

```
kd> db 83322020 83322020+25c
83322020 03 00 20 00 00 00 00 00-28 20 32 83 28 20 32 83 .. .. ( 2. ( 2. 00 00 00 00 00 00 *SYSTEM#.....
83322030 30 20 32 83 30 20 32 83-00 e5 47 1f 00 00 00 00 0 2.0 2...G..... 00 00 00 00 00 00 7.....
83322040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .. 4c b6 26 75 20 06 .....L.&u .
83322050 ac 20 00 00 00 00 00 00-29 00 00 00 01 00 00 00 : .....). .... 00 00 00 00 00 00 .d2.....
83322060 60 20 32 83 60 20 32 83-00 00 00 00 00 00 00 00 ` 2. ` 2..... b1 60 0e 00 00 00 .....
83322070 9c 05 4c 83 9c 05 4c 83-00 00 00 00 01 00 00 00 ..L...L..... 00 00 00 00 00 00 ...
83322080 00 00 00 00 08 24 00 00-00 00 00 0d 01 00 00 00 .....$. .... 00 00 00 00 00 00 .....
83322090 00 00 00 00 00 00 00 00-ad eb 77 48 00 00 00 00 .....wH.... 00 00 00 00 00 00 .....
833220a0 00 00 00 00 00 00 00 00-aa 2a 77 94 60 25 ca 01 .....*w.`%.. 00 00 01 00 00 00 p.....
833220b0 00 00 00 00 00 00 00 00-00 00 00 00 44 09 00 00 .....D... e4 91 c0 1a e4 91 .<.....
833220c0 30 0e 41 83 30 3e 3c 83-60 09 00 00 50 6d 01 00 0.A.0><.`...Pm.. 00 00 00 00 00 00 .....
833220d0 5c 02 00 00 00 70 19 00 00-80 cb 01 00 80 03 00 00 \...p..... 00 00 00 00 00 00 .....
833220e0 5c 02 00 00 00 e0 bc 03-00 f0 f9 02 5c 0e 41 83 \.....\A. 00 00 00 00 00 00 ....x:
833220f0 5c 3e 3c 83 00 00 00 00-e0 fc 2d 83 90 72 ea 91 \><.....-r.. 00 00 00 00 00 00 ....<
83322100 23 3a e9 91 f3 07 01 00-00 00 00 00 00 00 00 00 #:..... 00 00 00 00 00 00 .....
83322110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322120 15 01 00 00 00 00 00 00-00 f5 42 ff 00 00 00 00 .....B..... 00 00 00 00 00 00 .....
83322130 28 bd e9 91 00 00 6f 4a-98 d4 39 83 00 00 00 00 (. ....o]..9..... 00 00 01 00 00 00 .....
83322140 1c 00 00 00 04 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322150 00 00 00 00 38 37 83 8e-00 00 00 00 00 f0 fd 7f .....87..... 00 00 00 00 00 00 .....
83322160 00 00 00 00 00 00 00 00-00 a0 bf .....cmd. 00 00 00 00 00 00 .....
83322170 65 78 65 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
```

Rootkitek

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2560`94772
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_RUNDOWN_REF
+0x09c UniqueProcessId : 0x00000944
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
+0x000 TokenSource : _TOKEN_SOURCE
+0x000 SourceName : "*SYSTEM#"
[00] 42 '*'
[01] 83 'S'
[02] 89 'Y'
[03] 83 'S'
[04] 84 'T'
[05] 69 'E'
[06] 77 'M'
42 '*'
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526`b
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

Előadó:

Barta Csaba

Rövid tartalom

Definíció

Rootkitek rövid története

Felhasználói és kernel mód

Megoldandó problémák

- Driver betöltés
- Verziófüggőség
- Programhiba, debuggolás

Technikák

- DKOM
- Hooking, patching
- Filter driverek

Néhány szó és bevezetés a következő előadáshoz



Definíció

Rootkit:

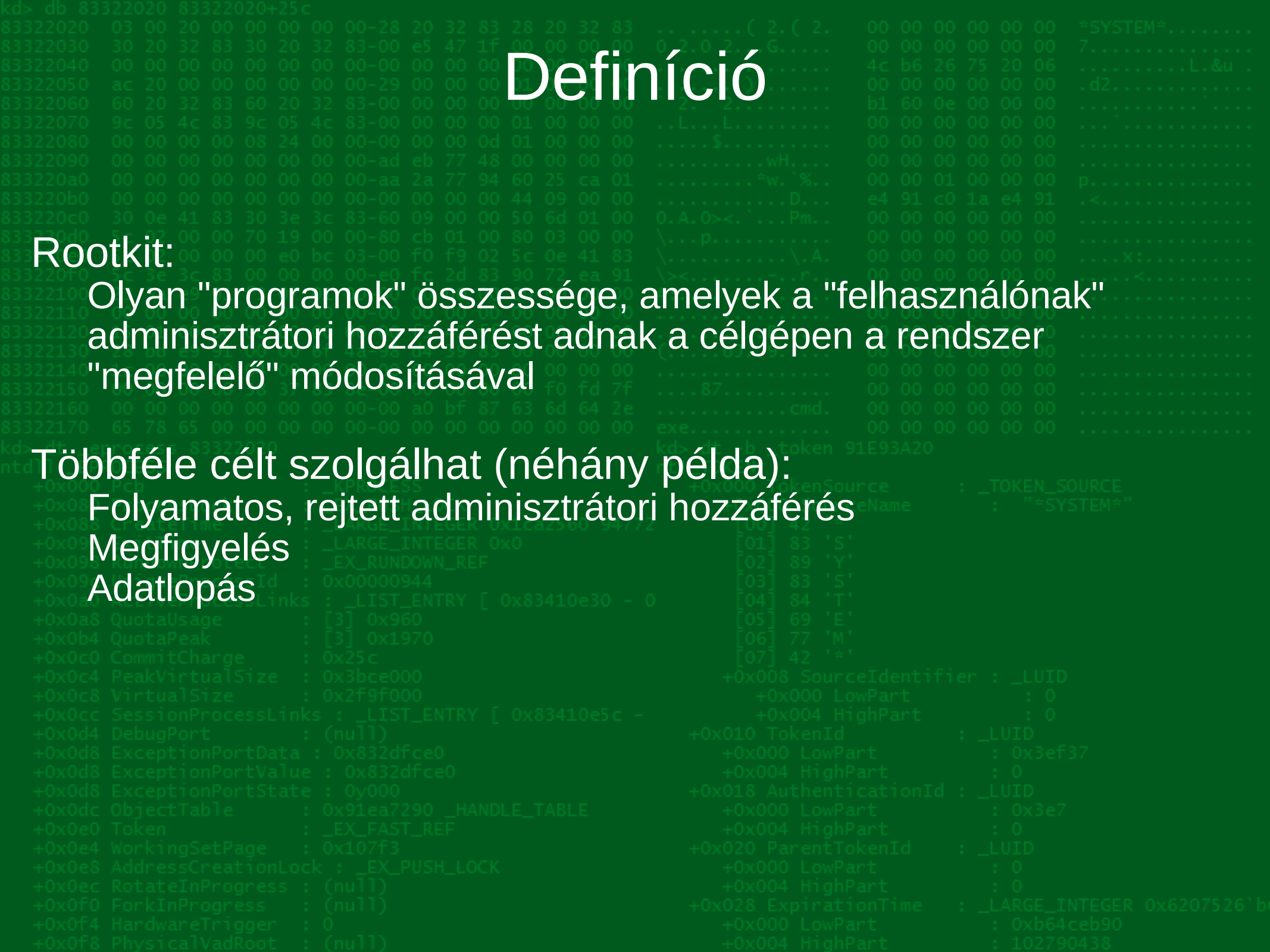
Olyan "programok" összessége, amelyek a "felhasználónak" adminisztrátori hozzáférést adnak a célgépen a rendszer "megfelelő" módosításával

Többféle célt szolgálhat (néhány példa):

Folyamatos, rejtett adminisztrátori hozzáférés

Megfigyelés

Adatlopás



Rootkitek rövid története

Első generációs rootkitek (1990)

- Eredendően módosított adminisztrációs parancsok UNIX-on
- Programokat cserélnék le a rendszeren
- User módban működnek

1990

Az első ismert rootkit /SunOS/ (Lane Davis és Steven Dake)



Rootkitek rövid története

Második generációs rootkitek (1999)

- OS függvényeket módosítanak
 - Hooking
 - Patching
- User és kernel módban működnek

1999

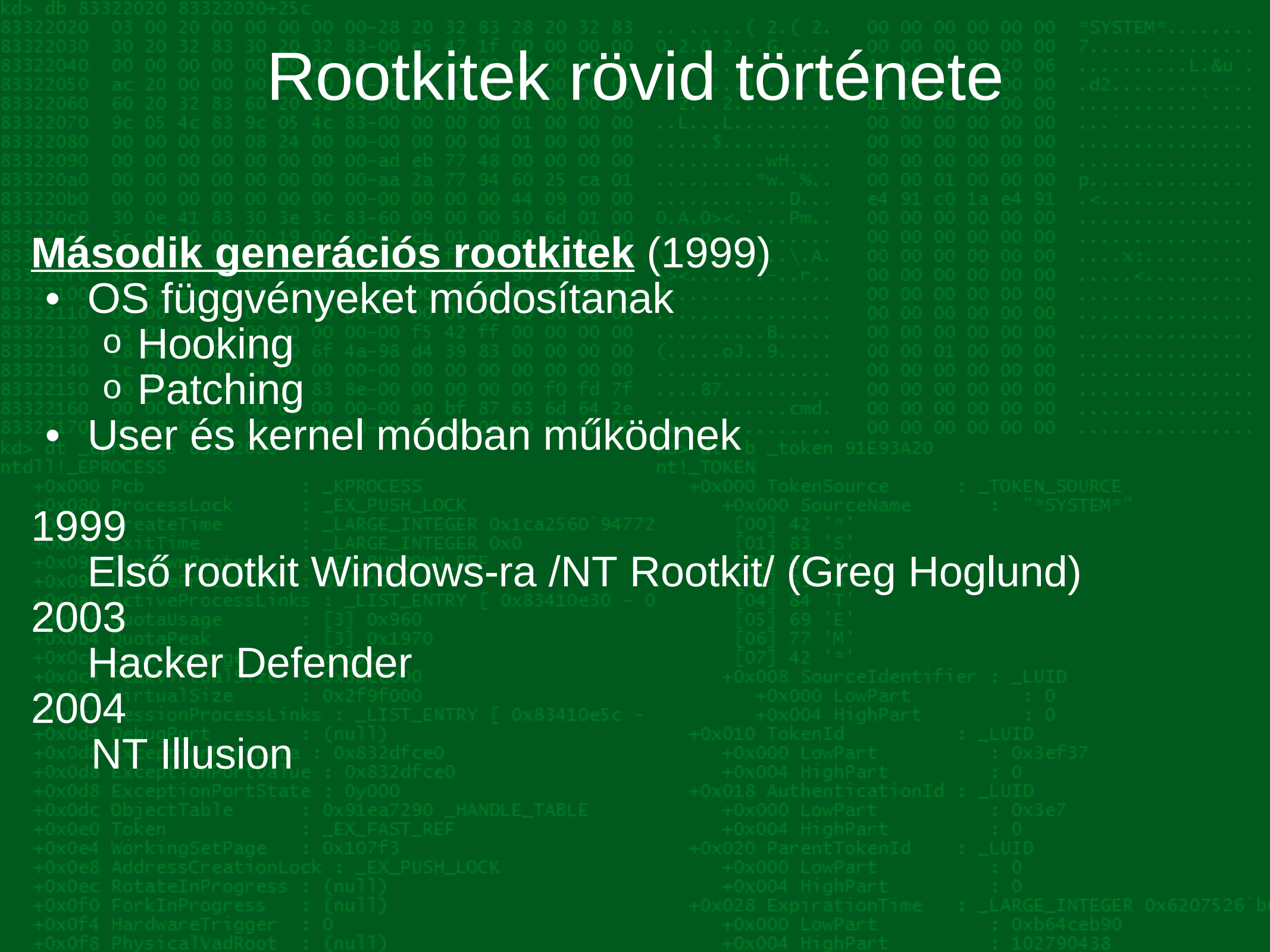
Első rootkit Windows-ra /NT Rootkit/ (Greg Hoglund)

