Bootkity

v teorii a praxi

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

Definice

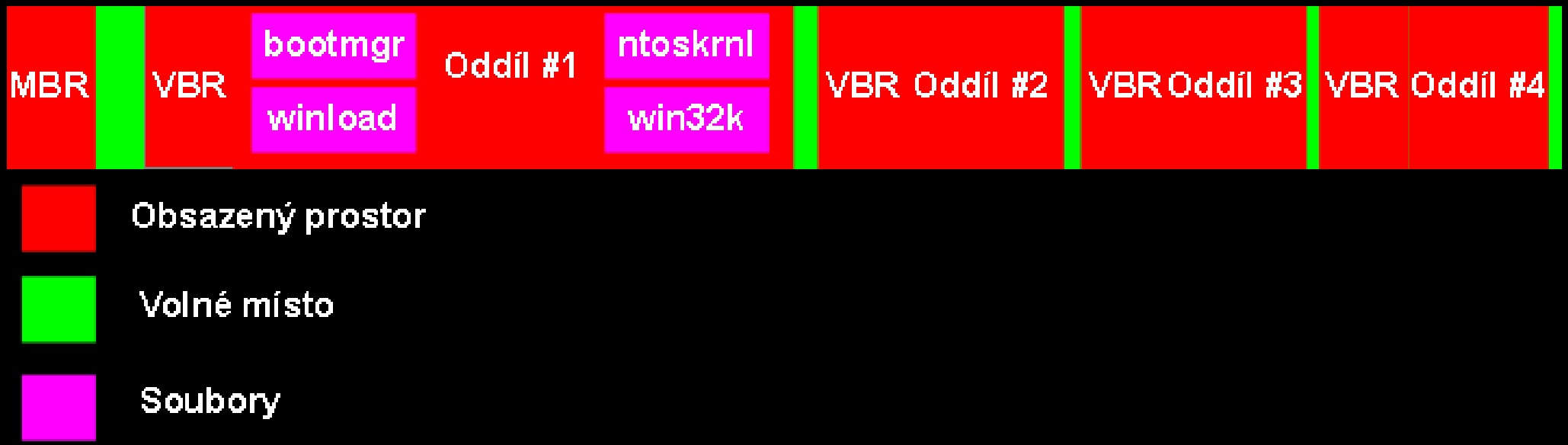
- Pod pojmem **bootkit** budeme rozumět software, který začíná být aktivní během procesu startu počítače ještě před zavedením operačního systému.
- Cílem této přednášky je ukázat, jakým způsobem může bootkit přežít zavedení operačního systému až do doby, kdy se může začít chovat jako standardní ovladač.
- Zajímá nás hlavně bootování s podporou BIOSu, (U)EFI ponecháme stranou.

Obsah

- Struktura (pevného) disku
- Důležité entity z pohledu startu Windows
- Implementace bootkitu
- Praktická ukázka

Struktura disku

- MBR = Master Boot Record
- VBR = Volume Boot Record
- Volné místo se obvykle nachází mezi MBR a prvním oddílem, mezi oddíly a na konci disku. To je pro bootkity velmi důležitá skutečnost



Master Boot Record

- **Cíl:** najít oddíl, ze kterého má být spuštěn operační systém, a předat mu řízení
- **Velikost:** 512 B (Windows)
- **Prostředí:** 16bitové (reálný režim procesoru)
- **Obsah:** kód, chybové hlášký, 64 B tabulka oddílů (16 B na každý), 2 B značka konce
- **Umístění:** první sektor disku
- **Další funkce:** řadič klávesnice, TPM

Volume Boot Record

- **Cíl:** najít, načíst a spustit **bootmgr**
- **Velikost:** 512 B – 4 KB
- **Prostředí:** 16bitové (reálný režim procesoru)
- **Obsah:** kód, důležité informace pro souborový systém
- **Umístění:** první sektory oddílu
- Konkrétní podoba VBR závisí na souborovém systému, kterým je oddíl formátován

Bootmgr

- **Cíl:** dostat se do 64bitového režimu a předat štafetu programu **winload.exe**
- **Velikost:** stovky KB
- **Prostředí:** 16bitové, 32bitové, 64bitové
- **Obsah:** kód a data (**startup.com** + **bootmgr.exe**)
- **Umístění:** kořenový adresář aktivního oddílu. Nesmí být komprimován či šifrován.

