

Malware Analysis – Part V

Author: Justin Acquaro

Abstract:

This paper will cover an analysis of real malware captured on a compromised machine. The analysis will follow the information provided from the SANS website (<http://handlers.sans.org/pbueno/ma5.html>)

Table of Contents

Malware Analysis – Part V	1
Abstract:	1
Table of Contents	2
Introduction	3
Offline Analysis	3
Online Analysis	7
Answers	8
Section A	11
Section B	13
Section C	16
Section D	18

Introduction

A user called the help desk complaining that his computer was too slow, after following the basic IR procedures; the Incident Response Team was called. The Incident Response Team checked his computer and found the cretzu compacted file, other information found listed in section A. The file found had the following name and MD5 checksum:

Malware MD5 and name: ecd45b584f7a1e50bb044646f4f31l3t - cretzu.exe-orig-ecd45b584f7a1e50bb044646f4abb0be

Offline Analysis

After downloading and unzipping the malware from the SANS site, I ran an MD5 check to make sure this file had not been tampered with. Below are the results from the checksum output:

```
echelon MALWARE # md5sum cretzu.exe-orig-ecd45b584f7a1e50bb044646f4abb0be  
ecd45b584f7a1e50bb044646f4abb0be cretzu.exe-orig-ecd45b584f7a1e50bb044646f4abb0be
```

As you can see the MD5sum did in fact match so my next step is to rename the file to cretzu.exe for easier analysis as well as run through the strings in the binary to determine if this file is packed or not. From the output of the strings utility I was able to determine that this file was packed with winrar. Below is the string which tells me so:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?> <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> <assemblyIdentity version="1.0.0.0" processorArchitecture="X86" name="Roshal.WinRAR.WinRAR" type="win32" />  
<description>WinRAR archiver.</description> <dependency> <dependentAssembly>  
<assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0" processorArchitecture="X86" publicKeyToken="6595b64144ccf1df" language="*" /> </dependentAssembly> </dependency> </assembly>
```

Using the unrar command on the cretzu.exe file I get the following output:

```
echelon MALWARE # unrar x cretzu.exe

UNRAR 3.51 freeware   Copyright (c) 1993-2005 Alexander Roshal

Extracting from cretzu.exe

; [ > owned by mad ! < ]

Path=%systemroot%\system32\drivers\
SavePath
Setup=%systemroot%\system32\drivers\sup.bat
Silent=1
Overwrite=1

Extracting aliases.ini           OK
Extracting control.ini           OK
Extracting mirc.ico               OK
Extracting mirc.ini               OK
Extracting moo.dll                OK
Extracting nicks.txt              OK
Extracting perform.ini            OK
Extracting popups.ini             OK
Extracting radmin.txt             OK
Extracting remote.ini             OK
Extracting run.exe                 OK
Extracting script.ini             OK
Extracting servers.ini            OK
Extracting sup.bat                 OK
Extracting sup.reg                 OK
Extracting svchost.exe            OK
Extracting users.ini              OK
All OK
```

Looks like “mad” is the culprit, this autorun script sets the working path to “%systemroot%\system32\drivers\” extracting all the files there as well as launching the sup.bat script silently. Sup.bat contains the following:

```
echelon MALWARE # cat sup.bat
@regedit /s sup.reg
@exit
```

This batch file inserts the data in sup.reg silently and exits without printing anything to the users screen. The contents of sup.reg are listed below:

```
echelon MALWARE # cat sup.reg
REGEDIT4
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"svchost.exe"="C:\\WINNT\\system32\\drivers\\svchost.exe"
"system32"="C:\\WINDOWS\\system32\\drivers\\svchost.exe"
```

This file will make 2 entries to the “HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run” key the first entry will start svchost.exe if it is located in the C:\\WINNT\\system32\\drivers\\ folder and the other will start svchost.exe if it is located in the C:\\WINDOWS\\system32\\drivers\\. This is obviously poorly written or thought out the authors original intent is to make sure is executable would run no matter what the %WINDIR% is. As a result he makes 2 entries one of which is bound to error upon startup alarming the user of its presence.

After taking a look at this svchost.exe file I determine that it is a mIRC (<http://mirc.com>) executable. mIRC is a free popular customizable internet relay chat client for windows. The following strings lead me to believe this is the executable.