2003

Hacker Defender

2004

NT Illusion



Rootkitek rövid története

Harmadik generációs rootkitek (2004)

- Elsősorban kernel módú rootkitek
- Kernel objektumok módosítása (DKOM)

2004

FU rootkit (Greg Hoglund)

2005

Shadow Walker (James Butler, Sherri Sparks)

2006

FUTo (Peter Silberman)



Rootkitek rövid története

Negyedik generációs rootkitek (2007)

- Virtualizációs rootkitek
- Az OS szempontjából hardver szintű

2007

Bluepill project (Joanna Rutkowska)



Felhasználói és kernel mód

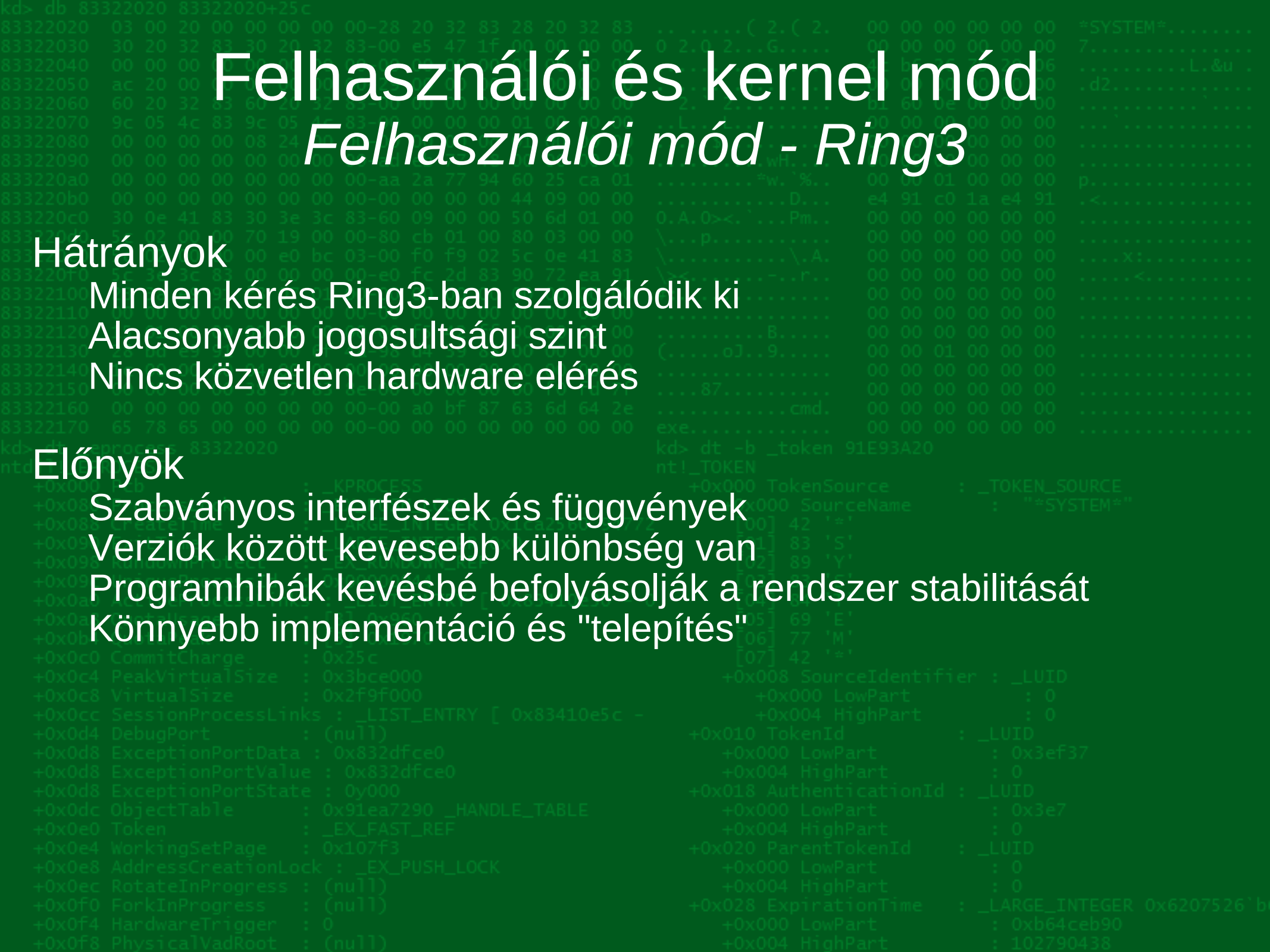
Felhasználói mód - Ring3

Hátrányok

- Minden kérés Ring3-ban szolgálódik ki
- Alacsonyabb jogosultsági szint
- Nincs közvetlen hardware elérés

Előnyök

- Szabványos interfészek és függvények
- Verziók között kevesebb különbség van
- Programhibák kevésbé befolyásolják a rendszer stabilitását
- Könnyebb implementáció és "telepítés"



Felhasználói és kernel mód

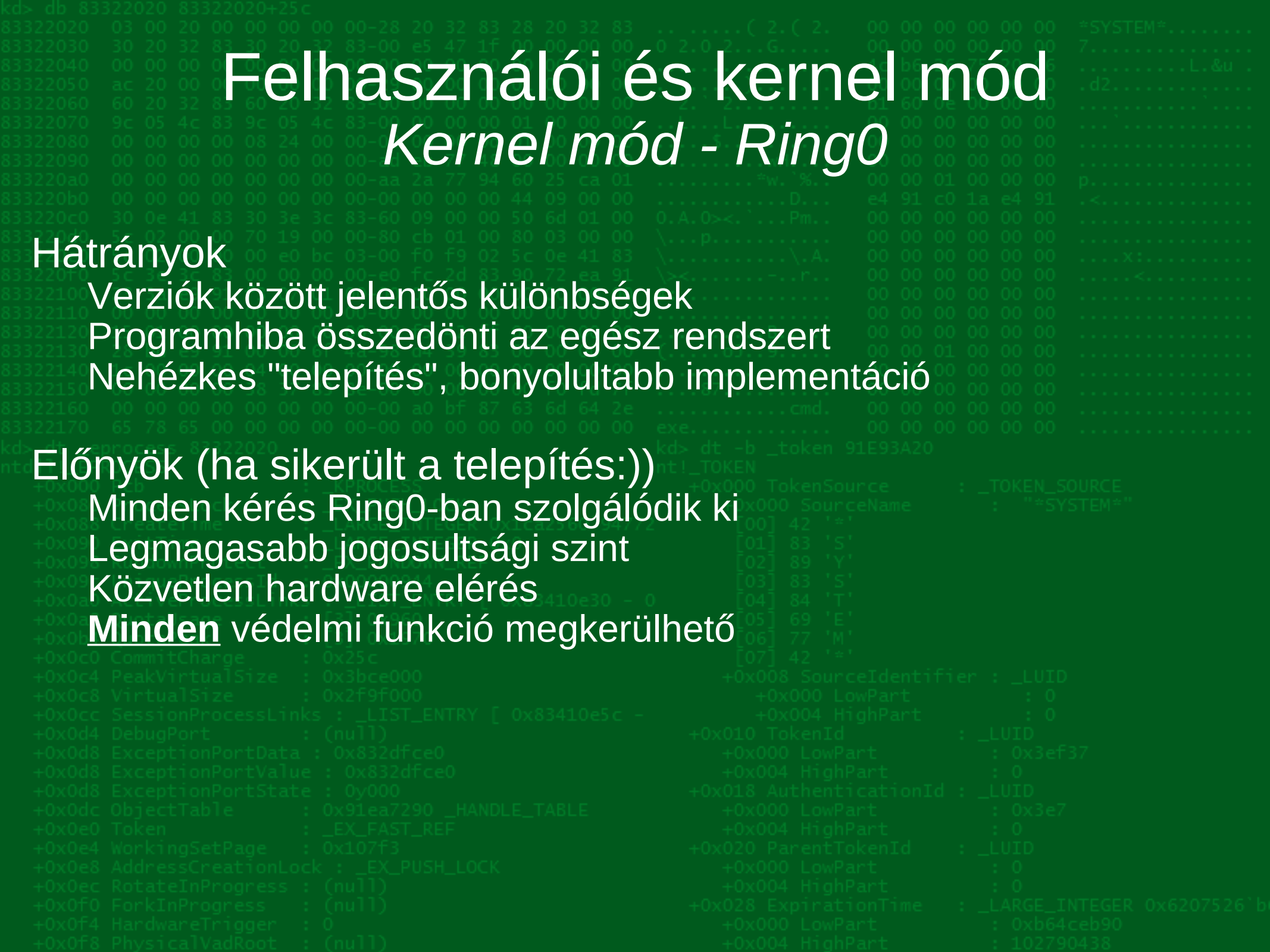
Kernel mód - Ring0

Hátrányok

- Verziók között jelentős különbségek
- Programhiba összedönti az egész rendszert
- Nehézkes "telepítés", bonyolultabb implementáció

Előnyök (ha sikerült a telepítés:))

- Minden kérés Ring0-ban szolgálódik ki
- Legmagasabb jogosultsági szint
- Közvetlen hardware elérés
- Minden** védelmi funkció megkerülhető



Megoldandó problémák

Driver betöltés

- Ahhoz, hogy a rootkit működőképes legyen, a kódnak be kell jutnia a kernel területre (betöltés)
- A driver betöltéshez adminisztrátori jogosultság kell (ez a megfelelő exploit birtokában nem lehet probléma:))
- A betöltésnek két módja van:

