პროცესების ანალიზი

რა არის პროცესი?

კომპიუტერულ სისტემაში არსებული ნებისმიერი პროგრამა ჩართვისას გარდაიქმნება პროცესებად. შესაბამისად კომპიუტერის მომხმარებელს შეუძლია ყოველთვის შეამოწმოს რა პროცესები ანუ პროგრამებია გაშვებული მის კომპიუტერში.

ასევე მნიშვნელოვანია, რომ ზოგიერთ პროგრამას აქვს ავტომატურად გაშვების შესაძლებლობა, ოპერაციული სისტემის ყოველი ჩატვირთვისას.

ამ ფუნქციებს თითქმის ყოველთვის იყენებენ მავნე კოდის ვირუსული ფაილები. ზოგიერთი მათგანი ქმნის იშვიათი სახელის მქონე პროცესებს, ასევე ამატებს საკუთარ პროცესს კომპიუტერის ავტომატური გაშვების ციკლში. შედეგად ყოველი რესტარტის ან კომპიუტერის ჩართვისას მავნე კოდი ახლიდან ჩაირთვება და განახორციელებს დამაინფიცირებელ მავნე ზემოქმედებას.

ავტომატურად გაშვებადი პროგრამები ანალიზი

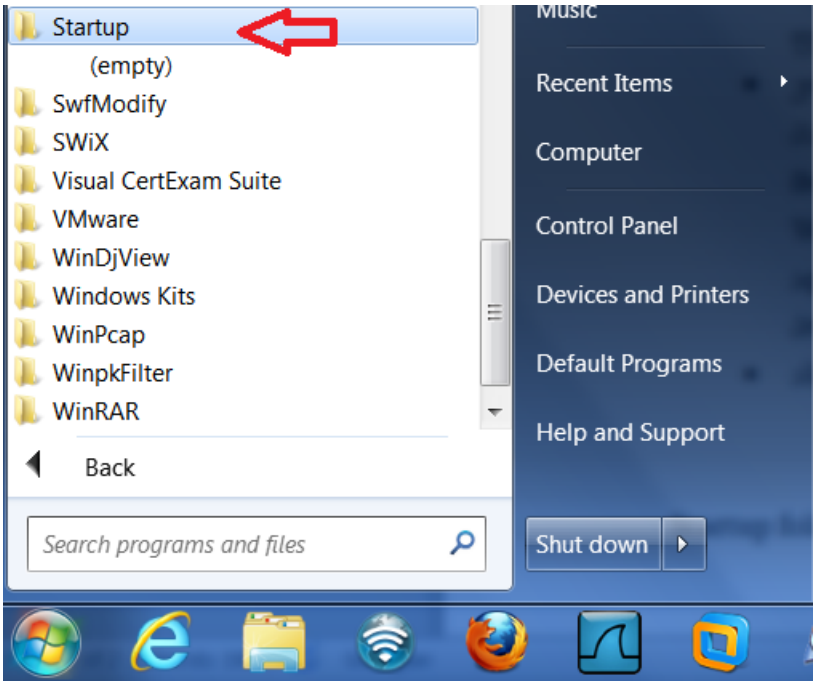
განვიხილოთ რამდენიმე გზა, თუ როგორ უნდა შევამოწმოთ რა პროგრამები ეშვება ჩვენი კომპიუტერის ყოველი ჩართვისას.

- პირველ რიგში, არსებობს რამდენიმე აუცილებელი პროგრამა, რომელიც ერთი და იგივე ტიპის ოპერაციულ სისტემაში ყოველი ჩართვისას ინიცირდება და გაეშვება, ეს პროგრამები აუცილებელია სისტემის ნორმალური ფუნქციონირებისათვის.

- კონკრეტული პროგრამის პარამეტრები. მრავალ პროგრამას გააჩნია პარამეტრების და კონფიგურაციის შეცვლის განყოფილება.

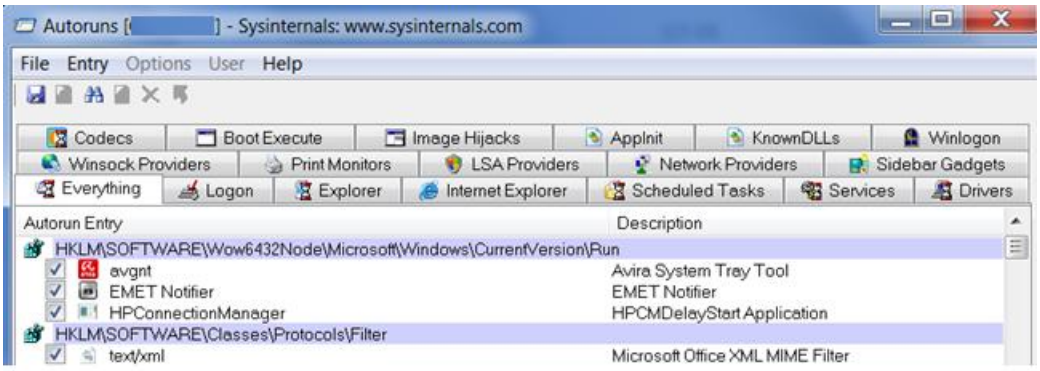
სწორედ აქ შეიძლება მოვნახოთ მსგავსი შინაარსის ჩანაწერი მაგ: “Start on Startup, Autorun, Run when Windows Starts, Autostart” და ა.შ. შესაბამისი ველის გამორთვისას პროგრამა აღარ გაეშვება ავტომატურად ყოველი ჩართვისას. ეს ეხება ლეგალურ პროგრამულ უზრუნველყოფებს.