```
mIRC
mIRC
mirc.ini
urls.ini
Messages
Channels
Finger
Links
MS Shell Dlg
mIRC_Toolbar
mIRC_Uninstall
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity version="1.0.0.0" processorArchitecture="X86" name="mIRC.mIRC.mIRC"
type="win32"/>
<description>Internet Relay Chat Software</description>
```

Some of the other files extracted are files normally found with a mIRC intallation, files include:

- Aliases.ini
- Mirc.ico
- Mirc.ini
- Popups.ini
- Servers.ini

All of the other files with the exception of “run.exe” and “moo.dll” seem to be script files for mIRC. The file moo.dll is used to get information about the host, such as uptime, cpu , screen, memory, and interface information. Below is output from the script which shows the use of this DLL.

```
n111= .notice $nick ^C2,15 [System: $dll(moo.dll,osinfo,_) ] $&
n112= [PC-Uptime:^C^C4,15 $dll(moo.dll,uptime,_) ^C^C2,15] $&
n113= [BoT-Ontime:^C^C4,15 $uptime(server,1) ^C^C2,15] $&
n114= [Processor: $dll(moo.dll,cpuinfo,_) ] $&
n115= [Screen: $dll(moo.dll,screeninfo,_) ] $&
n116= [RAM: $gettok($dll(moo.dll,meminfo,_) ,2-,32) ] $&
n117= [Internet: $dll(moo.dll,interfaceinfo,_) ] ^C
```

I can not find any reference to the file called “run.exe” in any of the other files; this leads me to believe that it is never run. If this file run.exe is ever run it would make another startup entry noted by the string:

```
Software\Microsoft\Windows\CurrentVersion\Run" ANTIVIRUSSERVICES P
c:\windows\services\antivirus\mir32.exe
```

It also appears to run this file from this location but doesn’t attempt to copy the file into that location or create that file. My guess is that this is a file left over from a variant of this malware. The following string may also give us some more information about the author.

```
C:\Documents and Settings\Corey\Desktop\projects\autostart\Project1.vbp
```

It seems that Corey should be a little more careful with metadata included in files created on his machine.

Other files seem to be scripts and or variables for this mIRC bot see the answers section for a list of functionality provided by each.

Upon startup it appears that the mIRC bot attempts to connect to one of the many Underet IRC servers located in servers.ini. It also chooses a random name from the file nicks.txt and appears to attempt to connect to the following channels “#Creatu”, “#Cretu”, and “#Creatzu”.

Online Analysis

Armed with a copy of VMWARE, ethereal, regmon, procexp, and filemon I set out to find out for sure if my offline analysis was accurate. I setup VMWARE running ethereal, regmon, procexp, and filemon then I ran the binary and took note (See Section B for all files).

Once I clicked the executable everything went according to plan, the files extracted to the “C:\windows\system32\drivers\” folder and the registry settings for startup were added. Rather than reboot the system and possibly miss some initial configuration or startup routines I decided to start the malware manually.

Clicking on the malware I noticed the blank icon loaded up in the system tray as well as some network traffic. Filemon and regmon started scrolling furiously, the mIRC client seems to setups some default system wide parameters; adding registry settings to recognize IRC related files. This seems to be a function of mIRC and not malicious. On startup the malware sets the NICK to a random name and connects to an IRC server in the Netherlands.

```
NICK Zx0hHr5aR
USER cacat "" "Amsterdam.NL.EU.undernet.org" :emerson
NOTICE AUTH :*** Checking Ident
PING :839433673
PONG :839433673
```

It sets the USERHOST to the same as the nick ,attempts to change the nick again, and sets the mode for +i and +x which makes the IRC user “invisible” and “partially hides the IP address of the client”. It then tries to JOIN 3 different channels #Creatu,#Cretu, and #Cretzu.

```
MODE Zx0hHr5aR +i
MODE Zx0hHr5aR +x
JOIN #Creatu,#Cretu,#Cretzu
```

The server disallows the NICK change, sets the 2 modes for +i and +x and gets denied access to the #Creatu and #Cretu channels for lack of password “+k”

