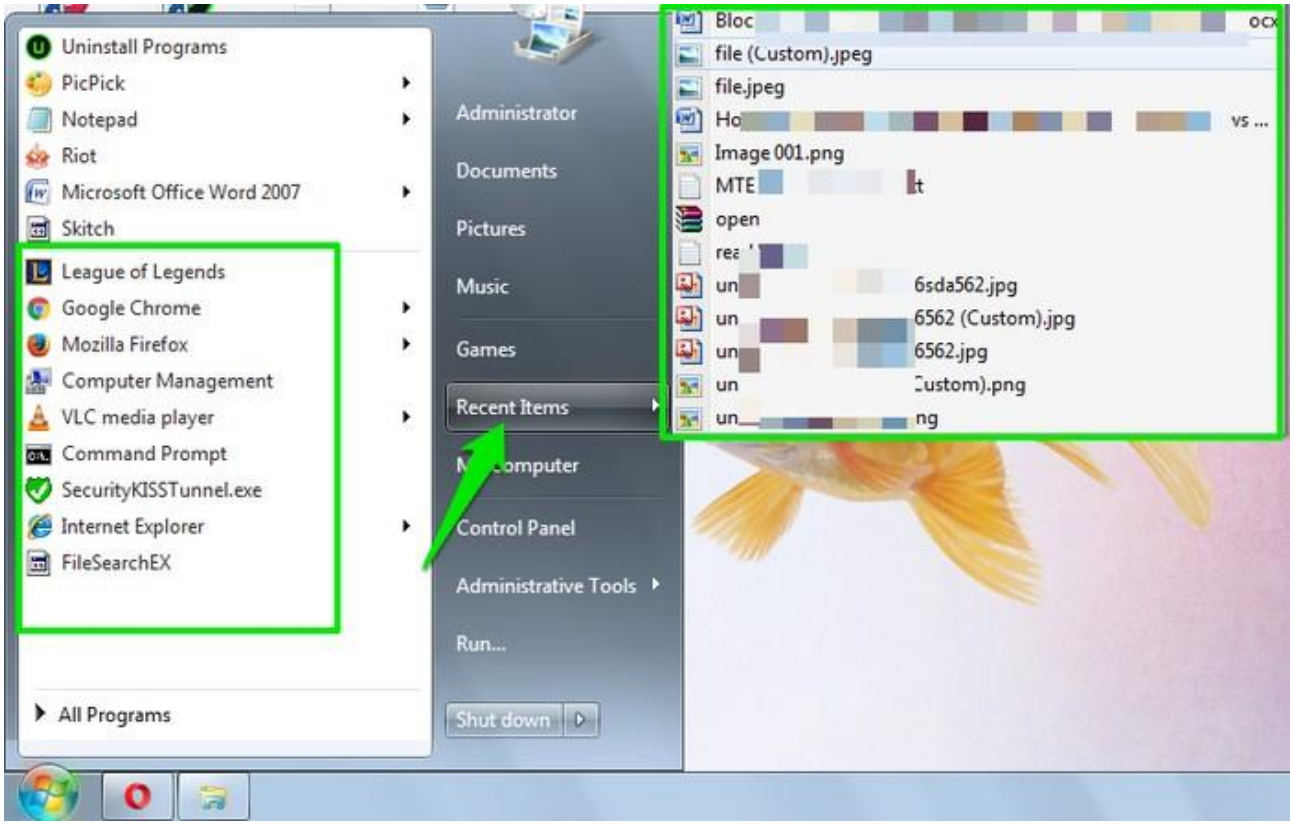
Sådan ved du, om der andre logger på din Windows-pc

Tror du nogen har logget ind på din Windows-pc, mens du var væk? Hvis din blodhund ikke kunne finde den skyldige, kender vi nogle nyttige måder til at finde ud af, om der var adgang til din pc eller ej. De har muligvis ikke efterladt en fysisk ledetråd, men der er en god chance for, at de har efterladt bevis i Windows selv. Nedenfor har vi anført nogle måder, du kan kontrollere for at se, om der var nogen uautoriseret adgang til din Windows-konto eller ej.

