RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

ბოლო დროის ყველაზე დიდი რუსული კიბერსადაზვერვო ოპერაცია – SOLARWINDS–ზე შეტევის MODUS OPERANDI

გიორგი უზარაშვილი

161

ექსპერტის აზრი

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

ექსპერტის აზრი

გიორგი უზარაშვილი

ბოლო დროის ყველაზე დიდი რუსული კიბერსადაზვერვო ოპერაცია – SOLARWINDS–ზე შეტევის MODUS OPERANDI

161

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

2020 წელს SolarWinds-ზე განხორციელებული შეტევა არის აშშ-ის ისტორიაში ერთ-ერთი ყველაზე მასშტაბური კიბერსადაზვერვო კამპანია, რომელმაც დააზიანა ისეთი უწყებები, როგორიცაა აშშ-ის თავდაცვის დეპარტამენტი (DoD), ეროვნული უსაფრთხოების დეპარტამენტი (DHS), ინფრასტრუქტურისა და კიბერუსაფრთხოების დაცვის სააგენტო (CISA).[1] ცნობისათვის, SolarWinds-ი არის აშშ-ში რეგისტრირებული კომპანია, რომელიც კერძო და საჯარო სექტორს უწევს IT სფეროსთან დაკავშირებულ არაერთ მომსახურებას, მათ შორის, სთავაზობს ისეთ ხელსაწყოებს, რომლებიც გამოიყენება ქსელური ინფრასტრუქტურის დისტანციური მართვის მიზნებისათვის.[2] შეტევა მოგვიანებით, მიმდინარე წლის აპრილში, ოფიციალურად ბრალად შეერაცხა[3] რუსეთის საგარეო დაზვერვის სამსახურს (СВР - Служба Внешней Разведки). მისი შედეგების სიმძიმეს განაპირობებს არა მხოლოდ ის გარემოება, რომ შემტევმა მხარემ, სავარაუდოდ, წვდომა მოიპოვა იმ ინფორმაციის ნაწილზე მაინც, რომელსაც ფლობენ აშშ-ის ზემოხსენებული უწყებები, არამედ, პირველ რიგში, ამ ოპერაციის სადემონსტრაციო ეფექტი. კერძოდ, შემტევმა მხარემ აჩვენა, რომ რუსული კიბერსადაზვერვო აქტორების წინაშე დაცული არავინაა, მათ შორის, არც ის უწყებები, რომელთაც თავადვე აქვთ ეროვნული კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების უზრუნველყოფის ვალდებულება მთელი ქვეყნის მასშტაბით.

შესაბამისად, SolarWinds-ზე განხორციელებული შეტევა აშშ-ს აზიანებს არა მხოლოდ უსაფრთხოების, უფრო კონკრეტულად კი, კიბერდაცულობის თვალსაზრისით, არამედ მნიშვნელოვან გამოწვევას უქმნის მის რეპუტაციას. კერძოდ, კითხვის ნიშნის ქვეშ აყენებს, რამდენად ჰყავთ აშშ-ის უსაფრთხოების ორგანოებს მაღალი კვალიფიკაციური პერსონალი და აქვთ სათანადო ტექნიკური აღჭურვილობა მნიშვნელოვანი ინფორმაციული აქტივების დასაცავად და ამგვარი შეტევების აღსაკვეთად. ამასთან, იქმნება საფრთხე, რომ ეს შემთხვევა მომავალში წაახალისებს სხვა მტრულ აქტორებს, მსგავსად იმოქმედონ აშშ-ის წინააღმდეგ. ასეთი აქტორები კი, პირველ რიგში, არიან ჩინეთი და ირანი.

შესაბამისად, SolarWinds-ზე განხორციელებულმა შეტევამ, წესით, აშშ-ის კიბერუსაფრთხოების სისტემაში არსებითი განახლების პროცესი უნდა გამოიწვიოს, რადგან ამ სექტორში თუ არ

შეიცვლება ბიზნესპროცესები, საკმაოდ მაღალია ხელახალი კომპრომეტაციის რისკი.

ზემოაღნიშნულის გათვალისწინებით, ბაიდენის ადმინისტრაცია, სავარაუდოდ, არ აპირებს შემოიფარგლოს მხოლოდ სანქციებით, როგორც მოიქცა ტრამპის ადმინისტრაცია, როდესაც 2016 წლის ბოლოს მხოლოდ სანქციები დაუწესა რუსეთის სამხედრო დაზვერვის სამსახურს. ამრიგად, მოსალოდნელია გაცილებით მწვავე საპასუხო ზომები[4], ვინაიდან ფაქტია, რომ მხოლოდ სანქციების პოლიტიკა ვერ იქნება შემაკავებელი ფაქტორი კრემლისათვის. შესაბამისად, სავარაუდოა, რომ SolarWinds-ზე შეტევა გასცდება „უსაფრთხოების ყოფითი ინციდენტის“ ფარგლებს და შეიძენს მზარდი პოლიტიკური დაძაბულობის ხასიათს.

