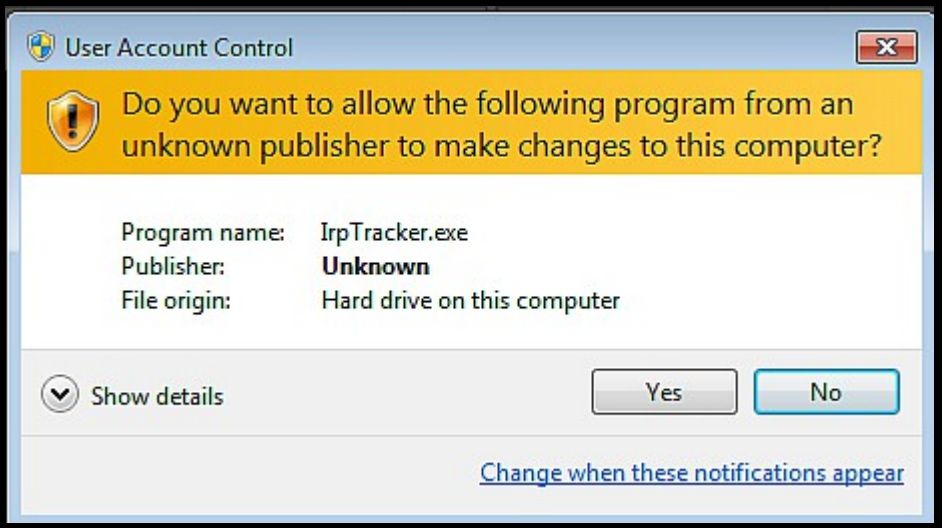
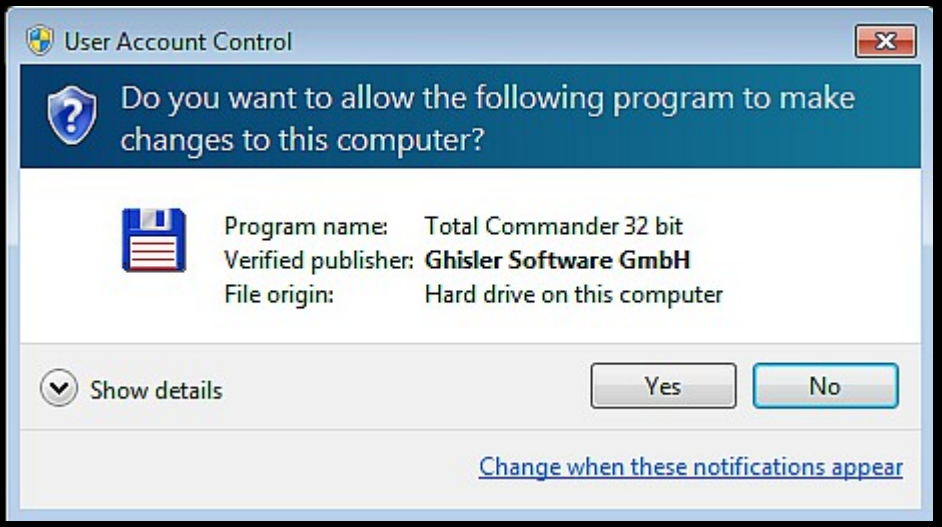
User Account Control

a jak jej obejít

Martin Dráb
martin.drab@email.cz
http://www.jadro-windows.cz

Co to je UAC


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: IrpTracker.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

