Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 18-21 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

„PROMETEI“ - ახალი „ბოტნეტი“ კიბერდანაშაულისთვის”
“PROMETEI” – THE NEW “BOTNET” FOR CYBERCRIME”

ნათია ფილაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, IV კურსის სოციოლოგიის მიმართულების სტუდენტი.
Natia Pilashvili _ Ivane Javakhishvili Tbilisi State University, Sociology_Junior;
მარიამ კიკლიაშვილი _ ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის ბაკალავრიატის, IV 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. დღესდღეობით კრიპტოვალუტა ერთ-ერთი უდიდესი ინტერესის საგანია, ვინაიდან იგი სწრაფი ზრდადობით გამოირჩევა და უფრო და უფრო მეტ ქვეყანაში იმკვიდრებს ადგილს. სწორედ, „Prometei“ არის კრიპტოვალუტის მოსაპოვებლად გამოყენებული სრულიად ახალი კიბერდანაშაულის იარაღი, რომლის საშუალებითაც უამრავი ადამიანი ფინანსურად დაზარალდა.

ANNOTATION: In the 21st century, with the rapid advancement of technology, there is a growing trend of undetected and unsolved crimes in cybercrime, often referred to as the "crime of the future". Malware, which is one of the main mechanisms of cybercrime, makes it easy for each of us to fall victim to them. Cryptocurrency is one of the biggest topics of interest today, as it is growing rapidly and is gaining ground in more and more countries. „Prometei“ is a completely new cybercrime tool used to mine for cryptocurrency, and has already financially affected many people.

საკვანძო სიტყვები: *კიბერდანაშაული, მალვეარი, „ბოტნეტი“,„Prometei“, კრიპტოვალუტა.*

KEYWORDS: *cyber crime, malware, botnet "Prometei", crypto currency*

„ბოტნეტი“ წარმოადგენს ინტერნეტ ქსელში ჩართულ კომპიუტერთა ერთობლიობას, რომელთა თავდაცვის უნარი დარღვეულია. მათი მართვა მესამე პირის მიერ დისტანციურად ხდება. „ბოტი“(bot) - ასე უწოდებენ დაინფიცირებულ მოწყობილობას. მოწყობილობის დაინფიცირება ხდება კომპიუტერულ ქსელში მალვეარის შეჭრით, აგრეთვე იგი ცნობილია, როგორც მავნე პროგრამა. „ბოტნეტის“ მართვა მეტწილად IRC(Internet Relay Chat)-იდან ხდება, თუმცა მისი მართვა შესაძლებელია ვებგვერდიდანაც. საზიანო პროგრამების გამოყენების შემთხვევაში კომპიუტერები შესაძლოა, შეიტყუონ ბოტნეტში, მას შემდეგ, რაც მომხმარებელი ეწვევა დავირუსებულ საიტს და გადმოტვირთავს ამა თუ იმ ინფორმაციას. საზიანო ვირუსი შესაძლოა მიმაგრებული ფაილის სახითაც აღმოჩნდეს კომპიუტერში.

ტერმინ „ბოტნეტის“ გამოყენება შეგვიძლია კომპიუტერების ნებისმიერ ჯგუფზე, მაგალითად ასეთივეა IRC ბოტი. „ბოტ“-ის მფლობელს შეუძლია ჯგუფის დისტანციური კონტროლი, IRC-ის საშუალებით უმთავრესად კრიმინალური მიზნებისთვის. სერვერი ცნობილია (C&C) სერვერის სახელწოდებით. „ბოტის“ გაშვება ხდება მალულად, და გამოიყენება ფარული გზები (მაგ. ტვიტერი ან მესიჯი) კომუნიკაციის დასამყარებლად C&C სერვერთან. დამნაშავის ხელში გადადის რამდენიმე სისტემა სხვადსხვა ხელსაწყოს მეშვეობით. ახალი ”ბოტები” ავომატურად ასკანერებენ სისტემაში არსებულ მონაცემებს უადვილდებათ დანაშაულის ჩადენა, თუკი მომხმარებლის სისტემაში არასაიმედო პაროლები არსებობს.

რაც უფრო მეტი ინფორმაციის მოპოვებას შეძლებს ”ბოტი” სისტემიდან, მით უფრო ფასეული გახდება ”ბოტნეტის” მფლობელისთვის. კომპიუტერული სისტემიდან მონაცემების მოპარვას ”ბოტნეტში” ჩართვის შედეგად ასევე ეწოდება „Scrumping”-იც. „ბოტნეტს” უმთავრესად ჰყავს ერთი ან რამდენიმე მაკონტროლებელი პირი, რომელთაც არ გააჩნიათ ერთგვარი იერარქია, მათი ურთიერთობა დამყარებულია ინდივიდუალურ მეგობრულ კავშირებზე. 2006 წლის მონაცემებით მსგავსი ქსელის საშუალო ზომა შეადგენდა 20 000 კომპიუტერს, თუმცა ამჟამად ოპერირებენ უფრო ფართო ქსელებიც.

