რუსული კიბერშეტევა უკრაინაზე - იანვარი, 2022

GCSD

რუსული კიბერშეტევა უკრაინაზე - იანვარი, 2022

ავტორი: ანდრო გოცირიძე

ანდრო გოცირიძე - კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი. თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიუროს დირექტორი 2014 - 2017 წწ, გენერალური ინსპექტორი 2012-2014 წწ. სხვადასხვა დროს მუშაობდა თავდაცვის სამინისტროსა და სადაზვერვო სამსახურების ხელმძღვანელ თანამდებობებზე, 2008-2012 წლებში იყო სს „პრივატბანკისა“ და სს „ბანკი კონსტანტას“ უსაფრთხოების დეპარტამენტის უფროსი. მისი უშუალო მონაწილეობით დამუშავდა ეროვნული და თავდაცვის სამინისტროს კიბერუსაფრთხოების პოლიტიკა და სტრატეგიები, საფუძველი ჩაეყარა კიბერრეზერვის პროექტს და სამშვიდობო მისიებში დაჭრილი ჯარისკაცების კიბერუსაფრთხოების სფეროში ტრენერებად ინტეგრაციას, დაინერგა კიბერცნობიერების ამაღლების მრავალკომპონენტიანი სისტემა.

კითხულობს ლექციებს BTU, შავი ზღვის საერთაშორისო და კავკასიის უნივერსიტეტებში, ასევე GFSIS (რონდელის ფონდი)-ის, საგარეო საქმეთა სამინისტროს დიპლომატიური ინსტიტუტისა და მედიის განვითარების ფონდის მიერ ორგანიზებულ სხვადასხვა პროექტებში. არის 2015-16 წ. NATO PFPC მიერ შექმნილი Cyber Security Generic Reference Curriculum თანაავტორი.

GCSD

გასულ კვირას დასავლეთსა და რუსეთს შორის უშედეგო მოლაპარაკებების ფონზე უკრაინის სამთავრობო საიტებზე მასირებული კიბერშეტევა განხორციელდა, რამაც ათეულობით სამთავრობო საიტის საწყისი გვერდის შეცვლა, ე.წ defacement[1] გამოიწვია. მწყობრიდან გამოვიდა უკრაინის ათამდე, მათ შორის საგარეო საქმეთა და ფინანსთა სამინისტროს ვებგვერდები, ასევე სახელმწიფო სერვისების სააგენტოს კომპიუტერული სისტემა, სადაცასახული იყო ვაქცინაციის მონაცემები.

ჰაკერების მიერ რუსულ, უკრაინულ და პოლონურ ენებზე გავრცელებული მესიჯი უკრაინელ ხალხს უარეს მომავალს უწინასწარმეტყველებდა და ამცნობდა, რომ მათი პერსონალური მონაცემები გასაჯაროვებულია. უკრაინის სპეცსამსახურებმა გამოყენებულ მავნე პროგრამულ უზრუნველყოფაში რუსული კვალი დაინახეს[2], ხოლო აშშ-ის ადმინისტრაციამ განაცხადა, რომ რუსეთი, სავარაუდოდ საომარი მოქმედებების განახლებას აპირებს.

სენსიტიური მონაცემების გაჟონვის ეფექტი ჯერ ჯერობით არ დასტურდება, თავად defacement კი არ ითვლება იმ ტიპის შეტევად, რამაც შესაძლოა მსხვერპლი ან მნიშვნელოვანი ზარალი გამოიწვიოს, თუმცა კიბერშეტევის მსოფლიო რეზონანსი არა იმდენად ტექნიკური ეფექტით, რამდენადაც მოვლენების შესაძლო განვითარებით არის განპირობებული. ცნობილია, რომ defacement, ტერორისტული ორგანიზაციებისა და ჰაქტივისტების გარდა, რუსული სპეცსამსახურებისა და მათთან აფილირებული ჯგუფების საყვარელ მეთოდად ითვლება. რუსული დაზვერვა ამ ტექნოლოგიურად მარტივ შეტევას ფსიქოლოგიური ეფექტის მისაღწევად იყენებს და მოწინააღმდეგის დემორალიზებას, სახელმწიფო ინსტიტუტებისადმი რწმენის შემცირებას, საზოგადოების პოლარიზაციას, პარტნიორებთან და მოკავშირეებთან ურთიერთობების ძირის გამოთხრას ცდილობს.

