მავნე პროგრამების სახეობები

პროგრამებს Malware, Spyware და Riskware კატეგორიაში მიიჩნევენ როგორც განსაკუთრებით დიდი საფრთხის გამომწვევად. ამ კატეგორიაში არსებული პროგრამები სხვა საფრთხეებთან ერთად შეიძლება შეიცავდეს ვირუსების, ვორმების (Worm) და ტროიანების (Torjan) სხვადასხვა სახეობებს. ამ საზიანო პროგრამების ეფექტი შესაძლოა მოიცავდეს მომხმარებლის კონფიდენციალური ინფორმაციის მიღებას, კომპიუტერის უკანონო მიზნებისათვის გამოყენებას ან მის მწყობრიდან გამოყვანას.

მალვეარი (Malware)

მალვეარი არის მავნე პროგრამა, რომელიც თავდამსხმელების მიერ გამოიყენება კომპიუტერის ფუნქციონირებისათვის ხელის შესაშლელად და პირად ინფორმაციასთან წვდომის მოსაპოვებლად. ის შეიძლება იყოს კოდი, სქრიფტი ან სხვა პროგრამა. მალვეარი არის ტერმინი, რომელიც გულისხმობს ინტრავირუსულ პროგრამა.

მალვეარი მოიცავს კომპიუტერულ ვირუსებს, რენსომვეარს, ვორმებს, ტროიანებს, რუთკიტებს, კილოგერებს, სპაივეარს, ედვეარს და საზიანიო BHO-ს, აგრეთვე სხვა საზიანო პროგრამებს. მალვეარის ძირითადი საფრთხეები არის ვორმები ან ტროიანები და არა ვირუსები. მალვეარი არ არის იგივე რაც დეფექტიური პროგრამა, რომელიც არის პროგრამა, რომელსაც აქვს ლეგიტიმური მიზანი, მაგრამ შეიცავს საზიანო ბაგებს, რომლებიც არ იქნა შესწორებული ბაზარზე გამოშვებამდე. ზოგიეთრი მალვეარი შეიძლება მოდიოდეს კომპანიის ოფიციალური ვებ გვერდიდან. ამის მაგალითია პროგრამა, რომელსაც კომპანიები იყენებენ მარკეტინგული სტატისტიკის მოსაპოვებლად და მომხმარებელთა კვლევის დროს უსაფრთხო მონაცემებს იღებენ მომხმარებლის კომპიუტერიდან.

მალვეარის არსებობამ საჭირო გახადა ისეთი დამცავი პროგრამების შექმნა, როგორიცაა ანტივირუსები, ანტიმალვეარები და ფაიერვოლი. თითოეული ეს პროგრამა აქტიურად არის გამოყენებული კერძო მომხმარებლების მიერ მათი კომპიუტერების დასაცავად და ნებადაურთავი წვდომისაგან თავის ასარიდებლად.

კომპიუტერული ვირუსი

კომპიუტერული ვირუსი არის კომპიუტერული პროგრამა, რომელსაც აქვს გამრავლების და ერთი კომპიუტერიდან მეორეზე გავრცელების უნარი. ტერმინი

ვირუსი არის ფართოდ გავრცელებული, თუმცა ხშირად იგი არასწორად გამოიყენება და მალვეარს არასწორად უწოდებენ ვირუსს.

მალვეარი მოიცავს კომპიუტერულ ვირუსებს, კომპიუტერულ ვორმებს, რენსომვეარს, ტროიანებს. ისეთი მალვეარი, როგორიცაა ტროიანები და ვორმები ხშირად ეშლებათ და ვირუსებად მოიხსენიებენ. მათ შორის კი ტექნიკური განსხვავებაა: ვორმს შეუძლია გამოიყენოს საფრთხეები და ავტომატურად გამრავლდეს კომპიუტერში და სხვა ქსელში არსებულ კომპიუტერებშიც. ხოლო ტროიანი არის პროგრამა, რომელიც თითქოს უსაფრთხოა, მაგრამ მალავს საზიანო ფუნქციებს. ვორმებსაც და ტროიანებსაც შეუძლიათ ზიანი მიაყენონ კომპიუტერული სისტემის მონაცემებს ან კომპიუტერული სისტემის მუშაობას.

