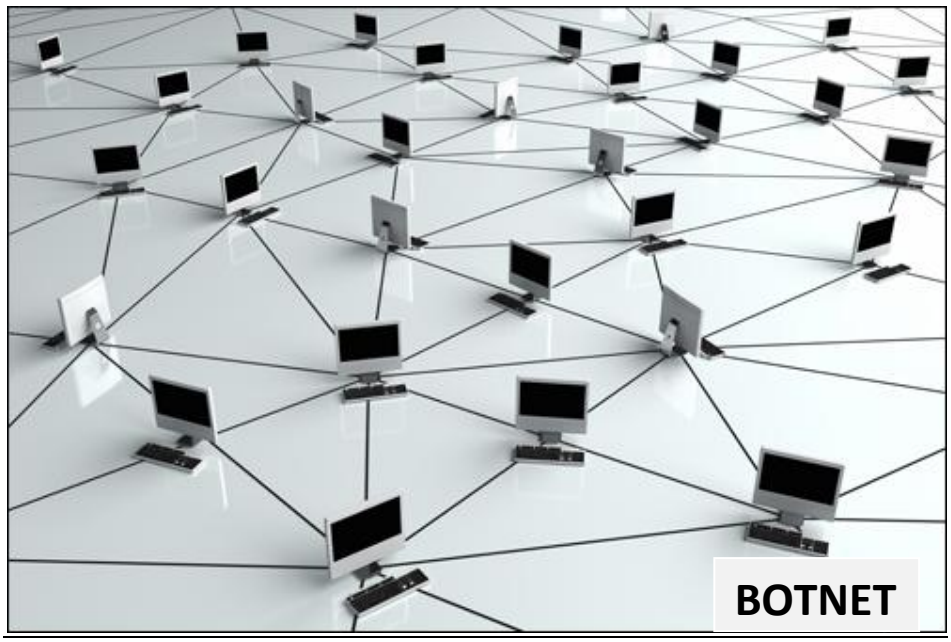
ბოტნეტი



ბოტნეტი არის ინტერნეტ ქსელში ჩართული კომპიუტერების ერთობლიობა, რომელთა თავდაცვის უნარი არის დარღვეული და ხდება მათი დისტანციური მართვა მესამე პირის მიერ. დაინფიცირებულ მოწყობილობას ეწოდება „ბოტი“ (bot) და იგი იქმნება როდესაც ხდება კომპიუტერში შეჭრა მალვეარისაგან, აგრეთვე ცნობილი როგორც მავნე პროგრამა. ბოტნეტი უმეტესად იმართება IRC-იდან (Internet Relay Chat) მაგრამ მისი მართვა შესაძლებელია ვებ გვერდიდანაც.

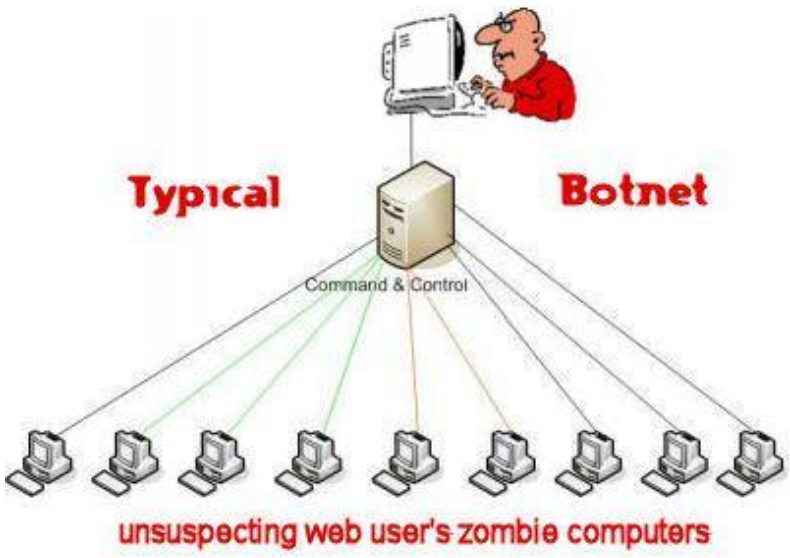
კომპიუტერები შეიძლება შეტყუებული იყოს ბოტნეტში, როდესაც ისინი გამოიყენებენ საზიანო პროგრამებს. ეს შეიძლება მოხდეს იმის შედეგად, რომ მომხმარებელი ეწვიოს არასანდო საიტს და გადმოტვირთოს ესა თუ ის ინფორმაცია. აგრეთვე შესაძლებელია საზიანო ვირუსი მოვიდეს მიმაგრებული ფაილის სახითაც.

