# Ultimate Process Manager
# by
# Lodus Software

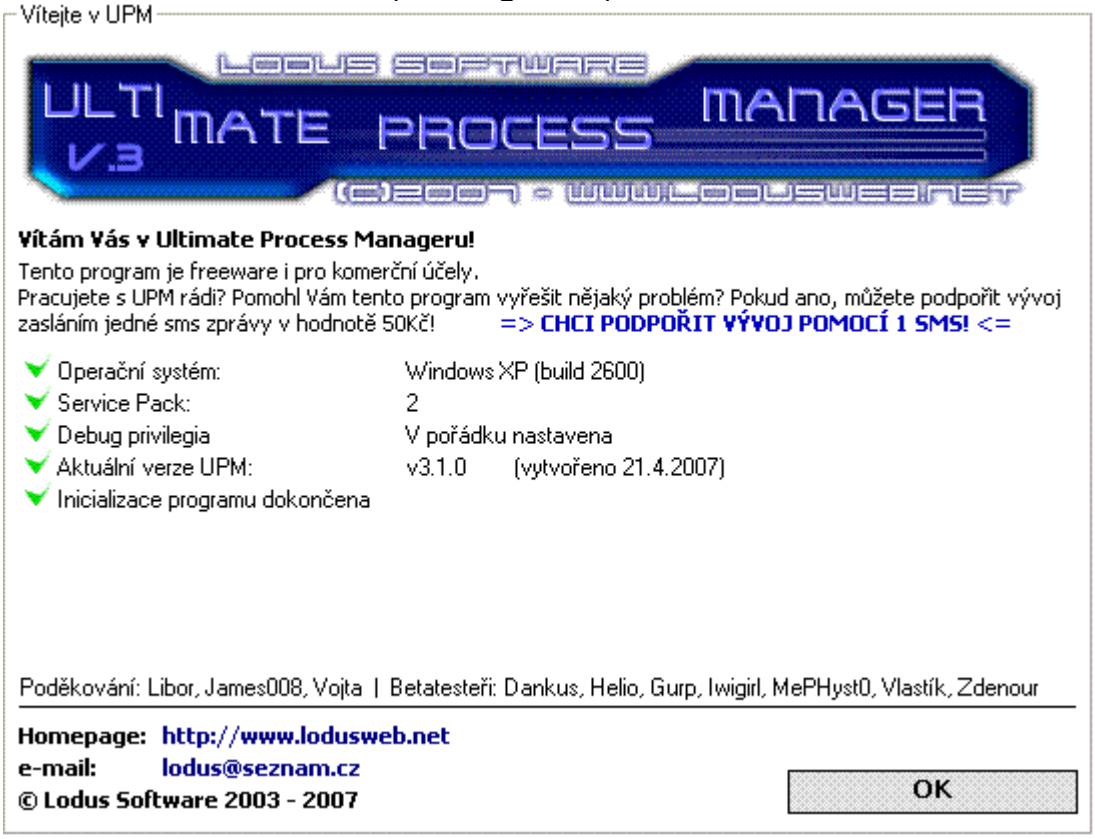
## NÁPOVĚDA

**UPOZORNĚNÍ:**
**AUTOR (LODUS SOFTWARE) NERUČÍ ZA ŠKODY ZPŮSOBENÉ POUŽÍVÁNÍM TOHOTO PROGRAMU. JEHO NEUVÁŽENÝM POUŽÍVÁNÍM MŮŽETE VÁŽNĚ POŠKODIT OPERAČNÍ SYSTÉM. PROGRAM ULTIMATE PROCESS MANAGER NENÍ URČEN PRO BĚŽNÉ UŽIVATELE, ALE UŽIVATELE POKROČILÉ A ZNALÉ SYSTÉMU MICROSOFT WINDOWS XP.**

**ULTIMATE PROCESS MANAGER JE FREEWARE A JE DOVOLENO JEJ VOLNĚ ŠÍŘIT. PROGRAM JE MOŽNÉ VYUŽÍT PRO KOMERČNÍ ÚČELY. JE ZAKÁZÁNO JAKKOLI ZASAHOVAT DO KÓDU PROGRAMU NEBO POUŽÍVAT JEHO SOUČÁSTI BEZ POVOLENÍ AUTORA.**

**Obsah**

## 1.1. Úvodní obrazovka (O Programu)




Okno vyvoláte kliknutím na tlačítko [O Programu] v hlavním menu programu.

- Operační system – **UPM je** původně **vytvořené pouze pro Windows XP**, nejlépe se service pack 2. Windows 2000 Proffesional SP4 a Windows 2000 server SP4 jsou rovněž podporovány s menší úpravou.

  *Zprovoznění UPM pod W2K:*
  *Upozornění: i po těchto úpravách nemusí UPM běžet bez problémů.*
  *W2k neobsahují knihovnu gdiplus.dll, kterou můžete zdarma stáhnout na internetu (http://www.dll-files.com/dllindex/dll-files.shtml?gdiplus), po stažení ji nakopírujte do adresáře Windows\System32.*

- Service pack – i přes kompatibilitu k service pack 1 je **doporučeno** mít nainstalovaný **service pack 2**
- Debug privilegia – slouží UPM pro přístup k systémovým procesům, pokud nejsou nastavena, znamená to, že uživatel nemá dostatečná práva pro práci se systémovými procesy. Některé viry zabraňují procesům nastavení těchto práv.
- Aktuální verze UPM – UPM se pokusí z internetu zjistit aktuálni verzi. V případě nové verze nabídne stažení.

**Chybová hlášení**

- Databáze procesů: Soubor nenalezen (proc.db) – tento soubor v sobě uchovává seznam registrovaných procesů. Pro běh UPM nemá žádný vliv, pokud nechcete využívat registrace procesů, tento soubor můžete smazat.
- Soubor s nastavením: Soubor nenalezen (nastaveni.usr) – tento soubor v sobě uchovává nastavení UPM. Pokud nebyl soubor nalezen, UPM použije defaultní nastavení. Nastavit UPM můžete pomocí dialogu Nastavení (Menu -> Nastavení).

