



The Russian DDoS One

Booters to Botnets



The Russian DDoS One

Booters to Botnets

- Dennis Schwarz
 - Sr. Security Research Analyst



- (Formerly) Security Analyst



Disclaimer #1

- “Failure [to properly attribute malware and threat actors] is always an option!”



Disclaimer #2

Google Translate

https://translate.google.com/#auto/en/русский%20язык

Google

Sign in

Translate

German Portuguese Spanish **Russian - detected**

русский язык

russkiy yazyk

See also язык, русский

English Russian Spanish **Translate**

Russian language

Translations of русский язык

noun Russian русский, русский язык, русская

Google Translate for Business: [Translator Toolkit](#) [Website Translator](#) [Global Market Finder](#)

[Turn off instant translation](#) [About Google Translate](#) [Mobile](#) [Community](#) [Privacy](#) [Help](#) [Send feedback](#)

Political Correctness #1



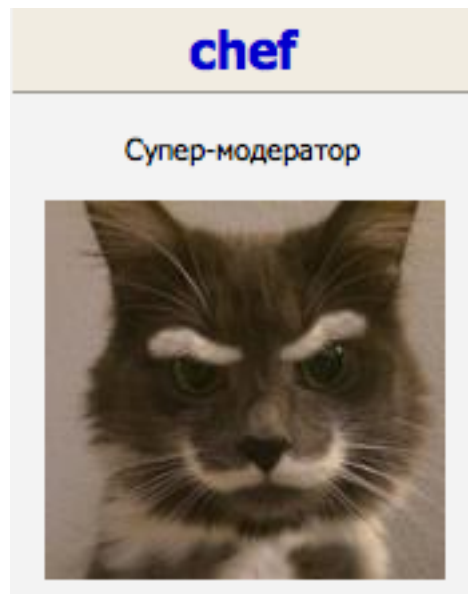
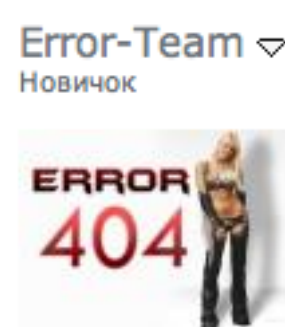
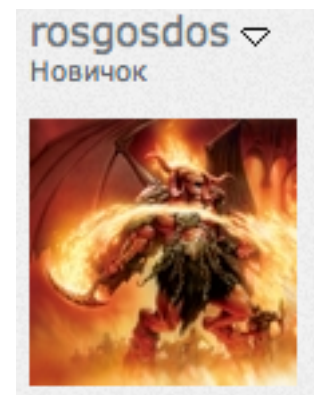
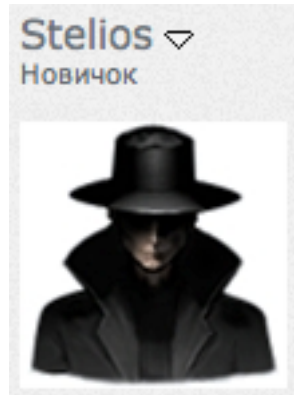
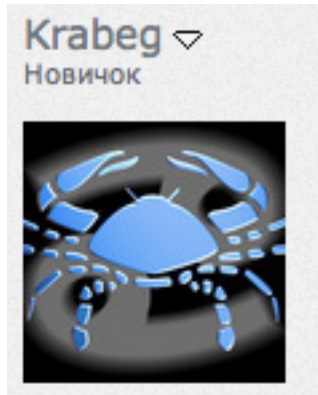
The Russian DDoS One or RD1

- Because why should APT groups be the only ones with fancy names?
- Informal grouping
- DDoS as a Service
 - DDoS booters
- Public Russian language underground/hacking

Forum Sampling



Threat Actor Sampling



Advertisement

20.03.2011 21:08

Vendettaa

Beginner

Date: 20.03.2011

Posts: 11

Reputation: 0

Order >> DDOS attack / DDOS Service / DDOS Service <<

Order >> DDOS attack / DDOS Service / DDOS Service <<

УСТРАНИМ ЛЮБОЙ САЙТ КОНКУРЕНТА

We offer services in the organization of a DDOS attack.

DDoS-attack - an attack on a computer system in order to bring it to failure, ie the creation of an environment in which users of the system can not access the resources provided by the system.

If you interfere with any site or server, or other online resource, we are ready to eliminate it 😊

Different methods of flood. Good prices!

[+] Http flood

[+] Https flood

[+] Icmp flood

[+] Post flood

[+] Syn flood

[+] Udp flood

[+] Dns stress

Price:

Hour from \$ 5 **

Day from \$ 60 **

Week from \$ 350 **

** In the case of the order is possible manibek for the remaining time.

Before you start to do the test for 5-10 minutes, advise, help to understand in the event of any problems.

Just provide discounts:

When paying for a week - 3% of the total

When paying for 2 weeks - 5% of the total

When paying for 30 days - 10% of the total

Just strictly adhere to the policy of anonymity (no logs during a conversation is not in progress) *, no one under any circumstances will not know who and why did we have this or that order.

* If the customer will give your own jabber server to register an account (complete lack of logging and complete anonymity)

In our work we use a privat DDoS bots. Can work on complex projects with anti-DDoS protection and the protection type CISCO™ GUARD.

Customers

- Gaming
- Rivalry
- Anti-competition
- Ransom
- Diversion

DDoS Attack Types

- ICMP flood
- UDP flood
- TCP flood
- TCP SYN flood
- HTTP GET/POST flood
- Slowloris
- DNS specific floods

Pricing

- Hourly: \$5-15
- Daily: \$40-80
- Weekly: \$260-400
- Trend Micro's Cybercriminal Underground Economy Series: Russian Underground Revisited

Service	2011 Price	2012 Price	2013 Price
DDoS attack: <ul style="list-style-type: none">• Lasts 1 hour• Lasts 24 hours	US\$4–10 US\$30–70	US\$2–25 US\$15–60	US\$2–60 US\$13–200

Reputation – Member Vouches

19.03.2012, 16:51

2

Aleks777

Nobody

Date: 19.03.2012

Posts: 1

Reputation: 0

Use the services of the vehicle, everything went perfectly!
'Il Obraschatsya else.

Quote

27.04.2012 18:57

3

gerhard

Nobody

Date: 27.04.2012

Posts: 1

Reputation: 0

I confirm! Seller adequate, pleasant to talk to. Conducted several tests, have chosen a more appropriate way, all for free. Prepay service, but had to quickly change the time service, and within 5 minutes everything was ready. Advise!

Quote

ARBOR[®]
NETWORKS

14

Reputation – Admin Test Targets

25.09.2012, 00:57

2


onthar

Admin

Date: 08.01.2008

Posts: 6,340


Reputation: 3759



Fixed 25.09.12

The test is successful. Specified resource (poseschalka to 3k) to stop responding for a minute.

Last edited by onthar; 25.09.2012 at 01:23 ..



Reputation – Dispute Resolution

- Forum admins
 - Judge
 - Jury
 - Executioner
- Doxing
 - “Blacklist” section on forums
 - Pastebin

“Working”

15.06.2014, 09:07	# 6
<p>Vendettaa Beginner</p> <p>Date: 20.03.2011 Posts: 11 Reputation: 0</p>	<p>work</p> <p>Quote</p>
29.06.2014 10:11	# 7
<p>Vendettaa Beginner</p> <p>Date: 20.03.2011 Posts: 11 Reputation: 0</p>	<p>true</p> <p>Quote</p>
08/17/2014, 7:58	# 8
<p>Vendettaa Beginner</p> <p>Date: 20.03.2011 Posts: 11 Reputation: 0</p>	<p>work</p>

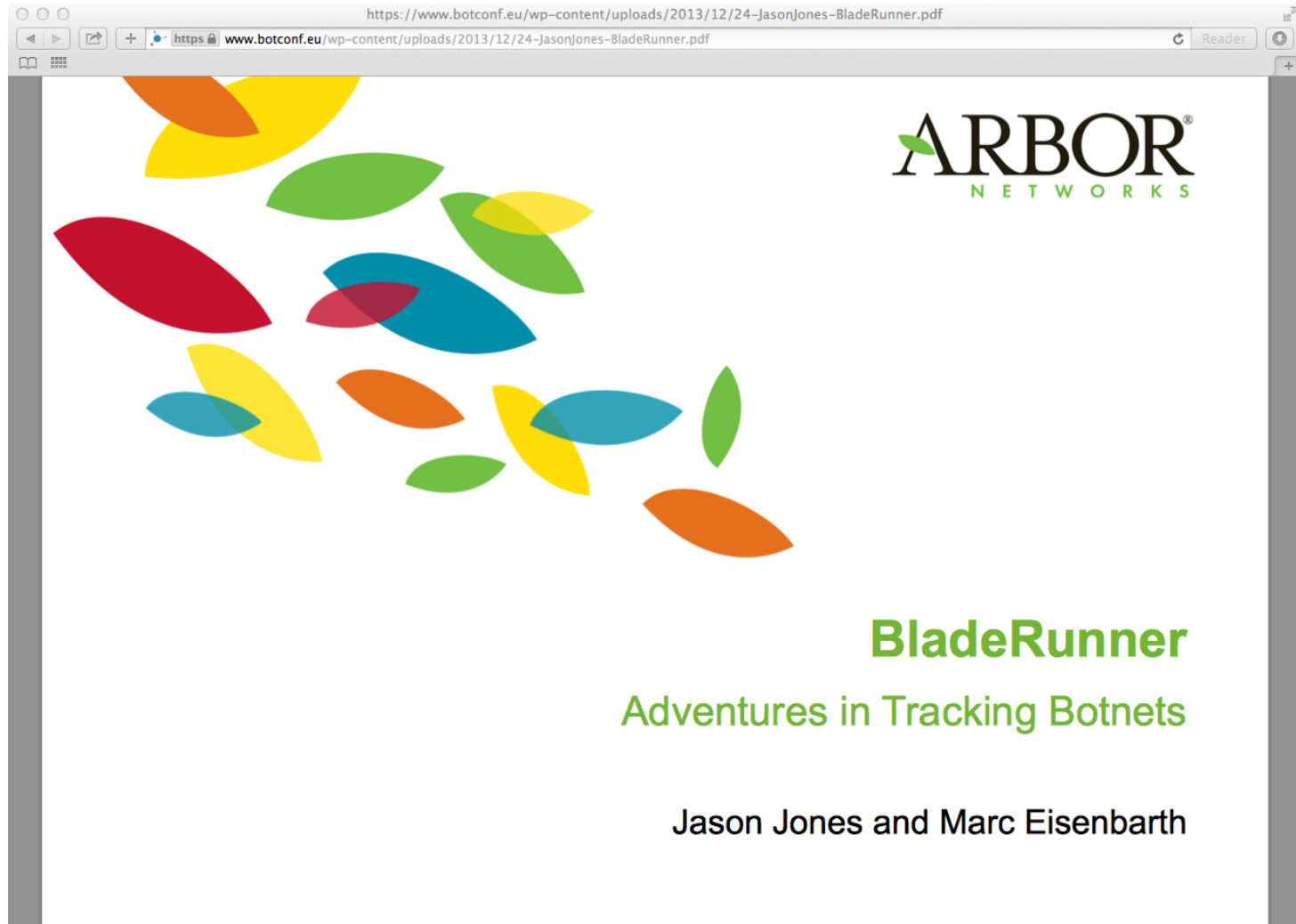
Communications

- ICQ
- Jabber
- Skype

DDoS Booters – Back-end Infrastructures

- “hmm, i dont know about wich booters you talking, but russian ddosers always used botnets” [sic] – AreYouAreDo

BladeRunner





The Many Booters of Stelios

Stelios – Ad

Google Translate From: Russian To: English View: Translation Original

http://brute.name/threads/13655/

DDoS Service 911

booter name

Stelios New Member Messages: 23

handle

DDoS Service 911

Срочная помощь в решении Ваших проблем. Самые доступные цены. 222423

jabber

banner

DoS-attack (from the English. Denial of Service) and DDoS-attack (from the English. Distributed Denial of Service) - a kind of attack on the computer system whose purpose is to bring the system to a state overload at which it can not access legitimate users, or this access is difficult.

Our DDoS service - the best remedy for pesky competitors that prevent you from working. Urgent help in solving your problems - a support network in almost around the clock!

We present you the service Ddos-services that can help you eliminate business rivals, etc. We will help you to test the anti-ddos protection for your server, site. In our Ddos-service, you can order a DDoS attack on almost any website or server! Carry out DDoS attacks on game servers, online shopping, political sites!

Our prices are the most affordable on the market DDoS services. Average price is only \$ 50 a night. Kolebatsya final price may be bigger, and the smaller side. Wholesale customers and regular customers Individual conditions!

Attention! In view of the widespread fraud in Ddos-orders DDoS services, do test only after the transfer under the protection code, in order to combat resellers and Kidal.

Payment Methods:
WebMoney
Perfect Money
ICQ or payment methods by arrangement.

