდან.

კიდევ ერთი ცნობილი, ჩინეთთან დაკავშირებული, კიბერშპიონაჟის დაჯგუფებაა Goblin Panda (იგივე APT27). აღნიშნული ბოროტმოქმედები რამდენიმე წელი იყენებდნენ Microsoft Word-ის ექსპლოიტს და შეუტიეს აზიის ქვეყნების სამთავრობო და ენერგოინფრასტრუქტურას.

გარდა ჩინეთისა და რუსეთისა, ვიეტნამი და ჩრდილოეთ კორეა ასევე ცნობილია, როგორც კიბერჯგუფების მმართველები. ჰაკინგდაჯგუფება Lazarus უკვე 6 წელზე მეტია მოქმედია და მიიჩნევა, როგორც Sony Pictures-ზე განხორციელებული შეტევის ავტორი, რომელიც შეფასდა მილიონობით დოლარად და, ასევე, განახორციელა შეტევა ბანგლადეშის ბანკების წინააღმდეგ 2016 წელს. ასევე, ისინი მიიჩნევიან WannaCry შეტევის ავტორებად, რომელმაც მოიცვა კომპანიები, ბანკები და საავადმყოფოები მთელი მსოფლიოს მასშტაბით [6].

საქართველო, ასევე, ერთ-ერთი პირველი ქვეყანა იყო, რომელიც კიბერშპიონაჟის მსხვერპლი აღმოჩნდა.

2011 წლის მარტში სსიპ მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფმა შენიშნა ინფორმაციული უსაფრთხოების ინციდენტი, რომელიც ძალიან ჰგავდა კიბერშპიონაჟს.

მავნე პროგრამა აგროვებდა სენსიტიურ და კონფიდენციალურ ინფორმაციას საქართველოს და ამერიკასთან დაკავშირებული დოკუმენტებიდან და ტვირთავდა შესაბამის კონტროლსერვერებზე.

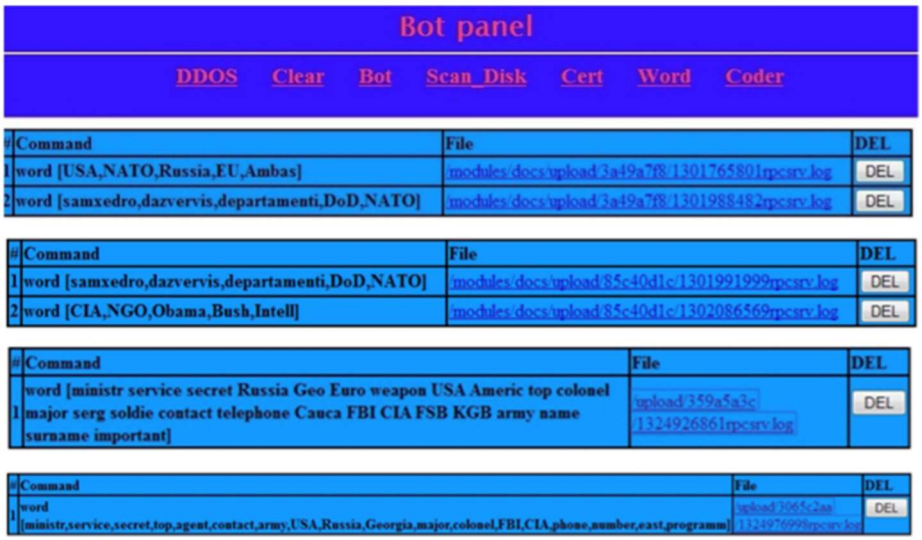
შემტევის სერვერებისა და მავნე ფაილების მოკვლევის შედეგად დადგინდა, რომ კიბერშეტევა იმართებოდა რუსეთიდან.

ვებსერვერის, მავნე ფაილებისა და სკრიპტების ანალიზის შედეგად დადგინდა, რომ:

1. ქართული ახალი ამბების ვებგვერდები გახდა კომპრომეტირების მსხვერპლი;
2. ვებგვერდის მონახულების შემდეგ, კომპიუტერი ინფიცირდებოდა უცნობი მავნე პროგრამით;
3. გაშვების შემდეგ, მავნე ფაილი სრულად აკონტროლებდა ინფიცირებულ მოწყობილობას;
4. ეძებდა „სენსიტიურ სიტყვებს“ დოკუმენტებსა და ფაილებში;
5. მავნე პროგრამა ახორციელებდა ვიდეო- და აუდიოჩაწერას, ჩაშენებული კამერისა და მიკროფონის გამოყენებით.

