Scientific and Practical Cyber Security Journal (SPCSJ) 4(2): 92-95 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

„რუტკიტი“, როგორც კიბერდანაშაულის იარაღი“
"Rootkit" as a weapon of cybercrime "

1. ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, III კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili_ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
2. 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. სწორედ, ერთ-ერთ ასეთ მავნე პროგრამას წარმოადგენს „რუტკიტი“, რომლის საშუალებითაც მსოფლიოში 60 000-მდე ადამიანი დაზარალდა.

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. One of these Malware programs is “Rootkit”, about 60,000 people around the world have been affected by this.

საკვანძო სიტყვები: *კიბერსივრცე, კიბერდანაშაული, დისტანციური მართვის მექნიზმი(RAT), მალვეარი(Malware), “რუტკიტი“;*

„რუტკიტი“, როგორც კიბერდანაშაულის იარაღი“

კიბერსივრცე ეს არის ინფორმაციულ - ტექნოლოგიური ინფრასტრუქტურის ურთიერთდაკავშირებული კომპლექსი, რომელიც თავის თავში აერთიანებს კომპიუტერულ სისტემებს, ინტერნეტის გლობალურ და ტელესაკომუნიკაციო ქსელებს. კიბერსივრცეში არსებული მდგომარეობა დღითიდღე უფრო შემაშფოთებელი ხდება. კარგად შესრულებულ კიბერშეტევას შეუძლია, როგორც გავლენის მოხდენა, ასევე ზიანის მიყენება ნებისმიერ სექტორზე. მისი საშუალებით შესაძლებელია ყველა დონეზე სახელმწიფო სტრუქტურების

პარალიზება. კიბერსივრცეში უსაფრთხოების უზრუნველყოფა მთელ რიგ სირთულეებთან არის დაკავშირებული.

ისეთი პროგრამები, როგორებიცაა „Malware“, „Riskware“ და „Spyware“ ქსელურ სისტემაში მიიჩნევიან განსაკუთრებით დიდი საფრთხის გამომწვევად. ამ საზიანო პროგრამების ეფექტი მოიცავს: კომპიუტერული სისტემის მწყობრიდან გამოყვანას, მომხმარებელთა კონფიდენციალური ინფორმაციის მიღებასა და მათ გამოყენებას უკანონო მიზნებისათვის.

მალვეარი („Malware”) წარმოადგენს ინტრავირუსულ პროგრამას. იგი მოიცავს კომპიუტერულ ვირუსებს, “ტროიანებს” (“ტროას ცხენი”), “რუტკიტებს”, “კილოგერებს”, “ედვეარს”, “რენსომვეარს”, “ვორმებს”, “სპაივეარს”, საზიანო “BHO”-სა და სხვა საზიანო პროგრამებს. მათმა არსებობამ საჭირო გახადა ისეთ დამცავ პროგრამათა შექმნა, როგორიც არის ანტიმალვეარები და ანტივირუსები. აღნიშნული პროგრამები აქტიურად გამოიყენება კერძო მომხმარებელთა მიერ, კომპიუტერების, პირადი ინფორმაციისა და მათზე უნებართვო წვდომისაგან თავის დასაცავად.

„რუტკიტი“ არის პროგრამა, რომელიც ცდილობს თავის არსებობას მალავს უსაფრთხოების პროგრამებისგან თავის აცილების გზით. კომპიუტერში შეღწევის შემდეგ, იგი საიდუმლო კონტროლის საშუალებას აძლევს დისტანციურ მომხმარებელს კომპიუტერის ოპერაციული სიტემაზე. მისი მიზანი არაა საკუთარი თავის რეპლიკაცია. ჰაკერები მას იყენებენ კომპიუტერული სისტემის დისტანციურ მართვის მექანიზმად(RAT –Remote Administration Tool). პროგრამა შეიძლება კომპიუტერზე იყოს, თუმცა ჩვენ ამის შესახებ არაფერი ვიცოდეთ. მიზანი მარტივია, კომპიუტერული მოწყობილობათა გამოყენება, როგორც ფინანსური, ასევე სხვა ტიპის მოგების მისაღებად.

