Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 71 - 74 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

“DARKCOMET”-ის როლი სირიის კონფლიქტში“
„THE ROLE OF “DARKCOMET” IN THE SYRIAN CONFLICT“

ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili_ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
მარიამ კიკლიაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Mariam Kikliashvili- Ivane Javakhishvili Tbilisi State University, Sociology_Junior;

ანოტაცია: XXI საუკუნეში, სწრაფი ტექნოლოგიური პროგრესის პარალელურად, გამოუვლენელი და გაუხსნელი დანაშაულების ყველაზე მზარდი ტენდენცია კიბერდანაშაულის კუთხით აღინიშნება, რომელსაც ხშირად „მომავლის დანაშაულსაც“ უწოდებენ. მავნე პროგრამები, რომლებიც კიბერდანაშაულის ერთ-ერთი მთავარი მექანიზმია, თითოეულ ჩვენგანს მათ მსხვერპლად ადვილად გვაქცევს. იმ შემთხვევაში კი როცა საქმე ეხება მასობრივ კონფლიქტებს, იგი უფრო მეტ მნიშვნელობას იძენს. სწორედ ამის ერთ-ერთი მაგალითია სირიის მთავრობის მიერ „DarkComet”-ის გამოყენებით სრული კონტროლის მოპოვება მის ოპონენტებზე და სასურველი ინფორმაციის მიღება მათსავე სამოქმედო გეგმებზე.

ANNOTATION: In the 21st century, in parallel with rapid technological progress, the increasing trend of unsolved and inexcusable crimes is marked by cybercrime, often referred to as "the crime of the future." Malicious software, one of the key mechanisms of cybercrime, makes it easy for us to be victims of it. And when it comes to mass conflicts, it becomes even more important. One example of this is the Syrian government's use of „DarkComet“, to gain full control over its opponents and obtain desired information on their action plans.

საკვანძო სიტყვები: კიბერდანაშაული, კიბერშეტევა, დისტანციური მართვის მექნიზმი(RAT), „ტროიანი“, „ DarkComet”, „სირიის კონფლიქტი.

ტექნოლოგიურმა პროგრესმა უამრავი სიახლე შემატა საზოგადოებრივ ცხოვრებას, რასაც ბევრ დადებითთან ერთად უარყოფითი ასპექტებიც ახლავს თან. ინტერნეტის მეშვეობით ინფორმაციისა და მომსახურების მიღება-გავრცელების ხელმისაწვდომობამ ერთი მხრივ ცხოვრება გაგვიმარტივა, თუმცა მეორე მხრივ კიბერდამნაშავეთა რეალურ სამიზნე ობიექტებად გვაქცია. კიბერდამნაშავეთაგან წამოსული საფრთხეები შეგვიძლია 2 ნაწილად დავყოთ: პროგრამული საფრთხეები და ინტერნეტ-თაღლითობა.

პროგრამული საფრთხეები ძირითადად მავნე პროგრამებთან, უსადენო ინტერნეტ-კავშირთან(Wi-Fi), კიბერშეტევებთან, მზა ჩანაწერებთან(Cookies) და ვირტუალური ფულის გამომუშავებასთან არის დაკავშირებული. მავნე პროგრამა გულისხმობს კომპიუტერული კოდს ან აპლიკაციას, რომელსაც თქვენი მოწყობილობისთვის, იქნება ეს კომპიუტერი, მობილური ტელეფონი თუ ტაბლეტი, დიდი ზიანის მიყენება შეუძლია და ამავდროულად თქვენი პირადი ინფორმაციის მოპარვაც.

სწორედ ერთ-ერთ ასეთ მავნე პროგრამას წარმოადგენს ეგრეთწოდებული „ტროიანი“ იგივე „ტროას ცხენი“. მისი სახელწოდება მოდის ქალაქ ტროასთან დაკავშირებული ბერძნული ლეგენდიდან, რომლის თანახმადაც, ბერძნებმა ტროას ასაღებად ააგეს უზარმაზარი ხის ცხენი, შიგნით ჩასვეს ბერძენი ჯარისკაცები, ცხენი ტროას კარიბჭესთან დატოვეს, თვითონ კი ჯარი უკან გააბრუნეს, თითქოს დაზავებას აპირებდნენ. ტროელებმა ცხენი ღმერთების საჩუქრად მიიჩნიეს და ქალაქში შეაგორეს; ღამით, როდესაც ყველას ეძინა, მეომრები გადმოვიდნენ ცხენიდან, ბერძენ ჯარისკაცებს გაუხსნეს ქალაქის კარიბჭე და ტროა მიწასთან გაასწორეს. დღეს ტროას ცხენს გადატანითი მნიშვნელობით იყენებენ, როგორც მტრისგან მიძღვნილ „საჩუქარს“, რითაც იგი ცდილობს მოწინააღმდეგისთვის მახის დაგებას.