Seneste aktivitet

Lad os starte med det grundlæggende. Hvis nogen har adgang til din konto, skal de have brugt den til noget. Du skal tjekke for ændringer på din pc, der ikke kom fra dig.

Udgangspunktet er de nylige programmer, der vises i Start-menuen. Klik på Start-menuen, så ser du de seneste programmer, der var åbne. Du vil kun se en ændring, hvis den indtrængende har adgang til et program, som du ikke har brugt for nylig. En af ulemperne er, at de altid kan slette varen herfra, hvis de er smarte nok. Hvis der endvidere var vist den nylige varevisning på din pc, skal du holde musemarkøren over knappen "Seneste poster" i højre side af Start-menuen, og du vil se alle de filer, der blev åbnet for nylig. Filindgangen forbliver der, selvom de faktiske filer slettes.

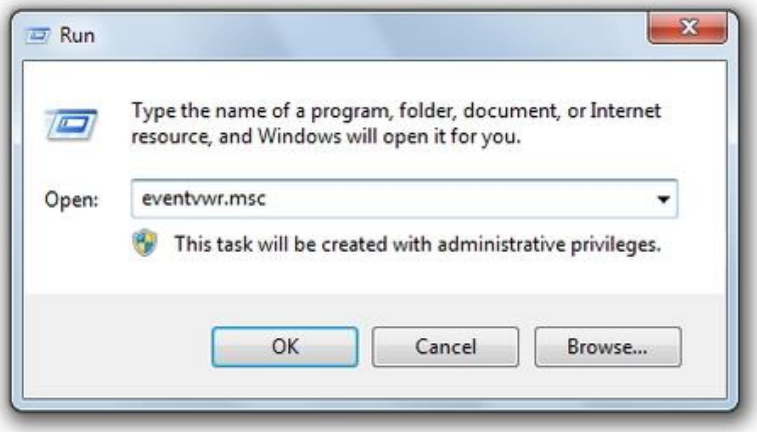


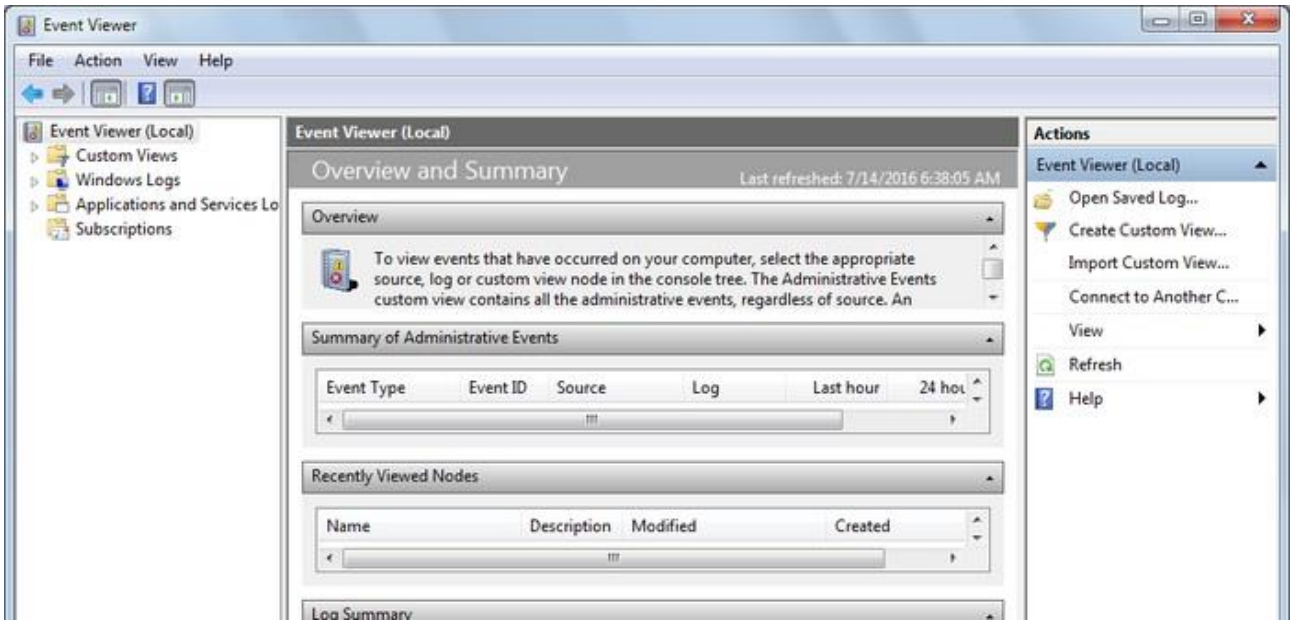
Andre almindelige steder at se efter ændringer inkluderer din browserhistorie, nylige dokumenter og indstillingen "Programmer" i kontrolpanelet for nyligt tilføjede programmer.

