ანტივირუსი

ანტივირუსი არის პროგრამა, რომელიც გამოიყენება კომპიუტერისათვის საზიანო პროგრამებისაგან თავის დასაცავდ. დღესდღეობით ტრადიციული ანტივირუსული პროგრამა არ არის საკმარისი კომპიუტერის დასაცავად ყველა შესაძლო საფრთხისაგან, როგორიცაა კიბერ თავდასხმები, ბოტნეტები, DdoS თავდასხმები, ფიშინგი, სპამი და სხვა. კომპიუტერული უსაფრთხოებისათვის პროგრამის მწარმოებელი კომპანიები ხშირად სთავაზობენ მომხმარებლებს ანტივირუსულ პროდუქტებს და სერვისებს.

მიუხედავად იმისა თუ რამდენად სრულყოფილია პროგრამა მას შეიძლება აღმოაჩნდეს სუსტი მხარეებიც. ანტივირულული პროგრამა შეიძლება საზიანო იყოს

კომპიუტერის ფუნცქიების შესრულებისათვის. გამოუცდელმა მომხმარებლებმა შეიძლება არ იცოდნენ ანტივირუსულ პროგრამასთან მუშაობა.

ისტორია

კომპიუტერული ვირუსები, რომლებიც შექმნილი იყო ადრეულ და შუა ოთხმოციან წლებში არ იყო ბოლომდე სრულყოფილი და არ შეეძლო ისეთი დიდი ზიანი მიეყენებინა კომპიუტერული სისტემისათვის ან მომხმარებლისათვის როგორიც დღეს შეუძლია. ეს სიტუაცია შეიცვალა მას შემდეგ რაც უფრო და უფრო მეტი პროგრამისტი გაეცნო ვირუსის პროგრამირებას და შექმნეს ისეთი ვირუსები, რომლებიც მანიპულირებენ დაინფიცირებულ კომპიუტერზე არსებული მონაცემებით ან ანადგურებენ მათ.

მიმდინარეობს კამათი იმის შესახებ თუ რომელი ანტივირუსული პროგრამა შეიქმნა პირველად. პირველი დოკუმენტირებული ანტივირუსული პროგრამა შეიქმნა კომპანია „Bernd Fix“ -ის მიერ 1987 წელს. აგრეთვე 1987 წელს გამოჩნდა კიდევ ორი ანტივირუსული პროგრამა, რომელიც შეიქმნა კომპანია „Atari ST“ -ის მიერ.

ფრედ კოჰენმა პირველმა დაბეჭდა აკადემიური ნაშრომი კომპიუტერული ვირუსების შესახებ 1984 წელს. მან დაიწყო ანტივირუსლი სტრატეგიების შემუშავება 1988 წელს, რომლებიც ანტივირუსული პროგრამების კომპანიების მიერ იქნა გამოყენებული და

კიდევ უფრო განვითარებული და სრულყოფილი სახე მიეცა. ფრედ კოჰენმა 1987 წელს გამოაქვეყნა ნაშრომსი სადაც საუბარი იყო იმაზე, რომ არ არსებობდა ალგორითმი რომელიც სრულად შეძლებდა ყველა სახის ვირუსის აღმოჩენას.

1987 წელს პირველად გამოჩნდა ორი ანტივირუსული მოწყობილობა: „Flushot Plus“ როს გრინბერგის მიერ და „Anti4us“ ერვინ ლანტინგის მიერ.

1988 წელს მეილინგ ლისტის „VIRUS-L“ დაგზავნა დაიწყო „BITNET/EARN“ ქსელში სადაც განიხილავდნენ ახალ ვირუსებს, მათი აღმოჩენისა და მათგან თავდაცვის გზებს. ზოგმა მეილინგ ლისტის წევრმა, მაგალითად ჯონ მაკაფიმ და ევგენი კასპერსკიმ მოგვიანებით დააარსეს პროგრამის მწარმოებელი საკუთარი კომპანიები და დაიწყეს ანტივირუსული პროგრამის კომერციული გაყიდვები.