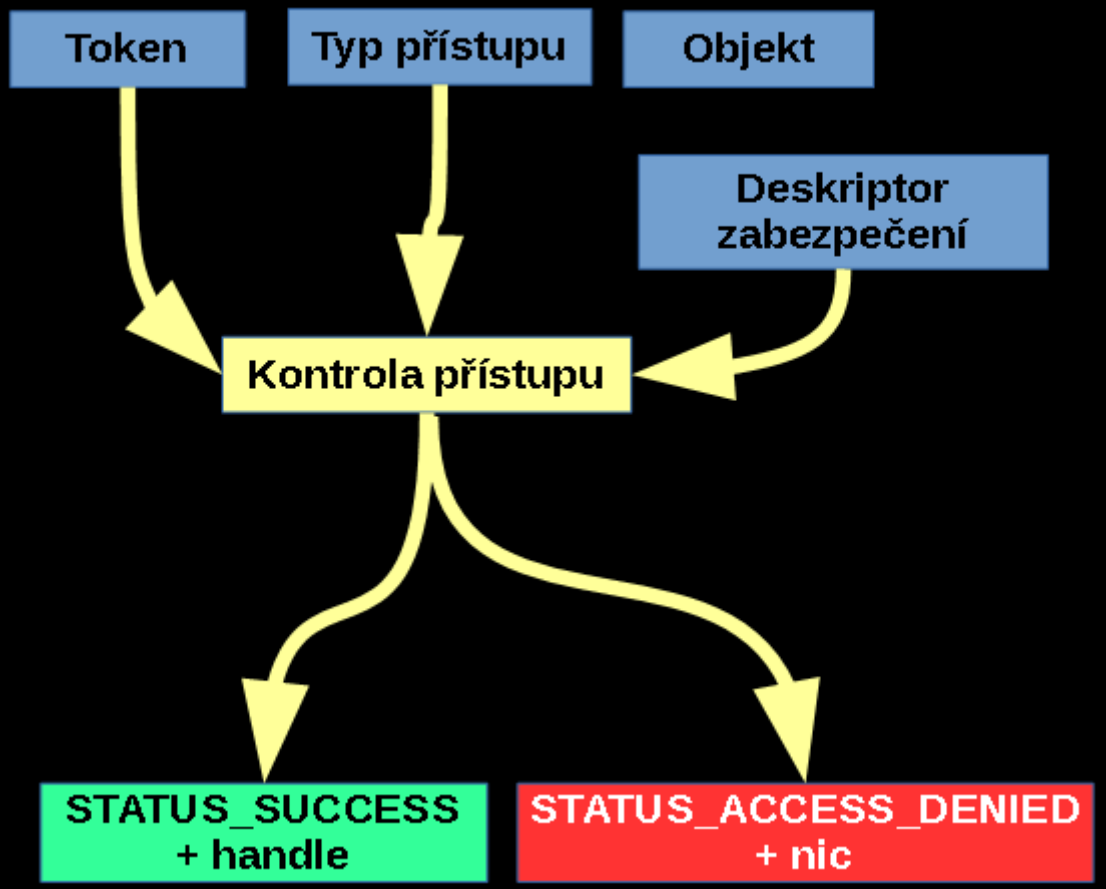

User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: Total Commander 32 bit
Verified publisher: Ghisler Software GmbH
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

Obecné informace

- **Windows Vista**
  - Dialog při libovolné nutnosti zvýšit oprávnění
  - I v Ovládacích panelech
  - Otravné, ale bezpečné (alespoň myslím)
- **Windows 7+**
  - Některé aplikace projdou dialogem automaticky (uživatel nic nepozná)
  - Neotravuje, ale zranitelné
  - Již od Windows 7 RTM (Leo Davidson)
    - O jeho práci si budeme povídat

Kontrola přístupu

- Token
  - SIDy uživatelských skupin
  - Úroveň integrity
  - Integritní politika
  - Privilegia



- Deskriptor zabezpečení
  - DACL (seznam položek):
    - Povolit přístup X SIDu Y
    - Zakázat přístup X SIDu Y
  - Úroveň integrity
  - Integritní politika

Odlišnost oprávnění

Vlastnost	Neprošly UAC dialogem	Prošly UAC dialogem
Skupina Administrators v DACL	Zákaz přístupu	Povolení přístupu Zákaz přístupu
Úroveň integrity	Normální (S-1-16-8192)	Vysoká (S-1-16-12188)
Zajímavá privilegia	NE	ANO

Hlavní myšlenka

- Vytvořit útočnou knihovnu vhodně vybraného jména
- Dostat ji k některé z aplikací automaticky procházející UAC dialogem (vybrat obětního beránka)
  - %windir%\system32\sysprep\Sysprep.exe
  - %windir%\system32\\cliconfg.exe
  - %windir%\system32\oobe\setupsqm.exe
  - ...
- Tuto aplikaci spustit
  - Načte útočnou knihovnu
  - Administrátorská oprávnění

