USB ფლეშ მოწყობილობები

USB მეხსიერების მოწყობილობა პატარა ზომის, ხელმისაწვდომი, იაფი, პორტაბელური და კომფორტული საშუალებაა, ფაილების დასამახსოვრებლად და ერთი კომპიუტერიდან სხვადასხვა კომპიუტერებზე გადასატანად. მაგრამ, ამასთანავე იგივე მახასიათებლები USB მეხსიერების მოწყობილობებს კიბერსაფრთხეების გავრცელების ერთ-ერთ მნიშვნელოვან ვექტორად აქცევს.

შექმნილია ისეთი ვირუსული ფაილები, რომლებიც აინფიცირებენ კომპიუტერს და ამ კომპიუტერზე ნებისმიერი USB ფლეშ მოწყობილობის შეერთებისას, ავტომატურად გადაიწერებიან მათზე. შედეგად ახლადდაინფიცირებული USB მოწყობილობებიდან ვირუსები ვრცელდება სხვადასხვა კომპიუტერებზე.

ასევე, თუ პიროვნებას ფიზიკური წვდომა აქვს კომპიუტერთან, მას შეუძლია სპეციალურად მომზადებული პროგრამული უზრუნველყოფა დააყენოს USB ფლეშ მეხსიერებაზე და კომპიუტერში შეერთებისას ავტომატურად მოხდება სასურველი ინფორმაციის მოძიება და კომპიუტერიდან ფარულად ფლეშ მეხსიერებაზე გადაწერა.

USB მოწყობილობებს ხშირად იყენებენ სარეზერვო ასლების დასამახსოვრებლად და საჭირო აქტუალური ინფორმაციის გადასატანად, თუმცა მათი ზომებიდან და პორტაბელურობიდან გამომდინარე, ხშირია მოწყობილობების დაკარგვის შემთხვევები. თუ ინფორმაცია არ არის სათანადო პაროლით დაცული და მთლიანად დაშიფრული, პრივატული მონაცემები სხვა ადამიანის ხელში აღმოჩნდება.

აღწერილია შემთხვევები როდესაც დაკარგულ ფლეშ მეხსიერებებზე განთავსებული იყო კონფიდენციალური და ორგანიზაციებისთვის მეტად სენსიტიური ინფორმაცია.

USB ფლეშ მეხსიერებების გამოყენებით მოხდა რამდენიმე სერიოზული კიბერშპიონაჟის შემთხვევა, ასევე სავარაუდოდ, ირანის ბირთვული ობიექტების

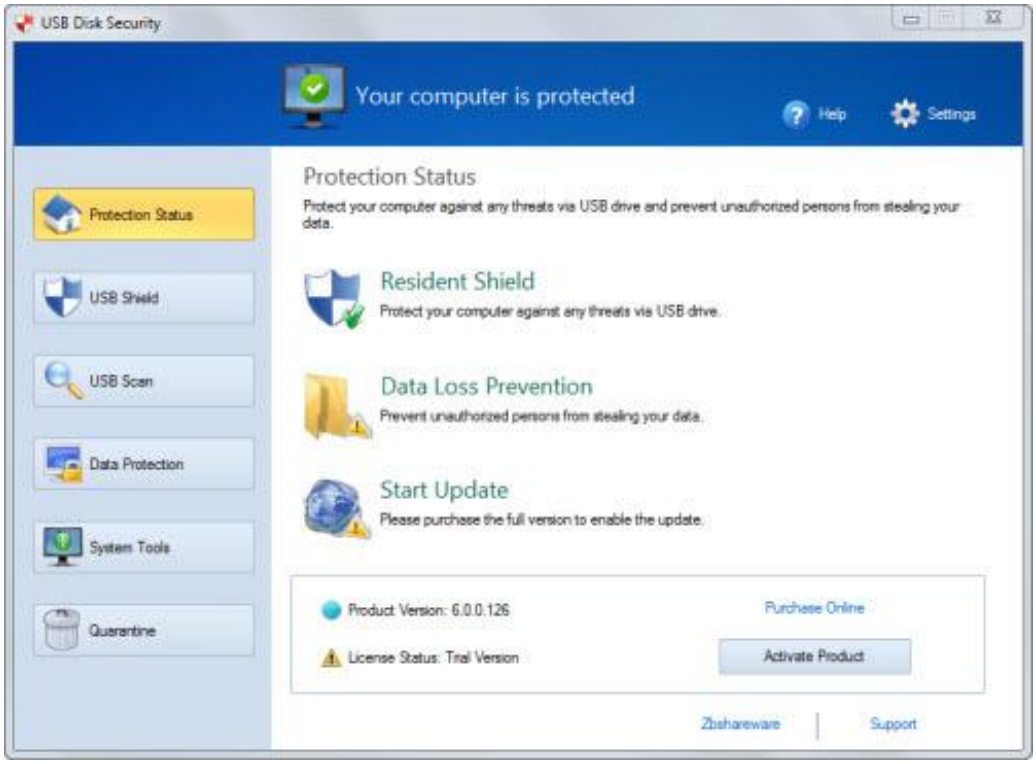
სამართავი კომპიუტერები დაზიანდა ფლეშ მეხსიერებით გადატანილი ვირუსული ფაილებით.