ინტერნეტის ფართოდ გავრცელებამდე, ვირუსების გავრცელება ძირითადად ხდებოდა „floppy“ დისკების მეშვეობით. ანტივირუსული პროგრამები მაგ დროისათის არ განახლდებოდა ისე ხშირად როგორც დღესდღეობით. დღეს ყველაზე ხშირად ვირუსები ვრცელდება ინტერნეტის მეშვეობით. უკანასკნელი წლების განმავლობაში ანტივირუსული პროგრამის მწარმოებელ კომპანიებს უხდებათ სხვა და სხვა ტიპის ვირუსებთან გამკლავება.

- არსებობს ისეთი ვირუსები, რომლებიც გვხვდება მაიკროსოფტ ვორდში. ზოგიერთი ვირუსი პირდაპირ დოკუმენტშია ჩაბეჭდილი. ეს კი შესაძლებელს ხდის დოკუმენტში არსებული ფარული ვისრუსების მეშვეობით დაზიანდეს კომპიუტერი.
- მომხმარებლის კომპიუტერი შეიძლება დაინფიცირდეს ვირუსის შემცველი დოკუმენტის მხოლოდ გახსნით ან შეტყობინების მიღებით.

ვინაიდან დღესდღეობით აქტუალური და ფართოდ გავრცელებულია ინტერნეტის მეშვეობით კავშირი, უფრო და უფრო მეტი ვირუსის ტიპს აქვს გავრცელების საშუალება. ამან გამოიწვია ანტივირუსული პროგრამის ხშირი განახლების აუცილებლობა.

ვირუსების აღმოჩენა

<u>სიგნატურის მეთოდი</u>

ეს მეთოდი არის ყველაზე ფართოდ გავრცელებული. იგი გამოიყენება მრავალი ანტივირუსული პროგრამის მწარმოებელი კომპანიების მიერ. ამ ტიპის ვირუსის აღმოჩენისათვის ანტივირუსულ პროგრამას ესაჭიროება სიგნატური ანუ ანაბეჭდი. ანაბეჭდის აღმოჩენა შესაძლებელია ანტივირუსის ბაზაში.

ანტივირუსული პროგრამის მწარმოებელი კომპანიები თავიანთ ლაბორატორიებში აანალიზებენ ვირუსებს და პოულობენ მათგან თავდაცვის გზებს. სასურველია ანტივირუსული ბაზის ხშირი განახლება, რათა მოხდეს ვირუსის დროული განეიტრალება.

<u>ალბათობის ანალიზის მეთოდი</u>

ალბათობის ანალიზის მეთოდი იყოფა ორ ნაწილად, ევრისტიკულ და ქცევის ანალიზის მეთოდებად.

ევრისტიკული ანალიზი - არის ტექნოლოგია რომელიც დაფუძნებულია ალბათობის ალგრითმებზე, რის შედეგადაც ხდება საეჭვო ობიექტების აღმოჩენა და გამოიყენება იმისთვის რომ კომპიუტერი არ დავირუსდეს სანამ ახალი ანაბეჭდები მომხმარებლის ანტივირუსის ბაზამდე მიაღწევს. ევრისტიკული ანალიზის პროცესში მოწმდება ფაილის სტრუქტურა და მისი შესაბამისობა ვირუსულ შაბლონებთან, ან უკვე ცნობილი ვირუსების მოდიფიცირებულ სახეებთან და კომბიანციებთან. ამ ტექნოლოგიას არ შეუძლია 100%-ით დაადგინოს ვირუსის არსებობა და როგორც ყველა ალბათობის მექანიზმს შესაძლებელია მცდარი შედეგი მოჰყვეს.