Winload.exe

- **Cíl:** načíst hlavní modul jádra a ovladače, které budou v rámci startu OS potřeba
- **Velikost:** stovky kilobajtů
- **Obsah:** standardní PE soubor
- **Prostředí:** 64bitové
- Stejně jako **bootmgr** čte a chová se podle konfigurace uložené v BCD.

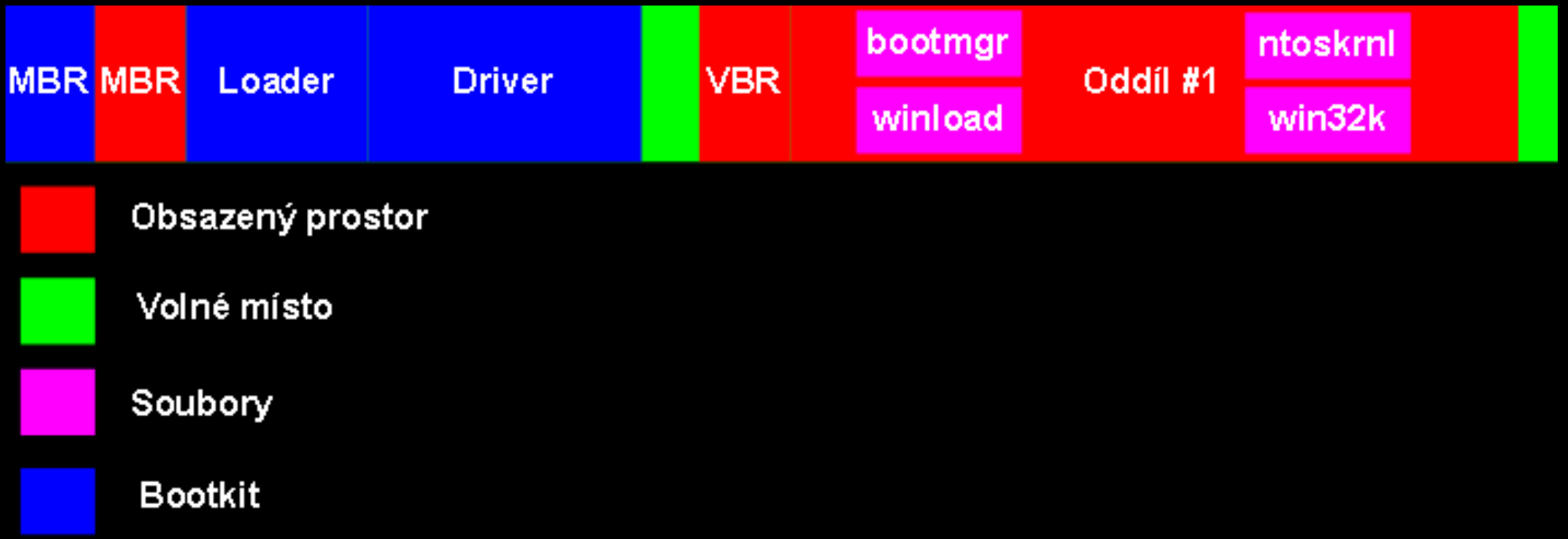
Ntoskrnl.exe & Win32k.sys

- **Ntoskrnl.exe**
  - Implementuje většinu mechanismů, bez kterých se žádný větší OS neobejde (VM, plánování, komunikace s HW, synchronizace, obsluha přerušení)
- **Win32k.sys**
  - Stará se o grafickou stránku celé věci (ne logo a texty zobrazované během bootování)
  - Inicializuje se až těsně před zobrazením modré přihlašovací obrazovky
  - Uvádím jej zde hlavně proto, že v implementaci mého bootkitu hraje významnou roli

Implementace bootkitu

Uložení na disku

- Data bootkitu
  - MBR (512 B)
  - Loader (512 B)
  - Driver (lehce nestandardní PE soubor)