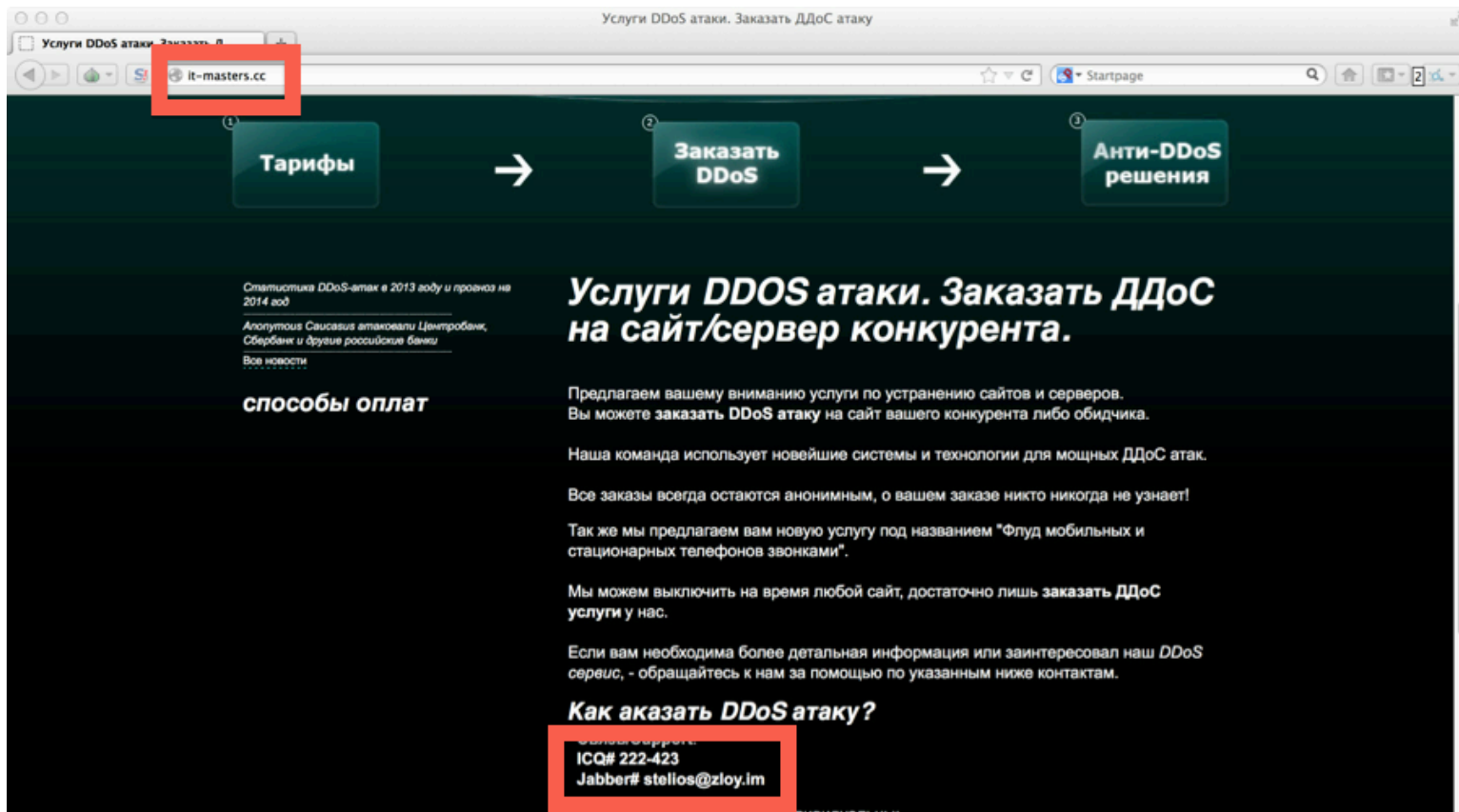
ICQ

Communication / Contact:
ICQ: 222423

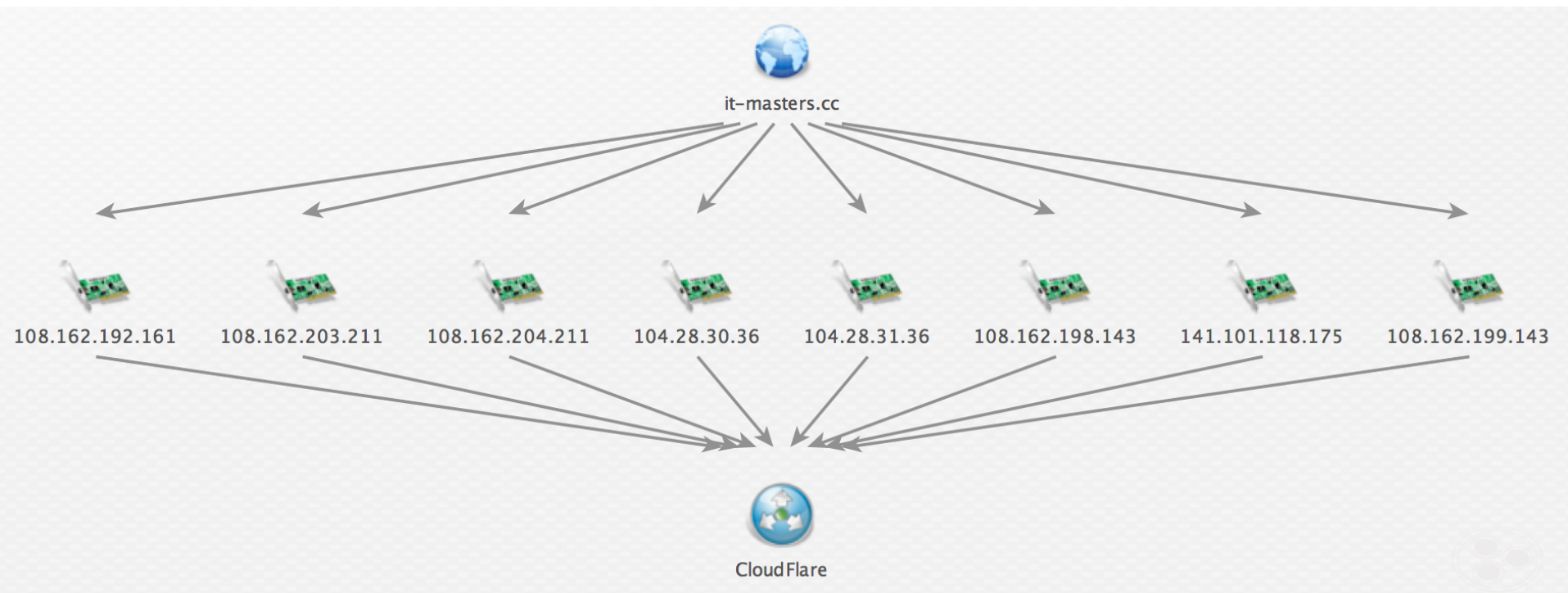
website

Our website: it-masters.cc

Stelios – it-masters.cc



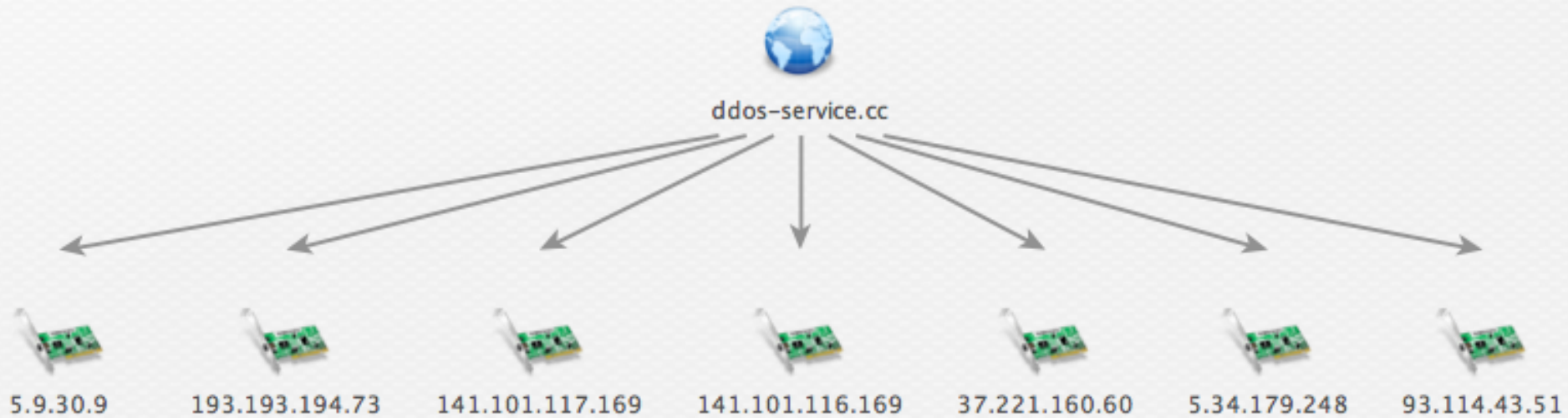
Stelios – it-masters.cc



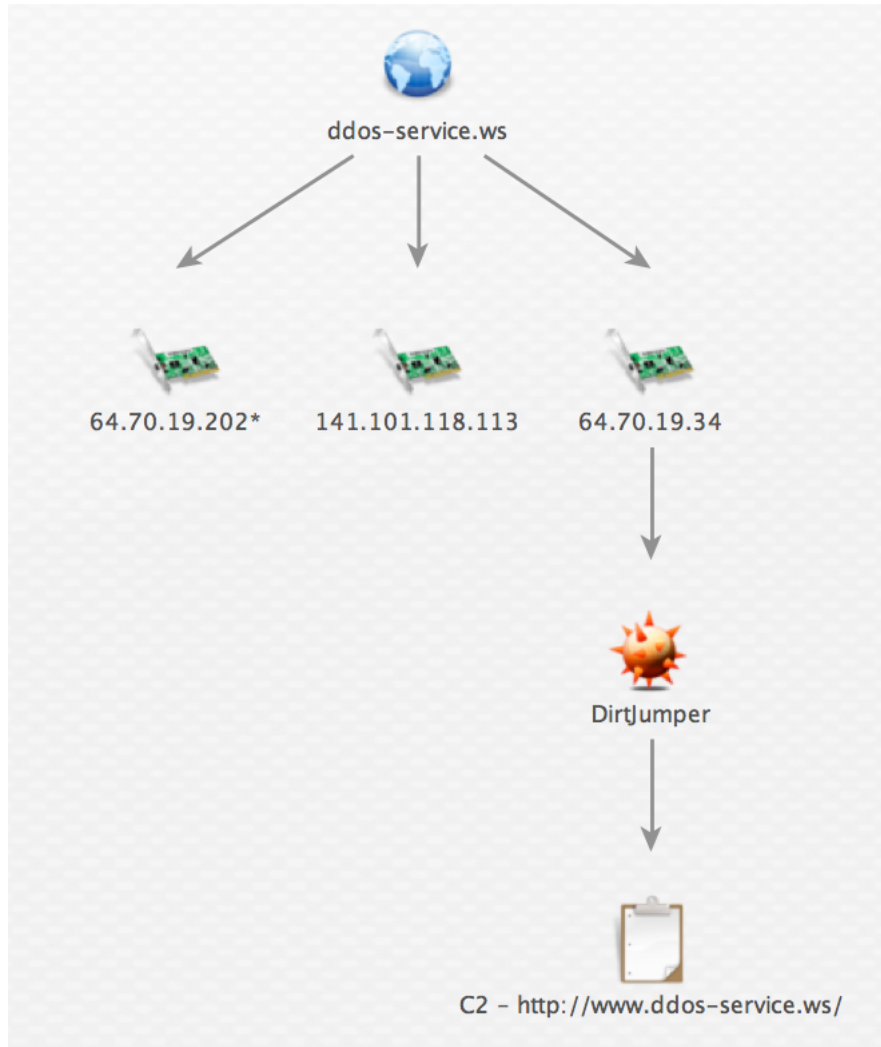
Stelios – Initial Pivots

- Handles
 - Satory (2013)
 - [maverbest](#) (2013)
 - [maverickxx](#) (2012)
 - [maverick](#) (2011)
 - BadGateway (2011)
- ICQ
 - 332212
 - 372223
 - 444556
- Jabber
 - [stelios@jabber.se](#)
 - [maverick@xmpp.jp](#)
 - [stelios@exploit.im](#)
- Websites
 - [ddos-service.cc](#)
 - [ddos-service.ws](#)

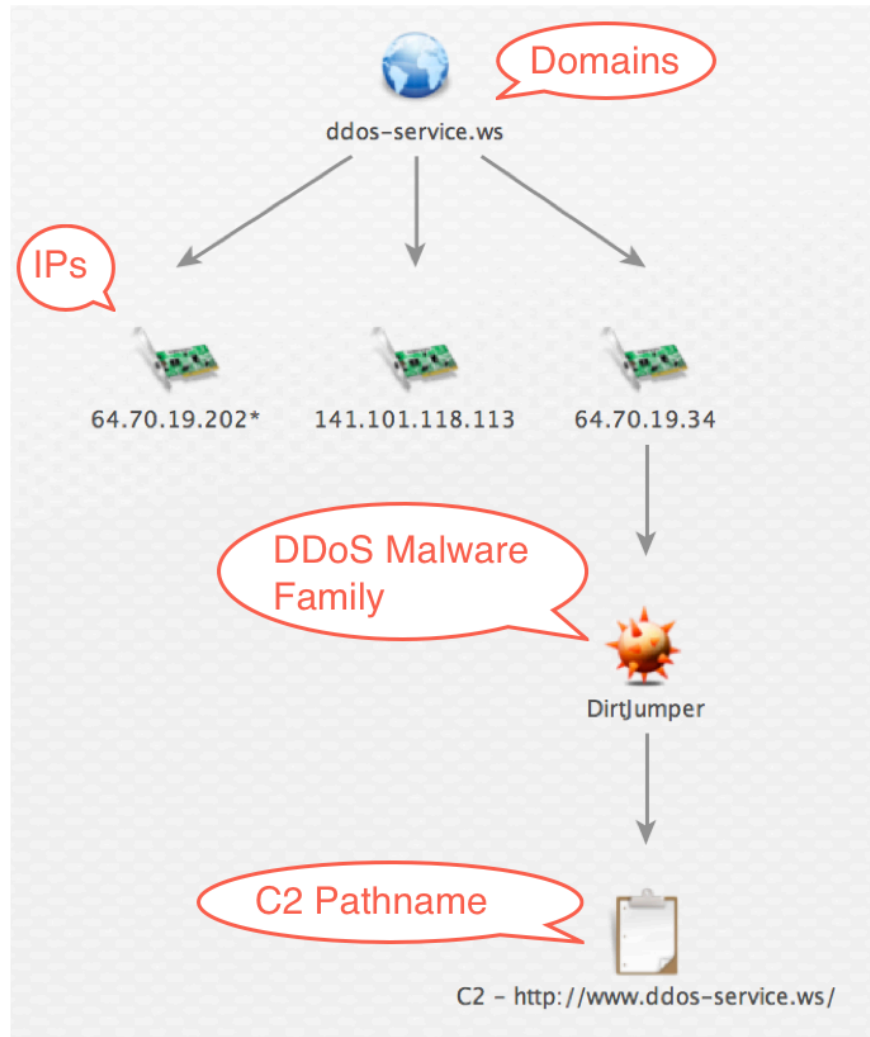
Stelios – ddos-service.cc



Stelios – ddos-service.ws



My Maltego Outline



Stelios – Nginx Identity

☐ **Promotional poster DDoS services** {site}

Views: 175 / Comments: 0



URL: www.ddos-service.ws

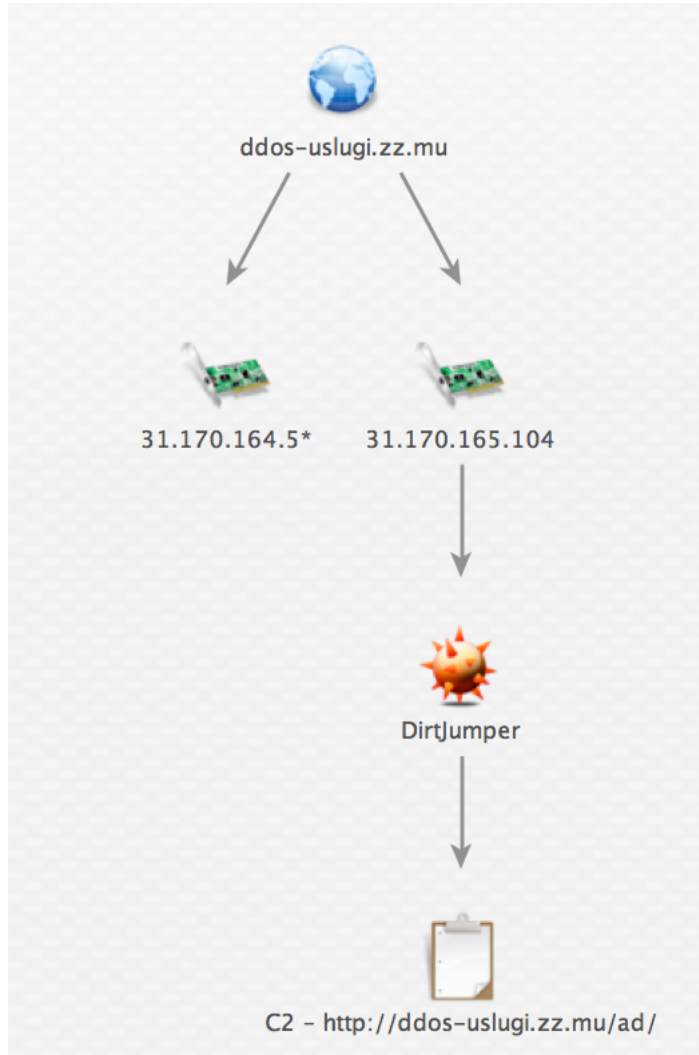
So there is the possibility of buying the site itself or design without domain price \$ 50 If interested please write in website ICQ 497065

Information: Published: August 19, 2013 at 10:32

Seller: [Nginx](#)

- Handle: Nginx (2013)
- ICQ: 497065
- Jabber: nginx@xabber.de
- Emails
 - ddos_ddos@aol.com
 - antiddos@ukr.net
- Websites
 - ddos-uslugi.zz.mu
 - ddos-service.nethouse.ru

Stelios – ddos-uslugi.zz.mu



Stelios – ddos-service.nethouse.ru



Stelios – C2 Patterns

- ddos-service.cc
- ddos-service.ws
- ddos-uslugi.zz.mu → “uslugi” Polish for “service” ?
- ddos-service.nethouse.ru

Stelios – Doxed

Stelios = maverick = Ø // Slexy 2.0

slexy.org/raw/szHgsmvrvr/

Author: maverick, Language: text. Description: **Stelios = maverick = Ø**, Timestamp : 2013-09-24 04:21:25 -0400 ...

Exploit.IN Forum -> Stelios aka Maverick icq 222423 stelios...