როგორ დავიცვათ თავი?

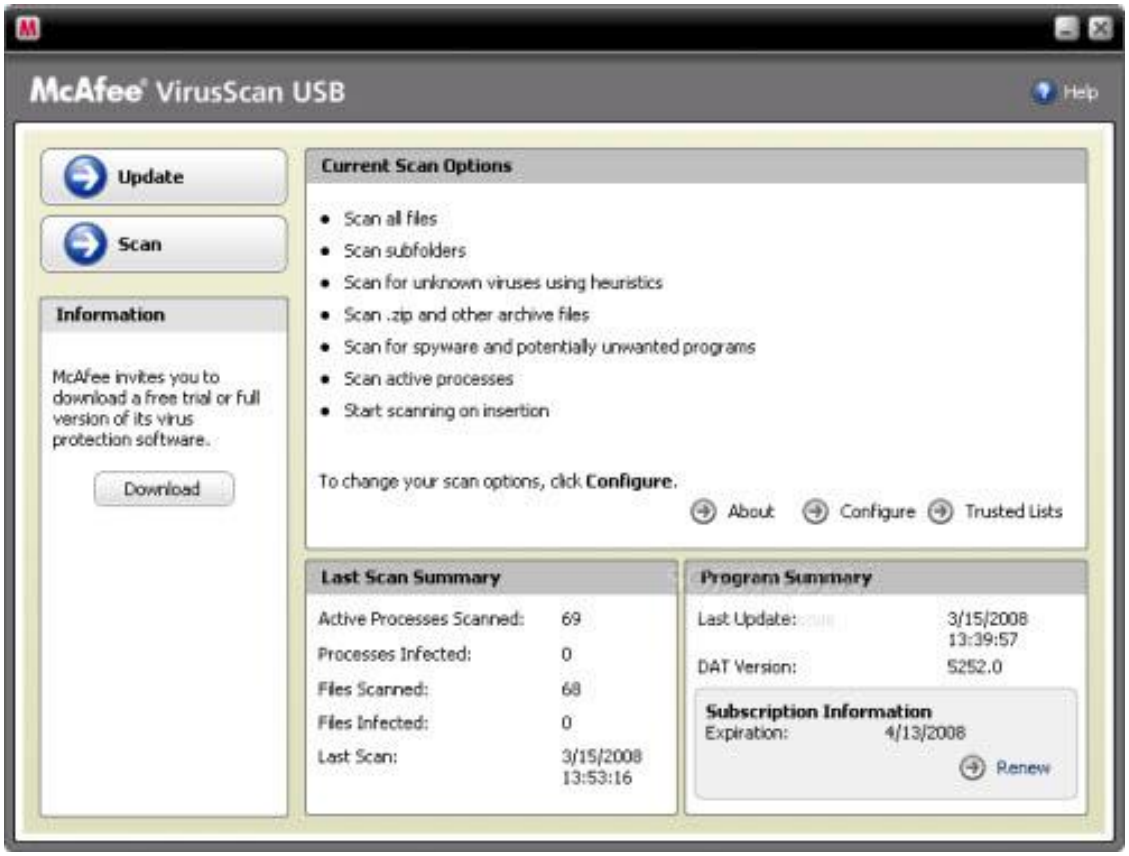
არსებობს რამდენიმე რჩევა, რომელთა გათვალისწინებით საგრძნობლად შეიძლება USB ფლეშ მეხსიერებებით განპირობებული რისკების შემცირება.