1. Service Control Manager (standard, dokumentált)
2. SystemLoadAndCallImage (limitált lehetőségek, nem dokumentált)

```
+0x000 CreateTime : _LARGE_INTEGER 0x1ca2560 94772 [00] 42 '!'
+0x004 UniqueProcessId : 0x00000944 [03] 83 'S'
+0x008 QuotaUsage : [5] 0x960 [04] 84 'T'
+0x00c QuotaPeak : [3] 0x1970 [05] 69 'E'
+0x010 CommitCharge : 0x25c [06] 77 'M'
+0x014 PeakVirtualSize : 0x3bce000 [07] 42 '!'
+0x018 VirtualSize : 0x2f9f000 +0x008 SourceIdentifier : _LUID
+0x01c SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c - +0x000 LowPart : 0
+0x020 DebugPort : (null) +0x004 HighPart : 0
+0x024 ExceptionPortData : 0x832dfce0 +0x010 TokenId : _LUID
+0x028 ExceptionPortValue : 0x832dfce0 +0x000 LowPart : 0x3ef37
+0x02c ExceptionPortState : 0y000 +0x004 HighPart : 0
+0x030 ObjectTable : 0x91ea7290 _HANDLE_TABLE +0x018 AuthenticationId : _LUID
+0x034 Token : _EX_FAST_REF +0x000 LowPart : 0x3e7
+0x038 WorkingSetPage : 0x107f3 +0x004 HighPart : 0
+0x03c AddressCreationLock : _EX_PUSH_LOCK +0x020 ParentTokenId : _LUID
+0x040 RotateInProgress : (null) +0x000 LowPart : 0
+0x044 ForkInProgress : (null) +0x004 HighPart : 0
+0x048 HardwareTrigger : 0 +0x028 ExpirationTime : _LARGE_INTEGER 0x6207526 b
+0x04c PhysicalVadRoot : (null) +0x000 LowPart : 0xb64ceb90
+0x050 : +0x004 HighPart : 102790438
```

Megoldandó problémák

Driver betöltés

Service Control Manager

- Ez a standard módja a driver betöltésnek
- Hátrányok
 - Az eventlogban és registry-ben nyomot hagy
- Előnyök
 - Nonpaged területre töltődik a programkód
 - Nem verziófüggő

SystemLoadAndCallImage

- Nem dokumentált funkció
- Hátrányok
 - Lapozható területre töltődik be a kód => a későbbi elérhetősége nem garantált
 - Verziófüggő
- Előnyök
 - Kevesebb nyomot hagy

Megoldandó problémák

Driver betöltés

Digitális aláírás

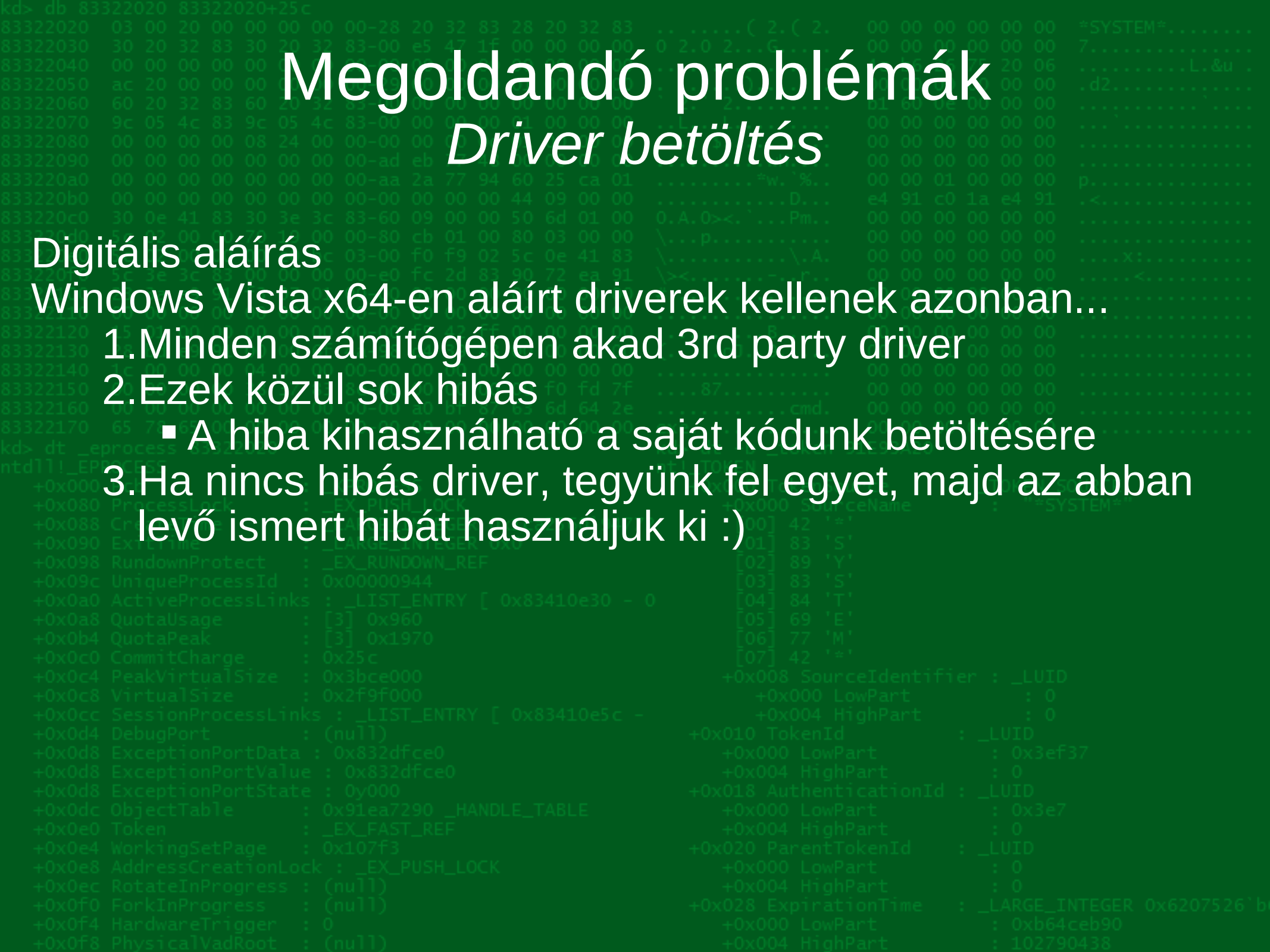
Windows Vista x64-en aláírt driverek kellenek azonban...

1. Minden számítógépen akad 3rd party driver

2. Ezek közül sok hibás

- A hiba kihasználható a saját kódunk betöltésére

3. Ha nincs hibás driver, tegyünk fel egyet, majd az abban levő ismert hibát használjuk ki :)



Megoldandó problémák

Driver betöltés

```
Administrator: Command Prompt - livekd
kd> uf /D SeValidateImageHeader
nt!SeValidateImageHeader:
8282fd1d 8bff      mov     edi,edi
8282fd1f 55        push   ebp
8282fd20 8bec     mov     ebp,esp
8282fd22 803d9c55798200 cmp     byte ptr [nt!g_CiEnabled (8279559c)],0
8282fd29 7520     jne    nt!SeValidateImageHeader+0x2e (8282fd4b) Branch
h

nt!SeValidateImageHeader+0xe:
8282fd2b 6853655068 push   68506553h
8282fd30 6a01     push   1
8282fd32 6a01     push   1
8282fd34 e8724ef4ff call   nt!ExAllocatePoolWithTag (82774bab)
8282fd39 8906     mov     dword ptr [esil,eax]
8282fd3b f7d8     neg     eax
8282fd3d 1bc0     sbb    eax,eax
8282fd3f 25e9ffff3f and    eax,3FFFFFFE9h
8282fd44 05170000c0 add    eax,0C0000017h
8282fd49 eb1f     jmp    nt!SeValidateImageHeader+0x4d (8282fd6a) Branch
h

nt!SeValidateImageHeader+0x2e:
8282fd4b a190557982 mov     eax,dword ptr [nt!g_CiCallbacks (82795590)]
8282fd50 85c0     test   eax,eax
8282fd52 7507     jne    nt!SeValidateImageHeader+0x3e (8282fd5b) Branch
h

nt!SeValidateImageHeader+0x37:
8282fd54 b8280400c0 mov     eax,0C0000428h
8282fd59 eb0f     jmp    nt!SeValidateImageHeader+0x4d (8282fd6a) Branch
h

nt!SeValidateImageHeader+0x3e:
8282fd5b 56        push   esi
8282fd5c ff7514   push   dword ptr [ebp+14h]
8282fd5f ff7510   push   dword ptr [ebp+10h]
8282fd62 ff750c   push   dword ptr [ebp+0Ch]
8282fd65 ff7508   push   dword ptr [ebp+8]
8282fd68 ffd0     call   eax

nt!SeValidateImageHeader+0x4d:
8282fd6a 5d        pop    ebp
```

OURCE
STEM*
37
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526 b
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438

Megoldandó problémák

Verziófüggőség

A kernel belső adatszerkezetei akár service packenként is változhatnak:

- optimalizálás
- hibajavítás
- új funkciók bevezetése

A kernelen belül a driverek számára elérhető API változik:

- új függvények jelennek meg
- egyes függvények megszűnnek
- egyes függvények paraméterezése megváltozik

=> A régebbi verzión működő kód az új verzión be sem töltődik, vagy "kékhalált" okoz

Megoldandó problémák

Verziófüggőség

```
C:\WINDOWS\system32\cmd.exe - livekd
kd> dt _eprocess
ntdll!_EPROCESS
+0x0000 Pcb : _KPROCESS
+0x006c ProcessLock : _EX_PUSH_LOCK
+0x0070 CreateTime : _LARGE_INTEGER
+0x0078 ExitTime : _LARGE_INTEGER
+0x0080 RundownProtect : _EX_RUNDOWN_REF
+0x0084 UniqueProcessId : Ptr32 Void
+0x0088 ActiveProcessLinks : _LIST_ENTRY
+0x0090 ProcessQuotaUsage : [2] Uint4B
+0x0098 ProcessQuotaPeak : [2] Uint4B
+0x009c CommitCharge : Uint4B
+0x00a8 QuotaBlock : Ptr32 _EPROCESS_QUOTA_BLOCK
+0x00ac CpuQuotaBlock : Ptr32 _PS_CPU_QUOTA_BLOCK
+0x00b0 PeakVirtualSize : Uint4B
+0x00b8 VirtualSize : Uint4B
+0x00bc SessionProcessLinks : _LIST_ENTRY
+0x00c0 DebugPort : Ptr32 Void
+0x00c4 ExceptionPortData : Ptr32 Void
+0x00c8 ExceptionPortValue : Uint4B
+0x00cc ExceptionPortState : Pos 0, 3 Bits
+0x00d0 ObjectTable : Ptr32 _HANDLE_TABLE
+0x00d4 Token : _EX_FAST_REF
+0x00d8 WorkingSetPage : Uint4B
+0x00dc AddressCreationLock : _EX_PUSH_LOCK
+0x00e0 RotateInProgress : Ptr32 _ETHREAD
+0x00e4 ForkInProgress : Ptr32 _ETHREAD
+0x00e8 HardwareTrigger : Uint4B
+0x00ec PhysicalVadRoot : Ptr32 _MM_AVL_TABLE
+0x00f0 CloneRoot : Ptr32 Void
+0x00f4 NumberOfPrivatePages : Uint4B
+0x00f8 NumberOfLockedPages : Uint4B
+0x0100 Win32Process : Ptr32 Void
```