[exploit.in](#) > ... > [Black List](#) > [Black List](#) > Translate this page

Aug 16, 2014 - 20 posts - 7 authors

Приветствую! Претензии по сути нет, суть этого поста в разоблачении **Stelios** aka **Maverick**. Данный индивид по подтвержденной ...

Maverick 444556, Внимание - кидала

kidala.info/kidala_ripper_18775.shtml > Translate this page

May 1, 2012 - Jabber(2) кидалы: **maverick@thesecure.biz**. Jabber(3) кидалы: **maverick@exploit.im**. Jabber(4) кидалы: **stelios@jabber.se**. Сайт кидалы: ...

VeNoM||.Stello[S] CSS - 3 Kill Together (with Maverick



www.youtube.com/watch?v=OWuAar3j0NI

Feb 22, 2010 - Uploaded by Stelios Tr.

Sign in to YouTube. Sign in with your Google Account (YouTube, Google+, Gmail, Orkut, Picasa, or Chrome) to ...

Advent Chaos - The Gaming Family Wiki

thegamingfamily.wikia.com/wiki/Advent_Chaos >

Upon arriving, though, there is an air of unease, as **Maverick** makes **Stelios** an offer, to join an organization called the Cult of Chaos. **Stelios** does not comply, ...

Maverick=Stelios кидала! - ShopWorld

shopworld.biz > ... > [Любям о людях](#) > [Black](#) > Translate this page

Aug 9, 2012 - 10 posts - 6 authors

Если у вас есть доказательства мультотства - прошу предоставить их, а так это лишь ваши пустые слова и домыслы.. Я могу тоже ...

Stelios – IPs

Krabeg

DDoSSer



Join date: 17 June 2012
Posts: 100

Say thank you: 42

4550085

maverick = stelios = THREW, rat, cheater!!!

Quote:

Originally posted by **Mavruša**

Hidden text (you must log in using your login or register and have 5 post (s)):
You do not have rights to see the hidden text contained here.

Mavruša, you're dumb deer where you saw that I had someone threw? Nowhere, because I do not throw, and you're out there asshole.

And that's what you threw and moor, is well known to all, moreover, you here a couple of days ago threw Chela on the headst the money, while the site was quite weak, it means that you have even 200 bots haven't you only show-off their pitch and can

Quote:

Message from **the log from blekmena (the neighing)**

[23.09.2013 14:59:36] <[Links can only see registered users. Зарегистрироваться...] > ddos nado?

[23.09.2013 15:05:34] < none > Stelios horseman of the Apocalypse

[23.09.2013 15:07:30] <[Links can only see registered users. Зарегистрироваться...] > ve tut?

[23.09.2013 15:08:16] <[Links can only see registered users. Зарегистрироваться...] > ya > maverick

[23.09.2013 15:08:55] <[Links can only see registered users. Зарегистрироваться...] > ve ahueli?

[23.09.2013 15:08:59] <[Links can only see registered users. Зарегистрироваться...] > mamka ebal

[23.09.2013 15:09] <[Links can only see registered users. Зарегистрироваться...] > rot toptal

[23.09.2013 15:14:26] <[Links can only see registered users. Зарегистрироваться...] > ale?

[23.09.2013 15:14:40] <[Links can only see registered users. Зарегистрироваться...] > lox ebani

Mavrušečka simply obsiraetsâ from ddosa, zaddosit', nothing is in any way trying to eliminate competitors by fake.

pastebin.ru/VS781gsR

pastebin.com/6pSfnktD

Data pages are removed, leaving only the Google cache.

91.121.166.108

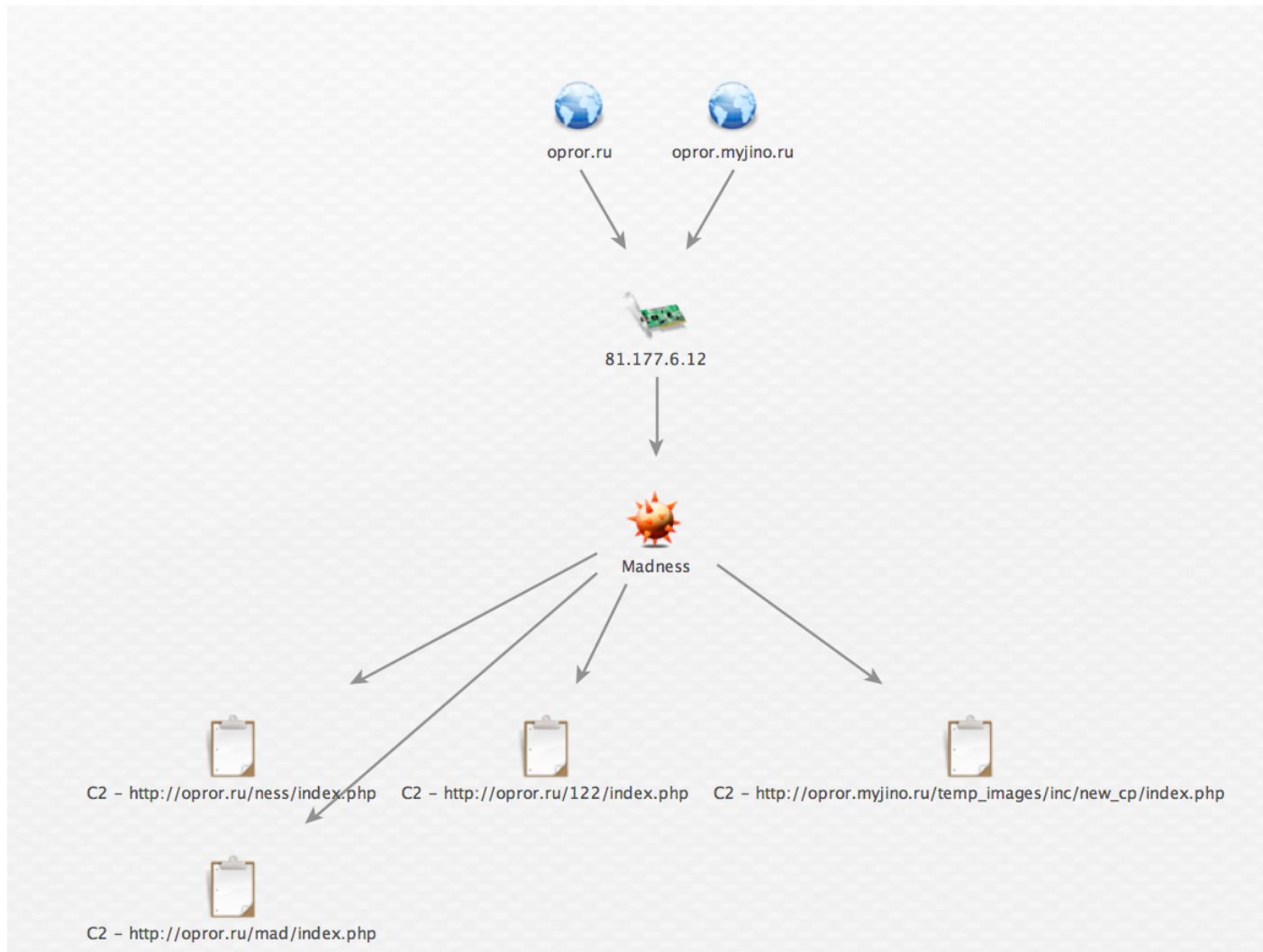
Here is the IP of the bastard, who all this dirt muddies:
91.121.166.108 (granted the admin of pastebina)

Please check this IP on the basis of the shop go online.

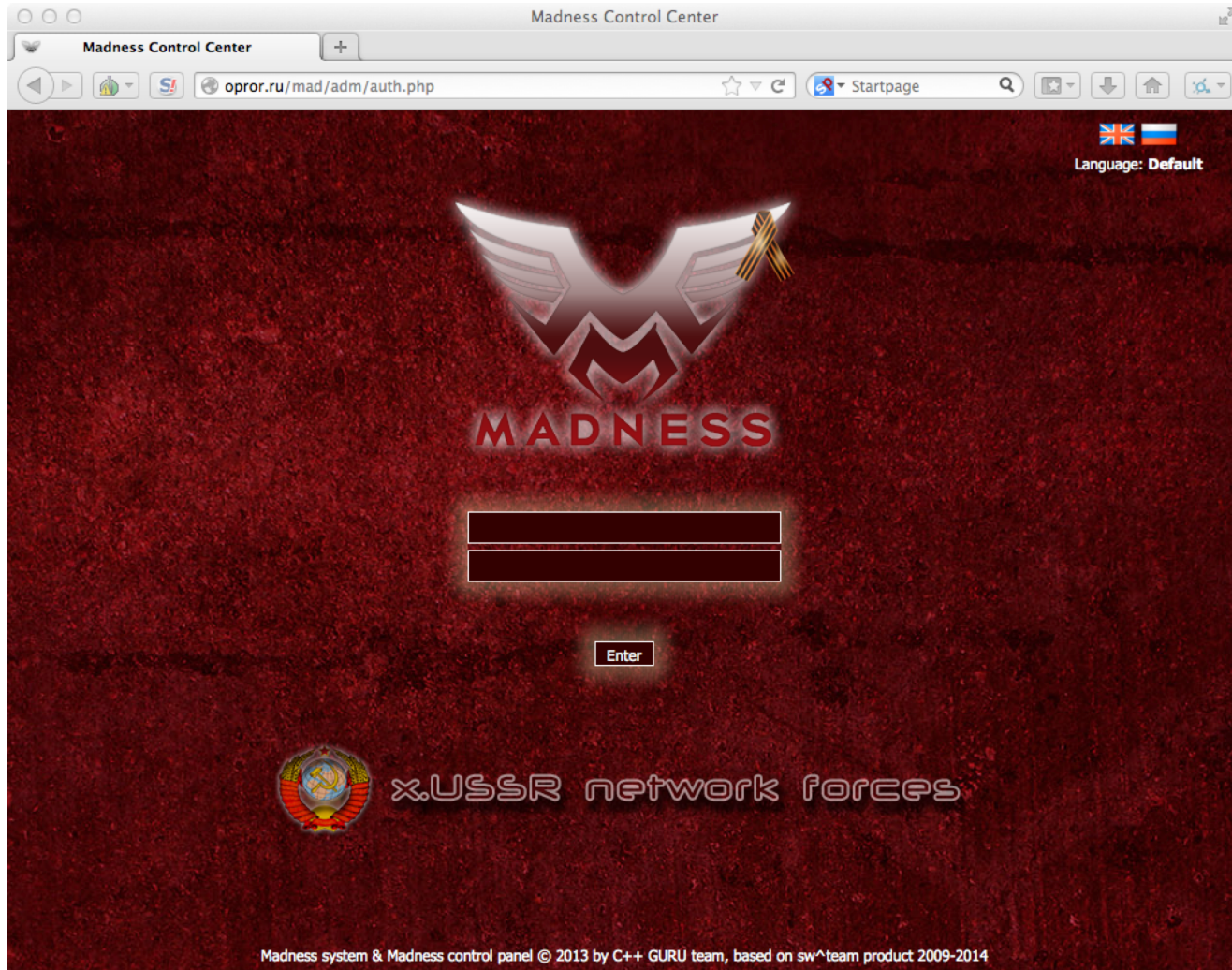
And here's more info, botnet Stelios (Moor):
81.177.6.12

81.177.6.12

Stelios – 81.177.6.12 – Opror



Stelios – Opror – Madness

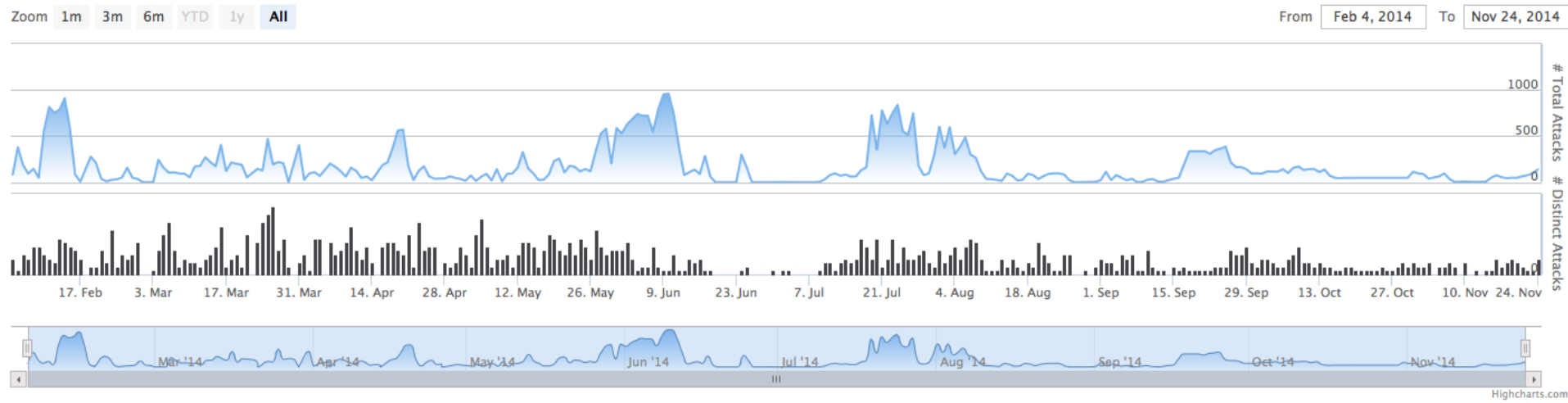


Stelios – Opror – BladeRunner

- First logged attack: February 4, 2014
- Last logged attack: November 25, 2014
- Distinct target domains: 509

Stelios – Opror – BladeRunner

BladeRunner Observed Attacks



Stelios – Opror – BladeRunner

www.groupanoo.com www.vottle.com

www.thetripp.net

www.pnc.com darkmoney.cc

ww.seitcheck.de/www-singleflirter-com/10959

www.treasury.pncbank.com

corepillar.com anti-aging-labs.com

apps.pnc.com it-masters.cc

valuta.so liberty24.net

waimai.meituan.com

ufolabs.net

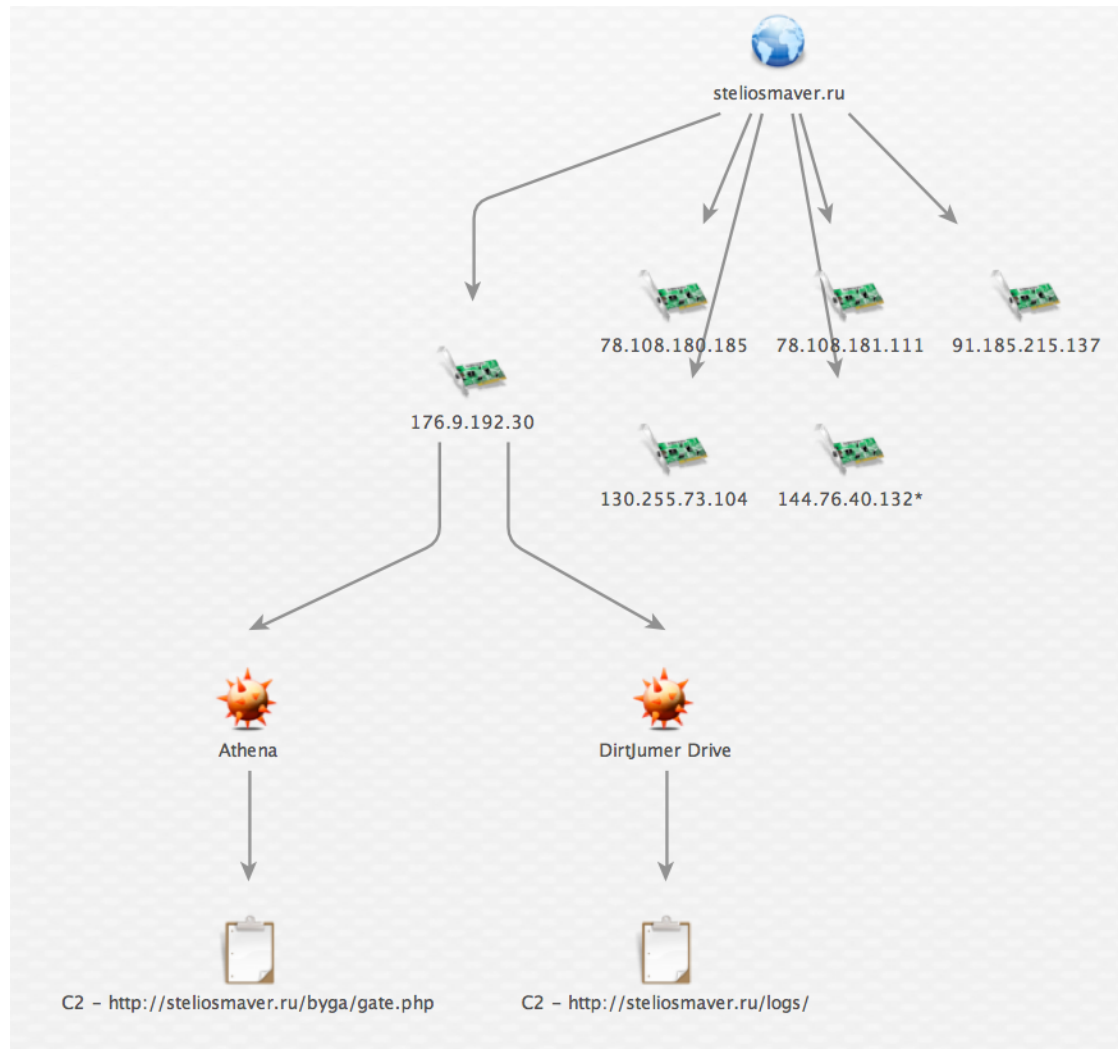
Stelios – Opror – BladeRunner?