Kontroller Windows Event Viewer

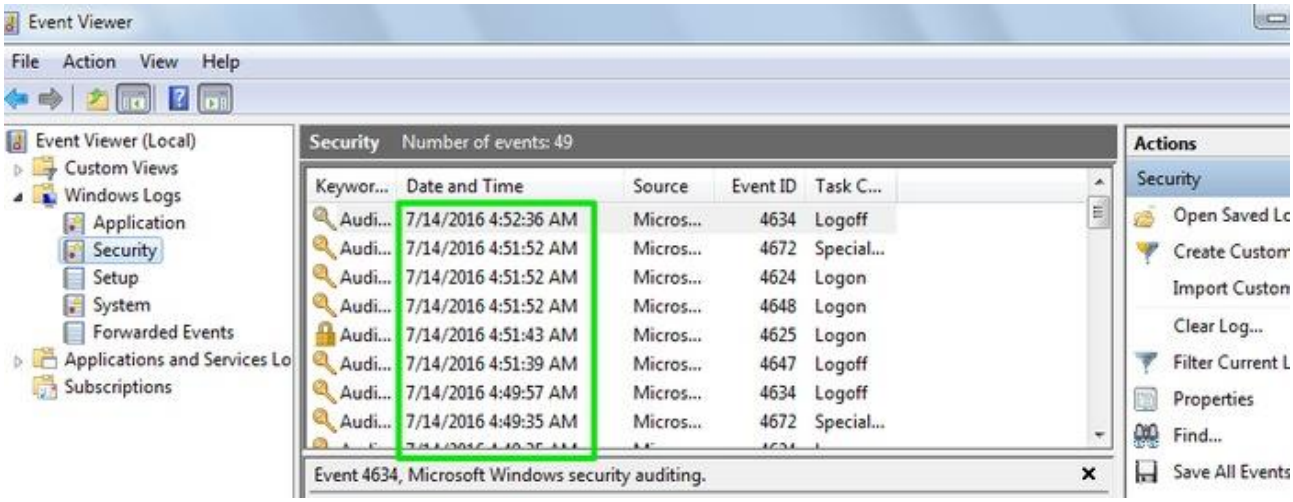
Ovenstående trin var bare for at advare dig om, at noget er galt. Lad os nu tage alvor og grave noget solidt bevis. Windows fører en fuldstændig oversigt over, når en konto er logget ind med succes, og også forsøg på fejl at logge ind. Du kan se dette fra Windows Event Viewer.

For at få adgang til Windows Event Viewer skal du trykke på “Win + R” og skrive `eventvwr.msc` i dialogboksen “Kør”. Når du trykker på Enter, åbnes begivenhedsviseren.