Megoldandó problémák

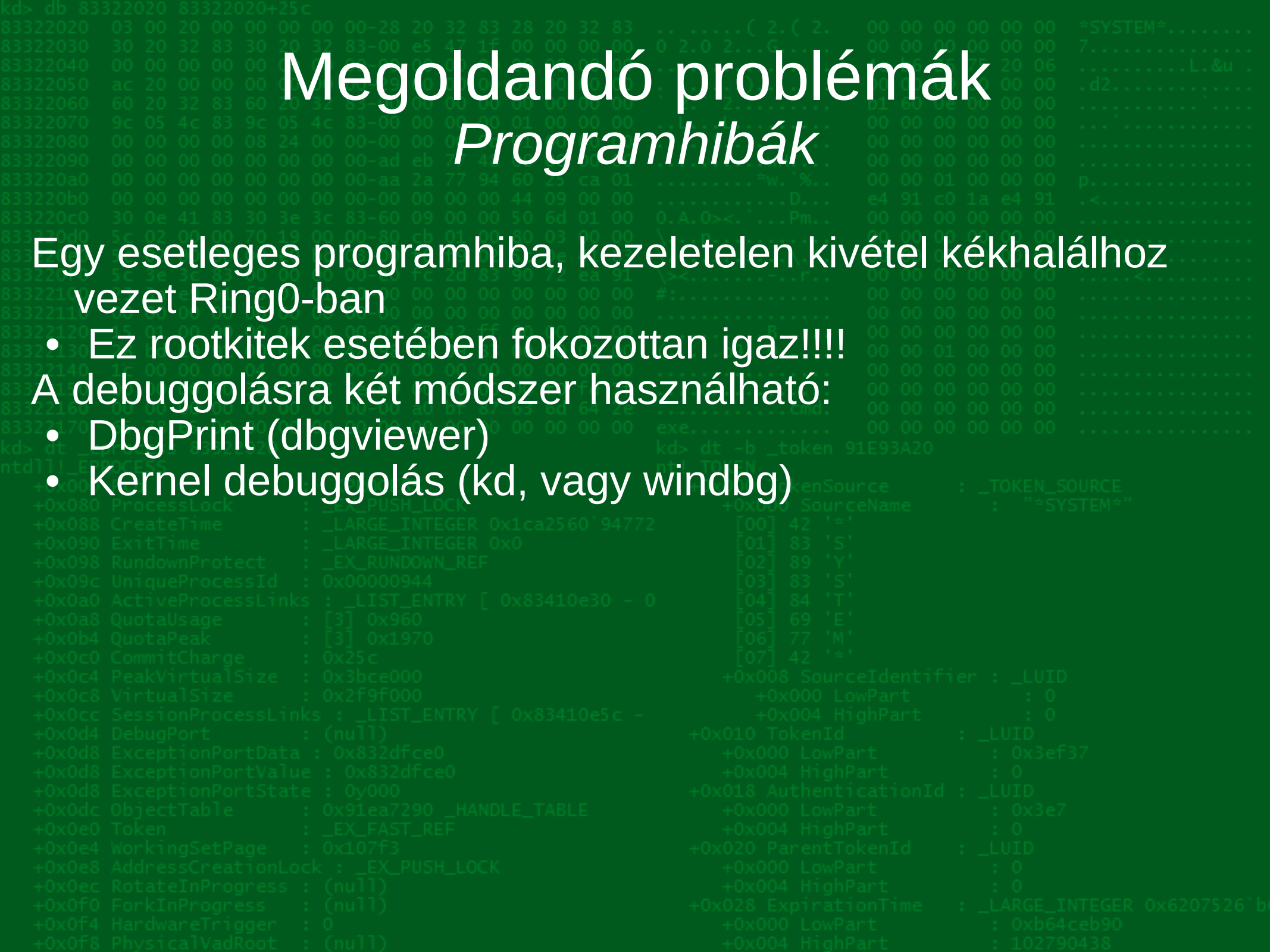
Programhibák

Egy esetleges programhiba, kezeletelen kivétel kékhalálhoz vezet Ring0-ban

- Ez rootkitek esetében fokozottan igaz!!!!

A debuggolásra két módszer használható:

- DbgPrint (dbgviewer)
- Kernel debuggolás (kd, vagy windbg)



Megoldandó problémák

Programhibák

A problem has been detected and windows has been shut down to prevent damage to your computer.

REFERENCE_BY_POINTER

If this is the first time you've seen this stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000018 (0xBAD0B0B0,0x91D28910,0x00000002,0xFFFFFFFF)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 30

Technikák

DKOM

A kernel által kezelt objektumok közvetlen módosítása

Objektumok, amelyeket módosítani szoktak:

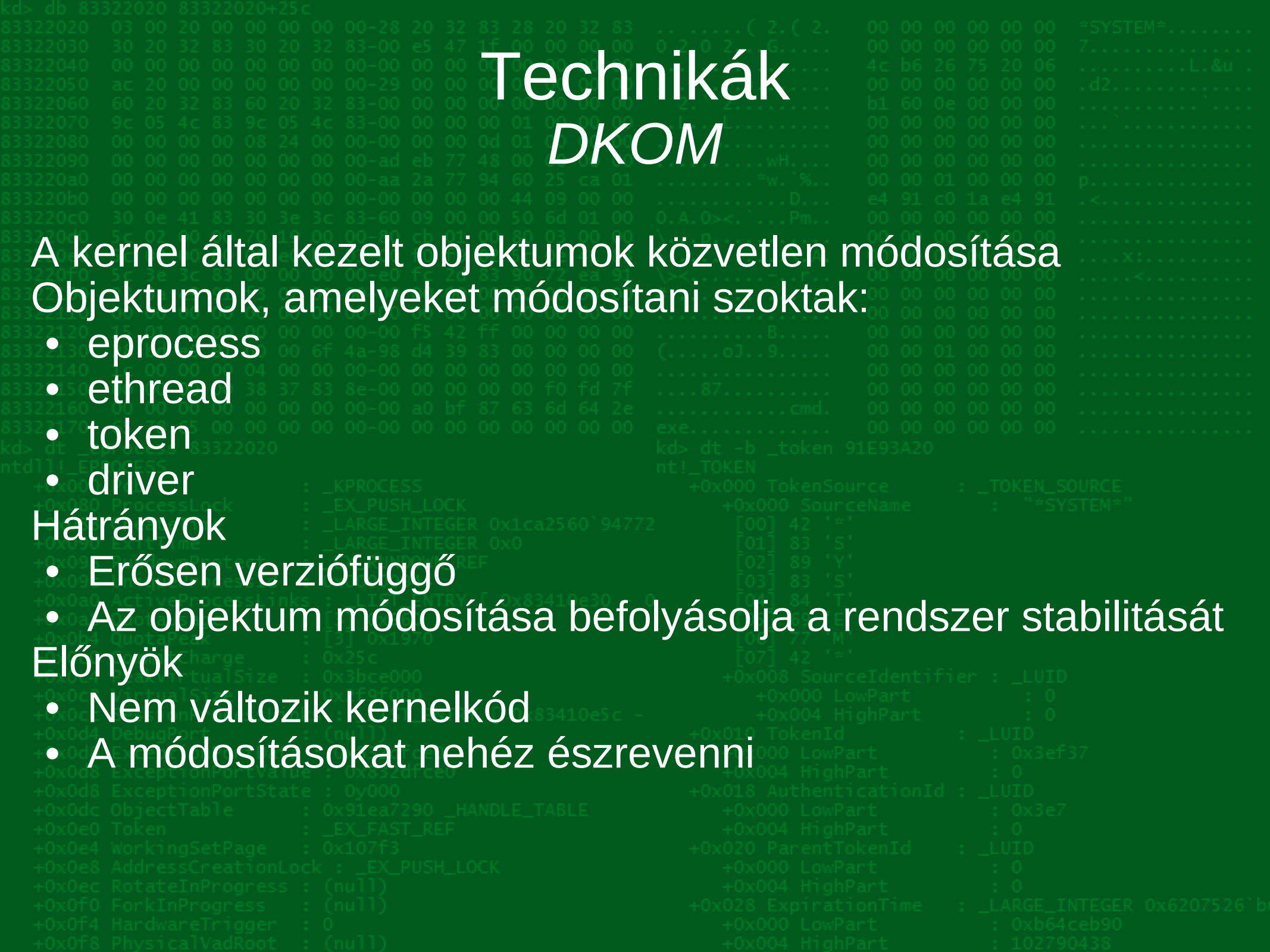
- eprocess
- ethread
- token
- driver

Hátrányok

- Erősen verziófüggő
- Az objektum módosítása befolyásolja a rendszer stabilitását

Előnyök

- Nem változik kernelkód
- A módosításokat nehéz észrevenni

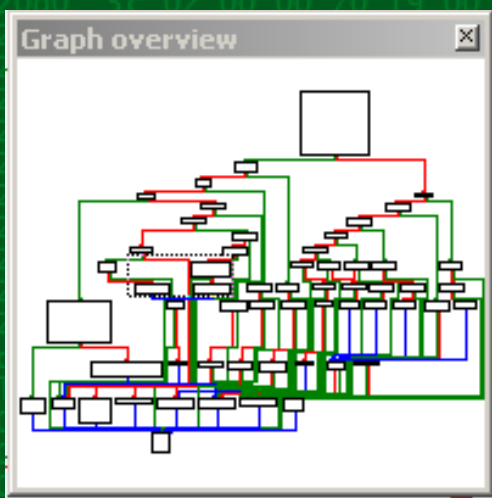


Technikák

DKOM

```
kd> dt _token
nt!_TOKEN
+0x000 TokenSource      : _TOKEN_SOURCE
+0x010 TokenId          : _LUID
+0x018 AuthenticationId : _LUID
+0x020 ParentTokenId   : _LUID
+0x028 ExpirationTime  : _LARGE_INTEGER
+0x030 TokenLock        : Ptr32 _ERESOURCE
+0x034 ModifiedId      : _LUID
+0x040 Privileges       : _SEP_TOKEN_PRIVILEGES
+0x058 AuditPolicy      : _SEP_AUDIT_POLICY
+0x074 SessionId       : UInt4B
+0x078 UserAndGroupCount : UInt4B
+0x07c RestrictedSidCount : UInt4B
+0x080 VariableLength   : UInt4B
+0x084 DynamicCharged   : UInt4B
+0x088 DynamicAvailable : UInt4B
+0x08c DefaultOwnerIndex : UInt4B
+0x090 UserAndGroups    : Ptr32 _SID_AND_ATTRIBUTES
+0x094 RestrictedSids   : Ptr32 _SID_AND_ATTRIBUTES
+0x098 PrimaryGroup     : Ptr32 Void
+0x09c DynamicPart      : Ptr32 UInt4B
+0x0a0 DefaultDacl      : Ptr32 _ACL
+0x0a4 TokenType        : _TOKEN_TYPE
+0x0a8 ImpersonationLevel : _SECURITY_IMPERSONATION_LEVEL
+0x0ac TokenFlags       : UInt4B
+0x0b0 TokenInUse       : UChar
+0x0b4 IntegrityLevelIndex : UInt4B
+0x0b8 MandatoryPolicy  : UInt4B
+0x0bc LogonSession     : Ptr32 _SEP_LOGON_SESSION_REFERENCES
+0x0c0 OriginatingLogonSession : _LUID
+0x0c8 SidHash          : _SID_AND_ATTRIBUTES_HASH
+0x150 RestrictedSidHash : _SID_AND_ATTRIBUTES_HASH
+0x1d8 pSecurityAttributes : Ptr32 _AUTHZBASEP_SECURITY_ATTRIBUTES_INFORMATION
+0x1dc VariablePart     : UInt4B
```