კიბერშეტევა იყო დაგეგმილი დაკვირვებით. სხვადასხვა ქართული ახალი ამბების ვებგვერდების კომპრომეტირების შემდეგ, იცვლებოდა კონკრეტული გვერდები (მაგ.: ნატოს დელეგაციის ვიზიტი საქართველოში, აშშ–საქართველოს შეხვედრები და შეთანხმებები, საქართველოს სამხედრო სიახლეები).

ინფიცირდებოდა მხოლოდ იმ ადამიანების მოწყობილობები, რომლებიც ეცნობოდნენ აღნიშნული ტიპის ინფორმაციას. პროგრამა იყო დაშიფრული და იყენებდა ძლიერ ტექნიკას, რის გამოც არცერთ უსაფრთხოების საშუალებას (მაგ.: ანტივირუსი) არ შეეძლო მისი ამოცნობა.



სურ. 7.

მავნე ფაილი ეძებდა სენსიტიურ სიტყვებს (სურ. 7) Microsoft Office-ის და .pdf დოკუმენტებში და შეეძლო:

- ნებისმიერი ფაილის მყარი დისკიდან დაშორებულ სერვერზე გაგზავნა;
- მყარ დისკზე Microsoft Office დოკუმენტების მოძებნა (სენსიტიური სიტყვები);
- მყარ დისკზე კონფიგურაციის ფაილების მოძებნა;
- ეკრანის ფოტოს აღბეჭდვა;
- აუდიოჩაწერა მიკროფონის გამოყენებით;
- ვიდეოჩაწერა ვებკამერის გამოყენებით;
- ლოკალური ქსელის სკანირება;
- ბრძანებების გაშვება დაინფიცირებულ სისტემაში.

კომპრომეტირებული კომპიუტერები, ძირითადად, იყო სამთავრობო დაწესებულებიდან და კრიტიკული ინფრასტრუქტურიდან, მათ შორისაა სამინისტროები, პარლამენტი, კრიტიკული ინფორმაციული სისტემის სუბიექტები, ბანკები, არასამთავრობო ორგანიზაციები.

მოგვიანებით, CERT.GOV.GE-მ სრული წვდომა მიიღო კონტროლსერვერზე, მოახდინა საკომუნიკაციო მექნიზმებისა და მავნე ფაილების დეშიფრაცია. მოპოვებული ინფორმაციის ანალიზის შედეგად, ჯგუფმა ამოიცნო კონკრეტული კიბერკრიმინალები და უწყებები.

ბოროტმოქმედის მდებარეობა იყო ლუბიანკას ქუჩა 13, მოსკოვი – რუსეთის შინაგან საქმეთა სამინისტროს ლოჯისტიკის დეპარტამენტი. სპეციალისტებმა ასევე მოიპოვეს რუსული დოკუმენტი ელფოსტიდან, სადაც კიბერდაჯგუფების წევრი დავალებებს აძლევდა სხვებს, თუ როგორ გამოეყენებინათ მავნე პროგრამა და დაეინფიცირებინათ მსხვერპლი.

4. როგორ ვმართოთ კიბერშპიონაჟის რისკი

კიბერშეტევების რისკის სრულად თავიდან არიდება, ცხადია შეუძლებელია. თუმცა, კომპანია

Verizon-ის ინფორმაციული უსაფრთხოების ინციდენტების გამოძიების ანგარიშის თანახმად [7] შესაძლებელია რისკის შემცირება. კონტროლის მექანიზმები შესაძლებელია იყოს შემდეგი:

- ორგანიზაციის კრიტიკული ფუნქციების განსაზღვრა და მათი კიბერშპიონაჟის რისკებთან დაკავშირება;
- უსაფრთხოების პოლიტიკების განსაზღვრა, რომელიც ითვალისწინებს ადამიანური რესურსების, ბიზნესისა და ოპერაციული უსაფრთხოების კონტროლს. ეს უნდა მოიცავდეს ცნობიერების ამაღლების, კორპორატიული მმართველობისა და უსაფრთხოების ოპერაციების წესებსა და პრაქტიკას;
- კომუნიკაციის კორპორატიული პრაქტიკის დამკვიდრება;
- შეფასების კრიტერიუმების (KPIs) შემუშავება, რათა შეაფასოს ოპერაცია და მოერგოს მომავალ ცვლილებებს;
- თეთრი სიის შექმნა კრიტიკული სერვისებისთვის, შეფასებული რისკის დონის მიხედვით;
- მოწყვლადობების შეფასება და პროგრამული უზრუნველყოფის რეგულარულად განახლება;
- წვდომის უფლებების განსაზღვრის აუცილებლობის პრინციპის დანერგვა და პრივილეგირებული ანგარიშების ბოროტად გამოყენების მონიტორინგის საშუალებების შემოღება;
- შინაარსის (კონტენტის) ფილტრაციის დაწესება ყველა შემომავალი და გამავალი არხისთვის (მაგ. ელფოსტა, ვებ-ი, ქსელის ტრაფიკი).