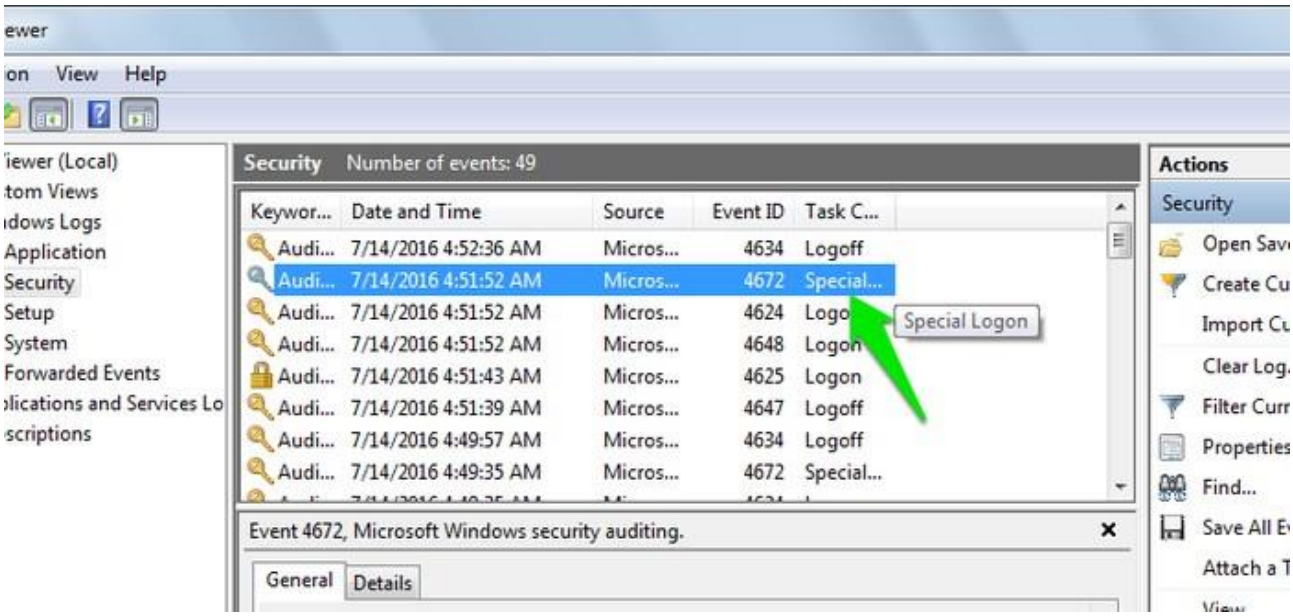




Dobbeltklik her på “Windows Logs” -knappen, og klik derefter på “Sikkerhed.” I det midterste panel ser du flere logonposter med dato- og tidsstempler. Hver gang du logger ind, registrerer Windows flere login-poster inden for en samlet periode på to til fire minutter. Fokus på tidspunktet for disse indtastninger. I mit eksempel er der flere login-poster fra 04:49 til 04:52. Det betyder, at jeg har logget ind på kontoen i denne periode. Alle tidligere login-poster vil også blive optaget, så kig bare efter det tidspunkt, hvor du var væk fra din pc for at se, om der er en post i denne periode.



Hvis der er en post, betyder det, at nogen fik adgang til din pc. Windows opgir ikke falske poster, så du kan stole på disse data. Derudover kan du også kontrollere, hvilken bestemt konto der blev adgang til i denne periode (hvis du har flere konti). For at kontrollere skal du dobbeltklikke på posten "Special Logon" i denne periode, og "Eventegenskaber" åbnes. Her ser du navnet på kontoen ved siden af "Kontonavn."



