Lucrare de laborator 2: Gestionarea conturilor utilizatorilor în Windows,

studierea Windows Registry

**Scopul lucrării:** Cunoașterea procedurii de gestionare a conturilor utilizatorilor și a permisiunilor acestor conturi, abilități de detectare a programelor malware utilizând Windows Registry.

# 1 Controlul contului utilizator în Windows

Majoritatea utilizatorilor de Windows activează cu un cont de administrator. Administratorul practic nu este limitat în accesarea calculatorului și acest fapt este folosit în mod activ de atacatori prin utilizarea virușilor.

Unele dintre cele mai importante obiective ale atacatorilor sunt:

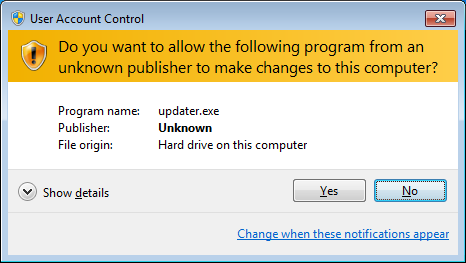
* sistemul de fișiere (de obicei: infectarea fișierelor executabile)

## serviciile Windows

## Windows Registry

## Și aici apare necesitatea, de a izola utilizatorul de sistemul de operare, chiar dacă activează cu dreptul de administrator. Acestui scop și servește serviciul Control Cont Utilizator (UAC – User Account Control).

## Când UAC este activat, orice încercare de a accesa fișierele de sistem, serviciile sau Registry va fi blocată și va apărea o fereastră care va cere o confirmare de la utilizator pentru a permite accesul (Figura 2.1).



## Figura 2.1

Putem găsi Control Cont Utilizator (UAC) prin tastarea UAC în fereastra de căutare a meniului Start.

**Configurarea UAC.** Când deschideţi fereastra UAC, veţi observa un cursor pe care îl puteţi utiliza pentru a regla setările UAC. În mod implicit, UAC este setat pentru a vă anunţa numai când programele încearcă să facă modificări în calculator (figura 2.3).

În afară de modul implicit, mai există trei niveluri ale UAC:

* Always notify me - Doresc mereu notificare
* Notify me only when applications try to make changes to my computer - Doresc notificare doar când programele încearcă să aducă modificări calculatorului (fără estomparea desktop-ului)
* Never notify me - Nu doresc niciodată notificare.