Technikák DKOM



```
call ds:PsGetCurrentProcessId
push eax
call sub_11894
cmp eax, edi
jmp short loc_12250
```

```
push ebp
mov ebp, esp
sub esp, 190h
mov eax, dword_223A0
xor eax, ebp
mov [ebp+var_4], eax
push ebx
mov ebx, [ebp+arg_4]
push esi
push edi
xor esi, esi
push ebx
push offset aSourceProcessId ; "Source processid: %d\n"
mov [ebp+Object], esi
mov [ebp+var_114], esi
mov [ebp+Handle], esi
mov [ebp+NewTokenHandle], esi
mov [ebp+var_10C], esi
call DbgPrint
mov eax, ds:PsProcessType
```

```
push dword ptr [edi]
mov esi, ds:PsGetCurrentProcessId
call esi ; PsGetCurrentProcessId
push eax
call sub_11C08
```

```
+0x0cc SessionProcessLinks : _LIST_ENTRY
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
```

```
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

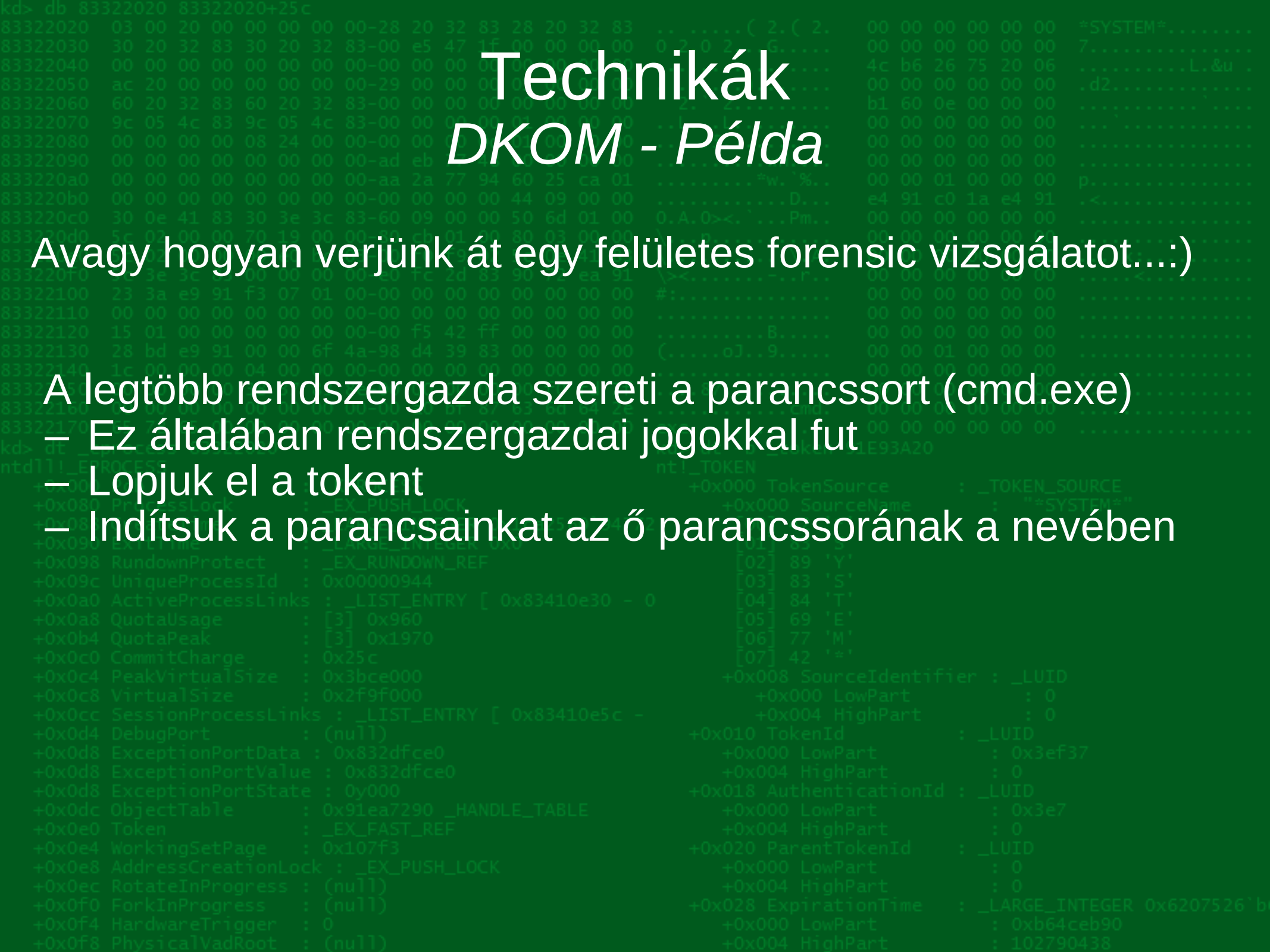
Technikák

DKOM - Példa

Avagy hogyan verjük át egy felületes forensic vizsgálatot...:)

A legtöbb rendszergazda szereti a parancssort (cmd.exe)

- Ez általában rendszergazdai jogokkal fut
- Lopjuk el a token
- Indítsuk a parancsainkat az ő parancssorának a nevében



```
kd> db 83322020 83322020+25c
83322020 03 00 20 00 00 00 00 00-28 20 32 83 28 20 32 83 .. ..( 2.( 2. 00 00 00 00 00 00 *SYSTEM#.....
83322030 30 20 32 83 30 20 32 83-00 e5 47 1f 00 00 00 00 0 2.0 2...G..... 00 00 00 00 00 00 7.....
83322040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 4c b6 26 75 20 06 .....L.&u .
83322050 ac 20 00 00 00 00 00 00-29 00 00 00 01 00 00 00 : .....). ..... 00 00 00 00 00 00 .d2.....
83322060 60 20 32 83 60 20 32 83-00 00 00 00 00 00 00 00 ` 2.` 2..... b1 60 0e 00 00 00 .....
83322070 9c 05 4c 83 9c 05 4c 83-00 00 00 00 01 00 00 00 ..L...L..... 00 00 00 00 00 00 ...
83322080 00 00 00 00 08 24 00 00-00 00 00 0d 01 00 00 00 .....$. ..... 00 00 00 00 00 00 .....
83322090 00 00 00 00 00 00 00 00-ad eb 77 48 00 00 00 00 .....wH.... 00 00 00 00 00 00 .....
833220a0 00 00 00 00 00 00 00 00-aa 2a 77 94 60 25 ca 01 .....*w.`%.. 00 00 01 00 00 00 p.....
833220b0 00 00 00 00 00 00 00 00-00 00 00 00 44 09 00 00 .....D... e4 91 c0 1a e4 91 .<.....
833220c0 30 0e 41 83 30 3e 3c 83-60 09 00 00 50 6d 01 00 0.A.0><.`...Pm.. 00 00 00 00 00 00 .....
833220d0 5c 02 00 00 00 70 19 00 00-80 cb 01 00 80 03 00 00 \...p..... 00 00 00 00 00 00 .....
833220e0 5c 02 00 00 00 e0 bc 03-00 f0 f9 02 5c 0e 41 83 \.....\A. 00 00 00 00 00 00 ....x:.....
833220f0 5c 3e 3c 83 00 00 00 00-e0 fc 2d 83 90 72 ea 91 \><.....-r.. 00 00 00 00 00 00 ....<.....
83322100 23 3a e9 91 f3 07 01 00-00 00 00 00 00 00 00 00 #:..... 00 00 00 00 00 00 .....
83322110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322120 15 01 00 00 00 00 00 00-00 f5 42 ff 00 00 00 00 .....B..... 00 00 00 00 00 00 .....
83322130 28 bd e9 91 00 00 6f 4a-98 d4 39 83 00 00 00 00 (...o3..9..... 00 00 01 00 00 00 .....
83322140 1c 00 00 00 04 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322150 00 00 00 00 38 37 83 8e-00 00 00 00 00 00 00 00 .....fd 7f ..... 00 00 00 00 00 00 .....
83322160 00 00 00 00 00 00 00 00-00 a0 bf 83 63 d6 42 e .....cmd. 00 00 00 00 00 00 .....
83322170 65 78 65 00 00 00 00 00-00 00 00 00 00 00 00 00 .....e..... 00 00 00 00 00 00 .....
```

DEMO

Hamarosan videó formában
<http://hacktivity.hu>

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2560 94772
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_RUNDOWN_REF
+0x09c UniqueProcessId : 0x00000944
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e30 - 0
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
kd> dt -b _token 91E93A20
ntdll!_TOKEN
+0x000 SourceName : _TOKEN_SOURCE
+0x004 SourceName : ""*SYSTEM#"
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526`b
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

Technikák

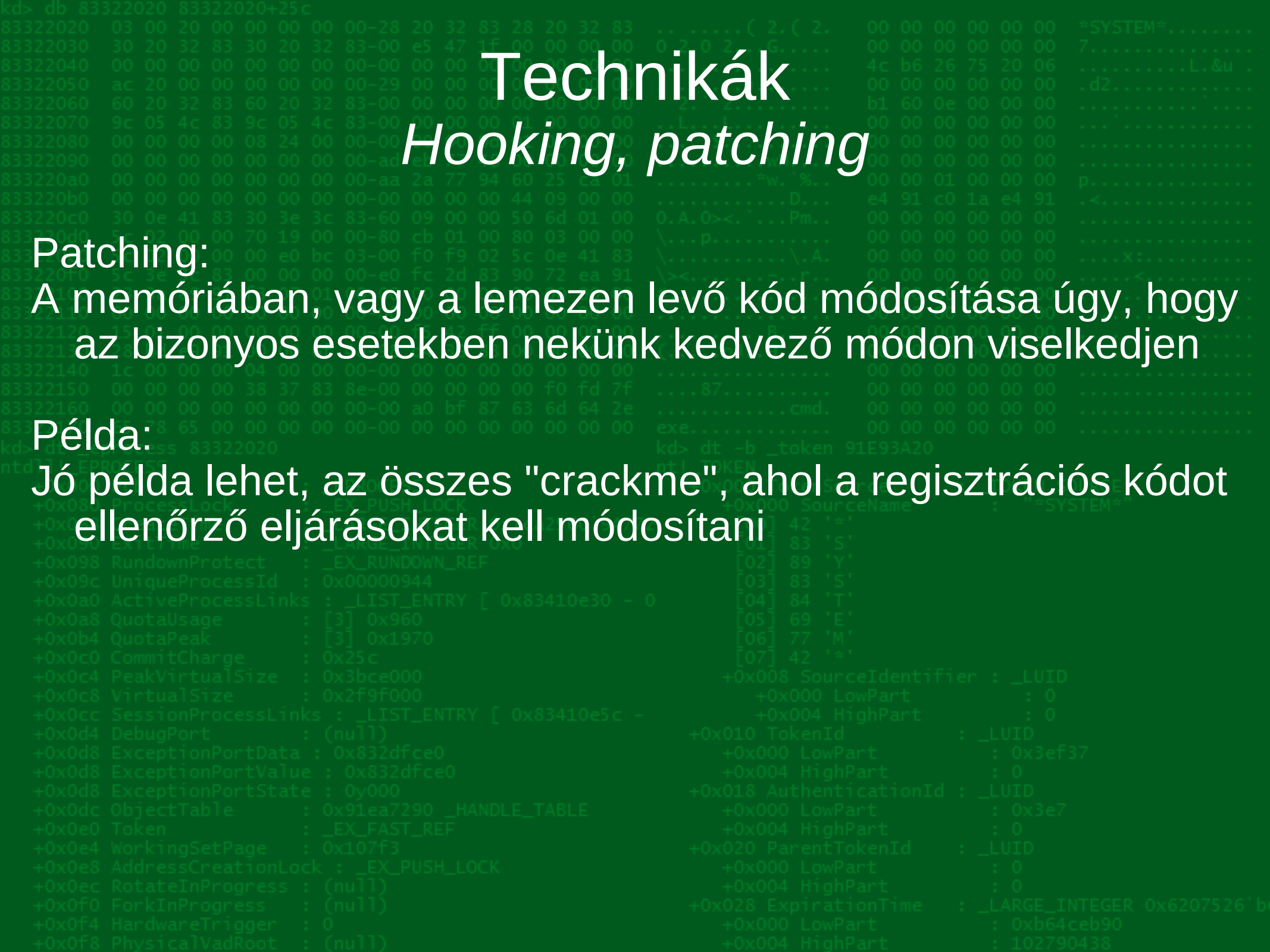
Hooking, patching

Patching:

A memóriában, vagy a lemezen levő kód módosítása úgy, hogy az bizonyos esetekben nekünk kedvező módon viselkedjen

Példa:

Jó példa lehet, az összes "crackme", ahol a regisztrációs kódot ellenőrző eljárásokat kell módosítani



Technikák

Hooking, patching

Detour patching

- Eljárás memóriában levő kódjának módosítása
- Egy részét felülírja egy jmp utasítással
- A vezérlést egy általunk írt kódot tartalmazó területre irányítjuk
- Az általunk írt kód végrehajtása
 - Lefut a mi kódunk
 - Lefuttatja a felülírt utasításokat (konzisztencia)
 - Visszaadja a vezérlést eredeti függvényre

Technikák

Hooking, patching

Detour patching példa:
nt!SeAccessCheck

Függvény felülírandó része
nt!SeAccessCheck

