Malware Analysis
and
Playpen Recuritment Talk

By

Alan S H Lam

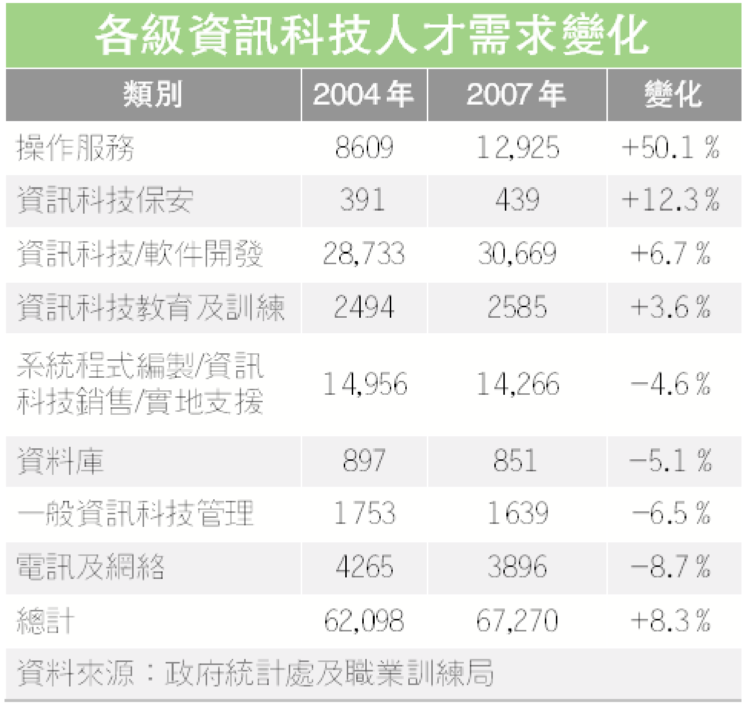
Seminar Outline

- What is Malware and its general behavior
- Tools for Malware analysis
- Basic steps for Malware analysis
- A live demo of a real case Malware analysis to show how a Malware
- Playpen Recruitment

IT Security Jobs are most wanted

網絡保安項目管理「吃香」

銀行及不少大機構本身有獨特的系統網絡，網絡保安、項目管理等皆是搶手人才，例如有8年經驗的項目管理人才月薪市價爲5萬元，但銀行往往多出20%至30%薪酬「搶人」



各級資訊科技人才需求變化

類別	2004年	2007年	變化
操作服務	8609	12,925	+50.1％
資訊科技保安	391	439	+12.3％
資訊科技/軟件開發	28,733	30,669	+6.7％
資訊科技教育及訓練	2494	2585	+3.6％
系統程式編製/資訊科技銷售/實地支援	14,956	14,266	−4.6％
資料庫	897	851	−5.1％
一般資訊科技管理	1753	1639	−6.5％
電訊及網絡	4265	3896	−8.7％
總計	62,098	67,270	+8.3％

資料來源：政府統計處及職業訓練局

From MingPao News Jan 18, 2007

What is Malware

- Malware is the short form for "Malicious Software". It implies any software instructions that were developed with the intention to cause harm. Some common examples of malware are worms, exploit code and trojan horses. (From SANS)
- Malware or malicious software is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. (From Wikipedia)

Things that under Malware

- Computer Virus
- Computer Worm
- Trojan Horse
- Spyware
- Botnet and Zombie

General Behaviors of Malware

- Changing network settings
- Disabling antivirus and antispyware tools
- Turning off the Microsoft Security Center and/or Automatic Updates
- Installing rogue certificates
- Cascading file droppers
- Keystroke Logging
- URL monitoring, form scraping, and screen scraping
- Turning on the microphone and/or camera
- Pretending to be an antispyware or antivirus tool
- Editing search results
- Acting as a spam relay
- Planting a rootkit or otherwise altering the system to prevent removal
- Installing a bot for attacker remote control
- Intercepting sensitive documents and exfiltrating them, or encrypting them for ransom
- Planting a sniffer

Source: SANS

Tools for Malware Analysis

Built-in Tools:

netstat in command prompt

shows pids (Process Identifiers) which can then be used to map ports to process names.

dir in command prompt

The command "dir /o:d" show when are the files recently modified or created in a directory. Similar to "ls -ltr" command in Unix.

Search in start menu

It can help you to search files and folder by the file name, file size, or modify date.

regedit

It help you to view and edit the register value on your system.

sigverif

This tool checks the digital signatures on all the system files, and will alert you of any that aren't correct, or not signed.

Other free Tools: for Malware Analysis

TCPView

Show you detailed listings of of all TCP and UDP endpoints on your system

Process Explorer

List all open processes and delineate between the parent processes and the processes that are spawned by the parent