SolarWinds-ზე შეტევა აქტუალურია საქართველოსთვისაც, რადგან ჩვენი ქვეყანა შედის SolarWinds-ის დაფარვის ზონაში და ამ გეოგრაფიულ არეალს ემსახურება ორგანიზაციის კიევის ოფისი.[5] ამრიგად, სავსებით შესაძლებელია, რომ საქართველოში არსებული ცალკეული კერძო თუ საჯარო დაწესებულებები სარგებლობდნენ SolarWinds-ის რიგი სერვისებით. სხვაგვარად, ბიზნესკონტაქტის არარსებობის შემთხვევაში, ნაკლებსავარაუდოა, რომ SolarWinds-ს საქართველო საკუთარი კომერციული ოპერირების ზონად გამოეცხადებინა.

იმ შემთხვევაშიც კი, თუ დავუშვებთ, რომ საქართველოში არსებული იურიდიული თუ ფიზიკური პირები არ სარგებლობენ უშუალოდ SolarWinds-ის კომპრომეტირებული სერვისით, დარწმუნებით შეიძლება ითქვას, რომ მათი მნიშვნელოვანი ნაწილი იყენებს ქსელური ინფრასტრუქტურის დისტანციური მართვის სხვა კერძო კომერციულ ხელსაწყოებს (Toolkit). შესაბამისად, სავსებით შესაძლებელია, რომ მათ დაცულ ინფრასტრუქტურაში მოხდეს SolarWinds-ის მსგავსი შეტევითი მეთოდით შეღწევა.

ამრიგად, წინამდებარე დოკუმენტის მიგნებები აქტუალურია საქართველოში არსებული ნებისმიერი ორგანიზაციისათვის, რომელიც გარკვეული ფორმით იყენებს კერძო სექტორის მიერ მოწოდებულ ციფრულ სერვისებსა თუ პროდუქტებს, ასევე – in-house შექმნილ ხელსაწყოებთან მიმართებით, რომელიც გამოიყენება შიდა ქსელური თუ სხვა ტიპის ინფრასტრუქტურის მენეჯმენტის მიზნებისთვის.

შეტევის აღწერა – ტექნიკური და ოპერატიული დეტალები

2020 წლის დეკემბერში აშშ-ში მოქმედმა კიბერუსაფრთხოების კერძო კომპანიამ FireEye გამოავლინა ამავე ქვეყანაში რეგისტრირებულ კომპანია SolarWinds-ის მიერ მოწოდებულ სერვისში ჩაშენებული მავნე კოდით ინფიცირების ფაქტი, რომლის უკანაც საწყის ეტაპზევე მოიაზრებოდა მავნე რუსული აქტორი[6]. 2021 წლის აპრილში ეს შეტევა ბრალად ოფიციალურად შეერაცხა რუსეთის ფედერაციის საგარეო დაზვერვის სამსახურს. შეტევის ძირითადი ფუნქციონალი გულისხმობდა მავნე კოდის ჩაშენებას SolarWinds-ის ერთ-ერთ სერვისში და მის აქტივაციას სამიზნე ორგანიზაციებში. SolarWinds-ის ამ კონკრეტულ სერვისს იყენებდნენ ბენეფიციარი ორგანიზაციები (დაახლოებით 18 000 ერთეული ორგანიზაცია მთელი მსოფლიოს მასშტაბით) ქსელური ინფრასტრუქტურის დისტანციური მართვისთვის.

SolarWinds-ის წინააღმდეგ განხორციელებული შეტევა შეიძლება 5 ფაზად დაიყოს. ეს დაყოფა ეფუძნება შეტევასთან დაკავშირებული ანგარიშებისა თუ სხვა მასალების დეტალურად შესწავლასა და, ასევე, ჩვენ მიერ ვირტუალურ გარემოში ჩატარებული (პროგრამული უზრუნველყოფა Virtual Box-ის ვირტუალური მანქანით, რომელიც დაინსტალირდა ოპერაციულ სისტემაზე Windows 10x64) ინფიცირებული .dll-failis ნაწილობრივი ანალიზის შედეგებს.