კომპიუტერული ვირუსი არის საზიანო პროგრამა, რომელიც მალულად აღწევს კომპიუტერულ სისტემებში, პროგრამებში ან ფაილებში და შეუძლია თავისი თავის კოპირება და ამგვარად კომპიუტერის დაინფიცირება. ასეთი პროგრამები ხშირად კომპიუტერს რაიმე სახის ზიანს აყენებენ, მათ კომპიუტერის პროგრამულ კოდში საზიანო ცვლილებები შეაქვთ, რომელთა შედეგად ზიანდება კომპიუტერი ან მომხმარებლის მონაცემები.

ადრე ვირუსებს წერდნენ გართობის და ინტერესის მიზნით, მაგრამ დღეს მათ უკვე მიზნობრივი საზიანო ფუნქციები ახასიათებთ, როგორიცაა მაგალითად კომპიუტერის დაზიანება ან მონაცემების მოპარვა, მომხმარებლის კომპიუტერის კონტროლი. ხშირად ტერმინით, კომპიუტერული ვირუსი, ყველა ტიპის მავნე პროგრამებს აღნიშნავენ. არადა ასეთი პროგრამები სხვადასხვა ფუნქციების მატარებელია და შესაბამისად, სხვადასხვა კატეგორიებად იყოფა, რომლებსაც ქვემოთ განვიხილავთ.

კომპიუტერულ სისტემაში ზოგიერთი ვირუსის არსებობა ადვილად შესამჩნევია მომხმარებლისათვის, მაგრამ ბევრი ვირუსი არ აჩენს არანაირ სიმპტომს და მომხმარებელს ეჭვიც არ უჩნდება, რომ კომპიუტერი დავირუსებულია. ზოგიერთი ვირუსი გამრავლების გარდა არაფერს არ აკეთებს.

ვიდრე ვირუსი მოახერხებს კომპიუტერის დააინფიცირებს პირველ რიგში ის უნდა მოხვდეს კომპიუტერში. არსებობს ვირუსის გავრცელების სხვადასხვა საშუალებები:

·მოძრავი მედია საშუალებები - ინფორმაციის მატარებელი მოწყობილობები (კომპაქტ-დისკები CD, USB მოწყობილობები)

·ინტერნეტი - ელექტრონული-ფოსტა, საზიანო კოდის შემცველი ვებ-გვერდები, ინტერნეტიდან გადმოწერილი პროგრამები ან ფაილები, მესენჯერ პრგრამები IM.

·ქსელი - ლოკალურ ქსელში საზიარო ფოლდერები Shared Folder, საზოგადო ქსელები Public Networks.

პიროვნებამ, რომელმაც დაწერა ვირუსი უნდა მოძებნოს გზა კომპიუტერში შემოსაღწევად. მან უნდა მოახერხოს რაიმე საიდუმლო ხერხით შემოუშვას ვირუსი თქვენს სისტემაში ან თქვენ მიგიტყუოთ და მოახერხოს რომ თქვენ თვითონ შეუშვათ ვირუსი თქვენს სისტემაში.

არსებობს მრავალი გზა, რითაც თავდამსხმელს შეუძლია ამის გაკეთება, მაგალითად:

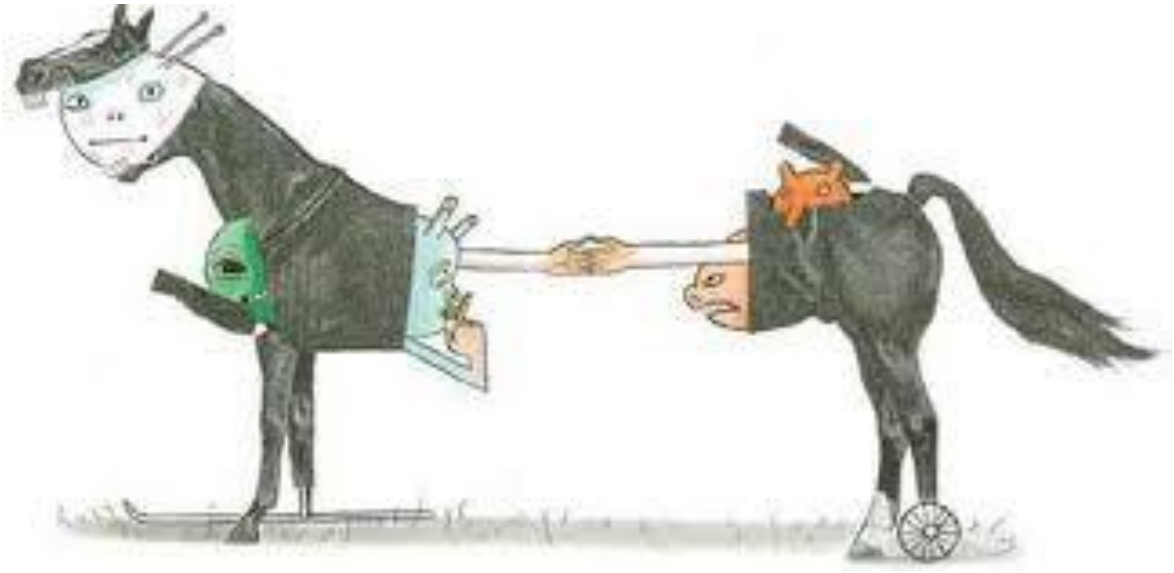
• იპოვნოს დაუცველი კომპიუტერული სისტემა და შემოგიგზავნოთ ვირუსი.