Filemon

monitors and displays file system activity on a system in real-time

LADS

List Alternate Data Streams

Autoruns

shows you what programs are configured to run during system bootup or login

Regmon

show you which applications are accessing your

Ad-aware

to find and remove adware and spyware

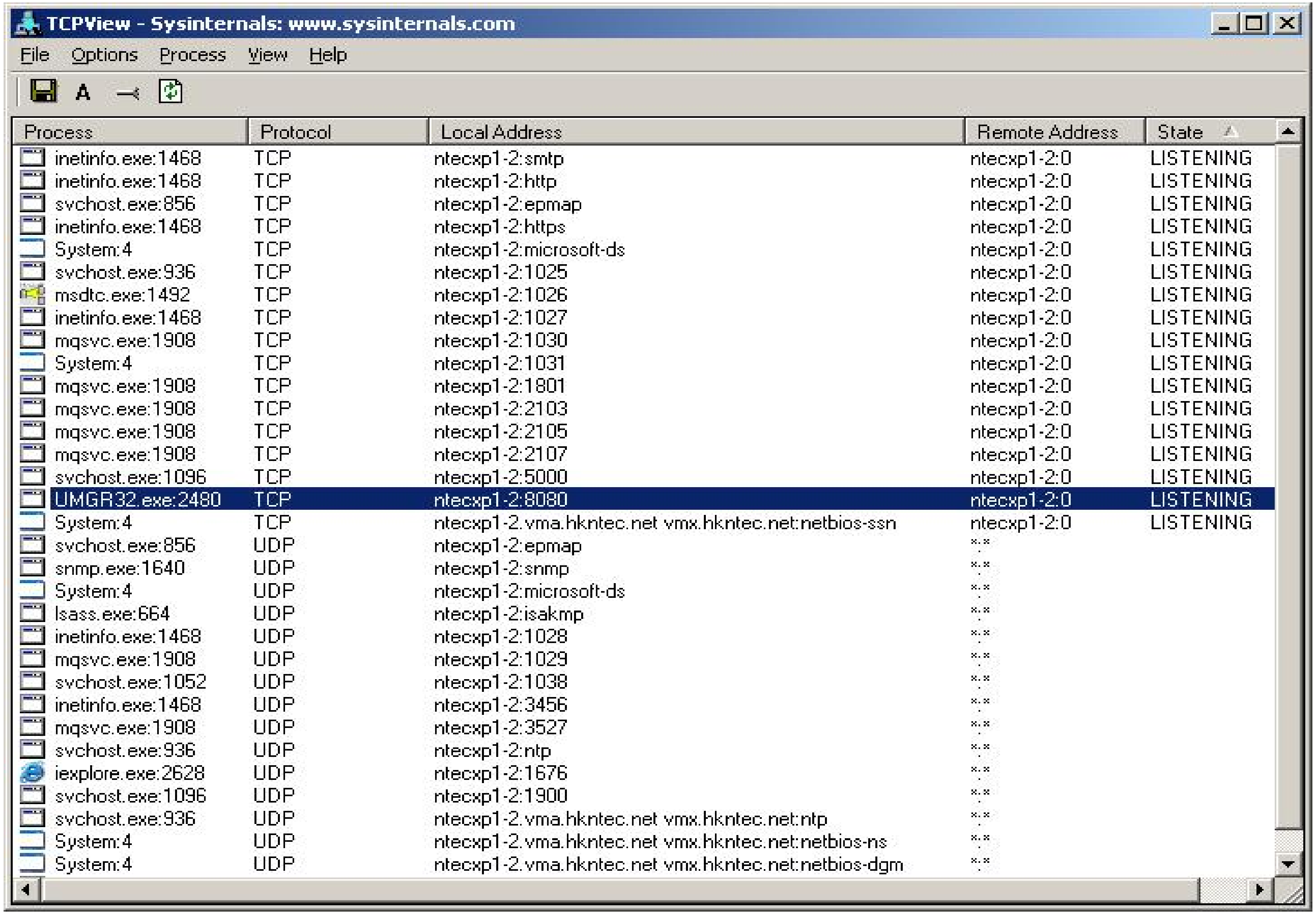
BHODemon

a guardian for Internet Explorer browser

Foremost

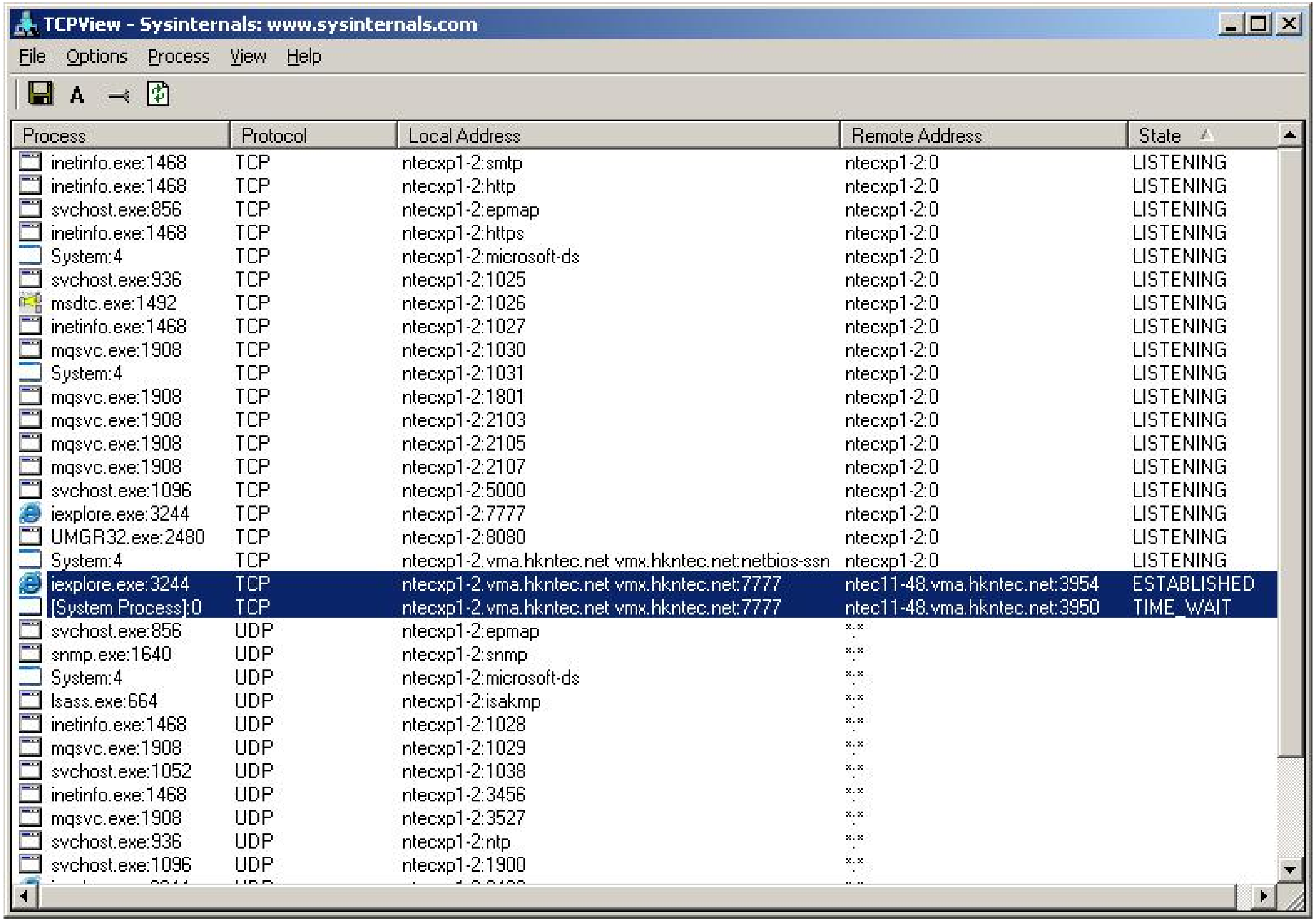
to recover files based on their headers, footers, and internal data structures

TCPView shows a Trojan Horse backdoor at 8080



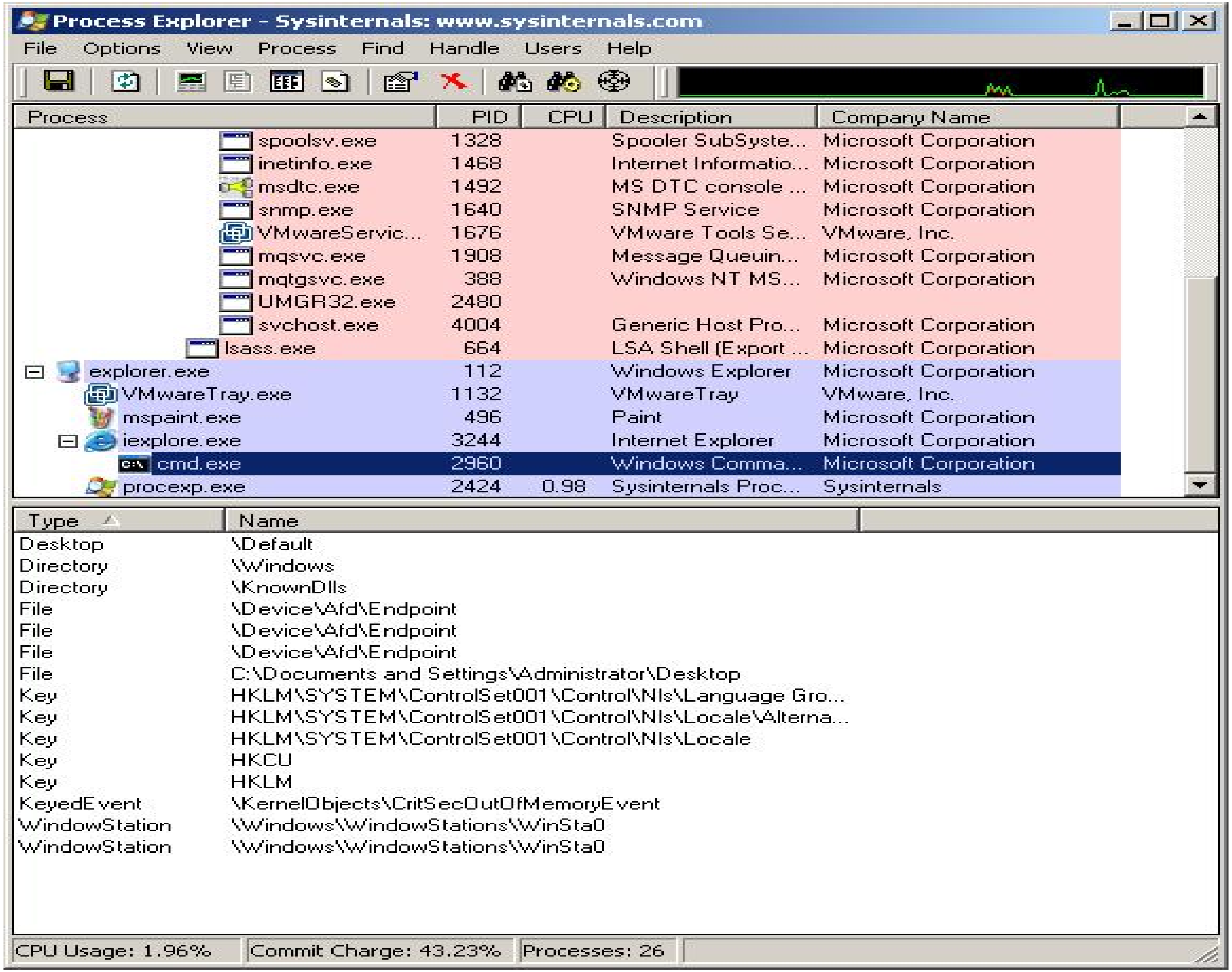
Process	Protocol	Local Address	Remote Address	State
inetinfo.exe:1468	TCP	ntecxp1-2:smtp	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:http	ntecxp1-2:0	LISTENING
svchost.exe:856	TCP	ntecxp1-2:epmap	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:https	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2:microsoft-ds	ntecxp1-2:0	LISTENING
svchost.exe:936	TCP	ntecxp1-2:1025	ntecxp1-2:0	LISTENING
msdtc.exe:1492	TCP	ntecxp1-2:1026	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:1027	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:1030	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2:1031	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:1801	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2103	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2105	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2107	ntecxp1-2:0	LISTENING
svchost.exe:1096	TCP	ntecxp1-2:5000	ntecxp1-2:0	LISTENING
UMGR32.exe:2480	TCP	ntecxp1-2:8080	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:netbios-ssn	ntecxp1-2:0	LISTENING
svchost.exe:856	UDP	ntecxp1-2:epmap	*:*	
snmp.exe:1640	UDP	ntecxp1-2:snmp	*:*	
System:4	UDP	ntecxp1-2:microsoft-ds	*:*	
lsass.exe:664	UDP	ntecxp1-2:isakmp	*:*	
inetinfo.exe:1468	UDP	ntecxp1-2:1028	*:*	
mqsvc.exe:1908	UDP	ntecxp1-2:1029	*:*	
svchost.exe:1052	UDP	ntecxp1-2:1038	*:*	
inetinfo.exe:1468	UDP	ntecxp1-2:3456	*:*	
mqsvc.exe:1908	UDP	ntecxp1-2:3527	*:*	
svchost.exe:936	UDP	ntecxp1-2:ntp	*:*	
iexplore.exe:2628	UDP	ntecxp1-2:1676	*:*	
svchost.exe:1096	UDP	ntecxp1-2:1900	*:*	
svchost.exe:936	UDP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:ntp	*:*	
System:4	UDP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:netbios-ns	*:*	
System:4	UDP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:netbios-dgm	*:*	