ტერმინი „ბოტნეტი“ შეგვიძლია გამოვიყენოთ კომპიუტერების ნებისმიერ ჯგუფზე, ისეთზე როგორიცაა IRC ბოტი. ბოტნეტის წამომწყებს, იგივე „ბოტ“ მფლობელს შეუძლია აკონტროლოს ჯგუფი დისტანციურად ძირითადად IRC-ის მეშვეობით და ძირითადად კრიმინალური მიზნებისათვის. სევერი ცნობილია როგორც (C&C) სერვერი.

ბოტი ტიპიურად გაიშვება მალულდ და იყენებს ფარულ არხს (მაგ.RFC 1459 (IRC), ტვიტერს ან მესიჯს) იმისათვის რომ დაამყაროს კომუნიკაცია C&C სერვერთან. დამნაშავე ხელში იგდებს რამოდენიმე სისტემას სხვადსხვა ხელსაწყოს გამოყენებით. ახალ ”ბოტებს” შეუძლიათ ავომატურად დასკანონ გარემო და გაუადვილდეთ დანაშაულის ჩადენა მარტივი და არასაიმედო პაროლების არსებობის შემთხვევაში.

რაც უფრო მეტი ზიანის მიყენებას შეძლებს ”ბოტი” მით უფრო ფასეული ხდება იგი ”ბოტნეტის” კონტროლერისათვის. კომპიუტერული რესურსების მოპარვას იმის შედეგად რომ სისტემა გაერთიანდა ”ბოტნეტში” აგრეთვე უწოდებენ ” scrumping”-საც.

’ბოტნეტი” ძირითადად შედგება ერთი ან რამოდენიმე კონტროლერისგან, რომლებსაც იშვიათად აქვთ ბრძანებლობის იერარქია, ისინი ეყრდნობიან ინდივიდუალურ მეგობრულ ურთიერთობებს. 2006 წლის მონაცემებით ქსელის საშუალო ზომა იყო 20 000 კომპიუტერი, თუმცა ამაზე ფართო ქსელებიც აგრძელებენ ოპერირებას.



ბოტნეტის ფორმირება

ეს მაგალითი გვიჩვენებს თუ როგორ იქმნება ბოტნეტი და როგორ გამოიყენება სპამ მეილის გასაგზავნად.

1. ბოტნეტის ოპერატორი აგზავნის ვირუსს ან ვორმს და აინფიცირებს ჩვეულებრივი მომხმარებლების კომპიუტერს.
2. ბოტი დაინფიცირებულ კომპიუტერზე შედის კონკრეტულ C&C სერვერზე.
3. სპამერი იძენს ბოტნეტის სერვისებს ოპერატორისაგან
4. სპამერი აწვდის შეტყობინებას ოპერატორს, რომელიც სპამ შეტყობინებების გაგზავნის განკარგულებას გასცემს.

ბოტნეტი გამოიყენება სხვადასხვა მიზნებისათვის მაგ: პაროლების მოსაპოვებლად, საკრედიტო ბარათების ნიმრების ხელში ჩასაგდებად, აპლიკაციების მოსაპარად და სხვა საზიანო მიზნების მისაღწევად. კიბერ დამნაშავეები ბოტნეტს იყენებენ მრავალი კრიმინალური საქმიანობისათვის, დაწყებული სპამის გაგზავით დამთავრებული სახელმწიფო ქსელებზე კიბერ შეტევებით.