I ფაზა

საწყის ეტაპზე შემტევმა მხარემ მოახერხა შეეღწია კომპანია SolarWinds-ის დაცულ ინფრასტრუქტურაში. შედეგად, იგი ფარულად ჩაინერგა SolarWinds Orion-ის პროგრამული განახლების (Update) შემმუშავებელ პროგრამისტთა კომუნიკაციის პროცესში. აღსანიშნავია, რომ კონკრეტულ პროგრამულ სერვისზე მომუშავე სპეციალისტების პრაქტიკით, ისინი ინაწილებენ ფუნქციებს და ცალკეულ მოდულებს, რომელსაც თითოეული მათგანი დამოუკიდებლად ამუშავებს და რაღაც ეტაპზე ახორციელებს მის გაერთიანებას კოლეგა პროგრამისტის შემუშავებულ პროდუქტთან.[7] რუსეთის საგარეო დაზვერვის სამსახურს, კონკრეტულად კი, მის კიბერსადაზვერვო დაჯგუფებას (APT 29), სწორედ ამ პროცესთან ჰქონდა წვდომა. შესაბამისად, იგი პარალელურად თვითონაც ამუშავებდა მავნე კოდის მოდულებს, რომელიც ლეგიტიმურ კოდთან ერთად უნდა ჩაშენებულიყო პროგრამული განახლების პაკეტში.

შეტევის განხორციელების პროცესში არსებითი იყო SolarWinds-ის ინფრასტრუქტურაზე წვდომა, რადგან SolarWinds-ის შიდა ინფრასტრუქტურაზე წვდომამ APT 29-ს საშუალება მისცა უზრუნველეყო საკუთარი მავნე კოდის თავსებადობა ინფიცირებული პროგრამული განახლების სხვა ლეგიტიმურ ნაწილებთან. შედეგად, მისი აღმოჩენის ალბათობა მინიმუმამდე შემცირდა.

სწორედ ეს ეტაპი წარმოადგენს ჩვენი კვლევის ყველაზე პრობლემურ ნაწილს, რადგან ღია წყაროებში არ არსებობს სარწმუნო ინფორმაცია შემტევი აქტორის მხრიდან SolarWinds-ის შიდა ქსელური ინფრასტრუქტურის კომპრომეტაციის თაობაზე. არსებობს მხოლოდ ვერსიები, რომლებიც ჯერჯერობით არ არის გამყარებული სათანადო ციფრული მტკიცებულებებით.

ამრიგად, ძირითადად ორი ვერსია იკვეთება. პირველის თანახმად, კომპანიის შიდა ქსელის კომპრომეტაცია განახორციელა ინსაიდერმა. აქ ისიც უნდა გავითვალისწინოთ, რომ აღმოსავლეთ ევროპაში SolarWinds-ს აქვს ოფისები, ასევე ცნობილია, რომ ამ რეგიონში რუსეთის სპეცსამსახურებს აქვთ მნიშვნელოვანი გავლენა და სხვადასხვა ორგანიზაციაში ინფილტრაციისთვის საჭირო ოპერატიული რესურსი[8].

მეორე ვერსიით, რომლის ავტორიცაა ამავე კომპანიის ყოფილი აღმასრულებელი დირექტორი, რუსულმა კიბერსადაზვერვო აქტორმა SolarWinds-ში შეაღწია სტაჟიორის მარტივი პაროლის შერჩევითი გატეხვის მეთოდით (Password Brute Force Attack).[9] ეს ვერსია გარკვეულ წინააღმდეგობებს შეიცავს: ერთი მხრივ, მის ავტორს არ წარმოუდგენია არავითარი ფაქტობრივი მასალა საკუთარი პოზიციის დასასაბუთებლად, ხოლო, მეორე მხრივ კი, ამ ვერსიის მართებულობის შემთხვევაში, დადასტურდება კომპანიის ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემური ჩავარდნა, რადგან დაუშვებელია სტაჟიორს ჰქონდეს იმ დონის დაშვება შიდა ინფორმაციულ ინფრასტრუქტურაზე, რომ მისი ავტორიზაციის მონაცემების კომპრომეტაციამ გამოიწვიოს ყველაზე მნიშვნელოვანი შიდასაუწყებო ინფორმაციული აქტივების უკანონო ექსპლოატაცია.

II ფაზა

ამ ფაზის მიმდინარეობისას მოხდა Solarwinds-ის კონკრეტული სერვისის განახლების პროცესის გადაჭერა, მასში შეღწევა და ლეგიტიმურ მოდულებში მავნე კოდის იმგვარად ჩაშენება, რომ იგი შეუმჩნეველი ყოფილიყო უშუალოდ განახლების პაკეტზე მო-

მუშავე პროგრამისტებისთვის. ერთ-ერთი მავნე კოდის ნაწილი, რომელიც შემტევმა მხარემ ჩააშენა ლეგიტიმურ კოდში, მიეკუთვნებოდა StellarParticle-ის ჯგუფს (არაოფიციალური სახელწოდებით SUNPOST-ი), რომელიც, თავის მხრივ, გამოიყენეს SolarWinds Orion-ის პროგრამული განახლების პაკეტში არალეგიტიმური წვდომის არხის ე.წ Backdoor ჩასაშენებლად[10]. ამ უკანასკნელს კიბერუსაფრთხოების სხვადასხვა კომპანია მოიხსენიებს კოდური სახელწოდებით SUNBURST.[11] მავნე კოდის შეუმჩნევლად გაბნევა შემტევი აქტორისთვის მისი ოპერაციული უსაფრთხოების ქვაკუთხედს წარმოადგენდა, რადგან თუ მოცემულ ეტაპზე გაიშიფრებოდა, მაშინ მთელი ოპერაცია ჩავარდებოდა და მის შეტევის მეთოდიკასაც მსხვერპლი ორგანიზაციის ინფორმაციული უსაფრთხოების პერსონალი მარტივად გაიგებდა.[12]