```
:Amsterdam.NL.EU.undernet.org 302 Zx0hHr5aR :Zx0hHr5aR=+~cacat@167.206.73.32
:Amsterdam.NL.EU.undernet.org 433 Zx0hHr5aR weinrich :Nickname is already in use.
:Zx0hHr5aR!~cacat@167.206.73.32 MODE Zx0hHr5aR :+i
:Zx0hHr5aR!~cacat@167.206.73.32 MODE Zx0hHr5aR :+x
:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Creatu :Cannot join channel (+k)
:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Cretu :Cannot join channel (+k)
```

Once we join the #Cretzu channel we see the channel list of people which was at the time of my connection ~350; 66 of which are Channel Ops (Determined by parsing user list with script written in section C). Nothing else was noted on the system with the exception of a few joins and leaves from the channel.

Answers

1. Is this file packed? If so, which packer?

- a. This file was packed with winrar

2. Without running the file, is it possible to identify what this malware can and will do?

- a. See offline analysis

3. Now, using any methods available to you, which changes, if any, will this malware do in the system, among new files and registry entries...?

- a. Changes include, modification to windows startup registry keys as well as files being loaded in the %WINDIR%\system32\drivers\ folder. Other changes to the system registry where made but reflect changes made by the mIRC client and not the malware wrapper around it.

4. Now, what is the purpose of this malware?

- a. This malware is an attempt at creating a BOT network, used for DDOS style attacks and remote scanning possibly for insecure radmin services.

5. When will this malware be triggered/start?

- a. The malware is not started right away but rather on next system reboot

6. Can you explain the netstat output?

- a. The netstat output shows the connection made by the malware to an IRC server:

“TCP 192.168.0.53:1036 195.47.220.2:6667 ESTABLISHED”

As well as what appears to be the scanning features of the BOT scanning a range of IP's on port 4899 which seems to be 'Radmin':

```
TCP 192.168.0.53:1088 xxx.80.0.50:4899 SYN_SENT
TCP 192.168.0.53:1089 xxx.80.0.51:4899 SYN_SENT
TCP 192.168.0.53:1090 xxx.80.0.52:4899 SYN_SENT
TCP 192.168.0.53:1091 xxx.80.0.53:4899 SYN_SENT
TCP 192.168.0.53:1092 xxx.80.0.54:4899 SYN_SENT
TCP 192.168.0.53:1093 xxx.80.0.55:4899 SYN_SENT
TCP 192.168.0.53:1094 xxx.80.0.56:4899 SYN_SENT
TCP 192.168.0.53:1095 xxx.80.0.57:4899 SYN_SENT
TCP 192.168.0.53:1096 xxx.80.0.58:4899 SYN_SENT
```

TCP 192.168.0.53:1097 xxx.80.0.59:4899 SYN_SENT

7. What about the TaskManager screenshot? What useful information can you get?

- a. The last “svchost.exe” process is being run under a user’s context and scvhost.exe at least in my experiences is always run as SYSTEM or a SERVICE. This sends up red flags for me.

8. About the creztu file, please explain each of the files that it contains :)

aliases.ini	Aliasing commands for mIRC
Control.ini	As if mIRC version 6.01 “The control dialog lists, ie. ignore, voice, protect, op, are now stored in a control.ini file”
Mirc.ico	A blank icon to hide mIRC from showing in the taskbar
Moo.dll	Dll for getting OS and hardware information
Nicks.txt	Random names used to generate a NICK
Perform.ini	Used to set commands to perform automatically on connect.
Popups.ini	Sets the popups which are like alias but require mouse intervention rather than typing /<command>
Radmin.txt	Header for scan results of port 4899 “Radmin”
Remote.ini	By default the remote users list, variables and scripts are saved in the remote.ini file.
Run.exe	Looks like left over from another variant of this BOT/ Backdoor / Trojan
Script.ini	Scripts for this BOT such as a SCANNER, file find, random name gen....etc
Servers.ini	List of IRC servers in the Undernet range
Sup.bat	Install script file run by the winrar SFX
Sup.reg	Reg file containing the registry entries added start the mIRC BOT up
Svchost.exe	mIRC application with a name change
Users.ini	Sets the users which can talk to the bot

9. Which other information about the channel can you provide?

I was only able to join the #Cretzu channel which had ~ 350 users 66 of them had operator status. The other 2 channels appear to be locked with the +k option.

10. How would you call this Malware and describe what this category of malware do?

Backdoor/IRC Bot. typically used for DDOS attacks, but can be used for a number of things such as warez file sharing, hacking, and harvesting information such as credit cards.

11. Please explain the logs above.

This log is an IRC session log most which shows in order of events:

- a. Ping from the server to the client
- b. Client disconnect indicated by a Connection reset by peer
- c. User join
- d. Client disconnect indicated by a Connection reset by peer
- e. User changing NICK
- f. User join
- g. Client disconnect by timeout
- h. User join

Below is a more readable version of the log files:

```
PING :Lelystad.NL.EU.UnderNet.Org
:5mui`lei!shoby17---@68-112-234-6.dhcp.oxfr.ma.charter.com QUIT :Read error: Connection
reset by peer
:angelique!~cacat@172.206.142.94 JOIN #Creat
:Jo_m46!~cacat@ip68-9-84-60.ri.ri.cox.net JOIN #Creat
:Nht_Boy!~shashank@107.67.63.81.cust.bluewin.ch QUIT :Read error: Connection reset by peer
:angelique!~cacat@172.206.142.94 NICK :PatruOchi
:mari37!phillip@81-235-146-201-no33.tbcn.telia.com JOIN #Creat
:|paritul!mitul_@cpe-67-11-255-16.satx.res.rr.com QUIT :Ping timeout
:SHOGHUN!cacat@ACCE8E5E.ipt.aol.com JOIN #Creat
```

Section A

What follows bellow are some real data from the compromised machine.