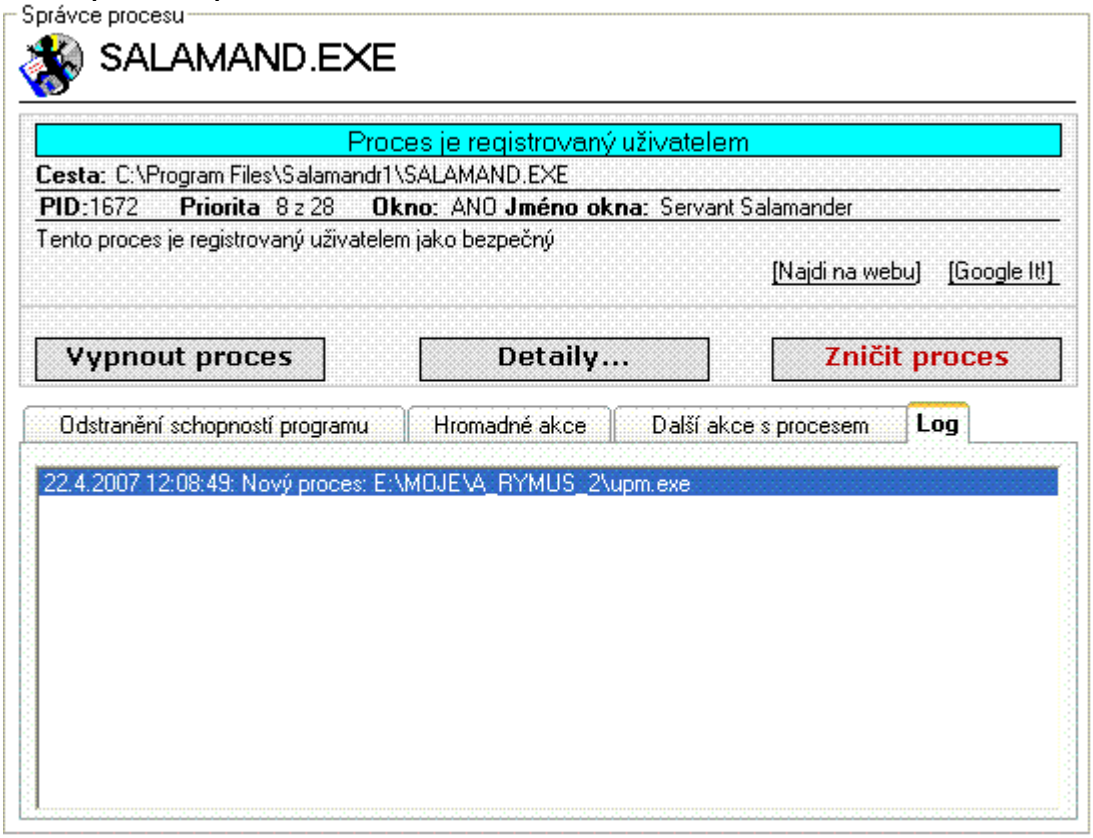
**Dotace**

UPM je freeware a chtěl bych, aby tomu tak zůstalo, k tomu můžete pomoci i Vy jednoduchým zasláním jedné dotační SMS v hodnotě pár desítek Kč. Více zde: http://www.lodusweb.net/index.php?option=com_content&task=view&id=27&Itemid=82

## 1.1 Seznam procesů

Zobrazení všech běžících procesů. Zatržením políčka Filtr reg. Budou vypisovány jen neregistrované procesy (nezávisle na chybných hashích). Tlačítko Scanner zobrazí okno scanneru, které je popsáno dále v nápovědě.

## 1.2 Správce procesu

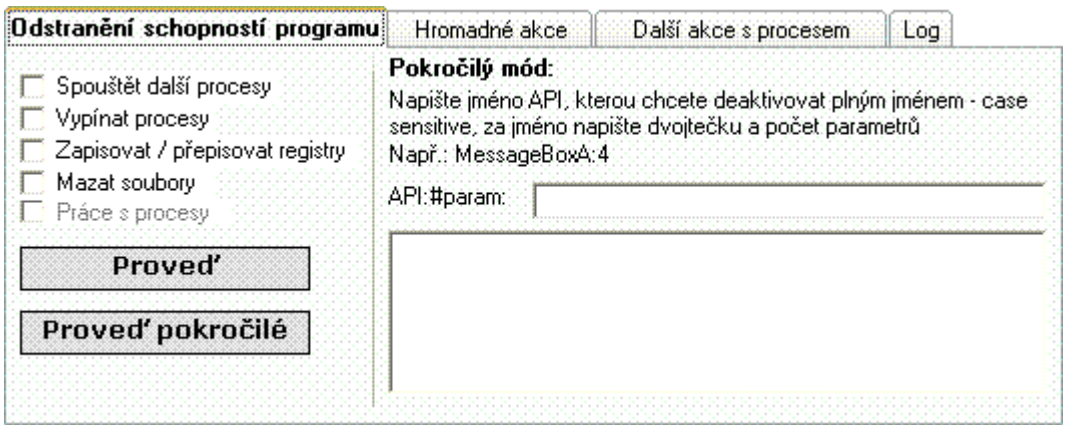



Okno vyvoláte označením procesu a kliknutím na tlačítko [Správce procesu].

- Vypnout proces – vypne označený proces

- Detaily – zobrazí detaily (viz další body nápovědy)
- Zničit proces – vypne a následně smaže spustitelný soubor náležící procesu. Není možné zničit registrovaný proces. Defaultně je nastaveno zálohování souborů, které mají být zničeny. Záloha se provádí do adresáře s UPM do složky Záloha.
- Najdi na webu – otevře stránku, která je zadána v Nastavení s parametrem jména procesu.
- Google It! – vyhledá jméno procesu na Google.com

### 1.2.1 Odstranění schopností programu




Odstranění schopností programu je velice užitečná věc, která zakáže konat označenému procesu dané akce.

