RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

რუსეთის შეცვლილი შეტევითი ტაქტიკა და ვექტორები კიბერსივრცეში

გიორგი ტიელიძე

171

ექსპერტის აზრი

RONDELI FOUNDATION
საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

გიორგი ტიელიძე

რუსეთის შეცვლილი შეტევითი ტაქტიკა და ვექტორები კიბერსივრცეში

171

2021

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით. გამოცემაში გამოთქმული მოსაზრებები ეკუთვნის ავტორებს და შეიძლება არ ასახავდეს საელჩოს თვალსაზრისს.

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN

შესავალი

ბოლო პერიოდში კიბერსივრცეში რუსეთის ფედერაციის სადაზვერვო სამსახურების შეტევითი ტაქტიკა საგრძნობლად შეიცვალა. უმეტესად ეს იმით გამოიხატება, რომ რუსეთის სპეცსამსახურები დასავლეთის ქვეყნებში განლაგებულ ძირითად სამიზნეებს საკუთარი კიბერდაზვერვითი ქვედანაყოფების მეშვეობით კი არ უტევენ, არამედ ქვეყანაში მოქმედ კიბერკრიმინალურ დაჯგუფებებს იყენებენ. აღსანიშნავია, რომ მათი მომსახურებით რუსეთის ფედერაცია ადრეც სარგებლობდა, მაგრამ ახლა, კრემლმა ეს დაჯგუფებები დასავლეთის ქვეყნების კრიტიკული საინფორმაციო სისტემების წინააღმდეგ წარმოებული შეტევითი ოპერაციების ავანგარდში დააყენა.

როგორც ცნობილია, რუსეთში დაუსჯელად მოქმედებს არაერთი ორგანიზებული დანაშაულებრივი ჯგუფი (მაგ.: DarkSide, Evil Corp, Revil და სხვ.), რომლებიც ბოლო დროს განსაკუთრებით გააქტიურდნენ ჩრდილოატლანტიკური ალიანსის წევრ სახელმწიფოებთან მიმართებით და შეტევებს ახორციელებენ მათი კრიტიკული ინფრასტრუქტურის წინააღმდეგ. ამის მაგალითებია აშშ-ში Colonial Pipeline-ის და კორპორაცია JBS-ის წინააღმდეგ მოწყობილი შეტევები, რომელთა შედეგად მოხდა ამ ორგანიზაციების საინფორმაციო და საკომუნიკაციო სისტემებში არსებული სამართავი ფაილების შიფრაცია. სისტემური ფაილების დეშიფრაციის გასაღებისთვის (ე.წ. დეკრიპტორი) კი შემტევმა მხარემ რამდენიმე მილიონი აშშ დოლარი მოითხოვა. ფინანსურ ზიანთან ერთად, რომელიც დაშიფრული მონაცემების დეშიფრაციისთვის გამოსასყიდის გადახდას უკავშირდება, ორივე კომპანიის ფუნქციონირების მოშლის შედეგად აშშ-ის ფინანსური და ეკონომიკური სექტორი სერიოზულად დაზარალდა, რადგან კომპანია Colonial Pipeline აშშ-ის ტერიტორიაზე ნავთობპროდუქტების მთავარი გამანაწილებელია, ხოლო JBS კი – ხორცპროდუქტების მთავარი დისტრიბუტორი. იდენტური სიტუაცია შეიქმნა კომპანია Kaseya-ს ქსელური ინფრასტრუქტურის მართვის პროგრამულ საშუალებაზე შეტევის შემთხვევაშიც, როდესაც ევროპაში ასეულობით კომპანიამ ან/და მისმა ფილიალმა შეწყვიტა ფუნქციონირება.

უნდა აღინიშნოს, რომ რუსული ორგანიზებული კიბერდანაშაულებრივი ჯგუფების გააქტიურება საფრთხეს უქმნის საქართველოს საჯარო და კერძო კრიტიკული საინფორმაციო სისტემის სუბიექტებსაც. დადასტურებულია, რომ ამ ჯგუფების მიერ გამოყენებულ მავნე კოდებში ნაპოვნია მოდულები, რომელთა მთავარი დანიშნულება ფინანსური დაინტერესების მოტივით დაინფიცირებული კომპიუტერებიდან სხვადასხვა სენსიტიური მონაცემის მოპოვება იყო. ამასთანავე ცნობილია, რომ 2008 წლის აგვისტოს ომის დროს, რუსეთის სპეცსამსახურებთან ერთად, ორგანიზებული დანაშაულებრივი დაჯგუფება RBN (Russian Business Network) უტევდა საქართველოს საინფორმაციო რესურსებსა და კერძო სექტორს.