```
C:\Documents and Settings\malware>netstat -an
```

Active Connections

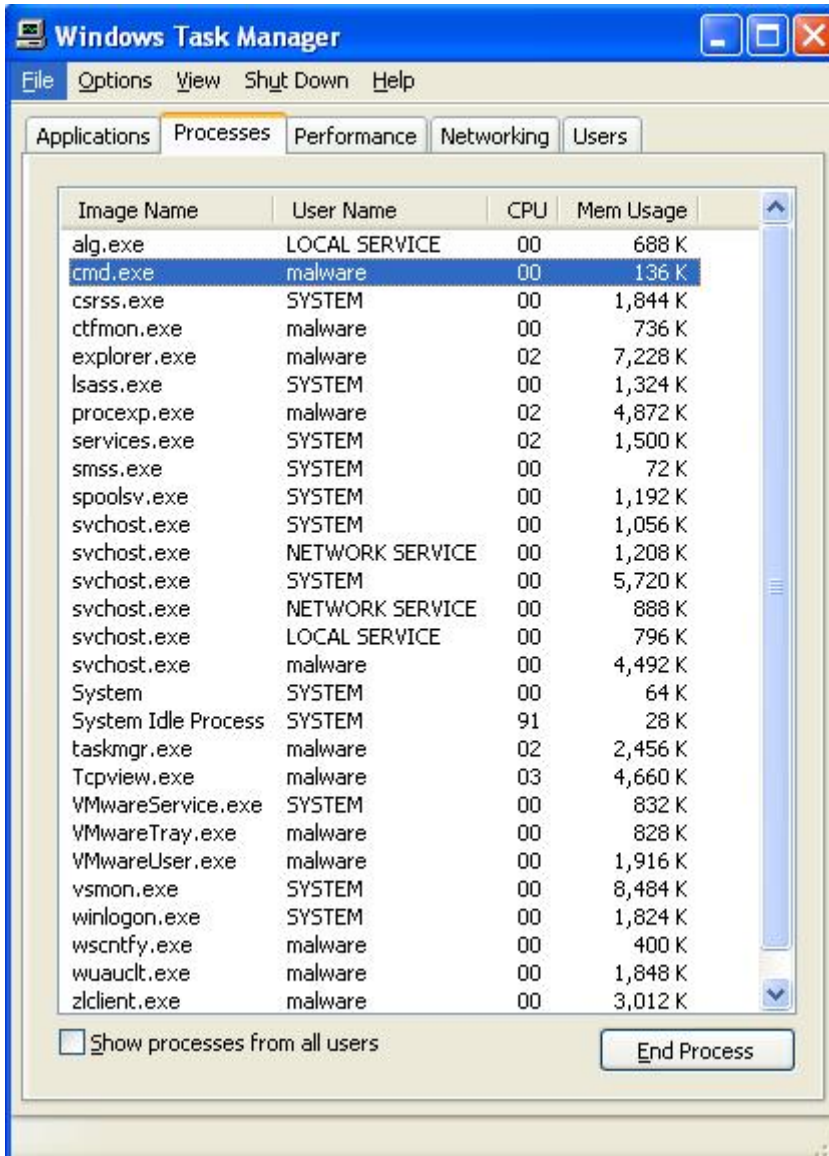
```
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1025 0.0.0.0:0 LISTENING
TCP 192.168.0.53:139 0.0.0.0:0 LISTENING
TCP 192.168.0.53:1036 195.47.220.2:6667 ESTABLISHED
TCP 192.168.0.53:1088 xxx.80.0.50:4899 SYN_SENT
TCP 192.168.0.53:1089 xxx.80.0.51:4899 SYN_SENT
TCP 192.168.0.53:1090 xxx.80.0.52:4899 SYN_SENT
TCP 192.168.0.53:1091 xxx.80.0.53:4899 SYN_SENT
TCP 192.168.0.53:1092 xxx.80.0.54:4899 SYN_SENT
TCP 192.168.0.53:1093 xxx.80.0.55:4899 SYN_SENT
TCP 192.168.0.53:1094 xxx.80.0.56:4899 SYN_SENT
TCP 192.168.0.53:1095 xxx.80.0.57:4899 SYN_SENT
TCP 192.168.0.53:1096 xxx.80.0.58:4899 SYN_SENT
TCP 192.168.0.53:1097 xxx.80.0.59:4899 SYN_SENT
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1026 *:*
UDP 0.0.0.0:1088 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.0.53:123 *:*
UDP 192.168.0.53:137 *:*
UDP 192.168.0.53:138 *:*
UDP 192.168.0.53:1900 *:*
```

Excerpt of some logs acquired on the machine