• დაცულ კომპიუტერულ სისტემაში იპოვნოს ხარვეზი (vulnerability) და გამოიყენოს ეს ვირუსის შესაღწევად.

• მოატყუოს მომხმარებელი და დააჯეროს მას, რომ საზიანო ფაილი მისთვის სასურველი ფაილია.

ტროიანი (Trojan Horse)

ტროიან ჰორსი, იგივე ტროიანი არის მალვეარი, რომელსაც აქვს უნარი შეასრულოს სასურველი ფუნქცია და გაამარტივოს მომხმარებლის კომპიუტერულ მონაცემებზე წვდომა. ტროიანის მიზანი არაა სხვა ფაილებში შეღწევა ვირუსის მსგავსად. ტროიან ჰორსებს შეუძლიათ მოიპარონ ინფორმაცია ან ავნონ კომპიუტერულ სისტემას. ტროიანებმა შეიძლება გამოიყენონ დრაივ დაუნლოადები ან დააინსტალირონ თავი ონლაინ თამაშების ან ინტერნეტ აპლიკაციების მეშვეობით იმისათვის, რომ მიაღწიონ სასურველ კომპიუტერამდე.



ტერმინი ტროიან ჰორსი არის წარმოქმნილი ბერძნული მითოლოგიიდან ტროას ცხენის ლეგენდის შესახებ. ტროიანი თავს აჩვენებს მომხმარებელს თითქოს იგი არის სრულიად სანდო და უვნებელი. აგრეთვე, მომხმარებელს რაღაც ფორმით სთავაზობს საჩუქრებს, რათა მსხვერპლს მოტყუებით დააინსტალირებინოს თავი კომპიუტერულ სისტემაში.

Trojan-Spy - ტროიან შპიონი, მომხმარებლის კომპიუტერში მალულად აინსტალირებს პროგრამებს ისეთებს, როგორიცაა მაგალითად keyloggers, რის საშუალებითაც მესამე პირს შეუძლია მომხმარებლის მიერ კლავიატურაზე აკრეფილი ინფორმაცია წაიკითხოს.

Trojan-PSW- იპარავს პაროლებს და სხვა მნიშვნელოვან ინფორმაციას. მას აგრეთვე შეუძლია სხვა საზიანო პროგრამების დაყენებაც.

Trojan-Downloader -ინტენეტის საშუალებით ფარულად იწერს საზიანო ფაილებს მოშორებული სერვერიდან და შემდგომ ავტომატურად აინსტალირებს მომხმარებლის კომპიუტერზე.

Trojan-Dropper - შეიცავს ერთ ან რამდენიმე საზიანო პროგრამას, რომელსაც ის ფარულად აინსტალირებს და გამოიყენებს მომხმარებლის კომპიუტერზე.

Trojan-Proxy - საშუალებას აძლევს მომხმარებლის კომპიუტერის მეშვეობით არავტორიზებულმა პირებმა ანონიმურად ისარგებლონ ინტერნეტით.

Trojan-Dialer - მომხმარებლის კომპიუტერს სატელეფონო ხაზის მეშვეობით აკავშირებს ინტერნეტ ქსელთან. მას აგრეთვე შეუძლია მომხმარებელი გადაამისამართოს არასასურველ ვებ გვერდებზე.