TCPView shows a established connection at 7777



Process	Protocol	Local Address	Remote Address	State
inetinfo.exe:1468	TCP	ntecxp1-2:smtp	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:http	ntecxp1-2:0	LISTENING
svchost.exe:856	TCP	ntecxp1-2:epmap	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:https	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2:microsoft-ds	ntecxp1-2:0	LISTENING
svchost.exe:936	TCP	ntecxp1-2:1025	ntecxp1-2:0	LISTENING
msdtc.exe:1492	TCP	ntecxp1-2:1026	ntecxp1-2:0	LISTENING
inetinfo.exe:1468	TCP	ntecxp1-2:1027	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:1030	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2:1031	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:1801	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2103	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2105	ntecxp1-2:0	LISTENING
mqsvc.exe:1908	TCP	ntecxp1-2:2107	ntecxp1-2:0	LISTENING
svchost.exe:1096	TCP	ntecxp1-2:5000	ntecxp1-2:0	LISTENING
iexplore.exe:3244	TCP	ntecxp1-2:7777	ntecxp1-2:0	LISTENING
UMGR32.exe:2480	TCP	ntecxp1-2:8080	ntecxp1-2:0	LISTENING
System:4	TCP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:netbios-ssn	ntecxp1-2:0	LISTENING
iexplore.exe:3244	TCP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:7777	ntec11-48.vma.hkntec.net:3954	ESTABLISHED
[System Process]:0	TCP	ntecxp1-2.vma.hkntec.net vmx.hkntec.net:7777	ntec11-48.vma.hkntec.net:3950	TIME_WAIT
svchost.exe:856	UDP	ntecxp1-2:epmap	*:*	
snmp.exe:1640	UDP	ntecxp1-2:snmp	*:*	
System:4	UDP	ntecxp1-2:microsoft-ds	*:*	
lsass.exe:664	UDP	ntecxp1-2:isakmp	*:*	
inetinfo.exe:1468	UDP	ntecxp1-2:1028	*:*	
mqsvc.exe:1908	UDP	ntecxp1-2:1029	*:*	
svchost.exe:1052	UDP	ntecxp1-2:1038	*:*	
inetinfo.exe:1468	UDP	ntecxp1-2:3456	*:*	
mqsvc.exe:1908	UDP	ntecxp1-2:3527	*:*	
svchost.exe:936	UDP	ntecxp1-2:ntp	*:*	
svchost.exe:1096	UDP	ntecxp1-2:1900	*:*	

