WannaCry - ჭკვიანი ვირუსი უცნობი წარსულით

12 მაისს, მსოფლიოს მასშტაბით 150-ზე მეტ ქვეყანაში, 230,000 კომპიუტერზე აქამდე არსებულთა შორის ერთ-ერთი ყველაზე ჭკვიანი ვირუსი გავრცელდა. ვირუსს Ransomware ხასიათი ჰქონდა, რაც ნიშნავს, რომ ის ჯერ ბლოკავდა კომპიუტერის ფუნქციონირებისთვის ყველა აუცილებელ ფაილს და შემდეგ ითხოვდა გამოსასყიდს 300 ან 600 დოლარის ექვივალენტი ბიტკოინების (ელექტრონული ვალუტა) სახით, რათა მომხმარებელს კომპიუტერზე კონტროლი აღედგინა. ვირუსი მხოლოდ Windows-ის საოპერაციო სისტემებზე გავრცელდა. არსებული ინფორმაციით, ვირუსმა გამოიწვია ინგლისში რამდენიმე სამედიცინო დაწესებულების ფუნქციონირების შეწყვეტა, პორტუგალიაში მან შეაფერხა სატელეფონო პროვაიდერის მუშაობა, რუსეთში კი ისეთი სახელმწიფო დაწესებულებების საქმიანობა იყო პარალიზებული, როგორიცაა შსს, საგზაო უსაფრთხოების ინსპექცია (ГИБДД), სბერბანკი, რკინიგზის კომპანია და სხვ.[1]

რუსეთის პრეზიდენტმა, ვლადიმირ პუტინმა, 2017 წლის 15 მაისს გამართულ პრეს-კონფერენციაზე განაცხადა, რომ 12 მაისს გავრცელებული ინტერნეტ-ვირუსის, WannaCrypt (ასევე: WannaCry/WannaCrypt0r 2.0/Wanna Decriptor)-ის პირველწყარო აშშ-ის სპეცსამსახურები იყო, რაზეც კომპანია Microsoft-ის ოფიციალური განცხადება დაიმოწმა.

Microsoft-მა თავის ოფიციალურ ბლოგზე მართლაც განაცხადა პუტინის პრეს-კონფერენციამდე ერთი დღით ადრე, რომ გლობალური ჰაკერული თავდასხმის დროს გამოყენებული ე.წ. „ექსპლოიტი“[2] ემთხვეოდა 2017 წლის დასაწყისში აშშ-ის უშიშროების ეროვნული სააგენტოდან (NSA) მოპარული ექსპლოიტებიდან ერთ-ერთს. მოპარული ექსპლოიტებისგან მომდინარე შესაძლო საფრთხის თავიდან ასარიდებლად, Microsoft-მა 14