Vis detaljer om sidste login ved opstart

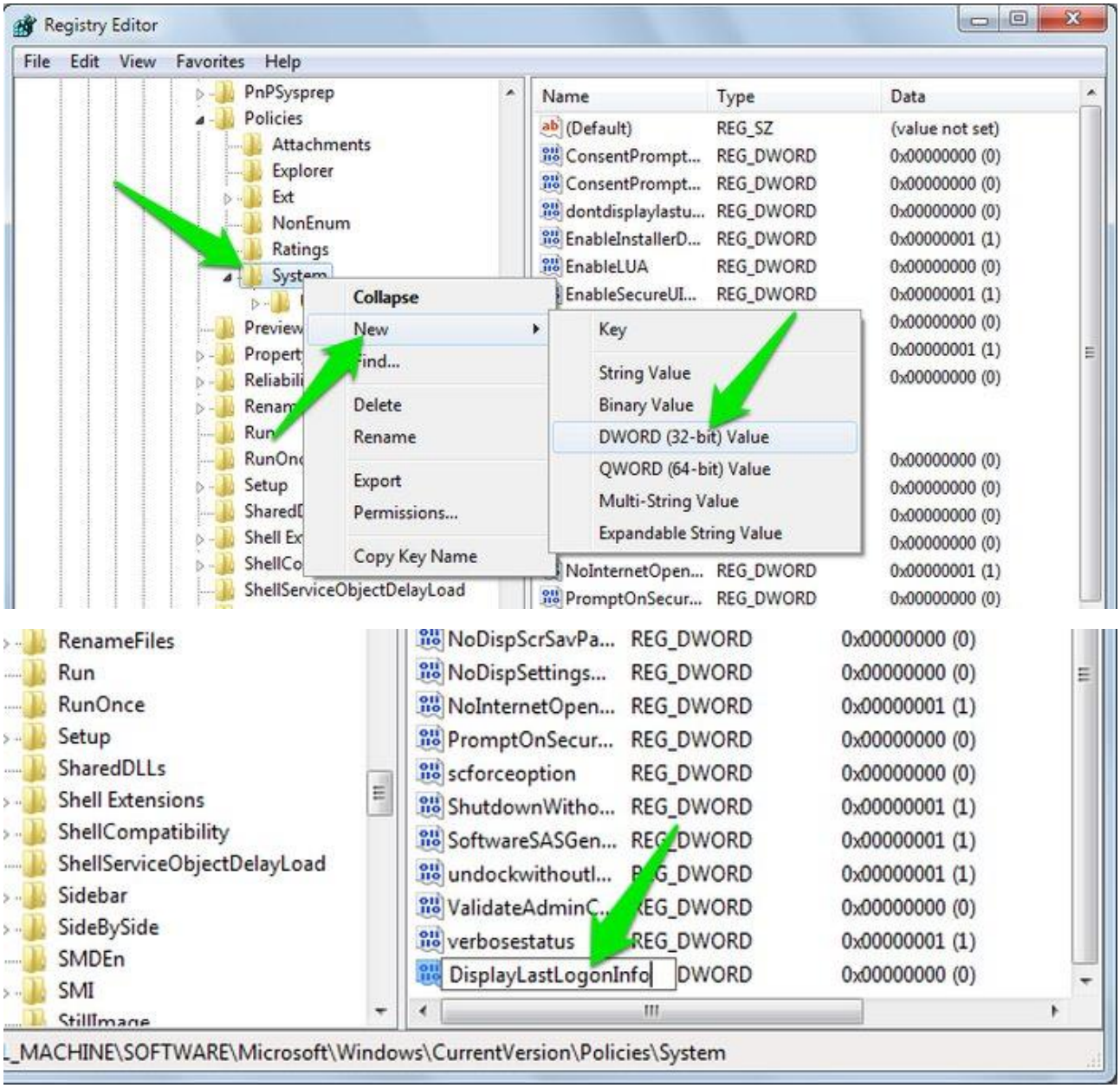
Ovenstående metode er ret solid til at fange indtrængende, men hvis de var smarte nok, kunne de have ryddet alle hændelseslogfiler. I dette tilfælde kan du indstille de sidste loginoplysninger, så de vises, så snart pc'en starter. Dette viser dig, hvornår kontoen sidst var logget ind, og eventuelle mislykkede forsøg. Disse oplysninger kan ikke slettes, men det vil kun hjælpe dig til fremtidig uautoriseret adgang, da du opretter dem lige nu.