Process Explore shows a cmd shell spawned from IE browser

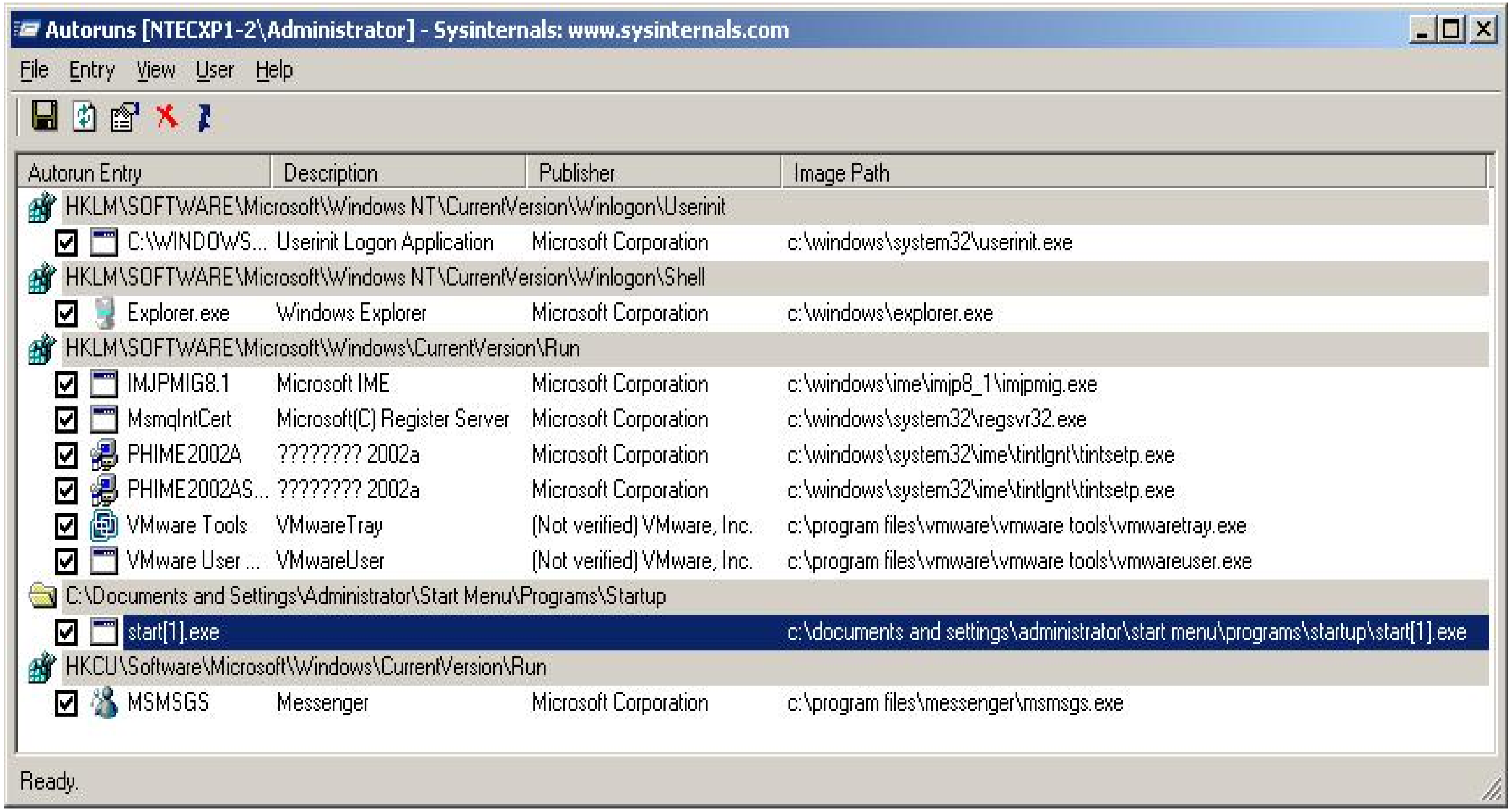


Process	PID	CPU	Description	Company Name
spoolsv.exe	1328		Spooler SubSyste...	Microsoft Corporation
inetinfo.exe	1468		Internet Informatio...	Microsoft Corporation
msdtc.exe	1492		MS DTC console ...	Microsoft Corporation
snmp.exe	1640		SNMP Service	Microsoft Corporation
VMwareServic...	1676		VMware Tools Se...	VMware, Inc.
mqsvc.exe	1908		Message Queuin...	Microsoft Corporation
mqtgsvc.exe	388		Windows NT MS...	Microsoft Corporation
UMGR32.exe	2480			
svchost.exe	4004		Generic Host Pro...	Microsoft Corporation
lsass.exe	664		LSA Shell (Export ...	Microsoft Corporation
⊟ explorer.exe	112		Windows Explorer	Microsoft Corporation
VMwareTray.exe	1132		VMwareTray	VMware, Inc.
mspaint.exe	496		Paint	Microsoft Corporation
⊟ iexplore.exe	3244		Internet Explorer	Microsoft Corporation
cmd.exe	2960		Windows Comma...	Microsoft Corporation
procexp.exe	2424	0.98	Sysinternals Proc...	Sysinternals

Type	Name
Desktop	\Default
Directory	\Windows
Directory	\KnownDlls
File	\Device\Afd\Endpoint
File	\Device\Afd\Endpoint
File	\Device\Afd\Endpoint
File	C:\Documents and Settings\Administrator\Desktop
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Language Gro...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\Alterna...
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale
Key	HKCU
Key	HKLM
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

CPU Usage: 1.96%   Commit Charge: 43.23%   Processes: 26

Autoruns shows the start[1].exe program

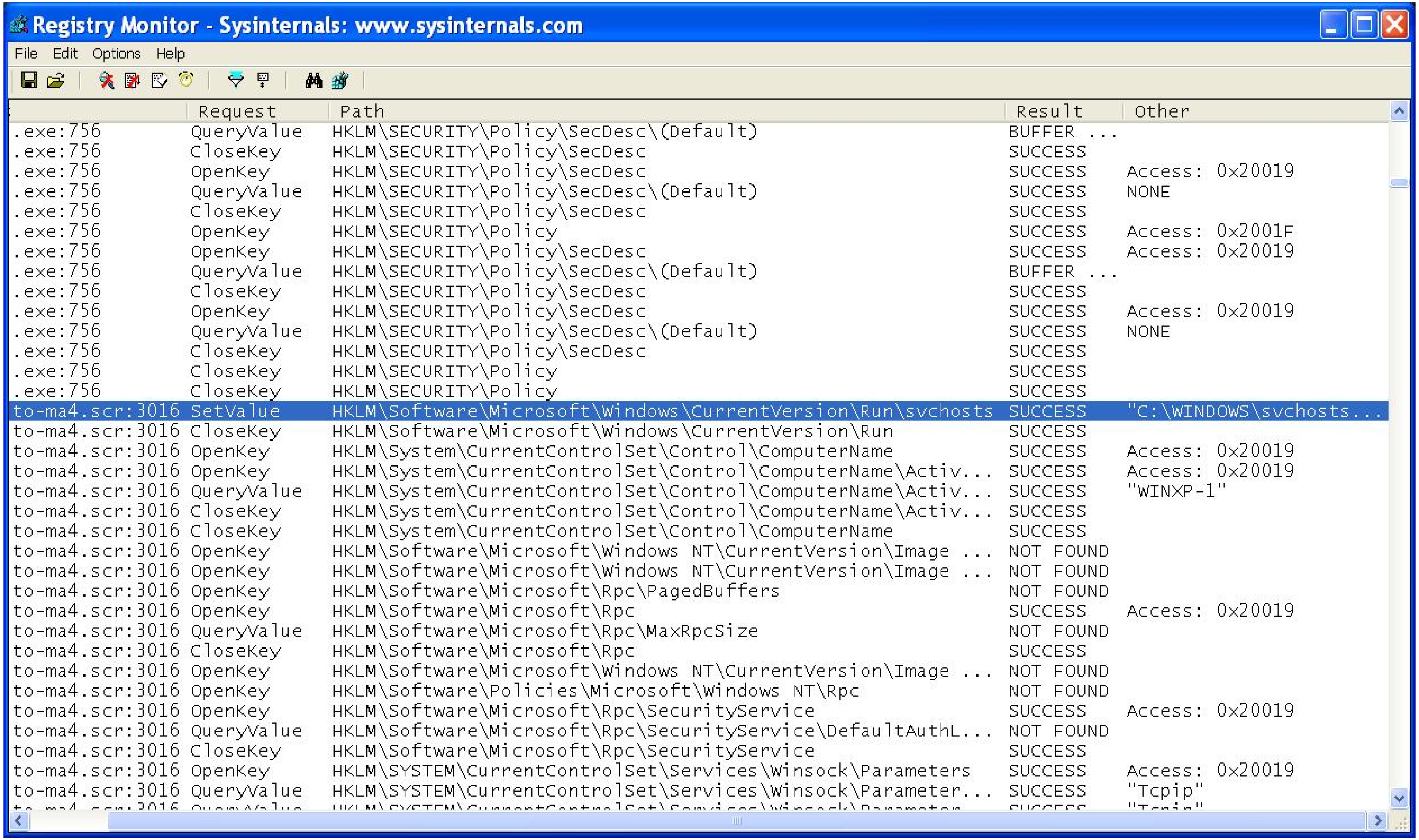


Autoruns [NTECXP1-2\Administrator] - Sysinternals: www.sysinternals.com

Autorun Entry	Description	Publisher	Image Path
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
☑ C:\WINDOWS...	Userinit Logon Application	Microsoft Corporation	c:\windows\system32\userinit.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
☑ Explorer.exe	Windows Explorer	Microsoft Corporation	c:\windows\explorer.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ IMJPMIG8.1	Microsoft IME	Microsoft Corporation	c:\windows\ime\imjp8_1\imjpmig.exe
☑ MsmqIntCert	Microsoft(C) Register Server	Microsoft Corporation	c:\windows\system32\regsvr32.exe
☑ PHIME2002A	???????? 2002a	Microsoft Corporation	c:\windows\system32\ime\tintlgnt\tintsetp.exe
☑ PHIME2002AS...	???????? 2002a	Microsoft Corporation	c:\windows\system32\ime\tintlgnt\tintsetp.exe
☑ VMware Tools	VMwareTray	(Not verified) VMware, Inc.	c:\program files\vmware\vmware tools\vmwaretray.exe
☑ VMware User ...	VMwareUser	(Not verified) VMware, Inc.	c:\program files\vmware\vmware tools\vmwareuser.exe
C:\Documents and Settings\Administrator\Start Menu\Programs\Startup			
☑ start[1].exe			c:\documents and settings\administrator\start menu\programs\startup\start[1].exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run			
☑ MSMSGS	Messenger	Microsoft Corporation	c:\program files\messenger\msmsgs.exe