სპამის დაგზავნა არის ყველაზე გავრცელებული ვარიანტი. მრავალათასიანი ბოტნეტის მეშვეობით სპამერებს შეუძლიათ გააზავნონ მილიონობით

ელექტრონული წერილი მცირე დროის მონაკვეთში და ასევე ამ გზით გაავრცელონ ვირუსი, რომელიც შემდგომ გაზრდის ინფიცირებული კომპიუტერების რაოდენობას.

კიბერ შანტაჟი - ბოტნეტი ფართოდ გამოიყენება DDoS კიბერ შეტევებისთვისაც (Distributed Denial of Service - სერვისის შეჩერება). ამ ტიპის შეტევის დროს ზომბირებული კომპიუტერებიდან ერთდროულად იგზავნება ათასობით მოთხოვნა სამიზნე სერვერზე (ვებ-გევრდზე), შედეგად სერვერი ვერ ასწრებს ამდენი მოთხვნის დამუშავებას, იტვრთება და ხდება ხელმიუწვდომელი.

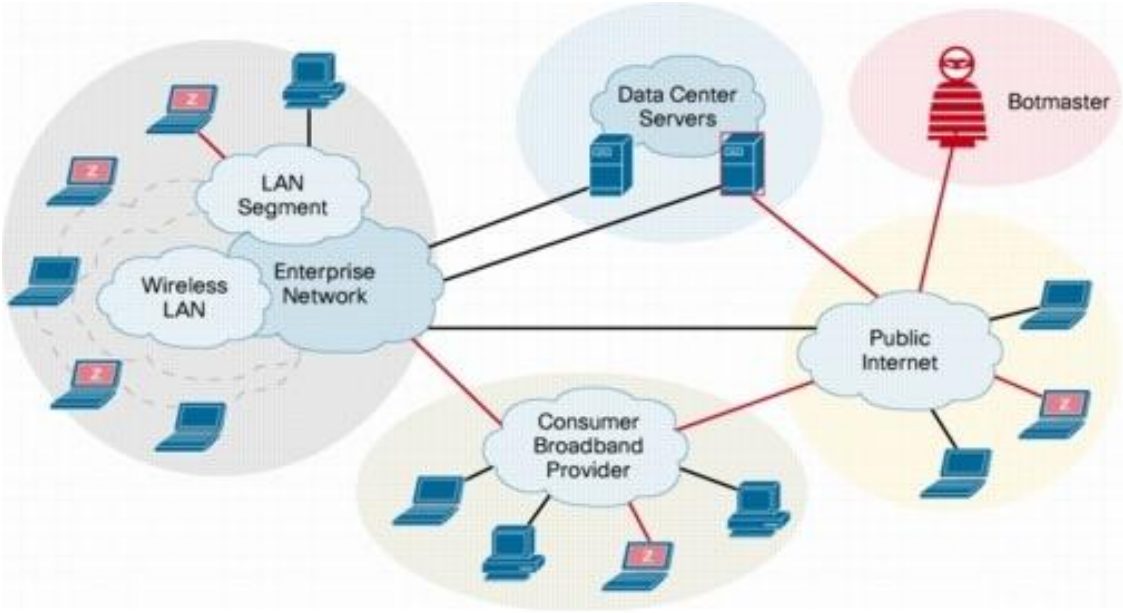
რადგან დღეს ბევრი კომპანია მუშაობს ინტერნეტის მეშვეობით, მათი ვებ გვერდის ან ელექტრონული სერვისის გათიშვა ნიშნავს ბიზნესის შეჩერაბას და ფულის დანაკარგს, იმისათვის რომ თავიანთ სერვერებს დაუბრუნონ სტაბილურობა ფულს უხდიან შანტაჯისტებს. DDoS შეტევებს შეიძლება ახასაიათებდეს პოლიტიკური დატვირთვაც და შეიძლება ატარებდეს პროვოკაციულ ხასიათს. ამ შემთხვევაში შეტევის სამიზნე ხდებიან სამთავრობო დაწესებულებების სერვერები.