ძირითადი რუსული ორგანიზებული კიბერდანაშაულებრივი ჯგუფების მიმოხილვა

სანამ უშუალოდ კრემლის სპეცსამსახურების მიერ კიბერკრიმინალური დაჯგუფებების გამოყენების სპეციფიკაზე ვისაუბრებდეთ, რომელიც განსაკუთრებით SolarWinds Orion-ზე რფ საგარეო დაზვერვის სამსახურის შეტევის შემდგომ გამოიკვეთა, მიზანშეწონილია მიმოვიხილოთ ამჟამად რფ-ის სადაზვერვო და სამართალდამცავ უწყებებთან უშუალოდ დაკავშირებული ორგანიზებული კრიმინალური დაჯგუფებები და ფაქტობრივ გარემოებებზე დაყრდნობით გამოვააშკარაოთ მათი დანაშაულებრივი თანამშრომლობა.

DarkSide-ი არის რუსეთის ფედერაციაში მოქმედი ორგანიზებული კიბერდანაშაულებრივი ჯგუფი, რომელიც ძირითადად Ranswomware-ის ტიპის შეტევებითაა დაკავებული. ბოლო დროს ჯგუფმა სხვადასხვა დარკნეტ ფორუმზეც განათავსა თავისი მავნე კოდები, რომლებიც, შესაძლოა, გარკვეული საფასურის სანაცვლოდ გამოიყენოს მესამე მხარემ Ranswomare-ის ტიპის შეტევების საწარმოებლად.[1] შესაბამისად, DarkSide-ის დანაშაულებრივი საქმიანობის სფერო გაფართოვდა და მას დაემატა შეტევების განსახორციელებლად საჭირო ცოდნისა და საშუალებების გაყიდვის სერვისი, რომელიც კიბერუსაფრთხოების პროფესიულ წრეებში მოიხსენიება, როგორც Ransomware as a Service (RaaS). DarkSide-ი აქტიურია საზოგადოებასთან ურთიერთობის კუთხითაც: იგი პოსტავს სხვადასხვა დარკნეტ ფორუმზე და აქვს საკუთარი ბლოგი, სადაც არაერთხელ მიუთითა, რომ მის შეტევებს განაპირობებს არა პოლიტიკური მიზნები, არამედ ეკონომიკური სარგებლის მიღების სურვილი.

ბოლო წლებში DarkSide-მა განახორციელა არაერთი შეტევა. მათ შორის, განსაკუთრებით აღსანიშნავია მიმდინარე წლის 7 მაისს აშშ-ის უმსხვილესი ნავთობპროდუქტების სადისტრიბუციო კომპანიის Colonial Pipeline-ის წინააღმდეგ განხორციელებული Ransomware-ის ტიპის შეტევა, რომელმაც მწყობრიდან გამოიყვანა კომპანიის საინფორმაციო და საკომუნიკაციო სისტემები და შედეგად, დაახლოებით ერთი კვირის განმავლობაში შეწყდა აშშ-ის აღმოსავლეთ სანაპიროსთვის განკუთვნილი ნავთობპროდუქტების 45%-ის მიწოდება.[2] ამით აშშ-ის ეკონომიკას ფედერალურ დონეზე მიადგა ათეულობით მილიონი დოლარის ზარალი, ხოლო ე.წ. ანაცდენი სარგებლის მასშტაბი ჯერაც არ არის სრულად დადგენილი. Colonial Pipeline-მა შეტევის აღსაკვეთად და დაშიფრული ფაილების განშიფვრისათვის გამოსასყიდის სახით 5 მილიონი აშშ დოლარი გადაიხადა, თუმცა, საბოლოოდ, აშშ გამოძიების ფედერალურმა ბიურომ მალევე მოახერხა გადახდილი თანხის უდიდესი ნაწილის, 4.4 მილიონი დოლარის, მსხვერპლისთვის დაბრუნება.[3]

კიდევ ერთი ორგანიზებული კიბერდანაშაულებრივი გაერთიანება, რომელიც აშშ-ისა და დასავლეთ ევროპის ქვეყნებში ახორციელებს ფართომასშტაბიან, ფინანსური სარგებლით მოტივირებულ დანაშაულებრივ ქმედებებს, დარკნეტში ცნობილია სახელწოდებით Revil. ამ დაჯგუფებამ თავდასხმა

მოაწყო ბრაზილიაში დაფუძნებულ ხორცის გადამამუშავებელ კომპანია JBS-ზე, რომელიც აშშ-ში ფლობს ხორცპროდუქტების მთავარ სადისტრიბუციო ქსელს. შეტევის შედეგად, Colonial Pipeline-ის შემთხვევის ანალოგიურად, დაიშიფრა JBS-ის სისტემური მართვის ფაილები და მასში გამოსასყიდის სახით მსხვერპლმა ორგანიზაციამ გადაიხადა 11 მილიონი აშშ დოლარი – კრიპტოვალუტა ბიტკოინში ანგარიშსწორებით[4]. უნდა აღინიშნოს, რომ DarkSide-ის მსგავსად, Revil-იც ინტენსიურად იყენებს RaaS მოდელს და ერთგვარი შუამავლის როლს ასრულებს მსხვერპლსა და შემტევ მხარეს შორის. ამ პროცესში იგი გარკვეულ საფასურსაც იღებს გაწეული მომსახურებისთვის.[5] აღსანიშნავია, რომ Revil-მა შეტევა განახორციელა პროგრამული სერვისების მომწოდებელ კომპანია Kaseya-ზეც. თუმცა, როგორც ირკვევა, აშშ-ის უმაღლესი ხელისუფლების ჩარევისა და რუსეთის ფედერაციასთან მოლაპარაკებების შედეგად, გარკვეული პერიოდის განმავლობაში, ჯგუფი Revil-ი და მისი ინფრასტრუქტურა საერთოდ გაქრა დარკნეტიდან, ხოლო Kaseya-მ მოახერხა უფასოდ მიეღო უნივერსალური დეკრიპტორი (დეშიფრაციის გასაღები)[6] თავისი ბენეფიციარი მსხვერპლი კომპანიებისთვის.[7]