**Zjednodušené:**

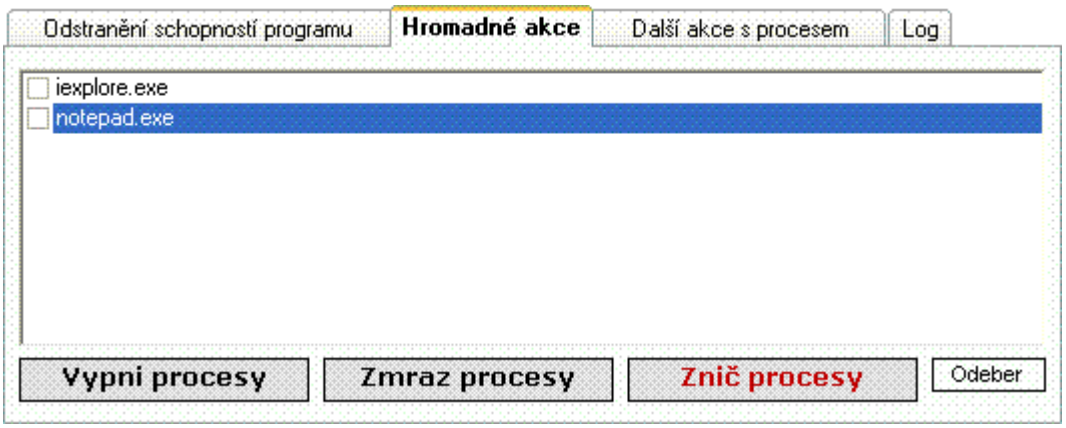
- Spouštět další procesy – označený proces nebude schopný spustit žádný soubor a ani spustit žádný další proces.
- Vypínat procesy – zakáže označenému procesu vypínat ostatní procesy
- Zapisovat / přepisovat registry – zakáže označenému procesu zapisovat nebo přepisovat jakékoliv hodnoty v registru.
- Mazat soubory – zakáže označenému procesu mazat jakékoliv soubory
- Práce s procesy – zakáže použití API OpenProcess (s jakýmikoliv parametry)

**Pokročilý mód:**

Zakáže používat zadanou API funkci. Návratová hodnota je nastavena na 0.

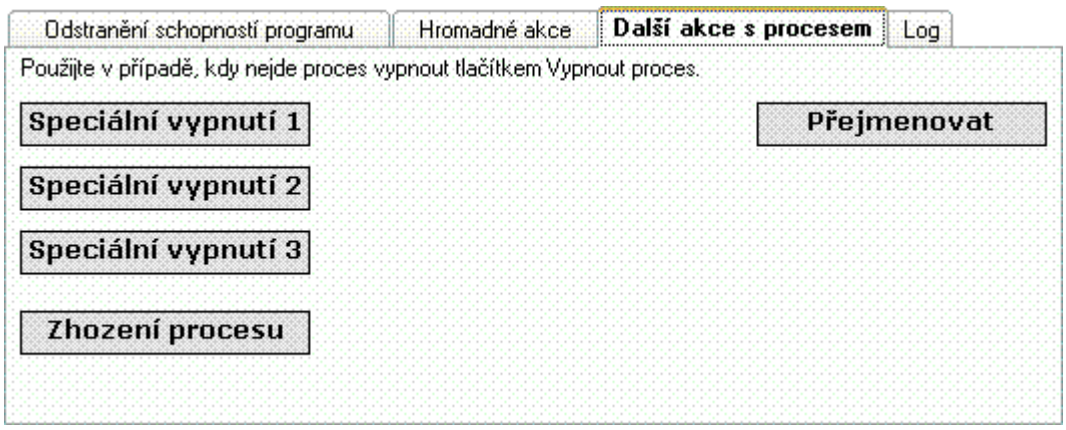
Upozornění: neuváženou prací s touto funkcí je možné Windows restartovat. Veškeré změny touto funkcí jsou provedeny pouze v paměti RAM – nejsou měněny žádné soubory. Po restartu procesu nebo celého systému je vše jako před použitím funkce Odstraniění schopností programu.

### 1.2.2 Hromadné akce




- Vypni procesy – vypne všechny procesy v seznamu (nezávisle na zaškrtnutí)
- Zmrar procesy – zmrazí všechny procesy v seznamu (suspenze všech vláken procesu). „Odmrazit“ proces můžete samostatně ve Správce vláken (Menu-> [Nástroje pro proces]).
- Znič procesy – zničí (vypne a smaže) všechny procesy v seznamu
- Odeber – odebere ze seznamu zaškrtnuté položky

### 1.2.3 Další akce s procesem




Některé viry mohou také blokovat používání standardních postupů pro vypínání procesů. Proto jsou v UPM ještě další 4 postupy pro vypnutí procesu.

*Zhození procesu – zápis insrukce int3 na EIP*

**[!] Přejmenovat** - funkce přejmenovat přejmenuje spustitelný souboru procesu. Pokud nechcete procesy mrazit nebo odebírat schopnost Spouštět další procesy (což v některých případech není možné), doporučuji použít funkci Přejmenovat a následně se pokusit proces vypnout, případně restartovat systém. Zabráníte tak jeho dalšímu spuštění.