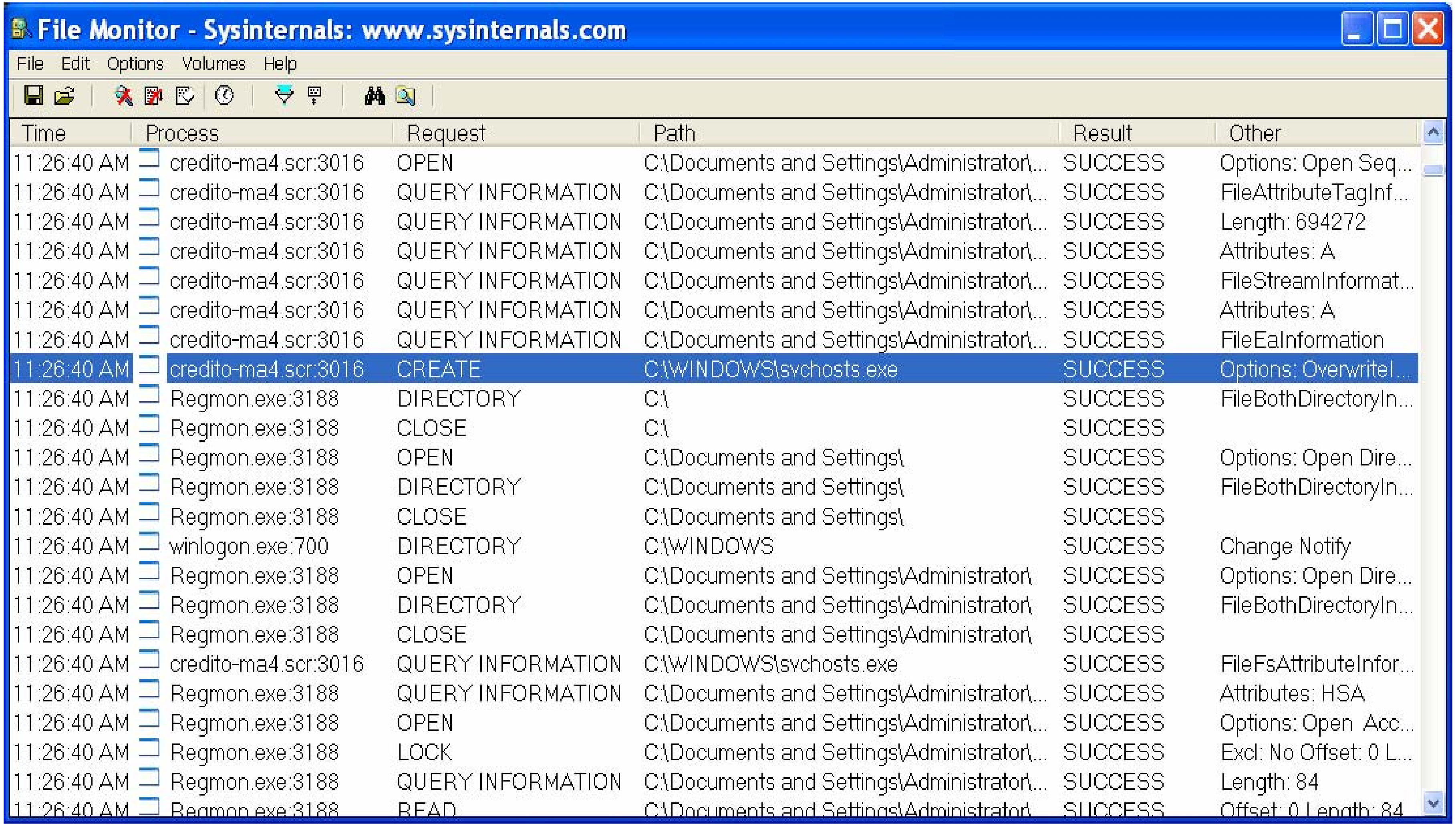
Ready.

Regmon shows a register modification by a malware



```
                 Request     Path                                                          Result      Other
.exe:756         QueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                        BUFFER ...
.exe:756         CloseKey    HKLM\SECURITY\Policy\SecDesc                                  SUCCESS
.exe:756         OpenKey     HKLM\SECURITY\Policy\SecDesc                                  SUCCESS     Access: 0x20019
.exe:756         QueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                        SUCCESS     NONE
.exe:756         CloseKey    HKLM\SECURITY\Policy\SecDesc                                  SUCCESS
.exe:756         OpenKey     HKLM\SECURITY\Policy                                          SUCCESS     Access: 0x2001F
.exe:756         OpenKey     HKLM\SECURITY\Policy\SecDesc                                  SUCCESS     Access: 0x20019
.exe:756         QueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                        BUFFER ...
.exe:756         CloseKey    HKLM\SECURITY\Policy\SecDesc                                  SUCCESS
.exe:756         OpenKey     HKLM\SECURITY\Policy\SecDesc                                  SUCCESS     Access: 0x20019
.exe:756         QueryValue  HKLM\SECURITY\Policy\SecDesc\(Default)                        SUCCESS     NONE
.exe:756         CloseKey    HKLM\SECURITY\Policy\SecDesc                                  SUCCESS
.exe:756         CloseKey    HKLM\SECURITY\Policy                                          SUCCESS
.exe:756         CloseKey    HKLM\SECURITY\Policy                                          SUCCESS
to-ma4.scr:3016  SetValue    HKLM\Software\Microsoft\Windows\CurrentVersion\Run\svchosts   SUCCESS     "C:\WINDOWS\svchosts...
to-ma4.scr:3016  CloseKey    HKLM\Software\Microsoft\Windows\CurrentVersion\Run            SUCCESS
to-ma4.scr:3016  OpenKey     HKLM\System\CurrentControlSet\Control\ComputerName            SUCCESS     Access: 0x20019
to-ma4.scr:3016  OpenKey     HKLM\System\CurrentControlSet\Control\ComputerName\Activ...   SUCCESS     Access: 0x20019
to-ma4.scr:3016  QueryValue  HKLM\System\CurrentControlSet\Control\ComputerName\Activ...   SUCCESS     "WINXP-1"
to-ma4.scr:3016  CloseKey    HKLM\System\CurrentControlSet\Control\ComputerName\Activ...   SUCCESS
to-ma4.scr:3016  CloseKey    HKLM\System\CurrentControlSet\Control\ComputerName            SUCCESS
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image ...   NOT FOUND
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image ...   NOT FOUND
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Rpc\PagedBuffers                      NOT FOUND
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Rpc                                   SUCCESS     Access: 0x20019
to-ma4.scr:3016  QueryValue  HKLM\Software\Microsoft\Rpc\MaxRpcSize                        NOT FOUND
to-ma4.scr:3016  CloseKey    HKLM\Software\Microsoft\Rpc                                   SUCCESS
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image ...   NOT FOUND
to-ma4.scr:3016  OpenKey     HKLM\Software\Policies\Microsoft\Windows NT\Rpc               NOT FOUND
to-ma4.scr:3016  OpenKey     HKLM\Software\Microsoft\Rpc\SecurityService                   SUCCESS     Access: 0x20019
to-ma4.scr:3016  QueryValue  HKLM\Software\Microsoft\Rpc\SecurityService\DefaultAuthL...   NOT FOUND
to-ma4.scr:3016  CloseKey    HKLM\Software\Microsoft\Rpc\SecurityService                   SUCCESS
to-ma4.scr:3016  OpenKey     HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters     SUCCESS     Access: 0x20019
to-ma4.scr:3016  QueryValue  HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameter...   SUCCESS     "Tcpip"
to-ma4.scr:3016  QueryValue  HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameter      SUCCESS     "Tcpip"
```