რუსულ ორგანიზებულ დანაშაულებრივ ჯგუფებზე საუბრისას აუცილებლად უნდა შევეხოთ Evil Corps-ის სახელით ცნობილ კრიმინალურ სინდიკატსაც. მან სხვადასხვა მავნე პროგრამის გამოყენებით უკანონოდ, ფარულად მიითვისა აშშ-ის მოქალაქეების კუთვნილი 100 მილიონამდე დოლარი. ეს ჯგუფი ინტენსიურად იყენებდა აშშ-ში მყოფ პოსტსაბჭოთა ქვეყნების მოქალაქეებს, რათა სწორედ მათ გაენაღდებინათ უკანონოდ მითვისებული თანხები და გადაერიცხათ რუსეთსა და უკრაინაში, სადაც ცხოვრობდნენ Evil Corps-ის ლიდერი მაქსიმ იაკუბეცი და მასთან დანაშაულებრივ კავშირში მყოფი სხვა პირები[8]. წინა ორი ჯგუფისგან განსხვავებით, აშშ-ის სამართალდამცავი უწყებების ბრძოლა გაცილებით ეფექტიანი აღმოჩნდა Evil Corps-ის წინააღმდეგ: დადგინდა ჯგუფის ხელმძღვანელის ვინაობა, რომელზეც გამოცხადდა საერთაშორისო ძებნა და საჯაროდ გაცხადდა მისი კავშირი რუსეთის სადაზვერვო სამსახურებთან.[9]

დაბოლოს, ამ ქვეთავის შეჯამებისას, უნდა ითქვას შემდეგი მნიშვნელოვანი გარემოების შესახებ: მიუხედავად იმისა, რომ გარკვეული პერიოდით ჯგუფები DarkSide-ი და Revil-ი გაუჩინარდნენ და მათი ინფრასტრუქტურა ხელმიუწვდომელი იყო, მას შემდეგ, რაც SolarWinds Orion-ის გამო აშშ-სა და რფ-ს შორის შექმნილი დაძაბულობა განიმუხტა, ისინი კვლავ დაბრუნდნენ კიბერსივრცეში ძველი (Revil) ან შეცვლილი (Darkside) სახელწოდებებით.[10] იდენტური სიტუაციაა Evil Corps-თან დაკავშირებითაც, რომელიც თავისი ინფრასტრუქტურისა და მის მართვაში ჩართული პირების ნაწილის დაპატიმრების მიუხედავად, 2020 წელს კვლავ დაბრუნდა სხვა სახელით (WastedLocke Ransomware Group).[11]

რუსული ორგანიზებული კიბერდანაშაულებრივი ჯგუფების კავშირი რუსულ სპეცსამსახურებთან

ზემოაღნიშნული ჯგუფების რუსეთის სპეცსამსახურებთან კავშირის შესახებ არაერთი მტკიცებულება არსებობს და ეს ღიად არის გაცხადებული როგორც აშშ-ის ოფიციალური უწყებების, ისე კიბერუსაფრთხოების სხვადასხვა ავტორიტეტული ორგანიზაციების მხრიდან. შესაბამისად, ამ საკითხზე მსჯელობისას მაქსიმალურად რომ ავარიდოთ თავი სხვადასხვა ტიპის კონსპირაციას, დავეყრდნობით მხოლოდ აშშ-ის ოფიციალური უწყებების მიერ გასაჯაროებულ ინფორმაციას და ტექნიკური ექსპერტიზის იმ მონაცემებს, რომლებიც გამოაქვეყნეს კიბერუსაფრთხოების სფეროში მოქმედმა ცნობილმა კომპანიებმა.

აშშ-ის სავაჭრო დეპარტამენტის მონაცემებით Evil Corps-ის ხელმძღვანელი მაქსიმ იაკუბეცი ოფიციალურად იყო დაკავშირებული რუსეთის ფედერალური უშიშროების სამსახურთან, რომლის მითითებითაც პერიოდულად ახორციელებდა თავდასხმებს დაზვერვისათვის ღირებულ სამიზნეებზე.[12]

