Venom – shellcode generator

"apache2 domain name attack vector"

Has the ability to deliver our payloads in two diferent ways:
1 – using social engineering (http://mega-upload.com)
2 – using mitm+dns_spoof (redirect all domains to your phishing webpage)

Module Description:

'venom domain name attack vector' *when active uses http://mega-upload.com fake domain (*build inside shell/aux folder*) to deliver our payloads to target host by using 'social engineering' technic to trick target into executing our payload.*

If we decide to deliver our payloads using mitm+dns_spoof *technic then we need to further config settings in '*/usr/share/ettercap/etter.dns' *like un-comment (#) all* .com *domains, it will redirect all traffic (*.com domains*) from target host to our fake webpage.*

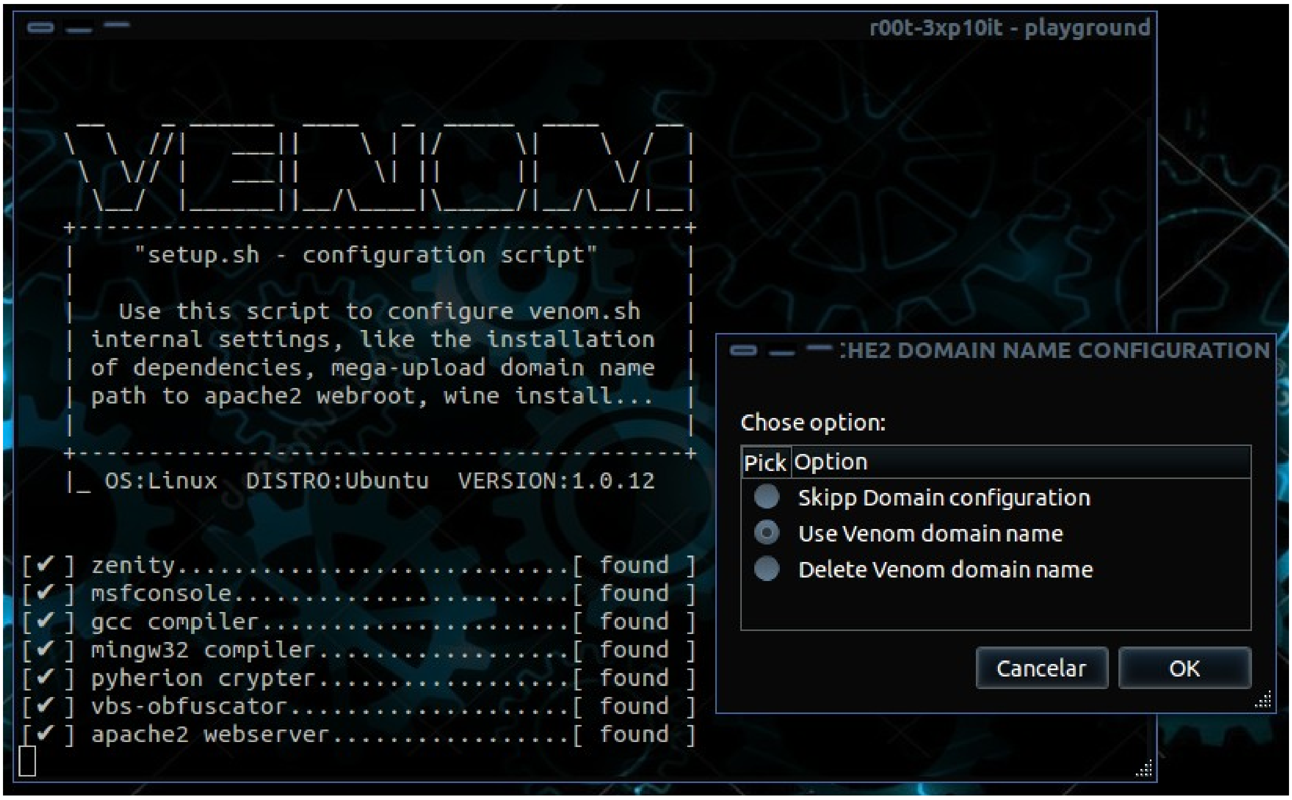
Note: social engineering and mitm+dns_spoof can not work simultaneously.
"Its up to you to decide witch one to use"...