ქცევის ანალიზის მეთოდი - არის ტექნოლოგია რომელიც აანალიზებს ფაილს ან პროგრამას მისი კომპიუტერში განხორციელებელი ოპერაციის მიხედვით, მაგრამ ვირუსებისთვის დამახასიათებელი ბევრი მოქმედება შეიძლება ასევე განხორციელებულ იქნას ჩვეულებრივი პროგრამების მიერ, ასე რომ ეს მეთოდიც არ იძლევა 100%-ით დაცვას. ქცევის ანალიზის შემთხვევაში უძლურია ტრადიციული, ვირუსების ბაზაზე დაყრდნობილი სკანირების მეთოდი, შედეგად იგი ვერ გებულობს ახალია თუ ძველი ვირუსი , მაგრამ კომპიუტერი ბოლომდე დაუცველი მაინც არ რჩება, ის ყველა საეჭვო პროგრამის მოქმედებას აანალიზებს რეალურ დროში და ვინაიდან არ შეუძლია მკურნალობა ან წაშლა, ბლოკავს საეჭვო პროგრამებს თუ ფაილებს.

თაღლითური ანტივირუსები

2009 წლიდან გავრცელდა ე.წ ”ყალბი” ანტივირუსები - პროგრამული უზრუნველყოფა რომელსაც რეალურად არ გააჩნდა ანტივირუსის ფუნქციები, მაგრამ ვიზუალურად ჰგავს მას. მათი ძირითადი მიზანი იყო თაღლითური გზით ფულის გამოძალვა, ვითომდა კომპიუტერის ვირუსებისგან გასაწმენდად. ყალბი-ანტივირუსი ავტომატურად ინსტალირდებოდა მომხმარებლის კომპიუტერზე და ასკანირებდა მას, რის შემდეგაც სთავაზობდა ვითომდა აღმოჩენილი ვირუსების წაშლას პროგრამის გააქტიურების გზით. მომხარებელს უნდა გაეგზავნა SMS შეტყობინება კონკრეტულ ნომერზე და მიეღო გააქტიურების კოდი. ამავე დროს მომხმარებელს არ ჰქონდა საშუალება დაეხურა ან გაეთიშა ყალბი ანტივირუსის პროგრამა.

ამიტომ ყურადღება მიაქციეთ რომელი კომპანიის ანტივირუსს აინსტალირებთ თქვენს კომპიუტერზე და რომელი ვებ-გვერდიდან იწერთ მას, რადგან მსგავსი ტყუილი ანტივურუსების გავრცელება ხდებოდა ელექტრონული ფოსტით მიღებული საეჭვო წერილებისა და საეჭვო ვებ გვერდების მეშვეობით , რომლებიც სთავაზობდნენ უფასო ანტივირუსს

. 

თანამედროვე ანტივირუსული პროგრამული უზრუნველყოფა ძირითადად განკუთვნილია Windows-ის ოპერაციული სისტემისათვის. ეს იმით არის განპირობებული, რომ ეს პლათფორმა არის ერთერთი ყველაზე პოპულარული და ამიტომ განსაკუთრებით ამ პლათფორმისათვის იქმნება დიდი რაოდენობით ვირუსები და მავნე პროგრამები, მაგრამ დღესდღეობით უკვე გამოდის ანტივირუსები სხვა პლათფორმებისათვის როგორიცაა Linux და Mac OS X, რადგან ამ სისტემებისათვისაც დაიწყეს ვირუსების გავრცელება.