www.groupanoo.com www.vottle.com
www.thetripp.net
www.pnc.com darkmoney.cc
ww.seitcheck.de/www-singleflirter-com/10959
www.treasury.pncbank.com
corepillar.com anti-aging-labs.com
apps.pnc.com it-masters.cc
valuta.so liberty24.net
waimai.meituan.com
ufolabs.net

Stelios – steliosmaver.ru

- Stelios
- Maverick
- Maverbest

Stelios – steliosmaver.ru



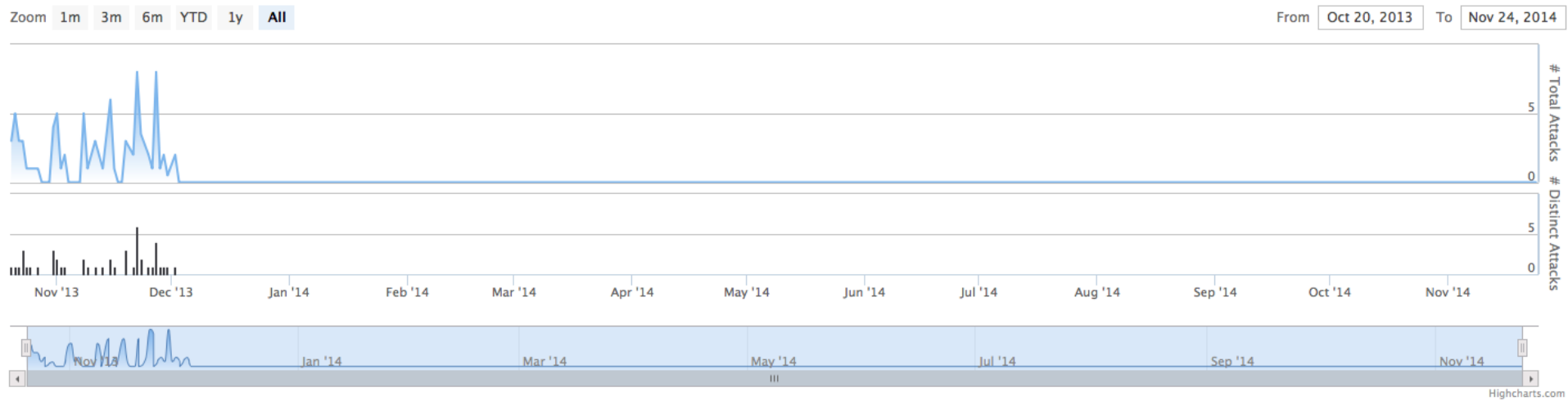
Stelios – steliosmaver.ru – BladeRunner

- First logged attack: October 20, 2013
- Last logged attack: December 1, 2013
- Distinct target domains: 41

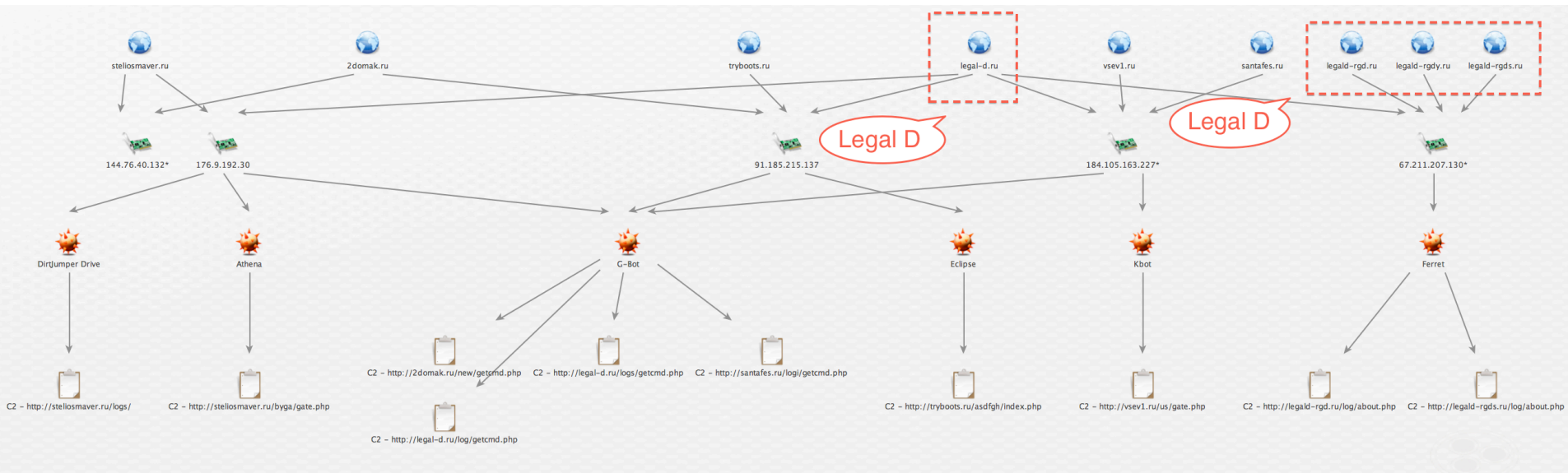


Stelios – steliosmaver.ru – BladeRunner

BladeRunner Observed Attacks



steliosmaver.ru – Legal D





Legal D, DDoS Esquire

Legal D – Ad

The screenshot shows a web browser window with a Google search bar at the top. Below the search bar is a translation widget. The main content is a forum thread. On the left, a user profile for 'legal D' is shown, with a red box around the name. The thread title is '[Recommend] № 1 DDOS SERVICE! DDOS SERVICE! SERVICES DDOS! "LEGAL DDOS (support)"'. Below the title, the text 'DDOS SERVICE' is followed by '«LEGAL DDOS» (Support)' in a red box. The thread content includes a definition of a DDoS attack and a list of terms of service.

Google

Translate From: Russian To: English View: Translation Original

19.10.2011, 21:11
legal D
Beginner
Posts: 13
Reputation: 0

[Recommend] № 1 DDOS SERVICE! DDOS SERVICE! SERVICES DDOS! "LEGAL DDOS (support)"

DDOS SERVICE
«LEGAL DDOS» (Support)

*DDoS-attack - the attack on the computer system in order to bring it to failure, ie, the creation of conditions in which the legitimate users of the system can not access the resources provided by the system.
A distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users.*

We provide service ddos attacks on your servers, sites, to verify the stability for this type of hacker attacks. Ddos attack we spend only to test your servers and websites for stability. There is no purpose in any way to block access to the server or site. Presumption, we believe that the purpose of the attack that you give - is your personal resource and you want it to check for immunity to this type of attack.

Terms of Service:

- Do not participate in schemes of blackmail, and other laws infringing schemes.
- Can refuse to accept the order to suit your personal wishes.

Resource that you give for the attack, we believe that it is your personal resource.

- For all wrongful acts responsibility rests solely with you, our goal is solely to help you configure your servers by testing.
- Considering that you will not violate the anonymity of working with us, for all actions, even if they are not completely clean, you will not suffer the responsibility)

Legal D – Paradise DDoS Bot

Google

Translate From: Russian To: English View: Translation Original

legal D Beginner

DDoS BoT [legal D recommends] sell / sale

Paradise DDoS BoT sell / sale

New Ddos Bot

For I had written a new DDoS bot. I test it actually made a list of what I would like to change and what to add. All my recommendations and suggestions have been made and now it is included in a part of my artillery, occupying today the first place among other windows bots.

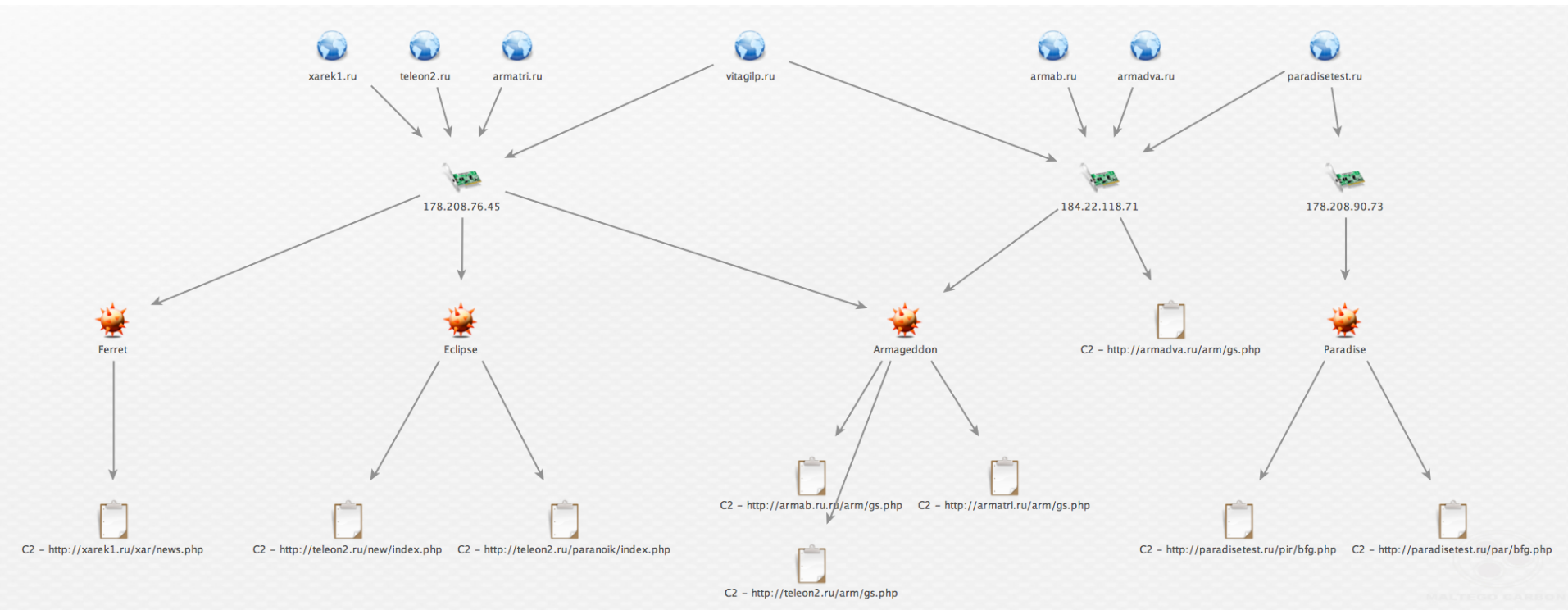
The advantages of the bot are:

- Clean coding, no component type synapse.
- Killmodul bots to destroy competitors.
- Drops the bot to different folders.
- The ability to adjust the attack
- Secrecy in the system, the bot does not load the processor and does not consume a lot of RAM, making it almost invisible in the system.
- Bot works on all versions of windows starting with 98 and ending with windows 8.
- Bot not need admin rights, it can work under yuzersky account.
- All rules send http request, all the headlines are as close to legitimate.
- The golden mean between performance and dolgozhitelnostyu bot.
- Easy and simple to manage.

Types of attacks:

- HTTP flood - effective against web servers such apache, nginx, attacks on port 80.
- HTTP DATA flood - effective for disabling Web sites that host post requests.
- TCP flood - effectively Scored for any open tcp ports.
- UDP flood - effective for clogged channel server and open udp any clogged ports.

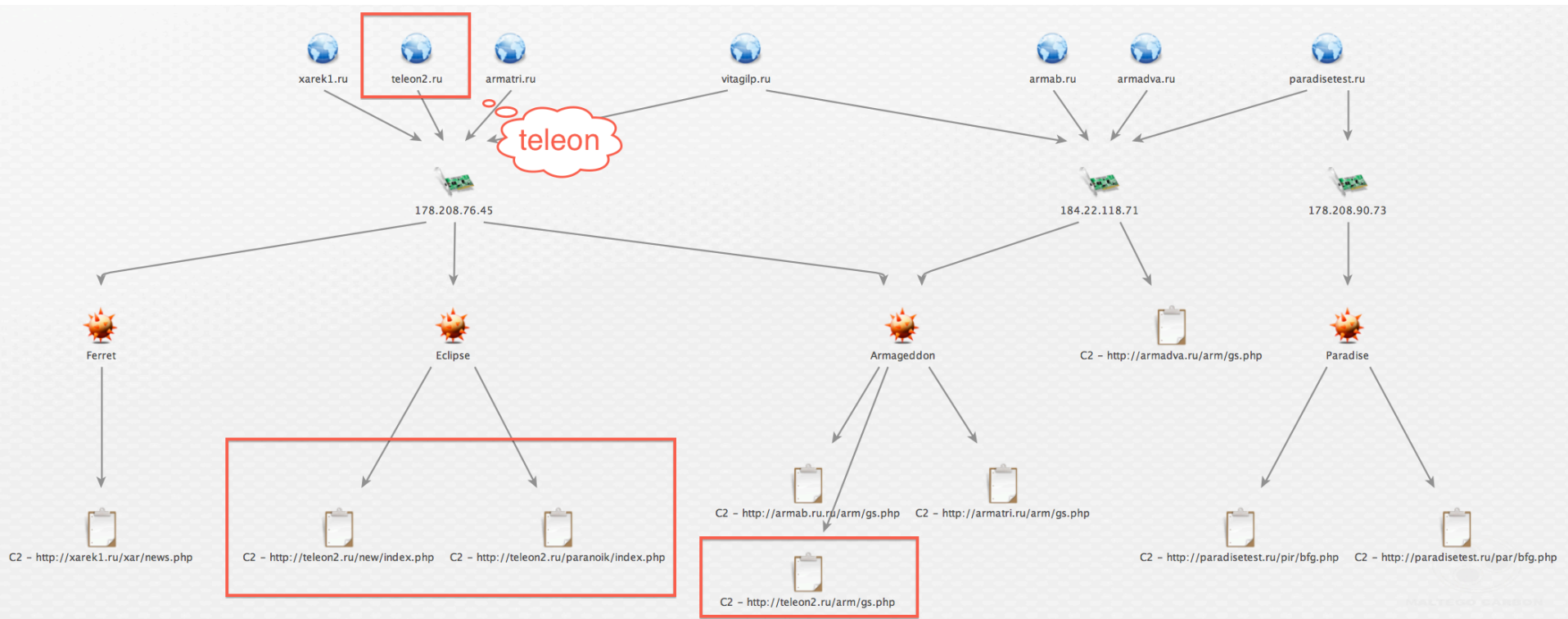
Legal D – paradisetest.ru



Legal D – paradisetest.ru

- DDoS malware
 - Paradise
 - Armageddon
 - Eclipse
 - Ferret
- teleon2.ru

Legal D – Teleon C2s



Legal D – Teleon C2s

legal D

15/08/2013, 11:58

Good afternoon.