„ტროიანი“ მიეკუთვნება ისეთ მავნე კომპიუტერულ პროგრამას, რომელიც ერთი შეხედვით უვნებლად გამოიყურება, ან თავს ინიღბავს ყველასთვის კარგად ცნობილ პროგრამად, რადგან მომხმარებლები მათ ინსტალირებას არ ერიდებიან და საფრთხეს ნაკლებად ხედავენ, მაგალითად „Facebook“, რომელიც არაერთხელ გამხდარა ჰაკერების იარაღი. მსგავსი ხრიკებით რიგითი კომპიუტერის მომხმარებელები ადვილად ტყუვდებიან და საკუთარი ნებით საშუალებას აძლევენ „ტროას ცხენს“ შევიდეს მათ კომპიუტერულ სისტემაში. მის მიზანს არ წარმოადგენს საკუთარი თავის რეპლიკაცია. ჰაკერები მას კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმად(RAT -Remote Administration Tool) იყენებენ .

ერთ-ერთი ყველაზე ცნობილი „ტროას ცხენი“ არის “DarkComet”. ის დისტანციური წვდომის ინსტრუმენტია, რომელიც შეიმუშავა ფრანგმა პროგრამისტმა ჟან-პიერ ლესუურმა, რითიც ცდილობდა პროგრამირებაში საკუთარი შესაძლებლობების წარმოჩენას და არანაირი სხვა მიზანი მას არ ამოძრავებდა. “DarkComet” საშუალებას აძლევს მომხმარებელს გააკონტროლოს სისტემა გრაფიკული ინტერფეისით(GUI – Graphical User Interface). მისი საშუალებით შესაძლებელია ფოტოების გადაღება ვებკამერიდან, საუბრის მოსმენა კომპიუტერთან მიერთებული მიკროფონიდან; მას

შეუძლია მოახდინოს დაინფიცირებული აპარატის სრული კონტროლიზება, როგორც ნებისმიერი ფაილის გადატანა დაინფიცირებულ აპარატზე, ისე ნებისმიერი დოკუმენტის მოპარვა. როგორც ბლოგი “Malwarebytes” გვეუბნება, პროგრამა “DarkComet”-ის შეძენა ჰაკერების ფორუმზე 2012 წელს შესაძლებელი იყო 25 ევროდ, რაც მის ფინანურ ხელმისაწვდომობაზე მიუთითებს. “DarkComet”-ის ფართო გავრცელება სწორედ 2012 წლიდან დაიწყო და ასოცირდება ისეთ ფართომასშტაბიან მოვლენასთან, როგორიცაა სირიის კონფლიქტი.

The Syrian Malware Team(SMT) წარმოადგენს სირიის მავნე პროგრამების სამთავრობო ჰაკერების ჯგუფს, რომელიც იყენებდა დისტანციური მართვის მექანიზმს(RAT). კიბერუსაფრთხოების ფირმის “FireEyes”-ის ცნობით ეს ჯგუფი პირველად გამოჩნდა 2011 წელს და აქტიური იყო 2014 წლის ივლისამდე. როგორც „ESG“(Environmental, Social, and Governance)-ის უსაფრთხოების მკვლევრებმა დაადგინეს „DarkComet“-ს მჭიდრო კავშირი ჰქონდა სირიის მთავრობასა და პოლიტიკურ დისიდენტებთან.