## 1.3 Detaily procesu

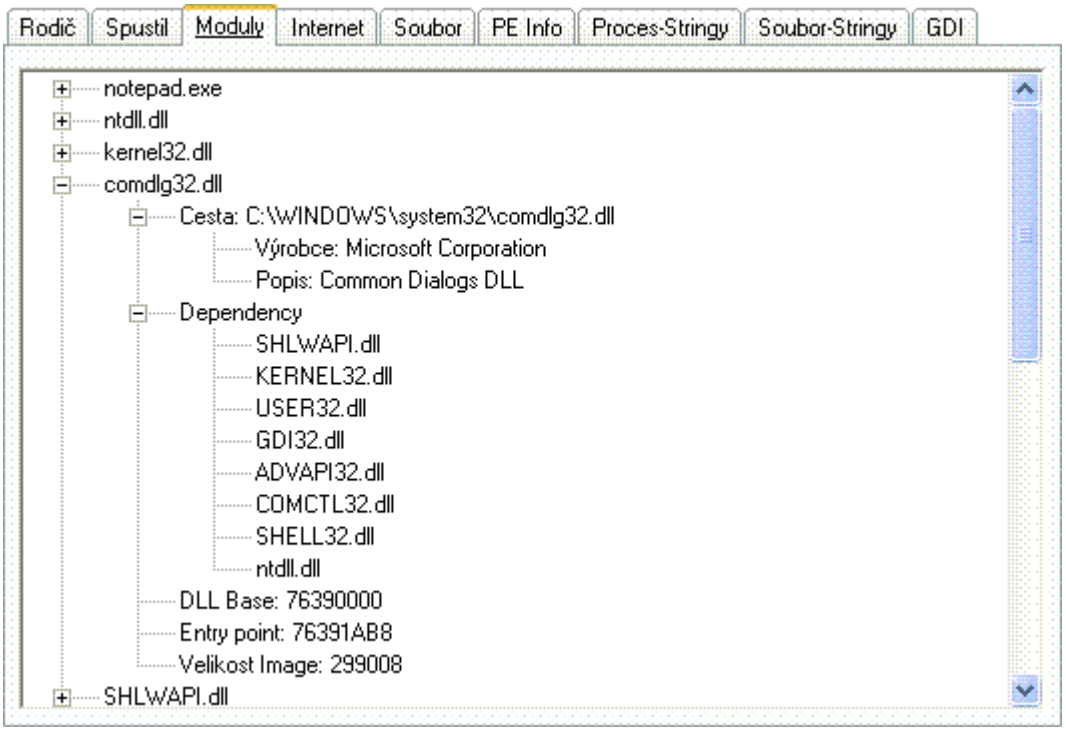
### 1.3.1 Rodič

Zobrazení rodiče označeného procesu (tj. proces, kterým byl označený proces spuštěn). Zobrazí i ostatní děti procesu.

### 1.3.2 Spustil

Zobrazí všechny procesy, které spustil označený proces.

### 1.3.3 Moduly




Zobrazí všechny moduly, které jsou nahrané v paměti označeného procesu.

- Dependency – závislost dané knihovny na ostatních
- Velikost image – velikost image bytech (decimální)

Tip: ve většině případů je v podobných oknech možné použít pravé tlačítko pro rozšířenou práci s objekty.

- Zobraz i DLL Microsoftu – pokud políčko odškrtnete, nebudou zobrazeny knihovny podepsané Microsoftem
- Zobraz funkce – zobrazí všechny exportované funkce dané DLL knihovny

Tip: krátkým podržením kurzoru myši nad seznamem se zobrazí nápověda pro další akce

### 1.3.4 Internet

Zobrazí aktivní připojení označeného procesu k síti Internet.

### 1.3.5 Soubor

Zobrazí detaily o souboru

- Handly – zobrazí všechny otevřené handly označeného procesu. Tyto handly je pak možné zavřit.
- Uložit do TXT – export vybraných detailů o procesů do TXT souboru

### 1.3.6 PEB / PE Info

Zobrazení adresy začátku struktury PEB a zobrazení hodnot struktury NT Header, která je načtena z paměti běžícího procesu (!). Pokud není možné proces otevřít, nebo jsou zobrazeny Detaily pouze určitého souboru, jsou načtena data přímo z tohoto souboru. U hodnoty EntryPoint je zobrazeno i jméno sekce, do které EntryPoint ukazuje.

### 1.3.7 Proces – stringy

Po kliknutí na tlačítko Zjisti UPM začne vypisovat do seznamu všechny textové řetězce nalezené v paměti procesu. Velikost textových řetězců je minimálně 5 znaků. Maximální počet zobrazených řetězců je 65 535.

### 1.3.8 Soubor – stringy

Totéž co Proces – stringy, ale s tím rozdílem, že textové řetězce jsou načítány ze souboru.

### 1.3.9 Proces – stringy

Zobrazení GDI objektů

## 1.4 Nástroje (pro proces)

Upozornění: neuváženým používáním těchto nástrojů můžete způsobit pád programu. Nástroje jsou určeny především pro programátory znalé Windows API.

### 1.4.1 Správce vláken

Zde je možné zmrazit (suspendovat), nebo odmrazit (resume) vlákna procesu, případně dané vlákna ukončit. U suspendovaných vláken je možné měnit hodnoty registrů (dvojtým klikem na hodnotu, kterou chcete změnit).

### 1.4.2 Memory editor

Dvojitým klikem na byte v tabulce je možno jej editovat. Je možné vkládat i pole bytů (byty zadávejte v hexadecimálním tvaru, zarovnané na délku dvou znaků), přepnutím na ASCII bude zapsán na adresu vložený textový řetězec bez null-terminate znaku.

- Kopíruj jak vidím – uloží do schránky obsah memory vieweru
- Kopíruj speciálně – uloží do schránky hex dump obsahu memory vieweru ve formátu Defined Dword Assembleru.
- Jít na adresu (klávesová zkratka G) – skok na zadanou adresu v hexadecimálním tvaru

### 1.4.3 DLL injekce a CRT

- Inject! – nainjektí do procesu zadanou DLL knihovnu (způsob CreateRemoteThread na LoadLibrary). Nedojde ke spuštění knihovny.
- CreateRemoteThread Vytvoř – vytvoří nové vlákno na zadané adrese. Pokud nechcete zadávat adresu, stačí napsat jméno API, UPM se adresu pokusí získat. Je možné zadat libovolné množství parametrů, které budou umístěny v zásobníku vytvořeného vlákna. Parametry zadávejte v hexadecimální podobě a oddělujte čárkou.