ამგვარი შეტევა რუსეთმა საქართელოს წინააღმდეგაც განახორციელა 2019 წლის ნოემბერში. მაშინ, ელექტრონული გრაფიტი საქართველოს პრეზიდენტის, სასამართლოსა და მუნიციპალიტეტების საიტზე გამოჩნდა. ექსპრეზიდენტ სააკაშვილის ფოტომ და მოწოდებამ „I will be back” ფართო რეოზნანსი გამოიწვია. საერთაშორისო თანამეგობრობამ ეს შეტევა რუსეთის სადაზვერვო სამსახურებს მიაკუთვნა და მას პოლარიზაციისკენ მიმართული, საქართველოს სუვერენიტეტის საწინააღმდეგო და დემოკრატიის ძირგამომთხრელი ქმედება უწოდა[3].

სხვა ტიპის შეტევებთან ერთად, ამგვარი თავდასხმა განხორციელდა რუსეთთან აფილირებული ჰაკერების მიერ 2008 წლის ივლისში საქართველოს პრეზიდენტის ვებგვერდზე, სადაც განთავსდა ფაშისტური სიმბოლიკა. მკითხველს მოეხსენება, რომ ეს პირველი პრეცედენტი იყო, როდესაც რუსეთმა კიბერშეტევები საბრძოლო მოქმედებების მხარდამხარ, უშუალოდ საბრძოლო ამოცანის შესრულების გასამარტივებლად გამოიყენა.

---

[1] დაბალტექნოლოგიური კიბერშეტევის ფორმა, რომელიც არასანქცირებულად ცვლის საიტის (ვებგვერდის) გარეგნულ იერსახეს, ხშირად პირველ გვერდს. ძირითადად, გამოიყენება ჰაქტივისტების ან კიბერტერორისტების მიერ საპროტესტო მესიჯის, პროპაგანდისტული მასალის ან სხვა კონტენტის გასავრცელებლად. ამ ტიპის თავდასხმა განხორციელდა რუსეთთან აფილირებული ჰაკერების მიერ 2008 წლის ივლისში საქართველოს პრეზიდენტის ვებგვერდზე, სადაც განთავსდა ფაშისტური სიმბოლიკა.

[2] https://www.reuters.com/world/europe/ukraine-some-signs-that-cyber-attack-linked-hacker-groups-associated-with-russia-2022-01-14/

[3] https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

რუსეთის მიერ კიბეროპერაციების გამოყენება საინფორმაციო, შეზღუდული მასშტაბის, ჰიბრიდული თუ სრულმასშტაბიანი ომის დროს სიახლეს არ წარმოადგენს. კრემლის ჰიბრიდული აქტივობები სამხედრო ძალის გამოყენებასთან ერთად ითვალისწინებს საინფორმაციო ოპერაციების, პროვოკაციების, კიბერთავდასხმების, საბოტაჟის და ეკონომიკური დივერსიებისა თუ ზეწოლის განხორციელებას.

კიბეროპერაციებს აღნიშნულ ტაქტიკაში ერთ-ერთი საკვანძო ადგილი უჭირავს და სულ უფრო მეტი ამოცანის გადასაჭრელად გამოიყენება. 2014-2016 წლებში უკრაინის კონფლიქტებისას, განსაკუთრებით კი ყირიმის ანექსიის დროს კიბერელემენტი მზარდი ინტენსივობით გამოყენებოდა. აღნიშნულმა ქმედებებმა სეროზული დარტყმა მიაყენა უკრაინის მთავრობის მიერ საკუთარი საინფორმაციო სივრცის თუ კრიტიკული ინფრასტრუქტურის დაცვის შესაძლებლობას. კიბეროპერაციებმა საშუალება მისცა რუსეთს, წარმატებულად მოეხდინა უკრაინის პოლიტიკური და სამხედრო ინსტიტუტების მართვისა და კომუნიკაციისა უნარის ნაწილობრივი მოშლა. 2015 წლის მიწურულს რუსეთმა პირველად სცადა კიბერშეტევის გამოყენება კინეტიკური ეფექტის მისაღწევად: უკრაინის კრიტიკულ ინფრასტრუქტურაზე, კერძოდ - ენერგეტიკულ სექტორზე განხორციელებულმა მაღალტექნოლოგიურმა კიბერშეტევა, ასიათასობით აბონენტი დატოვა ელექტროენერგიის გარეშე. სწორედ აღნიშნულმა შეტევამ გააჩინა განცდა, რომ რუსეთი მომავალ კონფლიქტში არ შემოიფარგლება მხოლოდ DDoS[4] და Defacement შეტევებით ან კიბერშპიონაჟის ოპერაციებით და არ არსებობს გარანტია, რომ იგი არ განახორციელებს კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართულ აქციას, რასაც, გარკვეულ ეტაპზე, შესაძლოა ნგრევა და მსხვერპლიც კი მოჰყვეს. გასათვალისწინებელია, რომ სუსტად დაცული ინფრასტრუქტურის პირობებში ისეთი თავდასხმებიც კი, როგორიცაა DDoS და Defacement შეტევა, შესაძლოა არაპროპორციული ზარალის მიზეზი გახდეს.