```
PING :Lelystad.NL.EU.UnderNet.Org :`5mui`lei!shoby17---@68-112-234-
6.dhcp.oxfr.ma.charter.com QUIT :Read error: Connection reset by peer
:angelique!~cacat@172.206.142.94 JOIN #Creat :Jo_m46!~cacat@ip68-9-84-
60.ri.ri.cox.net JOIN #Creat :Nht_Boy!~shashank@107.67.63.81.cust.bluewin.ch QUIT
:Read error: Connection reset by peer :angelique!~cacat@172.206.142.94 NICK
:PatruOchi :mari37!phillip@81-235-146-201-no33.tbcn.telia.com JOIN #Creat
```

:|paritul|!mitul_@cpe-67-11-255-16.satx.res.rr.com QUIT :Ping timeout
:SHOGHUN!cacat@ACCE8E5E.ipt.aol.com JOIN #Creat

Also, bellow is a screenshot of the TaskManager:



Section B

NICK Zx0hHr5aR

USER cacat "" "Amsterdam.NL.EU.undernet.org" :emerson

NOTICE AUTH :*** Checking Ident

PING :839433673

PONG :839433673

:Amsterdam.NL.EU.undernet.org 001 Zx0hHr5aR :Welcome to the UnderNet IRC Network, Zx0hHr5aR
:Amsterdam.NL.EU.undernet.org 002 Zx0hHr5aR :Your host is Amsterdam.NL.EU.undernet.org, running
version u2.10.11.07(pre3)
:Amsterdam.NL.EU.undernet.org 003 Zx0hHr5aR :This server was created Tue Jun 28 2005 at 00:45:46
CEST
:Amsterdam.NL.EU.undernet.org 004 Zx0hHr5aR Amsterdam.NL.EU.undernet.org u2.10.11.07(pre3)
dioswkgx biklmpstvr bklov
:Amsterdam.NL.EU.undernet.org 005 Zx0hHr5aR WHOX WALLCHOPS WALLVOICES USERIP
CPRIVMSG CNOTICE SILENCE=15 MODES=6 MAXCHANNELS=10 MAXBANS=45 NICKLEN=12
MAXNICKLEN=15 :are supported by this server
:Amsterdam.NL.EU.undernet.org 005 Zx0hHr5aR TOPICLEN=160 AWAYLEN=160 KICKLEN=160
CHANTYPES=#& PREFIX=(ov)@+ CHANMODES=b,k,l,imnpstr CASEMAPPING=rfc1459
NETWORK=UnderNet :are supported by this server
:Amsterdam.NL.EU.undernet.org 251 Zx0hHr5aR :There are 25455 users and 73699 invisible on 25
servers
:Amsterdam.NL.EU.undernet.org 252 Zx0hHr5aR 54 :operator(s) online
:Amsterdam.NL.EU.undernet.org 253 Zx0hHr5aR 165 :unknown connection(s)

USERHOST Zx0hHr5aR

:Amsterdam.NL.EU.undernet.org 254 Zx0hHr5aR 42072 :channels formed
:Amsterdam.NL.EU.undernet.org 255 Zx0hHr5aR :I have 5017 clients and 1 servers
:Amsterdam.NL.EU.undernet.org NOTICE Zx0hHr5aR :Highest connection count: 5034 (5033 clients)
:Amsterdam.NL.EU.undernet.org 375 Zx0hHr5aR :- Amsterdam.NL.EU.undernet.org Message of the Day
-
:Amsterdam.NL.EU.undernet.org 372 Zx0hHr5aR :This service is provided by EuroNet Internet &
Wanadoo - <http://www.wanadoo.nl>
:Amsterdam.NL.EU.undernet.org 372 Zx0hHr5aR :.Type /MOTD to read the AUP before continuing using
this service..
:Amsterdam.NL.EU.undernet.org 372 Zx0hHr5aR :The message of the day was last changed: 2003-7-10
21:21
:Amsterdam.NL.EU.undernet.org 376 Zx0hHr5aR :End of /MOTD command.
:Amsterdam.NL.EU.undernet.org NOTICE Zx0hHr5aR :on 1 ca 1(2) ft 10(10)