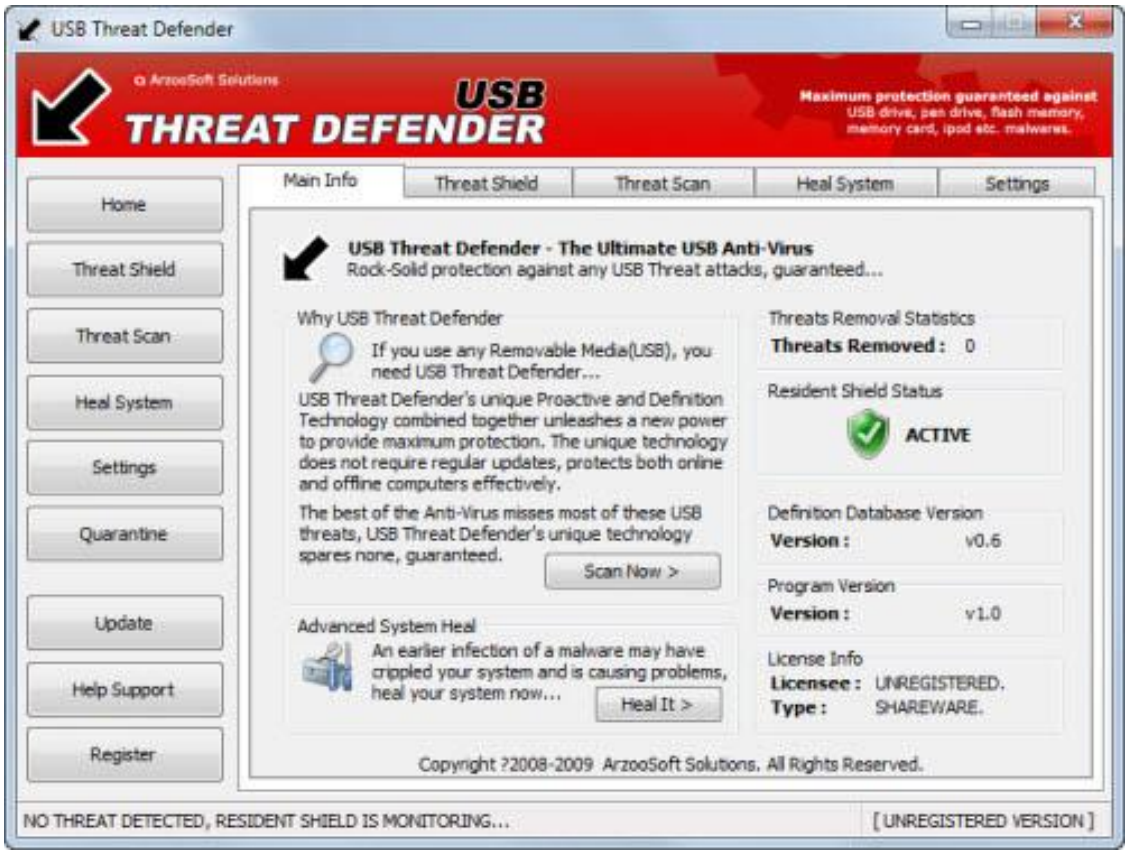
- გამოიყენეთ USB ფლეშ მეხსიერებისთვის განკუთვნილი სპეციალური უსაფრთხოების პროგრამები. (დისკის დაშიფრვა, პაროლის დაყენება). არსებობს მრავალი უფასო პროგრამული პროდუქტი აღნიშნული მოქმედებების ჩასატარებლად. მაგ:

- Autorun ფუნქციის გათიშვა, როგორც USB მეხსიერებებზე ასევე კომპიუტერის ოპერაციულ სისტემაში.(იმისათვის, რომ ფლეშ მეხსიერების კომპიუტერში შეერთებისას ავტომატურად არ მოხდეს ვირუსული ფაილის გაშვება და ინფიცირება). Panda USB Vaccine, USB Disk Security და ა.შ.



- ანტივირუსული პროდუქტების გამოყენება და მათი მუდმივი განახლება უახლესი ვერსიების და დაცვის მექანიზმების მისაღებად. Antivirus, Antispyware, Firewall, Windows Update და ა.შ.





- არ შეაერთოთ USB მოწყობილობები უცხო და ნაკლებად სანდო კომპიუტერებში. აუცილებლობის შემთხვევაში, სასურველია ფლეშ მეხსიერების რეგულარული შემოწმება ანტივირუსული პროდუქტებით.

- პერსონალური და ბიზნეს-კორპორატიული მიზნებით სხვადასხვა მოწყობილობების გამოყენება.

- ასევე მნიშვნელოვანია, ფლეშ მეხსიერებაზე არსებული ინფორმაციის სარეზერვო ასლების შექმნა.