Osnove digitalne forenzike

Gorazd Božič, Tadej Hren
ARNES, Jamova 39, Ljubljana
si-cert@*arnes.si*

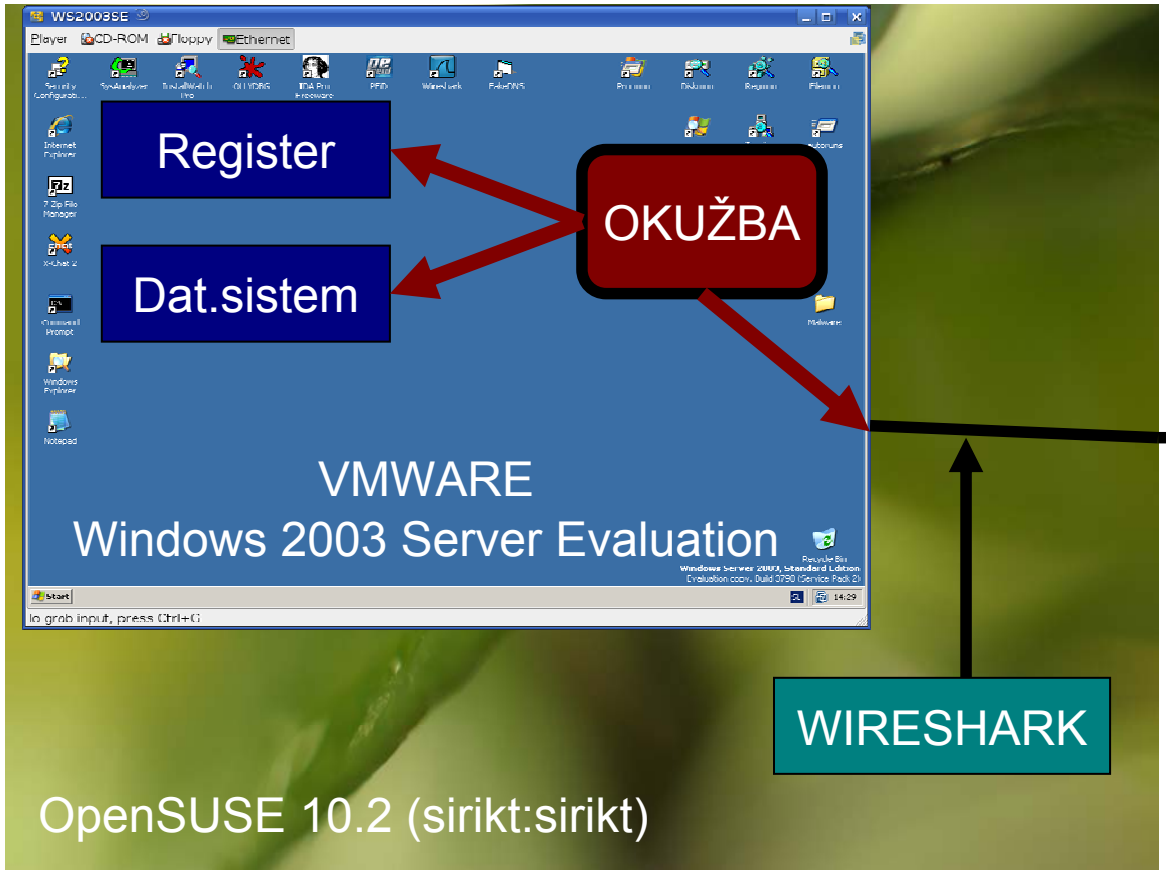
Sirikt 2007, Kranjska Gora, 21.4.2007

Kaj bomo delali?

- Analiza delovanja bota
  - spremembe v datotečnem sistemu
  - spremembe v registru
  - omrežna komunikacija

Testno okolje

Akademska in raziskovalna mreža Slovenije

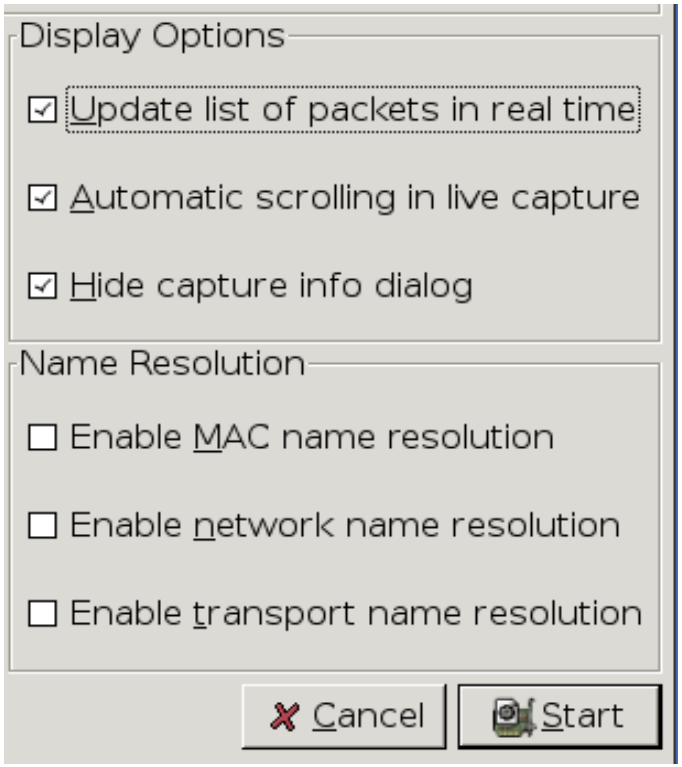


Debian
- IRCD
- HTTPD

WIRESHARK

Akademska in raziskovalna mreža Slovenije

- Applications -> System -> Network
- Geslo uporabnika root: Arnes2007

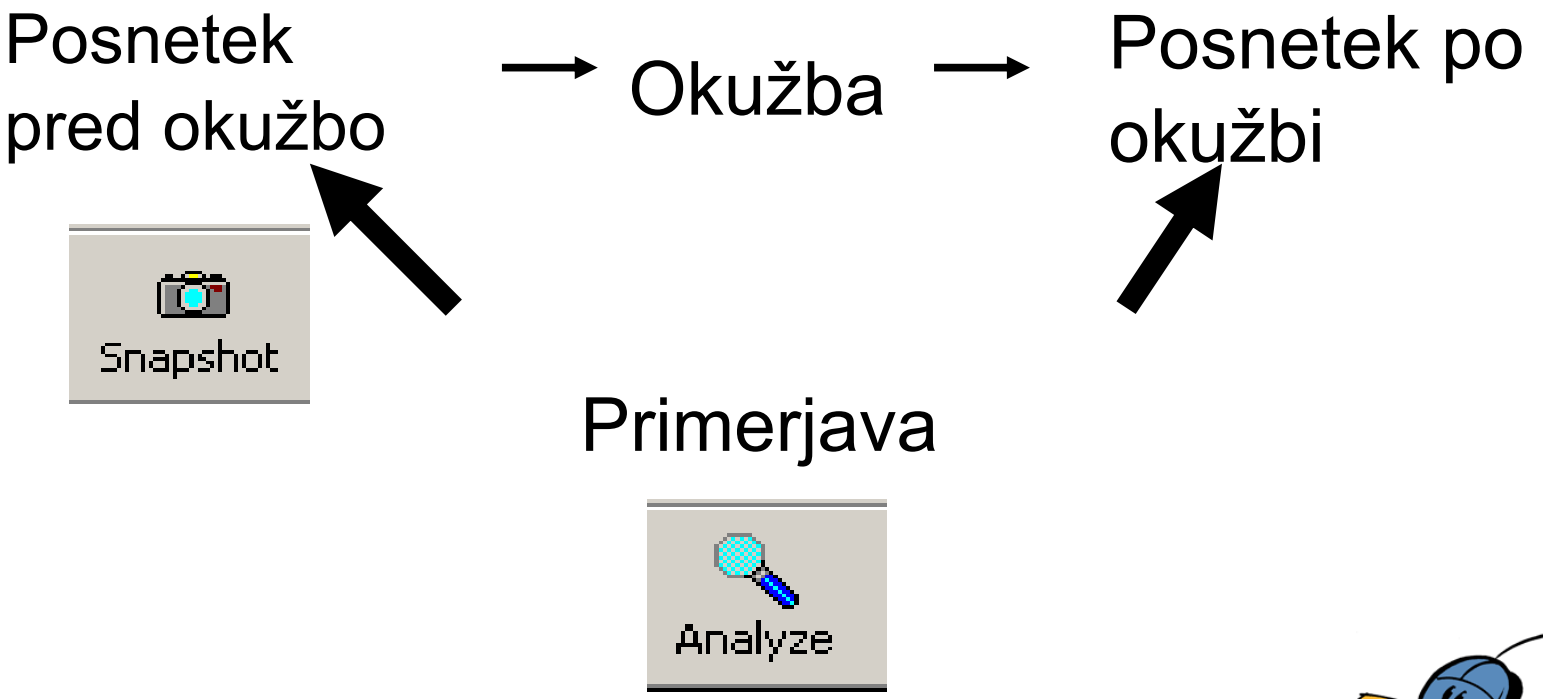


VMWARE PLAYER

- Application -> System -> More programs
- Windows 2003 server se nahaja v Desktop -> WS2003SE -> WS2003SE.vmx

SPREMEMBE V DATOTEČNEM SISTEMU IN REGISTRU

- Installwatch Pro



DATOTEČNI SISTEM

- Added files:
  - c:\windows\system32\update.exe
- Deleted files:
  - c:\Documents...\Desktop\Malware\S3xxxy.exe

REGISTER

Akademska in raziskovalna mreža Slovenije

- Added registry
  - KEY
    - HKCU\Software\Microsoft\Current Version\Run\
    - HKLM\Software\Microsoft\Current Version\RunServices
    - HKLM\Software\Microsoft\Current Version\Run
  - VALUE
    - Microsoft Update Machine
  - Data
    - “update.exe”

ZAGONSKI KLJUČI V REGISTRU

- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
- HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
- C:\Documents and Settings\All Users\Start Menu\Programs\Startup
- C:\Documents and Settings\{Username}\Start Menu\Programs\Startup

SYSINTERNALS ORODJA

- http://www.microsoft.com/technet/sysinternals/default.mspx
  - Process Explorer (procexp)
  - Autoruns (autoruns)
  - Process Monitor (Procmon)
  - TCPView (tcpview)
  - ...

OMREŽNA KOMUNIKACIJA

- IRC - BOTNET

  /server irc.arnes.si 6667

  /join #kanal geslo

  /nick vzdevek

- DNS
  - DNS strežnik
  - FakeDNS (Malcode Analyst Pack, http://labs.idefense.com)
  - c:\windows\system32\drivers\etc\hosts

TESTNI IRC STREŽNIK

- IP naslov: 193.2.1.176

notepad c:\windows\system32\drivers\etc\hosts

127.0.0.1 localhost
193.2.1.176 irc1.abuselol.net

KANAL IN GESLO


```
    192.168.230.128        TCP     7666 > 2063 [
    193.2.1.176            TCP     2063 > 7666 [
    192.168.230.128        TCP     7666 > 2063 [
ytes captured)
(00:0c:29:37:8d:c2), Dst: 00:50:56:e7:38:d7
128 (192.168.230.128), Dst: 193.2.1.176 (193
ort: 2063 (2063), Dst Port: 7666 (7666), Seq
```

```
d c2 08 00 45 00    .PV.8... )7....E.
0 a8 e6 80 c1 02    ...|@... ........
d 05 fa d7 50 18    ......0. 8k}...P.
0 23 6c 6f 6c 23    ...p..JO IN #lol#
8 4f 53 54 20 53     lol..US ERHOST S
a 4d 4f 44 45 20    VN|10593 6..MODE
0 2b 78 2b 55 0d    SVN|1059 36 +x+U.
3 20 6c 6f 6c 0d    .JOIN #l ol# lol.
3 56 4e 7c 31 30    .USERHOS T SVN|10
0 53 56 4e 7c 31    5936..MO DE SVN|1
d 0a 4a 4f 49 4e    05936 +x +U..JOIN
d 0a 55 53 45 52     #lol# l ol..USER
0 35 39 33 36 0d    HOST SVN |105936.
```

POVEZAVA NA BOTENT Z IRC KLIENTOM

- Xchat (http://www.xchat.org)
  - nickname: poljubno (obvezno spremeniti!)
  - username: poljubno (!)
  - realname: poljubno (!)
  - networks: irc1.abuselol.net
  - povezava na kanal #lol#, geslo je lol

UPORABA BOTNETA

- Primeri ukazov napadalca

.login <password>

.execute <visibility> <file> [parameters]

.open <file>

.join <channel> [key]

.log

.sysinfo

.download <url><destination><actions>

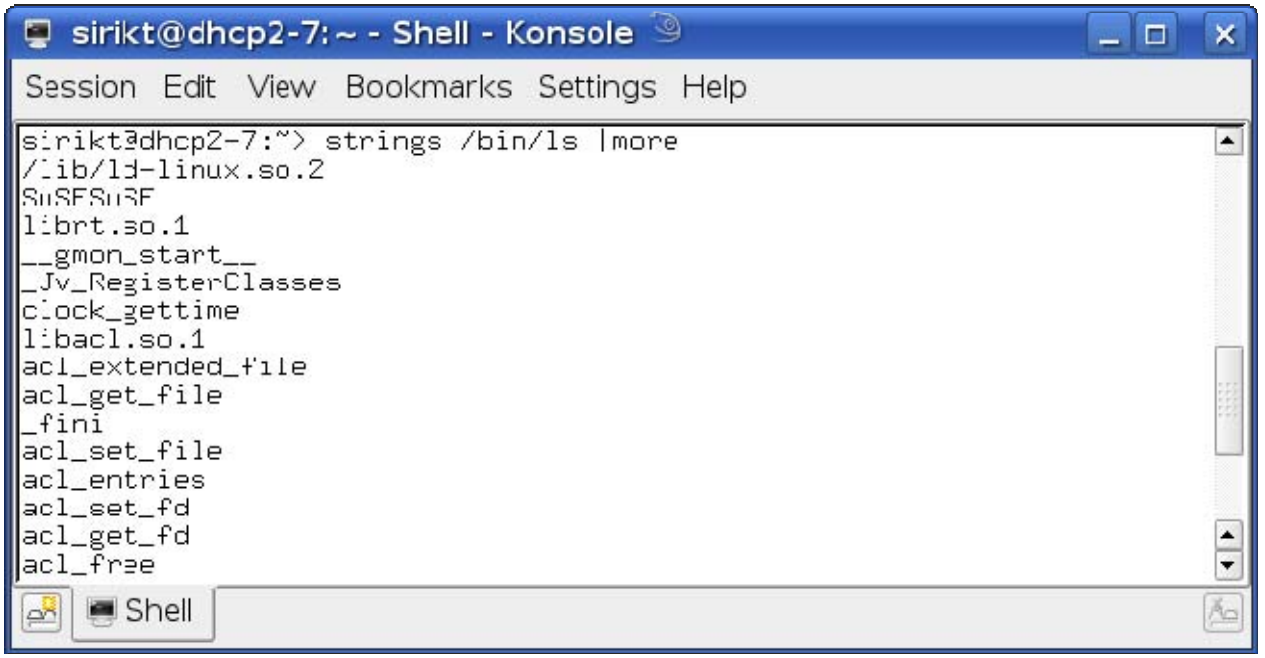
.update <url><id>

ukazi za ddos napade, samodejno širjenje

.remove

Kaj se najde v "strings"

- ukaz strings



- Process Explorer
  - proces -> properties -> strings
  - image <-> memory

NALOGA

- Kje se bot nahaja na disku
- Kako se požene ob zagonu sistema
- Na kateri IRC strežnik se poveže
- Na kateri kanal, geslo kanala
- Kako lahko sistem očistimo
- Najdite geslo za upravljanje z boti

POMOČ PRI ANALIZI ZLONAMERNE KODE

- spletni pregledovalniki sumljivih datotek
  - http://virustotal.com
  - http://virusscan.jotti.org

VIRUSTOTAL.COM primer

Complete scanning result of "s3xxxy.exe", received in VirusTotal at 04.05.2007, 09:18:08 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AhnLab-V3	2007.4.5.0	04.05.2007	Win32/IRCBot.worm.Gen
AntiVir	7.3.1.48	04.05.2007	Worm/Rbot.JK
Authentium	4.93.8	04.04.2007	W32/Ircbot1.gen
Avast	4.7.936.0	04.04.2007	Win32:Rbot-CSN
AVG	7.5.0.447	04.04.2007	IRC/BackDoor.SdBot2.KJR
BitDefender	7.2	04.05.2007	Generic.Sdbot.61E6AA7A
CAT-QuickHeal	9.00	04.04.2007	no virus found
ClamAV	devel-20070312	04.05.2007	Exploit.DCOM.Gen
DrWeb	4.33	04.05.2007	Win32.HLLW.MyBot.based
eSafe	7.0.15.0	04.04.2007	suspicious Trojan/Worm
eTrust-Vet	30.7.3544	04.05.2007	Win32/Rbot!generic
Ewido	4.0	04.04.2007	no virus found
FileAdvisor	1	04.05.2007	no virus found
Fortinet	2.85.0.0	04.05.2007	no virus found
F-Prot	4.3.1.45	04.04.2007	W32/Ircbot1.gen
F-Secure	6.70.13030.0	04.05.2007	Backdoor.Win32.Rbot.gen
Ikarus	T3.1.1.3	04.05.2007	Backdoor.Win32.IRCBot.az
Kaspersky	4.0.2.24	04.05.2007	Backdoor.Win32.Rbot.gen
McAfee	5001	04.04.2007	W32/Sdbot.worm.gen.g
Microsoft	1.2405	04.05.2007	Backdoor:Win32/Rbot!5337
NOD32v2	2168	04.04.2007	a variant of Win32/Rbot
Norman	5.80.02	04.04.2007	W32/Malware
Panda	9.0.0.4	04.05.2007	Suspicious file
Prevx1	V2	04.05.2007	no virus found
Sophos	4.16.0	03.30.2007	W32/Rbot-Gen
Sunbelt	2.2.907.0	04.03.2007	no virus found
Symantec	10	04.05.2007	W32.Spybot.Worm
TheHacker	6.1.6.085	04.04.2007	no virus found
VBA32	3.11.3	04.04.2007	Backdoor.Win32.Rbot.gen
VirusBuster	4.3.7:9	04.04.2007	Worm.RBot.Gen.16
Webwasher-Gateway	6.0.1	04.05.2007	Worm.Rbot.210944

POMOČ PRI ANALIZI ZLONAMERNE KODE

- sandbox orodja:
  - http://www.cwsandbox.org/
  - http://sadbox.norman.no/live.html
  - http://research.sunbelt-software.com/Submit.aspx

CWSANDBOX.ORG primer

Akademska in raziskovalna mreža Slovenije

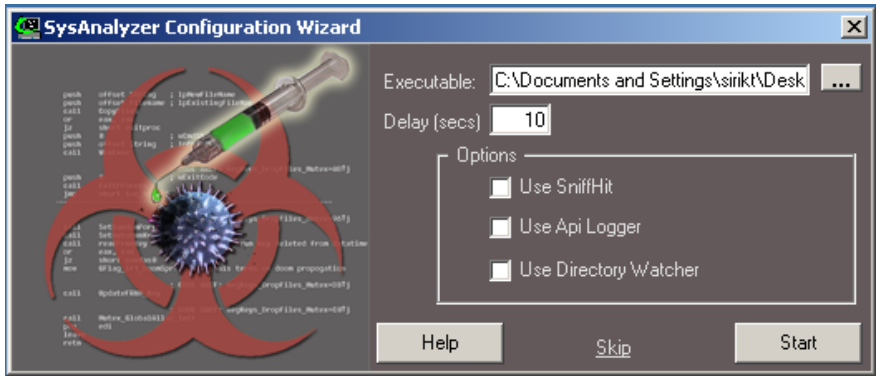
analysis.xml

```
<?xml version="1.0"?>
<!-- This analysis was created by CWSandbox (c) Carsten Willems 2006-->
<analysis cwsversion="1.107" time="03.04.2007 08:31:38" file="e55a4e32eab2b88c37ecf0bdd2d93874.exe"
logpath="C:\analysis\log\e55a4e32eab2b88c37ecf0bdd2d93874.exe\run_1\">
<calltree>
<process_call index="1" pid="1284" filename="c:\e55a4e32eab2b88c37ecf0bdd2d93874.exe" starttime="00:00.70
startreason="AnalysisTarget"/>
</calltree>

<processes>
<process index="1" pid="1284" filename="c:\e55a4e32eab2b88c37ecf0bdd2d93874.exe" filesize="243076"
md5="e55a4e32eab2b88c37ecf0bdd2d93874" username="nepenthes" parentindex="0" starttime="00:00.703"
terminationtime="02:01.109" startreason="AnalysisTarget" terminationreason="Timeout" executionstatus="OK"
<virusscan_section>
<scanner name="ClamAV" application_version="0.88.2" signature_file_version="3005">
<classification>OK</classification>
<additional_info/>
</scanner>
<scanner name="BDC/Linux-Console" application_version="7.0.2492" signature_file_version="31296">
<classification>OK</classification>
<additional_info/>
</scanner>
<scanner name="AntiVir Workstation" application_version="2.1.10-32" signature_file_version="6.38.0.165">
<classification>OK</classification>
<additional_info/>
</scanner>

</virusscan_section>
<dll_handling_section>
<load_dll dll="c:\e55a4e32eab2b88c37ecf0bdd2d93874.exe" successful="1" address="&#x24;400000"
size="987136"/>
<load_dll dll="C:\WINDOWS\system32\ntdll.dll" successful="1" address="&#x24;7C910000" size="749568"/>
<load_dll dll="C:\WINDOWS\system32\kernel32.dll" successful="1" address="&#x24;7C800000" size="1073152"/>
<load_dll dll="C:\WINDOWS\system32\user32.dll" successful="1" address="&#x24;77D10000" size="589824"/>
<load_dll dll="C:\WINDOWS\system32\GDI32.dll" successful="1" address="&#x24;77EF0000" size="290816"/>
```

SYSANALYZER

Akademska in raziskovalna mreža Slovenije

- http://labs.idefense.com/software/malcode.php



KAJ GRE LAHKO NAROBE

- Rootkit
  - antirootkit orodja, seznam na http://www.antirootkit.com
- Zlonamerni program lahko zazna, da se ga analizira
  - virtualnno okolje
  - debugger