Analysis of ngrBot

By Kimberly

Archived: 2026-04-05 20:39:51 UTC

```
000.  Note: parameters within "[" and "]" are required, and parameters within "<" and ">" are optional.
001.
002.        !dl [url] <md5> <-r> <-n>
003.
004.        The bot downloads and executes a file from the specified URL.
005.
006.        Parameters
007.        url         URL of the file to download and execute
008.        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
009.        -r          Enable RusKill on downloaded file
010.        -n          Disables PDef+ on the system until reboot or until it is manually re-enabled
011.
012.  -------------------------
013.
014.     !up [url] [md5] <-r>
015.
016.        The bot updates its file, but the update does not take effect until the system is restarted.
017.
018.        Parameters
019.        url         URL of the file to update to
```

```
020.        md5         MD5 hash of the update file
021.        -r         Reboot immediately
022.
023.  -------------------------
024.
025.      !die
026.
027.        The bot disconnects from the IRC server and does not reconnect until its system reboots.
028.
029.  -------------------------
030.
031.     !rm
032.
033.        The bot will remove itself from the system.
034.
035.  -------------------------
036.
037.     !m [state]
038.
039.        Enable/disable all output to IRC regarding to commands and features.
040.
041.        Parameters
042.        state    Enable (on) or disable (off) muting of all output to IRC
043.
044.  -------------------------
045.
```

```
046.    !v
047.
048.        The bot displays its version, customer name, the MD5 hash of its file, and its installed filepath.
049.
050.    -------------------------
051.
052.    !vs [url] [state]
053.
054.        The bot creates a browser instance and visits the specified link.
055.
056.        Parameters
057.        url         URL to open
058.        state    Open in a visible (1) or invisible (0) window
059.
060.    -------------------------
061.
062.    !rc <-n|-g>
063.
064.        The bot disconnects from the IRC server and waits 15 seconds before reconnecting.
065.
066.        Parameters
067.        -n    Only reconnect if the bot is currently marked as "new"
068.        -g    Only reconnect if the bot did not previously succeed in determining its country using GeoIP
069.
070.    -------------------------
```

```
071.
072.    !j [<[rule] [options]> channel] <key>
073.
074.    The bot joins the specified channel. If rules are specified, the bot will only join if the rules apply to it.
075.
076.    Parameters
077.    rule        Optional rule for the bot to check for. Supported options are -c (country) and -v (version)
078.    options       Options for selected rule
079.    With -c,    you can put a single or multiple comma-separated country code(s)
080.    With -v,    you can put a single or multiple comma-separated version(s)
081.    channel       Channel to join
082.    key           Key of channel to join
083.
084. -------------------------
085.
086.    !p [<[rule] [options]> channel]
087.
088.    The bot parts the specified channel.
089.
090.    Parameters
091.    rule        Optional rule for the bot to check for. Supported options are -c (country) and -v (version)
092.    options       Options for selected rule
093.    With -c,    you can put a single or multiple comma-separated country code(s)
094.    With -v,    you can put a single or multiple comma-separated version(s)
```

```
095.        channel        Channel to part
096.
097.  -------------------------
098.
099.      !s <rule>
100.
101.        The bot joins the channel for its country (e.g. Russian bots (RU) join #RU).
102.
103.        Parameters
104.        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)
105.
106.  -------------------------
107.
108.     !us <rule>
109.
110.        The bot parts the channel for its country (e.g. Russian bots (RU) part #RU).
111.
112.        Parameters
113.        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)
114.
115.  -------------------------
116.
117.     !mod [module] [state]
118.
119.        Enable/disable modules that use hooks.
```

```
120.          Note: disabling bdns will only unblock AV and other preset sites, not sites set using the !mdns command.
121.
122.      Parameters
123.      module        Module to change. Supported modules: msn, msnu, pdef, iegrab, ffgrab, ftpgrab, bdns, usbi
124.      state        Enable (on) or disable (off) module
125.
126.  -------------------------
127.
128.    !stats <-l|-s>
129.
130.      Retrieves statistics for spreading and/or login grabbing. If no parameters are specified, it will display both.
131.
132.      Parameters
133.      -l    Display login grabber stats
134.      -s    Display spreading stats
135.
136.  -------------------------
137.
138.    !logins <site|-c>
139.
140.      Retrieves all grabbed and cached logins and prints them to channel or PM. Can also be used to clear login cache.
141.
142.      Parameters
143.      site    Site to retrieve logins for (case insensitive, see here for the list of sites)
```

```
144.        -c        Clear login cache
145.
146.  -------------------------
147.
148.     !stop
149.
150.        The bot will end all running flood tasks.
151.
152.  -------------------------
153.
154.     !ssyn [host] [port] [seconds]
155.
156.        Parameters
157.        host        Host to flood with SYN requests
158.        port        Port to flood. If 0, the bot uses a random port
159.        seconds        Number of seconds to flood the target
160.
161.  -------------------------
162.
163.     !udp [host] [port] [seconds]
164.
165.        Parameters
166.        host        Host to flood with UDP packets
167.        port        Port to flood. If 0, the bot uses a random port
168.        seconds        Number of seconds to flood the target
169.
```

```
------------------------

    !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
```

```
196.        message        Message to spread via MSN
197.
198.  -------------------------
199.
200.  !http.int [interval]
201.
202.        Set the number of Facebook messages in a conversation before one is changed with your spreading message. See here for more information.
203.           Note: use '#' for a random interval between 1 and 9.
204.
205.        Parameters
206.        interval    Number of Facebook messages before spread
207.
208.  -------------------------
209.
210.     !http.set [message]
211.
212.        Set the message that will be used for Facebook spreading. See here for more information.
213.           Note: use '#' for a random digit and '*' for a random lowercase letter.
214.
215.        Parameters
216.        message        Message to spread via Facebook
217.
218.  -------------------------
219.
220.     !mdns [url|[domain1 <domain2|ip2>]|[ip1 <ip2>]]
221.
```

```
222.        The bot will block access to or redirect the specified domain/IP address.

223.        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.

224.        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.

225.

226.        Parameters

227.        url             Plaintext file with one redirect/blocking rule per line, rules are
formatted in the same way as the command parameters.

228.        domain1         Requests for this domain will be redirected to domain2 or ip2 if they are
set, otherwise it is blocked

229.        ip1             Requests for this IP address will be redirected to ip2 if it is set,
otherwise it is blocked

230.        domain2         DNS queries for domain1 will be redirected to this domain if set

231.        ip2             DNS queries for ip1 or domain1 will be redirected to this IP address if
set
```

Source: http://stopmalvertising.com/rootkits/analysis-of-ngrbot.html