III ფაზა

SolarWinds-ზე შეტევის ეს ეტაპი გულისხმობდა სამიზნე ორგანიზაციაში პირველად შეღწევას, უშუალოდ მას შემდეგ, რაც კონკრეტულმა ბენეფიციარმა გაუშვა ინფიცირებული პროგრამული განახლების პაკეტი საკუთარ საკომუნიკაციო და საინფორმაციო სისტემებში. ამ პროდუქტში ჩაშენებული მავნე კოდის პირველადი ფუნქციონალი ე.წ. Backdoor-ი აგროვებდა ორგანიზაციის შიდა ინფრასტრუქტურის თაობაზე ინფორმაციას და ტექსტური ფორმატით უგზავნიდა შემტევ მხარეს. შემტევი მხარე, მიღებულ ინფორმაციაზე დაყრდნობით, რომელიც ძირითადად შეიცავდა მონაცემებს დაინფიცირებული ორგანიზაციის ქსელური ინფრასტრუქტურის კონფიგურაციის თაობაზე, იწყებდა სამიზნე ორგანიზაციის შიდა სპეციფიკაზე მორგებულ შეტევას. შესაბამისად, ინფიცირების შემდგომი ტაქტიკა და მეთოდიკა განსხვავებული იყო. ამრიგად, მიღებული მონაცემები შემტევ მხარეს აძლევდა ზუსტ სურათს, თუ სად იყო ინფორმაციული უსაფრთხოების ე.წ. შავი ხვრელები, რომელთა ექსპლუატირებით სადაზვერვო აქტორმა ინფიცირებულ ორგანიზაციასთან კიდევ ერთი დამატებითი წვდომის არხი, ე.წ. Backdoor-ი, ჩააშენა. შემტევი მხარის ხსენებულ მიდგომას უდიდესი მნიშვნელობა აქვს შეტევის განგრძობადობისა და უწყვეტობისთვის. კერძოდ, APT 29 ცდილობდა პირველადი წვდომის არხი შეენიღბა მაქსიმალურად, ვინაიდან სამიზნე ორგანიზაციიდან ინფორმაციის არალეგალური, ფართომასშტაბიანი ექსტრაქცია ქმნიდა სადაზვერვო საქმიანობის გაშიფვრის მაღალ რისკებს. შესაბამისად, სადაზვერვო აქტორი მართებულად აანალი-

ზებდა, რომ თუ მოხდებოდა პირველადი წვდომის არხის გაშიფვრა, შემტევი მხარისათვის იხურებოდა თავად კომპანია SolarWinds-ის პროდუქტში ჩაშენებული მავნე კოდის შემდგომი ექსპლუატირების შესაძლებლობა.

IV ფაზა

შეტევის მეოთხე ეტაპზე APT 29-მ დაიწყო სადაზვერვო ოპერაციის ყველაზე აქტიური და მასშტაბური ფაზა, რაც გულისხმობდა სამიზნე ორგანიზაციიდან ოპერატიულად საინტერესო მონაცემების შერჩევასა და მის ექსფილტრაციას. აღნიშნულის განსახორციელებლად შემტევი მხარე იყენებდა Cobalt Strike-ის მავნე კოდის მოდიფიცირებულ ვერსიას. თავის მხრივ, Cobalt Strike-ი მიეკუთვნება კიბერსავარჯიშოების ხელსაწყოთა ტიპს, რომელთაც აქვთ ფართომასშტაბიანი და მრავალეტაპიანი შეღწევადობის ტესტისათვის (Penetration Test) საჭირო არაერთი კომპლექსური და ეფექტური შეტევითი ფუნქციონალი.[13] ამასთან, სადაზვერვო აქტორმა საკუთარი ოპერატიული პრიორიტეტების შესაბამისად შეცვალა ხსენებული ხელსაწყოს ფუნქციების ნაწილი, რათა გვერდი აევლო სამიზნე ორგანიზაციის ქსელური თუ შიდა ინფორმაციული უსაფრთხოების შესაბამისი კონფიგურაციის ჩარჩოსთვის.[14]