ტერმინი „rootkit“ არის "root" („Unix“ - ის მსგავსი ოპერაციული სისტემების პრივილეგირებული ანგარიშის ტრადიციული სახელი) და სიტყვა "kit"-ის (პროგრამული კომპონენტები, რომლებიც ახორციელებენ ამ ხელსაწყოს) ნაერთი.

„რუტკიტი“ შესაძლოა სპამების სახითაც იყოს წარმოდგენილი და დამალული იყოს ნებისმიერ ფაილში, განსაკუთრებით კი არალიცენზირებულ პროგრამებში. „რუტკიტის“ ამოცნობა ანტივირუსისთვის ფაქტობრივად შეუძლებელია. ის ანტივირუსს მარტივად უვლის გვერდს და ოპერაციულ სისტემაში ფარულად იდებს ბინას, საიდანაც ჰაკერს მისთვის სასურველ ინფორმაციას აწვდის.

ყოველწლიურად, 60,000-მდე ადამიანი ხდება „რუტკიტის“ მსხვერპლი. სპამებით შემოტევის ყველაზე დიდი მაჩვენებელი კორპორაციებში, გასულ წლებში ფიქსირდებოდა ევროპისა და ამერიკის რეგიონში, თუმცა ბოლო პერიოდში აზია დაწინაურდა.

ლეინ დევისმა და სტივენ დეიკმა შექმნეს ყველაზე ძველი და ცნობილი „რუტკიტი“ 1990 წელს „Sun Microsystems 'SunOS UNIX“ ოპერაციული სისტემისთვის. „Windows NT“

ოპერაციული სისტემისთვის პირველი მავნე „რუტკიტი“ გამოჩნდა 1999 წელს, რომელიც შექმნა გრეგ ჰოგლუნდმა.

2005 წელს, პროგრამული უზრუნველყოფის ინჟინერმა მარკ რასინოვიჩმა შექმნა „რუტკიტის“ გამოვლენის ინსტრუმენტი „RootkitRevealer“, რის შემდეგაც აღმოაჩინა „რუტკიტი“ მის ერთ-ერთ კომპიუტერზე. მომხდარმა სკანდალმა საზოგადოების ცნობიერების ამაღლება გამოიწვია „რუტკიტის“ შესახებ.

„რუტკიტის“ ორი ძირითადი ტიპია: მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ და ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტი“. მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ თავსდება კომპიუტერის ოპერაციულ სისტემაში, როგორც პროგრამები. ისინი ახორციელებენ თავიანთ მიზანს აპარატზე მუშაობის პროცესში მეხსიერების გადაწერით, რომელსაც პროგრამა იყენებს. ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტი“ მუშაობს კომპიუტერის ოპერაციული სისტემის ყველაზე დაბალ დონეზე და თავდამსხმელს ანიჭებს ყველაზე ძლიერ პრივილეგიებს კომპიუტერში. ბირთვის რეჟიმის(“Kernel-mode”) „რუტკიტის“ დამონტაჟების შემდეგ, თავდამსხმელს აქვს სრული კონტროლი კომპიუტერულ სისტემაზე და შესაბამისად, შეუძლია ნებისმიერი მოქმედების განხორციელება საკუთარი მიზნებისთვის. ბირთვის რეჟიმის (“Kernel-mode”) „რუტკიტი“, როგორც წესი, უფრო რთული აღმოსაჩენი და აღმოსაფხვრელია, ვიდრე მომხმარებლის რეჟიმის(“User-mode”) „რუტკიტი“ და უფრო ნაკლებადაა გავრცელებული.

ბოლო წლების განმავლობაში, წარმოიქმნა მობილური „რუტკიტის“ ახალი კლასი, სმარტფონებზე, კონკრეტულად Android მოწყობილობებზე შეტევისთვის.