ამასთანავე, უნდა არსებობდეს შესაბამისი ინფორმაციული უსაფრთხოების პოლიტიკა, რომელიც შეეხება მოწყვლადობებს, ისეთ პროცედურებს, როგორიცაა ტექნიკური და პროგრამული უზრუნველყოფის გაახლება. აგრეთვე, სარეზერვო ასლები უნდა გაკეთდეს დროულად და მოხდეს მათი ვერიფიცირება.

კიდევ ერთი რამ, რაც მაგალითების საფუძველზე შეგვიძლია ვისწავლოთ, არის პაროლების დაცვა, მონაცემთა ბაზების დაშორებულ სერვერებზე განთავსება და უსაფრთხოების სისტემების არსებობის საჭიროება.

Crowdstrike ასევე გვთავაზობს 2 მეთოდს კიბერშპიონაჟის თავიდან ასარიდებლად [3]:

1) დაზვერვა (Threat Intelligence): საფრთხის წყაროს მოქმედების შესასწავლად დაზვერვითი საქმიანობა ერთ-ერთი ეფექტური მეთოდია. დღესდღეობით უფრო მნიშვნელოვანია ის, თუ რა დგას შეტევის უკან, და არა უბრალო ფაქტი, რომ შეტევა განხორციელდა;
2) საფრთხეების კვლევა (Threat Hunting): ამგვარი ტექნოლოგიის დანერგვა სულ უფრო საჭირო ხდება. ორგანიზაციების დიდ ნაწილს სჭირდება 24/7-ზე, ადამიანის მიერ მართული, საფრთხეების კვლევის პროცესი, რომლებიც დაეხმარება კიბერთავდაცვისკენ მიმართულ ტექნიკურ საშუალებებს.

დასკვნა

ამრიგად, საჯარო ადმინისტრირებაში კიბერშპიონაჟის არსის, გავლენისა და შედეგების გააზრება და მისი რისკის მართვა ერთ-ერთი ძირითადი

პრიორიტეტია. მოქალაქეების, სახელმწიფო ინსტიტუტებისა და, ზოგადად, ქვეყნის დაცვა შეუძლებელი იქნება შესაბამისი კონტროლის მექანიზმების დანერგვის გარეშე, რომელიც შეამცირებს ასეთი შპიონაჟის ტიპის შეტევების რისკს.

განხილული მაგალითების საფუძველზე შეიძლება ითქვას, რომ საბოლოო მომხმარებლები, დასაქმებულები არიან თავდაცვის წინა ხაზზე, რის გამოც, ინფრასტრუქტურის დაცვის საკვანძო მიმართულება სწორედ პერსონალის ცნობიერების ამაღლება უნდა იყოს, რომ ისინი არ გახდნენ ფიშინგშეტევების მსხვერპლი და არ გაამჟღავნონ პირადი და სენსიტიური ინფორმაცია. როდესაც დასაქმებულს ესმის პოტენციური საფრთხე, ასევე აქვს ცოდნა იმ საშუალებების შესახებ, რითაც ხდება ინფორმაციული უსაფრთხოების რისკების შემცირება, ის უკვე ნაკლებად მოწყვლადია და შეუძლია თავიდან აირიდოს ამგვარი შეტევები, რაც საბოლოოდ ხელს უშლის მოწინააღმდეგე სახელმწიფოს მიერ დაფინანსებულ ბოროტმოქმედებს მიზნების მიღწევაში.