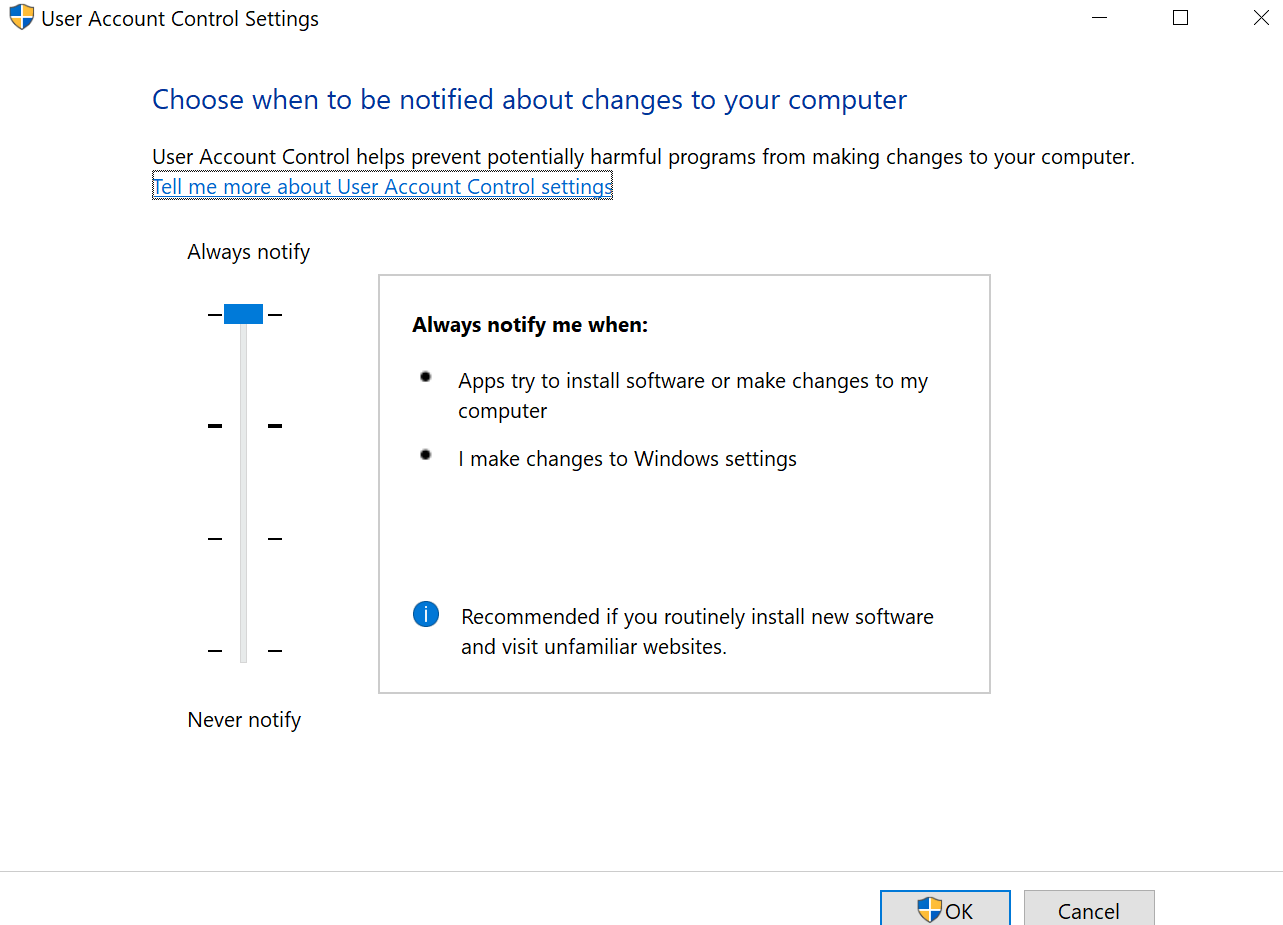


Figura 2.3

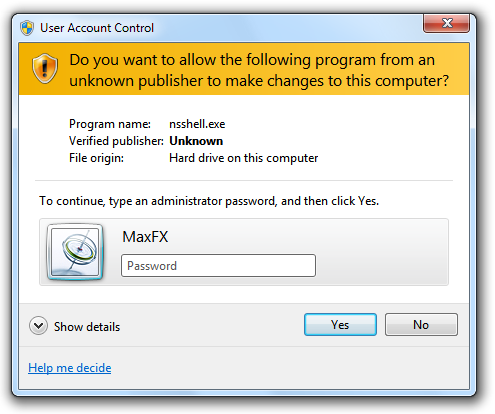
Dacă mutaţi cursorul în sus, UAC va fi setat: "Doresc mereu notificare". Această setare este cea mai sigură şi vă va anunţa de fiecare dată când efectuaţi modificări în setările Windows, sau atunci când un program încearcă să instaleze vreo aplicaţie sau să aducă modificări calculatorului.

Dacă mutaţi cursorul două niveluri în jos, UAC vă va notifica doar când programele încearcă să aducă modificări în calculator, dar fără estomparea desktop-ului . Din punct de vedere al securităţii, această setare este mai puţin sigură decât cea implicită.

Ultima opţiune a UAC -ului este "Nu doresc niciodată notificare". Aceasta este echivalentă cu dezactivarea UAC-lui. Când utilizaţi această setare, dacă sunteţi conectat ca administrator, programele pot efectua modificări în calculator fără indicarea de avertismente. Aceasta este opţiunea cea mai puţin sigură, se recomandă să nu o utilizaţi!

De ce se recomandă să nu dezactivați UAC-ul?