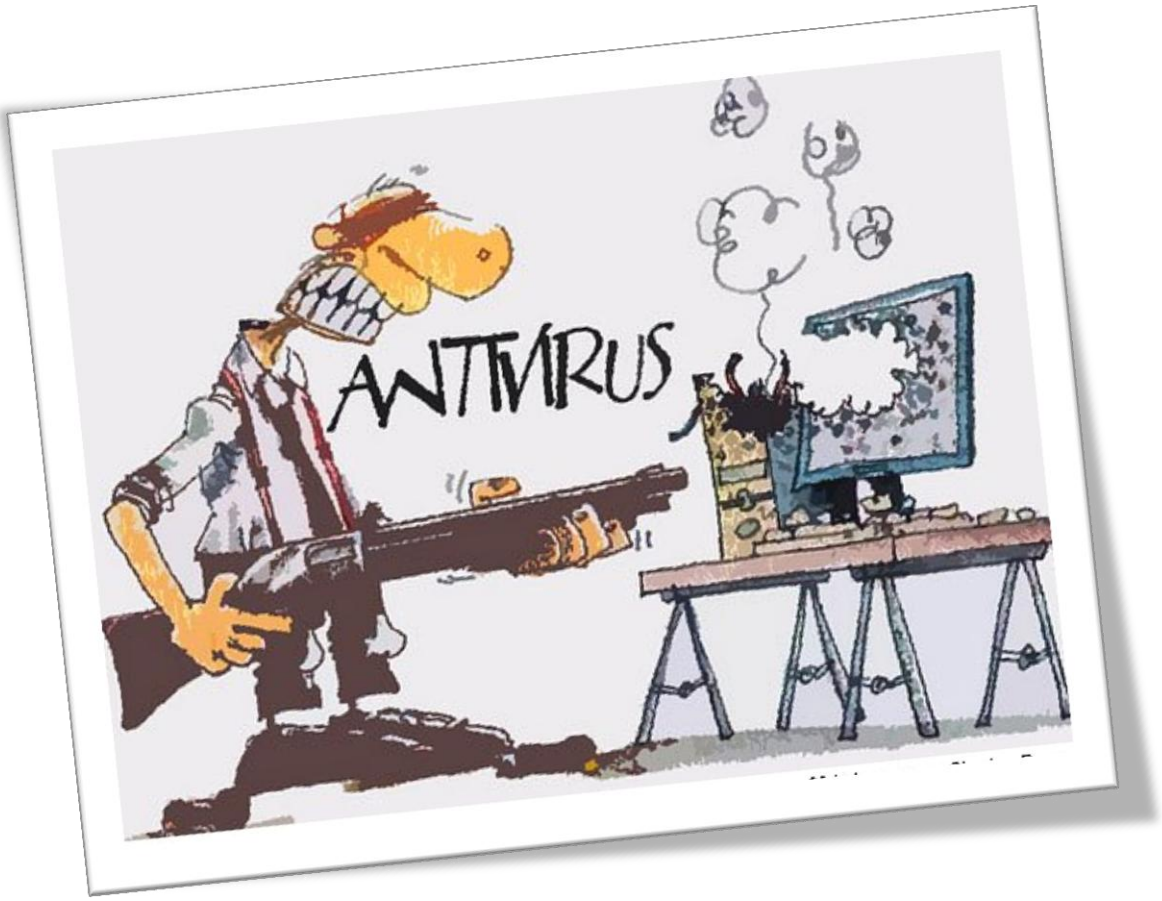
გარდა კომპიუტერების და ლეპტოპების ანტივირუსებისა არსებობს ასევე სხვა მობილური მოწყობილობების დაცვის საშუალებები, სხვადასხვა პლატფორმებისათვის Windows Mobile, Symbian, iOS, BlackBerry, Android რადგან ისინიც აღმოჩნდნენ ვირუსის ინფიცირების რისკის ქვეშ.

ამდაგვრად ანტივირუსების კლასიფიცირება ხდება ოპერაციული სისტემების მიხედვით:

• ანტივირუსული პროგრამები რომლებიც განკუთვნილია Microsoft Windows-ის ოპერაციული სისტემებისათვის.

• ანტივირუსული პროგრამები რომლებიც განკუთვნილია UNIX-ის პლატფომისათვის (ამაში შედის, Linux, Mac OS, BSD და სხვა ოპერაციული სისტემები).

• ანტივირუსული პროგრამები რომლებიც განკუთვნილია მობილური მოწყობილობების პლატფორმებისათვის (Windows Mobile, Symbian, iOS, BlackBerry, Android).


ANTIVIRUS