ინტერნეტში ანონიმური წვდომა - ზომბირებული კომპიუტერის მეშვეობით დამნაშავეს შეუძლია განახორციელოს კიბერ დანაშაული, მაგალითად გატეხოს სხვისი ვებ-გვედი ან გადარიცხოს მოპარული ფულადი სახსრები და ამ დროს დარჩეს ანონიმური, რადგან ამ დროს ზომბი კომპიუტერი გამოიყენება როგორც ე.წ. პროქსი სერვერი (Proxy) დამნაშავის რეალური მისამართის დასამალად.

ბოტნეტის გაყიდვა ან გაქირავება - ბოტნეტის მეშვეობით ფულის შოვნა დამნაშავეებს შეუძლიათ მათი არენდით გადაცემით სხვა პირებზე ან უკვე მზა ქსელის გაყიდვით, ასე რომ ბოტნეტის შექმნა მისი შემდგომი გაყიდვა-გაქირავების მიზნით არის კიდევ ერთი კიბერ დანაშაულის მიმართულება.

კონფიდენციალური და პირადი ინფორმაციის მოპარვა - ამ ტიპის დანაშაული ალბათ არასდროს არ შეწყვეტს კიბერ დამნაშავეების მოხიბლვას, რადგან ბოტნეტის მეშვეობით შესაძლებელია მომხმარბელთა პაროლების (მაგალითად ელ-ფოსტის, Skype-ის, ICQ-ს, ვებ გვერდის პაროლები) და სხვა კონფიდენციალური მონაცემების მოპარვა. ბოტი, რომლითაც ინფიცირებულია კომპიუტერი შეუძლია გადმოიწეროს სხვა მავნე პროგრამა მაგ. ტროიანი, რომელიც იპარავს პაროლებს , შედეგად ყველა ზომბირებული კომპიუტერზე ავტომატურად გავრცელდება ეს პროგრამა რისი მეშვეობითაც დამნაშავეებს შეეძლებათ მიიღონ სხვა ინფიცირებული კომპიუტერების მომხმარებელთა პაროლები.

როგორ ხდება ბოტნეტის ფორმირება და გავრცელება?



ბოტ-პროგრამის შესაქმნებლად იყენებენ სხვადასხვა პროგრამირების ენებს. ბოტების გავრცელება ხდება ავტომატურად ბოტნეტის ანუ სხვა, უკვე ზომბირებული კომპიუტერების მეშვეობით. ძირითადად არის 2 გზა :

1. სპამ წერილის მეშვეობით რომელიც შეიცავს სახიფათო ვებ-გვერდის ბმულს ან წერილს მიმაგრებული აქვს ფაილი რომელიც შეიცავს მავნე პროგრამას.
2. ინფიცირებულ სახიფათო ვებ გვერდზე შესვლისას სადაც განთავსებულია ე.წ. i-frame მალულად ხდება კომპიუტერის დავირუსება მავნე ჩამტვირთავი კოდით, რომელიც შემდგომ ინტერნეტიდან ავტომატურად იწერს სხვადასხვა მავნე პროგრამებს და უკავშირდება ბოტნეტის მართვის ცენტრს.

რატომ ხდება კომპიუტერების დაინფიცირება?

საქართველოში უმეტეს კომპიუტერზე დაყენებულია Window-ის არალიცენზირებული ”გატეხილი” ვერსიები, რომელიც არ აკეთებს მუდმივ განახლებებს, ამის გამო აქვს ბევრი ”ხვრელი” საიდანაც შეიძლება კომპიუტერის დავირუსება. იგივე შეეხება ანტივურუსებსაც, მაგრამ შესაძლებელია რომ ლიცენზირებულმა ანტივირუსმაც კი ვერ აღმოაჩინოს ჩამტვრითავი კოდი, იმიტომ რომ იგი სპეციალურად ისე არის დაწერილი რომ გვერდი აუაროს ანტივურუსის დაცვას.

შემდგომ პროგრამა თვითონ იწყებს სხვა დანარჩენი ნაწილების თუ მავნე პროგრამების გადმოწერას კომპიუტერში, რომლებიც შეასრულებენ მართვის ცენტრის სხვადასხვა ბრძანებებს.