კარგად ცნობილი „რუტკიტის“ მაგალითებია:

„Machiavelli“ - პირველი “რუტკიტი”, რომელიც მიზანში იღებს “Mac OS X”-ის ოპერაციულ სისტემას და გამოჩნდა 2009 წელს. ეს “რუტკიტი” ქმნის ზარების დაფარულ სისტემას.

„Zeus” - რომელიც პირველად იდენტიფიცირდა 2007 წლის ივლისში და ფარულად იპარავდა საბანკო ინფორმაციას მოხმარებლების კომპიუტერული სისტემებიდან.

“Stuxnet” - პირველი ცნობილი “რუტკიტი” სამრეწველო კონტროლ-სისტემებისთვის.

“Flame” - კომპიუტერის „მავნე პროგრამა“, რომელიც აღმოაჩინეს 2012 წელს. თავს ესხმის კომპიუტერებს, რომლებიც მუშაობენ “Windows OS” კომპიუტერულ სისტემაზე. მას შეუძლია ჩაიწეროს ხმა, შექმნას „სქრინშოთები“ (“screenshots”) და გააკონტროლოს კლავიატურაზე წვდომა.

დღეს ჩვენი ყოველდღიური ცხოვრება უშუალოდ დაკავშირებულია ციფრულ ტექნოლოგიასთან, რაც მნიშვნელოვნად ზრდის კიბერდანაშაულების რიცხვს. ყოველი ახალი შემთხვევა უნდა იყოს ჩვენთვის მაგალითი, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე

ინტერნეტ სივრცეში ყოფნისას და არ გავხდეთ „ჩვენივე ნებით“ ჰაკერებისა და მავნე პროგრამების შემდეგი მსხვერპლი.

საჭიროა პრევენციული ღონისძიებების აქტიური გატარება. „მნიშვნელოვანია მაღალი სტანდარტების შეტევების პრევენციის სენსორული სისტემების დანერგვა, ფართო მასშტაბის კიბერკონტრდაზვერვის გეგმისა და თავდაცვითი სტრატეგიების შემუშავება. ამ თვალსაზრისით პრიორიტეტულია უწყებათაშორისი კოორდინაცია და კომუნიკაცია. მნიშვნელოვანია ქვეყნის შიგნით საკანონმდებლო ბაზის არა მარტო შემუშავება, არამედ აღსრულება. ამ პრობლემასთან გამკლავება ასევე საჭიროებს მჭიდრო საერთაშორისო თანამშრომლობას.”[1]

ბიბლიოგრაფია

1. "What is a rootkit and how to remove it" Written by Serge Malenkovich on March 28, 2013 https://www.kaspersky.com/blog/rootkit/1508/?fbclid=IwAR3fQU_Cldd3WgxwKomc2IJ7n_nO-Fj62IDPv2Kobkl-A3T26zh3qx7MbFQ
2. "ROOTKIT: WHAT IS A ROOTKIT?
   Rootkit: What Is a Rootkit, Scanners, Detection and Removal Software" https://www.veracode.com/security/rootkit?fbclid=IwAR0hx_sd739-mYTSAn8Q4u8R48BTrIA-OF-7_z832CaHaQnir_lF2hB-_3M
3. "What is Malware? How Malware Works & How to Remove It" by Joseph Regan on July 11, 2019 https://www.avg.com/en/signal/what-is-malware?fbclid=IwAR1up9OviyqJypGSZeKYi_j8UtryCh89ZFIaPAC3JNN1EH1kjWjtTkzSeYA
4. სისხლის სამართლის კერძო ნაწილი. წიგნი 2. მ.ლეკვეიშვილი, ნ.თოდუა და გ.მამულაშვილი. გამომცემლობა ,,მერიდიანი“, თბ. 2017

[1] სისხლის სამართლის კერძო ნაწილი. წიგნი 2. მ.ლეკვეიშვილი, ნ.თოდუა და გ.მამულაშვილი. გამომცემლობა ,,მერიდიანი“, თბ. 2017, გვ 145;