რუთკიტი (Rootkit)

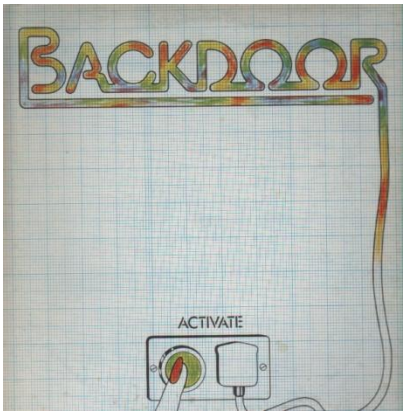
რუთკიტი არის პროგრამა რომელიც ცდილობს თავისი არსებობის დამალვას კომპიუტერის უსაფრთხოების პროგრამებისგან თავის აცილებით. კომპიუტერში შეღწევის შემდეგ საშუალებას აძლევს დისტანციურ მომხმარებელს საიდუმლოდ აკონტროლოს კომპიუტერის ოპერაციული სიტემა.

რუთკიტის აღმოჩენა არის საკმაოდ რთული, რადგან მას აქვს უნარი გაუმკლავდეს იმ პროგრამას, რომელიც მის აღმოსაჩენად უნდა იქნას გამოყენებული.

კომპიუტერული სისტემის რუთკიტისგან გაწმენდა საკმაოდ რთული საქმეა, ხშირად საჭირო ხდება ხელახალი ინსტალაცია, ვინაიდან მხოლოდ ამ გზით ხდება შესაძლებელი მისგან თავის დაღწევა.

ბექდორი (Backdoor)

ბექდორი არის ჯაშუშური პროგრამა რომელიც გამოიყენება არა მხოლოდ ინფორმაციის მიტაცებისთვის, არამედ კომპიუტერის უკანონოდ სამართავადაც. აქვს ცალკე არსებული ადმინისტრაციული შესაძლებლობა, რომელიც თავს არიდებს სტანდარტულ უსაფრთხოების მექანიზმებს კომპიუტერული პროგრამების, კომპიუტერის ან ქსელის მალულად სამართავად.



ვორმი (Worm)

კომპიუტერული ჭია არის საზიანო პროგრამა, რომელიც იყენებს კომპიუტერს და ქსელის შესაძლებლობებს, რათა ავტომატურად გავრცელდეს სხვა კომპიუტერებზე. ვირუსისგან განსხვავებით ის არ საჭიროებს, კომპიუტერში არსებულ რომელიმე პროგრამაზე იყოს დამოკიდებული. კომპიუტერული ჭია თითქმის ყოველთვის იწვევს მინიმალურ ზიანს ქსელში, თუნდაც შეუძლია მოიხმაროს მომხმარებლის ინტერნეტ სიჩქარე, ხოლო ვირუსები თითქმის ყოველთვის აზიანებს ან ცვლის ფაილებს და მონაცემებს კომპიუტერში.

ქსელური-ჭია (Net-Worm) - მრავლდება თავისი თავის სრულიად დამოუკიდებელი კოპიების ქსელში გავრცელებით.

P2P-ჭია (P2P-Worm) - ვრცელდება P2P პროგრამების და ქსელის (Emule, KaZaa, Imesh, Torrent) მეშვეობით, ძირითადად მაცდუნებელი ფაილის სახით.

ელ-ფოსტის ჭია (Email-Worm) - ვრცელდება ელექტრონული ფოსტის საშუალებით, ძირითადად მიბმული ფაილის (attachment) სახით.

IRC-ჭია (IRC-Worm) - ვრცელდება ინტერნეტ ჩატის ქსელის მეშვეობით.

IM-ჭია (IM-Worm) - ვრცელდება სწრაფი შეტყობინებების პროგრამების და ქსელის (IM, ICQ, Skype, Yahoo და MSN Messenger) მეშვეობით.

Bluetooth-ჭია (Bluetooth-Worm) ვრცელდება ბლუთუსის მოწყობილობების მეშვეობით.

ინტერნეტ ბრაუზერები, რომლებიც იყენებიან მავნე პროგრამის არსებობას - ძალიან მნიშვნელოვანი მიმართულებაა, როდესაც თქვენი ბრაუზერი ამოწმებს ვებ-გვერდის საწყის კოდს და გატყობინებთ ვებ-გვერდი დაინფიცირებულია თუ არა. ამ ფუნქციას იყენებენ ისეთი ინტერნეტ ბრაუზერები როგორიცაა: Internet Explorer, Mozilla Firefox, Google Chrome, Safari და Opera.

შეტყობინება რომელიც გამოდის, როდესაც თქვენი ინტერნეტ ბრაუზერი აღმოაჩენს, რომ ვებ-გვერდი შეიცავს მავნე კოდს.