წლების განმავლობაში ხორციელდებოდა მასშტაბური შეტევები სამთავრობო საინფორმაციო რესურსსა თუ ზოგიერთი პოლიტიკოსის და საზოგადო მოღვაწის პერსონალურ გვერდებზე. რუსმა ჰაკერებმა გამოიყენეს ფიშინგი, მავნე პროგრამული უზრუნველყოფა, DDoS და TDoS[5] შეტევები, კიბერშპიონაჟისა და კიბერკრიმინალის სხვა ფორმები უკრაინის სამთავრობო და სამხედრო ქსელების, ტელეკომუნიკაციების და კერძო სექტორის საინფორმაციო ტექნოლოგიების ინფრასტრუქტურის მწყობრიდან გამოსაყვანად. კიბერშეტევები განხორციელდა კომუნიკაციის შეფერხების მიზნით, ასევე სამთავრობო გეგმებისა და დოკუმენტაციის ხელში ჩასაგდებად, საჯარო და კერძო ვებ-გვერდების გასათიშად. განსაკუთრებული მნიშვნელობის იყო DDoS შეტევები საგარეო საქმეთა სამინისტროს, უსაფრთხოების თუ თავდაცვის სექტორის, უკრაინის პრეზიდენტის საიტებზე, მიზანმიმართული თავდასხმები თაღლითური ელექტრონული ფოსტის მეშვეობით, ცენტრალური საარჩევნო კომისის მუშაობის მოშლის მცდელობები საპრეზიდენტო და საპარლამენტო არჩევნებისას 2014 წელს; მთელ კონფლიქტს ფონად გასდევდა კიბერზემოქმედების ათეულობით მცდელობა. აღსანიშნავია უკრაინელი სამხედროებისათვის დანებების მოწოდებით მოკლე ტექსტური შეტყობინებების მასირებული დაგზავნა. არსებობს მრავალი მონაცემი სოციალურ ქსელებში ყალბი

---

[4] DDOS (A distributed-denial-of-service) - კომპრომეტირებული კომპიუტერების მეშვეობით გენერირებული დიდი რაოდენობით მონაცემთა მოთხოვნის ნაკადის მიმართვა სერვერისკენ, რომელიც მიმართულია ქსელის გამტარობის და ოპერატიული მეხსიერების გადასავსებად, რასაც შესაძლოა შედეგად მოჰყვეს სამიზნე სისტემის მწყობრიდან გამოყვანა და ბიზნეს-პროცესის მოშლა.

[5] TDoS (telephone denial of service) -მავნე, არასასურველი ზარების ნაკადი, რომელიც გადატვირთვის გზით შეუძლებელს ხდის კონტაქტ-ცენტრის ან ისეთი ორგანიზაციის მუშაობას, რომელიც დამოკიდებულია შეტყობინებების შესვლაზე.

ანგარიშებით განხორციელებულ დეზინფორმაციის გავრცელებასა და ტრადიციული სოციალური ინჟინერიის მეშვეობით განხორციელებულ შეტევებზე.