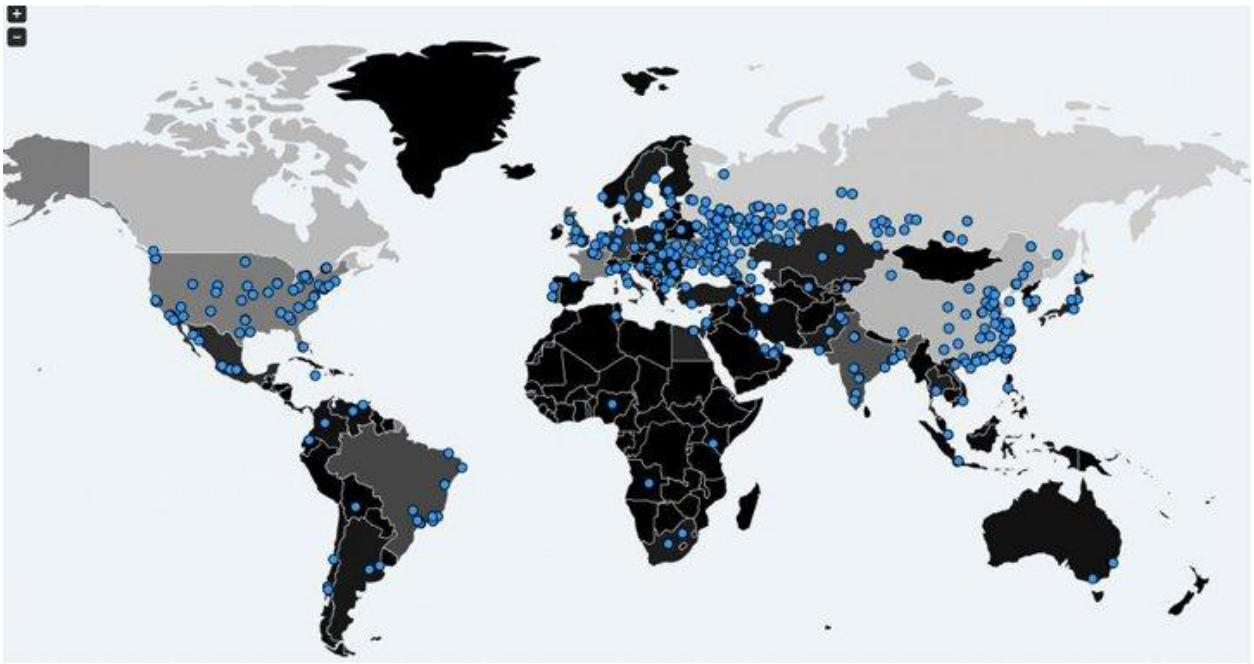
[1] http://www.bbc.com/russian/features-39928406

[2] ინგლ. ექსპლოატაცია/გამოყენება. კომპიუტერული პროგრამა, პროგრამული კოდის ფრაგმენტი ან ბრძანებების მიმდევრობა, რომელიც იყენებს პროგრამულ უზრუნველყოფაში არსებულ სისუსტეებს გამომთვლელ სისტემაზე თავდასხმისთვის. შეტევის მიზანი შეიძლება იყოს როგორც სისტემაზე კონტროლის დამყარება (რაც სწორედ WannaCrypt-მა მოახდინა), ასევე მისი ფუნქციონირების დარღვევა. ასევე გამოიყენება სახელმწიფო უშიშროების სამსახურების მიერ კომპიუტერულ სისტემებზე საიდუმლოდ კონტროლის დასამყარებლად.

მარტს გამოუშვა პატჩი[3], რომლის დაყენების შემთხვევაშიც, Windows-ის მომხმარებლები დაცულნი იქნებოდნენ შესაძლო კიბერ-შეტევებისგან. მოპარული ექსპლოიტები (სულ 12 ცალი, მათ შორის ETERNALBLUE, 12 მაისის კიბერ-შეტევის მთავარი იარაღი) კიბერ-კრიმინალურმა ჰაკერულმა ჯგუფმა Shadow Brokers მალევე გაასაჯაროვა, რამაც მთელი მსოფლიოს მასშტაბით ყველა ის კომპიუტერი, რომელზეც Microsoft-ის მიერ გამოშვებული პატჩი არ იყო დაყენებული, მოწყვლადი გახადა კიბერ-შეტევისადმი. ჯერჯერობით უცნობია, თუ ვინ გამოიყენა გასაჯაროებული ექსპლოიტები გლობალური კიბერ-შეტევისთვის, თუმცა არაა გამორიცხული, შეტევის ავტორი თავად Shadow Brokers იყოს. აღსანიშნავია, რომ გლობალური ჰაკერული შეტევის შედეგების ზუსტად პროგნოზირება შეუძლებელია, რამდენადაც ის დამოკიდებულია კომპიუტერის მომხმარებლების დაცულობის დონეზე, მომხმარებლის ქცევაზე (გადავა თუ არა ამა თუ იმ მავნე ბმულზე) და ჰაკერული პროგრამის შეჩერების მექანიზმის აღმოჩენის სისწრაფეზე. მისი პროგნოზირება შეუძლებელია - კიბერ-შეტევა შესაძლოა არც შედგეს, თუკი ჰაკერების მიერ გაშვებული ვირუსი საწყისშივე აღკვეთა რომელიმე სხვა ჰაკერმა თუ კიბერ-უსაფრთხოების სპეციალისტმა. ამდენად, ის ფაქტი, რომ შეტევის შედეგად ყველაზე მეტად რუსული კომპიუტერები დაზარალდა, არ უნდა იქნას ინტერპრეტირებული, ისე, თითქოს ეს შეტევა რუსეთზე ყოფილიყო გამიზნული.