სირიის მთავრობა იყენებდა „DarkComet“-ის პროგრამას, რათა წვდომა ჰქონოდა ოპონენტების კომპიუტერულ სისტემაზე. მთავრობამ ის გამოიყენა, როგორც ჯაშუში. „არაბული გაზაფხულის“ მოძრაობისთვის კი ერთ-ერთი ყველაზე დამახასიათებელი ნიშანია ის, რომ ისინი იყენებენ ონლაინ სოციალურ ქსელებს და ძლიერ ეყრდნობიან ისეთ პროგრამას კომუნიკაციისთვის, როგორიცაა „Skype“. სიირის მთვარობამ „DarkComet“, სწორედ „Skype”-ის მეშვეობით გაავრცელა და შეძლო, რომ ერთი აქტივისტის დაკავებითა და მის პირად მონაცემებში შეღწევით, წვდომა ჰქონოდა მასთან კავშირში მყოფ აქტივისტებთან. ასევე სამთავრობო ჯგუფის წევრები, როგორც ქალი ანტისამთავრობო აქტივისტები უკავშირდებოდნენ მსხვერპლებს „Skype”-ით ან „Facebook”-ით, უგზავნიდნენ ქალის ფოტოს, რომელიც შეიცავდა მავნე პროგრამას. როდესაც ამ სურათს ხსნიდნენ, “DarkComet” აქტიურდებოდა მათ კომპიუტერზე და ფარულად აკავშირებდა სამთავრობო სისტემასთან. მთავრობის მიზანსაც სწორედ ეს წარმოადგენდა, მათ შეძლეს ანტისამთავრობო ჯგუფების სამოქმედო გეგმების გაშიფვრა, რის შემდეგაც დაიწყო მასობრივი დაკავებები.

მას მერე, რაც „DarkComet“ დაუკავშირდა სირიის რეჟიმს, ჟან-პიერ ლესუურმა შეწყვიტა ინსტრუმენტის შემუშავება და განაცხადა: ”- მე არასოდეს წარმომედგინა, რომ მთავრობა მას ჯაშუშობაში გამოიყენებდა, ეს რომ მცოდნოდა, არასოდეს შევქმნიდი ასეთ ხელსაწყოს.”

დღევანდელი მონაცემებით “DarkComet”-ის პროგრამაზე მუშაობა შეწყვეტილია, ხოლო მისი გადმოტვირთვა ოფიციალური ვებ-გვერდიდან აღარაა შესაძლებელი.

ამ შემთხვევამ ნათლად დაგვანახა, რომ სწრაფი ტექნოლოგიური პროგრესის საუკუნე, არის დრო, როცა ჩვენი ყოველდღიური ცხოვრება უშუალოდაა დაკავშირებული ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან, რაც მნიშვნელოვნად ზრდის კიბერდანაშაულის რისკებს. განვიხილეთ ერთ-ერთი ყველაზე ცნობილი „ტროიანი“ - Dark Comet”, რომლის შემქმნელს ისევე ვერ წარმოედგინა ამ ხელსაწყოს ბოროტად გამოყენება, როგორც აინშტაინს, ის, რომ მისი ფორმულა საფუძველი გახდებოდა ბირთვული იარაღის შექმნისა, რომლის ბოროტი მიზნებით გამოყენებამაც XX საუკუნეში უდიდესი ტრაგედიები გამოიწვია.

ბიბლიოგრაფია

1. McMillan, Robert. “How The Boy Next Door Accidentally Built a Syrian Spy Tool”(07/11/2012) https://www.wired.com/2012/07/dark-comet-syrian-spy-tool/?fbclid=IwAR1_9WwMBqk2iTsGLwXfmCn03Gt-1b0BK3MmERTEZOL2iAL2Ve69gfV_qHU
2. “DarkComet”(2012) https://www.enigmasoftware.com/darkcomet-removal/?fbclid=IwAR1iDHGo3W5J3PCL2sxpP5cyEmGWBzdJzzN1XI1jCuQvel5v1dowPc8006Q
3. “DarkComet Surfaced in The Targeted Attacks in Syrian Conflict”(23/02/2012) https://blog.trendmicro.com/trendlabs-security-intelligence/darkcomet-surfaced-in-the-targeted-attacks-in-syrian-conflict/?fbclid=IwAR0rc-2t2SlPbV-63JKASqZ6aX7fI5NJgQ29qVf6xXZGU8XXFCr1gJbT8AI
4. “DarkComet Analysis – Understanding the Trojan used in Syrian Uprising”(16/03/2012) https://resources.infosecinstitute.com/darkcomet-analysis-syria/?fbclid=IwAR39kzxgBnRkuD2X0F37f8F9XtNXyLvMOoFPT6dwO0eQiLP3tXQogmRHqCI#gref
5. "Spy code creator kills project after Syrian abuse". BBC. 10 July 2012. https://www.bbc.com/news/technology-18783064?fbclid=IwAR0DG-AyU1c3KDSDqqKoC9qyTuOkEQqYq6p7oXL5OgDrUFKVYMn4JIa5Yi8
6. “The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict”. Zürich, October 2017. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf?fbclid=IwAR1vUGDqF2xq-SyHH4MoECftOB-CIBMtGX_3ZWX4eDN5pyxk1Zks_Aq6QIo