### 1.4.4 Paměť

VirtualAllocEx, VirtualQueryInfoEx, VirtualFreeEx.

- Zapsat soubor do paměti – zapíše zadaný soubor do zadané paměti. Pokud je zadaná paměť = 0, UPM automaticky alokuje dostatečnou paměť pro zapsání souboru. Pokud zaškrtnete Přepni do CRT, budete po zapsání souboru do paměti přepnuti do karty s CreateRemoteThread.

### 1.4.5 Regiony

Zobrazení regionů paměti. Dvojtým klikem na daný region jej zobrazíte v memory editoru.

### 1.4.6 API Hook Scanner

- API Scan – projde všechny exportované funkce zaškrtnutých modulů a otestuje, zda-li první instrukce funkce není skok, pokud ano, je nález vypsán. Jsou testovány instrukce JMP, Call, Push & Ret.

  Normální háky pro ntdll.dll a kernel32.dll:

| | | |
|---|---|---|
| ntdll.dll | ceil | @ 0x7C901E1E |
| ntdll.dll | floor | @ 0x7C901F5D |
| kernel32.dll | ProfileUserMapping | @ 0x7C82C86D |
| kernel32.dll | DebugBreak | @ 0x7C859B72 |
| kernel32.dll | tUserDefaultLangID | @ 0x7C80BF64 |
| kernel32.dll | registerConsoleIME | @ 0x7C874B86 |

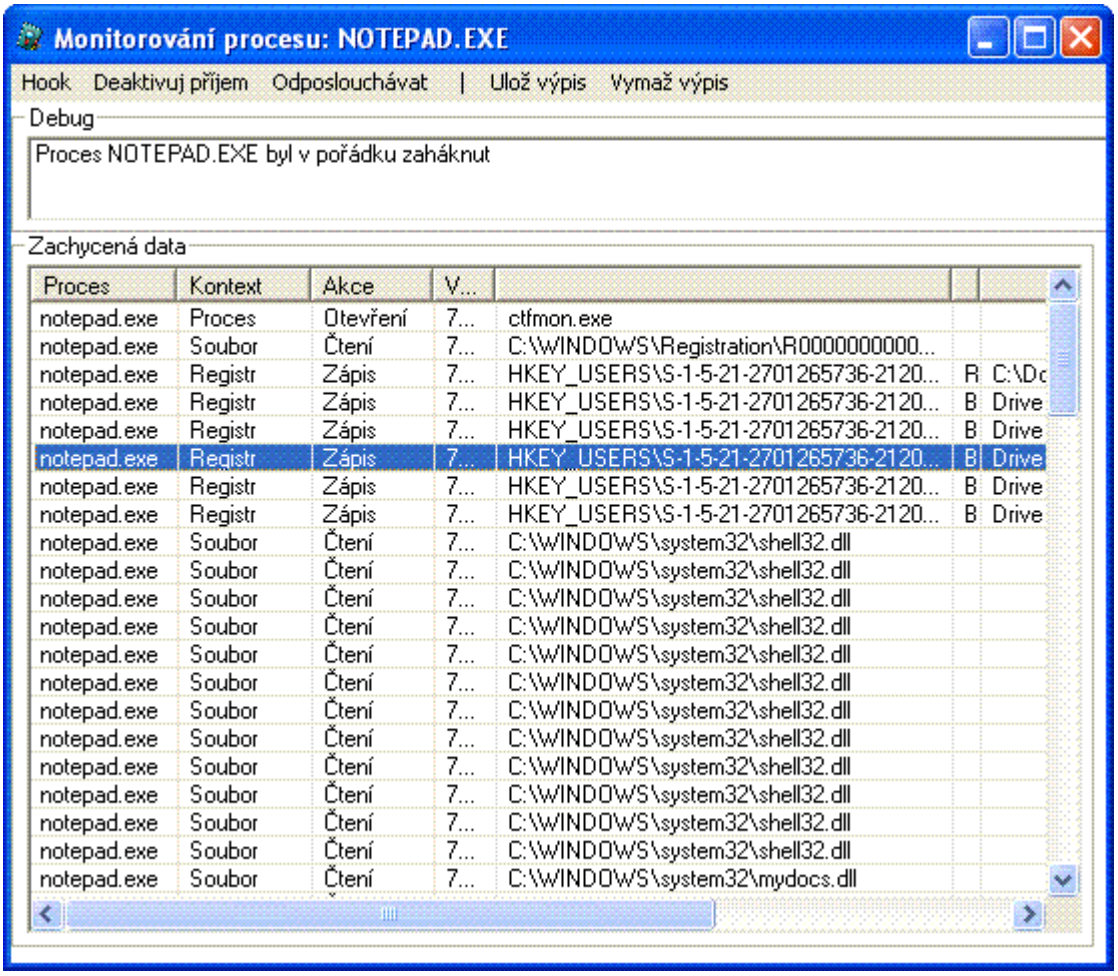
- IAT Scan – je testována tabulka IAT, zda-li ukazatele ukazují do správného modulu. Pokud ne, je nález vypsán. Díky Windows API Forwarding obsahuje kernel32.dll a některé ostatní knihovny v IAT ukazatele, které ukazují přímo na ekvivalenty dané funkce v ntdll.dll.

Tip: stisknutím klávesy Enter ve všech informačnách listboxech je jejich obsah uložen do schránky.

## 1.5 Registrovat

Zaregistruje označený proces. Více v kapitole Scanner.