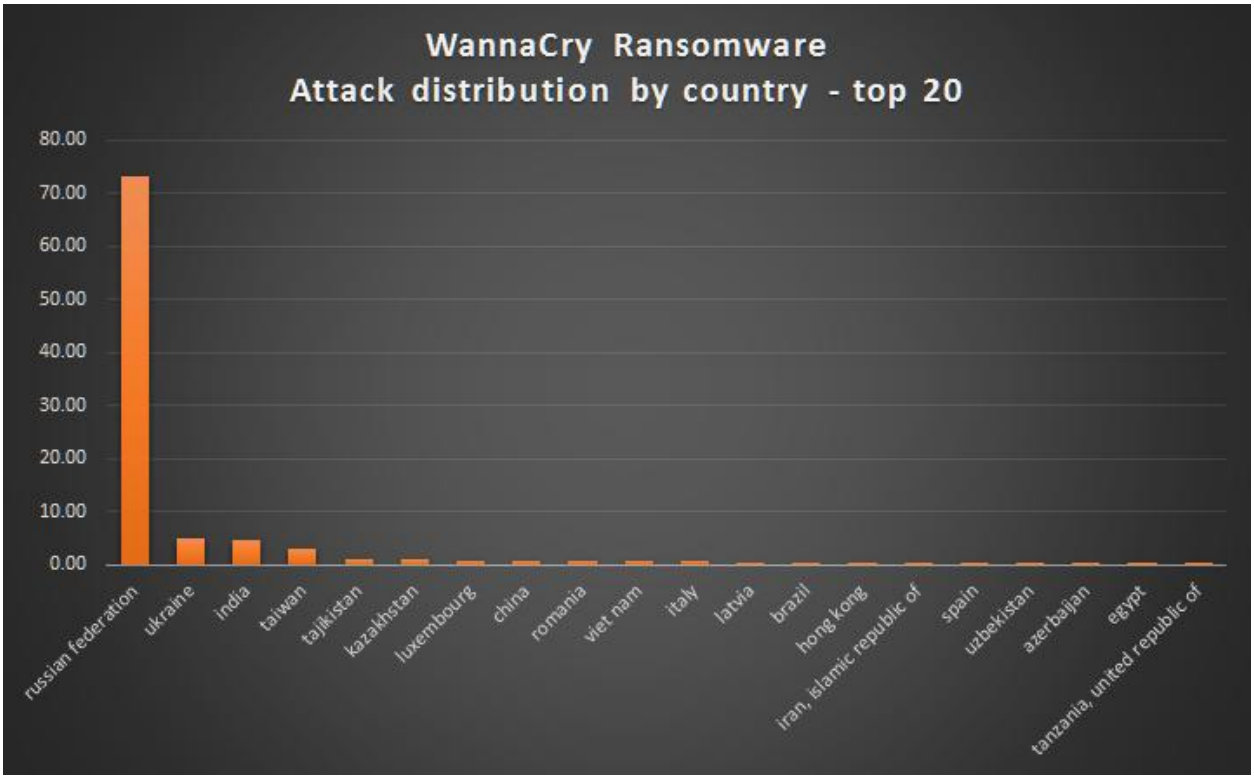
გრაფიკი 1. კიბერ-შეტევით დაზარალებული ობიექტები მსოფლიოს მასშტაბით.