"note: everytime we change our ip address*, we need to run* setup.sh
if we desire to use apache2 venom domain name attack vector again"

"*note:* shell/aux/venom.conf *its build everytime we use* setup.sh"

social engineering (http://mega-upload.com)

1º to be hable to use this option we need to run 'shell/aux/setup.sh' *and config* 'Use Venom domain name' *attack vector settings.*



```
 __    _ ______  ____   _  _____  ____    __
 \ \  //|  ___||    \ | |/     \|    \  /  |
  \ \// |  ___||     \| ||     ||     \/   |
   \__/ |_____||__/\____|\_____/|__/\__/|__|
+---------------------------------------------+
|     "setup.sh - configuration script"       |
|                                             |
|    Use this script to configure venom.sh    |
|  internal settings, like the installation   |
|  of dependencies, mega-upload domain name   |
|  path to apache2 webroot, wine install...   |
|                                             |
+---------------------------------------------+
|_ OS:Linux  DISTRO:Ubuntu  VERSION:1.0.12


[✔ ] zenity..........................[ found ]
[✔ ] msfconsole......................[ found ]
[✔ ] gcc compiler....................[ found ]
[✔ ] mingw32 compiler................[ found ]
[✔ ] pyherion crypter................[ found ]
[✔ ] vbs-obfuscator..................[ found ]
[✔ ] apache2 webserver...............[ found ]
```

:HE2 DOMAIN NAME CONFIGURATION

Chose option:

Pick	Option
○	Skipp Domain configuration
●	Use Venom domain name
○	Delete Venom domain name

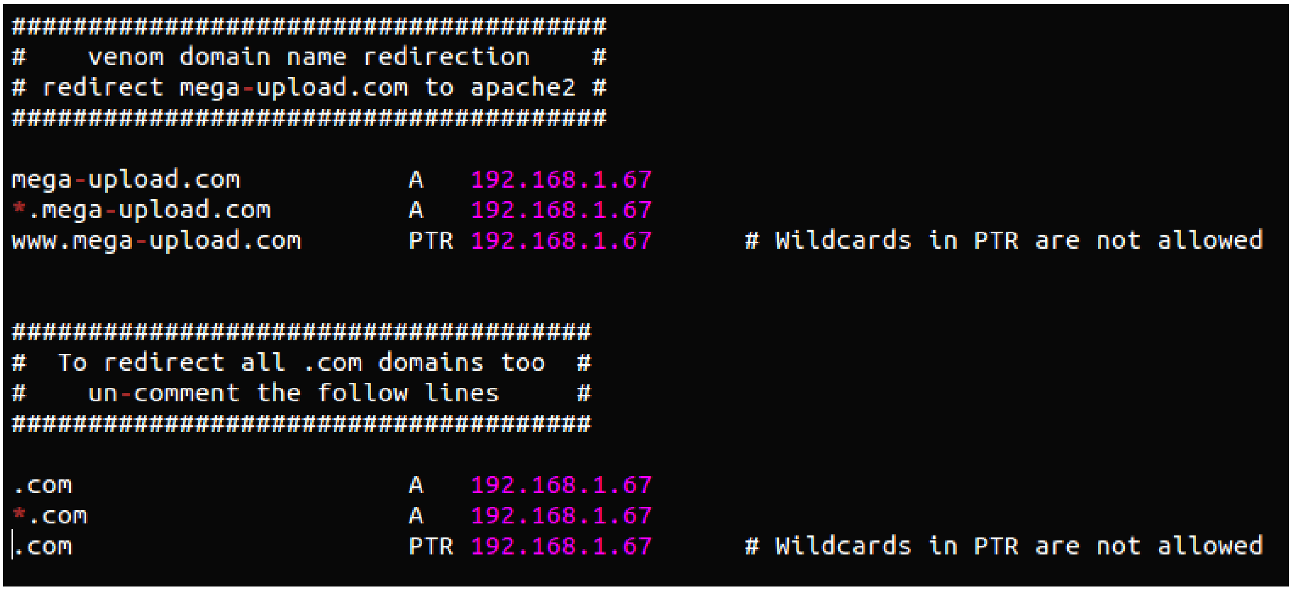
<u>note:</u> *this option will add your ip address into* 'shell/aux/etter.dns' *filter, before replacing the ettercap default dns filter by this one.*