## 1.6 Monitorování



Proces NOTEPAD.EXE byl v pořádku zaháknut

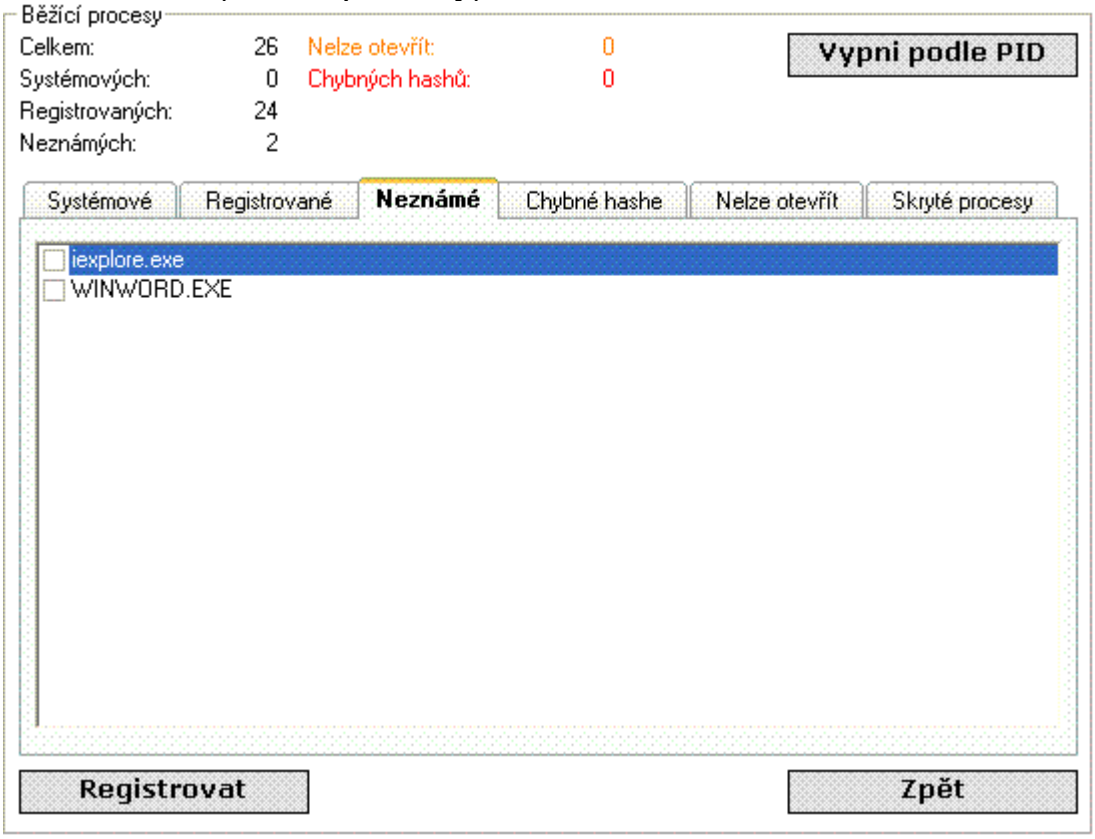
| Proces | Kontext | Akce | V... | | | |
|---|---|---|---|---|---|---|
| notepad.exe | Proces | Otevření | 7... | ctfmon.exe | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\Registration\R0000000000... | | |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | R | C:\D |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | B | Drive |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | B | Drive |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | B | Drive |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | B | Drive |
| notepad.exe | Registr | Zápis | 7... | HKEY_USERS\S-1-5-21-2701265736-2120... | B | Drive |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\shell32.dll | | |
| notepad.exe | Soubor | Čtení | 7... | C:\WINDOWS\system32\mydocs.dll | | |

Okno je přístupné z Menu, tlačítkem Monitorování. Monitorování slouží jako specializovaný API monitor, který je schopen odposlouchávat práci se soubory (zápis, čtení), s registry (nastavení hodnoty) a práci s procesy (OpenProcess, CreateRemoteThreadEx, ReadProcMem, WriteProcMem). Odposlechnuté volání těchto funkcí zobrazí do tabulky s detaily, jako je adresa, odkud byla daná funkce v procesu volána a s jakými parametry.

- Odposlouchávat – zde si můžete zvolit, které akce budete odposlouchávat.
- Hook – klikněte pro zahájení monitorování (odposlechu)
- Aktivuj / deaktivuj příjem – aktivuje nebo deaktivuje zapisování výsledků monitorování do výpisu.

*API jsou hákovány pomocí způsobu detour.*

## 1.7 Scanner (Běžící procesy)




Scanner je přístupný z hlavního menu - Běžící procesy, nebo tlačítkem pod seznamem procesů. Úkolem scanneru je zobrazit procesy, které jsou registrované jako systémové, registrované a neznámé. Zde můžete procesy také hromadně registrovat, odregistrovat nebo případně přeregistrovat.

### 1.7.1 Rozdělení procesů

V UPM můžete procesy rozdělit do tří hlavních skupin a dvou podskupin.

- Systémové – systémové procesy jsou hlavní kritickou součástí Windows. Pokud je proces takto označený, není možné jej vypnout nebo zničit. Pokud žádné omezení nechcete, přečtěte si na konci kapitoly „Editace databáze procesů“.
- Registrované – registrovaný proces určuje sám uživatel a určuje tak důvěru k danému procesu. Registrace nového procesu, nebo jeho odregistrace se provádí v hlavním okně Scanneru. Takto registrovaný proces lze vypnout, ale nejde zničit.
- Neznámé – neznámé procesy, které nejsou registrovány

**CHYBNÉ HASHE**

Registrace a následná kontrola procesu jen dle jména není příliš vhodná. UPM tak kontroluje i takzvané hashe. Hash je kontrolní součet, který by měl být unikátní pro daný soubor. Při jakékoliv změně v souboru se tak změní i jeho hash. Pokud je tedy nějaký z procesů označen

jako Chybný hash!, byl změněn jeho binární obsah. Což vždy **nemusí znamenat virovou nákazu!** Může se jednat pouze o novou verzi programu, případně jinou modifikaci. Každopádně je nutné být obezřetný. Stejně tak chybný hash u systémového procesu nemusí znamenat nic špatného, všechny přednastavené hashe v databázi pochází z Windows XP Professional Service Pack 2 CZ.