[3] ინგლ. ნაკერი. პროგრამული უზრუნველყოფა (software), განკუთვნილი კომპიუტერული პროგრამის ან მისი მხარდამჭერი მონაცემების გასაახლებლად, შესაკეთებლად ან გასაუმჯობესებლად.



წყარო: *https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html*

გრაფიკი 2. კიბერ-შეტევით ყველაზე მეტად დაზარალებული ქვეყნები (პროცენტული გადანაწილება).



წყარო: *https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/*

როგორც გრაფიკი 1 და 2-დან ჩანს, შეტევით უმეტესწილად რუსეთში მდებარე კომპიუტერები დაზარალდა, რომელსაც მოსდევს უკრაინა, ინდოეთი, ტაივანი და სხვ. გრაფიკებიდან შეგვიძლია ვივარაუდოთ, რომ რუსეთის განსაკუთრებული ზარალი მოცემულ ჰაკერულ თავდასხმაში განპირობებულია ზოგადად, ჰაკერული თავდასხმის უკონტროლობით და რუსეთში კომპიუტერული სისტემების დაუცველობით, რაც, თავის მხრივ, აიხსნება პირატული Windows-ის ფართო გამოყენებით. პირატული Windows-ის არსებობის შემთხვევაში, მომხმარებელთა უმრავლესობა არ აყენებს ე.წ. უსაფრთხოების განახლებებს, რათა არ მოხდეს მისი პირატული ვერსიის იდენტიფიცირება Microsoft-ის მიერ, ამან კი ისინი მოწყვლადი გახადა მოცემული კიბერ-შეტევისადმი, რადგანაც მისგან სრულად დაცულნი მხოლოდ 14 მარტს გამოშვებული განახლების დაყენების შემთხვევაში იქნებოდნენ. იმან, რომ Windows-ის რუსი მომხმარებლების დიდ ნაწილს არალიცენზირებული ვერსია აქვს

დაყენებული, გაზარდა მათი ინფიცირების რისკი ჰაკერული შეტევის დროს, რამაც, სავარაუდოდ, გამოიწვია მათი ინფიცირების მაღალი მაჩვენებელი.

რას წარმოადგენს Shadow Brokers?

Shadow Brokers, რომელიც პირველად 2016 წლის ზაფხულში გამოჩნდა, რეგულარულად აქვეყნებს აშშ-ის უშიშროების სამსახურებიდან მოპარულ საიდუმლო ექსპლოიტებს. დღეის მდგომარეობით, ჯგუფმა უკვე ხუთჯერ გამოაქვეყნა NSA-ს ექსპლოიტები. პირველ და მეორე გამოქვეყნებას ონლაინ-აუქციონის სახე ჰქონდა, რომელზეც შესაძლებელი იყო მოცემული მასალების შეძენა ბიტკოინებით. მესამე გამოქვეყნებისას, თანდართულ შეტყობინებაში, ჯგუფი იუწყებოდა, რომ უკმაყოფილოა ხალხის დაბალი აქტიურობით აუქციონში და გადადის პირისპირ ვაჭრობის სტრატეგიაზე. 2017 წლის 8 აპრილს გასაყიდად გამოტანილი NSA-დან მოპარული ექსპლოიტები წარმოადგენდა ჯგუფის მეოთხე გამოჩენას. 8 აპრილს გამოქვეყნებულ მასალებს თან ერთვოდა მათი ოფიციალური საჯარო წერილი დონალდ ტრამპის მისამართით, სათაურით „არ დაგავიწყდეთ თქვენი დასაყრდენი“, რომელიც იწყება შემდეგი სიტყვებით: „ღრმად პატივცემულო ძვირფასო პრეზიდენტო ტრამპ, რა ჯანდაბას სჩადიხართ?“. წერილიდან ჩანს, რომ ჯგუფს აქვს მკვეთრი ანტი-გლობალისტური, შეიძლება ითქვას, ფაშისტური მსოფლმხედველობა, რუსეთი კი მათ ბუნებრივ მოკავშირედაა მოხსენიებული გლობალიზმის წინააღმდეგ ბრძოლაში. წერილში ტრამპი გაკრიტიკებულია მისი არჩევნებამდელი პოზიციების შეცვლისთვის, მათ შორის ხაზგასმულია უკმაყოფილება სირიის კონფლიქტში ჩარევის გამო. ასევე, ნათქვამია, რომ ჯგუფი მხარს უჭერს ტრამპის ადმინისტრაციის მთავარი სტრატეგისტის, სტივ ბენონის იდეოლოგიას და პოლიტიკას და გმობს ტრამპს უშიშროების ეროვნული საბჭოდან (NSC) მისი გათავისუფლების გამო. ბენონი 2016 წლის საპრეზიდენტო არჩევნებამდე ულტრამემარჯვენე ვებსაიტის, „ბრაიტბარტის“ აღმასრულებელი დირექტორი იყო, რომელიც ცნობილია თავისი რასისტული, ქსენოფობიური, მიზოგინიური და ანტისემიტური პლატფორმით.