- ასევე მსგავსი სახით პროგრამები განთავსდება Startup საქაღალდეში:

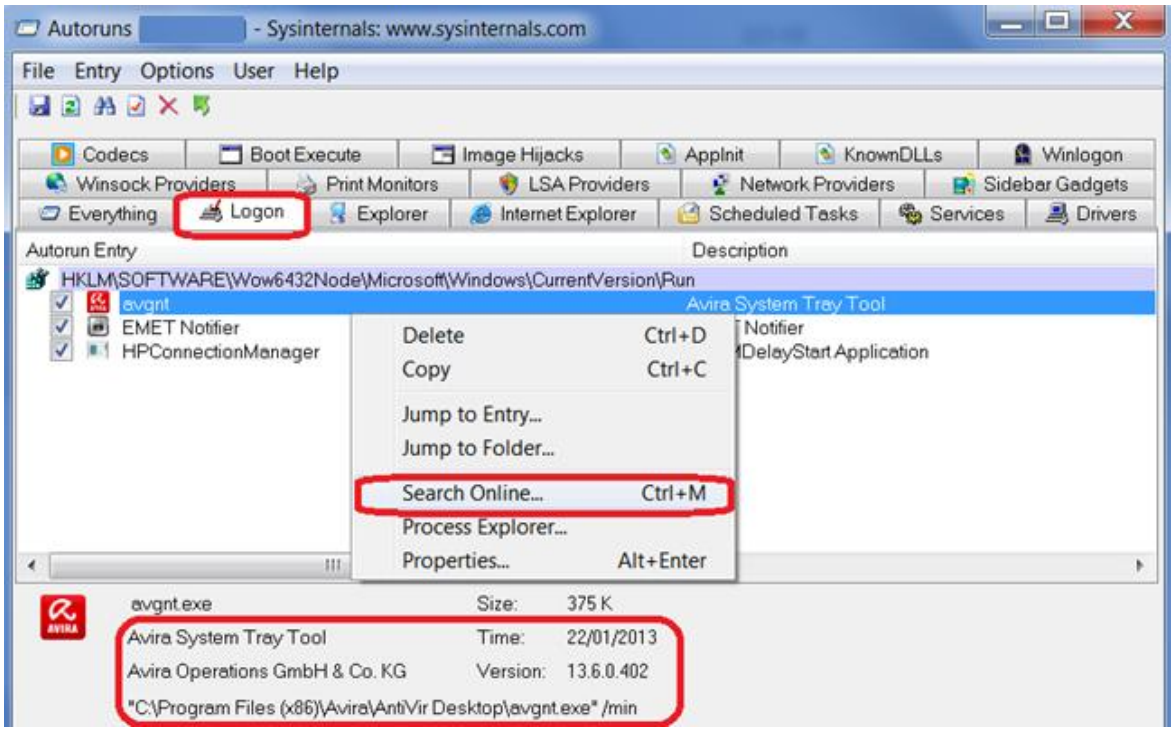


ამ საქაღალდეში არსებული ნებისმიერი პროგრამა ავტომატურად გაეშვება სისტემის ჩართვისას.

- თუმცა მავნე პროგრამების უმრავლესობა იყენებს შედარებით რთულ გზას საკუთარი პროგრამის ავტომატური გაშვების დასამალად. იმისათვის, რომ ვიპოვოთ ავტომატურად გაშვებადი პროგრამების უმრავლესობა, შესაძლებელია გამოვიყენოთ უფასო და საკმაოდ მრავალფუნქციური უტილიტა Sysinternals Autoruns. მისი მოძიება შესაძლებელია www.microsoft.com -ზე.