ცხადია, შემდგომ ეტაპზე უნდა შეფასდეს კიბერშპიონაჟის რისკების შემცირების წარმოდგენილი მეთოდების გამოყენების შესაძლებლობა ქართულ რეალობაში, ვინაიდან მათი ნაწილი დიდ ფინანსურ რესურსს მოითხოვს, ნაწილი – თანამშრომელთა ცნობიერების საკმაოდ მაღალ დონეს, ნაწილი კი – საჯარო სექტორში დასაქმებული კიბერუსაფრთხოების სპეციალისტების ძლიერ ტექნიკურ შესაძლებლობებს. აუცილებელია გამოიკვეთოს ის კონკრეტული გადაწყვეტები, რომლებიც ყველაზე მეტად დაიცავს ჩვენს ინფორმაციული უსაფრთხოების ინფრასტრუქტურას. თუმცა, სფეროს განვითარების კვალდაკვალ შესაძლებელია გამოვლინდეს ინფორმაციული უსაფრთხოების რისკების მართვის იმგვარი ინოვაციური მეთოდები, რომლებიც, მათ შორის, შეამცირებენ კიბერშპიონაჟის რისკებს.

ლიტერატურა

1. Gillis, A. S. (2021). *Cyber Espionage*. SearchSecurity. Retrieved from: https://searchsecurity.techtarget.com/definition/cyber-espionage ;
2. Swami, N. (2020). *What Is Cyber Espionage? How To Protect Your Data?* Teceze. Retrieved from: https://www.teceze.com/what-is-cyber-espionage-how-to-protect-your-data ;
3. Baker, K. (2022). *Cyber Espionage.* Crowdstrike. Retrieved from: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/;
4. Carnegie Mellon University. (n.d). *Social Engineering.* Retrieved from https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html
5. *Cyber-Espionage Report.* (n.d.). Verizon. Retrieved from: https://enterprise.verizon.com/resources/reports/2020-2021-cyber-espionage-report.pdf

6. *What is Cyber Espionage?* (n.d.). vmware. Retrieved from: https://www.vmware.com/topics/glossary/content/cyber-espionage ;
7. *2019 Data Breach Investigations Report.* (2019). Verizon. Retrieved from: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf
8. Villanova University. (2021). *What is Cyber Espionage*? Retrieved from: https://www.villanovau.com/resources/iss/cyber-espionage/ ;
9. CERT-Georgia. (n.d). *Cyber Espionage Against Georgian Government.*
10. Pitlik, D. (2019). *The Dark Side of Governments: A Growing Threat of APT Groups*. NETSCOUT. Retrieved from: https://www.netscout.com/blog/dark-side-governments-growing-threat-apt-groups ;
11. ENISA Threat Landscape. (2020). *Cyber Espionage.* Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

UDC 355/359
SCOPUS CODE 3320
HTTPS://DOI.ORG/10.36073/1512-0996-2022-3-186-198

Cyber Espionage Aims, Tactics and Threat Management Opportunities in the Georgian Public Administration

Akaki Shekeladze Department of Industrial Innovations and Operations Management, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: ashekeladze@gmail.com

Reviewers:
K. Khmaladze, Professor, Faculty of Power Engineering, GTU
E-mail: khmaladzek@yahoo.com
M. Tughushi, Associate Professor, Faculty of Economics and Business, TSU
E-mail: miron.tugushi@tsu.ge

Abstract. There are number of cases against the states among the cyber-attacks occurred in the recent years, when there was a breach of diplomatic secrets, confidential or personal data with various malicious aims from the

perpetrator's side. With the development of technologies, not only the frequency, but also the severity of such cyber-attacks is rising, giving an alarm to the governments. The victims have been both developed and developing countries, including Georgia, which was one of the first to be addressed and the strong tactics of the malicious attack deserved to be noted by several cyber security experts.

One of the methods of compromising information security is cyber espionage, which, as recent cases have demonstrated, is one of the most important cyber threats the states are facing. The focus of the article is on the aims of cyber espionage, as well as on the methods and means used by criminals to achieve malicious goals. In the process of demonstrating the goals, the reader will be shown relevant statistics and information on crime tactics.

Well-known examples of cyber espionage and their consequences are presented. The case of cyber espionage against Georgia, which was one of the first in the world, is also considered. It is through such examples that we learn about experiences that, on the one hand, provide the basis for fear and, on the other hand, makes us able to think and develop a methodology for dealing with the threat.

Finally, attention is drawn to the possible methods that can avoid such cases in the public administration and minimize the harmful consequences.

Keywords: cyber defence; cyber espionage; cyber security; information security; public administration.

განხილვის თარიღი 31.03.2022
შემოსვლის თარიღი 07.04.2022
ხელმოწერილია დასაბეჭდად 23.09.2022