V ფაზა

შეტევის საბოლოო ეტაპზე შემტევი მხარე იწყებდა ორგანიზაციის შიგნით ე.წ. გვერდით მოძრაობას (Lateral Movement), რომლის უმთავრესი მიზანი იყო, რაც შეიძლება მეტ რესურსზე წვდომის მოპოვება მსხვერპლ ორგანიზაციაში, რადგან SolarWinds-ის ინფიცირებული პროგრამული განახლების პაკეტის სისტემაში გაშვება რიგ ორგანიზაციებში ავტომატურად არ იწვევდა ინფორმაციულ ინფრასტრუქტურაზე სრულ წვდომას შიდა ქსელური კონფიგურაციისა თუ მის ცალკეულ სეგმენტთა ერთმანეთისაგან მკაცრი გამიჯვნის გამო. შესაბამისად, სადაზვერვო აქტორის ერთ-ერთ უმთავრეს ამოცანას წარმოადგენდა მაქსიმალურად გაეფართოებინა შეტევის არეალი და მოეხდინა ინფორმაციული ინფრასტრუქტურის იმ სეგმენტის ინფიცირებაც, რომელიც, უსაფრთხოების პრინციპებიდან გამომდინარე, გარე ქსელთან პირდაპირ არ იყო დაკავშირებული. ამასთან, გვერდითი მოძრაობის ერთ-ერთ პრიორიტეტულ მიმართულებას წარმოადგენდა ე.წ. Rootkit-ის ტიპის მავნე კოდის შემცველი ხელსაწყოების ინსტალაცია ინფიცირებულ სისტემებში, რათა მათი მეშვეობით სადაზვერვო აქტორს შეენარ-

ჩუნებინა წვდომა სამიზნე ორგანიზაციებში იმ შემთხვევაშიც კი, თუ ჩატარდებოდა კომპრომეტირებული სისტემების კომპლექსური განახლება.

შეტევის შერაცხადობა (Attribution)

როგორც უკვე აღინიშნა, მიმდინარე წლის 15 აპრილს აშშ-ის პრეზიდენტის ადმინისტრაციამ გამოაქვეყნა განცხადება, რომლის თანახმადაც, SolarWinds-ზე შეტევა ბრალად ოფიციალურად შეერაცხა რფ-ის საგარეო დაზვერვის სამსახურის კიბერსადაზვერვო დაჯგუფებას, იგივე APT 29-ს.[15] ამ განცხადების შემდგომ აშშ-ის სპეცმსახურებმა გამოაქვეყნეს ერთობლივი შეფასებისა და რეკომენდაციების დოკუმენტი, რომელშიც საუბარია CBP-ის მიერ SolarWinds Orion-ის პლატფორმის ექსპლოატირების შედეგად ამავე პროგრამული უზრუნველყოფის ბენეფიციარი უწყებების ინფიცირების მეთოდსა და ტექნიკაზე, ასევე ამ პროცესში გამოყენებული მავნე კოდის ცალკეული მოდულების თაობაზე.[16]

აღნიშნული საინფორმაციო და ტექნიკური ანალიზის ტიპის დოკუმენტების გამოქვეყნების მიუხედავად, ჯერჯერობით არ არსებობს საჯარო დოკუმენტი, რომელიც ფაქტობრივ გარემოებებზე დაყრდნობით დაასაბუთებდა, რატომ შეერაცხება აღნიშნული შეტევა მაინც და მაინც რფ-ის საგარეო დაზვერვის სამსახურს და არა, მაგალითად, სამხედრო დაზვერვას, რომელიც დასავლეთის ქვეყნებში უფრო ცნობილია მავნე კიბერაქტივობებით. შესაბამისად, ჩვენი დოკუმენტის ფარგლებში წარმოდგენილი იქნება რამდენიმე არგუმენტი, რითაც ვეცდებით, დამატებითი ფაქტობრივი მონაცემებით გავამყაროთ SolarWinds-ზე შეტევის CBP-ისთვის შერაცხადობა.

ამ კუთხით, პირველ რიგში, მნიშვნელოვანია რეალურ სივრცეში რუსეთის სპეცსამსახურების ოპერატიული დაინტერესების ობიექტებისა და მიზნების იდენტიფიცირება, ვინაიდან სწორედ აღნიშნული გარემოება წარმოადგენს ამ ტიპის შეტევის ვექტორის ერთ-ერთ მთავარ მაიდენტიფიცირებელ ფაქტორს, რა თქმა უნდა, ტექნიკური და ოპერატიული მეთოდიკის ანალიზთან ერთად. სხვაგვარად, მხოლოდ modus operandi-ზე დაყრდნობით ხსენებული შეტევის რომელიმე კონკრეტული სპეცსამსახურისთვის ბრალად შერაცხვა არასრულყოფილი იქნება, თუ გავითვალისწინებთ, რომ უკანასკნელ წლებში რიგი სპეცსამსახურები (მაგალითად, რუსული APT 29 TURLA ჯგუფი) აქტიურად ახორციელებენ

სხვა სადაზვერვო უწყებების ინფიცირებას და მათი ინფრასტრუქტურის გამოყენებას, რათა ოპერაციის ჩავარდნის შემთხვევაში, გამოძიების კვალი შეწყდეს შუალედურ ქვეყანაში და შედეგად, შეტევის რეალური განმახორციელებელი დაუდგენელი დარჩეს.[17]