ამ შემთხვევაში საინტერესოა პროგრამის Logon განყოფილება:

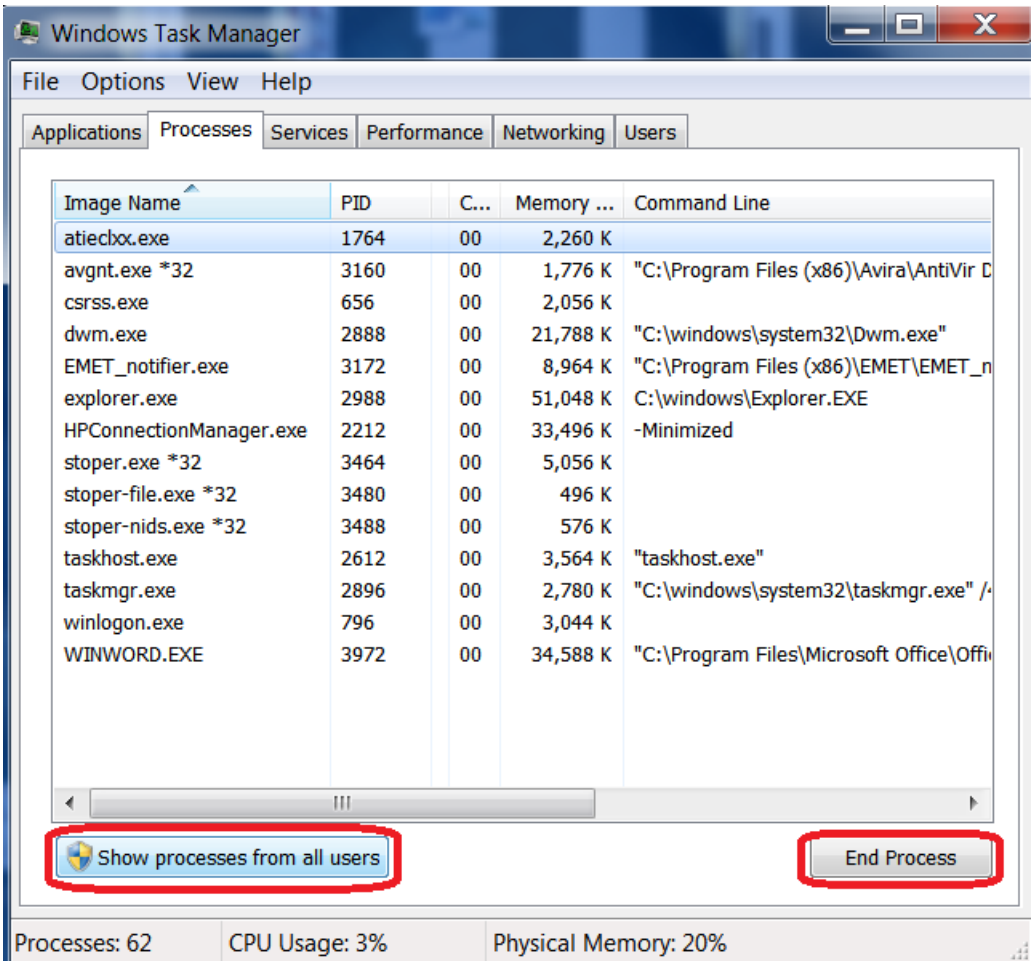


Logon განყოფილებაში გამოჩნდება იმ პროგრამების ჩამონათვალი რომლებიც ავტომატურად გაეშვება სისტემის ჩართვისას. საეჭვო დასახელების აღმოჩენის შემთხვევაში შესაძლებელია ონლაინ ძიების ფუნქციის გამოყენება, რაც უფრო მეტ ინფორმაციას მოგვცემს პროგრამის მავნეობასთან დაკავშირებით. ასევე ნებისმიერ მონიშნულ პროგრამას მიეთითება მისი მწარმოებელი კომპანიის ან პროდუქტის სახელი.