You on the forum topic I created a proposal DDoS services and sales DDoS bot. DDoS services on the market work for about 2 years, it can be seen by registering for different hack forums. **August 2013** we passed inspection and lots of positive feedback.

<http://www.xaker.name/forvb/showthread.php?t=23657> my topic.

It left a man with the nickname review ramiss1980. Alerting everyone that it is better to me not to do business.

So that's the case. People are already 4 forum writes things like that. All his previous reviews have been removed, as he would accuse me of kidkov, saying that I was thrown and all warned not to work with me, in fact no reason to do so. As he himself says he DDoS complete zero, and not only in DDoS and general knowledge related to IT. This is the whole problem. The situation is such that the person I ordered DDoS services were all happy, and then he wanted to buy a DDoS bot. I stated in the topic of this work. I have prepared a set for him, helped to put on the server, all set up. But he had constant problems and questions. I gave the developer **icq 803077 == Legal D** but then again, the client has decided that he does not work bot and instaly not knock. As it turned out in the end, it was only because the panel was covered in the wrong for he was waiting for me and wrote to me that the bot is not working and so on I did not by itself can be given to a single customer all the time. By the end, he said that he would write my reputation. I suggest to him to solve everything peacefully, as it is suggest to the referee forum where he previously vylazhivat review, but it does not take this option. From all this we can conclude that a person simply have nothing to do, and all his problems were only due to the lack of knowledge in this area, and not wanting to buy them.

Recent posts that I am writing it

803077 (15:35:15 23/07/2013)

Roma in general, I gave you set the bot and he stood on the server. otstuk is myself prvoeryal, then it was not because I did not filled in the folder pane, and the boat was on the domains I have, create yourself panel reg py I'll give myself domains that used to manage them, or sign up I'll do a rebuild on them , zalyu test bots that used to saw and goodbye, and then I'm tired already this fuss!

803077 (13:35:21 30/07/2013)

Roma, you have me just take the time, what I did not know all this scam !!! I am willing to give you another 1 new bot that just went on sale in the gift that you were not offended !!!

legal D

Here's a piece of correspondence where a person to me too a couple of days fooling, and eventually okazyvaetsya he just did not clean the cache and the problem was this.

Roma (01:41:33 2/07/2013)

the old man. panel does not plow. urgently needed. I understand the case, but I'm already 3 weeks no one test. although the money put huge.

Roma (03:35:59 2/07/2013)

answer.

Roma (03:36:10 2/07/2013)

forces there. pad does not work .. (

Roma (03:36:17 2/07/2013)

not included.

teleon/log_in.php

Roma (12:45:50 2/07/2013)

Well, you do something? I had no strength. 3 weeks have not advanced a single step

803077 (21:16:07 2/07/2013)

link / teleon / log_in.php

803077 (21:16:10 2/07/2013)

here?

RosGosDos – Ad

DDoS Tools "RosGosDos" / ddos service / ddos service \

rosgosdos



Пользователь

Posts: 2
Reputation: 0
Offline

Post # 1 | 19/10/2014 9:42

"RosGosDos" - disable your website!

Попробовать снова

ICQ: 608013222

Contacts:

> ICQ: 608013222

> Jabber: rgd@xep.li

Guaranteed receiving orders from 8:00 to 24:00 GMT.

Prices for "DDoS" services:

> From \$ 50 night

Attention! In the price specified minimum price, it depends on the subject matter and purpose of protection!
% Discounts for large orders (from 2 sites or 2 days)!

Prices for additional services:

> Education DDoS + DDoS bot + Live + server cost of \$ 600

> Private DDoS software - prices from \$ 400

Conditions for our customers:

> Our service is almost 4 years old! Our experience even more!

> Monitoring of the goal!

> Use only the private and samopisny software

> We put any antiddos (qrator, cloudflare, cisco guard and date of birth)

RosGosDos – Details

- ICQ
 - 603226303
 - 608013222
 - 857837
- Jabber
 - rgd@xep.li
 - rgdsupport@exploit.im
 - rgd@jabber.fm
 - rgdcrypt@jabber.mu
- Website: buyddos.ru
- Email: rosgosdos@gmail.com

Legal D – RD1 Threat Actors

- Legald-rgd.ru
- Legald-rgds.ru
- Legald-rgdy.ru
- Legald-rgdi.ru
- Legald-rgdo.ru
- Legald-rgdq.ru
 - RosGosDos / rgd@ / rgdsupport@ / rgdcrypt@
- legal-d.ru
 - Stelios / Maverick / Maverbest → steliosmaver.ru
- Teleon → teleon[123].ru
- Xarek ? → xarek[123456].ru

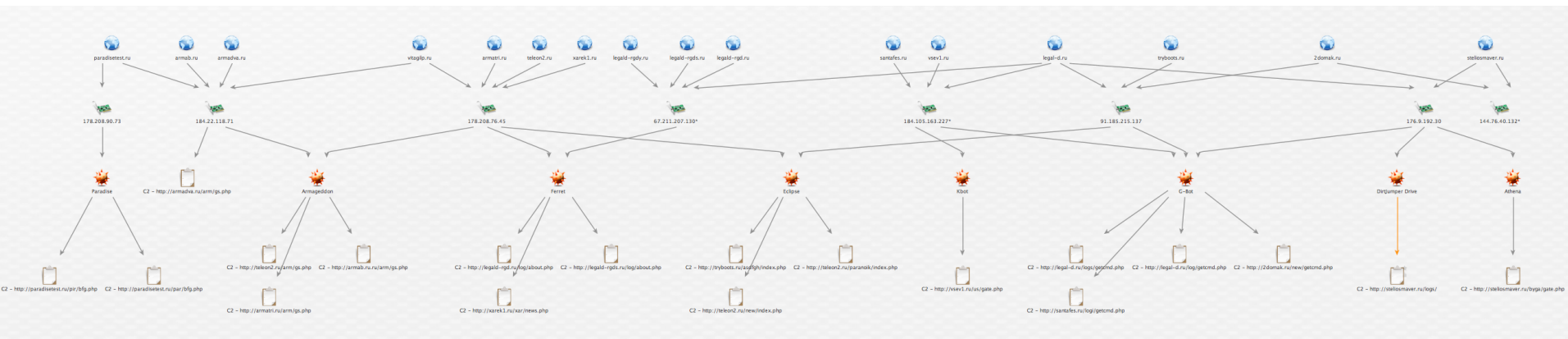
Legal D – DDoS Malware Families

- Ferret
- Eclipse
- Armageddon
- Paradise
- Athena
- DirtJumper Drive
- G-Bot

Legal D – Busy RD1 Threat Actor

- DDoSing service
- Coder/seller of Paradise bot
- DDoS hosting provider for the RD1?

Legal D – steliosmaver.ru



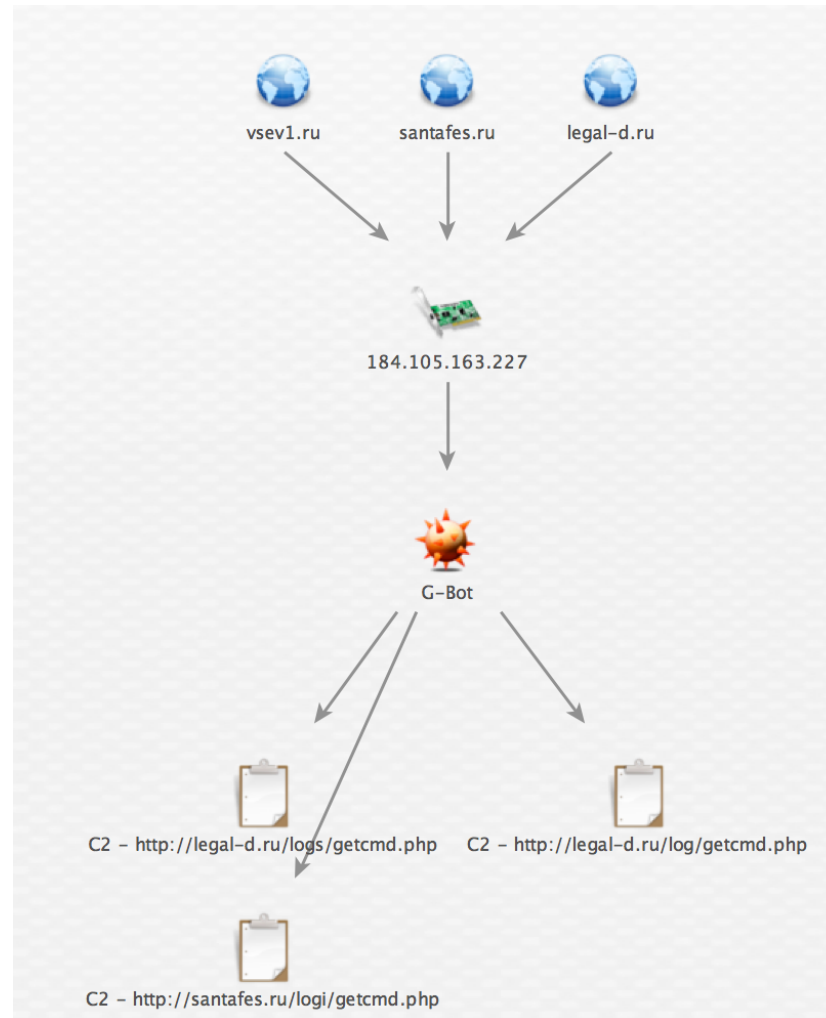
Ferret – legald-rgd[oq].ru – BladeRunner

- First logged attack: February 7, 2014
- Last logged attack: March 3, 2014
- Distinct target domains: 6

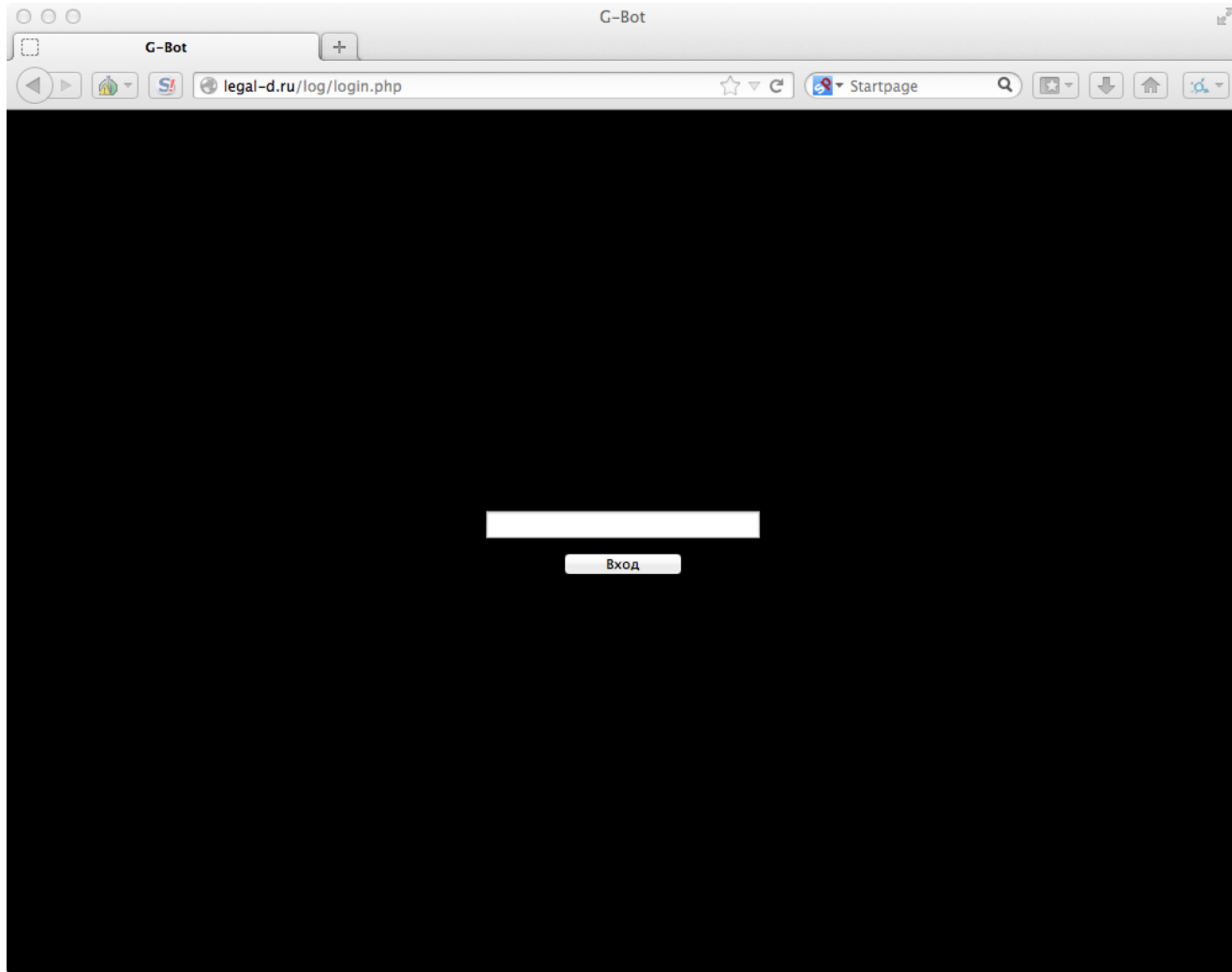


karpovka.net
www.poxodniki.ru
www.23kota.ru
vega.fuib.com
www.psychsocialis.ru

Legal D – Active Domains



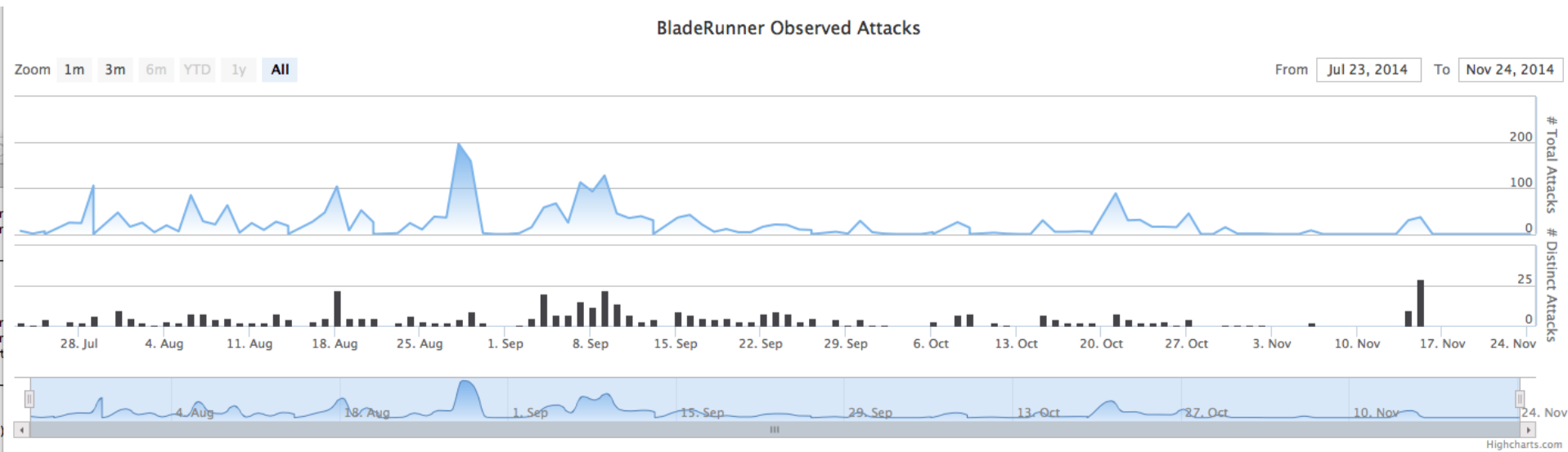
G-Bot – legal-d.ru/santafes.ru



G-Bot – legal-d.ru/santafes.ru – BladeRunner

- First logged attack: July 23, 2014
- Last logged attack: November 15, 2014
- Distinct target domains: 246