Du redigerer Windows-registreringsdatabasen til dette, så sørg for at oprette en sikkerhedskopi af det . Tryk på “Win + R” og indtast `regedit` i dialogboksen Kør for at åbne Windows-registreringsdatabasen.

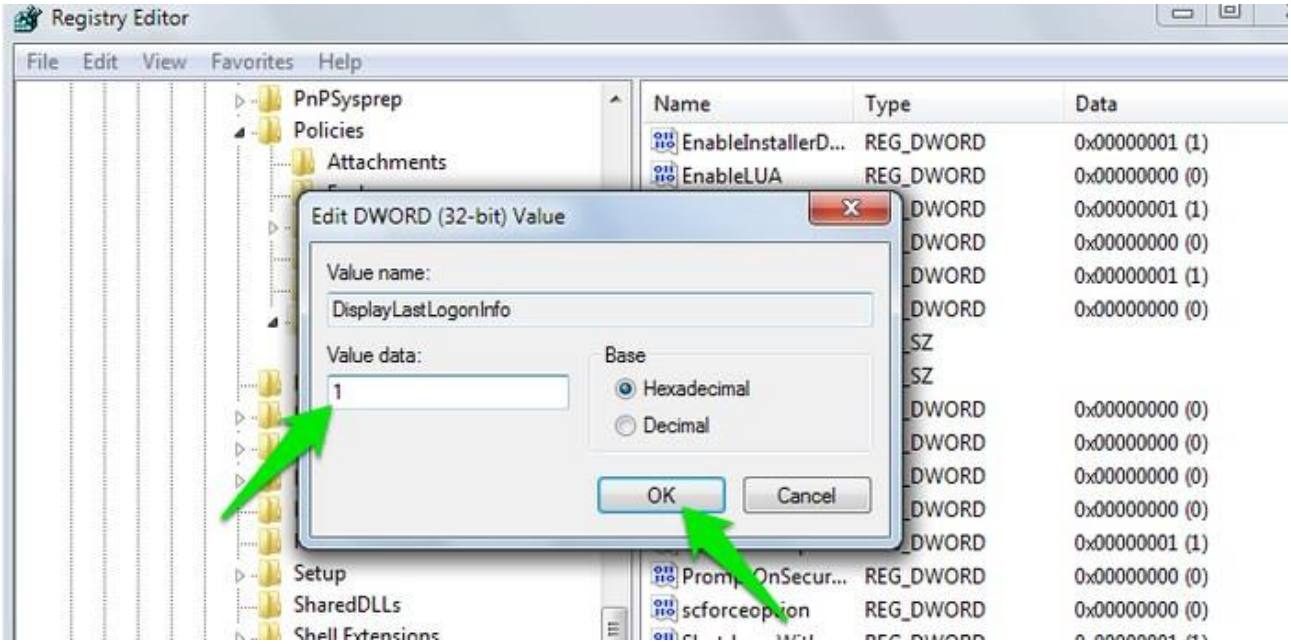
I registreringsdatabasen skal du flytte til nedenstående placering:

```
HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \
CurrentVersion \ Policies \ System
```

Højreklik nu på "System" -mappen og vælg "DWORD-værdi" fra "Ny" indstillingen. En post oprettes klar til omdøbning; skal du navngive det "DisplayLastLogonInfo."



Dobbeltklik på denne post, og indstil dens værdi til “1.” Nu når du (eller en anden) logger ind på din pc, vil du først se, hvornår du sidst var logget ind og eventuelle mislykkede forsøg.



Konklusion

Ovenstående metoder skal være i stand til at fortælle, om din pc havde adgang til en anden. De vil dog ikke fortælle dig "hvem" der faktisk har adgang til din konto. Så ja, du har stadig brug for den blodhund for at spore indtrængende. Hvis du kender andre måder til at finde ud af, om nogen logger ind på din Windows-pc bag din ryg.