ჯგუფის აქტიურობის მეხუთე ტალღა 14 აპრილზე მოდის. სწორედ მეხუთე ტალღამ გახადა შესაძლებელი მომხმარებლების მიერ ETERNALBLUE-ზე წვდომის მიღება, რამაც 12 მაისის გლობალური ჰაკერული შეტევა გამოიწვია.

ცენტრალური სადაზვერვო სააგენტოს (CIA) ყოფილი თანამშრომლის, ედუარდ სნოუდენის თანახმად, Shadow Brokers, სავარაუდოდ, დაკავშირებულია რუსეთთან. ედუარდ სნოუდენმა ასევე დააკავშირა ეს კიბერ-შეტევა დემოკრატების ეროვნული კონვენციის (DNC) სისტემაზე ჰაკერულ შეტევასთან, რომელსაც აშშ-ში წინასაარჩევნო პერიოდში ჰქონდა ადგილი და რომელმაც მნიშვნელოვნად გაზარდა დონალდ ტრამპის გაპრეზიდენტების შანსები. აღსანიშნავია, რომ თავად სნოუდენი აშშ-ის ცენტრალური სადაზვერვო კომიტეტის (CIA) ყოფილი თანამშრომელია. მან 2013 წელს გაასაჯაროვა აშშ-ის საიდუმლო სამსახურების სადაზვერვო ინფორმაცია, რის შემდეგაც ქვეყანა დატოვა და გაემგზავრა რუსეთში, სადაც მიიღო თავშესაფარი 2020 წლამდე.