ისევ გასულ კვირას განხორციელებულ კიბერშეტევას რომ დავუბრუნდეთ, იგი დროში დაემთხვა რუსეთის ჯარების უპრეცედენტო მობილიზაციას უკრაინის საზღვართან და დასავლეთსა და რუსეთს შორის ამ უკანასკნელისათვის უშედეგოდ წარმართულ მოლაპარაკებებს. ამჟამად, სხვადასხვა მონაცემებით, უკრაინის საზღვართან ასი ათასამდე რუსი სამხედროა მობილიზებული. საზღვრისპირა რაიონებში შეინიშნება რუსეთის სამხედრო ტექნიკის, ტანკების, არტილერიისა და „ისკანდერის“ ტიპის რაკეტების გადაადგილება. უკრაინის სამხედრო დაზვერვის მონაცემებზე დაყრდნობით, იზრდება რუსეთის შეიარაღებული ძალების საბრძოლო მზადყოფნის დონე დონეცკისა და ლუგანსკის ოლქების დროებით ოკუპირებულ ტერიტორიაზე და მიმდებარე რეგიონებში. უკრაინული დაზვერვა გასული წლის მიწურულს ვარაუდობდა, რომ 2022 წლის თებერვალში რუსეთი იერიშს ოდესასა და მარიუპოლზე მიიტანდა, ასევე, გააქტიურდებოდა გარკვეული დაჯგუფება ბელარუსის მხრიდან[6]. საინტერესოა, რომ კიევის მონაცემებით, აღნიშნული კიბერშეტევის უკან ბელარუსის დაზვერვასთან დაკავშირებული ჰაკერული დაჯგუფება UNC1151 იდგა[7], ხოლო გამოყენებული მავნე პროგრამული უზრუნველყოფა რუსული დაზვერვისათვისაა დამახასიათებელი. მათი მოსაზრებით, ჯგუფი UNC1151 -ის თავდასხმა შესაძლოა სხვა უფრო დესტრუქციული მოქმდებების შესანიღბად იყოს გამოყენებული. ამ ფონზე ბელარუსი ჰაკერების გამოჩენა უკრაინულ კიბერსივრცეში შესაძლოა საომარი მოქმედებების დაწყების მკვეთრი სიგნალი იყოს. ამასთან, ამ ტიპის შეტევა, როგორც წესი, მოწინააღმდეგის დემორალიზაციას და საინფორმაციო ომის მესიჯების გავრცელებას ემსახურება. ამ ფონზე, ყურადსაღებია, რომ თებერვალში რუსეთი ბელარუსთან ერთად გეგმავს ერთობლივ წვრთნებს „Союзная решимость - 2022", რომელიც უკრაინისა და პოლონეთის საზღვრისკენ იქნება მიმართული. სადაზვერვო მონაცემებზე დაყრდნობით, ამავე პერიოდს უკავშირდება უკრაინის წინააღმდეგ ახალი აგრესიის ვარაუდებიც[8].

UNC1151 ბელარუსის სადაზვერვო სამსახურებთან აფილირებული ჰაკერული ჯგუფია, რომელიც პასუხისმგებელია ლიეტუვაში, ლატვიაში, უკრაინისა და პოლონეთში კიბეროპერაციებით განხორციელებულ პროპაგანდისტულ კამპანიაზე ნატოს აღოსავლეთით გაფართოების საწინააღმდეგო ნარატივებით. მავნე პროგრამული უზრუნველყოფა, რომელიც გამოყენებულ იქნა უკრაინაზე უკანასკნელი თავდასხმისას, ძალიან ჰგავს ცნობილი რუსული დაჯგუფება APT-29-ის მიერ ადრე არაერთხელ გამოყენებულ მალვეარს. ეს უკანასკნელი რუსულ სპეცსამსახურებთან აფილირებულ ჰაკერულ ჯგუფად ითვლებოდა, თუმცა უკანასკნელი ატრიბუციით დადგინდა, რომ ის უშუალოდ რუსეთის საგარეო დაზვერვის სამსახურის სტრუქტურული ერთეულია[9]. სავარაუდოდ, იგივე უნდა ითქვას ბელარუსის დაზვერვისა და UNC1151 -ის კავშირზე: ცნობილი მაღალტექნოლოგიური ჰაკერული ჯგუფები უშუალოდ სადაზვერვო უწყებას წარმოადგენენ, თუმცა, სადაზვერვო ორგანიზაციების მკაცრი კონსპირაციისა და

---

[6] https://www.bloomberg.com/news/articles/2021-11-21/u-s-intel-shows-russian-plans-for-potential-ukraine-invasion

[7] https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

[8] https://edition.cnn.com/2022/01/14/politics/us-intelligence-russia-false-flag/index.html

[9] https://www.gov.uk/government/news/russia-uk-exposes-russian-involvement-in-solarwinds-cyber-compromise

კიბეროპერაციების გართულებული ატრიბუციის გამო, მათ სტრუქტურასა და იერაქრიაზე მსჯელობა პრობლემატურია.