NICK :weinrich

MODE Zx0hHr5aR +i

MODE Zx0hHr5aR +x

JOIN #Creatu,#Cretu,#Cretzu

:Amsterdam.NL.EU.undernet.org 302 Zx0hHr5aR :Zx0hHr5aR=+~cacat@167.206.73.32
:Amsterdam.NL.EU.undernet.org 433 Zx0hHr5aR weinrich :Nickname is already in use.
:Zx0hHr5aR!~cacat@167.206.73.32 MODE Zx0hHr5aR :+i
:Zx0hHr5aR!~cacat@167.206.73.32 MODE Zx0hHr5aR :+x
:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Creatu :Cannot join channel (+k)
:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Cretu :Cannot join channel (+k)
:Zx0hHr5aR!~cacat@167.206.73.32 JOIN #Cretzu
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :Zx0hHr5aR fat-a linux5543 THE_DON
__jit__ __unatic Gest luci10 @Golanu__retu__ Fb8oQu7nK supar9187 cr3tu__ JuPaN2585 Te-
Sarut aziz Smntanel Chicken^ Cretz468 Muie2178 Muie2713 karl Muie6244 ____asa_ Mirinda
@WeLLs_ Muie5266 @Regina__ @lasa-ma_reatza__ buton DaniMAD_ ido^ cta_ fredy Senzuala_
____sa_ @Nu__ nzhtnwysgt @Cr3tzu_ Suzana__ @Pin_ @azor_runeta__ Gagica_ ipatic Cretu6153
AnuS Catieree Sexoasa_mechera_Accept____tanta
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :Robert`o_Maximus15 Regina_Otalat
Husen Ui7gZl6bX Constanta aleboss tarfa guleksi yuh_szasha printesa_elia29 Freaka02 @Creatu_
DeNNyS`_cajit____oasa_ Buc Copila_ Muie1105 __echera_stramba_@_nstanta Susanu__ecajit__
@Fata_ Estana46 BNCisi cta__tu__ mwe_dragos14 supar1403 JuPaN_doc34 Cretu2296_rumoasa_
@Sampo__etzu__ Dalena90 sherban19 Cretu__ Iuanita Cretzu_ Paine` sweet_jupana__arat__
Muie_oltaj^^ @fetitza_

MODE #Cretzu

:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :sunos____ Gaby1 cr3tu9827 __parat__
stapa8012 _|____ necajit_ linux6799 Cretu__ Muie2571 sunos__ Cretu_ Bruneta_ _|____
Desiree__ __anu__ Georgeta_ fata__ Game_Over Ffeliccia57 cvv_ris24 Belea_ Creat3293 __apanu__
trku Galileo__ @Creat4991 cr3tu__ axuo rugieri yingsha `r`G` @__ta__ reata__ tata iubit__
@print9752 NyCk-18 Da_33 ____tesa_ yee Sen}{}{ Discovery stapanu_ cr3tu8610 necajit__ Nebunatic16
necaj3843 |SD stapa7408
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :supar8005 Schikatomo21 Golanu aeneas T-
Online sedef __3aTzZa belea Nkameron ____os____ cr3tu7731 necaj5933 @mwe suparat__ Creatza_
Cretu857 _ancomat_ Osalam cc_ Cretu9912 batrana __ntesa_ reymond99 sebiropa ____na tandrei
Nick_34 SutFeroce anru15 PlantaSme BLONDA17 utu19 @_retzuL_ gaouz_ __intesa_ Geo_19 @Singura
onstanta CretzuL frumoasa Blonda Creat9983 @Falgo CretzuL_ Da____ frumos_ palySME _rintesa_
__chera_ @CretuL_ Cretu4085
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :urata_ Stapa3419 cr3tu__ @dumy__
