არასანქცირებული მონიტორინგი

ვინაიდან ინტერნეტი, ისევე როგორც მობილური და რადიო კავშირგაბმულობა სხვადასხვა ტექნიკური საშუალებებით იმართება, შესაძლებელია ინტერნეტ აქტივობის მონიტორინგი, ჩაწერა, გაანალიზება, როგორც საჭირო და აუცილებელი, ასევე არასასურველი ბოროტი მიზნებით.

იმისათვის რომ ინტერნეტ მომხმარებლის კომუნიკაცია და აქტივობა მაქსიმალურად პრივატული იყოს, საჭიროა ინტერნეტ მომხმარებელმა დაიცვას ინტერნეტ უსაფრთხოების ნორმები, წესები და შეძლებისდაგვარად გამოიყენოს უსაფრთხო კავშირის საშუალებები და ინტერნეტ გადაწყვეტილებები.

კიბერ-კრიმინალები ყოველდღურად ქმნიან მავნე პროგრამებს. არსებობს ისეთი პროგრამების ტიპი, რომელთა ძირითადი დანიშნულება და ფუნქციაა, დაინფიცირებული კომპიუტერული სისტემის სრული მართვა და მონიტორინგი. კომპიუტერზე განხორციელებეული ნებისმიერი ქმედება (აკრეფილი ტექსტი, პაროლები, მონახულებული საიტები, ფოტოები, ვიდეოკავშირი, მიმოწერა, ელ-ფოსტა) შესაძლებელია გადაეგზავნოს მავნე ვირუსული კოდის ავტორს, ისე რომ კომპიუტერის მფლობელმა ამის შესახებ არაფერი იცოდეს.

ასეთი პროგრამები როგორც წესი მაღალი დონის კომპიუტერული სპეციალისტების მიერ იქმნება და მათგან თავდაცვა და დაინფიცირების აღმოჩენა საკმაოდ რთულია. თუმცა არსებობს გარკვეული მითითებები და რჩევები რომელთა გათვალისწინების შემთხვევაშიც საგრძნობლად მცირდება დაინფიცირების და არასანქცირებული მონიტორინგის რისკი.

ამ ტიპის მავნე პროგრამები სხვადასხვანაირად ხვდება სამიზნე კომპიუტერში:

- თუ კიბერდამნაშავეს ფიზიკური წვდომა აქვს კომპიუტერთან, მაშინ საქმე გაცილებით მარტივადაა. ფლეშ მოწყობილობიდან ან ინტერნეტიდან 1-2 წუთის განმავლობაშიც კი შესაძლებელია სამიზნე კომპიუტერის დაინფიცირება.

- ასევე ხშირად ელექტრონულ ფოსტაზე მიმაგრებულია საინტერესო შინაარსის ფაილები ან ლინკები. მათი მონახულებისას სისტემა ავტომატურად ინფიცირდება.

ასეთი პროგრამები როგორც წესი, მომხმარებლისგან ფარულ რეჟიმში მუშაობს, რთულია როგორც მათი აღმოჩენა, ასევე კომპიუტერიდან წაშლა. ზოგიერთი მათგანი ხისტი დისკის სრულად წაშლის ან გამოცვლის შემთხვევაშიც კი აგრძელებს მოქმედებას.

ხშირად კომპიუტერული პროგრამის ნაცვლად მონიტორინგის ფუნქციას ასრულებს, კომპიუტერის პერიფერიული ნაწილი. შექმნილია კლავიატურაში, მაუსში, სხვადასხვა ტიპის შნურებში ჩამონტაჟებული მავნე მოწყობილობები. შედეგად კომპიუტერზე განხორციელებული ნებისმიერი ქმედება თუ ინტერნეტ აქტივობა გადაეცემა კიბერკრიმინალს.

როგორ აღმოვაჩინოთ ფარული მონიტორინგის პროგრამა საკუთარ კომპიუტერში?

შემდეგი სიმპტომები ხშირად ასეთი სახის პროგრამებით დაინფიცირებაზე მიუთითებს:

- ვებ სერფინგის დროს განუწყვეტელი Pop-up სარეკლამო გვერდების გახსნა ერთსა და იმავე თემაზე.
- აკრეფილი ვებ გვერდების ნაცვლად სხვა ვებ გვერდებზე გადაყვანის გახშირება.
- ბრაუზერის ფანჯარაში გაჩენილი ახალი ჩანართები და „დამხმარე“ მოდულები.
- ეკრანის ქვედა მარჯვენა კუთხეში ე.წ. Taskbar-ში უცხო, ახალი Icon-ების შემჩნევა.
- ბრაუზერში არ მუშაობს ზოგიერთი კლავიში.
- სხვადასხვა Windows Error Message, კომპიუტერის გაცილებით ნელა მუშაობა, პროგრამების გახსნის ან ფაილების შენახვისას ხშირი ე.წ. «გაჭედვები“, ჩართვის ან გამორთვის განსაკუთრებით გაჭიანურება.

ზემოთ ჩამოთვლილი ნიშნები შეიძლება სხვადასხვა ლეგიტიმურმა პროგრამებმაც განსხვავებული მიზეზებით გამოიწვიოს, თუმცა რამდენიმე მათგანის ერთდროულად გამოვლენა უკვე საეჭვოა და საჭიროა Antivirus, Antispyware ტიპის ხელსაწყოებით კომპიუტერის შემოწმება.

როგორ დავიცვათ თავი ფარული მონიტორინგის ხელსაწყოებისგან?