G-Bot – legal-d.ru/santafes.ru – BladeRunner

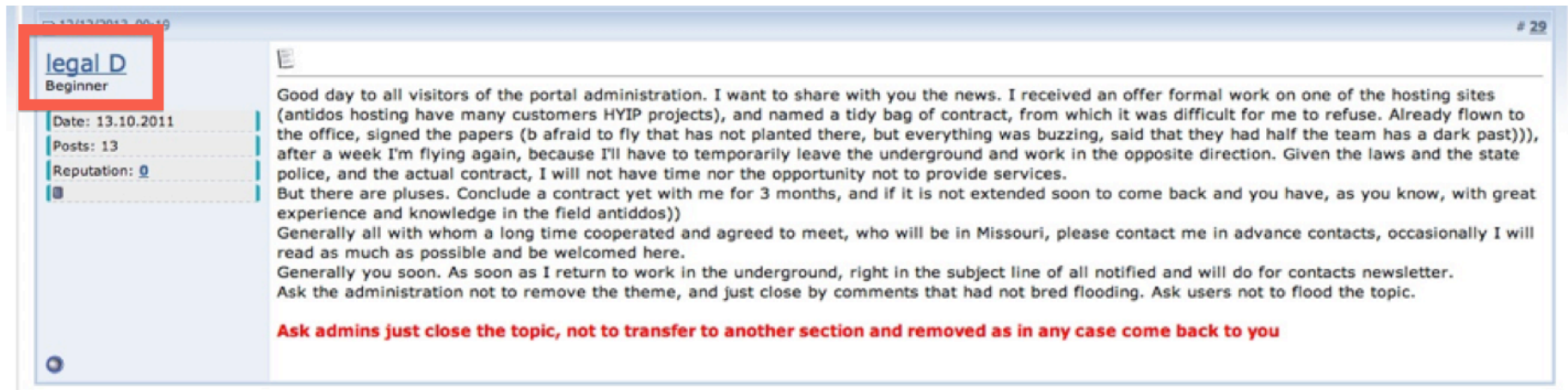


G-Bot – legal-d.ru/santafes.ru – BladeRunner

fxt fxtrendscam.co
sozdanie-prodvizhenie-saita.su autobazar.us
100dorog41.ru
www.0564.ua babyboom21.ru
zonahack.ru interuno.ru medik-centr.ru
fxtrend fireleads.ru
www.m-spravka.ru 1kr.ua
www.stanki.ru clickuk.org
mediklist.net my.morskoybank.com
fxtrendscam.com

Legal D – Leaves the RD1

- High-Yield Investment Program (HYIP)
 - This is a “legitimate business”



The screenshot shows a forum post interface. On the left, a user profile for 'legal D' is displayed, with the name highlighted by a red box. The profile includes the title 'Beginner', a date of '13.10.2011', 'Posts: 13', and 'Reputation: 0'. The main post area contains a message in Spanish, starting with 'Good day to all visitors of the portal administration...' and ending with a red instruction: 'Ask admins just close the topic, not to transfer to another section and removed as in any case come back to you'. The post is marked as #29 in the top right corner.

legal D
Beginner

Date: 13.10.2011
Posts: 13
Reputation: 0

Good day to all visitors of the portal administration. I want to share with you the news. I received an offer formal work on one of the hosting sites (antidos hosting have many customers HYIP projects), and named a tidy bag of contract, from which it was difficult for me to refuse. Already flown to the office, signed the papers (b afraid to fly that has not planted there, but everything was buzzing, said that they had half the team has a dark past))), after a week I'm flying again, because I'll have to temporarily leave the underground and work in the opposite direction. Given the laws and the state police, and the actual contract, I will not have time nor the opportunity not to provide services. But there are pluses. Conclude a contract yet with me for 3 months, and if it is not extended soon to come back and you have, as you know, with great experience and knowledge in the field antidos)) Generally all with whom a long time cooperated and agreed to meet, who will be in Missouri, please contact me in advance contacts, occasionally I will read as much as possible and be welcomed here. Generally you soon. As soon as I return to work in the underground, right in the subject line of all notified and will do for contacts newsletter. Ask the administration not to remove the theme, and just close by comments that had not bred flooding. Ask users not to flood the topic.

Ask admins just close the topic, not to transfer to another section and removed as in any case come back to you



Are You There AreYouAreDo

AreYouAreDo – RD1 Connection

Quote:

Posted by **Log with Aredia:**

AreYouAreDo (16:31:48 24/09/2013)

there was a different story

AreYouAreDo (16:32:09 24/09/2013)

Moor site and site Metakhim... my friends

AreYouAreDo (16:32:09 24/09/2013)

I saw how

AreYouAreDo (16:32:15 24/09/2013)

asked to remove.

AreYouAreDo (16:32:22 24/09/2013)

I was told that vouched for him Metakhim

AreYouAreDo (16:32:25 24/09/2013)

I have to Metachim

AreYouAreDo (16:32:38 24/09/2013)

Metakhim said that the problems are not necessary and therefore off the Moor

AreYouAreDo (16:32:42 24/09/2013)

and turned off

Krabeg (21:06:39 24/09/2013)

*> Metakhim said that the problems are not necessary and therefore off the Moor
ie Metakhim ordered anti-ddos and parallel Moor mutil?*

AreYouAreDo (21:06:51 24/09/2013)



yes

AreYouAreDo (21:07:09 24/09/2013)

he ordered protection for yourself

AreYouAreDo


AreYouAreDo – Ad



Translate

From: Russian To: English

View: Translation Original



AREYOUAREDO TEAM

10.04.2014 conduct an effective attack on the projects featured on: **DDoS-guard, Qrator, Cloudflare, etc.** *More in secure communications.*


Home

Services

Terms

FAQ

Order



Оператор Online
Начать диалог
БЕЗОПАСНАЯ СВЯЗЬ

14:00 - 02:00 MSK

ICQ: 522899
backup link

Good day.

We offer services in the field of information security on the Internet.

Our main specialization is the organization of network-based attacks on the information infrastructure of your enemies, as well as protecting your information infrastructure from such attacks.

Why choose us?

- Professionalism. We work only with their own technologies and developments;
- Experience. Almost three years, we are constantly improving our technology in this field and apply new advanced solutions;
- Quality. Our experience allows us to exploit different vulnerabilities to a server, which makes the attack in our execution as efficient as possible;
- Power. Thanks to the continuous improvement of our technology, we have a huge combat capability;
- Domestic resource. Bypass in foreign countries;
- Anonymity. You can be sure that the data on your order will not get to the third parties;
- Decency. Adequate conditions to return the funds;
- See for yourself. Carry out an attack on the **free** test Web-server;

Trust the professionals!

DDoS attack

Day	from \$ 50 *
Week	from \$ 300 *
Month	from \$ 1000 *

Hacking Site

from \$ 500 *

* - For each site / server is assessed individually

Hack-mail

Individuals	200 \$
Corporate	from \$ 500

Protection against DDoS (cloudy proxying)

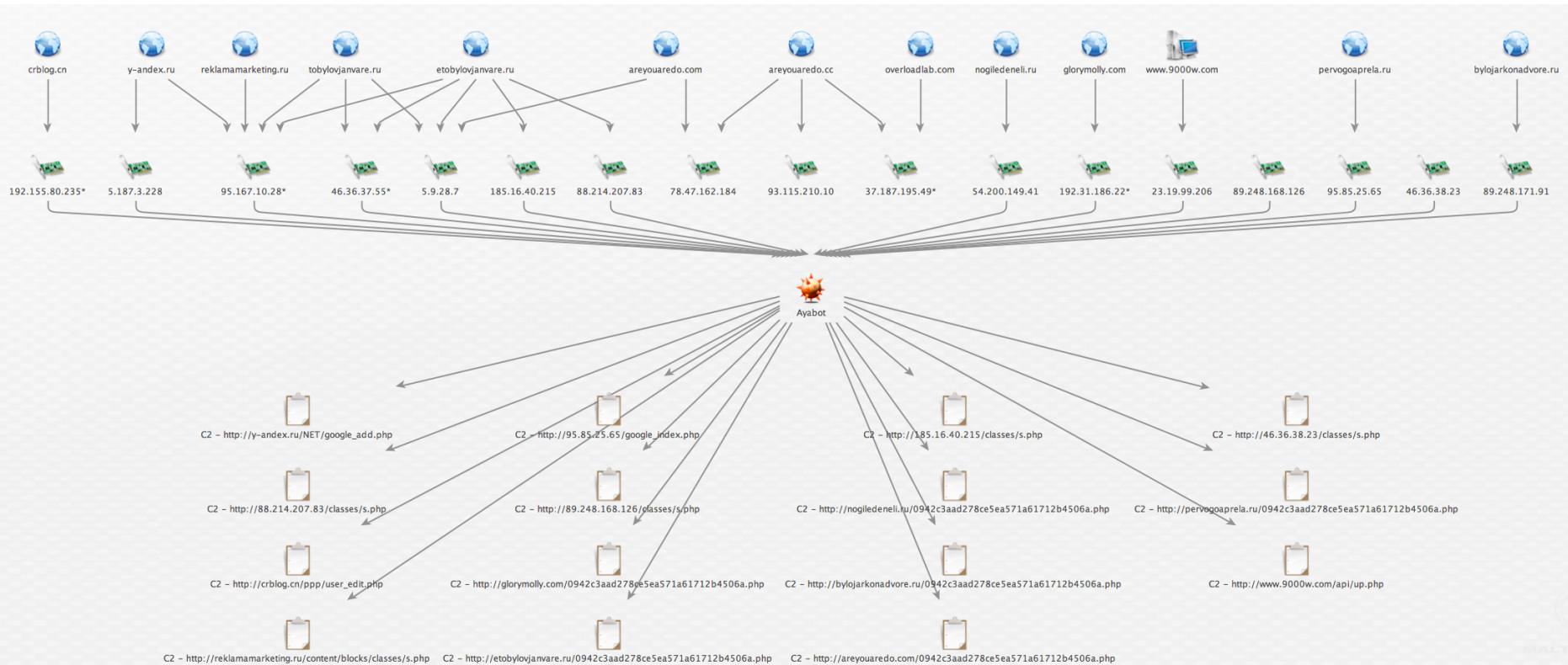
Day	from \$ 35 *
Month	from \$ 150 *

* - Depending on the characteristics and complexity of the attack, the cost of security services may vary

мы принимаем
WebMoney

мы принимаем
Яндекс деньги

AreYouAreDo – Infrastructure



AreYouAreDo – Ayabot

- Proprietary DDoS bot
- AreYouAreDo → Ayabot

AreYouAreDo – Ayabot – BladeRunner

- First logged attack: August 22, 2013
- Last logged attack: June 19, 2014*
- Distinct target domains: 31*

AreYouAreDo – Ayabot – BladeRunner

www.igrafan.com
rugrad.eu
zar-par.ru **www.ddos-service.cc**
qna.center softrok-k.ru
it-masters.cc xi-xi.me **www.bitermo.ru**
goles-ahy.info
pizzarich.ru www.pilguni.ru
forum.ramgk.com **week02.ru**
na-raione.com bratish.info
vse.rv.ua tmsauto.ru

AreYouAreDo – Impromptu Interview

19:55:03 Me : where does the name "Aya" come from? is it just you behind the bot or is AreYouAreDo a team?

19:55:31 AreYouAreDo: AreYouAreDo

20:01:15 Me : how long have you been in active in the hacking / DDoS scene ?

20:02:19 AreYouAreDo: couple of years

20:12:12 Me : how do you distribute it ? exploit kit, social engineering, spam, Trojan Download networks ?

20:14:11 AreYouAreDo: its distributes it self. you did not noticed?

20:16:24 AreYouAreDo: well, if you dig, you find out

20:17:21 AreYouAreDo: exploits are very expensive

20:38:32 Me : how do you handling money ? without getting traced back to you, etc. ?

20:40:01 AreYouAreDo: well , ill say not clear true, but enough to understand. online game currencies

20:40:19 Me : hmm.. any bitcoin stuff or is that not secure enough ?

20:40:53 AreYouAreDo: bitcoin is not popular for russian customers

AreYouAreDo – Overloadlab

The screenshot shows a web browser window with the URL overloadlab.com. The page features the Overloadlab logo and the tagline "High load and DDoS testing service." Below this, there are four pricing plans: Hour, Day, Week, and Month. Each plan includes a price, an "ORDER NOW" button, and a list of features. The Day plan is highlighted as the selected option.

Hour	Day	Week	Month
\$15*	\$70*	\$400*	\$1400*
ORDER NOW	ORDER NOW	ORDER NOW	ORDER NOW
Moneyback guarantee	Moneyback guarantee	Moneyback guarantee	Moneyback guarantee
Basic support	Basic support	Professional support	Professional support
-	Free test	Free test	Free test
-	24/7 site monitoring	24/7 site monitoring	24/7 site monitoring

* - basic load cost, prices may vary depending on the required load.

ABOUT US

We provide high load testing services for network resources.

For three years, we are engaged in research of high loads, especially the DDoS-attacks. We have a distributed network of servers designed to simulate high load's incidents.

Pre-installed software in our network allows you to simulate these types of attacks as HTTP (post), HTTP (browser), SYN,


Feedbacks

Vladimir, web-developer
Kept site was down for a while, in spite of all attempts to defend himself. Truly quality testing!



Storm Team / S-Team / Huntsman

Storm Team – Ad



huntsman
Moderator

Posts:	35
Sympathy:	4
Credit:	8
Gender:	Male

DDoS order, as a means of decommissioning of the competing parties has become increasingly popular. The very notion of **DDoS** comes from abbreviary DDos meaning Distributed Denial of Service- distributed denial of service.

"Anatomy" DDoS attack in most instances consists of the use of different vulnerabilities processing method request SYN, mainly Internet Protocol TCP / IP, using procs servers complicates The identification Ip.

In quickening amount DDoS attacks on various types of servers recently played and raspostrenenie Windows NT / XP versions of based the last. It is known that the Windows operating system is vulnerable to DDoS attacker absolute majority, to use simple tools (flood).

Also since it is worth noting that the attack on a particular server dostotochno proved beneficial as well. Provider to protect against attack high load forced to deploy additional capacity (input filters) for spot filtering garbage traffic. All this and so heats a large enough demand for such services.

We are a group of IT professionals specializing in providing. We organize all kinds of actually DDoS attacks (ICMP-flood, SYN-flooding, or **DDoS attacks** on the DNS-server, etc.) using the most advanced software used in the industry.

The prices of our services:

- 1 frequency from 10 \$
- 24 chasa- from \$ 70
- Week - from \$ 350
- Month - from \$ 1300

Attention: Prices on medium difficulty ...