ამრიგად, დამატებით არის მხედველობაში მისაღები, რომ ეს ოპერაცია იყო წმინდად სადაზვერვო ტიპის და მას არ გააჩნდა კიბერსაბოტაჟის ან სხვა ტიპის აქტიური ღონისძიებების ხასიათი. ეს ფაქტორი დიდწილად ამცირებს მოცემული ოპერაციის რფ-ის ГРУ-ს (Главное Разведывательное Управление) მიერ განხორციელების შესაძლებლობას, ვინაიდან რუსეთის სამხედრო დაზვერვის მიერ ორგანიზებული შეტევების ანალიზი ცხადყოფს, რომ მათთვის კონკრეტული სადაზვერვო ოპერაცია წარმოადგენს ე.წ. აქტიური ღონისძიებების ნაწილს და გათვლილია მოკლევადიან პერიოდზე. კერძოდ, მას შემდეგ, რაც ГРУ მოიპოვებს მისთვის საჭირო მონაცემებს და დადგება კრემლისთვის ხელსაყრელი მომენტი ამ ინფორმაციის გამოქვეყნებისათვის, რუსეთის სამხედრო დაზვერვა, როგორც წესი, „აქტიური ღონისძიებების“ ფარგლებში ასაჯაროებს ამ ტიპის ინფორმაციას და შედეგად, პრაქტიკულად თავადვე სპობს საკუთარ სადაზვერვო პლაცდარმს.[18] მოცემული ოპერაცია კი იყო ორგანიზებული იმგვარად, რომ სამიზნე დაწესებულებებიდან რაც შეიძლება დიდხანს მომხდარიყო მნიშვნელოვანი ინფორმაციის უსაფრთხო ექსფილტრაცია და ამ პროცესის უწყვეტობა წარმოადგენდა გენერალურ ხაზს მთელი ოპერაციის განმავლობაში.

ამასთან, ნაკლებსავარაუდოა, რომ მოცემული ოპერაციის უკან იდგეს რუსეთის ფედერალური უშიშროების სამსახური (Федеральная Служба Безопасности – ФСБ), მიუხედავად იმისა, რომ ФСБ-ს მიერ ჩატარებული კიბეროპერაციებიც დიდწილად წმინდად სადაზვერვო მიზანს ემსახურება. ამასთან, APT 29 TURLA ჯგუფი უშუალოდ უკავშირდება ФСБ-ს, რომლის ძირითადი ოპერატიული ფოკუსი კიბერსივრცეში სადაზვერვო საქმიანობის წარმოებაა.[19]

აღსანიშნავია, რომ ФСБ SolarWinds-ზე შეტევის ოპერაციას ალბათ მაინც ვერ განახორციელებდა, საკუთარ სამიზნეთა სპეციფიკურობისა და ოპერატიული მოქმედების განსხვავებული არეალის გამო. ФСБ-ის ოპერაციების ძირითადი გეოგრაფიული ზონა არის ევროპის კონტინენტი, განსაკუთრებით კი, ყოფილი საბჭოთა კავშირის ან საბჭოთა ბლოკის ქვეყნები და მათ ტერიტორიებზე განლაგებული ორგანიზაციები და დაწესებულებები თუ მცხოვრები ფიზიკური პირები, რადგან ФСБ ამ გეოგრაფიულ

ზონებს მიიჩნევს რფ-ის ტერიტორიის გაგრძელებად, ე.წ. „ახლო საზღვარგარეთად“ (ближнее зарубежье; Near Abroad)[20] და მათზე ავრცელებს საკუთარ მანდატს. აღნიშნულს ისიც ადასტურებს, რომ ФСБ-ს რუსეთის მიერ ოკუპირებულ თუ ანექსირებულ ტერიტორიებზე, თითქოსდა საზღვრის დაცვის საბაბით, განლაგებული ჰყავს საკმაოდ მნიშვნელოვანი კონტინგენტი,[21] რაც მას, რფ-ის სხვა სპეცსამსახურებთან შედარებით, უპირატესობას ანიჭებს.