**Editace databáze procesů**
Seznam registrovaných procesů je v textovém souboru proc.db, který se nachází u exe souboru upm.exe. Stačí jej o tevřít např. v Poznámkovém bloku.

Záznam je tvořen v tomto tvaru:
[značka]=[jméno procesu]:[hash];

| Značka | Smysl |
|---|---|
| U | proces je USER – registrovaný uživatelem |
| S | proces je SYSTEM – registrovaný jako systémový |

Pokud chcete přidat proces jako systémový, zaregistrujte jej a následně upravte značku U na S. Pokud chcete ze systémového udělat uživatelský, stačí přepsat S na U.

### 1.7.2 Další dělení procesů

- **Nelze otevřít** – nastává v případě, kdy proces nejde „otevřít“ (OpenProcess) s právy PROCESS_ALL_ACCESS. Pokud je vše v pořádku, zde by **neměl být uveden žádny proces.** Pokud zde uvedeny nějaké procesy jsou, poukazuje to na problémy s právy přístupu. Je-li v Úvodní obrazovce u položky Debug privilegia napsáno „V pořádku nastavena“, s největší pravděpodobností je systém nakažen virem. Pokud je u Debug privilegií napsána chyba, jedná se o nedostatečná práva přihlášeného uživatele.
- **Skryté procesy –** v dnešní době je na internetu i mnoho virů, které se umí schovat ze standardních výpisů. Tento scanner se pokusí tyto skryté procesy najít. *Podotýkám, že se jedná o metody použité v Ring3, proto nemusí odhalit všechny skryté procesy.* Tento výpis by měl být prázdný.

Dělení procesů a nedovolené akce s nimi jsou dále používány pod označením „politika procesů UPM“.

## 1.8 Strom procesů

Stromový výpis běžících procesů.
Tip: použijte pravé tlačítko pro více akcí

## 1.9 Další nástroje

- Uložit log – vytvoří ucelený výpis ze zadaných položek v Další nástroje do textového souboru

### 1.9.1 Po spuštění

Zobrazení všech programů a modulů, které jsou spouštěny / nahrávány po spuštění systému a dalších klíčů, jako jsou například Toolbary prohlížeče Internet Explorer, BHO (Browser Helper Objects), atd.

- Smaž hodnoty – smaže z registru zaškrtlé hodnoty
- Smaž i soubory – smaže hodnoty a k nim přiřazený soubor, pokud proces, kterému náleží spustitelný soubor běží, UPM se jej pokusí vypnout.

Vypínání a mazání procesů, souborů podléhají politice procesů UPM.

| Ikonka | Smysl |
|---|---|
|  | Uvedený výrobce souboru je Microsoft |
|  | Soubor je registrován uživatelem |
|  | Soubor má uvedeného výrobce |
|  | Soubor je registrován, ale neodpovídá hash |
|  | Soubor nemá uvedeného výrobce |

### 1.9.2 Služby

Zobrazení služeb a akce s nimi.

### 1.9.3 Ovladače

Zobrazení aktuálně nahraných ovladačů

### 1.9.4 Operační paměť

Velice užitečná věc, kterou jsem vytvořil přímo pro potřeby odstranění DLL virů z paměti systému.
UPM vypíše po kliknutí na tlačítko Zjistit všechny DLL knihovny, které jsou načteny ve všech běžících procesech. Následně s nimi můžete pomocí pravého tlačítka provádět různé akce.

- Najít v dalších procesech – viz bod 1.9.5 Hledání DLL

### 1.9.5 Hledání DLL

Tento modul spolupracuje s modulem Operační paměť. Po zadání jména a kliknutí na tlačítko Najít zobrazí UPM všechny procesy, ve kterých je DLL načtena.

- Uvolni – uvolní DLL knihovnu z paměti procesu (FreeLib)
- Přesunout – přesune soubor DLL knihovny do zadané cílové složky
- Přejmenuj – přejmenuje soubor DLL knihovny
- Smazat – uvolní ze všech procesů danou knihovnu a smaže ji

UPOZORNĚNÍ: Pokud byla nalezena knihovna i v procesu csrss.exe, její uvolnění, případně i smazání způsobí BSOD (modrou obrazovku) a restart systému. Proto v tomto případě raději použijte Přejmenuj a restartujte počítač manuálně.

### 1.9.6 Blokace

Viry a zvláště malware blokují nejrůznější nástroje, jako je třeba regedit, task manager atp. Pomocí tohoto nástroje můžete dané položky opět zpřístupnit. UPM uchovává hodnoty, které by měly být nastaveny, pro jejich aplikaci zvolte Opravit. Tlačítkem Nastavit můžete nastavit vlatní hodnotu. Také je možné tento nástroj použít pro nastavení zákazu (Admin mode).

- Vypnutý Windows Firewall – samozřejmě pokud používáte jiný firewall, tak tuto hodnotu neopravujte.

### 1.9.7 Soubory

Tento modul slouží pro akce se soubory, které jsou otevřeny a používány jiným programem. Například mazání souborů, přejmenování, kopírování, výpis procesů, které s daným souborem pracují atd.

### 1.9.8 Skript

Pro jednodušší práci na dálku umožňuje UPM i použití skriptovacího jazyka, který dovolí některé akce dostupné v UPM.

Vždy aktuální seznam příkazů najdete na domovské stránce www.lodusweb.net v sekci UPM.

## 1.10 Okna

Následující funkce se vztahují k oknu, které bylo vybráno křížkem (chyťte křížek a pusťte ho na objekt, se kterým chcete pracovat), nebo ručně zadaným hWnd (v decimálu, hexadecimální tvar musí začínat 0x nebo končit h).