We accept:

- Webmoney
- Yandex Money
- QIWI + 6%
- PM + 6%

Attention: Overlooking the payment can be negotiated separately

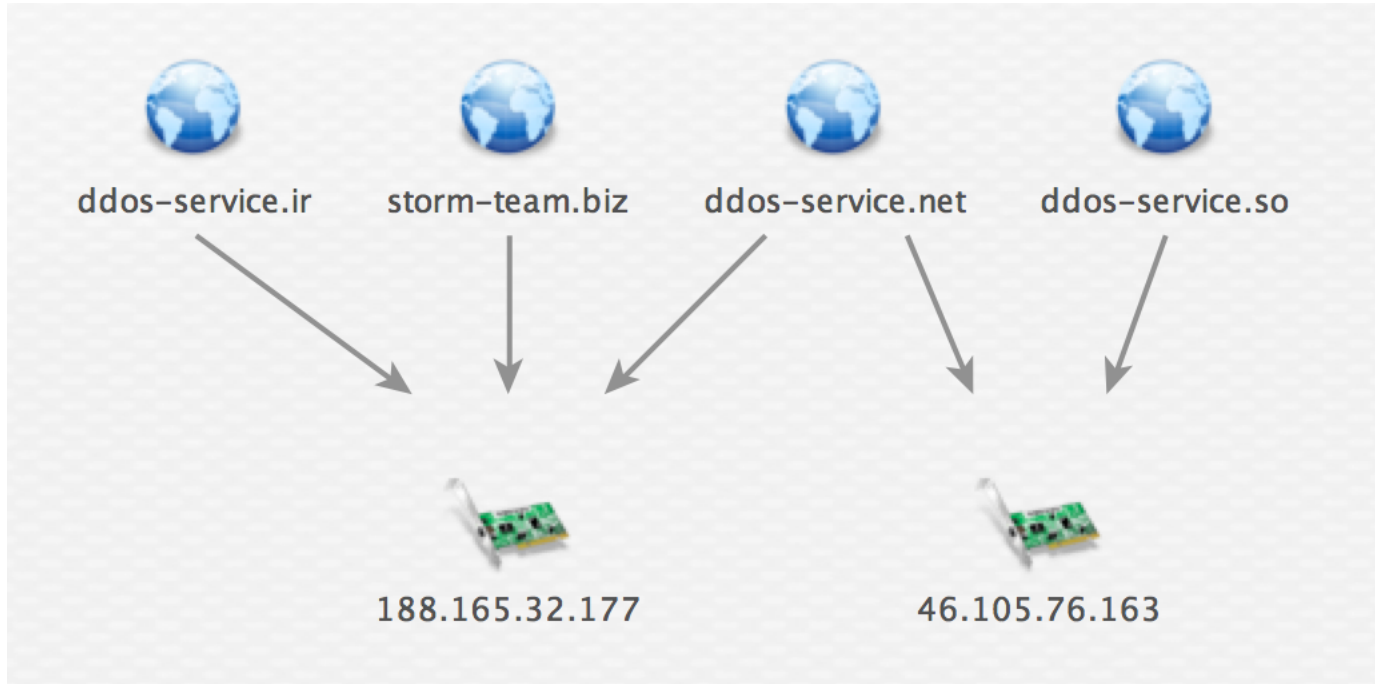
Jabber: **s-team@logov.net**
ICQ: 762760
skype: storm-team502

Last Edit: Κυ66οτα в 15:58

Storm Team – Details

- Websites
 - ddos-service.net
 - ddos-service.so
 - ddos-service.ir
 - storm-team.biz
- Jabber: s-team@l0g0v.net
- ICQ: 762760
- Twitter: [@DDOSTeam](https://twitter.com/DDOSTeam)

Storm Team – Front-end Infrastructure



Storm Team – Accidental DDoS Targets

06/12/2014, 10:07

Krabeg ▾
Beginner
Avatar Krabeg

Krabeg offline
Join Date: 17-06-2012
Posts: 8
Reputation: 0
ICQ: 4550085

Storm Team (icq 41111181) - Reseller

The response message on the board **huntzman'a** shopworld.biz (admin which he resigned):
<http://shopworld.biz/showpost.php?p=11114&postcount=75>

Explicit resellerstvo by **Storm Team**:

Quote:

Message from **(Conversation on ICQ)**
Storm Team (icq 41111181)

Storm Team (09:59:42 12/06/2014)
You have added

Storm Team (09:59:42 12/06/2014)
cookie

Krabeg (10:01:53 12/06/2014)
listen

Storm Team (10:02:58 12/06/2014)
ataukesh than crab *(from the message I knew immediately what will be discussed)*

Krabeg (10:03:29 12/06/2014)
Well, in many ways, but what?

Storm Team (10:03:38 12/06/2014)
Well

Storm Team (10:03:47 12/06/2014)
yukoz you put

Storm Team (10:03:50 12/06/2014)
at yukoz conductive, a

Storm Team (10:05:23 12/06/2014)
schA

Storm Team (10:05:50 12/06/2014)
energydiet24.ru
energydiets.ru
energydiet-hd.ru
(Stupidly decided to throw me your orders, well, of course, because nothing hunstmenu DDoS)

Storm Team (10:05:56 12/06/2014)
Try any valnut

Storm Team (10:18:23 12/06/2014)
?

ot simple

Storm Team

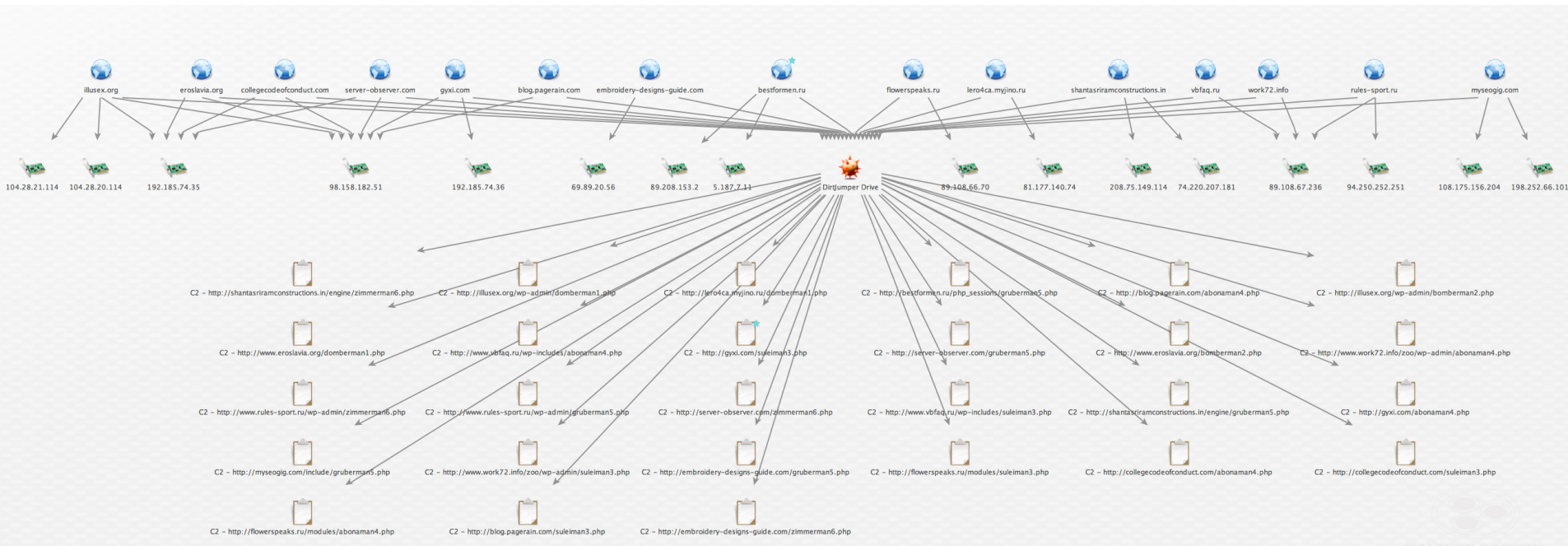
June 12, 2014

Accidental paste of DDoS targets

Storm Team – Accidental DDoS Targets

- First logged attack: June 12, 2014
- Last logged attack: June 21, 2014
- Distinct C2 hosts: 15

Storm Team – Back-end Infrastructure



Storm Team – Back-end Infrastructure

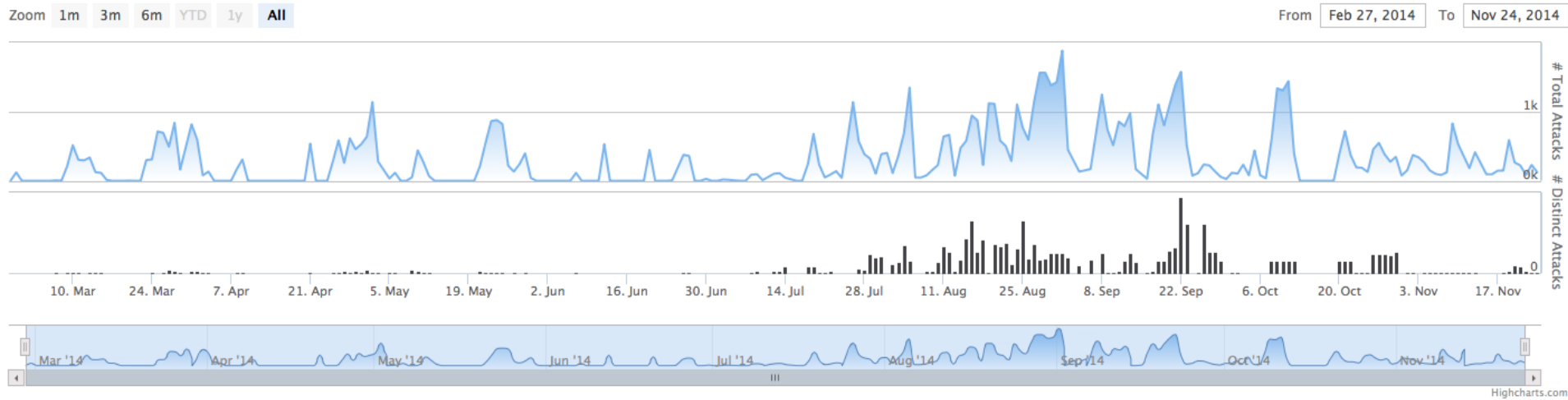
- 33 C2s lead to DirtJumper Drives
- Shared IPs
- URL filenames
 - abonaman4.php (6)
 - chtogde1.php (5)
 - zimmerman6.php (4)
 - snowthread.php (4)
 - domberman1.php (3)
 - gruberman5.php (6)
 - suleiman3.php (6)
 - bomberman2.php (2)

Storm Team – Back-end – BladeRunner

- First logged attack: February 13, 2014
- Last logged attack: November 25, 2014
- Distinct target domains: 1535

Storm Team – Back-end – BladeRunner

BladeRunner Observed Attacks



Storm Team – Back-end – BladeRunner

diplom-garant.com
roxen.ru qiwi-kapital.ru adlerleto.ru
promo-s.pro
ra-opora.ru diplom-vo.com www.kupit-diplom-vysshee.ru
hobbygames.ru fmsshop.biz
oldcvety.com oboi.com rapo.ru
outlawing.net batterygator.ru www.mskpresent.ru
gama-gama.ru artm.pro design4free.org mediklist.net
iq-msk.com
topright.ru www.redcube.ru surva.ru
litsa.su
2ndfl-novosibirsk.com bankspravok.com
podarihit.ru open-fin.ru www.ibatt.ru
ra-mart.com www.diplomru.com besttvseries.ru




Chef the RD1 Troll

Chef – Ad

01/23/2013 15:13

chef

Super Moderator




Last Activity:
3 minute (s) ago


Register: 07.08.2009

Posts: 614

Thanked total: 761
for this post: 0

 2070072

order DDoS, DDoS attack on the site, DDoS services, buy ddos



DDOS SERVICE

«PRIVATE DDOS»

Greetings to all, we are glad to offer you quality DDoS services for a reasonable price. If you have a business rivals or someone you just offended, then take it out on the website is a one of the best solutions.

As a result of the attacks, the site of your competitor will not play in your specified period of time (from several hours to several weeks, and so on) Thus, your abuser, the competitor will spend a lot of time and nerves lose attendance and profits.

Used his botnet from a huge number of bots, located throughout the world and, therefore, are in different time zones.

This allows you to keep the primary part of the bots in online-mode.

Unable to close the block DDOS attacks in the country.

Supports all types of attacks (ICMP SYN / ACK UDP HTTP Flood, etc.)

The average price - \$ 100 per night (price may be constantly changing depending on the project)

Minimum order value - \$ 50

Working with large projects! Customers for long terms - discount.

We work on 100% prepayment

Provide test services within 10 minutes free. (Suspicious persons test fee - \$ 5)

Interested serious people interested in long term cooperation.

When ordering, use this form of treatment: "The purpose, the period when the start is needed, I have a reputation out there that you are advised to something in the budget is limited to such a wallet is not limited to the main result ".If you anything is not clear in the description of our themes, or want to clarify any point, please contact us and we will explain everything to you.

On the organization to handle DDoS

ICQ: 2070072 (OTR)

Jabber: [\[Links visible only to registered users.](#) [Зарегистрироваться...](#)] **(OTR)**

ARBOR[®]
NETWORKS

87

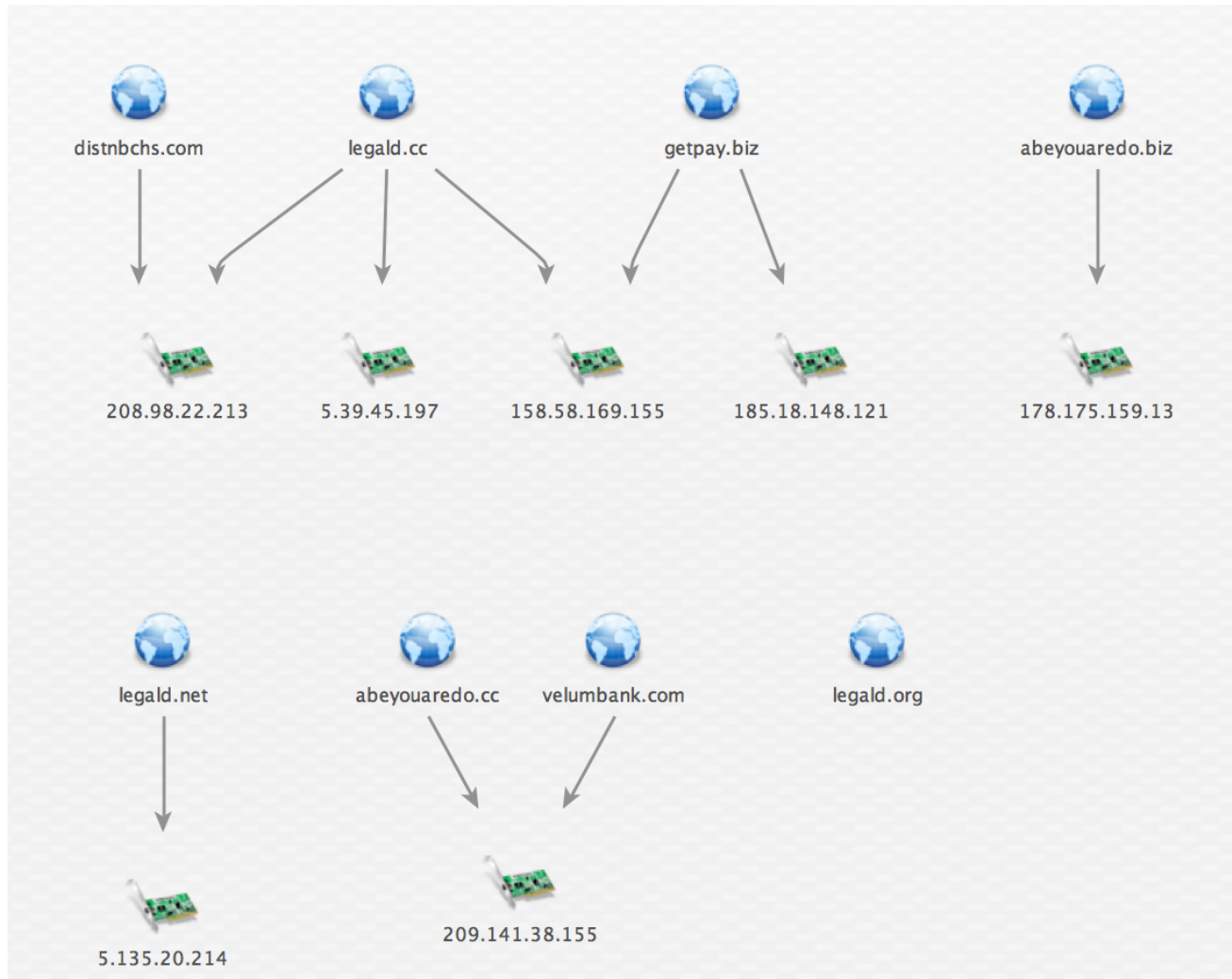
Chef – Details

- Booter: PRIVATE DDOS
- ICQ
 - 2070072
 - 403031
- Jabber
 - privateddos@exploit.im
 - legal.d@0nl1ne.at
 - twisted_ddos@0nl1ne.at

Chef – Booter Websites

- <http://legald.net/> → Legal D
- <http://legald.cc/> → Legal D
- <http://legald.org/> → Legal D
- <http://abeyouaredo.biz> → AreYouAreDo
- <http://abeyouaredo.cc> → AreYouAreDo

Chef – Booter Infrastructure




Chef – Ferret DDoS Bot?