Filemon shows a file creation by a malware



Time	Process	Request	Path	Result	Other
11:26:40 AM	credito-ma4.scr:3016	OPEN	C:\Documents and Settings\Administrator\...	SUCCESS	Options: Open Seq...
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	FileAttributeTagInf...
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	Length: 694272
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	Attributes: A
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	FileStreamInformat...
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	Attributes: A
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	FileEaInformation
11:26:40 AM	credito-ma4.scr:3016	CREATE	C:\WINDOWS\svchosts.exe	SUCCESS	Options: OverwriteI...
11:26:40 AM	Regmon.exe:3188	DIRECTORY	C:\	SUCCESS	FileBothDirectoryIn...
11:26:40 AM	Regmon.exe:3188	CLOSE	C:\	SUCCESS	
11:26:40 AM	Regmon.exe:3188	OPEN	C:\Documents and Settings\	SUCCESS	Options: Open Dire...
11:26:40 AM	Regmon.exe:3188	DIRECTORY	C:\Documents and Settings\	SUCCESS	FileBothDirectoryIn...
11:26:40 AM	Regmon.exe:3188	CLOSE	C:\Documents and Settings\	SUCCESS	
11:26:40 AM	winlogon.exe:700	DIRECTORY	C:\WINDOWS	SUCCESS	Change Notify
11:26:40 AM	Regmon.exe:3188	OPEN	C:\Documents and Settings\Administrator\	SUCCESS	Options: Open Dire...
11:26:40 AM	Regmon.exe:3188	DIRECTORY	C:\Documents and Settings\Administrator\	SUCCESS	FileBothDirectoryIn...
11:26:40 AM	Regmon.exe:3188	CLOSE	C:\Documents and Settings\Administrator\	SUCCESS	
11:26:40 AM	credito-ma4.scr:3016	QUERY INFORMATION	C:\WINDOWS\svchosts.exe	SUCCESS	FileFsAttributeInfor...
11:26:40 AM	Regmon.exe:3188	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	Attributes: HSA
11:26:40 AM	Regmon.exe:3188	OPEN	C:\Documents and Settings\Administrator\...	SUCCESS	Options: Open Acc...
11:26:40 AM	Regmon.exe:3188	LOCK	C:\Documents and Settings\Administrator\...	SUCCESS	Excl: No Offset: 0 L...
11:26:40 AM	Regmon.exe:3188	QUERY INFORMATION	C:\Documents and Settings\Administrator\...	SUCCESS	Length: 84
11:26:40 AM	Regmon.exe:3188	READ	C:\Documents and Settings\Administrator\	SUCCESS	Offset: 0 Length: 84

Basic steps for Malware analysis

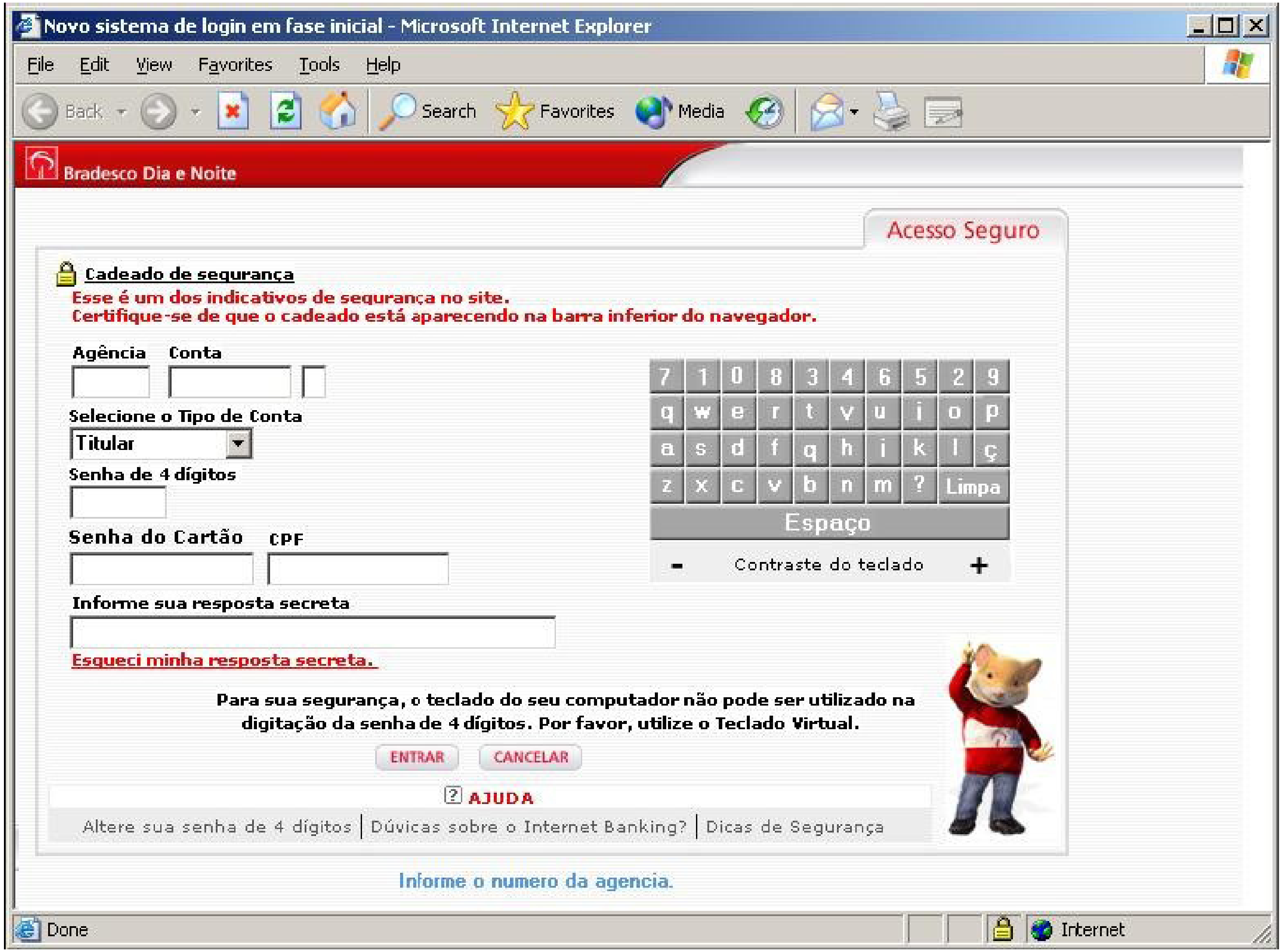
1. Visual Analysis: File size, type, strings, MD5 signature… etc
2. Behavioral Analysis: Run the malware in a well controlled and protected environment
3. Code Analysis: Reviewing its code

Case Study of a Malware

Upon inflection

1. copies itself to C:\WINDOWS\svchosts.exe
2. adds a registry entry to “HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”, ensuring “C:\WINDOWS\svchosts.exe” is run on system startup
3. sends a mail via smtp indicating successful installation
4. remains in memory, using DDE to check the URL being displayed in the foreground IE window. Once a matching URL (one of a list of Brazilian Internet banking sites) is typed, it:
    - creates a window over the IE browser to display an on-line bank login form to let the victim to type in his/her financial details
    - once the victim enter his/her details, under the assumption he/she is logging into the on-line banking site, the malware sends those login details back the attacker via an smtp mail
    - the malware then displays a “system error” dialog to the user, and removes itself from the system (quit from the memory and undo the registry)

The Malware creates a window over the IE browser to display an on-line bank login form



Cadeado de segurança

Esse é um dos indicativos de segurança no site.
Certifique-se de que o cadeado está aparecendo na barra inferior do navegador.

Agência Conta

Selecione o Tipo de Conta

Titular

Senha de 4 dígitos

Senha do Cartão CPF

Informe sua resposta secreta

Esqueci minha resposta secreta.

Para sua segurança, o teclado do seu computador não pode ser utilizado na digitação da senha de 4 dígitos. Por favor, utilize o Teclado Virtual.

Altere sua senha de 4 dígitos | Dúvicas sobre o Internet Banking? | Dicas de Segurança

Informe o numero da agencia.

Appendix

- Sysinternals
  - http://www.microsoft.com/technet/sysinternals/default.mspx
- Ethereal
  - http://www.ethereal.com/
- Foremost
  - http://foremost.sourceforge.net/
- Sandboxie
  - http://www.sandboxie.com/
- VMWare
  - http://www.vmware.com/

What is Playpen ?