- Přístupné – zpřístupnění okna (zašedlá tlačítka atp.)
- Viditelné – nastaví viditelnost okna
- TopMost – okno vždy na popředí
- Popiska – změní titulek okna
- Pozice – změna souřadnic okna
- Přepni – přenese dané okno do popředí

- Heslo pod hvězdičkami – máte-li heslo v textovém poli, které místo písmen uvádí různé znaky, jako například hvězdičky, kolečka, tato funkce Vám heslo ukáže.
- Screenshot – vytvoří Screenshot (fotku daného označeného okna, všechny obrázky z programu v této nápovědě jsou dělány právě touto funkcí). Soubory se screenshoty jsou ukládány do adresáře s UPM ve složce s názvem screenshoty.
- Průhlednost okna – nastaví průhlednost okna

### 1.10.1 Neviditelná okna

Zde je možné projít všechna neviditelná okna náležícím všem procesům, popřípadě jen označenému. Dvojklikem na položku budete přepnuti do karty Prvky, kde okno můžete zviditelnit.

## 1.11 Spustit

Rozšířené spouštění souborů a procesů.

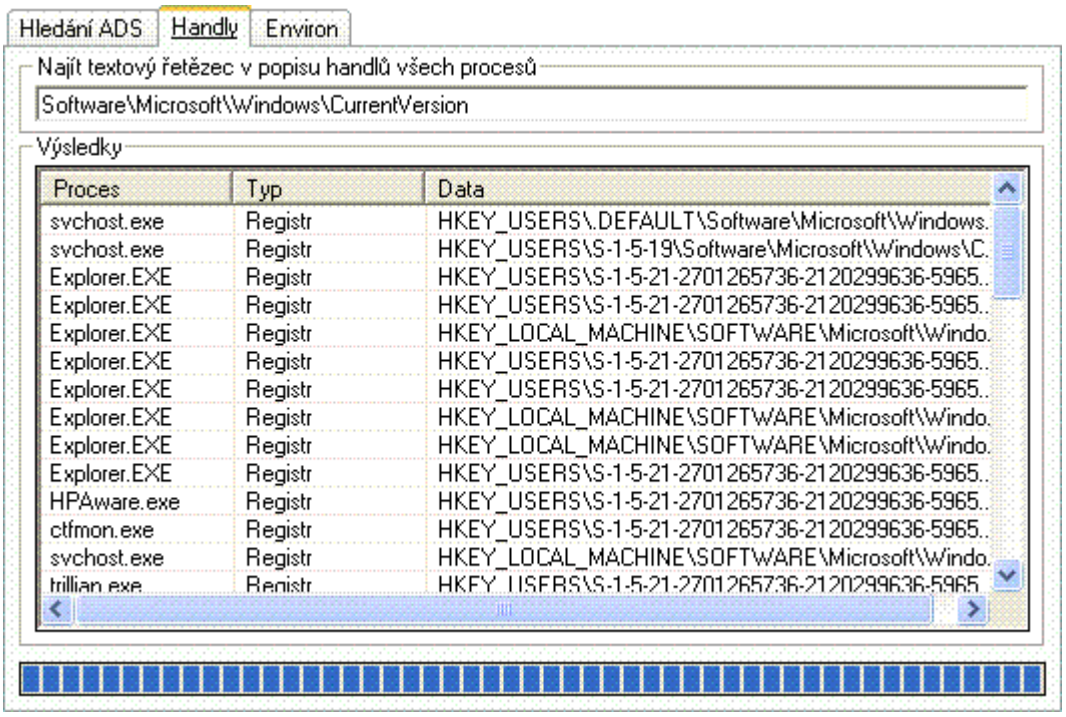
## 1.12 ADS, Systém

### 1.12.1 ADS – Alternate Data Stream

Vyhledává na zadaném disku ADS. Více o ADS se můžete dozvědět zde:
http://www.lodusweb.net/index.php?option=com_content&task=view&id=74&Itemid=57

### 1.12.2 Handly

Globální hledání handlů ve všech procesech. Chceme například zjistit, který proces chodí do registru „Software\Microsoft\Windows\CurrentVersion“, tak si je necháme najít.




### 1.12.3 Environment

Zatím jen výpis Environmentálních proměnných systému

### 1.12.4 Zástupci „Spustit...“

Výpis a možná editace zástupců, které používá systém pro snadnější spouštění aplikací.

## 1.13 MD5 Souborů

Tato funkce Vám umožní hromadnou kontrolu dat s vysokou přesností hashovacího algoritmu MD5.

## 2.0 Všeobecné tipy pro UPM

- ve většině nabídek a oken je možné používat kontextová menu – pravým tlačítkem myši
- nabídky a výpisy (např. Po spuštění, ...) se dají obnovovat klávesou F5
- **ukázáním na daný objekt zobrazíte možné klávesové zkratky!**

## 3.0 Časté problémy s viry a jejich řešení pomocí UPM

### Dva hlídající se procesy

Popis: Proces A hlídá proces B a naopak. Při vypnutí jednoho z nich ho ten druhý opět zapne.

UPM umožňuje několik postupů:

1) oba procesy můžete zmrazit a následně je vypnout
2) jeden z procesů můžete přejmenovat a pak jej vypnout
3) jednomu z procesů můžete odebrat schopnost Spouštět další procesy

### Vir si obnovuje klíč po spuštění

Popis: Vir po smazání hodnoty Po spuštění  hodnotu zapíše znovu (zapís do Blokací, atd).

Možná řešení:

1) proces viru vypnout / zmrazit
2) procesu odebrat schopnost Zapisovat / přepisovat registry

### Nemám přístup k regedit / task manageru / měnění pozadí

Popis: vir mi zablokoval přístup k výše uvedeným programům / modulům systému
Řešení: Další nástroje -> Blokace, v případě dalších problému s obnovováním blokace viz bod výše.

## 4.0 Závěr

Nezbývá nic víc, než jen dodat hodně štěstí a chladnou hlavu při odstraňování virů.

Pokud by Vám v nápovědě cokoliv chybělo, stačí se obrátit na fórum: http://forum.lodusweb.net v sekci Ultimate Process Manager.

S pozdravem,
Autor programu UPM,
Lodus

http://www.lodusweb.net
email: lodus /at/ seznam /./ cz
icq: 17‘80‘50‘881