ის, რომ ოპერაცია ფსიქოლოგიურ ეფექტზე იყო გათვლილი და ის საინფრომაციო ომის ერთ ერთი შემადგენელი ნაწილია, კიდევ ერთი გარემოებით დასტურდება: პროპაგანდისტული მესიჯი რუსულისა და უკრაინულის გარდა, პოლონურ ენაზეც გავრცელდა, რაც, სავარაუდოდ, ნაცისტური ოკუპაციის პირობებში პოლონეთის ზოგიერთ რეგიონში უკრაინული ჯგუფების მიერ ჩადენილ დანაშაულებს უნდა უკავშირდებოდეს. ზოგიერთი უკრაინელი ექსპერტის მონაცემებით, პოლონური მესიჯისათვის კომპიუტერული თარგმანია გამოყენებული, ისევე, როგორც UNC1151 -ის მიერ განხორციელებული Ghostwriter ოპერაციისას[10].

რუსული მოქმედებების საპასუხოდ, ჩრდილოატლანტიკური ალიანსი მომდევნო კვირას ხელს აწერს უკრაინასთან კიბერუსაფრთხოების სფეროში მჭიდრო თანამშრომლობის შეთანხმებას, რომელიც, ასევე უკრაინას წვდომას აძლევს მავნე პროგრამული უზრუნველყოფის შესახებ ინფორმაციის მიმოცვლის ერთიან ბაზაზე. კონკრეტულ სეტევაზე რეაგირების მიზნით უკრაინაში უკვე მუშაობენ ალიანსისა და სეერტებული შტატების ექსპერტები. საგულისხმოა, რომ საქართველოს ამ პლატფორმაზე წვდომა უკვე აქვს და მისი სრულფასოვანი ადმინისტრირება კერძო სექტორში განტავსებული კრიტიკული ინფრასტრუტურის სუბიექტების ჩართულობით უკიდურესად მნიშვნელოვანია რუსული აგრესიის რისკების მიტიგაციისათვის.

როგორც რუსული კიბეროპერაციების ისტორია გვიჩვენებს, რუსეთი ამ თავდასხმებს ინფორმაციული ოპერაციების, პროვოკაციების, სამხედრო ოპერაციების წინმსწრებ ან ტანმხლებ პროცესად განიხილავს. თუკი რუსეთი უკრაინაში განმეორებით შეჭრას გადაწყვეტს, კიბერშეტევები ამ შეჭრის მნიშვნელოვანი ნაწილი იქნება, მიუხედავად იმისა, რომ ამჯერად საბრძოლო მოქმედებების თეატრი სახმელეთო ოპერაცია იქნება თანმხლები საავიაციო და საზღვაო მხარდაჭერით.

ბუნებრივია, ჰიბრიდული ომის ეს კლასიკური გამოვლინება, რომელსაც მსოფლიო უკრაინის საზღვარტან აკვირდება, ვერ იქნება ერთ კონკრეტულ შედეგზე ორიენტირებული და რუსეთი დასავლეთის რეაქციის, უკრაინის საბრძოლო მზადყოფნის და საკუთარი რესურსის გათვალისწინებით შეეცდება რამდენიმე სხვადასხვა მიზნის მიღწევას:

- ომის ზღვარზე ბალანსირებით რუსეთმა მოახრეხა დაბრუნებულიყო მოლაპარაკების მაგიდასთან. მისი შემდგომი სამიზნე იქნება, გამოსძალოს დასავლეთს ალიანსის შემდგომ არგაფართოებაზე თანხმობა
- სამხედრო მოქმედებების დაწყების მუქარით და ექსპრეზიდენტ პოროშენკოს ფაქტორით მოახდინოს შიდაარეულობის პროვოცირება და შესაძლო რეჟიმის ცვლილება
- სამხედრო ოპერაციის გზით მიიტაცოს ყირიმის ნახევარკუნძულისა და ოკუპირებული რეგიონების დამაკავშირებელი მეტი ტერიტორია, შეზღუდოს უკრაინის გავლენა შავ ზღვაზე და შეძლებისდაგვარად, მის მიერვე ინსპირირებული კრიზისის დარეგულირების მიზნით მიაღწიოს უკრაინისაგან უკვე მიტაცებული ტერიტორიების ავტონომიის ან სრულ აღიარებას

[10] https://www.reuters.com/world/europe/exclusive-ukraine-suspects-group-linked-belarus-intelligence-over-cyberattack-2022-01-15/

იმ ფონზე, როდესაც რუსეთი ყოველმხრივ ეცდება დააშინოს დასავლეთი და უკრაინა, დაათმობინოს მათ რაც შეიძლება მეტი, მნიშვნელოვანია, დასავლეთმა შეინარჩუნოს მტკიცე პოზიცია და აიძულოს რუსეთი, ეძებოს დიპლომატიური გამოსავალი ჩიხური სიტუაციიდან.