Enclosure in which a baby or young child may play

http://playpen.ie.cuhk.edu.hk

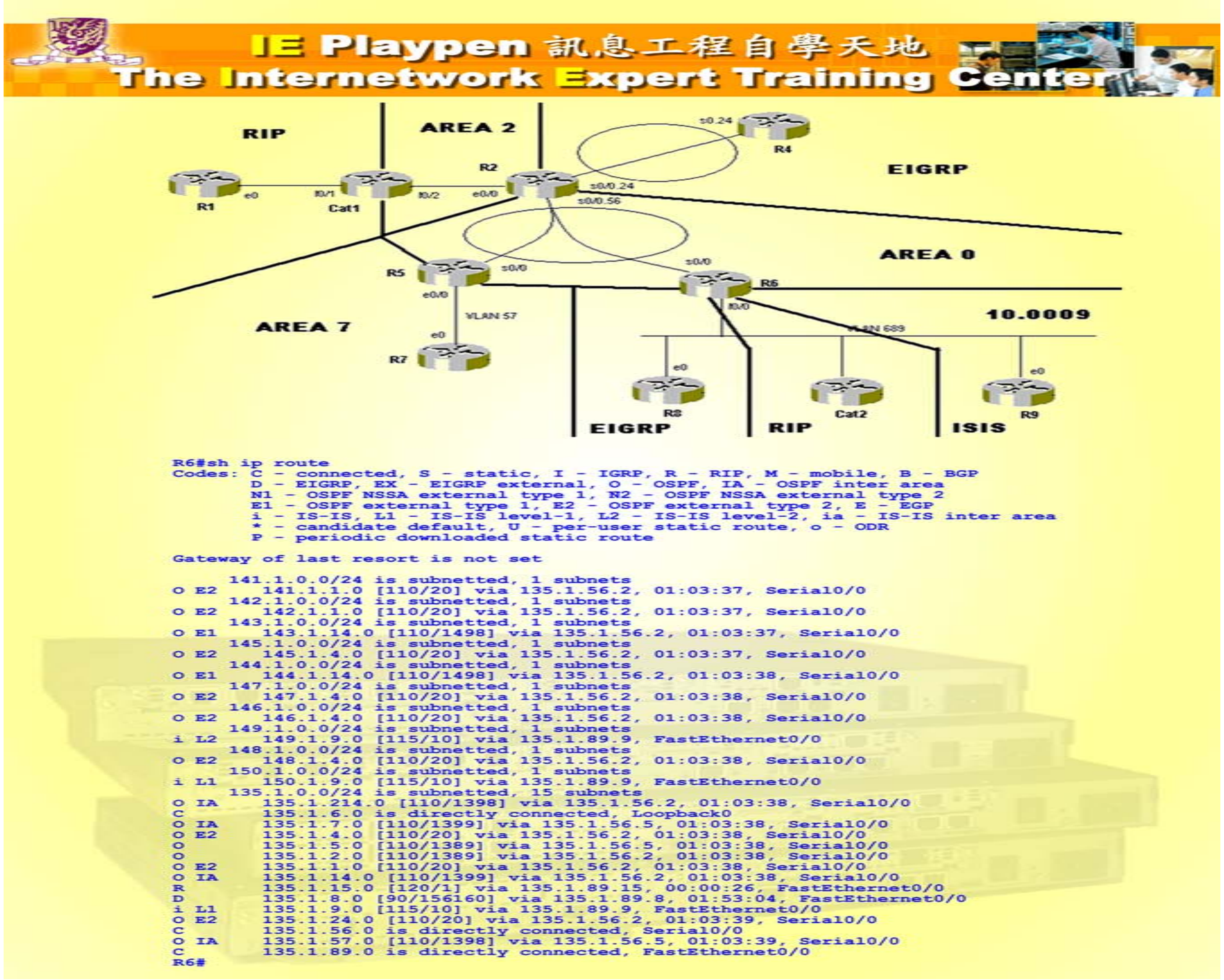
Objectives of Playpen

- Let students have the hand on experiment of managing a network
- Provide some useful Internet services for their community
- Provide a playground to test and develop students work
- Provide a platform for students to try some experiments that they cannot try on original lab or production network

Past Activities in Playpen

1. 3-Days Linux workshop
2. Firewall seminar
3. HoneyNet project seminar
4. Super Worm seminar
5. Next attack in Internet seminar
6. Worm Analysis seminar
7. Academic Networks in Asia seminar
8. Open day showcase demo project in 2002 and 2003
9. Web Portal project (http://playpen.ie.cuhk.edu.hk)
   (now in production and is still actively under enhancement)
10. Playpen network infrastructure enhancement
11. Game server project
12. PPTP based VPN using Window server project
13. Window server project
14. Access grid testing project
15. Simple video streaming testing project
16. System reborn card testing project
17. Library System
18. Buffer Overflow workshop
19. Computer Networking workshop
20. Phishing Seminar
21. Self learn Cisco equipment kit https://www.ie.cuhk.edu.hk/rack2/
22. Man-In-The-Middle (MITM) attack Seminar
23. Linux Talk 2005
24. Enhancement of Self Learn Network Equipment Kit for lab courses and summer workshops support
25. Security course and FYP support

Internetwork Expert Lab Setting

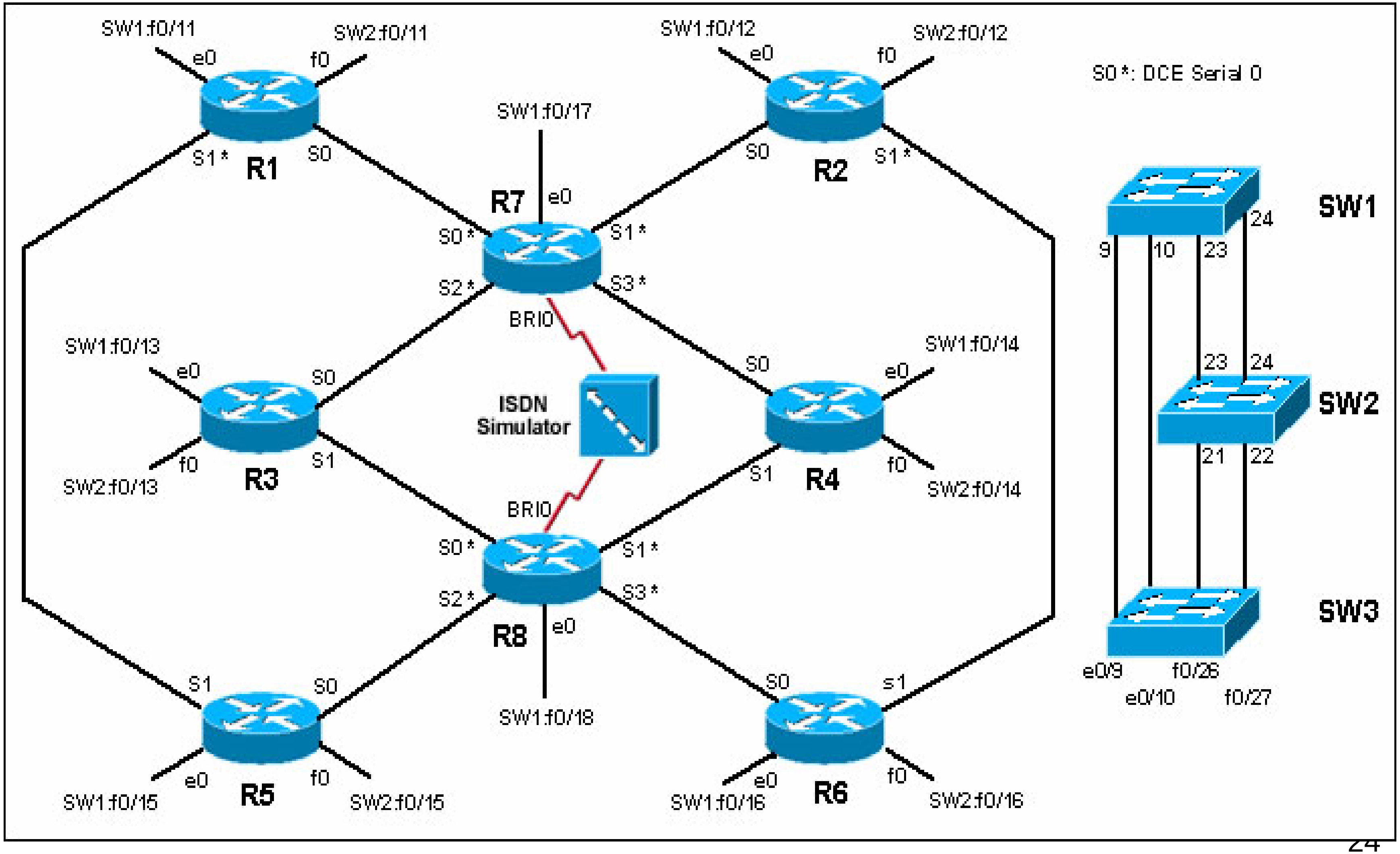


```
R6#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     141.1.0.0/24 is subnetted, 1 subnets
O E2    141.1.1.0 [110/20] via 135.1.56.2, 01:03:37, Serial0/0
     142.1.0.0/24 is subnetted, 1 subnets
O E2    142.1.1.0 [110/20] via 135.1.56.2, 01:03:37, Serial0/0
     143.1.0.0/24 is subnetted, 1 subnets
O E1    143.1.14.0 [110/1498] via 135.1.56.2, 01:03:37, Serial0/0
     145.1.0.0/24 is subnetted, 1 subnets
O E2    145.1.4.0 [110/20] via 135.1.56.2, 01:03:37, Serial0/0
     144.1.0.0/24 is subnetted, 1 subnets
O E1    144.1.14.0 [110/1498] via 135.1.56.2, 01:03:38, Serial0/0
     147.1.0.0/24 is subnetted, 1 subnets
O E2    147.1.4.0 [110/20] via 135.1.56.2, 01:03:38, Serial0/0
     146.1.0.0/24 is subnetted, 1 subnets
O E2    146.1.4.0 [110/20] via 135.1.56.2, 01:03:38, Serial0/0
     149.1.0.0/24 is subnetted, 1 subnets
i L2    149.1.9.0 [115/10] via 135.1.89.9, FastEthernet0/0
     148.1.0.0/24 is subnetted, 1 subnets
O E2    148.1.4.0 [110/20] via 135.1.56.2, 01:03:38, Serial0/0
     150.1.0.0/24 is subnetted, 1 subnets
i L1    150.1.9.0 [115/10] via 135.1.89.9, FastEthernet0/0
     135.1.0.0/24 is subnetted, 15 subnets
O IA    135.1.214.0 [110/1398] via 135.1.56.2, 01:03:38, Serial0/0
C       135.1.6.0 is directly connected, Loopback0
O IA    135.1.7.0 [110/1399] via 135.1.56.5, 01:03:38, Serial0/0
O E2    135.1.4.0 [110/20] via 135.1.56.2, 01:03:38, Serial0/0
O       135.1.5.0 [110/1389] via 135.1.56.5, 01:03:38, Serial0/0
O       135.1.2.0 [110/1389] via 135.1.56.2, 01:03:38, Serial0/0
O E2    135.1.1.0 [110/20] via 135.1.56.2, 01:03:38, Serial0/0
O IA    135.1.14.0 [110/1399] via 135.1.56.2, 01:03:38, Serial0/0
R       135.1.15.0 [120/1] via 135.1.89.15, 00:00:26, FastEthernet0/0
D       135.1.8.0 [90/156160] via 135.1.89.8, 01:53:04, FastEthernet0/0
i L1    135.1.9.0 [115/10] via 135.1.89.9, FastEthernet0/0
O E2    135.1.24.0 [110/20] via 135.1.56.2, 01:03:39, Serial0/0
C       135.1.56.0 is directly connected, Serial0/0
O IA    135.1.57.0 [110/1398] via 135.1.56.5, 01:03:39, Serial0/0
C       135.1.89.0 is directly connected, FastEthernet0/0
R6#
```