- სასურველია არ გავხსნათ Pop-up სარეკლამო გვერდებზე არსებული საეჭვო შემოთავაზებები და Link-ები

- თავი შეიკავეთ უფასო პროგრამების გადმოწერისგან საეჭვო რეპუტაციის საიტებიდან. ხშირად ასეთ არალიცენზირებულ, მცდარი გზით მოპოვებულ პროგრამებში ჩაშენებულია დამაინფიცირებელი მონიტორინგის ხელსაწყოები.

- ხშირად განაახლეთ Antivirus, Antispyware, Firewall. ასევე შედეგის მომტანია სხვადასხვა ანტივირუსის გამოყენება, ვინაიდან ხშირად ზოგეირთი ანტივირუსული პროდუქტი ვერ უმკლავდება მავნე პროგრამას, მაშინ როდესაც სხვა კომპანიის პროდუქტი უკვე შლის აღნიშნულ ვირუსს.

- იმ შემთხვევაში თუ მაინც არსებობს ეჭვი მონიტორინგის პროგრამის არსებობაზე, უმჯობესია საქმე მიანდოთ კოპმიუტერის „ექსპერტ“ Forensic სპეციალისტს.

ქსელური მონიტორინგი

არასანქცირებული მონიტორინგის ერთ-ერთი გზაა ქსელური მონიტორინგი. ამ შემთხვევაში კოპმიუტერული სისტემა აბსოლუტურად ხელუხლებელია. მომხმარებლისთვის განსაკუთრებით რთულია ასეთი ტიპის მონიტორინგის აღმოჩნა, ვინაიდან ინტერნეტ აქტივობის მონიტორინგი, ჩაწერა და მიყურადება ხორციელდება არა კოპმიუტერზე არამედ უშუალოდ - ქსელური მოწყობილობიდან ინტერნეტ სერვის პროვაიდერამდე. აღნიშნული ტექნიკა გამოიყენება მრავალი

ქვეყნის ოფიციალური სამართალდამცავი სტრუქტურების მიერ, თუმცა კიბერდამნაშავეები ხშირად მიმართავენ აღნიშნულ სქემას, განსაკუთრებით მაშინ თუ ინტერნეტ მომხმარებელი იყენებს Wireless, უსადენო კავშირის საშუალებებს.

ამ შემთხვევებშიც აუცილებელია უსაფრთხოების ზომების დაცვა. რთული პაროლის დაყენება, უცხო მაგრამ ხელმისაწვდომი უფასო ინტერნეტ ქსელების სიფრთხილით გამოყენება. ღია ტიპის ინტერნეტ ქსელებში ჩართვისას (ინტერნეტ კაფე, სკვერი, კინოთეატრი, ორგანიზაცია) სასურველია არ გამოიყენოთ ინტერნეტ კომერცია, საბანკო გადარიცხვები, სხვა სენსიტიური ინტერნეტ აქტივობა.

მობილური მოწყობილობები

მონიტორინგის საფრთხე არამარტო კომპიუტერულ სისტემებს, არამედ უკვე მობილურ მოწყობილობებსაც ემუქრება. არსებობს სპეციალური პროგრამები რომლებიც ფარულად ინსტალირდება მობილურებში, ტაბლეტებში და შემდგომ ნებისმიერ განხორციელებულ ზარს, მესიჯს, გახსნილ ინტერნეტ გვერდს, ფოტოს და ა.შ გადასცემს წინასწარ მითითებულ ტელეფონის ნომერზე ან ელ-ფოსტის მისამართზე. ზოგიერთ ასეთი ტიპის პროგრამას აქვს დისტანციურად მიკროფონის ჩართვის და გარშემო საუბრის მოსმენის ფუნქცია.

სხვა ტიპის მობილური ვირუსები სპეციალურ ფასიან ნომრებზე აგზავნიან მოკლე ტექსტურ შეტყობინებებს, ფინანსური სარგებლის მიღების მიზნით. ამიტომ აუცილებელია ანტივირუსული და AntiSpyware პროგრამების გამოყენება მობილურ მოწყობილობებზე.

ბოლო პერიოდში განსაკუთრებით პოპულარულია მონიტორინგის პროგრამების გავრცელება სოციალური ქსელებით. დარეგისტრირებულ მომხმარებლებს საკუთარი მეგობრებისგან ავტომატურად ეგზავნებათ რაიმე აქტუალური საინტერესო ვიდეოს ან ფოტოს ლინკი.

მექანიზმი: ბრაუზერში გამოდის შეტყობინება, რომ რომელიმე ფოტო/ვიდოეს სანახავად აუცილებელია სხვადასხვა ტიპის პატარა ზომის პროგრამის გადმოწერა. განსაკუთრებული სიფრთხილეა საჭირო ასეთ შემთხვევებში, ვინაიდან რეალურად ასეთი გზით გადმოწერილი პროგრამების 99% მავნე ვირუსული პროგრამაა და კომპიუტერის დაინფიცირების, მართვის და შემდგომი მონიტორინგის ფუნქცია

აკისრია. ზოგიერთი ასეთ პროგრამა შეიძლება უფასო ანტივირუსის სახითაც შეინიღბოს.

Facebook, Twitter, Google+ მონაცემების მიხედვით ასეთი მავნე ლინკების და შეცდომაში შემყვანი საიტების რაოდენობა ზოგჯერ დღეში 10,000-ს აჭარბებს.