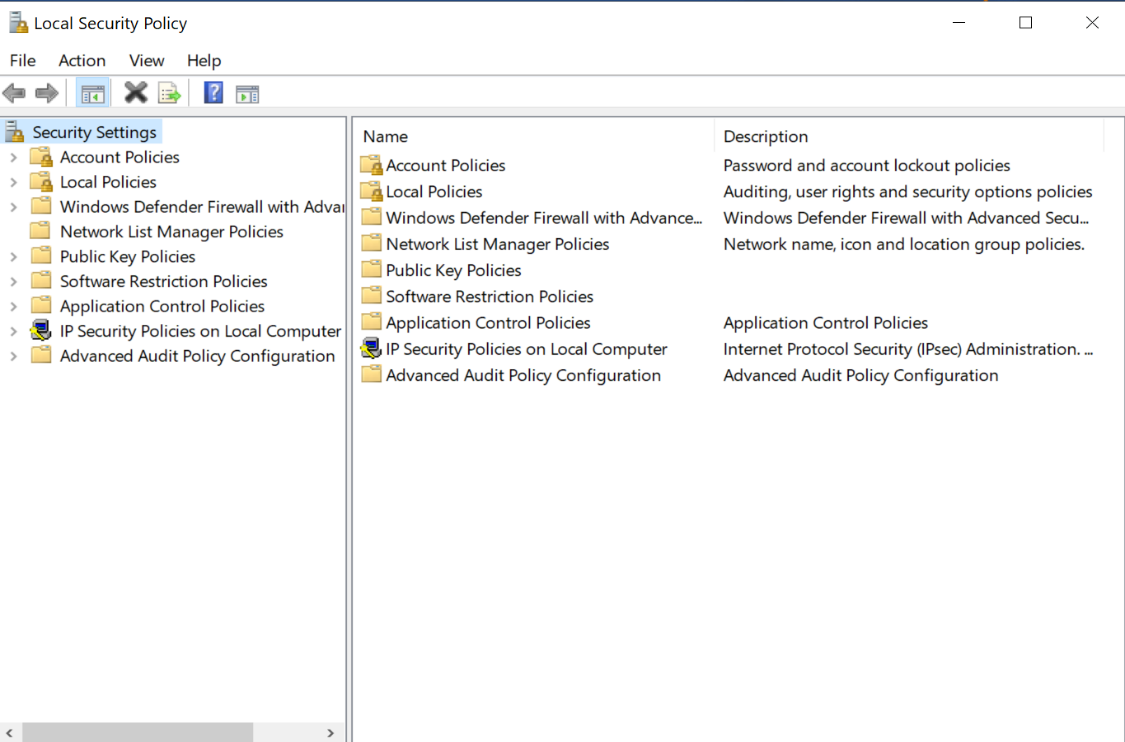
De exemplu a apărut un avertisment cănd ați conectat un stick USB (figura 2.4)



## Figura 2.4

## După cum se poate observa, culoarea a mesajului de avertizare a UCA este galbenă. La o inspecție mai atentă, veți observa că programul nu are un editor de încredere, și un certificat de autenticitate. Programul nsshell.exe este un trojan.

Un deosebit interes prezintă **Politicile de securitate**. Le puteți accesa prin fereastra de căutare -> **Local Security Policy (Win**Key+**R**in the Run Box type **secpol.msc**).



Studiați aceste politici și rezultatele le plasați în raport.