რუსეთის სპეცსამსახურებთან პირდაპირ კავშირზე მიუთითებს კიდევ ერთი ცნობილი კრიმინალის ევგენი ბოგაჩევის საქმიანობა და მის მიერ შემუშავებულ მავნე კოდში „Zeus“ ჩაშენებული მოდულები. უფრო კონკრეტულად კი, Zeus-ი თავდაპირველად გამოიყენებოდა ინფიცირებულ კომპიუტერებში არსებული საბანკო ინფორმაციის რეალურ დროში (მომენტი, როდესაც მსხვერპლს კონკრეტულ ონლაინ საბანკო პლატფორმაზე შეჰყავს საკუთარი ავტორიზაციის მონაცემები) მოსაპოვებლად.[13] 2015 წელს ბოგაჩევმა განაახლა და გამოუშვა Zeus-ის მოდიფიცირებული ვერსია, სახელწოდებით GameOverZeus. მასში აღმოჩნდა მავნე კოდის მოდულები. ამ მოდულებში გაწერილი საკვანძო სიტყვების მეშვეობით შესაძლებელი იყო საქართველოში, თურქეთსა და უკრაინაში ინფიცირებულ კომპიუტერებში იმ ტიპის დოკუმენტების მოძიება და ექსფილტრაცია, რომლებშიც მითითებული იყო აღნიშნული საკვანძო სიტყვები. უფრო კონკრეტულად კი, საქართველოსთან მიმართებით მავნე კოდი კონფიგურირებული იყო იმგვარად, რომ მსხვერპლ კომპიუტერებში მოეძებნა ნებისმიერი ფაილი, რომლის დასახელებაში ან უშუალოდ ტექსტში ეწერა შემდეგი საკვანძო სიტყვები: **საიდუმლო, რუსეთი, კრასნოდარი, საგარეო დაზვერვა.** საძიებო თემატიკა მსგავსი იყო თურქეთსა და უკრაინაშიც. სურათზე 1, საილუსტრაციოდ წარმოდგენილია გაშიფრული მავნე კოდის მოდულებში არსებული საძიებო სიტყვების კატალოგი ქართულ, თურქულ და უკრაინულ ენებზე:[14]

სუჰათი 1. წყარო: მ. სენდი, ტ. ვეჰნეჰი და ე. პეტეჰსონი

რუსეთის სპეცსამსახურებისა და მის ტერიტორიაზე მოქმედი ორგანიზებული კიბერდანაშაულებრივი დაჯგუფებების კავშირზე მიუთითებს კიდევ ერთი მნიშვნელოვანი გარემოება. კერძოდ, DarkSide-ის და Revil-ის მიერ დაწერილი მავნე კოდები ისეა კონფიგურირებული, რომ ისინი არ უნდა გაეშვას იმ კომპიუტერებზე, რომელთა სისტემურ პანელზე ინსტალირებულია რუსული ან ყოფილი საბჭოთა კავშირის რესპუბლიკების რომელიმე სხვა ენა (გამონაკლისია ბალტიისპირეთის სახელმწიფოთა ენები).[15] Revil-ის ასეთი პოლიტიკა ძირითადად იმ გარემოებას უკავშირდება, რომ პოსტსაბჭოთა ქვეყნებში ნაკლებია ფინანსურად მძლავრი ისეთი ორგანიზაციები, რომლებიც Colonial Pipeline-ის ან JBS-ის მსგავსად თანახმა იქნებიან და შეძლებენ მილიონობით დოლარი გადაიხადონ დაშიფრული მონაცემების განშიფვრაში.

ამასთანავე, საქართველოსა და უკრაინის გამოკლებით, რფ-ის სამართალდამცავ სისტემას საკმაოდ კარგი კავშირები აქვს პოსტსაბჭოთა ქვეყნების კოლეგა უწყებებთან. ამიტომ სავარაუდოა, რომ, საჭიროების შემთხვევაში, ისინი სამართლებრივი დახმარების თხოვნით რუსულ მხარეს მიმართავენ. დიდი ალბათობით, რუსეთი გამოეხმაურება მეზობელი სახელმწიფოების თხოვნას, რადგან მათ უმრავლესობასთან კრემლს სტრატეგიულად მნიშვნელოვანი ურთიერთობები აქვს და მოერიდება ამ კავშირების დაზიანებას.

გარდა ამისა, კომპიუტერების სისტემურ პანელზე რუსული ენის დამატება წარმოადგენს ძირითად დამზღვევს, რათა Revil-ის მსხვერპლთა წრის მასიური გაფართოებისას არ დაინფიცირდეს რუსეთის მოქალაქეების კომპიუტერები ან იქაური ფინანსური კორპორაციები, რაზეც კრემლი აუცილებლად მოახდენს

რეაგირებას. მით უმეტეს, რომ ამ კორპორაციების დიდ ნაწილს თავად რუსეთის სპეცსამსახურები მფარველობენ, რაც წარსული პრაქტიკითაც დასტურდება.[16]