დასკვნა

კომპანია SolarWinds-ზე შეტევა წარმოადგენს აშშ-ის ისტორიაში ყველაზე დიდი მოცულობისა და ზიანის მომტან კიბერსადაზვერვო ოპერაციას, რომლის თაობაზეც დეტალური ინფორმაცია ფართო საზოგადოებისათვის ცნობილი გახდა. ოპერაცია რამდენიმე ფაზად ჩატარდა, რომელთაგანაც საკვანძო მნიშვნელობის მქონე იყო SolarWinds Orion-ის სერვისის განახლების პაკეტის გადაჭერა და მის საწყის კოდში მავნე ფუნქციური მოდულების ისე ჩაშენება, რომ იგი შეუმჩნეველი დარჩა როგორც თავად კომპანიის (SolarWinds) პროგრამისტებისა და ინფორმაციული უსაფრთხოების მენეჯერთათვის, ისე კომპანიის ბენეფიციართა კიბერუსაფრთხოების უზრუნველმყოფი პერსონალისთვის, რომელთაც ჩამოტვირთეს და საკუთარ სისტემაში გაუშვეს განახლების ინფიცირებული პაკეტი. ასეთ ორგანიზაციებს კი მიეკუთვნებოდნენ აშშ-ის ეროვნული უსაფრთხოების სამსახურები, მათ შორის ის სტრუქტურული დანაყოფებიც კი (მაგ., DHS CISA), რომელთა პასუხისმგებლობაა აშშ-ის კრიტიკული საინფორმაციო სისტემების დაცვა.

შესაბამისად, ნათელია, რომ SolarWinds-ზე შეტევის შედეგად მიღებულ ზიანს, უშუალოდ უსაფრთხოების განზომილებასთან ერთად, მნიშვნელოვანი რეპუტაციული დანაკარგებიც ახლავს. კერძოდ, რუსულმა მხარემ მოცემული შეტევით სცადა იმის დემონსტრირება, რომ კრემლის სპეცსამსახურებისგან დაცული არავინაა და შესაბამისად, რუსეთს შეუძლია ასიმეტრიულად, მათ შორის, კიბერსივრცეშიც, უპასუხოს სანქციებსა თუ სხვა ტიპის შემზღუდველ ღონისძიებებს.

ამ ყველაფერს აცნობიერებს ასევე აშშ-ის უმაღლესი პოლიტიკური ხელმძღვანელობა, რომელმაც მიმდინარე წლის 15 აპრილს რფ-ის საგარეო დაზვერვის სამსახურისთვის ხსენებული შეტევის ბრალად შერაცხვის პარალელურად, სანქციები დაუწესა იმ საჯარო თუ კერძო დაწესებულებებს, რომლებსაც კავშირი აქვთ CBP-სთან.

ამასთან, მოსალოდნელია, რომ ოფიციალური ვაშინგტონის პასუხი მარტოოდენ სანქციებით არ შემოიფარგლება, რადგან, როგორც ზემოთ უკვე აღინიშნა, 2016 წლის სანქციების შემთხვევა რუსეთის სამხედრო დაზვერვის წინააღმდეგ ადასტურებს, რომ კრემლისთვის მხოლოდ სანქციები არ არის ეფექტური მექანიზმი კიბერსივრცეში მავნე ქმედებებისგან თავის შესაკავებლად. საპასუხო „მტკივნეულ ღონისძიებებზე“ არაერთხელ პირდაპირ მიანიშნეს აშშ-ის უმაღლესი პოლიტიკური თანამდებობის პირებმა, რაც, ალბათ, არ უნდა გულისხმობდეს მარტოოდენ სანქციების პოლიტიკის გაგრძელებას. ამრიგად, მოსალოდნელია, რომ წინამდებარე დოკუმენტში განხილულ შეტევას უახლოეს მომავალში გაგრძელება ექნება, რომელიც შესაძლოა გახდეს დამატებითი დაძაბულობის წყარო აშშ-სა და რუსეთს შორის.

შენიშვნები

1. Forbes, DHS, DOJ And DOD Are All Customers Of SolarWinds Orion - The Source Of The Huge US Government Hack, ხელმისაწვდომია ბმულზე: https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=65540ef925e6, ბოლოს ნანახია: 13/06/2021

2. SolarWinds: We Make IT Look Easy, ხელმისაწვდომია ბმულზე: https://www.solarwinds.com/company/home ; ბოლოს ნანახია 13/06/2021

3. ტერმინი „ბრალად შერაცხვა“ გამოიყენება კიბერუსაფრთხების სფეროში ინგლისურ ენაში დამკვიდრებული ტერმინის „Attribution” ქართულ შესატყვისად. ეს უკანასკნელი ასევე წარმოადგენს საერთაშორისო სამართლებრივ ინსტიტუტს, რომლის ოფიციალური თარგმანიც ქართულ ენაში არის „ბრალად შერაცხვა“. იხ. მაგალითად, ადამიანის უფლებათა ევროპული სასამართლის გადაწყვეტილების ქართული ოფიციალური თარგმანი საქმეზე „ფონდი – სრებრენიცას დედები ნიდერლანდების წინააღმდეგ“, პარაგრაფი 5.12, ხელმისაწვდომია ბმულზე: http://catalog.supremecourt.ge/blog/index.php/2014-05-22-15-22-04/130-2014-06-24-10-10-34, ბოლოს ნანახია 13/06/2021

4. New York 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 14/06/2021

5. SolarWinds, SolarWinds Reseller Locator; ხელმისაწვდომია ბმულზე: https://partner.solarwinds.com/reseller/find/; ბოლოს ნანახია: 14/06/2021