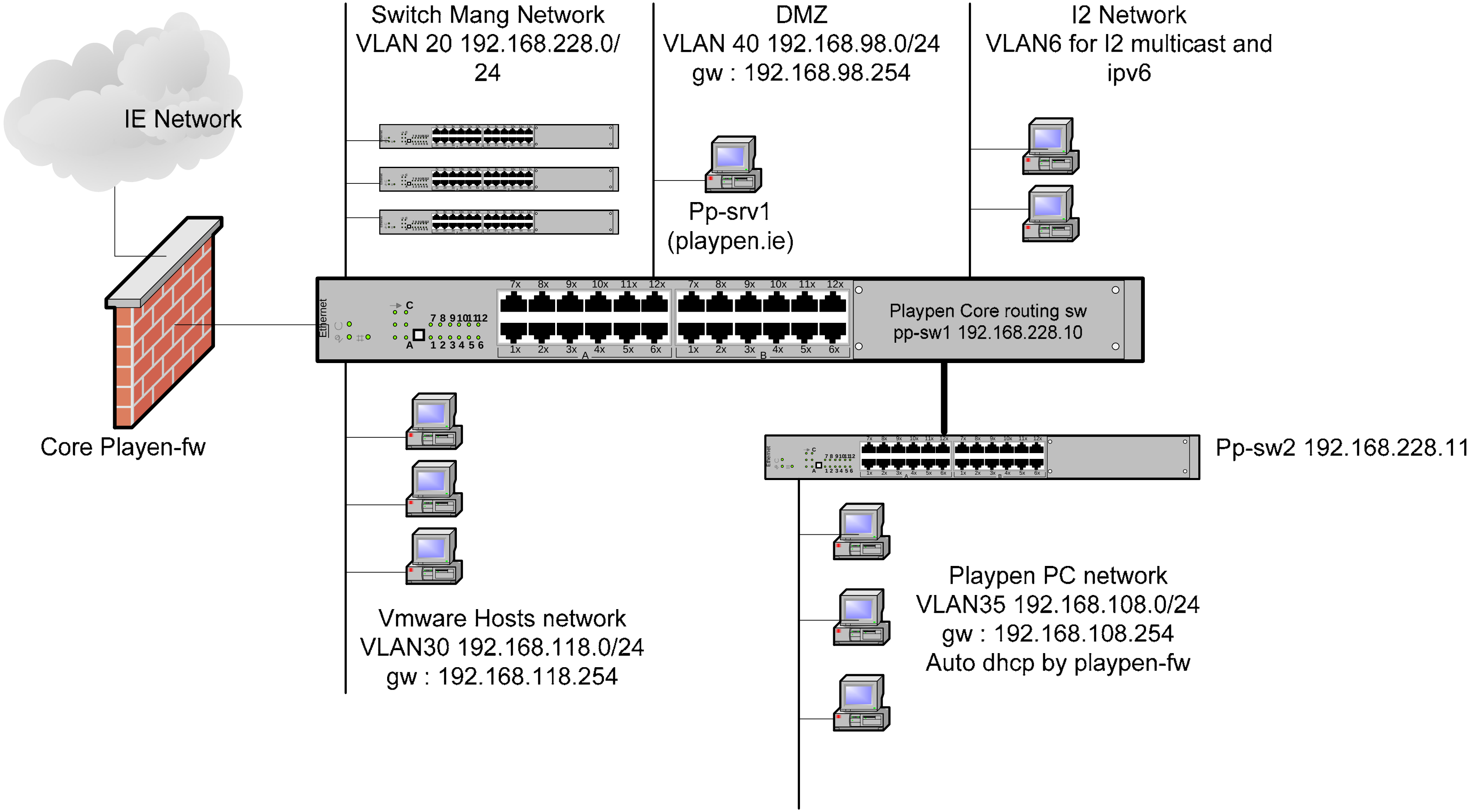
Equipment in Playpen

- Over 15 PC
- Over 5 servers which can emulate over 80 virtual hosts
- Over 26 Routers (2500, 2600, 1721, 7513)
- Over 5 switches (2900, 3500, LS1010)
- ISDN equipment
- Other different OS and machines (Solaris, Linux, Iris... etc)

Self learn Cisco equipment kit



IE Playpen Network Diagram



IE Network

Core Playen-fw

Switch Mang Network
VLAN 20 192.168.228.0/
24

DMZ
VLAN 40 192.168.98.0/24
gw : 192.168.98.254

Pp-srv1
(playpen.ie)

I2 Network
VLAN6 for I2 multicast and
ipv6

Playpen Core routing sw
pp-sw1 192.168.228.10

Pp-sw2 192.168.228.11

Vmware Hosts network
VLAN30 192.168.118.0/24
gw : 192.168.118.254

Playpen PC network
VLAN35 192.168.108.0/24
gw : 192.168.108.254
Auto dhcp by playpen-fw