საგულისხმოა ისიც, რომ რფ-ის სპეცსამსახურებსა კრიმინალურ აქტორებს შორის თანამშრომლობა არ ხორციელდება მხოლოდ კონფიდენციალურობის დაცვის პირობით. თუ კიბერკრიმინალით დაკავებული პირის საქმიანობა განსაკუთრებით ღირებულია რუსული სადაზვერვო უწყებებისთვის, ისინი მას საკუთარ რიგებშიც იღებენ ოფიცრის სტატუსით და რიგ შემთხვევებში აწინაურებენ კიდეც, კონკრეტულ სტრუქტურაში საშუალო და მაღალი რგოლის თანამდებობებზე. ამის საუკეთესო მაგალითია დმიტრი დოკუჩაევი, რომელიც Carding-ის (საკრედიტო ბარათების მოპარვა-გაყალბება) კუთხით რუსულ დარკნეტში ცნობილი პიროვნება იყო. შემდეგ, გარკვეული პერიოდი, ფედერალური უშიშროების სამსახურთან შეთანხმებით ოფიციალური საფარის გარეშე მუშაობდა, 2014 წლიდან კი ფედერალური უშიშროების სამსახურის მე-18 განყოფილების (საინფორმაციო ტექნოლოგიების ცენტრი) თანამშრომელი გახდა.[17]

რუსეთის სპეცსამსახურების შეტევის ვექტორისა და ტაქტიკის ცვლილება კიბერსივრცეში

როგორც ვნახეთ, ღია წყაროებზე დაყრდნობით ცალსახად დასტურდება რუსულ სპეცსამსახურებსა და რუსეთში არსებულ ორგანიზებულ კიბერკრიმინალურ გაერთიანებებს შორის კავშირი. ამ ქვეთავში კი განვიხილავთ, თუ როგორ ცვლის რფ-ის სადაზვერვო უწყებები საკუთარ შეტევით ტაქტიკასა და ვექტორს ამ ჯგუფების გამოყენებით.

SolarWinds Orion პლატფორმის გამოყენებით, აშშ-ის კრიტიკულ საინფორმაციო სექტორზე განხორციელებული შეტევის საპასუხოდ, თეთრმა სახლმა მიმდინარე წლის **15 აპრილს** სანქციები დაუწესა რუსეთის საგარეო დაზვერვის სამსახურს და მასთან უშუალო კავშირში მყოფ ორგანიზაციებს, რომლებიც ამ უწყებას შეტევითი დანიშნულების კიბერინსტრუმენტებით ამარაგებდნენ.[18] თეთრი სახლის მიერ დაწესებული სანქციები საკმაოდ მოცულობითია და მნიშვნელოვნად შეაფერხებს როგორც რუსეთის საგარეო დაზვერვის კიბერშეტევითი პოტენციალის განვითარებას, ისე მასთან უშუალო კავშირში მყოფი ორგანიზაციების კომერციულ ოპერირებას საერთაშორისო ბაზრებზე. ამასთანავე, თეთრ სახლში სანქციების დაწესების თაობაზე გაკეთებულ განცხადებაში აღნიშნულია, რომ აშშ ადეკვატურად და მკაცრად იმოქმედებს ყველა მსგავსი ტიპის ინციდენტზე[19].

ჩანს, რუსეთმა ეს „გაკვეთილი“ გაითვალისწინა. მაგრამ, როგორც რუსულ უმაღლეს პოლიტიკურ და უსაფრთხოების ხელმძღვანელობას სჩვევია, გადაწყვიტა შეემოწმებინა რამდენად შეასრულებდა აშშ-ის ახალი ადმინისტრაცია 15 აპრილს განცხადებულ დანაპირებს საპასუხო ზომების თაობაზე, მით უმეტეს, იმ ფონზე, რომ ის სულ რამდენიმე თვით ადრე მოვიდა ხელისუფლებაში.

შედეგად, მიმდინარე წლის **7 მაისს** DarkSide-მა განახორციელა ზემოხსენებული კიბერშეტევა Colonial Pipeline-ზე. ამ ქმედებით რფ-მ მოახერხა ორი ტაქტიკური, მაგრამ მნიშვნელოვანი მიზნის მიღწევა:

- შეამოწმა აშშ პრეზიდენტის ადმინისტრაციის მზაობა, უპასუხოს კრემლს ნაცვალგების პრინციპის საფუძველზე;
- ქმედება ისე განახორციელა, რომ არ გამოიწვია სრულმასშტაბიანი დაპირისპირება კიბერსივრცეში.

ამ მიზნებს რუსეთის სპეცსამსახურმა DarkSide-ის მეშვეობით ისე მიაღწია, რომ კიბერშეტევაზე პასუხისმგებლობა კრიმინალურ აქტორს დააკისრა, ხოლო კრემლმა პირდაპირი პასუხისმგებლობა აირიდა.[20]

კიბერშეტევას მალევე მოჰყვა შეერთებული შტატების პრეზიდენტის პასუხი (2021 წლის 13 მაისი). მან განაცხადა: „ჩვენ არ გვჯერა, რომ რუსეთის მთავრობა მონაწილეობდა ამ თავდასხმაში. მაგრამ გვაქვს საფუძვლიანი მიზეზი ვივარაუდოთ, რომ დამნაშავეები, რომლებმაც თავდასხმა განახორციელეს, რუსეთში ცხოვრობენ და თავდასხმაც იქიდან მოხდა“. პრეზიდენტმა ბაიდენმა რუსულ მხარეს მოუწოდა აღეკვეთა ამ შეტევის დამგეგმავი და განმახორციელებელი პირების საქმიანობა და ისინი სისხლის სამართლის პასუხისგებაში მიეცა. [21]