@asdfghjk_ Pula3584 suparat_ borivoj SCUMPYCOOL @Creatza__ @rea_ GeorgiaK rillos^^ alo Hed
NuMaInt rwsydeyi heung-do @asdfghjk @mwe__ @carnat @aaaa SayBitch Lharold Georg8699
__tzu__ windows_ Creatu__ @_uPaNu__ L-amP2232 MAD1 Cretzu__ Guta5114 ____giana
print4617 __rgiana Cretz5146 Cretzu__ Bruneta @msr Pula7081 DonMarco Georgiana _retzu__ Plz
sexi_SNC together ____eta__ @Regina @tnx__ aNu__
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :TaLen8868 ____nT__ @Cr3tZzZu Daci_
TaeMINE` ne-popa LLaLa^^^ dretuppam Am1AniBa Cretu dragutza_ @bonita AlerG DNOS Fats Pizda_
stapanu necajit__ rat__ Satena_aLenT__ GoLaNu_ GoLaNuL_ JuPaNa ____at__ stapanu__
__ajit__ ____nu__ uparat__ stapa1085 TxT_bancomat_ma_Algo exe4193 _olanitza cr3tu4000
Cretu_ Creatu ____anta Bruneta__ Blonda__ JuPaNu__ GaOz @txt hackera_ __etu__ cr3tu9844
Muie2923 Nokia__ sexi__ lanitza tien-fu
:Amsterdam.NL.EU.undernet.org 353 Zx0hHr5aR @ #Cretzu :Givannio @__stanta @Smechera_
bancomat @IOvE____ @Suparata @Cretzu` @golanitza @SuPaRaT @Draguta @Sufar @Cr3tzu
@Creatza @Te-Iubesc @frumusica @__-Iubesc @GirL_ @fetitza @Te-Vreau @Cretzu @mama_
@alintata @Georgi @Cr3aTzZa @Smechera @back_ @Cr3tu @Telubesc_ @Back @CT_ @GirL
Nebunatic Heepaaa @Georgia sKlLeR_FZ A^n^c^a Hackera
:Amsterdam.NL.EU.undernet.org 366 Zx0hHr5aR #Cretzu :End of /NAMES list.
:Amsterdam.NL.EU.undernet.org 324 Zx0hHr5aR #Cretzu +stn
:Amsterdam.NL.EU.undernet.org 329 Zx0hHr5aR #Cretzu 1115391458

:Cretu9922!~lol@203.128.20.19 JOIN #Cretzu
:msr!~tita@61.211.225.12 MODE #Cretzu +o Cretz468
:carnat_!~carnatel@24.75.96.110 JOIN #Cretzu
:mwe___!~mwe@ez1serv1.ez1web.com MODE #Cretzu +o carnat_
:THE_DON!uxrggx@east-69-72-55-110.dynamic-dialup.coretel.net NICK :arcus29
:CT_!~cta@83.17.141.210 JOIN #Cretzu

JOIN #Creatu

JOIN #Cretu

:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Creatu :Cannot join channel (+k)
:Amsterdam.NL.EU.undernet.org 475 Zx0hHr5aR #Cretu :Cannot join channel (+k)
:fat-a!~Artif@client-82-3-242-231.gld.adsl.virgin.net NICK :Ac|Drw
:Ac|Drw!~Artif@client-82-3-242-231.gld.adsl.virgin.net NICK :Marupt
:`su`!bha@cpc2-blfs6-5-0-cust107.belf.cable.ntl.com JOIN #Cretzu
:aniardCJ!~cacat@mtl58-12b-159-170.dialup.sprint-canada.net JOIN #Cretzu
:___panu___!~stapanu@196.22.216.218 JOIN #Cretzu
:nprof_t!DouaiceMar@e246218.upc-e.chello.nl JOIN #Cretzu
:Odata-N!cacat@ip059.205-51-69.sogetel.net JOIN #Cretzu
:rea___!~bad@220.229.200.221 JOIN #Cretzu
:Sampo_!~sampo@mail.wize.com.tw MODE #Cretzu +o rea___
:Muie6746!~muie@221.133.167.128 JOIN #Cretzu
:Gh5cLu0hG!~cacat@mtl58-12b-159-170.dialup.sprint-canada.net JOIN #Cretzu
:carnat_!~carnatel@24.75.96.110 JOIN #Cretzu

Section C