2. Operarea cu Windows Registry

|  |
| --- |
| Atenție! În caz de modificare eronată a unei chei de registry, fapt ce poate deteriora sistemul de operare și ca rezultat inoperabilitatea calculatorului. Se recomandă efectuarea acestui laborator pe o mașină virtuală cu Windows XP.  **Înainte de a modifica o cheie de registry se recomandă să creați o copie de rezervă a cheii.**  Conform Microsoft Computer Dictionary, Windows registry este definită astfel:  *O bază de date centrală ierarhizată utilizată în Microsoft Windows pentru stocarea informaţiei necesare configurării sistemului pentru utilizarea de către unul sau mai mulţi utilizatori, pentru aplicaţii şi dispozitive hardware.*  **(**informații detaliate **-** [**https://support.microsoft.com/ro-ro/help/256986/windows-registry-information-for-advanced-users**](https://support.microsoft.com/ro-ro/help/256986/windows-registry-information-for-advanced-users)**)**  Registry conţine informaţii pe care Windows le accesează continuu în timpul funcționării, cum ar fi profilurile fiecărui utilizator, aplicaţiile instalate pe calculator şi tipurile de documente ce pot fi create de aplicații, setările de proprietăţi pentru foldere şi pictogramele de aplicaţii, ce hardware există în sistem şi porturile care sunt utilizate.  Fereastra editorului de regiştri (Registry Editor se lansează cu comanda *regedit* introdusă în R**un** **Win**Key+**R**) este prezentată în figura de mai jos şi prezintă într-o manieră unificată sistemul de regiştry al sistemului de operare.    Figura 2.5 Fereastra Registry Editor  O analogie utilă în modul de înţelegere a structurii registry-ului a sistemului de operare este comparaţia între acesta şi Windows Explorer (WE). Porţiunea din stânga a ferestrei Registry Editor este asemănătoare Explorer Bar-ului din WE. Cheile şi subcheile ce aparţin celor 5 secţiuni sunt asemănătoare folderelor şi subfolderelor WE, iar o cheie este similar fişierului dintr-un folder. Porţiunea din dreapta ferestrei Registry Editor este asemănătoare ferestrei de conţinut din WE şi conţine valoarea cheii (numele fişierului), tipul acesteia (extensia fişierului) şi data (conţinutul fişierului).  Sistemul de registry este structurat pe 5 secţiuni. În tabelul de mai jos este prezentat rolul fiecăreia dintre cele 5 chei.    Registry memorează şi orice operaţiune realizată de utilizatorul calculatorului (ultimele pagini Web vizitate, ultimele documente accesate, comenzile executate din Run, stick-urile de memorie utilizate, echipamentele hardware conectate la calculator, etc). De asemenea se memorează ultima structură de registry care asigură funcţionarea corectă a sistemului de operare. Atunci când s-a produs o eroare neaşteptată şi eventual sistemul s-a închis pentru a preveni o degradare şi mai accentuată a sistemului de operare, la pornirea calculatorului se apasă tasta F8 şi se alege varianta de lansare a Windows-ului *Last* *Known Good Configuration*. Această opţiune implică ştergerea unei chei din registry.  Programul Malware, ca și orice aplicație are necesitatea de pornire. De aceea, el folosește deseori registry, în special, secțiunile Run.  În registry Editor secțiunea **HKEY\_LOCAL\_MACHINE,** selectați ramura  **Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.**  În jumătatea dreaptă a ferestrei se afișează o listă de chei pentru o această ramură. Găsiți cheia **Userinit** și verificați conținutul (figura 2.6).    Figura 2.6  Înainte de a modifica cheia salvați o copie de rezervă a ramurii cum se indică în figurile 2.7, 2.8.  Puteți crea o copie de rezervă și a întregului registry (volum peste 200 MB)    Figura 2.7    Figura 2.8  În mod normal, valoarea cheie **userinit** este C: \ WINDOWS \ system32 \ userinit.exe. Prezența altor înregistrări pot indica prezența de malware pe calculator (figura 2.9). Pentru a modifica (șterge) înregistrările suspecte din cheie, executați clic dublu pe butonul din stânga al mouse-ului. După editare, faceți clic pe OK .    Figura 2.9  Apoi, accesați folderul în care se află fișierul suspect și ștergeți-l manual. După aceasta, reporniți calculatorul. Controlați din nou înregistrările din cheie, dacă înregistrarea suspectă nu a apărut din nou – sistemul a fost devirusat.  În registry, Startup-ul este prezent în mai multe ramuri:   * **HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run** - programe care pornesc la logare. Această secțiune conține programele a tuturor utilizatorilor din sistem.   + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce** - programe care pornesc o singură dată la intrarea utilizatorului în sistem. După aceasta cheile programelor sunt eliminate automat. Această secțiune conține programele a tuturor utilizatorilor din sistem.   + **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx** - programe care pornesc o singură dată când se îcarcă sistemul. Această secțiune este utilizată la instalarea programelor. După aceasta cheile programelor sunt eliminate automat. Această secțiune conține programele a tuturor utilizatorilor din sistem.   + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run** - programe care pornesc la intrarea utilizatorului curent în sistem.   + **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce** - programe care pornesc o singură dată la intrarea utilizatorului curent în sistem. După aceasta cheile programelor sunt eliminate automat. * **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices** - programe care pornesc împreună cu sistemul până la logarea utilizatorului. * **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce** - programe care pornesc o singură dată la pornirea sistemului.   În registry editor accesați ramura:  **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run**  În partea dreaptă a ferestrei, executați clic dreapta și alegeți – String Value (figura 2.10)  Și întrodiceți un nou parametru - Paint    Figura 2.10  Executați dublu clic pe parametrul - Paint, și întroduceți calea spre această aplicație (figura 2.11) - **C:\WINDOWS\System32\mspaint.exe**    Figura 2.11  Resetați calculatorul, aplicațiea Paint va porni automat după încărcarea sistemului.  **Util.** Dacă doriți să aflați versiunea BIOS din *registry*, urmați ramura:  HKEY\_LOCAL\_MACHINE\HARDWARE\DESCRIPTION\System\BIOS (figura 2.12)    Figura 2.12  Dacă vă deranjează fondalul ferestrelor de sistem (W8) puteți să le modificați prin registry. Ramura HKEY\_CURRENT\_USER\Control Panel\Colors (figura 2.13)  Valorile culorilor de ex. - 180 180 180 (nuanță de gri) este culoarea în RGB.  Concret culoarea o puteți vedea, de exemplu, în Paint, Edit Colours    Figura 2.13  Pentru scanarea Windows Registry se propune utilitarul jvl6 Power Tools din sursa - <http://www.macecraft.com>  Se cere adresa mail, și după descărcare o puteți utiliza gratis timp de 14 zile (figura 2.14).    Figura 2.14  Executați clic - *Clean and fix my computer* (figura 2.15) și optați pentru modul de  siguranță (safety) - OK    Figura 2.15  După scanare va apărea o fereastră cu lacunele depistate. |
|  |

**3 Conținutul raportului:** Explicați controlul contului în Windows, Local Security Policy. Explicați ce reprezintă *Windows Registry*, structura pe secțiuni, modurile de modificarea a cheilor (inclusiv și cazul de depistare de malware), folosirea utilitarului *jvl6 Power Tools* (folosiți mai multe opțiuni de optimizare a sistemului ), concluzii.