Spustitelné soubory

- Formát Portable Executable (PE)
- DLL knihovny, EXE soubory, ovladače (SYS)
- Obsah:
  - **Kód** (soubor funkcí a procedur),
  - **Data** (globální proměnné, konstanty),
  - **Exportované symboly** (podprogramy, proměnné poskytované jiným spustitelným souborům)
  - **Importované symboly** (podprogramy a proměnné z jiných knihoven potřené k správnému fungování daného souboru)
    - Jméno knihovny neobsahuje cestu

Načítání

- **Automatické.** Knihovna exportuje symboly importované jinou knihovnou, kteoru aplikace chce načíst
- **Explicitní.** Knihovna je načtena, protože o to aplikace explicitně požádala.
- **Líné načtení (delay load)**. Knihovna je načtena až v okamžiku, kdy aplikace některý z exportovaných symbolů opravdu použije (kombinace obou předchozích).
- Ani v jednom případě se často uvede jen jméno souboru knihovny, ne celá cesta.

Prohledávané oblasti

	Standardní prohledávání		Alternativní prohledávání	
	SafeDllSearchMode		SafeDllSearchMode	
	Povolen	Zakázán	Povolen	Zakázán
Složka aplikace	1	1		
Systémový adresář	2	3	2	3
Sys. adresář (16bit)	3	4	3	4
Adresář Windows	4	5	4	5
Aktuální adresář	5	2	5	2
%PATH%	6	6	6	6
Plné jméno souboru			1	1

Kopírování k beránkovi

- Beránci obvykle sídlí v systémovém adresáři nebo v jeho podstromě
  - Zápis vyžaduje administrátorská oprávnění
- Některé procesy mohou i do takových míst kopírovat soubory (ne přepisovat) za využití COM objektu IFileOperation.
  - Průzkumník Windows (explorer.exe)
- Je třeba je ke kopírování donutit
  - Injekce kódu

Více o výběru beránka

- Seznam aplikací automaticky procházejících UAC dialogem lze najít na internetu
- Nebo tipnout
  - Podívat se po aplikacích s méně známými názvy v systémovém adresáři či jeho podstromu.
- Spustit vybranou aplikaci a zjistit, jaké DLL knihovny používá a ověřit, které z nich nejsou známé či v manifestu.

Ukázka

- Obětní beránek
  - %windir%\system32\\cliconfg.exe
- Název knihovny
  - NTWDBLIB.DLL
- Kroky
  - Vložení knihovny do procesu Průzkumníka
  - Knihovna zjistí, zda disponuje administrátorskými právy
    - Pokud ne, nakopíruje se do systémového adresáře a spustit obětního beránka, počká na jeho ukončení a smaže se.
    - Pokud ano, spustí Příkazový řádek a ukončí proces.

Obrana

- Používat plné cesty k souborům knihoven + alternativní prohledávání
- Knihovna patří mezí tzv. známé
  - Klíč registru KnownDlls (KnownDlls32 pro WOW64)
    - HKLM\SYSTEM\CurrentControlSet\Controls\Session Manager
  - Knihovny přednačteny, obvykle sídlí v systémovém adresáři
- Plná cesta ke knihovně uvedena v manifestu (součást souboru aplikace) – elementy <file>

Příklad obrany manifestem

- Obětní beránek
  - %windir%\system32\sysprep\sysprep.exe
- V manifestu je napsáno (Windows 8.1):
  - **“Specifically load these DLLs from the specified path. This is done as a defence-in-depth approach to closing a known UAC exploit related to Sysprep.exe being auto-elevated.“**
  - Ale na **shcore.dll** zapomněli

Reálné zneužití

- Carberp
  - „open source“
- GoodKit
- Win32/Tilon (LD)
- WinNT/Pitou (LD)
- WinNT/Simda (ISecurityEditor)
- … (určitě budou i další)

Zdroje a zajímavé odkazy

- **Leo Davidson**
  - http://www.pretentiousname.com/misc/win7_uac_whitelist2.html
- **UACMe**
  - https://github.com/hfiref0x/UACME
- **Kernelmode.info**
  - http://www.kernelmode.info/forum/viewtopic.php?f=11&t=3643

???

- **Email:** martin.drab@email.cz
- **Web:** http://www.jadro-windows.cz
- **ICQ:** 332970040