```
STRING=""Zx0hHr5aR fat-a linux5543 THE_DON ____jit__ ____unatic Gest luci10 @Golanu_
_retu__ Fb8oQu7nK supar9187 cr3tu__ JuPaN2585
Te-Sarut aziz Smtanel Chicken^ Cretz468 Muie2178 Muie2713 karl Muie6244 ____asa_ Mirinda
@WeLLs_ Muie5266 @Regina__
@lasa-ma _reatza__ buton DaniMAD_ ido^ cta_ fredy Senzuala_ ____sa_ @Nu__ nzhtnwysgt
@Cr3tzu_ Suzana__ @Pin_ @azor
_runeta__ Gagica_ ipatic Cretu6153 AnuS Catieree Sexoasa _mechera_ Accept_ ____tanta Robert`o_
Maximus15 Regina_ Otalat Husen
Ui7gZl6bX Constanta aleboss tarfa guleksi yuh _szasha printesa_ elia29 Freaka02 @Creat_ DeNNyS`
__cajit__ ____oasa_ Buc
Copila_ Muie1105 _echera_ stramba_ @__nstanta Susanu_ _ecajit__ @Fata_ Estana46 BNCisi cta
____tu__ mwe_ dragos14 supar1403
JuPaN_ doc34 Cretu2296 _rumoasa_ @Sampo_ __etzu__ Dalena90 sherban19 Cretu__ Iuanita Cretzu_
Paine` sweet_ jupana_
__arat__ Muie_ oltaj^^ @fetitza_ sunos____ Gaby1 cr3tu9827 __parat__ stapa8012 _|____ necajit_
linux6799 Cretu____
Muie2571 sunos__ Cretu__ Bruneta_ _|____ Desiree__ ____anu__ Georgeta_ fata_ Game_Over
Ffelicia57 cvv_ ris24 Belea_
Creat3293 __apanu__ tcrku Galileo__ @Creat4991 cr3tu____ axuo rugieri yingsha `r`G` @__ta__
_reata__ tata iubit__
@print9752 NyCk-18 Da_33 ____tesa_ yee Sen}}>{{ Discovery stapanu_ cr3tu8610 necajit__ Nebunatic16
necaj3843 |SD
stapa7408 supar8005 Schikatomo21 Golanu aeneas T-Online sedef __3aTzZzA belea Nkameron
____os__ cr3tu7731 necaj5933 @mwe suparat__ Creatza_ Cretu857 _ancomat_ Osalam cc_ Cretu9912
batrana
__ntesa_ reymond99 sebiropa ____na tandrei Nick_34 SutFeroce anru15 PlantaSme BLONDA17
utu19 @ _retzuL_ gaoz_ __intesa_
Geo_19 @Singura _onstanta CretzuL frumoasa Blonda_ Creat9983 @Falgo CretzuL_ Da____ frumos_
palySME _rintesa_ ____chera_
@CretuL_ Cretu4085 urata_ Stapa3419 cr3tu__ @dumy__ @asdfghjk_ Pula3584 suparat_ borivoj
SCUMPYCOOL @Creatza__ @rea_ GeorgiaK
rlls^^ alo Hed NuMaInt rwarsydeyi heung-do @asdfghjk @mwe__ @carnat @aaaa SayBitch Lharold
Georg8699 __tzu__ windows_
Creat__ @_uPaNu__ L-amP2232 MAD1 Cretzu__ Guta5114 ____giana print4617 __rgiana
Cretz5146 Cretzu__ Bruneta @msr Pula7081
DonMarco Georgiana _retzu__ Plz sexi_ SNC together ____eta__ @Regina @tnx __aNu__
TaLen8868 ____nT__ @Cr3tZzZu Daci_
TaeMINE` ne-popa LLaLa^^^ dretuppam Am1AniBa Cretu dragutza_ @bonita AlerG DNOS Fats Pizda_
stapanu necajit ____rat__ Satena
_aLenT__ GoLaNu__ GoLaNuL_ JuPaNa ____at__ stapanu__ __ajit__ ____nu__ _uparat__
stapa1085 TxT_ bancomat_ ma_ Algo
exe4193 _olanitza cr3tu4000 Cretu_ Creata ____anta Bruneta__ Blonda__ JuPaNu__ GaOz @txt
hackera_ __etu__ cr3tu9844
Muie2923 Nokia__ sexi_ __lanitza tien-fu Givannio @__stanta @Smechera_ bancomat @IOvE____
@Suparata @Cretzu` @golanitza
@SuPaRaT @Draguta @Sufar @Cr3tzu @Creatza @Te-Iubesc @frumusica @__-Iubesc @GirL_
@fetitza @Te-Vreau @Cretzu @mama_ @alintata
@Georgi @Cr3aTzZzA @Smechera @back_ @Cr3tu @TeIubesc_ @Back @CT_ @GirL Nebunatic
Heepaaa @Georgia sKILeR_FZ A^n^c^a Hackera""
count=0
OP=0
```

for I in STRING.split():

```
count=count+1
if I[0] == '@':
    OP=OP+1
```

```
print "There are ",count," users in the channel"
print OP," of them are operators"
```

Section D

1. Procexp – Process Explorer – <http://sysinternals.com>
2. Regmon – Registry Monitor – <http://sysinternals.com>
3. filemon – File Monitor – <http://sysinternals.com>
4. ethereal - <http://www.ethereal.com/>
5. Gentoo - <http://www.gentoo.org/>
6. vmware - <http://www.vmware.com/>