<u>*note:*</u> *everytime we change our* ip address *we need to run* 'setup.sh' *to config the new IP settings to be used.*

<u>note:</u> *using* 'Delete Venom domain name' *option in* setup.sh *will revert ettercap etter.dns filter to its* 'default stage'..

mitm + dns_spoof (redirect all domains to your phishing webpage)

1º to be hable to use this option we need to edit the etter.dns *filter in '/usr/*share/ettercap/etter.dns*' and un-comment the follow lines:*



```
#######################################
#    venom domain name redirection    #
# redirect mega-upload.com to apache2 #
#######################################

mega-upload.com           A   192.168.1.67
*.mega-upload.com         A   192.168.1.67
www.mega-upload.com       PTR 192.168.1.67      # Wildcards in PTR are not allowed


######################################
#  To redirect all .com domains too  #
#    un-comment the follow lines     #
######################################

.com                      A   192.168.1.67
*.com                     A   192.168.1.67
.com                      PTR 192.168.1.67      # Wildcards in PTR are not allowed
```

note: *If we delete the* comments *(#) from* .com *domains then all* .com *domains will be redirected to our phishing webpage*

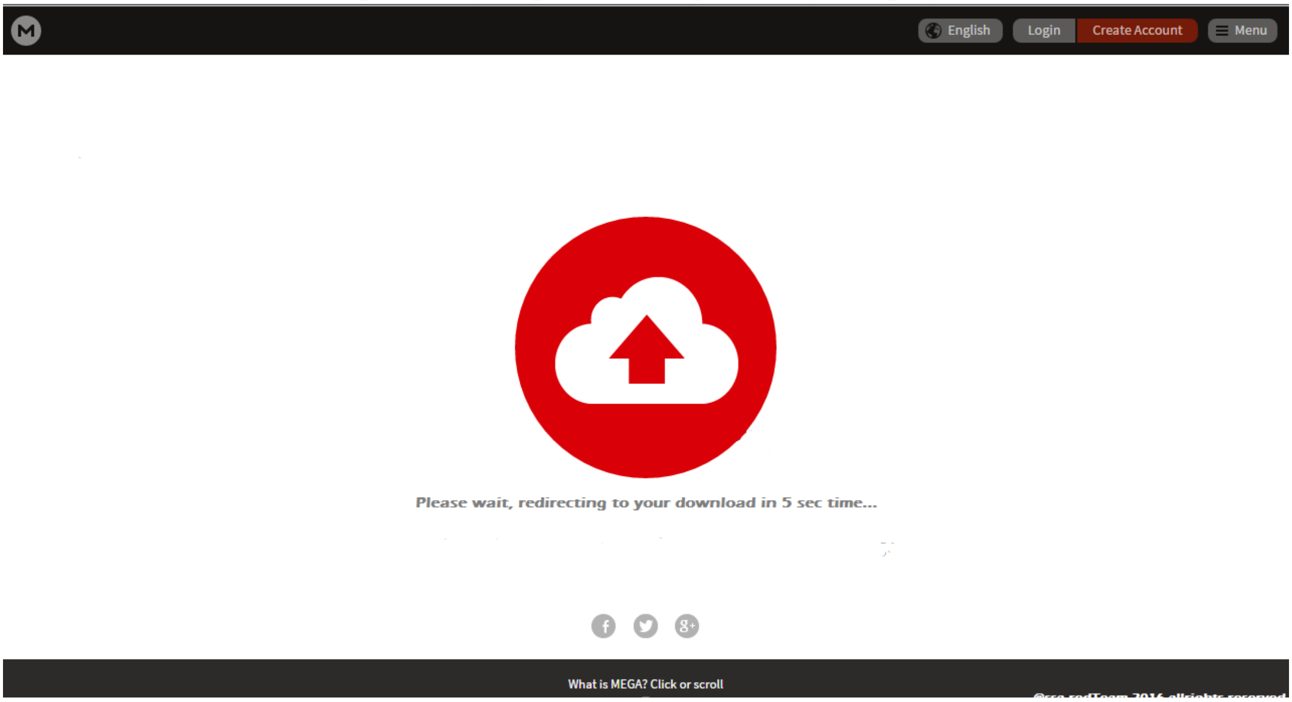
note: *if we comment all* .com in /usr/share/ettercap/etter.dns *then venom.sh will be forced to use* http://mega-upload.com *domain to deliver payloads.*

note: *using '*Delete Venom domain name*' option in* setup.sh *will revert ettercap etter.dns filter to its '*default stage*'..*

final notes:

The two technics will build a diferent index.html *based on the method used.*

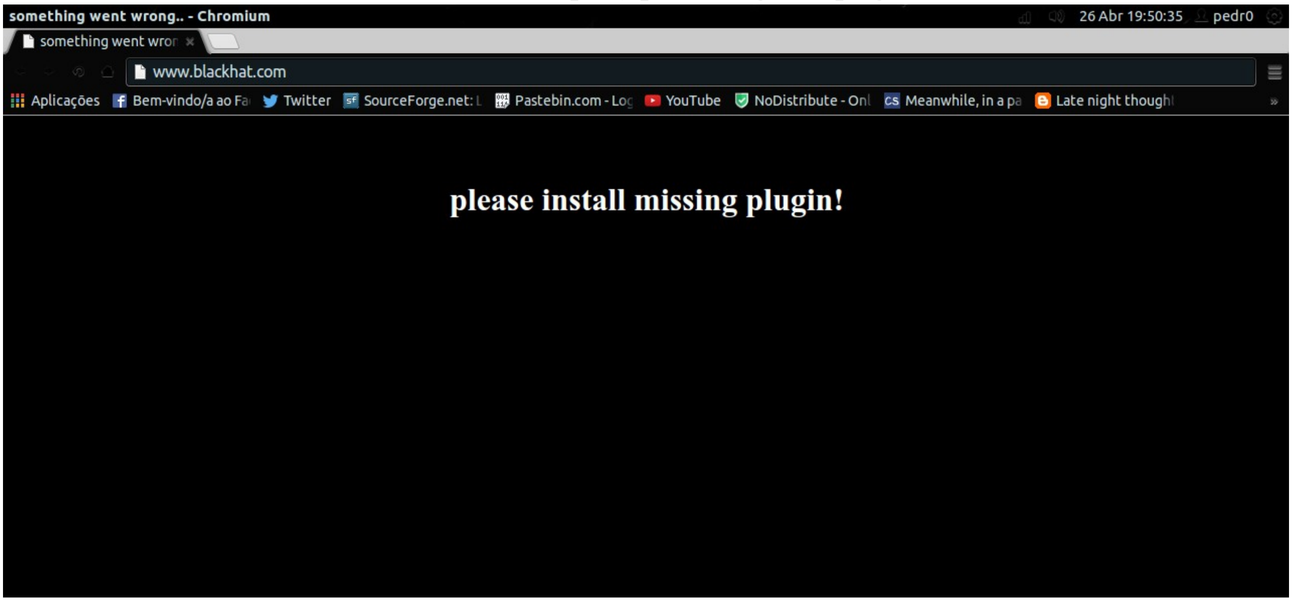
http://mega-upload.com phishing webpage:


English
Login
Create Account
Menu

Please wait, redirecting to your download in 5 sec time...

What is MEGA? Click or scroll
©rsa redTeam 2016 allrights reserved

mitm + dns_spoof phishing webpage:



please install missing plugin!

Author: r00t-3xp10it

collaborators: 0xyg3n | Suriya | Chaitanya

Copyright © 2016 - venom shellcode generator