დასკვნა

ჯერჯერობით უცნობია, ვინ შეიძინა/გამოიყენა Shadow Brokers-ის მიერ გამოქვეყნებული ექსპლოიტები. ის ფაქტი, რომ მოცემული ჯგუფი სიმპათიას გამოხატავს ვლადიმირ პუტინისადმი, რომ მან მოახდინა დემოკრატიული პარტიის სისტემაზე ჰაკერული თავდასხმა (რამაც აშშ-ის საპრეზიდენტო არჩევნების შედეგებზე მოახდინა გავლენა) და რომ მის მიერ გამოქვეყნებული მასალებისადმი ინტერესს გამოხატავდნენ რუსი კიბერ-დამნაშავეები ფორუმზე, მიუთითებს შესაძლო რუსულ კვალზე. თუმცა, წინასწარი დასკვნები შესაძლოა არაზუსტი აღმოჩნდეს. ფაქტია, რომ ზარალის გარეშე ამ თავდასხმიდან ვერც ერთი წამყვანი სახელმწიფო ვერ გამოვიდა. შესაძლოა საქმე სახელმწიფო აქტორთან საერთოდ არ გვქონდეს და 12 მაისის გლობალური ჰაკერული შეტევა უბრალოდ რომელიმე იდეოლოგიზირებული ან, უბრალოდ, მერკანტილური მიზნების მქონე ჯგუფის ორგანიზებული იყოს. არაა გამორიცხული, რომ თავდასხმა თავად Shadow Brokers-მა ჩაიდინა. ნიშანდობლივია, რომ ჯგუფის მიერ საიდუმლო მასალების გამოქვეყნება ემთხვევა მათი იდეოლოგიური „მამის“, სტივ ბენონის ეროვნული უშიშროების კომიტეტიდან გათავისუფლებას. არ უნდა დაგვავიწყდეს, რომ ჯგუფი უპირველესად ფინანსურ ინტერესებზეა დამყარებული და საიდუმლო მასალებს მხოლოდ ბიტკოინებზე ცვლის, 12 მაისის შეტევის მსხვერპლებს კი ჰაკერული პროგრამა სწორედ ბიტკოინების სანაცვლოდ სთავაზობდა კომპიუტერზე კონტროლის აღდგენას, რაც მოცემული ჯგუფის ხელწერაზე მიუთითებს. ასევე საინტერესოა,

რომ ჯგუფის განცხადებებში, რომლებიც ინგლისურ ენაზე ქვეყნდება, ყოველთვის მრავალი გრამატიკული შეცდომაა.

ამის ფონზე, ვლადიმირ პუტინის მიერ იმის მტკიცება, რომ რუსეთი არაფერ შუაშია და ვირუსის პირველწყარო აშშ იყო, არის მსმენელის შეცდომაში შეყვანის მცდელობა. ჰაკერულ ჯგუფებს შეუძლიათ ექსპლოიტების და სხვა სისუსტეების მოპარვა ნებისმიერი ქვეყნის უშიშროების სამსახურიდან, მაგრამ ეს არ ნიშნავს, რომ ჰაკერულ შეტევას დაზარალებული ქვეყანა უდგას სათავეში. სრულიად შესაძლებელია, რომ აშშ-დან მოპარული ჰაკერული საშუალებებით რუსულმა კიბერ-ტერორისტებმა ისარგებლეს, რომელთაც შესაძლოა მთავრობასთან არც ჰქონდეთ კავშირი. ასევე შესძლებელია, რომ რომელიმე ჰაკერულმა ჯგუფმა ასევე მოიპაროს რუსული უშიშროების სამსახურის (ФСБ) კიბერ-შეტევების დეპარტამენტის ექსპლოიტები და ამის საშუალებით მოაწყოს გლობალური შეტევა, თუმცა, ეს არ ნიშნავს, რომ შეტევის პირველადი წყარო რუსეთი იქნება.

შოთა გელოვანი

წყაროები

- Arstechnica. co.uk. *NHS hit by massive ransomware attack, many hospitals and clinics offline*. https://goo.gl/OxHNTy (ბოლო წვდომა: 19.05.17)
- Arstechnika.com. *An NSA-derived ransomware worm is shutting down computers worldwide*. https://goo.gl/4HQmNE (ბოლო წვდომა: 19.05.17)
- Eweek.com. *Shadow Brokers Allegedly Hack NSA's Equation Group*. https://goo.gl/lrrtn9 (ბოლო წვდომა: 19.05.17)
- Forbes.com. *An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak*. https://goo.gl/JsgE3Y (ბოლო წვდომა: 19.05.17)
- Forbes.com. *Russian Cybercriminals Are Loving Those Leaked NSA Windows Weapons.* https://goo.gl/U7vKzB (ბოლო წვდომა: 19.05.17)
- Medium.com. *Don't Forget Your Base*. https://goo.gl/gz5BoZ (ბოლო წვდომა: 19.05.17)
- Ria.ru. *Путин о мировой кибератаке: Россия тут ни при чем.* https://goo.gl/vq2PEs (ბოლო წვდომა: 19.05.17)