6. Office of Director of National Intelligence, Joint State of US FBI, DHS CISA, DNI and NSA, ხელმისაწვდომია ბმულზე: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2021/item/2176-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-the-office-of-the-director-of-national-intelligence-odni-and-the-national-security-agency-nsa ; ბოლოს ნანახია 14/06/2021

7. Microsoft, Deep Dive into the Solorigate Second-stage Activation: From SUNBURST to TEARDROP and Raindrop, ხელმისაწვდომია ბმულზე: https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/ ; ბოლოს ნანახია: 15/06/2021

8. Endgadget, SolarWinds Hack May Have Been Much Wider than First Thought, ხელმისაწვდომია ბმულზე: https://www.engadget.com/russia-solarwinds-hack-broader-than-expected-211046098.html ; ბოლოს ნანახია: 15/06/2021

9. CNN, Former SolarWinds CEO Blames Intern for ‘solarwinds123’ Password Leak; ხელმისაწვდომია ბმულზე: https://edition.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html, ბოლოს ნანახია: 15/06/2021

10. FireEye Threat Research, Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor, ხელმისაწვდომია ბმულზე: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html; ბოლოს ნანახია 15/06/2021

11. იქვე.

12. CrowdStrike, SUNSPOT: An Implant in the Build Process; ხელმისაწვდომია ბმულზე: https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/ ; ბოლოს ნანახია: 15/06/2021

13. Cobalt Stike, Cobalt Strike Features; xelmisawvdomia bmulze: https://www.cobaltstrike.com/features ; ბოლოს ნანახია: 15/06/2021

14. ZEDNET, Microsoft: This is How the Sneaky SolarWinds Hackers Hid Their Onward Attacks for So Long, ხელმისაწვდომია ბმულზე: https://www.zdnet.com/article/microsoft-this-is-how-the-sneaky-solarwinds-hackers-hid-their-onward-attacks-for-so-long/ ; ბოლოს ნანახია: 15/06/2021

15. US 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:15/06/2021

16. US FBI, DHS and DHS CISA, Cybersecurity Advisory: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders; ხელმისაწვდომია ბმულზე: https://us-cert.cisa.gov/ncas/alerts/aa21-116a ; ბოლოს ნანახია 15/06/2021

17. UK NCSC, Advisory: Turla Group Exploits Iranian APT to Expand Coverage of Victims, ხელმისაწვდომია ბმულზე: https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims; ბოლოს ნანახია 15/06/2021

18. ხსენებული შემთხვევის ერთ-ერთი საუკეთესო ილუსტრირებაა აშშ-ის საპრეზიდენტო არჩევნების დროს ჰილარი კლინტონის დისკრედიტაციისათვის ელფოსტის ნაკრების გამოქვეყნება. იმის მიუხედავად, რომ რფ-ის სამხედრო სადაზვერვო სამმართველოს შეეძლო შეენარჩუნებინა და განევითარებინა ფარული წვდომა კომპრომეტირებულ ანგარიშებზე, აქტიური ღონისძიების ფარგლებში მოპოვებული მონაცემების გამოყენებით პრაქტიკულად თავად გაშიფრა სადაზვერვო ოპერაცია. იდენტური სიტუაცია იყო საფრანგეთის საპრეზიდენტო არჩევნების დროსაც, როდესაც რუსეთის სამხედრო დაზვერვა სხვადასხვა კონფიდენციალური მონაცემების გამოქვეყნებით ცდილობდა ულტრამემარჯვენე რადიკალი კანდიდატის – მარინ ლე პენის სასარგებლოდ (ზოგადი ფაქტობრივი ინფორმაცია ამ შეტევის თაობაზე ხელმისაწვდომია: https://www.reuters.com/article/us-france-election-macron-cyber-idUSKBN17Q200)

19. ესტონეთის საგარეო დაზვერვის სამსახური, 2018 წლის მოხსენება, გვ. 57-60 ხელმისაწვდომია ბმულზე: https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf ; bolos nanaxia 15/06/2021

20. Atlantic Council, Lubyanka Federation: How the FSB Determines the Politics and Economics of Russia, ხელმისაწვდომია ბმულზე: https://www.atlanticcouncil.org/in-depth-research-reports/report/lubyanka-federation/; ბოლოს ნანახია: 16/06/2021

21. EU Observer, 10 Years on: Russia's Occupation of Georgian Territory, ხელმისაწვდომია ბმულზე: https://euobserver.com/opinion/142547 ; bolos nanaxia: 16/06/2021; Nikolai Mitrokhin, Infiltration, Instruction, Invasion: Russia's War in the Donbass, gv 227-228, xelmisawvdomia bmulze: https://spps-jspps.autorenbetreuung.de/files/07-mitrokhin.pdf ; bolos nanaxia: 16/06/2021