```
805ef232 mov     edi, edi
805ef234 push   ebp
805ef235 mov     ebp, esp
805ef237 push   ebx
805ef238 xor     ebx, ebx
```

Függvény változatlanul hagyott része
nt!SeAccessCheck+0x08:
805ef23a cmp byte ptr [ebp+24h, bl]
805ef23d jne nt!SeAccessCheck+0x36 (805ef268)]

Technikák

Hooking, patching

Detour patching példa: nt!SeAccessCheck

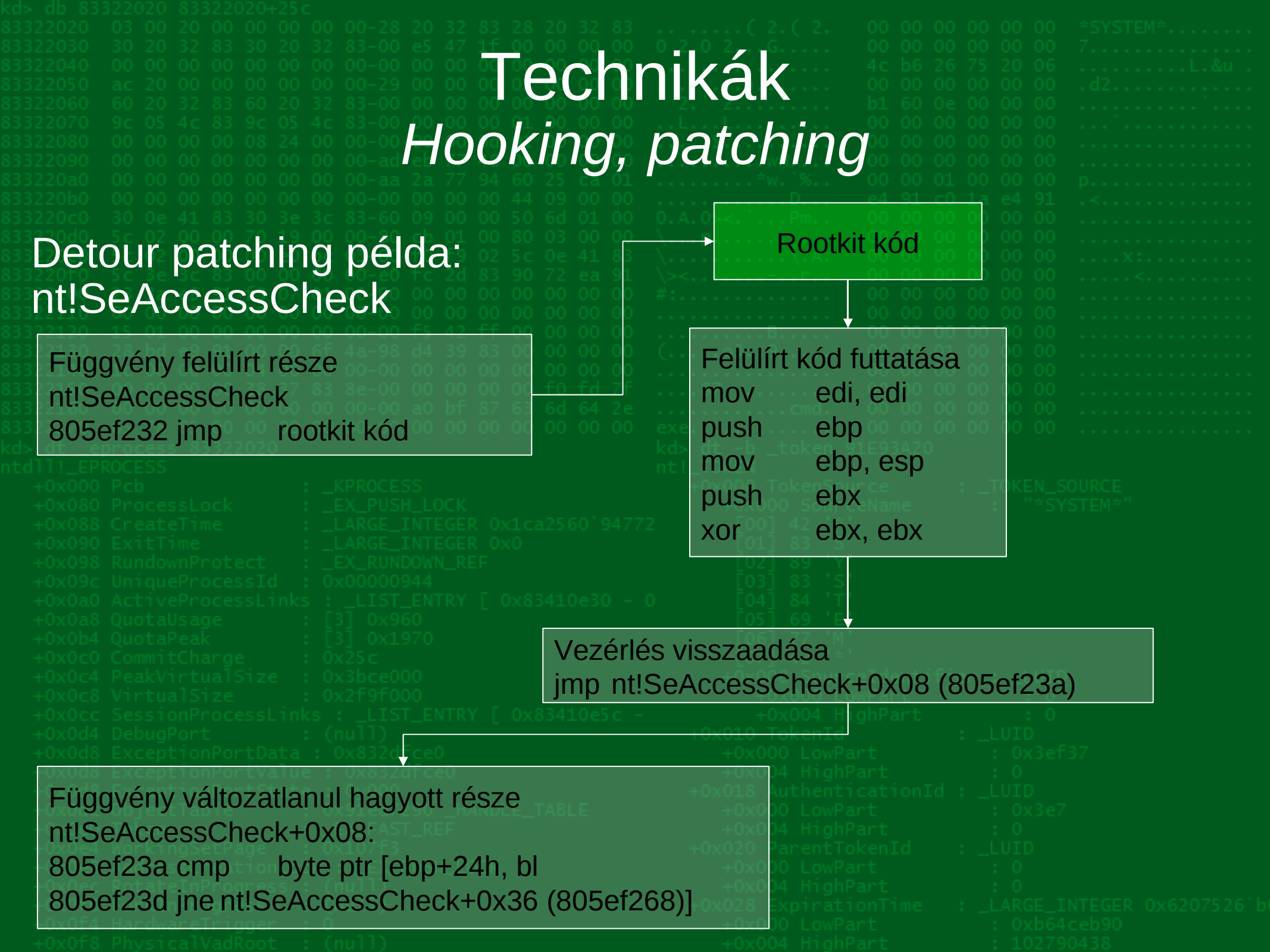
Függvény felülírt része
nt!SeAccessCheck
805ef232 jmp rootkit kód

Függvény változatlanul hagyott része
nt!SeAccessCheck+0x08:
805ef23a cmp byte ptr [ebp+24h, bl
805ef23d jne nt!SeAccessCheck+0x36 (805ef268)]

Rootkit kód

Felülírt kód futtatása
mov edi, edi
push ebp
mov ebp, esp
push ebx
xor ebx, ebx

Vezérlés visszaadása
jmp nt!SeAccessCheck+0x08 (805ef23a)



Technikák

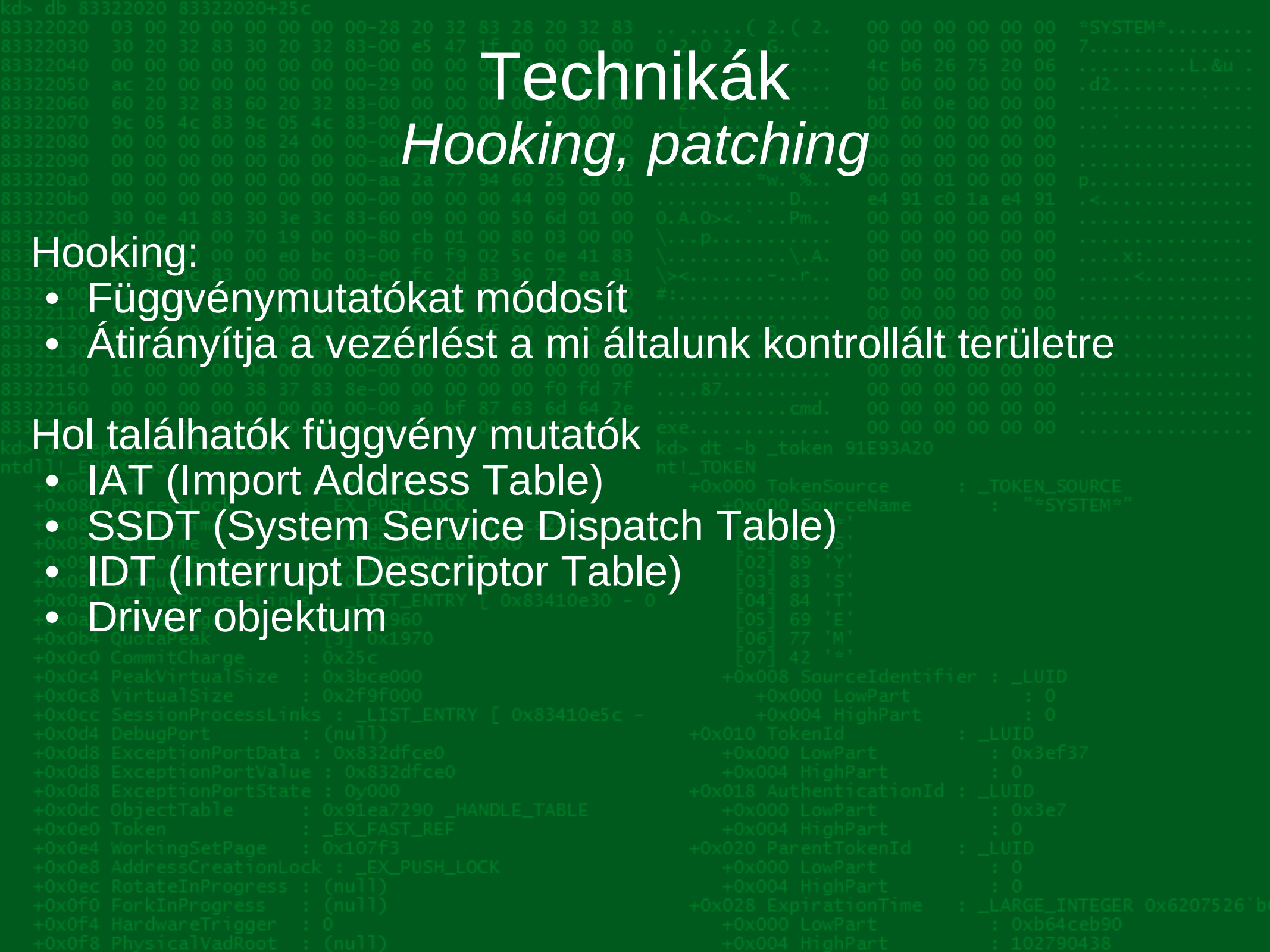
Hooking, patching

Hooking:

- Függvényt mutatókat módosít
- Átirányítja a vezérlést a mi általunk kontrollált területre

Hol találhatóak függvény mutatók

- IAT (Import Address Table)
- SSDT (System Service Dispatch Table)
- IDT (Interrupt Descriptor Table)
- Driver objektum



Technikák

Hooking, patching - Példa

IRP Hooking

- A driverek alapvetően IRP-ben érkező kéréseket szolgálnak ki
- Ehhez szükség van a megfelelő IRP handlerekre
- Az IRP handler futásidőben lecserélhető

Hogyan működik a keyboard loggerem

- Keyboard device megkeresése
- A device-hoz tartozó driver megkeresése
- A megfelelő IRP handler hookolása

Technikák

```
kd> dt -vb _driver_object 84ac5a00kd> dt -vb _driver_object 84ac5a00
hal!_DRIVER_OBJECThal!_DRIVER_OBJECT
struct _DRIVER_OBJECT, 15 elementsstruct _DRIVER_OBJECT, 15 elements, 0xa8 bytes
+0x000 Type : 4 +0x000 Type : 4
+0x002 Size : 168 +0x002 Size : 168
+0x004 DeviceObject : 0x84b +0x004 DeviceObject : 0x84b39e28
+0x008 Flags : 0x12 +0x008 Flags : 0x12
+0x00c DriverStart : 0x8b3 +0x00c DriverStart : 0x8b3b4000
+0x010 DriverSize : 0xd00 +0x010 DriverSize : 0xd000
+0x014 DriverSection : 0x84a +0x014 DriverSection : 0x84abf538
+0x018 DriverExtension : 0x84a +0x018 DriverExtension : 0x84ac5aa8
+0x01c DriverName : struc +0x01c DriverName : struct _UNICODE_STRING, 3 elements
"\Driver\kbdclass"
+0x000 Length : 0x +0x000 Length : 0x20
+0x002 MaximumLength : 0x +0x002 MaximumLength : 0x20
+0x004 Buffer : 0x +0x004 Buffer : 0x84abdf50 "\Driver\kbdclass"
+0x024 HardwareDatabase : 0x829 +0x024 HardwareDatabase : 0x829bf250
+0x028 FastIoDispatch : <null +0x028 FastIoDispatch : <null
+0x02c DriverInit : 0x8b3 +0x02c DriverInit : 0x8b3bd9f2
+0x030 DriverStartIo : <null +0x030 DriverStartIo : <null
+0x034 DriverUnload : <null +0x034 DriverUnload : <null
+0x038 MajorFunction : <28 e +0x038 MajorFunction : <28 elements
[00] 0x8b3b6000 [00] 0x8b3b6000
[01] 0x82706437 [01] 0x82706437
[02] 0x8b3b6294 [02] 0x8b3b6294
[03] 0x8b3b70ba [03] 0x9015d6c2
[04] 0x82706437 [04] 0x82706437
[05] 0x82706437 [05] 0x82706437
[06] 0x82706437 [06] 0x82706437
[07] 0x82706437 [07] 0x82706437
[08] 0x82706437 [08] 0x82706437
[09] 0x8b3b5f78 [09] 0x8b3b5f78
[10] 0x82706437 [10] 0x82706437
[11] 0x82706437 [11] 0x82706437
[12] 0x82706437 [12] 0x82706437
[13] 0x82706437 [13] 0x82706437
[14] 0x8b3bac22 [14] 0x8b3bac22
[15] 0x8b3ba3c2 [15] 0x8b3ba3c2
[16] 0x82706437 [16] 0x82706437
[17] 0x82706437 [17] 0x82706437
[18] 0x8b3b56c6 [18] 0x8b3b56c6
[19] 0x82706437 [19] 0x82706437
[20] 0x82706437 [20] 0x82706437
[21] 0x82706437 [21] 0x82706437
```

Technikák

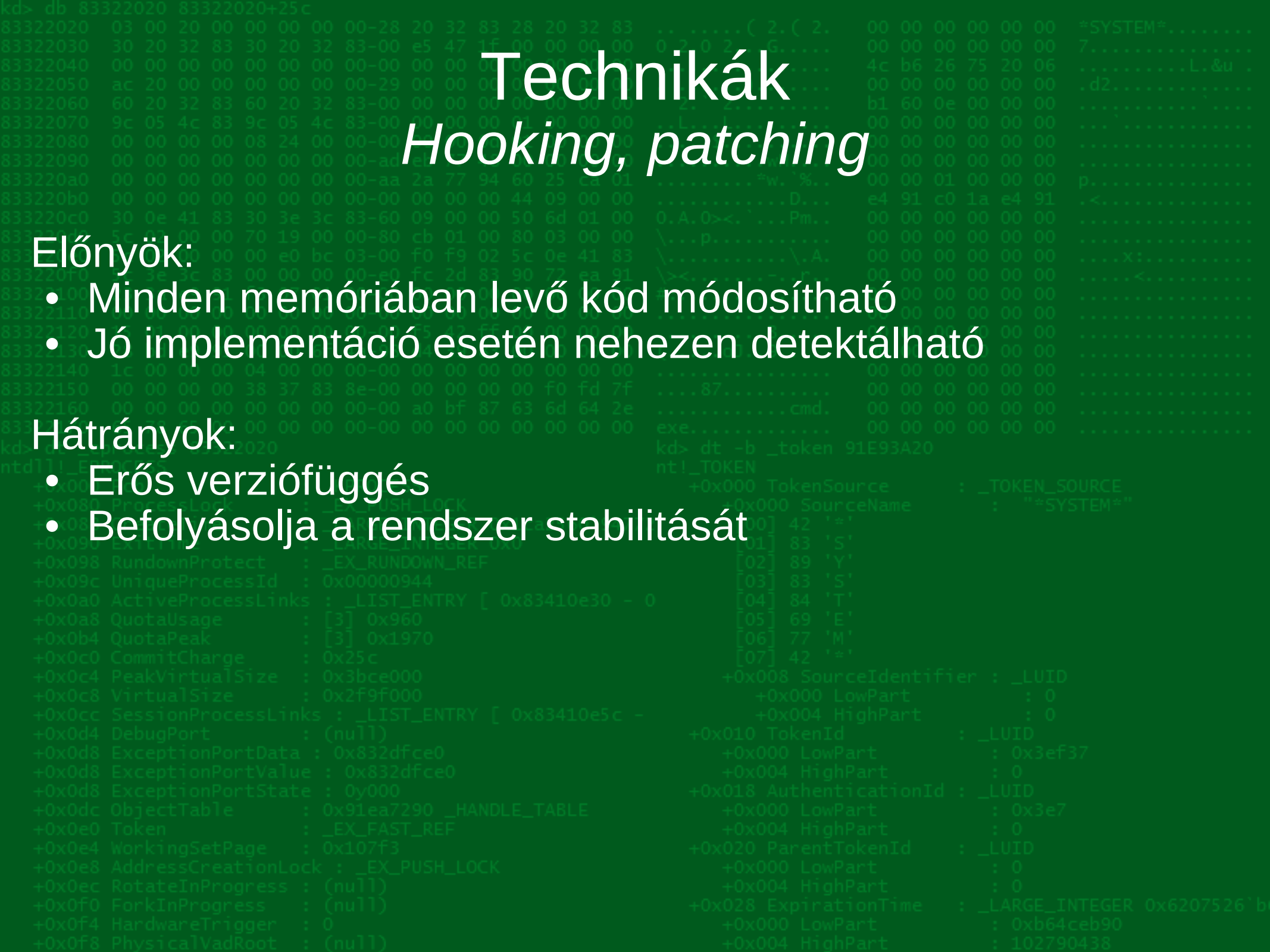
Hooking, patching

Előnyök:

- Minden memóriában levő kód módosítható
- Jó implementáció esetén nehezen detektálható

Hátrányok:

- Erős verziófüggés
- Befolyásolja a rendszer stabilitását



```
kd> db 83322020 83322020+25c
83322020 03 00 20 00 00 00 00 00-28 20 32 83 28 20 32 83 .. .. ( 2. ( 2. 00 00 00 00 00 00 *SYSTEM#.....
83322030 30 20 32 83 30 20 32 83-00 e5 47 1f 00 00 00 00 0 2.0 2...G..... 00 00 00 00 00 00 7.....
83322040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 4c b6 26 75 20 06 .....L.&u .
83322050 ac 20 00 00 00 00 00 00-29 00 00 00 01 00 00 00 : ..... )..... 00 00 00 00 00 00 .d2.....
83322060 60 20 32 83 60 20 32 83-00 00 00 00 00 00 00 00 ` 2. ` 2..... b1 60 0e 00 00 00 .....
83322070 9c 05 4c 83 9c 05 4c 83-00 00 00 00 01 00 00 00 ..L...L..... 00 00 00 00 00 00 ...
83322080 00 00 00 00 08 24 00 00-00 00 00 0d 01 00 00 00 ..... $. ..... 00 00 00 00 00 00 .....
83322090 00 00 00 00 00 00 00 00-ad eb 77 48 00 00 00 00 ..... wH..... 00 00 00 00 00 00 .....
833220a0 00 00 00 00 00 00 00 00-aa 2a 77 94 60 25 ca 01 ..... =w. `%. .. 00 00 01 00 00 00 p.....
833220b0 00 00 00 00 00 00 00 00-00 00 00 00 44 09 00 00 ..... D... e4 91 c0 1a e4 91 .<.....
833220c0 30 0e 41 83 30 3e 3c 83-60 09 00 00 50 6d 01 00 0.A.0><. `...Pm.. 00 00 00 00 00 00 .....
833220d0 5c 02 00 00 00 70 19 00 00-80 cb 01 00 80 03 00 00 \...p..... 00 00 00 00 00 00 .....
833220e0 5c 02 00 00 00 e0 bc 03-00 f0 f9 02 5c 0e 41 83 \..... \.A. 00 00 00 00 00 00 ....x:.....
833220f0 5c 3e 3c 83 00 00 00 00-e0 fc 2d 83 90 72 ea 91 \><..... -..r.. 00 00 00 00 00 00 ....<.....
83322100 23 3a e9 91 f3 07 01 00-00 00 00 00 00 00 00 00 #:..... 00 00 00 00 00 00 .....
83322110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322120 15 01 00 00 00 00 00 00-00 f5 42 ff 00 00 00 00 ..... B..... 00 00 00 00 00 00 .....
83322130 28 bd e9 91 00 00 6f 4a-98 d4 39 83 00 00 00 00 (...o3..9..... 00 00 01 00 00 00 .....
83322140 1c 00 00 00 04 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322150 00 00 00 00 38 37 83 8e-00 00 00 00 00 00 00 00 ..... fd 7f ..... 00 00 00 00 00 00 .....
83322160 00 00 00 00 00 00 00 00-00 a0 bf 83 63 d6 42 e ..... cmd. 00 00 00 00 00 00 .....
83322170 65 78 65 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... e e ..... 00 00 00 00 00 00 .....
```

DEMO

Hamarosan videó formában
<http://hacktivity.hu>

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2560 94772
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_RUNDOWN_REF
+0x09c UniqueProcessId : 0x00000944
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e30 - 0
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
kd> dt -b _token 91E93A20
ntdll!_TOKEN
+0x000 SourceName : _TOKEN_SOURCE
+0x004 SourceName : "SYSTEM#"
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526`b
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

Technikák

Filter driverek

- A driverekkel való kommunikáció IRP (interrupt request packet) formájában történik
- Ez részben dokumentálatlan
- Fontosabb kezelendő típusok:
 - IRP_MJ_READ (olvasás)
 - IRP_MJ_WRITE (írás)
 - IRP_MJ_DEVICE_CONTROL (IOCTL)



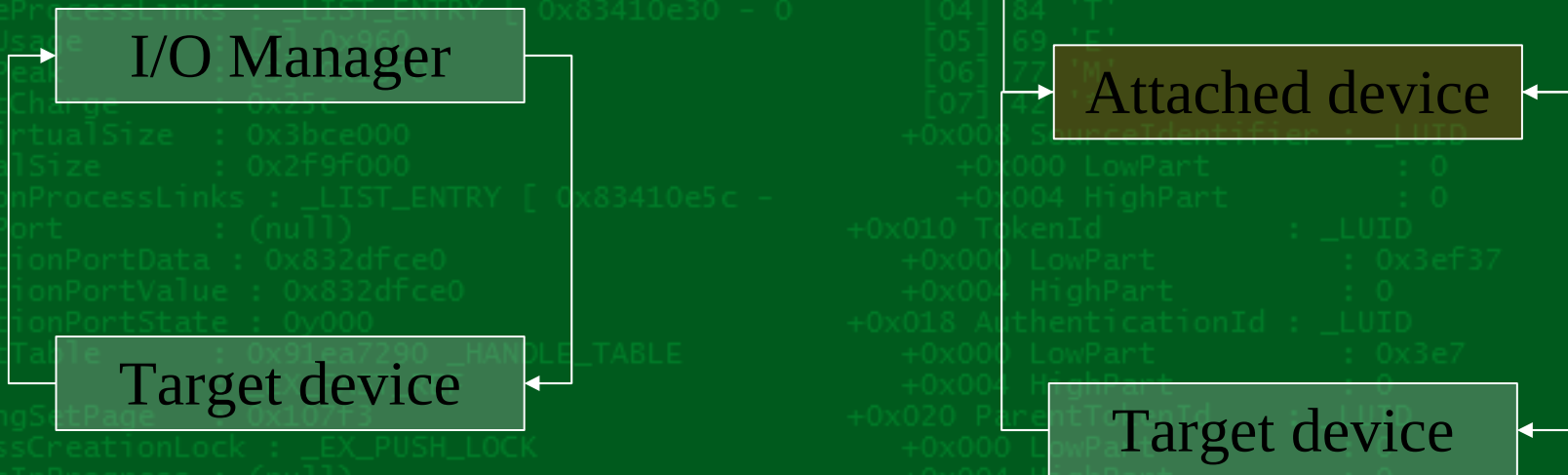
Technikák

Filter driverek

A driverek által létrehozott device objektumokat lehetőségünk van egymáshoz kapcsolni

Az erre használható függvények:

- IoAttachDevice
- IoAttachDeviceByPointer
- IoAttachDeviceToDeviceStack



Technikák

Filter driverek

Előnyök:

- Módosíthatjuk a filter láncban alattunk levő drivernek küldött, illetve az onnan visszafelé jövő IRP-eket
- Ezzel az alattunk levő driver által kiszolgált kérés eredményéből adatokat vehetünk ki, illetve adhatunk hozzá

Hátrányok:

- Könnyen észrevehető
- Nem biztos, hogy mi vagyunk a legközelebb a láncban a célponthoz

```
kd> db 83322020 83322020+25c
83322020 03 00 20 00 00 00 00 00-28 20 32 83 28 20 32 83 .. ..( 2.( 2. 00 00 00 00 00 00 *SYSTEM#.....
83322030 30 20 32 83 30 20 32 83-00 e5 47 1f 00 00 00 00 0 2.0 2...G..... 00 00 00 00 00 00 7.....
83322040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 4c b6 26 75 20 06 .....L.&u .
83322050 ac 20 00 00 00 00 00 00-29 00 00 00 01 00 00 00 : .....). ..... 00 00 00 00 00 00 .d2.....
83322060 60 20 32 83 60 20 32 83-00 00 00 00 00 00 00 00 ` 2.` 2..... b1 60 0e 00 00 00 .....
83322070 9c 05 4c 83 9c 05 4c 83-00 00 00 00 01 00 00 00 ..L...L..... 00 00 00 00 00 00 ...
83322080 00 00 00 00 08 24 00 00-00 00 00 0d 01 00 00 00 .....$. ..... 00 00 00 00 00 00 .....
83322090 00 00 00 00 00 00 00 00-ad eb 77 48 00 00 00 00 .....wH.... 00 00 00 00 00 00 .....
833220a0 00 00 00 00 00 00 00 00-aa 2a 77 94 60 25 ca 01 .....*w.`%.. 00 00 01 00 00 00 p.....
833220b0 00 00 00 00 00 00 00 00-00 00 00 00 44 09 00 00 .....D... e4 91 c0 1a e4 91 .<.....
833220c0 30 0e 41 83 30 3e 3c 83-60 09 00 00 50 6d 01 00 0.A.0><.`...Pm.. 00 00 00 00 00 00 .....
833220d0 5c 02 00 00 00 70 19 00 00-80 cb 01 00 80 03 00 00 \...p..... 00 00 00 00 00 00 .....
833220e0 5c 02 00 00 00 e0 bc 03-00 f0 f9 02 5c 0e 41 83 \.....\A. 00 00 00 00 00 00 ....x:.....
833220f0 5c 3e 3c 83 00 00 00 00-e0 fc 2d 83 90 72 ea 91 \><.....-r.. 00 00 00 00 00 00 ....<.....
83322100 23 3a e9 91 f3 07 01 00-00 00 00 00 00 00 00 00 #:..... 00 00 00 00 00 00 .....
83322110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322120 15 01 00 00 00 00 00 00-00 f5 42 ff 00 00 00 00 .....B..... 00 00 00 00 00 00 .....
83322130 28 bd e9 91 00 00 6f 4a-98 d4 39 83 00 00 00 00 (...o3..9..... 00 00 01 00 00 00 .....
83322140 1c 00 00 00 04 00 00 00-00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 .....
83322150 00 00 00 00 38 37 83 8e-00 00 00 00 00 00 00 00 .....fd 7f ..... 00 00 00 00 00 00 .....
83322160 00 00 00 00 00 00 00 00-00 a0 bf 83 63 d6 42 e .....cmd. 00 00 00 00 00 00 .....
83322170 65 78 65 00 00 00 00 00-00 00 00 00 00 00 00 00 .....e..... 00 00 00 00 00 00 .....
```

DEMO

Hamarosan videó formában
<http://hacktivity.hu>

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2560 94772
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_RUNDOWN_REF
+0x09c UniqueProcessId : 0x00000944
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e30 - 0
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
kd> dt -b _token 91E93A20
ntdll!_TOKEN
+0x000 SourceName : _TOKEN_SOURCE
+0x004 SourceName : ""*SYSTEM#"
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526`b
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

Néhány szó a bemutatott rootkitről

- Támogatott windows verziók
 - Windows XP SP2, SP3
 - Windows Server 2003 SP2
 - Windows Server 2008 SP1, SP2
 - Windows Vista SP1, SP2
 - Windows 7 Beta, RC1, Enterprise
- Fontosabb funkciók
 - Folyamatok elrejtése (process hiding)
 - Token lopás (Access Token stealing)
 - Állomány és könyvtár rejtés (File & Directory hiding)
 - Billentyű letütések naplózása (Keylogging)

Rövid összefoglaló

- Rootkitek története
- Felhasználói és kernel mód
- Alkalmazott technikák
- Saját rootkit demo

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2560'94772
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_RUNDOWN_REF
+0x09c UniqueProcessId : 0x00000944
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e30 - 0
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
```

```
kd> dt -b _token 91E93A20
nt!_TOKEN
+0x000 TokenSource : _TOKEN_SOURCE
+0x000 SourceName : "SYSTEM"
[00] 42 '*'
[01] 83 'S'
[02] 89 'Y'
[03] 83 'S'
[04] 84 'T'
[05] 69 'E'
[06] 77 'M'
[07] 42 '*'
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526'bf
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```

Elérhetőségek

e-mail cím
csaba.barta@gmail.com

Letöltés
<http://www.csababarta.com>

```
kd> dt _eprocess 83322020
ntdll!_EPROCESS
+0x000 Pcb : _KPROCESS
+0x080 ProcessLock : _EX_PUSH_LOCK
+0x088 CreateTime : _LARGE_INTEGER 0x1ca2166
+0x090 ExitTime : _LARGE_INTEGER 0x0
+0x098 RundownProtect : _EX_PUSH_LOCK
+0x09c UniqueProcessId : 0x000
+0x0a0 ActiveProcessLinks : _LIST_ENTRY [ 0x83410e30 - 0
+0x0a8 QuotaUsage : [3] 0x960
+0x0b4 QuotaPeak : [3] 0x1970
+0x0c0 CommitCharge : 0x25c
+0x0c4 PeakVirtualSize : 0x3bce000
+0x0c8 VirtualSize : 0x2f9f000
+0x0cc SessionProcessLinks : _LIST_ENTRY [ 0x83410e5c -
+0x0d4 DebugPort : (null)
+0x0d8 ExceptionPortData : 0x832dfce0
+0x0d8 ExceptionPortValue : 0x832dfce0
+0x0d8 ExceptionPortState : 0y000
+0x0dc ObjectTable : 0x91ea7290 _HANDLE_TABLE
+0x0e0 Token : _EX_FAST_REF
+0x0e4 WorkingSetPage : 0x107f3
+0x0e8 AddressCreationLock : _EX_PUSH_LOCK
+0x0ec RotateInProgress : (null)
+0x0f0 ForkInProgress : (null)
+0x0f4 HardwareTrigger : 0
+0x0f8 PhysicalVadRoot : (null)
+0x000 TokenSource : _TOKEN_SOURCE
+0x000 SourceName : "SYSTEM"
[00] 42 '='
[01] 83 'S'
[02] 20 ' '
[03] 20 ' '
[04] 84 'T'
[05] 69 'E'
[06] 77 'M'
[07] 42 '='
+0x008 SourceIdentifier : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x010 TokenId : _LUID
+0x000 LowPart : 0x3ef37
+0x004 HighPart : 0
+0x018 AuthenticationId : _LUID
+0x000 LowPart : 0x3e7
+0x004 HighPart : 0
+0x020 ParentTokenId : _LUID
+0x000 LowPart : 0
+0x004 HighPart : 0
+0x028 ExpirationTime : _LARGE_INTEGER 0x6207526
+0x000 LowPart : 0xb64ceb90
+0x004 HighPart : 102790438
```