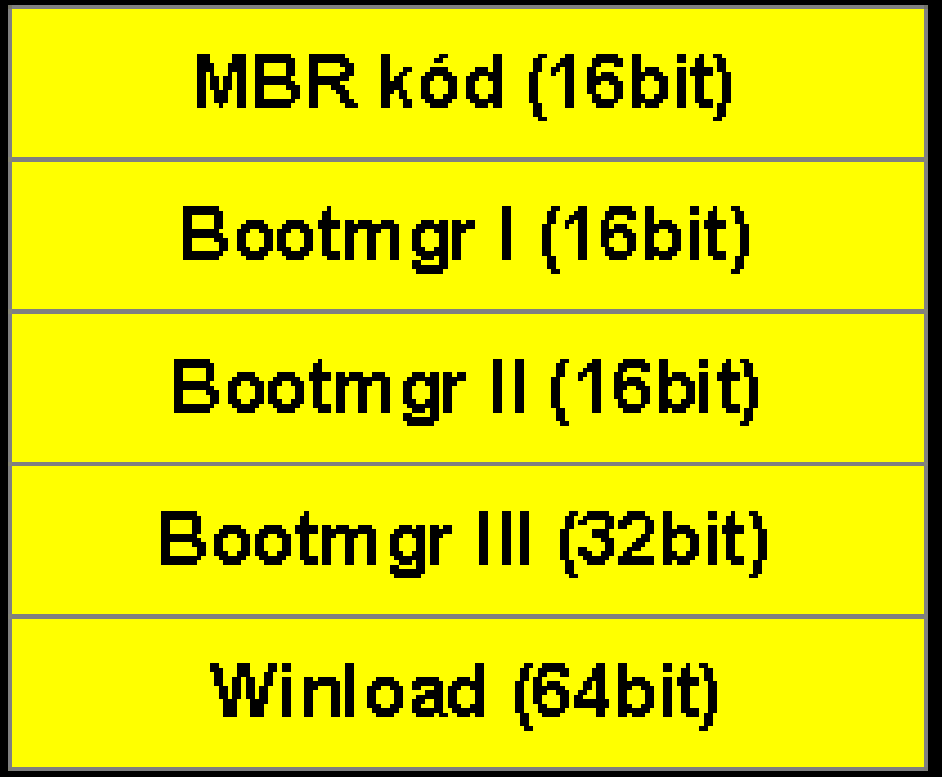


Algoritmus přežití

- Vykonat či emulovat chování originálního MBR
- Monitorovat data čtená z disku
- Při detekci, že se načítá **bootmgr**, **winload.exe** či **ntoskrnl.exe** tyto soubory příslušně modifikovat
- Počkat, dokud není jádro (hlavně **ntoskrnl.exe**) plně inicializováno
- Spustit svůj ovladač, kvůli kterému se celá maškaráda provádí

Master Boot Record

- Relokace
- Modifikovat adresu vektoru 13h, takže se bootkit dozví o každé diskové operaci
- Načíst **Loader**
- Detekovat, že byl o dokončeno čtení souboru **bootmgr** a zkopírovat do něj sekci **Bootmgr I**
- Spustit originální MBR



Bootmgr

- Bootmgr se nachází na známé a pevné fyzické adrese
- Sekce **Bootmgr I** je vykonána v 16bitovém režimu v momentě, kdy je **bootmgr.exe** již dekódován. Předá řízení sekci **Bootmgr II**.
- **Bootmgr II** zajistí přesměrování na **Bootmgr III** v čase, kdy se již bude **winload.exe** nacházet v paměti (řčekání na winload)
- **Bootmgr III** najde v paměti **winload.exe** a přesměruje funkci **OslArchTransferToKernel** na sekci **Winload** (přežití změny režimu)

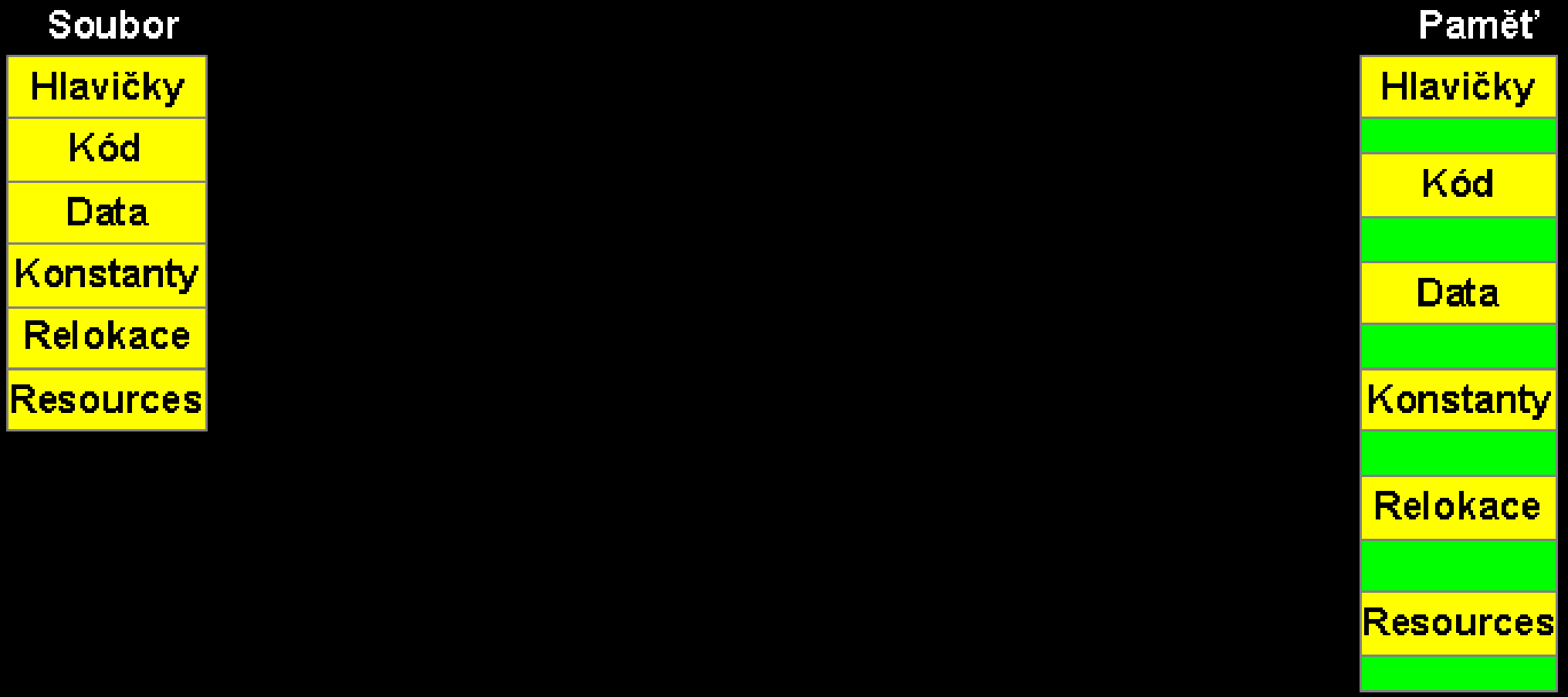
Winload

- Konečně 64bitové prostředí
- Kód je vyvolán těsně před rutinou **OslArchTransferToKernel**, v jednom z registrů je adresa KiSystemStartup z ntoskrnl.exe
- Nalezena adresa počátku **ntoskrnl.exe**
- Předáno řízení sekci **Winload** komponenty **Loader**
  - Do MBR se mi ten kód už nevešel
- Stále není zapnuto stránkování
  - Bylo vypnuto v sekci **Bootmgr III**

Loader

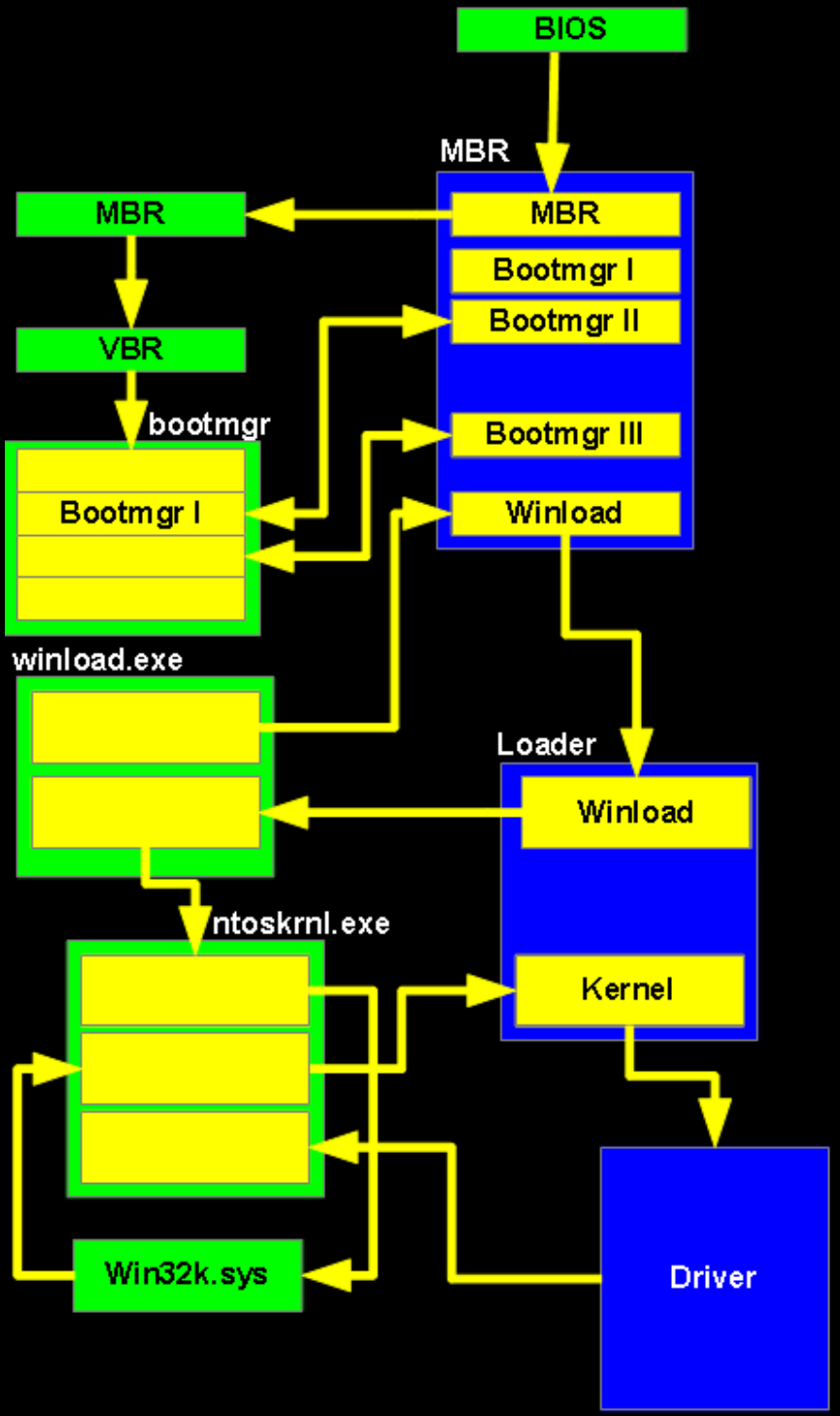
- **Winload**
  - Překopíruje sekci **Kernel** do mezery mezi sekcemi namapovaného souboru **ntoskrnl.exe**
  - Opraví adresy rutin používané v rámci sekce **Kernel**
  - Modifikuje **PsEstablishWin32Callouts**, aby předala řízení sekci **Kernel**
- **Kernel**
  - Alokuje paměť a načte do ní komponentu **Driver**
  - Spustí rutinu **DriverEntry**

Mapování PE souborů



Driver

- Omezení
  - Lze použít pouze funkcí z ntoskrnl.exe
  - Jádro jej nereprezentuje objektem Driver (DRIVER_OBJECT), neb o něm neví
    - Případně je tedy nutné si objekt Driver vytvořit sám (nedokumentováno)
- Postup
  - Provést relokace
  - Nalézt adresy funkcí, které importrtuje
  - Provést libovolný kód


BIOS
MBR
MBR
MBR
Bootmgr I
Bootmgr II
VBR
bootmgr
Bootmgr III
Bootmgr I
Winload
winload.exe
Loader
Winload
ntoskrnl.exe
Kernel
Win32k.sys
Driver

Problémy a zajímavosti

- Neexistuje mnoho dokumentace
  - http://fyyre.ivory-tower.de
- Zeptat se na fóru => budou si myslet, že jste původce všeho zla
- WinDbg lze použít nejdříve v bootmgr
  - Lze použít IDA s Bochs pluginem
- Závislost na aktualizacích a signaturách
- Závislost na rozložení oddílů na disku
- V MBR je opravdu, ale opravdu málo místa

Instalace

- Postup
  - Načíst ntoskrnl.exe a zjistit offesty funkcí, které budou potřeba v rámci sekce **Kernel** komponenty **Loader**
  - Načíst komponentu **Driver**
  - Načíst originální MBR
  - Zapsat vše na disk

Vylepšení přenositelnosti

- Najít signatury v bootmgr a winload.exe platné pro více platforem
- Nepoužívat pevné offsety v bootmgr, ale signatury platné pro více platforem
- Vyhledávat offsety funkcí ntoskrnl.exe na lepším místě, než je instalace bootkitu
- Při instalaci automaticky najít volné místo o dostatečné rozloze, neumisťovat kód jen před první sektor. Upravit MBR dle umístění dalších komponent
- Prozkoumat Windows XP/Server 2003/8

???

- **E-mail:** martin.drab@email.cz
- **ICQ:** 332970040
- **Jabber:** vrtule@jabber.cz
- **WWW:** http://www..jadro-windows.cz

Závěr