როგორც მოგვიანებით გამოჩნდა, აშშ ადმინისტრაციის ეს განცხადება და მიღებული ზომები, სამწუხაროდ, არ აღმოჩნდა შემაკავებელი ფაქტორი რუსეთის ფედერაციისთვის და რუსულმა მხარემ ორივე ტაქტიკურ მიზანს მიაღწია. უფრო კონკრეტულად, მიმდინარე წლის **30 მაისს** მორიგი შეტევა განახორციელა ცნობილმა რუსულმა ორგანიზებულმა კიბერდანაშაულებრივმა გაერთიანება Revil-მა და მწყობრიდან გამოიყვანა აშშ-ში ხორცის უმსხვილესი სადისტრიბუციო ქსელი და ქარხანა JBS.

კიბერშეტევის შემდეგ აშშ პრეზიდენტის ადმინისტრაციის პრესსპიკერმა ჯენ ფსაკიმ განაცხადა, რომ ამ შეტევაზე სათანადო რეაგირებისთვის აშშ განიხილავს ყველა ვარიანტს, მათ შორის, საპასუხო ქმედებებს ნაცვალგების პრინციპის საფუძველზე და გამოყენებული ინფრასტრუქტურის მოშლას.[22] თუმცა ამ ეტაპზე საკითხი იმით ამოიწურა, რომ მიმდინარე წლის 16 ივნისს მოწვეულ ჟენევის სამიტზე აშშ პრეზიდენტის ადმინისტრაციამ რფ პრეზიდენტს გადასცა კრიტიკული ინფრასტრუქტურის, კერძოდ, 16 სტრატეგიული ობიექტის სია, რომელსაც არ უნდა შეეხოს რუსეთის ტერიტორიიდან წარმოებული რაიმე ტიპის კიბერთავდასხმა.[23]

რუსულმა მხარემ, ჩვეულ სტილში, არ გაიზიარა აშშ პრეზიდენტის წინადადება და კიბერკრიმინალურმა სინდიკატმა Revil-მა კვლავ განახორციელა შეტევა. ამჯერად მისი სამიზნე იყო პროგრამული უზრუნველყოფის კომპანია Kaseya. მისი ქსელური მართვის პანელის კომპრომეტაციის შედეგად, ძირითადად, ევროპული კომპანიები დაზიანდა, თუმცა შეტევამ ნაწილობრივ ამერიკული

ბიზნესიც დააზარალა. ამ თავდასხმას მოჰყვა პრეზიდენტ ბაიდენის ზარი მოსკოვში. ბაიდენმა კვლავინდებურად მოუწოდა კოლეგას აღეკვეთა რუსეთის ტერიტორიაზე მოქმედი კიბერკრიმინალური აქტორების საქმიანობა.[24]

ყოველივე ზემოთქმულიდან გამომდინარე, ნათელია, რომ რუსულმა მხარემ აშშ-სა და ჩრდილოატლანტიკური ალიანსის წინააღმდეგ ინტენსიურად აამოქმედა თავის ტერიტორიაზე არსებული ორგანიზებული კიბერდანაშაულებრივი ჯგუფები. რფ ეფექტურად ახერხებს ამ ჯგუფების ნებისმიერი შეტევის ახსნას მარტივი, კრიმინალური მოტივებით. ასეთი მიდგომით, კრემლი მოცემულ მომენტამდე წარმატებით არიდებს თავს პირდაპირ პასუხისმგებლობას და უარყოფს პროცესში რაიმე ფორმით მონაწილეობას. ამ საქმეში რუსეთს ქმედით „დახმარებას“ უწევს ნეგატიური იმიჯი, რომელიც მან კრიმინალთან ბრძოლის კუთხით დაიმკვიდრა საერთაშორისო საზოგადოებაში. დასავლეთის ქვეყნების უსაფრთხოების სამსახურებისა და ზოგადად სამთავრობო წრეებისთვის საყოველთაოდ ცნობილი ფაქტია, რომ რუსეთის სამართალდამცავი სისტემა კორუმპირებულია და ნაკლებად შესწევს უნარი აკონტროლოს ორგანიზებული კრიმინალური სინდიკატების საქმიანობა. თუმცა ზემომოყვანილი ფაქტობრივი გარემოებები ნათლად გვიჩვენებს, რომ რუსეთის ფედერაციის სპეცსამსახურები სრულად მართავენ და იყენებენ თავის ტერიტორიაზე ბაზირებულ კიბერდამნაშავეებსა თუ მათ გაერთიანებებს.