„ბოტნეტის“ შექმნის 4 საფეხური:

1. „ბოტნეტის“ მაკონტროლებელი პირი გზავნის ვირუსს/ვორმს და მათი საშუალებით აინფიცირებს მომხმარებელთა კომპიუტერებს.

2. „ბოტი“ შედის კონკრეტულად C&C სერვერზე.
3. სპამერი ოპერატორისგან იღებს „ბოტნეტის“ სერვისებს.
4. სპამერი ოპერატორს უგზავნის შეტყობინებას და გასცემს სპამ შეტყობინების გაგზავნის ბრძანებას.

„ბოტნეტის“ გამოყენება სხვადასხვა მიზნებისთვის ხდება, ასეთი შესაძლოა იყოს, პაროლების მოპოვება, საკრედიტო ბარათების ნომერთა ხელში ჩაგდება, აპლიკაციების მოპარვა და სახელმწიფო ქსელებზე კიბერ შეტევებიც კი.

Cisco Talos Intelligence Group არის მსოფლიოში ყველაზე მასშტაბური კომერციული საფრთხეების სადაზვერვო ჯგუფი, რომელიც შედგება მსოფლიო დონის მკვლევრების, ანალიტიკოსებისა და ინჟინრებისგან. სწორედ ამ სადაზვერვო ჯგუფმა აღმოაჩინა ახალი ბოტნეტი, სახელწოდებით - Prometei, რომელიც 2020 წლის მარტიდან განსაკუთრებით აქტიური გახდა და ძირითადად ორიენტირებულია კრიპტოვალუტის მოპოვებაზე.

კრიპტოვალუტა წარმოადგენს ელექტრონულ ფულს, რომლის საფუძველიცაა „ბლოკჩეინის სისტემა“ და იგი სახელმწიფოსა თუ ბანკებიდან დამოუკიდებლად ოპერირებს. თანამედროვე ტექნოლოგიების მეშვეობით მათი ღირებულება დღითიდღე იზრდება, შესაბამისად სხვადასხვა პლატფორმებზე მიმდინარეობს ვაჭრობა მათი საშუალებით. ამ ვალუტას ფიზიკური სახე არ გააჩნი, მასთან დაკავშირებული ნებისმიერი ოპერაცია ხორციელდება ინტერნეტის მეშვეობით.

Prometei-ს მსხვერპლი გახდნენ აშშ-ს, ბრაზილიის, პაკისტანის, ჩინეთის, მექსიკის და ჩილეს მოქალაქეები. ოთხი თვის შემდეგ „ბოტნეტის“ მაკონტროლებლებმა მოიპოვეს დაახლოებით 5000$, საშუალოდ 1,250 აშშ დოლარი თვეში.

საერთო ჯამში, მკვლევრებმა 15-ზე მეტი გავრცელების ტექნიკა დაითვალეს Prometei–ში. ყველა მათგანს აკონტროლებს მთავარი მოდული, რომელსაც შეუძლია გაშიფროს (RC4)მონაცემები იქამდე, ვიდრე იგი HTTP-ით გააგზავნის მართვის სერვერზე.

ბოტნეტი იპარავს პაროლებს Mimikatz-ის შეცვლილი ვერსიის საშუალებით, რის მერეც ეს პაროლები Spreader მოდულს გადაეგზავნება SMB-ს ანალიზისა და ავთენტიფიკაციისათვის. იმ

მშემთხვევაში თუ ეს გზა არ იმუშავებს, გამრავლებისთვის გამოიყენება EternalBlue-ს ექსპლოიტი.

ყოველი ახალი კიბერდანაშაულის შემთხვევა კარგად გვიჩვენებს, თუ როგორი საფრთხის წინაშე დგას თითოეული ჩვენგანი ციფრულ ტექნოლოგიასთან და სოციალურ ქსელებთან გადაჯაჭვული ცხოვრების გამო, რაც დღევანდელობის განუყოფელი ნაწილია. საჭირო და მნიშვნელოვანია ეს მაგალითი იყოს ჩვენთვის, იმისთვის, რომ გამოვიჩინოთ უფრო მეტი სიფრთხილე ინტერნეტ სივრცეში ყოფნის დროს, რათა არ გავხდეთ მავნე პროგრამების მორიგი მსხვერპლი.

ბიბლიოგრაფია

1. “Prometei botnet exploits Windows SMB to mine for cryptocurrency” By Charlie Osborne for Zero Day | July 22, 2020 www.zdnet. com https://www.zdnet.com/article/prometei-botnet-is-infecting-machines-to-mine-for-cryptocurrency/
2. “Botnets “ Published under Glossary www.enisa.europa.eu https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets