

Grep for Evil

Leigh Metcalf, PhD

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Software Engineering Institute | Carnegie Mellon University

Title of the Presentation Goes Here
© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



The Evil Bit

RFC 3514 defined the evil bit:

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. We define a security flag in the IPv4 header as a means of distinguishing the two cases.

The Evil Bit

I didn't look for the evil bit in packets...

..but I did in domain names!

Using a passive DNS database, I looked for domains with DDOS in them.

ez-ddos.com



[home](#) [Our advantages](#) [Additional Information](#) [Additional services](#) [prices](#) [Payment](#)

EZ-DDOS.COM - professional, non-stop DDOS service specializing in the conduct of the most powerful high-speed attacks (up to 70 GBPS). We attack absolutely any goals in the IT segment. Here you can order a DDOS attack on any network resource. The best way to solve your problems. Fast. Qualitatively. Effectively. Low prices.



**Client Anonymity guaranteed
200%**



**We attack protected
from DDOS projects**



**Round the clock
support**

**The attack on the server (IP)
from 3500 rubles ./ (\$ 60.) ***

We attack any server - game (LineAge, Minecraft, CS et al.), E-mail, strimingovye (IP-TV), Cardsharing (satellite TV) and others. The attack - server channel clogged with multi-gigabit stream.

* - Price is for 24 hours (one day).

[Other prices "](#)

The attack on the website (URL) 3000 ./ rubles (\$ 50.) *

We attack any sites and forums - the media, the Internet shops, entertainment resources, and any other. The attack on the site can be done in three ways: SYN, HTTP, UDP, thereby achieving the maximum effect.

* - Price is for 24 hours (one day).

[About payment "](#)

COPYRIGHT © 2013-2017.

EZ-DDOS.COM - DDOS SERVICE №1 (POWER UP TO 70 GBPS)

EZ1@TECHIE.COM

[FEEDBACK 24/7](#)

[831577](#)

EZ@XMPP.US



Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release
and unlimited distribution."

ddos.su

4/13/2017

Distributed Denial of Service

Distributed Denial of Service

root@ddos#

```
64 bytes from 127.0.0.1: icmp_seq=292 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=293 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=294 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=295 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=296 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_seq=297 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=298 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=299 ttl=64 time=0.021 ms
64 bytes from 127.0.0.1: icmp_seq=300 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=301 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_seq=302 ttl=64 time=0.021 ms
64 bytes from 127.0.0.1: icmp_seq=303 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=304 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=305 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=306 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=307 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=308 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=309 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=310 ttl=64 time=0.015 ms
64 bytes from 127.0.0.1: icmp_seq=311 ttl=64 time=0.021 ms
64 bytes from 127.0.0.1: icmp_seq=312 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=313 ttl=64 time=0.020 ms
64 bytes from 127.0.0.1: icmp_seq=314 ttl=64 time=0.022 ms
64 bytes from 127.0.0.1: icmp_seq=315 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=316 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=317 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=318 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=319 ttl=64 time=0.017 ms
64 bytes from 127.0.0.1: icmp_seq=320 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=321 ttl=64 time=0.016 ms
64 bytes from 127.0.0.1: icmp_seq=322 ttl=64 time=0.016 ms
```

© 2009 DDoS. *****



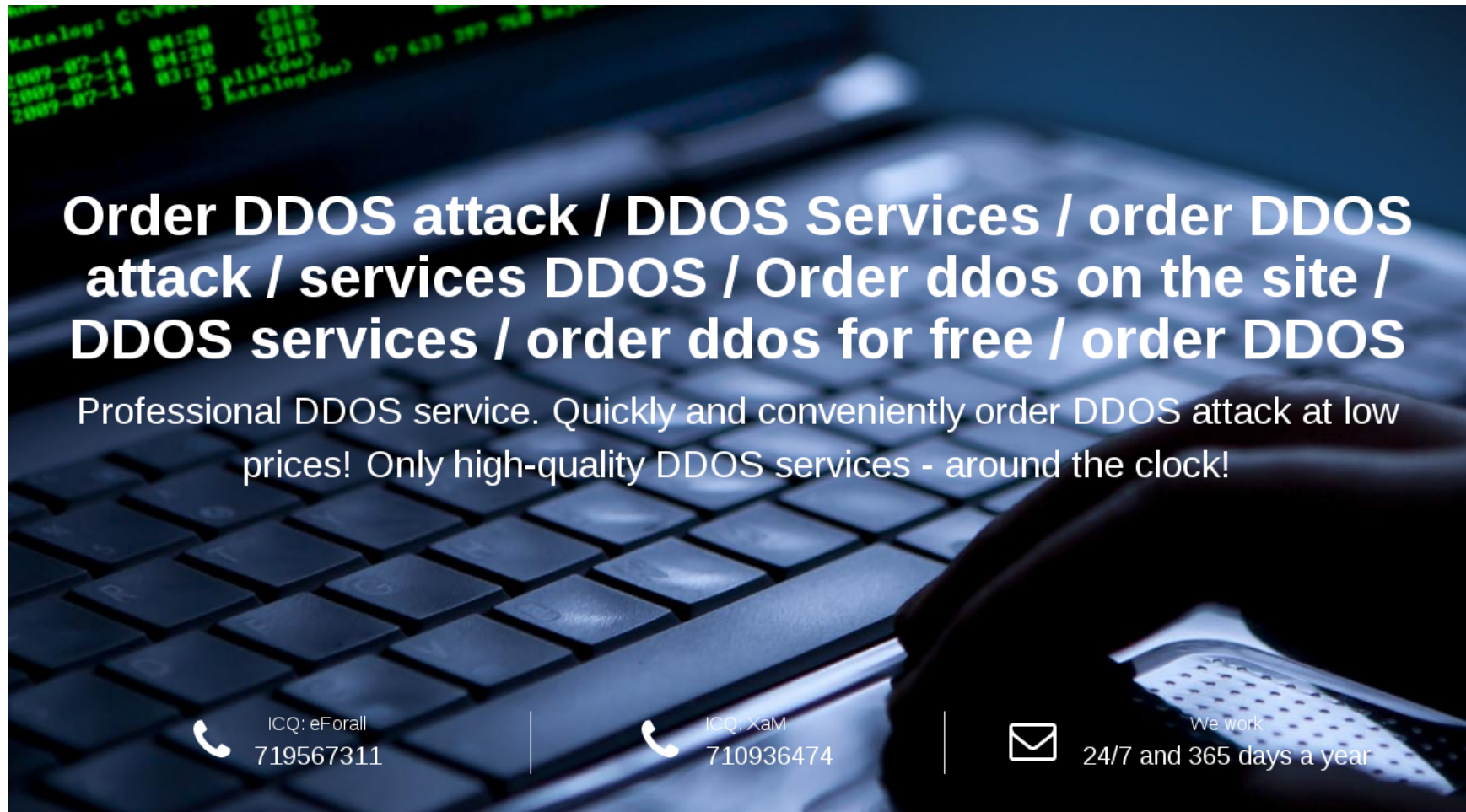
Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release

and unlimited distribution."

ddos-team.com



Order DDOS attack / DDOS Services / order DDOS attack / services DDOS / Order ddos on the site / DDOS services / order ddos for free / order DDOS

Professional DDOS service. Quickly and conveniently order DDOS attack at low prices! Only high-quality DDOS services - around the clock!

ICQ: eForall
719567311

ICQ: XaM
710936474

We work
24/7 and 365 days a year

attack-ddos.info

Order ddos attack in the best DDoS Service

Administrator The Services Created on: April 05, 2016

DDoS-cepbur

DDoS attack how many articles about it you can not reread. This service, popular on the Internet and every day, dozens of attacks from hackers on various network structures are conducted. **Order ddos** come not only to sites of simple online stores, bloggers, news portals, but also to infrastructures that are critical in the Internet as a whole. Recently, people's interest in ddos has become more active, they are ready to pay a few thousand a day for the victim not to show signs of life. But to find a quality **DDoS Service** not as easy as it seems. Every little schoolboy can spend a free ddos attack while wasting nothing. In the vast search engine you can download any botnet, customize it and enjoy not going deep into the knowledge of how it all works. Such people are full and more and more often people become victims of such small scammers who can not cope with the goals all the time.

Tired of looking for where to **order DDoS attack**?! Then our comprehensive solutions for conducting ddos attacks on the server and sites are at your service. We can test the majority of existing hosting providers for the stability of the network. The specialists will give you a free consultation on your popular issues related to ddos attacks, recommend actions to provide protection if this is required.

The botnet that we use is unique in its kind. It does not use any third-party modules, it was written completely from 0 to .NET language. A huge number of methods of attacks from the simplest L3 to complex L7. Flexible customization of the bot's aggressiveness and support for JS, Flash, Iframe protection of popular antidotes systems such as Cloudflare, OVH, DDOS Guard, Voxility ... Allows to disguise as an ordinary client of the network. Thus, it is guaranteed delivering a request to the victim's victim even through protection systems.

Price list for services

Paid, free or other tests do not. **Testers, resilers, scammers ... please do not disturb.**

ddos.ninja

DDOS NINJA



COMING SOON



Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release

and unlimited distribution."

Let's Digress into DDOS for a bit...

And talk about who DDOSes and why they DDOS

First Question – Why DDOS?

A DDOS is a politico-economic act:

- Estonia 2007
 - Revenge
- Spamhaus 2012
 - Revenge
- Hong Kong 2013
 - Censorship
- BBC 2016
 - Terror
- Mirai 2016
 - Revenge
- Swedish Railways 2017
 - Test?
- Danish Railways 2018
 - Test?
- Bitfinex Exchange 2018
 - Competition/economic gain

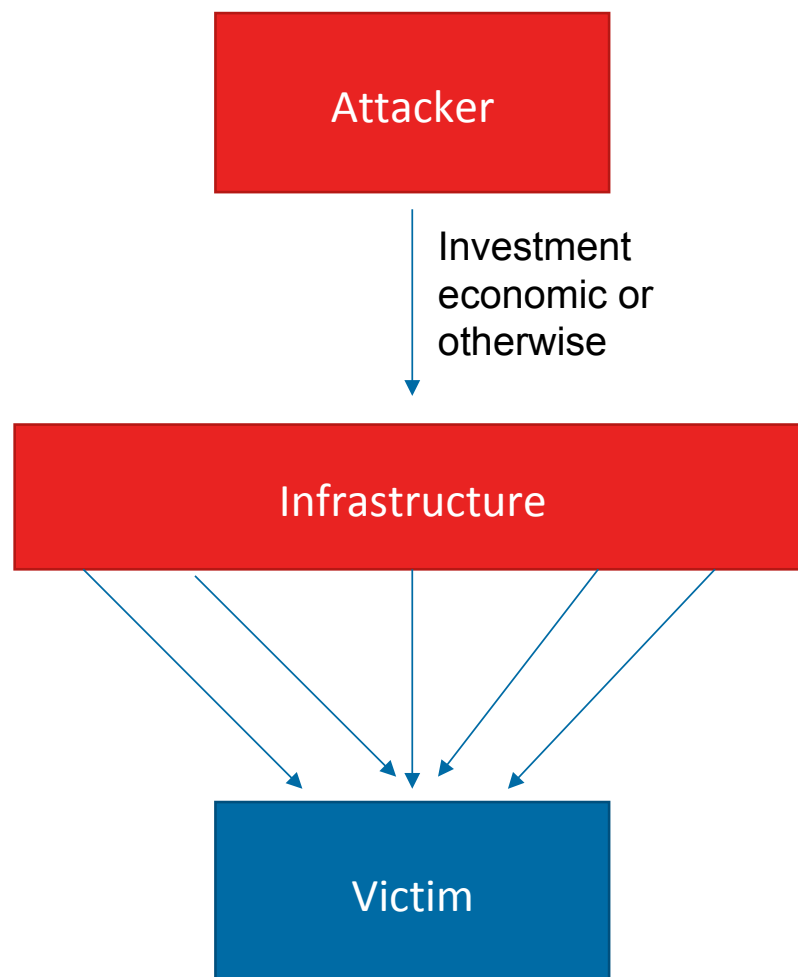
Provides users asymmetric power for high-profile results.

Who DDOS?

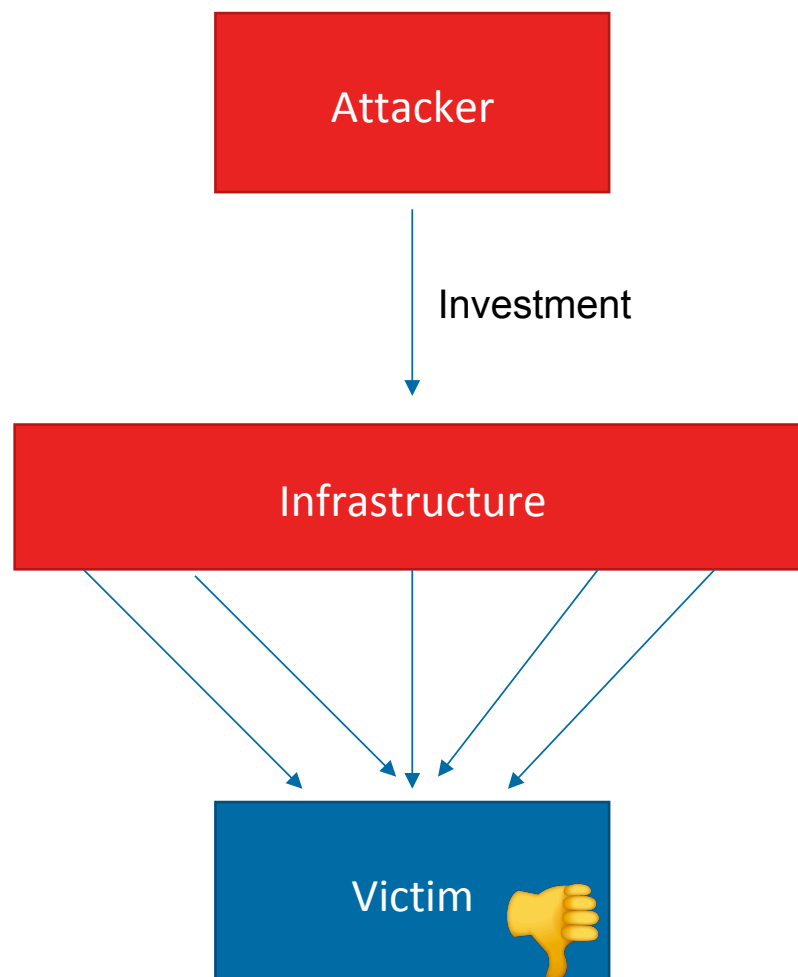
DDOS is surprisingly cheap.

- Barrier to entry is very low
- UI makes it easy for unskilled attackers to play in the game
- There are free stressers (aka, DDOS providers)
- Before the FBI took down Alpha Bay, I found DDOS for as low as \$5
- Just searching the web (duckduckgo.com is my friend) I found it for as low as \$10
- Unfortunately, I didn't go buy these to find out what I'd get. Something something something IRB board Something.
 - Also known as my boss saying "You want to WHAT?"

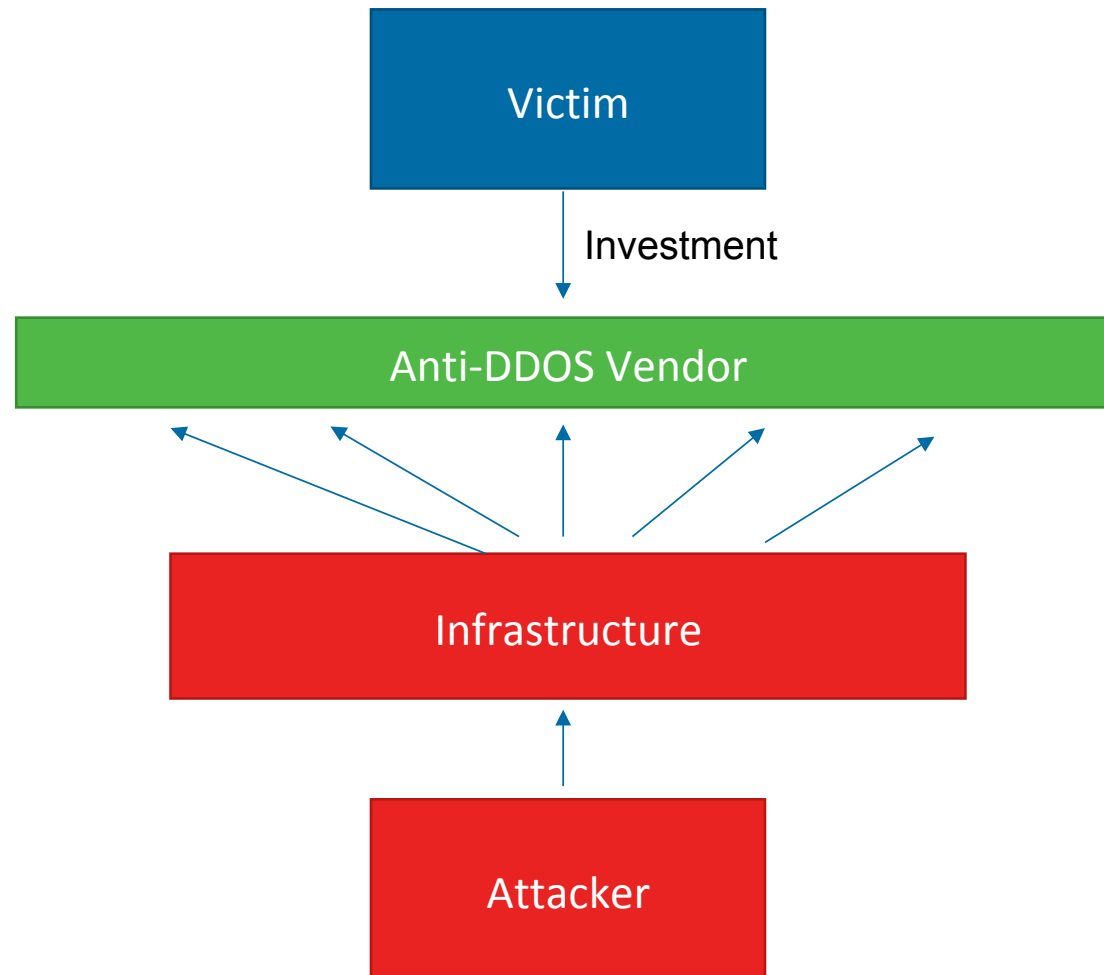
DDOS Traditional Attacker Economic Model



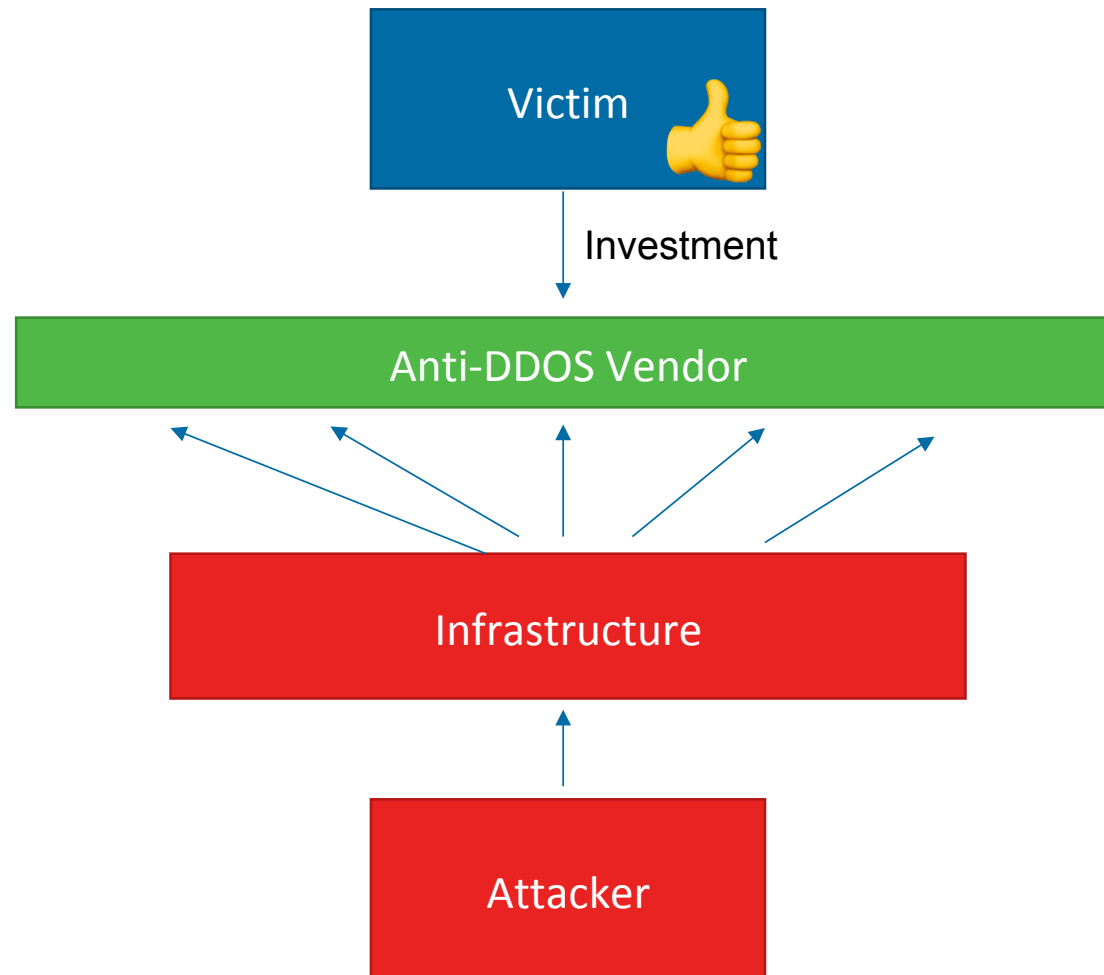
DDOS Traditional Attacker Economic Model



DDOS Traditional Victim Economic Model



DDOS Traditional Victim Economic Model

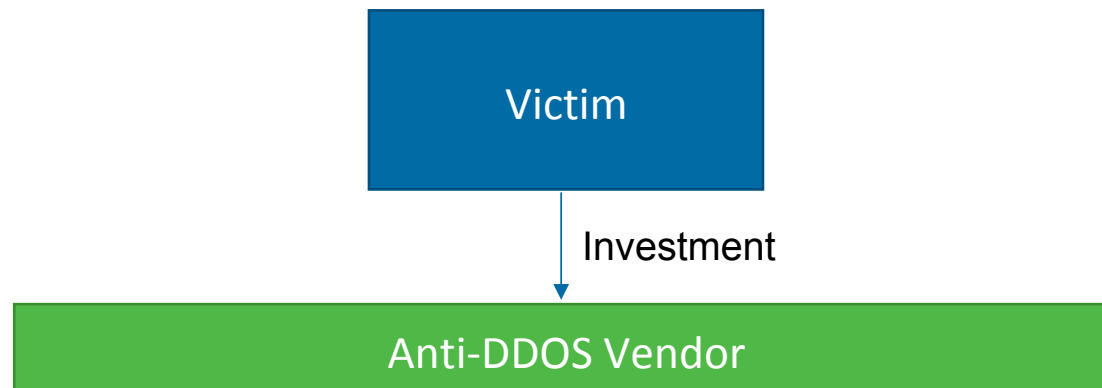


Anti DDOS Stops that DDOS

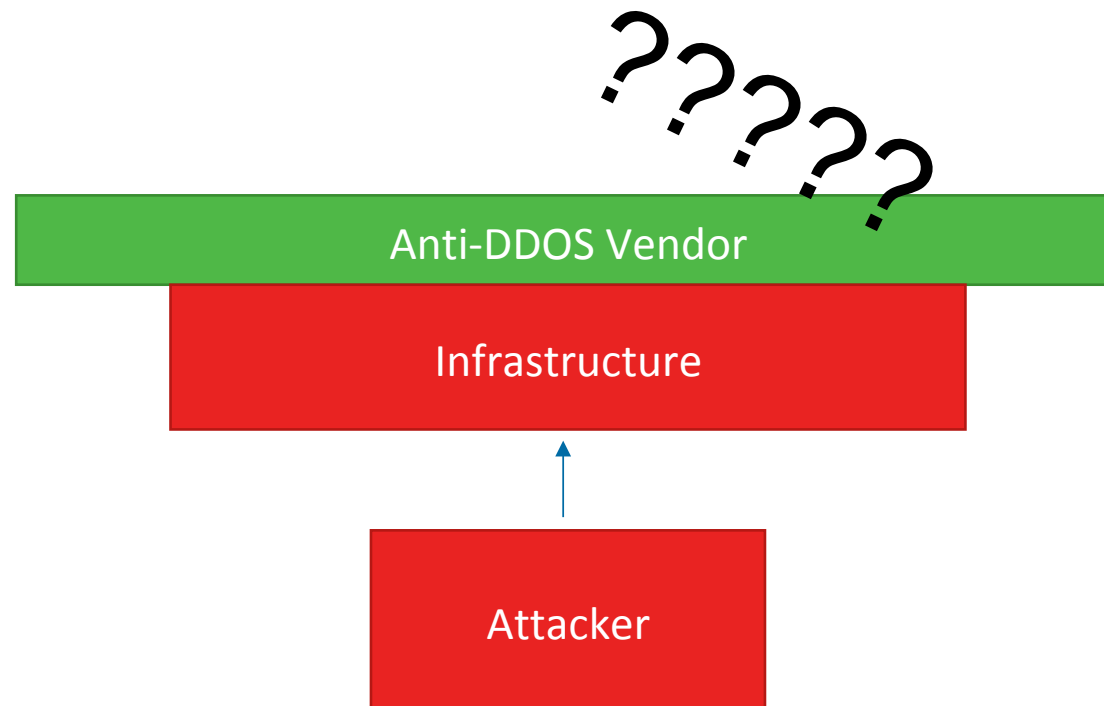
...right?

RIGHT?

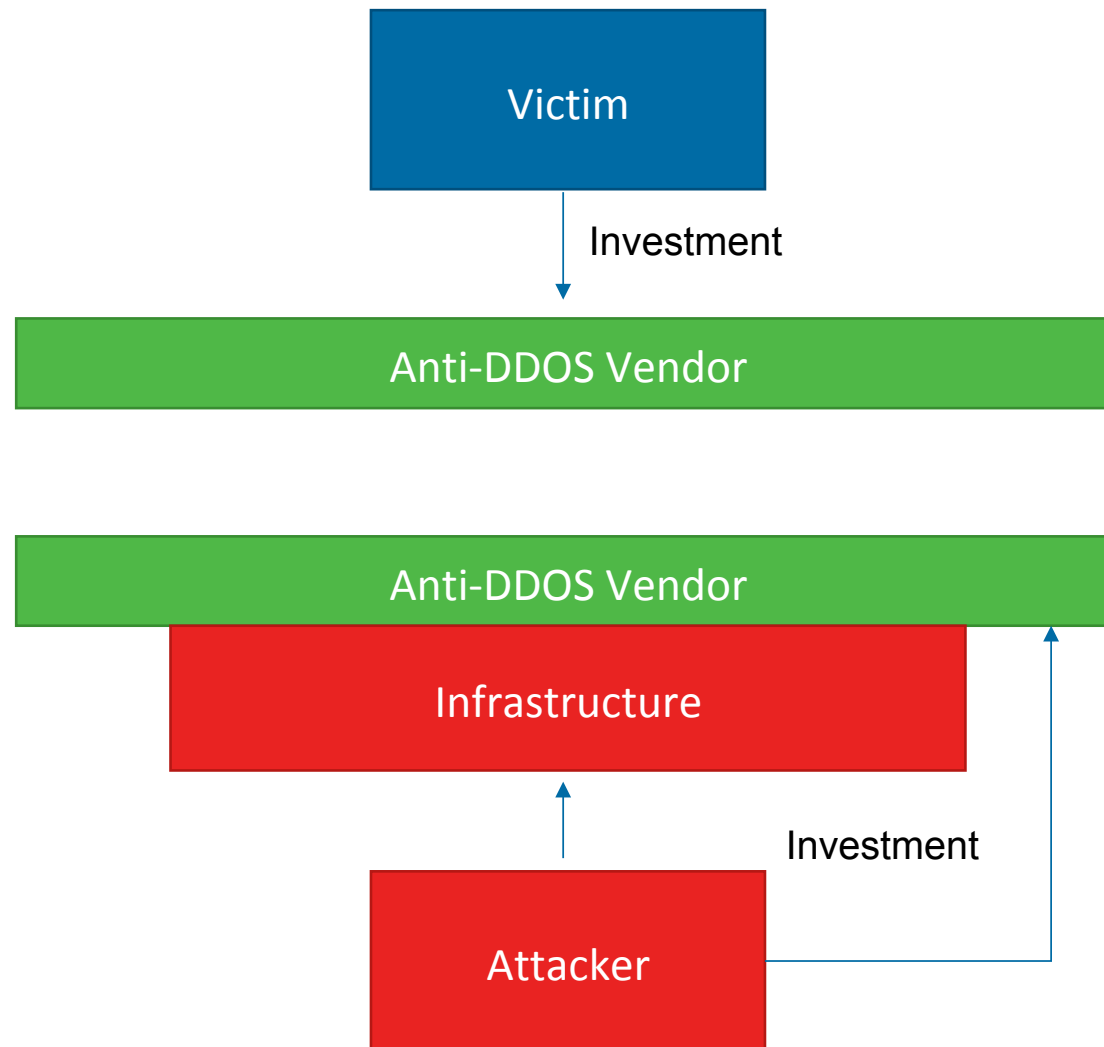
DDOS Economic Model: A Trend



DDOS Economic Model: A Trend



DDOS Economic Model: A Trend



Wanna buy a DDOS?

The screenshot shows the IPBooter website. At the top left is the 'IPBOOTER' logo. At the top right are navigation links: 'HOME', 'PRICING', 'LOGIN', and 'REGISTER'. The main heading is 'IP Booter - #1 Booter/Stresser'. Below it is a subheading: 'Running strong for 5+ months, IP Booter is the last booter/stresser you'll ever need. Reliability, Power, and Security!'. A list of features follows:

- Incredibly Fast (Instant Attacks)
- 100% Custom Source
- Minimal Logs (Optional Logging)
- Secure & Reliable (256-bit TLS Encryption)
- Standard & VIP Networks (Up to 40+ Gbps)
- Multiple Layer-4 Attack Methods (TCP & UDP)
- 24/7 Great Support (Ticket System)
- Very Affordable Pricing

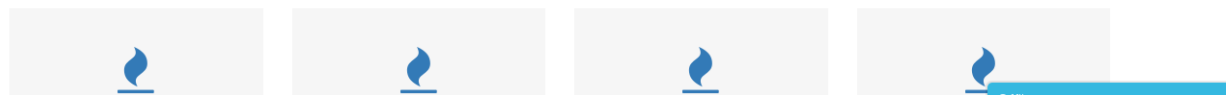
On the right side, there is a 'CREATE AN ACCOUNT' form with the following fields:

- Username
- Password
- Confirm Password

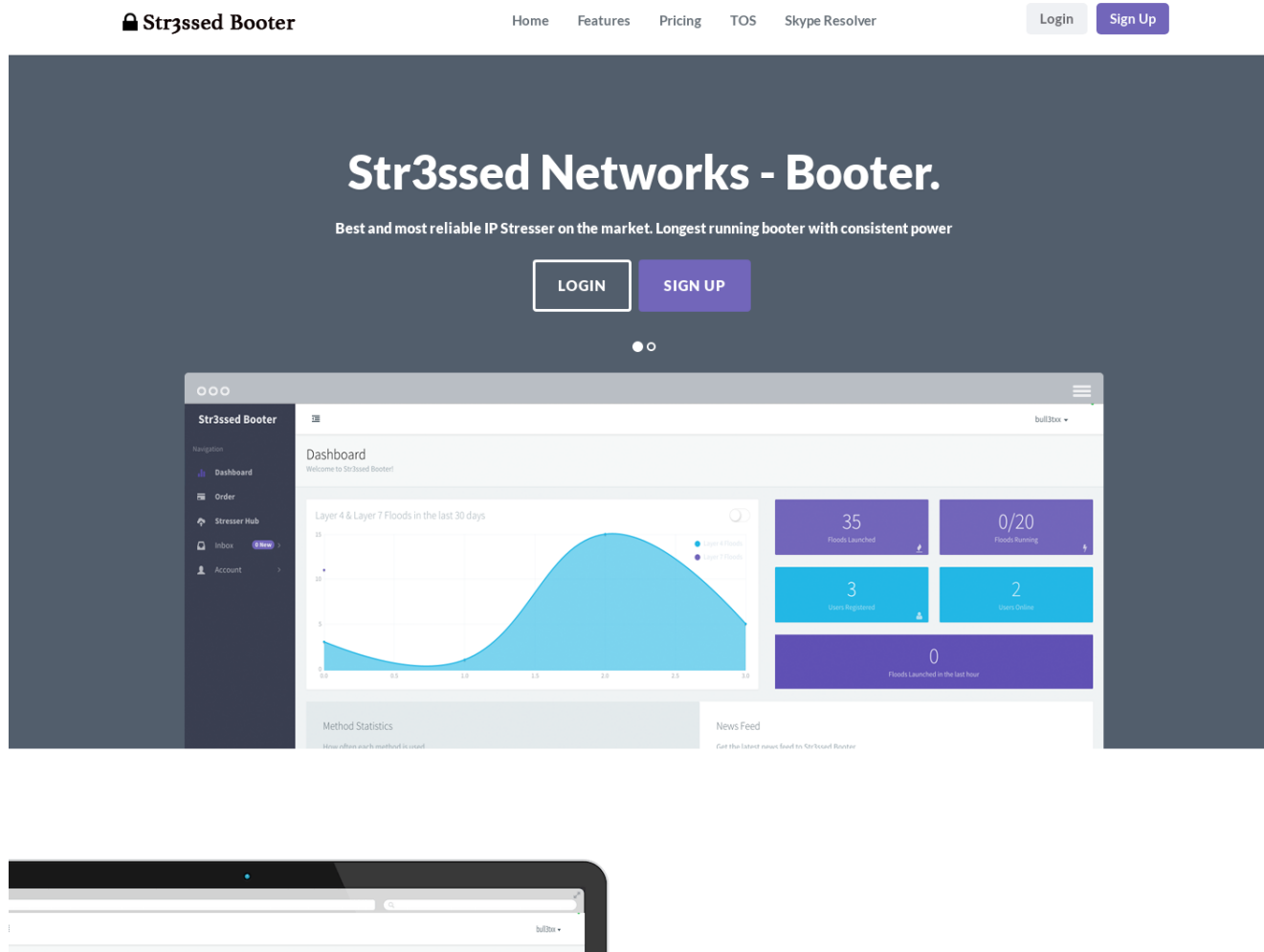
Below the password fields is a CAPTCHA section with a checkbox labeled 'I'm not a robot' and a reCAPTCHA logo. At the bottom of the form is a red 'REGISTER' button.

Competitive Pricing

Our plans are some of the most affordable on the market. Please register/login to view all our available plans. Custom plans are also available, just open a support ticket and one of our agents will gladly assist you as soon as possible.



str3ssed networks booter



Pssst, DDOS for sale!

[IP Stresser](#) [Home](#) [Stresser](#) [Purchase](#) [Terms](#) [FAQ](#) [Support](#) [Contact](#) [Welcome Guest](#) [Login](#) [Register](#)

Free Trial!

All members can enjoy up to 200 Mbps for 300 seconds... for free!

[Try For Free Today!](#)

* No credit card required, subject to terms of use and network availability.

Why IP Stresser

Customizable Plans
Build your plan from the ground up. Starting at only \$5 USD a month!

Free Trial
Who can turn down a free stresser? Try out our stresser for free!

Revolutionary Source
We custom coded our source code to meet the wants and needs of our customers.

Dedicated Servers
Our high end dedicated servers can satisfy even the most power hungry customers.

Guaranteed Power
We guarantee at least 99% of the output power of your stress tests. Nobody else will do that.

Custom Scripts
Our custom coded scripts allow advanced users greater flexibility and control.

Layer 4 Scripts

- DRDoS
- UDP
- UDP-Lag
- SYN

Layer 7 Scripts

- RUDY
- Slowloris
- ARME

Latest News

[Memorial Day Sale](#)

[Black Friday Sale](#)

[Scripts Updated](#)

[Memorial Day Sale](#)

[CloudFlare Memory Leak](#)

[Black Friday Sale](#)

[Scripts Updated](#)

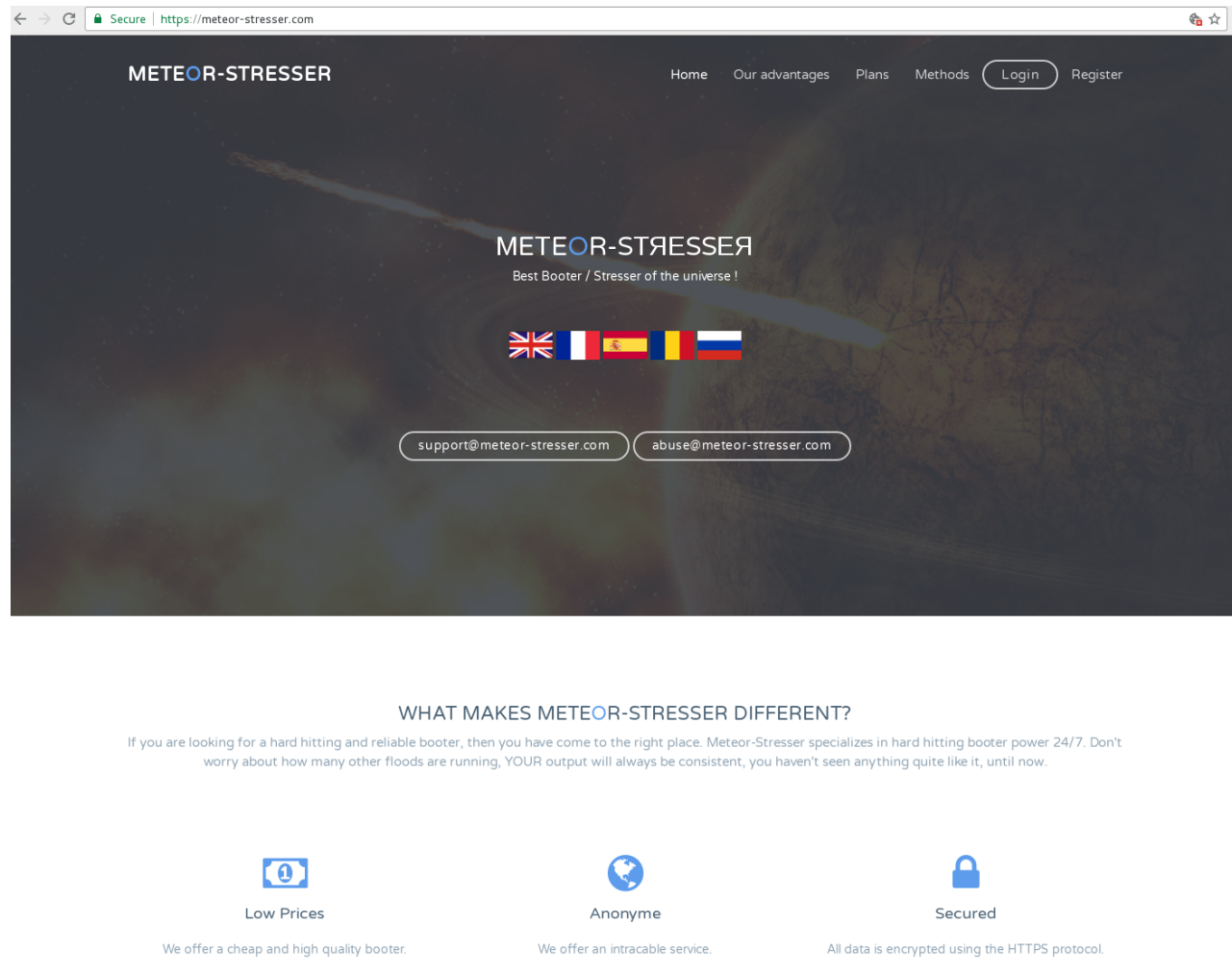
[Memorial Day Sale](#)

[Terms](#)
[Acceptable Use](#)

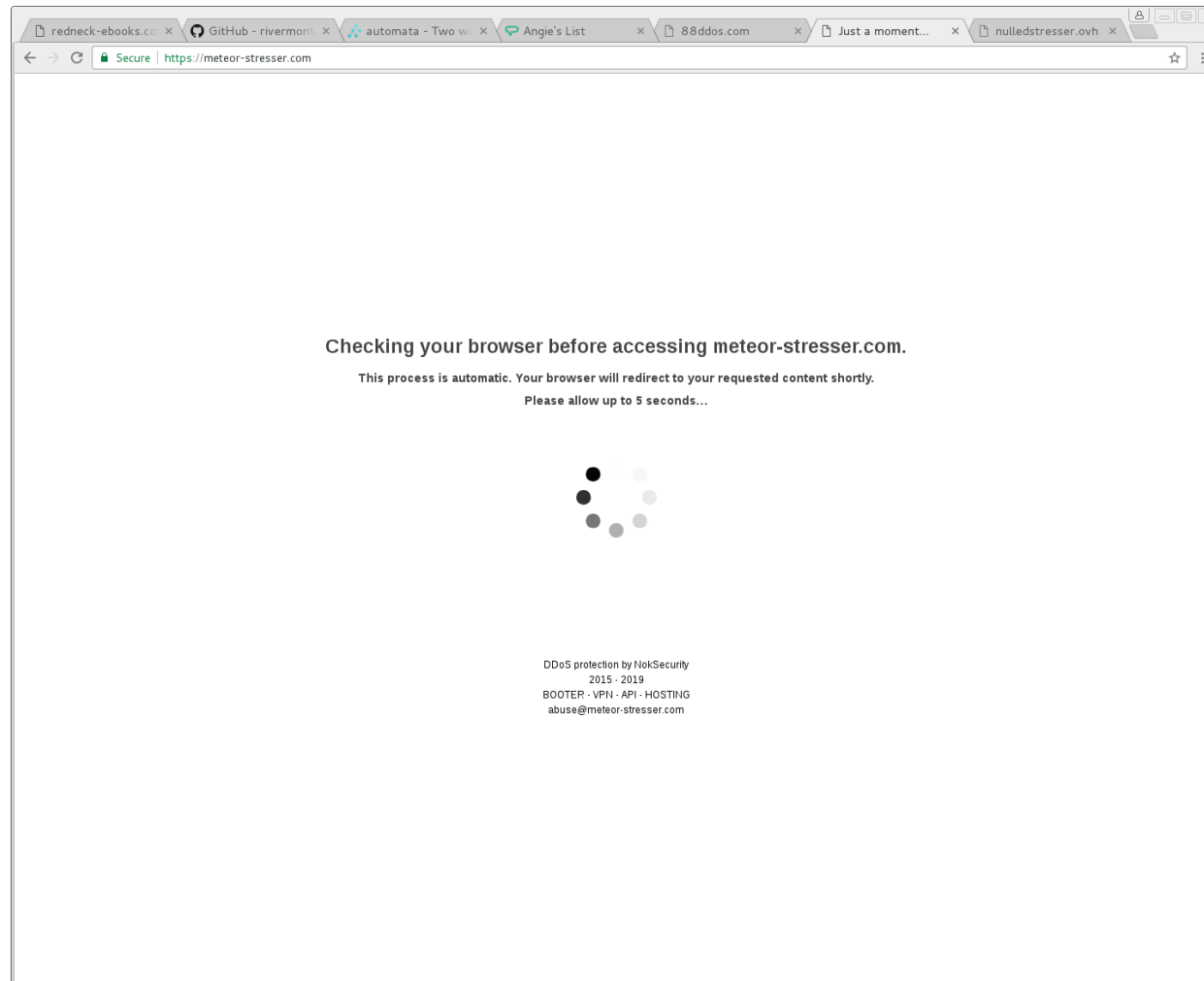
[FAQ](#)
[Support](#)

[About](#)
[Contact](#)

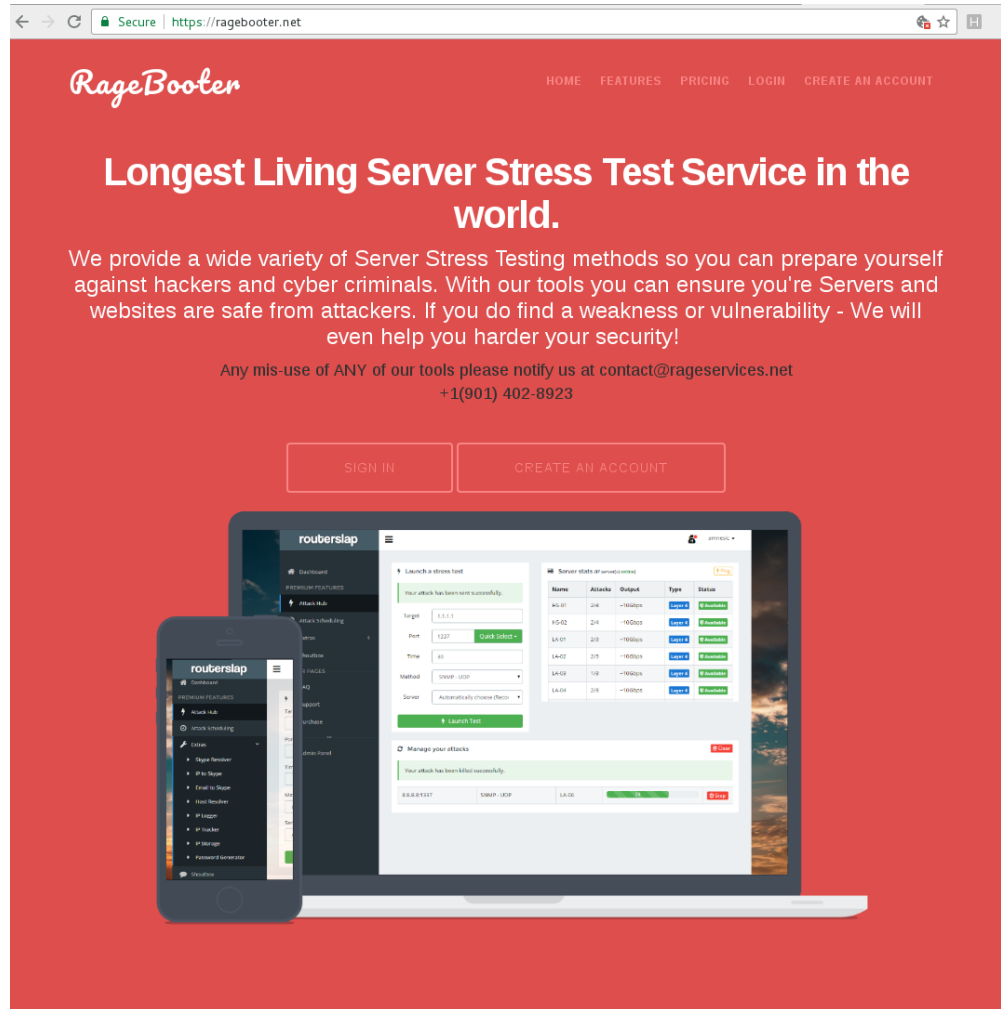
Meteor Stresser



But what is that when I go there?



Maybe it's just one domain?



There's also a Chinese ISP supporting...

4/13/2017

Botnet Botnet.Cc - Chinese DDOS website stress test platform - DDOS web end - China DDOS web end

Each package has our dedicated VIP node. We guarantee 15-30Gbps per attack.



BOTNET.CC
(I)

SKYPE
RESOLVER
(LOGIN.PHP)

INFORMATION
(LOGIN.PHP)

LOGIN
(LOGIN.PHP)

REGISTER
(REGISTER.PHP)

A revolutionary IP test platform

The best pressure on the market platform.



Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

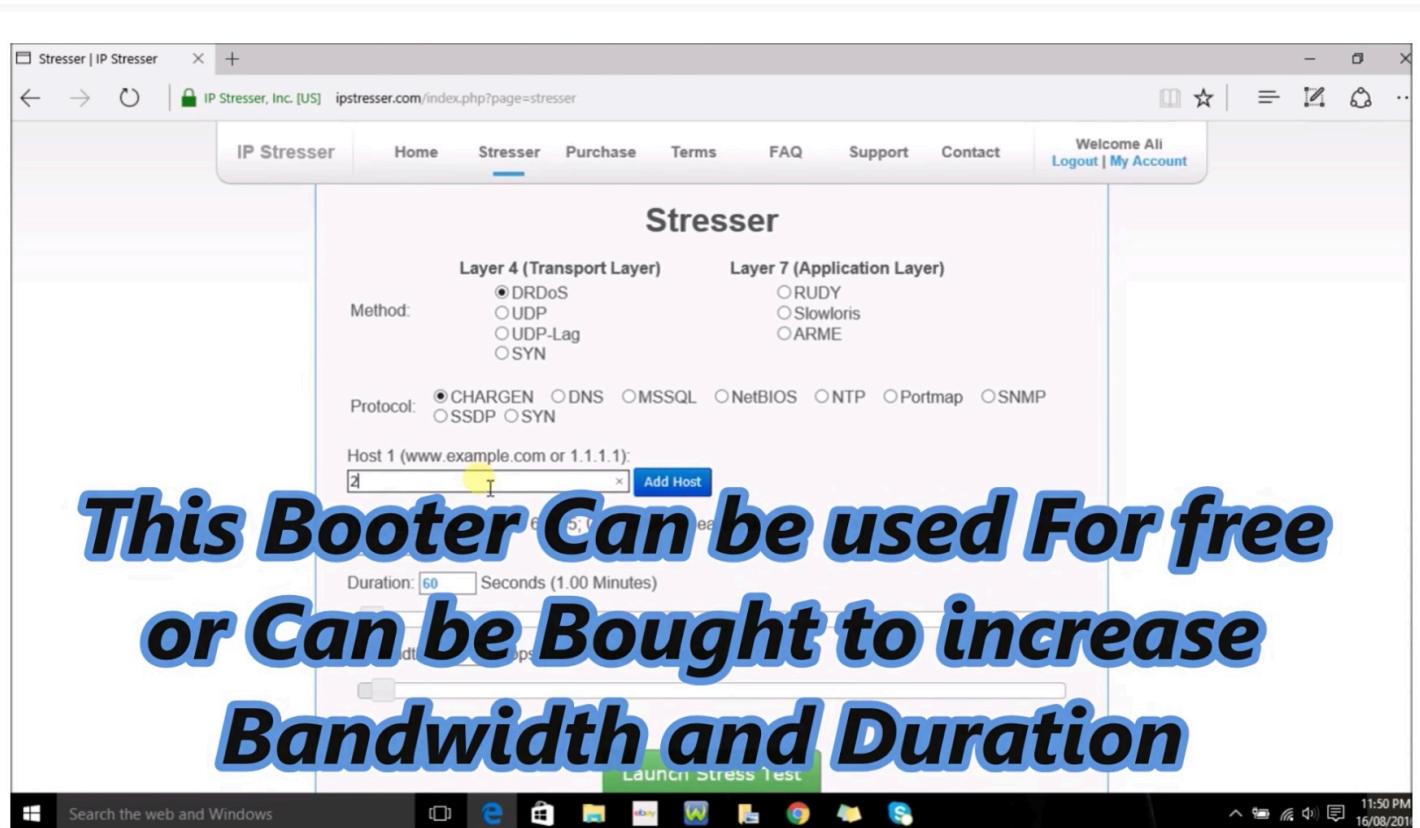
"[Distribution Statement A] Approved for public release
and unlimited distribution."

What about tacit DDOS support?

It's one thing to directly allow the DDOS vendors to sell...

...but what about other support?

Youtube videos!




Best Free Booters (2018)

99,220 views

820 65 SHARE

Youtube videos



Home

Inferno-Stresser [FREE]


Inferno-Stresser [PRO]

How to use

Disclaimer Notice

About

Inferno Stresser v2 - [FREE]



IP ADDRESS : 000.000.000.000

Ping IP

PORT : 80

SECONDS : 10

LAUNCH STRESS TEST !

Users Online : 2

14 : 37 : 38 PM

<http://inferno-stresser.com/>

Follow Us On Twitter & YouTube :

Latest Message Date : 13/Mar/2018

Use PRO Servers

Current Attacks

Look Up Tools

Notepad

Stress Test History :

Stress Tests Today : 79

Total Stress Tests : 143037

On-Going Stresses [FREE SERVERS] :

Server 1 : 0

Server 6 : 0

Server 2 : 0

Server 7 : 0

Server 3 : 0

Server 8 : 0

Server 4 : 0

Server 9 : 0

Server 5 : 0

Server 10 : 0

On-Going Attacks [PRO SERVERS] :

Server 1 :

Server 2 :

Server 3 :

Server 4 :

Server 5 :

[COMING BACK SOON]

Inferno Stresser v2 - Better than ever.

Starting your first security DDoS attack is extremely easy with InfernoStresser. Start by simply pasting in your target's IP address into the 'IP ADDRESS' text box(if you have not yet got it then you can use one of InfernoStresser's included look up tools to obtain it easily). Now you can proceed to typing in the port that you would like to DDoS attack on, depending on your target the port will vary. In most cases you will be stressing a home connection/website which in that case you will need to use port 80. But if you are DDoS'ing another type of server then use it's default port to DDoS on. Now you can choose the amount of seconds that you wish the DDoS attack lasts for, if you are on the free version then you will be limited to a maximum DDoS time of 100 seconds. If you would like to increase this then you should take a look at our paid PRO plans [here](#).

You are now all set and ready to launch your security network DDoS stress test with InfernoStresser, simply click the 'Start Attack' button(if you are on the free version you will be required to

2018-05-05 12-3...mp4

Tout afficher



DDOS | TOP 5 FREE BOOTER / STRESSER |

9,317 views

82

4

SHARE

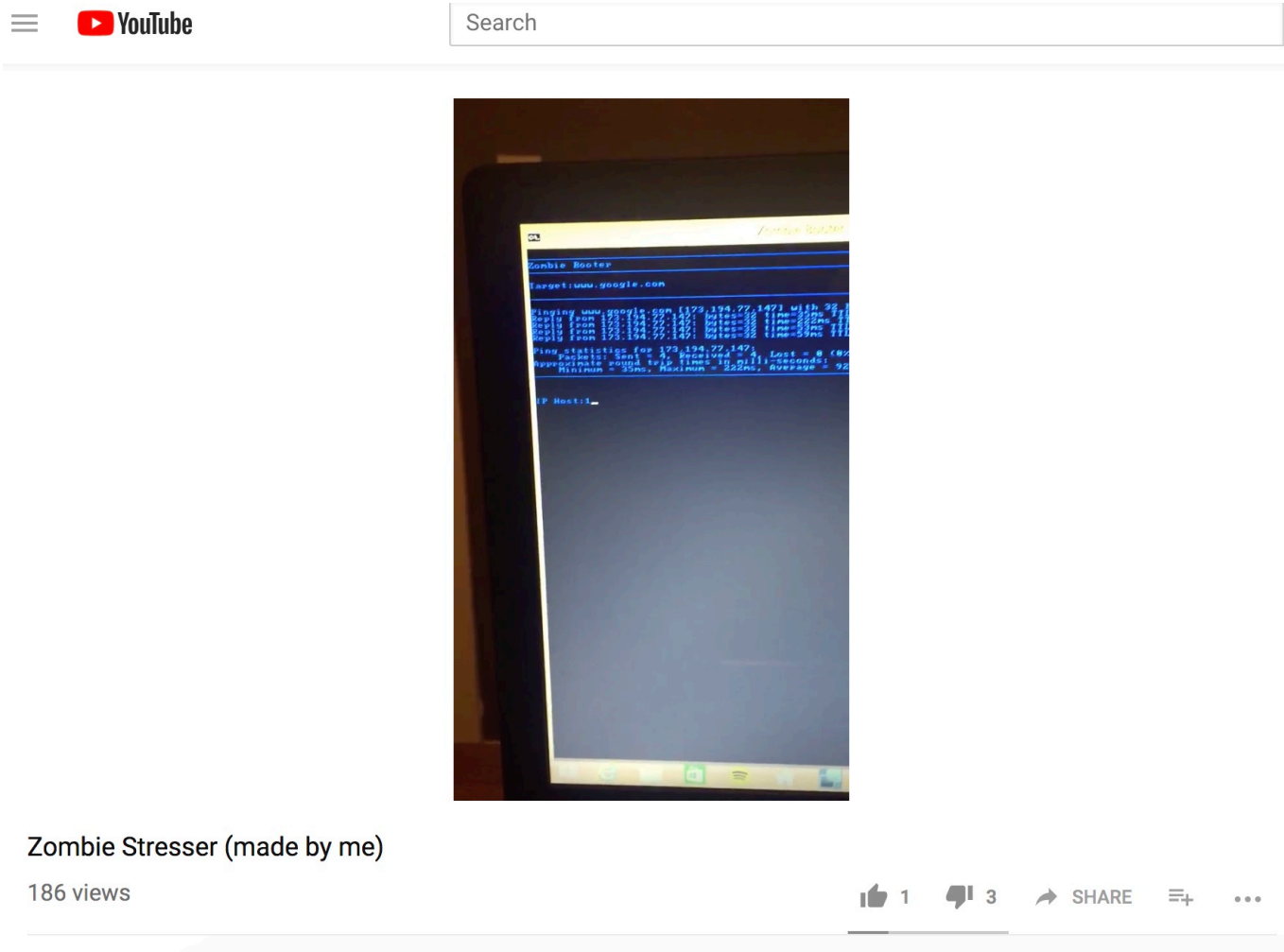
  Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release
and unlimited distribution."

30

Youtube videos



We also have blogspot sites

The screenshot shows a Blogger blog interface for a site named "Dark Booter". The header includes a search bar, a "G+" button, and a "More" dropdown. The user's email "leigh.metcalf@gmail.com" and links for "Dashboard" and "Sign Out" are in the top right. The main content area features a post dated "Tuesday, 29 January 2013" titled "Free Booter". The post content includes "Coyney's Network Stresser" with input fields for "Host:" and "Time:", a "Send Command" button, and links for "Domain Resolver" and "Skype Resolver". It is attributed to "By Coyney 2011-2013" and posted by "Dark Booter" at "00:42". Below the post are social media sharing icons and a section for "5 comments:", showing two comments from "Tech Max" dated "18 February 2014 at 10:55" with the text "lol" and "Reply" links. The right sidebar contains a "Blog Archive" section with a dropdown for "2013 (1)" and a sub-dropdown for "January (1)" listing "Free Booter". Below this is an "About Me" section with a "Dark Booter" profile picture and a link to "View my complete profile".

blogspot.ru sites



Want to do your own DDOS?

Articles

Cloud Storage

Business VoIP


Internet Speed Test

Twitter

Facebook

Google

Home / Browse / Security & Utilities / Security / UDP Floodflood



UDP Floodflood


UDP Flooder / DDoSer / Booter

Status: Beta Brought to you by: prjx8

★★★★★ 1 Review

Downloads: 26 This Week

Last Update: 2015-01-17

Download

Get Updates

Share This

Summary

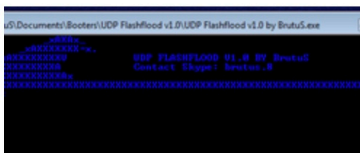
Files

Reviews

Support

DISCLAIMER: USE ON YOUR OWN RISK. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER OR CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES.

Project Samples



Or what about...

README.md

UBoat HTTP

A POC HTTP Botnet designed to replicate a full weaponised commercial botnet



license MIT awesome version 0.1.0

Disclaimer

This project should be used for authorized testing or educational purposes only.

The main objective behind creating this offensive project was to aid security researchers and to enhance the understanding of commercial HTTP loader style botnets . I hope this project helps to contribute to the malware research community and people can develop efficient counter measures :)

Usage of uboat without prior mutual consistency can be considered as an illegal activity. It is the final user's responsibility to obey all applicable local, state and federal laws. Authors assume no liability and are not responsible for any misuse or damage caused by this program.

What is a Botnet ?

Beyond DDOS

It makes sense that these guys would advertise themselves, they want people to buy them. That's their economic motive.

So I went looking for botnets.

botnet.cc



BOTNET.CC
(/)

SKYPE
RESOLVER
(LOGIN.PHP)

INFORMATION
(LOGIN.PHP)

LOGIN
(LOGIN.PHP)

REGISTER
(REGISTER.PHP)

A revolutionary IP test platform

The best pressure on the market platform.

LOGIN(LOGIN.PHP)

REGISTER(REGISTER.PHP)

Take down anyone with the best ip stresser / booter!

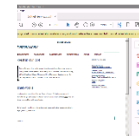


Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release
and unlimited distribution."

Botnet Servicex



botnetservicex

BUSSINESS

BANKING BOTNETS

POS BOTNETS

RANSOMWARES

BOTNET VIDEOS

FORUM

CONTACT

We are the best in our job!



Botnet-Servicex is a underground bussines dedicated to setup botnets. We give the control panel + exe totally fud + 400 bots. We have Banking, DDoS, Stealers, Bitcoin Miners and Pos Malwares. Best prices on the net, pay via Btc or Pm. You can contact with we via icq.

How our botnet works

The botnets have a control panel allocated in a Secure Private Server. We help you to use it, depending of the quantity of bots (pc zombies) you have you will receive more or less logs. We are working since 2009 without any problem with our clients.

Features

of the botnets depends the botnet you choose, it can be: grab password, steal password, attack web via ddos, grab dumps (track 2), load exe...

BtnSrvx Tests

December 5, 2016

[Good fudex and fast service....](#)

October 3, 2016

[Botnets work good, 1 day +40 CQ...](#)

September 28, 2016

[Secure Panels and Good Bots, I can...](#)

September 25, 2009

[Good](#)

September 20, 2009

[I recommend it because...](#)

Botnet-Servicex .Inc 2009-2017



Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release

and unlimited distribution."

Botnet Servicex

botnetservicex

[BUSSINESS](#) [BANKING BOTNETS](#) [DDOS BOTNETS](#) [POS BOTNETS](#) [RANSOMWARES](#) [BOTNET VIDEOS](#) [CONTACT](#)

Ransomware Winlockers



The Winlockers its a type of Malware, blocks the PC, encrypt the files and the victims need to pay a quantity of money to recov the PC. The pay usually in Btc, if the victim not pay the files of pc are deleted.

List and Prices

WinLocker Builder 4.0 - 100\$
MultiLocker v3.0 { Panel + Builder + Fud Exe + Lending Page + 100 Bots } - 200\$
Silent WinLocker V5.0 { Panel + Fud Exe + Lending Page + 100 Bots } - 250\$

Features

- Build Exe Malware (...)
- Control Pays of Bots
- And More

Botnet-Servicex .Inc 2009-2017

BtnSrvx Tests

December 5, 2016
[Good funcx and fast service...](#)

October 3, 2016
[Botnets work good. 1 day +40 CC...](#)

September 28, 2016
[Secure Panels and Good Bots. I can...](#)

September 25, 2016
[Good.](#)

September 20, 2016
[I recommend it because...](#)

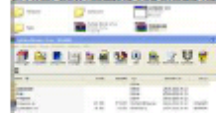
Cythosia botnet



Cythosia v2 is a simple HTTP Botnet which includes the standart Botnet features.

1.First of all Download it -->few false positive hits due that CythosiaBuilder is on some way hack tool

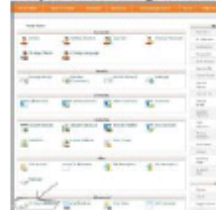
2. After Downloading you should have the .rar file. Extract it and it should look like this:



3. Now you need a Webhost to upload it. If you not already have one, i would suggest Free Web Hosting with PHP, MySQL and cPanel, No Ads
Create a account there with subdomain etc.

4. Once your subdomain is ready, go to your control panel.

5. In your Control Panel go to Advanced, then "Mysql Databases".

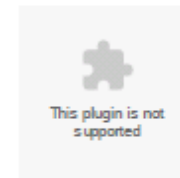
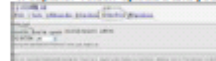


6. Fill out the required data.



7. Next to "mysql databases, there should be the task "phpmyadmin". Click on it. Then there should show up your created database. Click on "enter phpmyadmin".

8. Now you are in phpmyadmin. Goto to Import, then browse to to dump.sql, which you can find in the "webpanel" folder. Upload it and your done.



Werbung



miraiobotnet.eu

BENEFITS OF CHOOSING



LIGHTNING FAST

I'm always on duty, ready to provide sales and support at any given time!

Mirai botnet Shop ()

Trusted

Find out why!

BENEFITS OF CHOOSING ME



LIGHTNING FAST

I'm always on duty, ready to provide sales and support at any given time!



Software Engineering Institute | Carnegie Mellon University

Grep for Evil
August 28, 2018
© 2018 Carnegie Mellon University

"[Distribution Statement A] Approved for public release

and unlimited distribution."

freetrojanbotnet.com

Search:

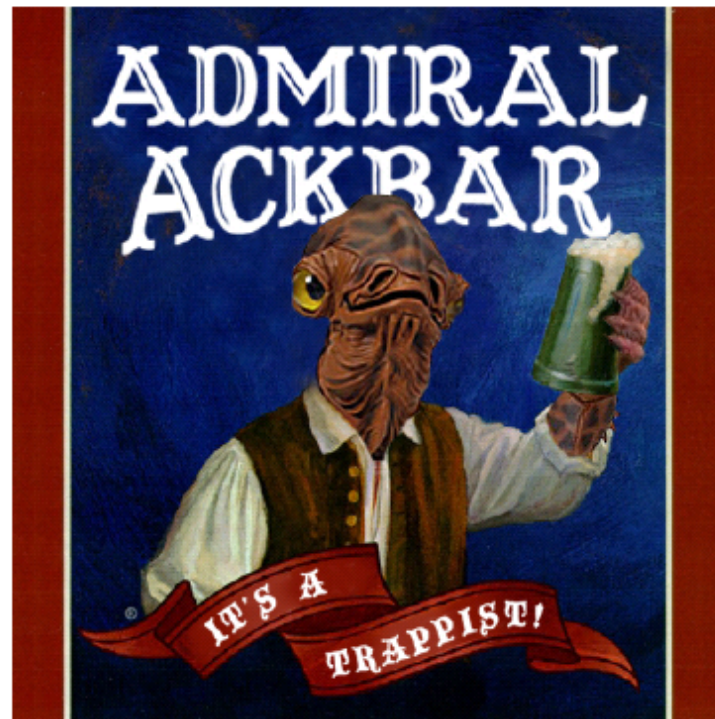
[VIP Section]

#DATE	#DESCRIPTION	#TYPE	#VIDEO	#RISK	#VERIFY	#PRICE	#FACEBOOK
07-08-2017	Zeus Botnet 5.0.0.1		video				facebook
07-02-2017	Will have a biggest update	any	video			0	facebook
02-12-2016	I NEED PANEL AND RINS BOT ANDROMEDA LAST VERSION	any	video			0	facebook
09-10-2016	Sell SMTP BruteForcer coded in c#	C#	video			100\$	facebook
05-08-2016	Citadel 6.0.1.1 (Xmas) Banking trojan	C++	video			0	facebook
03-09-2015	Rebot 1.0.0.1 full panel function+ Builder +100\$ full guide	C/C++	video			100\$	facebook

[Bot "Click Show ALL."]

#DATE	#DESCRIPTION	#TYPE	#VIDEO	#RISK	#VERIFY	#PRICE	#FACEBOOK
12-04-2017	Neutro HTTP Botnet v5.1 [Complete Panel + Builder]	C++	video			0	facebook
28-03-2017	Zeus Mod 2.0.0.1 fix work	C++	video			0	facebook
23-03-2017	Loli Stealer 1.6	C++	video			0	facebook
23-03-2017	DiamondBot botnet 4.2.0.00 Fix update new	C++	video			0	facebook
12-01-2017	Eglos HTTP BOTNET	C++	video			0	facebook
16-08-2016	Atrax Botnet (for hidden service, untraceable)	C	video			0	facebook
16-08-2016	Headal Bot Rtp Via version 6.6		video			0	facebook
16-08-2016	Headal Bot Rtp Via version 6.3		video			0	facebook
11-08-2016	DiamondBot botnet 4.2.0.00 FULL BUILDER	C++	video			0	facebook
10-08-2016	Poxy 2.2	C++	video			0	facebook
10-08-2016	Poxy 2.1	C++	video			0	facebook
16-07-2016	Megadodo Panel HTTP	C# (.NET)	video			0	facebook
14-06-2016	Blue botnet panel	VB6	video			0	facebook
14-06-2016	Neutro v3.0.4 HTTP Botnet Smart DDos Ferngraber CCGrabber ++ [Cracked by 0x22] New Edition	C/C++	video			0	facebook
14-06-2016	Neutro v3.0 HTTP Botnet Smart DDos Ferngraber CCGrabber	C/C++	video			0	facebook
14-06-2016	Neutro HTTP DDos Botnet Cracked by 0x22 & Lordi	C/C++	video			0	facebook
14-06-2016	[Update]Gadex - HTTP Bot (1.1.0.1) C++(ASM(Ring) Rootkit) Watchdog Anti Stable	C++/ASM	video			0	facebook
14-06-2016	Gadex v1.1.0 - HTTP Bot C & ASM, 36kb	C & ASM	video			0	facebook
14-06-2016	Blackout Botnet V2	C/C++	video			0	facebook
14-06-2016	Spy-0218 [web tool]	C/C++	video			0	facebook
14-06-2016	afenet v6.5 b	Python	video			0	facebook

Phishing – phishtown.com



[JOIN THE REBELLION](#)

[E-Mail the Admiral](#)

What about ransomware?

Why on earth would someone put ransomware in a domain name?

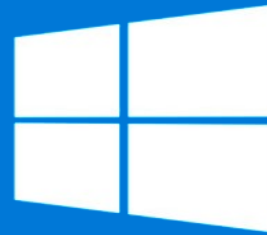
Well...

(DO NOT GO TO THESE SITES....)

microsoft-protection-from-ransomware.info

Windows Defender Alert : Zeus Virus Detected In Your Computer !!

Please Do Not Shut Down or Reset Your Computer.



The following data will be compromised if you continue:

1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Technical Support Immediately at +1 888-441-1595

Call Microsoft
Technical
Department:
(888)441 1595(Toll

Free)

microsoft-protection-from-ransomware.info

There's a phone number listed on this site. 888-441-1595

....It belongs to behappy2day.com. A mail order bride service.

ransomware-threat-detected-remove-it-now.info

The image shows a web browser window displaying a ransomware threat page. The page has a blue header with the Microsoft logo and navigation links (Store, Products, Support). The main content area is blue with white text that reads "Call for support: 1-888-822-3844". Below this is a link "Manage my account". At the bottom, there is a grid of Microsoft product logos: Windows, Windows Phone 8, Lumia devices, Xbox, Office, OneDrive, Surface, Microsoft Edge, Internet Explorer, Skype, Outlook.com, and MSN. A link "View all Microsoft products" is at the bottom center.

support.microsoft.com says:

**** Microsoft Warning Alert ****
Malicious Pornographic Spyware/Riskware Detected
Error # 0x80072ee7

Please call us immediately at: 1-888-822-3844
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.
Your computer has alerted us that it has been infected with a Pornographic Spyware and riskware. The following information is being stolen...

- > Financial Data
- > Facebook Logins
- > Credit Card Details
- > Email Account Logins
- > Photos stored on this computer

You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity. Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

Toll Free: 1-888-822-3844

☐ Prevent this page from creating additional dialogues.

[Stay Page](#) [Leave Page](#)

Call for support:
1-888-822-3844

Find downloads

ransomware-threat-detected-remove-it-now.info

Googling the phone number in this site goes to websites that claims it belongs to either Microsoft, Apple, iTunes...

I'm going to go out on a limb here and claim it's 'bad'.

Looking for ransomware in TXT records

I thought, why not? I'm grepping for evil.






























I have a passive DNS data set.

Let's see what happens!

(Spoiler Alert: I found some...)

Looking for ransomware in TXT records

Index of /ransomware

Name	Last modified	Size	Description
 Parent Directory	-		
 a(13).exe	2017-09-11 18:18	155K	
 a(14).exe	2017-09-11 18:18	209K	
 a(15).exe	2017-09-11 18:18	2.0M	
 a(16).exe	2017-09-11 18:18	1.3M	
 a(17).exe	2017-09-11 18:18	1.3M	
 a(18).exe	2017-09-11 18:18	224K	
 a(19).exe	2017-09-11 18:18	2.1M	
 a(20).exe	2017-09-11 18:18	224K	
 a(21).exe	2017-09-11 18:18	1.7M	
 a(22).exe	2017-09-11 18:18	224K	
 a(23).exe	2017-09-11 18:18	1.3M	
 a(24).exe	2017-09-11 18:18	319K	
 a(25).exe	2017-09-11 18:18	319K	
 a.exe	2017-09-11 18:18	319K	
 a2	2017-09-11 18:18	1.3M	
 a3.exe	2017-09-11 18:18	188K	
 a4.exe	2017-09-11 18:18	523K	
 a5.exe	2017-09-11 18:18	210K	
 a6.exe	2017-09-11 18:18	1.9M	
 a7.exe	2017-09-11 18:18	164K	
 a8.exe	2017-09-11 18:18	1.3M	
 a9.exe	2017-09-11 18:18	319K	
 a10.exe	2017-09-11 18:18	224K	
 a11.txt.exe	2017-09-11 18:18	1.3M	
 a12.txt	2017-09-11 18:18	1.2M	
 alliamisnetcat.exe	2017-09-12 15:36	58K	
 notanevil file	2017-09-12 15:36	0	
 ransom.zip	2017-09-12 15:37	14M	

Another thing I learned...

Do NOT go to sites with both **bank** and **login** in the name.

bankofamerica.com.login.sign-in....



Deceptive site ahead


Attackers on **bankofamerica.com.login.sign-in.signonv2.screen.castadotaciones.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ [Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

DETAILS

Back to safety

bankofamerica.com.login.sign-in....



Personal | Small Business | Wealth Management | Businesses & Institutions | About Us

Locations | Contact Us | Help | En español |

Enter your Online ID

Sign In


☐ Save this Online ID

Help/options

Enroll

Bank | Borrow | Invest | Protect | Learn

BankAmericard Cash Rewards™ credit card



\$100

Cash Rewards Bonus Offer

Offer details

1% cash back everywhere, every time

2% cash back at grocery stores

3% cash back on gas

Grocery/gas bonus rewards on \$1,500 in combined purchases each quarter.

Information for:


Simple, low pricing

\$6.95

\$6.95 per online equity and ETF trade with Merrill Edge®

Start Today™ »


Up to \$100 a year



To pay down your balance plus a competitive interest rate.

Learn more »

Lighten the load



Taking the heavy lifting out of moving.

See how »

Locations

[More search options](#)

Privacy & security

[Website Ad Practices](#)

No foreign transaction fees

The BankAmericard Travel Rewards® credit card makes using your card abroad easier. Avoid the foreign transaction fees of some cards that can be up to 3% of purchases. Plus, enjoy chip technology, which is more widely used internationally.

[Learn more about the BankAmericard Travel Rewards® card »](#)

Need help with your home loan payments?

If you're a homeowner struggling with your loan payments, you may want to learn about our home loan assistance programs. Bank of America is committed to helping homeowners and is a participant in the national mortgage settlement agreement.

[Learn more about home loan assistance »](#)

[Learn more about the National Mortgage Settlement »](#)

Popular links

- Order checks
- Order a debit card
- Order foreign currency

pnc-banking-...



Deceptive site ahead

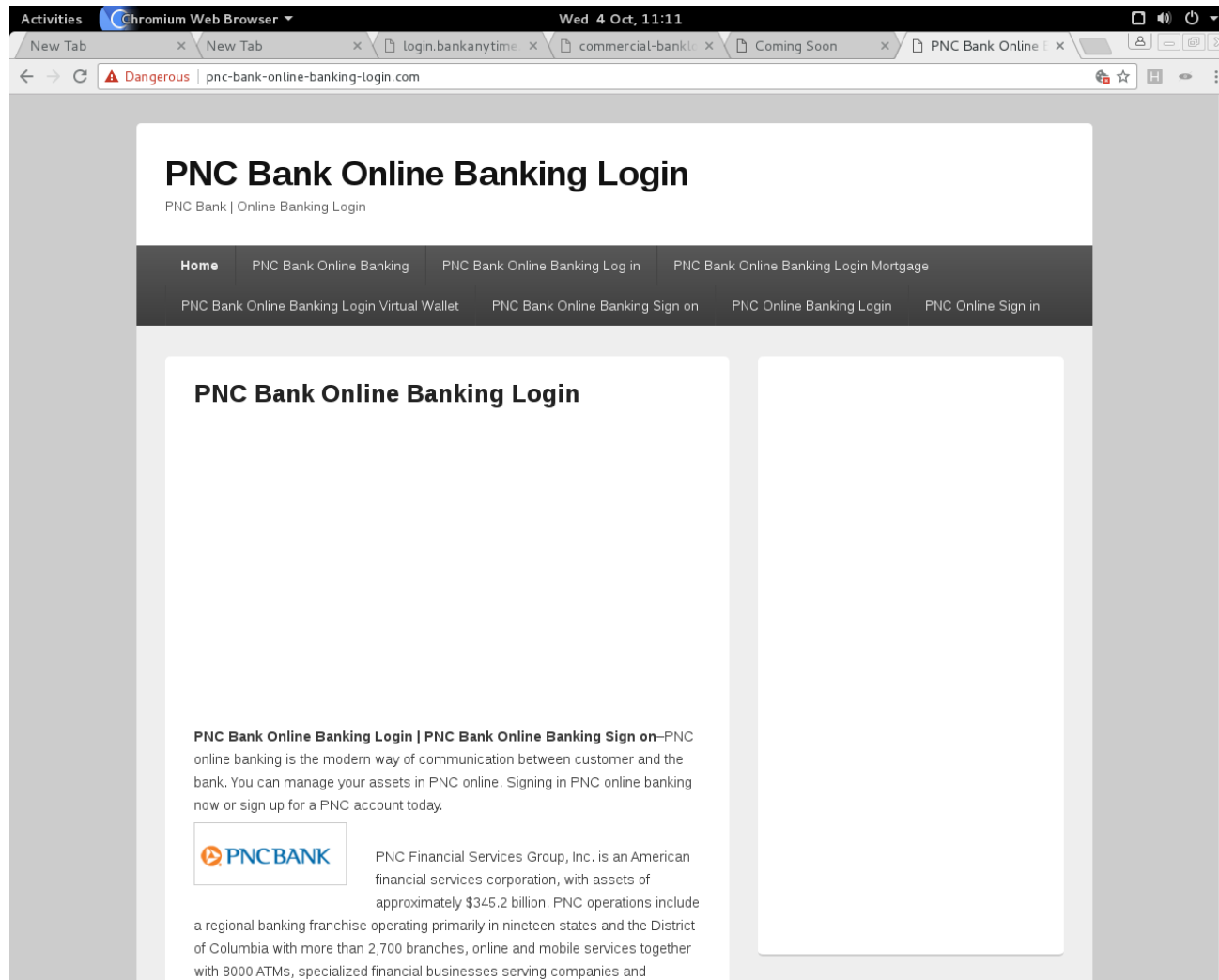
Attackers on [pnc-bank-online-banking-login.com](#) may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ [Automatically report](#) details of possible security incidents to Google. [Privacy policy](#)

DETAILS

Back to safety

pnc-banking-...



bank AND login

Neither of those were actually Bank sites.

Isn't it nice they tell me they are?

Zero Days

What else to look for?

How about 0days? I found a website that promised to sell me some.

0day.today



0DAY.today? Tör

Injeksi is the best database of exploits and vulnerabilities and a source of resources for security researchers and security professionals. Our goal is to collect exploits from our contributors and several mailing lists and convert them all in one, easy navigation in the database. This was written only for educational use. Use it at your own risk. The author will not be responsible for any damages. © 2007/16

Select your language

Do you accept these terms?

Yes, I accept them

User agreement

Anyone accessing 0day.today 1337day.com/ You need to accept the terms and conditions or leave immediately 0day.today 1337day. If you do not agree with the terms of 0day.today 1337day you need to leave 0day.today 1337day. The 0day.today 1337day team reserves you to participate in our project, all you have to do is register!

General Information

Official information about 0day.today 1337day and its team is published exclusively on the 0day.today 1337day website. Do not rely on the negative criticisms or rumors others say - it's a MYTH! We do not deface ANY website and we do NOT attack any web-servers. The 0day.today 1337day team operates solely in bug research, not malicious actions. 0day.today 1337day is released without any warranty and exists solely for educational purposes. 0day.today 1337day and its team are not responsible for illegal use of the information provided. 0day.today 1337day is your new digital friend who will help you avoid many security problems on your website!

Action, Law, Programmer & Source Code

We pay extra attention to follow all necessary European laws, but we exercise our right to exchange information in a secure way. All the submitted vulnerabilities will be forwarded to the manufacturers of the product and will be published to protect your local environment. If a vulnerability contains either malicious code, illegal comments and/or sensitive details, the vulnerability will be removed or modified.

0day.today 1337day Mission Statement

The 0day.today 1337day Mission is to provide a database of standards and technology to protect your information systems against possible threats. Some threats may be targeting the confidentiality or integrity of your information systems and the availability of your information and services. Here at 0day.today 1337day, we try to inform you as soon as possible when new security breaches are discovered so you can take appropriate action to patch/fix them.

Official Statement of the 0day.today 1337day Team

We do not approve or encourage anyone to modify any vendor licenses, deface websites, hack into databases and/or trade with fraudulent or stolen material. We do not publish advertisements/vulnerabilities which speak against certain religions, support terrorism/terrorism, or anything negative in nature. We do not allow any criminal activities or requests by members in our database or email. Such examples will be deleted instantly without any comment. 0day.today 1337day provides information to you 'as is' and will not be held responsible for any damage done to you. Injeksi contains information which may be considered illegal in some countries. Such information is provided here solely for educational purposes and is not intended to be used for illegal activities. © 0day.today 1337day Administration


0day.today 1337day Injeksi Exploit Market and 0day Exploits Database
Base de données Injeksi company vende exploits (local, remote, DoS, PoC, etc.)
Pour plus d'informations a contactez@inje.com
Copyright © 2008-2017 Injeksi Team

0day.today

[\[home \]](#)
[\[private \]](#)
[\[setup \]](#)
[\[Get Gold \]](#)
[\[platforms \]](#)
[\[postnet \]](#)
[\[hash \]](#)
[\[search \]](#)
[\[faq \]](#)
[\[agreement \]](#)
[\[contact \]](#)
[\[style \]](#)
[\[Price in Gold \]](#)
[4th: 20 429](#)
[\[100% \]](#)
[\[100% \]](#)

[\[contact us \]](#)
[\[M \]](#)

[\[100% \]](#)
[\[authentication \]](#)
[\[registration \]](#)
[\[secure account \]](#)



0day.today is the ultimate database of exploits and vulnerabilities and a great resource for vulnerability researchers and security professionals. Our aim is to collect exploits from all over the world and make them available to everyone in a simple and easy-to-use format. This was written solely for educational purposes. Use it at your own risk. The author will be not responsible for any damage. © 2017

0day.today Available within TOR at <http://tor.0day.today.onion>

OrientDB 2.2.x Remote Code Execution Exploit

[1337day-ID-20156]

Full title	OrientDB 2.2.x Remote Code Execution Exploit [Highlight]
Date add	00-10-2017
Category	remote exploits
Platform	java
Verified	✓
Price	free
Risk	[Security Risk Critical]
Ref. releases	R
Description	This Metasploit module leverages a privilege escalation on OrientDB to execute unauthorized OS commands. All versions from 2.2.2 up to 2.2.22 should be vulnerable.
Abuses	0
Comments	0
Views	74

free

Open Exploit

✓ Verified by 0day Admin

Author: [Ricardo Jorge Borges de Almeida](#)

RL: 29

Exploits: 1

Readers: 0

[Comments: 0]

So this looks easy, right?

I found:

DDOS

botnets

ransomware

0days...

And that's not even including the malware!

On the other hand...

Domain Name-based Blacklists				
Lists Gained				
Lists Lost				
Domain Names				
Report	Total Lists	Lists Gained	Lists Lost	Unique Indicators
2012.1	11	--	--	6468501
2012.2	11	0	0	9235902
2013.1	20	10	1	12592250
2013.2	20	0	0	5027066
2014.1	20	0	0	2772391
2014.2	20	0	0	10446624
2015.1	35	19	4	12231742
2015.2	35	0	0	13051429
2016.1	31	7	11	24359712
2016.2	26	4	9	26274848
2017.1	27	4	3	26805987
2017.2	26	5	6	40857873

While finding these domains was fun...

We're not even making a dent in the total amount of badness out there by just looking for the easy things.

In summary: Finding the guys that are hiding is hard.
Finding the guys that aren't hiding isn't.

Questions?

PS. Don't go to domains with both bank and login in them!