ამასთან ერთად, ზემოაღნიშნული შეტევების ანალიზი და ქრონოლოგია ცხადყოფს, რომ რუსეთისთვის მარტოოდენ სანქციების პოლიტიკა ან, კიდევ უარესი, მხოლოდ განცხადებები და მოწოდებები არასაკმარისია და ისინი ვერ ასრულებენ შემაკავებელი მექანიზმის ფუნქციას. უფრო მეტიც, რუსეთი თავის ქმედებებზე არაპროპორციულ პასუხს სისუსტედ აღიქვამს, რაც მას სხვადასხვა მიმართულებით, მათ შორის, კიბერსივრცეში, უკანონობის ჩასადენად ახალისებს. ეს მოსაზრება განსაკუთრებით რელევანტურია აშშ-ის მოქმედი ადმინისტრაციის მიმართ, რომელიც მნიშვნელოვნად განსხვავდება ტრამპის კაბინეტისგან რუსეთთან დამოკიდებულების თვალსაზრისით. შესაბამისად, მოსალოდნელია, რომ კრემლი სულ უფრო ხშირად ეცდება მსგავსი მიდგომებით გამოიწვიოს შეერთებული შტატები, თანაც ისე, რომ მისგან არ მიიღოს პროპორციული პასუხი ნამოქმედარზე. თავის მხრივ, ამას, რფ საკუთარი დეზინფორმაციული სისტემის წყალობით, ლოკალური გამარჯვების შემთხვევებად გაასაღებს როგორც შიდა აუდიტორიისათვის, ისე საერთაშორისო ასპარეზზე.

მიგვაჩნია, რომ ასეთ ვითარებაში სრულად გასაზიარებელია აშშ ეროვნული უშიშროების საბჭოს მდივნის მიდგომა, რომელიც ფიქრობს, რომ რუსეთის წინააღმდეგ სანქციებთან ერთად საჭიროა მცირე მასშტაბის თავდაცვითი ოპერაციებიც.[25] შესაძლოა, ეს ოპერაციები გულისხმობდეს შეტევით კომპონენტსაც. მხოლოდ მსგავს მიდგომას შეუძლია რუსეთიდან მომდინარე კიბერსაფრთხეების შემცირება და კიბერსივრცეში კრემლის ქმედებების მეტ-ნაკლებად პროგნოზირება.

დასკვნა

დასკვნის სახით უნდა ითქვას, რომ ბოლო პერიოდში რუსეთის ფედერაციის მიერ კიბერსივრცეში ქცევისა და შეტევის ვექტორების შეცვლას, რომელიც გულისხმობს სადაზვერვო ორგანოების კიბერდანაყოფების ნაცვლად, რუსეთში ბაზირებული ორგანიზებული კიბერდამნაშავეების გამოყენებას ნატოს წევრი ქვეყნების წინააღმდეგ მნიშვნელოვანი მოტივაცია და მიზნები აქვს. კერძოდ, კრემლი ამ მიდგომით ცდილობს კვლავ განაგრძოს დესტრუქციული ქმედებები კიბერსივრცეში, თუმცა ისეთი ფორმით, რომ არ გამოიწვიოს აშშ-ის ხელისუფლების რეაქცია და სადამსჯელო ღონისძიებები რუსული სადაზვერვო აპარატის მიმართ. აღნიშნული მიდგომა საინტერესოა იმ კუთხითაც, რომ მისი საშუალებით რუსეთი აშშ-სა და, ზოგადად, დასავლურ სამყაროს აჩვენებს, რომ კონვენციურ კიბერსაშუალებებთან ერთად (FSB, SVR, GRU კიბერდანაყოფები), მას ჰყავს არაკონვენციური ძალებიც, რომლებსაც საჭიროების დროს აამოქმედებს და მათი ვითომ პარტიზანული მოქმედება არანაკლები ზიანის მომტანი იქნება დასავლეთისთვის, თან ისე, რომ კრემლი შესაბამის ფასს არ გადაიხდის. ყოველ შემთხვევაში, არ იარსებებს სათანადო, მყარი სამართლებრივი არგუმენტები, რომლებიც დაფუძნებული იქნება ციფრულ მტკიცებულებებზე.

აშშ-სა და ჩრდილოატლანტიკურ ალიანსს სჭირდება საპასუხო სტრატეგიის შემუშავება, რომელიც დაეფუძნება პროპორციული ან/და ასიმეტრიული პასუხის პრინციპებს, რათა მაქსიმალურად მტკივნეული და დამაზიანებელი აღმოჩნდეს კრემლისთვის. ამ სტრატეგიის ნაწილი შესაძლოა გახდეს საქართველოც, იმ შემთხვევაში, თუ კრემლი საკუთარ არაკონვენციურ კიბერშეტევით საშუალებებს აამოქმედებს ჩვენი ქვეყნის წინააღმდეგ.

ბიბლიოგრაფია

1. *FireEye, Shining a Light on DARKSIDE Ransomware Operations,* ხელმისაწვდომია ბმულზე: *https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html;* ბოლოს ნანახია: 21/09/2021.

2. NPR, *What We Know About The Ransomware Attack On A Critical U.S. Pipeline,* ხელმისაწვდომია ბმულზე: https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline; ბოლოს ნანახია: 21/09/2021.

3. BBC, *Colonial Pipeline: US Recovers Most of Ransom, Justice Department Say*, ხელმისაწვდომია ბმულზე: https://www.bbc.com/news/business-57394041; ბოლოს ნანახია: 21/09/2021.