გაშვებული პროგრამები/პროცესები

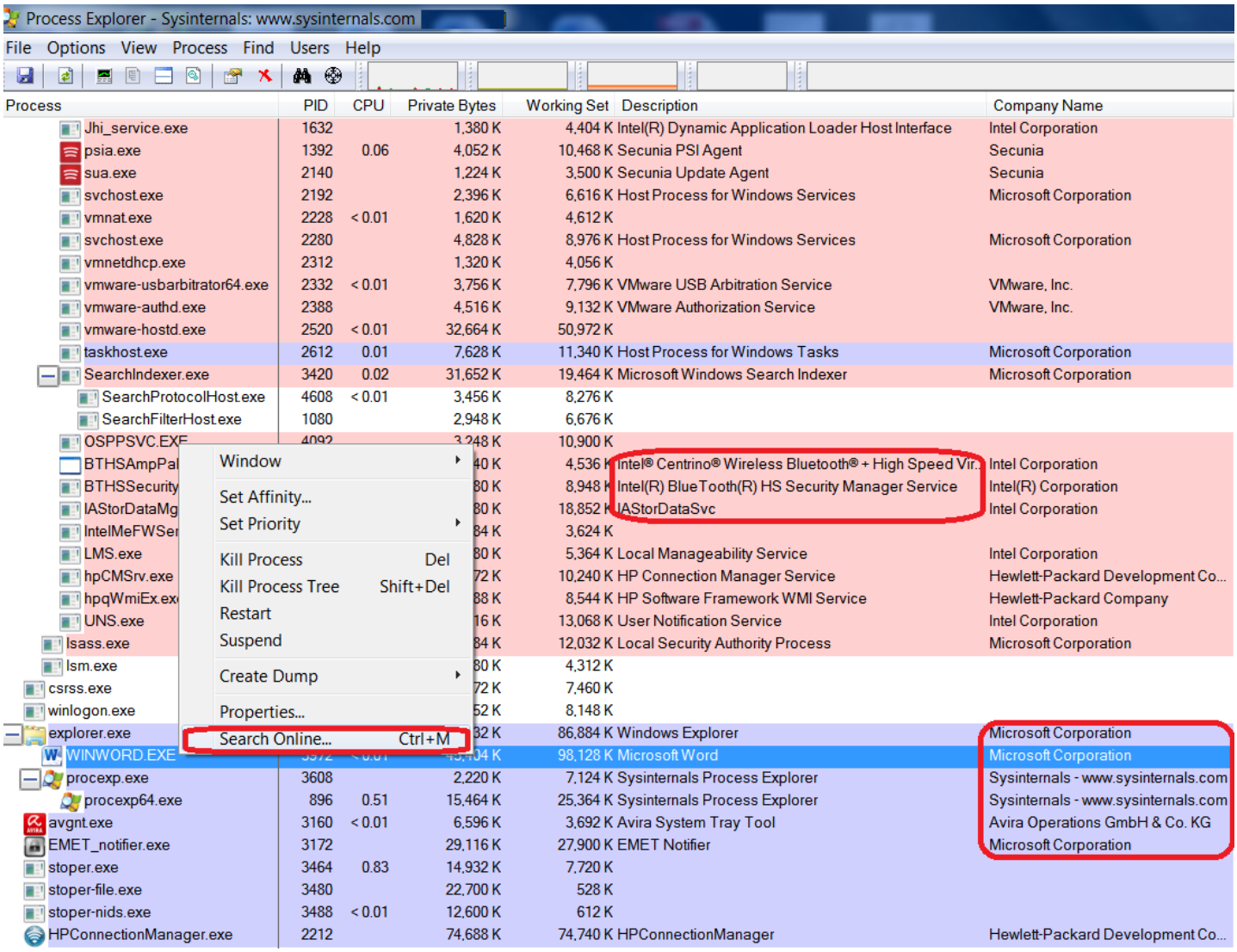
იმისათვის რომ ვნახოთ სისტემაში დროის კონკრეტულ მონაკვეთში გაშვებული პროცესები შესაძლებელია გამოვიყენოთ როგორც სტანდარტული Windows ხელსაწყო (მოყვება ნებისმიერ Windows სისტემას) , ასევე ალტერნატიული და უფრო მრავალფუნქციური საშუალება.

Task manager - გვიჩვენებს გაშებულ პროცესებს, მისი ჩართვა შესაძლებელია კლავიატურაზე Ctrl-Alt-Del კომბინაციის გამოყენებით. ასევე Taskbar-ზე მაუსის მარჯვენა ღილაკის დაწკაპუნებით და Start Task Manager ბრძანების არჩევით.



ამ ფანჯარაში შესაძლებელია სასურველი პროცესის მონიშვნა და End Process ღილაკით მისი შეჩერება. თუმცა გაშვებულ პროცესზე მეტი ინფორმაციის მოსაძიებლად უმჯობესია გამოვიყენოთ ხელსაწყო Process Explorer, Sysinternals-ის ხელსაწყოთა პაკეტიდან. მისი გადმოწერა შესაძლებელია www.microsoft.com -იდან.

პროგრამის ფანჯარა შემდეგნაირად გამოიყურება:



ნებისმიერი პროცესის მონიშვნისას შესაძლებელია სამი ძირითადი ქმედების განხორციელება.

1) ინფორმაციის შემოწმება პროგრამის მწარმოებელი კომპანიის ან ორგანიზაციის შესახებ. Microsoft Corporation, Vmware, Inc. Hewlett-Packard და ა.შ.

2) საკუთრივ პროცესის აღწერილობა: Microsoft Word, Local Manageability Service, Intel Bluetooth Service, Windows Explorer და ა.შ.

3) ნებისმიერი პროცესის დასახელების შემოწმება შესაძლებელია ონლაინ ძიების ფუნქციით, შესაბამისად გაირკვევა არის თუ არა საეჭვო პროცესი ცნობილი რომელიმე ანტივირუსული პროდუქტისთვის ან ზოგადად რა ფუნქცია აკისრია მას.