4. BBC, *Meat Giant JBS Pays $11m in Ransom to Resolve Cyber-Attack*, ხელმისაწვდომია ბმულზე: https://www.bbc.com/news/business-57423008 ; ბოლოს ნანახია: 21/09/2021.

5. Palo Alto Networks, *Understanding REvil: The Ransomware Gang Behind the Kaseya VSA Attack*, ხელმისაწვდომია ბმულზე: https://unit42.paloaltonetworks.com/revil-threat-actors/; ბოლოს ნანახია: 21/09/2021.

6. Zdnet, *Kaseya Says It Has Now Got the REvil Decryption Key and It Works*, ბოლოს ნანახია: 21/09/2021; ხელმისაწვდომია ბმულზე: *https://www.zdnet.com/article/kaseya-says-it-has-now-got-the-revil-ransomware-decryption-key-and-it-works/*

7. იქვე.

8. KrebsonSecurity, Inside 'Evil Corp,' a $100M Cybercrime Menace, ხელმისაწვდომია ბმულზ: https://krebsonsecurity.com/2019/12/inside-evil-corp-a-100m-cybercrime-menace/ ბოლოს ნანახია: 21/09/2021.

9. US DoJ, *Russian National Charged with Decade-Long Series of Hacking and Banking Fraud[..],* ხელმისაწვდომია ბმულზე: https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens; ბოლოს ნანახია 21/09/2021.

10. The Quartz, *The Colonial Pipeline Ransomware Gang is Back Under a New Name,* ხელმისაწვდომია ბმულზე: https://qz.com/2043312/the-colonial-pipeline-ransomware-gang-is-back-under-a-new-name/; ბოლოს ნანახია: 21/09/2021; Zdnet, *REvil Ransomware Group Resurfaces After Brief Hiatus,* ხელმისაწვდომია ბმულზე: https://www.zdnet.com/article/revil-ransomware-group-resurfaces-after-brief-hiatus/; ბოლოს ნანახია: 21/09/2021.

11. CybersecurityHelp, *Evil Corp Gang is Back with New WastedLocker Ransomware,* ხელმისაწვდომია ბმულზე: https://www.cybersecurity-help.cz/blog/1338.html; ბოლოს ნანახია: 21/09/2021.

12. US Department of Treasury, *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware*, ხელმისაწვდომია ბმულზე: https://home.treasury.gov/news/press-releases/sm845; ბოლოს ნანახია: 21/09/2021.

13. Analyst1, *Nation State Ransomware*¸ გვ, 7-8, ხელმისაწვდომია ბმულზე: https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf; ბოლოს ნანახია: 21/09/2021.

14. Michael Sandee, Tillmann Werner, Elliott Peterson: *Gameover Zeus – Bad Guys and Backends,* ხელმისაწვდომია ბმულზე: https://www.blackhat.com/docs/us-15/materials/us-15-Peterson-GameOver-Zeus-Badguys-And-Backends.pdf; ბოლოს ნანახია: 22/09/2021/

15. Trustwave, *Diving Deeper Into the Kaseya VSA Attack: REvil Returns and Other Hackers Are Riding Their Coattails,* ხელმისაწვდომია ბმულზე: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/diving-deeper-into-the-kaseya-vsa-attack-revil-returns-and-other-hackers-are-riding-their-coattails/; ბოლოს ნანახია: 22/09/2021.

16. Recorded Future, *Dark Covenant: Connections Between the Russian State and Criminal Actors, გვ-14-15;* ხელმისაწვდომია ბმულზე: https://www.recordedfuture.com/russian-state-connections-criminal-actors/ ; ბოლოს ნანახია: 22/09/2021.

17. იქვე.

18. The White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government,* ხელმისაწვდომია ბმულზე: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/; ბოლოს ნანახია: 22/09/2021.

19. იქვე.

20. Recorded Future, *Dark Covenant: Connections Between the Russian State and Criminal Actors, p. 15.*

21. The White House, *Remarks by President Biden on the Colonial Pipeline Incident,* ხელმისაწვდომია ბმულზე: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/; ბოლოს ნანახია: 22/09/2021.

22. ABC News, *White House Puts Blame on Russia for JBS Ransomware Attack, Weighs Responses,* ხელმისაწვდომია ბმულზე: https://abcnews.go.com/Business/white-house-contact-russia-meat-producer-jbs-hit/story?id=78021754; ბოლოს ნანახია: 22/09/2021.

23. Yahoo News, *Biden Gave Putin List of 16 Critical Infrastructure 'entities' that Must be Off-Limits to Cyberattacks,* ხელმისაწვდომია ბმულზე: https://news.yahoo.com/biden-gave-putin-list-16-175500657.html; ბოლოს ნანახია 22/09/2021.

24. CNN, Biden Warns Putin during Call that 'we Expect Him to Act' on Russian Ransomware Attacks, ხელმისაწვდომია ბმულზე: https://edition.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html; ბოლოს ნანახია: 22/09/2021

25. NY Times, *Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China*; ხელმისაწვდომია ბმულზე: https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html; ბოლოს ნანახია: 21/09/2021.