08/05/2013, 01:54

8

chef

Super Moderator




Last Activity:
19 minute (s) ago

Register: 07.08.2009

Posts: 614


Thanked total: 761
for this post: 0

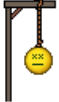
 2070072

On


Line

Agrees with hdsckr, the bot has turned out not bad 🤖

**НА ФОРУМЕ НЕ СРАТЬ!**
Администрация

All I beg to express discontent in the form of suicide


More than 5 similar messages about - Ban on the month, more than 10 - Ban for life 🤖



ARBOR[®]
NETWORKS

91

Copyleft

Copyleft – Ad

01/22/2013, 20:45

Thread Display Options

1

Copyleft

Windows v.3.51 (NT)

Last Activity:
1 week ago

Register: 05.01.2013

Posts: 127

Thanked total: 223
for this post: 0

443666329

copyleft@xep.li

[Copi] Team DDoS Service

We offer services in DDoS attacks.



Low prices:

Hour from \$ 7 // works from 5-10 hours
From \$ 70 per night
Week from \$ 400

In the case of non-fulfillment of the order is possible manibek for the remaining time.

Before ordering a test feature hotel 5-10 minutes

Discounts are available!
Discounts from 7 days to 10, 15 and Beyond "further more"

Ability to work for long periods of time, with individual quotation!
Accept to order almost any sites, sites with antiddos!

The test is successful

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

<http://fuckav.ru/showthread.php?t=14338>

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

[Links visible only to registered users. Зарегистрироваться...]

CopiLeft – Details

- ICQ: 443666329
- Jabber
 - copileft@xep.li
 - copileft@exploit.im
- Email: c0p1l3ft@rambler.ru

CopiLeft – copileft.myjino.ru

Код:

```
[Copi]Left долг 449$ (17:38:23 3/01/2013)
если там еще надо будет пополнить скажи друг)

-
[Copi]Left долг 449$ (17:38:32 3/01/2013)
я мизерный пополнил

-
iSupport (17:38:45 3/01/2013)
ну тут уж тебе хостер емейл пришлет

-
iSupport (17:38:50 3/01/2013)
когда бабл кончатся...
http://copileft.myjino.ru/opt/adm

-
iSupport (17:39:25 3/01/2013)
http://copileft.myjino.ru/opt/adm

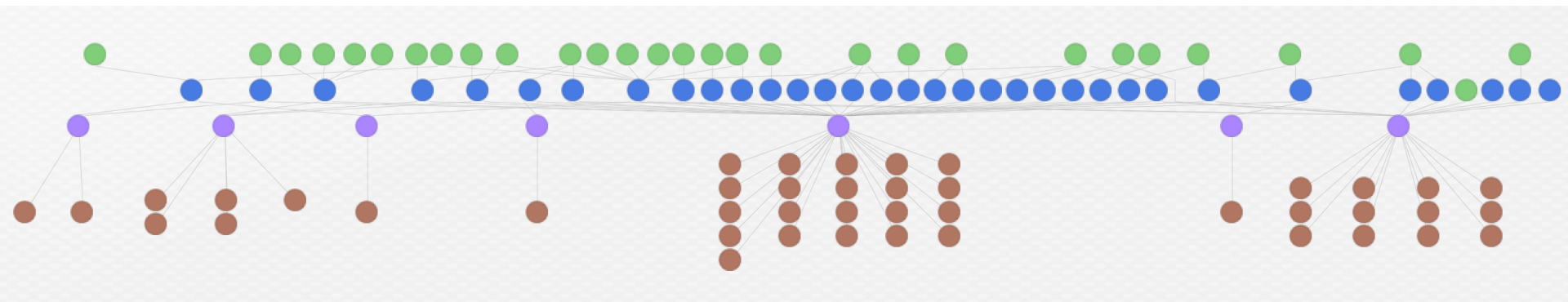
-
iSupport (17:39:31 3/01/2013)
optima/optima

-
[Copi]Left долг 449$ (17:39:35 3/01/2013)
там я вообще не понял как и что))) вот я пополнил на 160..там п

-
iSupport (17:40:07 3/01/2013)
там я подключил несколько нужных услуг

-
iSupport (17:40:25 3/01/2013)
и это немного увеличило сумму списываемую ежесуточно
```

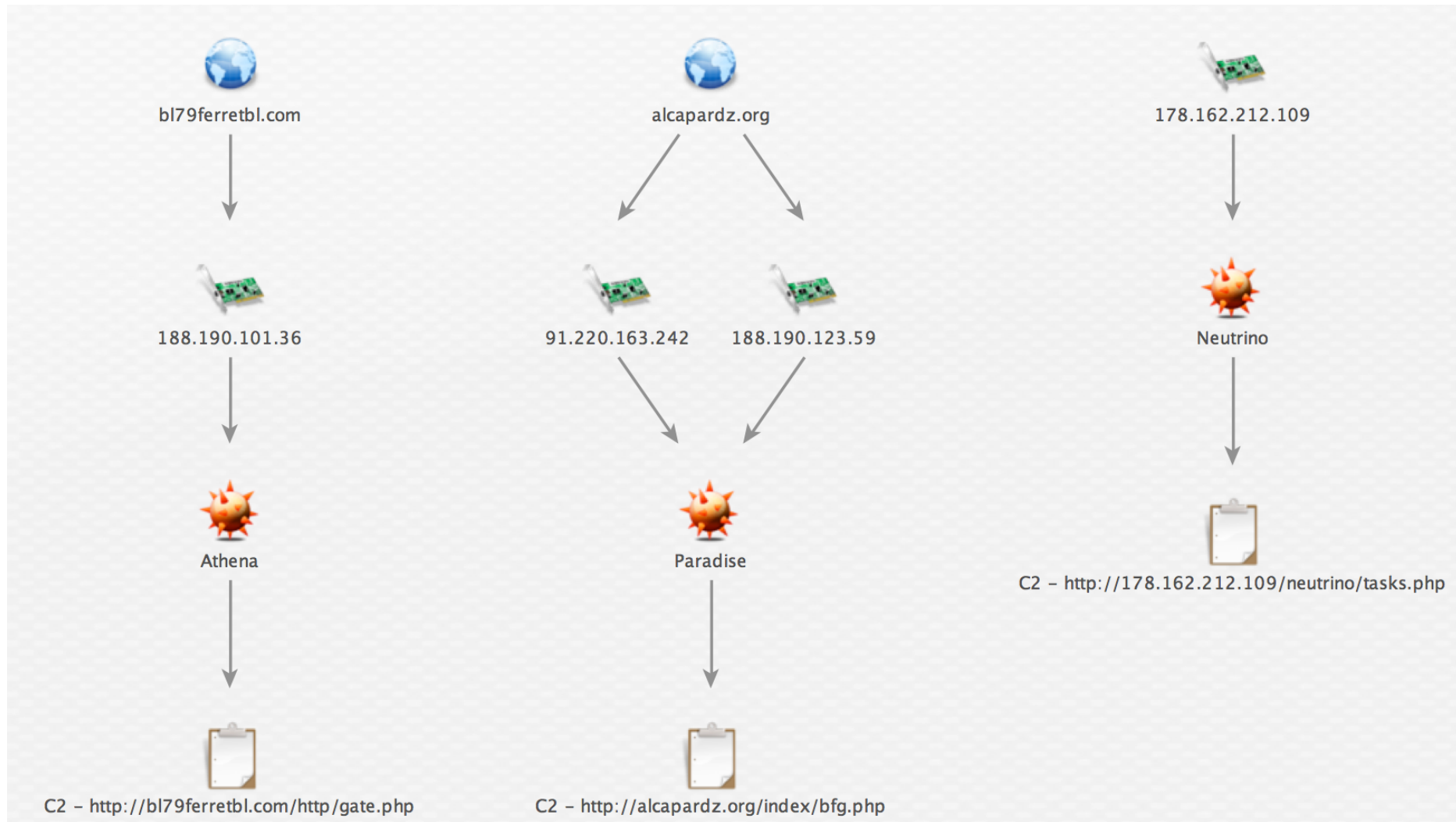
Copyleft – c0p1l3ft@rambler.ru



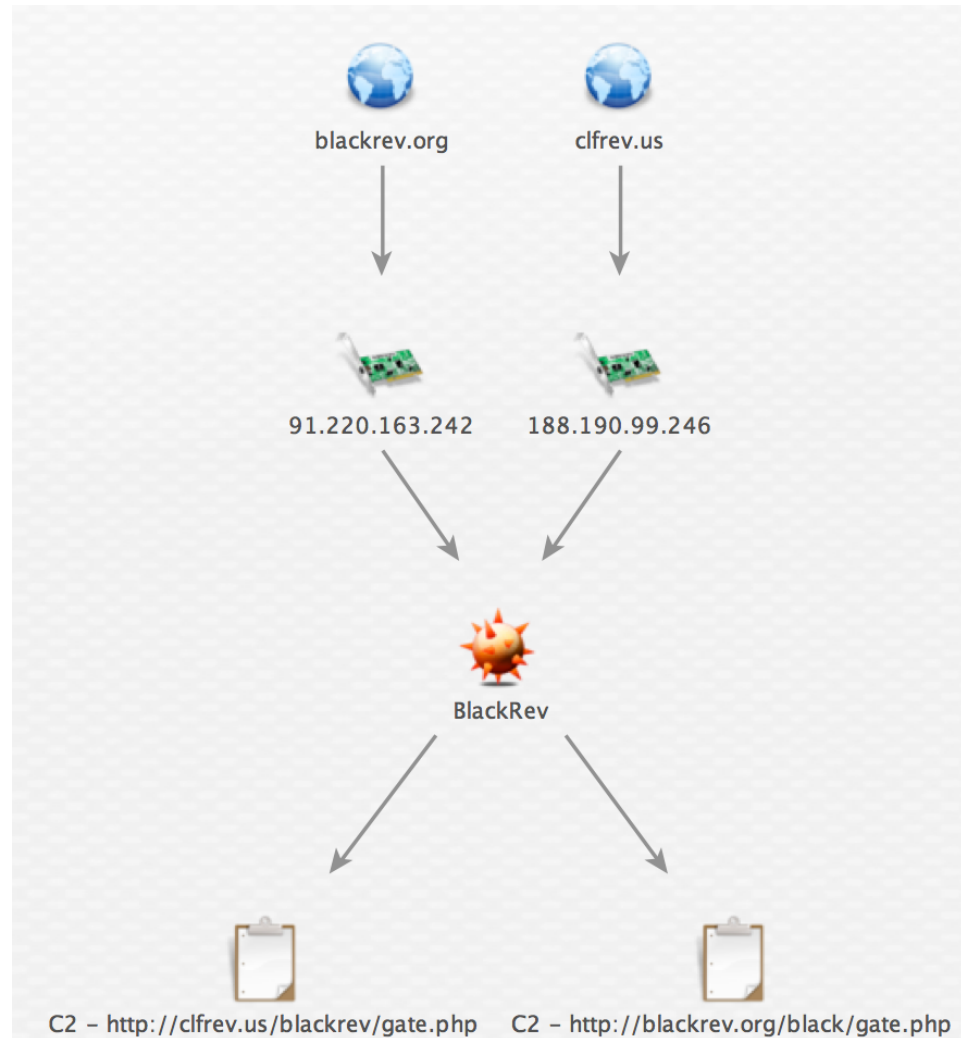
Copyleft – DDoS Malware Families

- Paradise
- Neutrino
- Athena
- BlackRev
- Ferret
- Madness
- DirtJumper Drive

Copyleft – Paradise / Athena / Neutrino



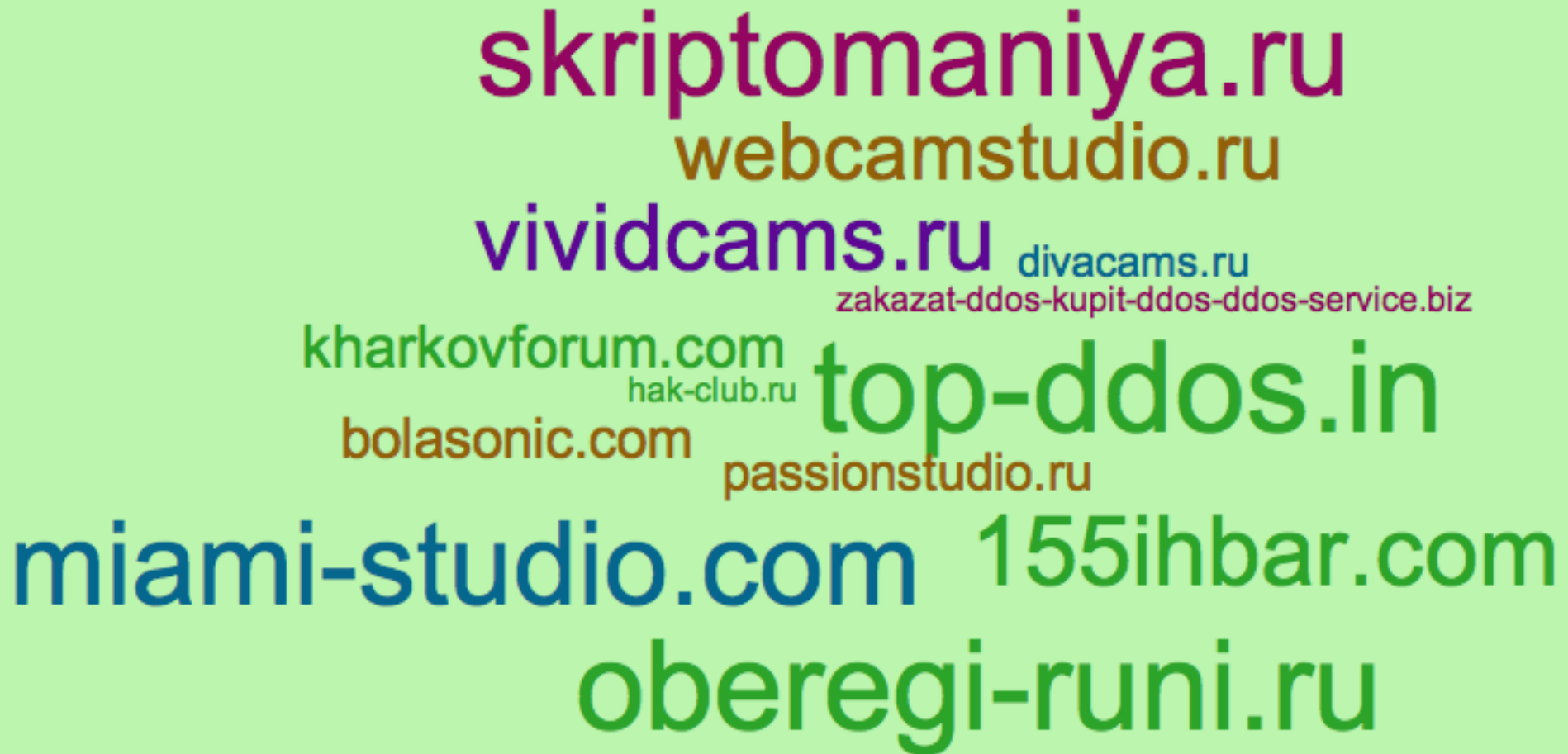
Copyleft – BlackRev



Copyleft – BlackRev – BladeRunner

- First logged attack: April 25, 2013
- Last logged attack: May 6, 2013
- Distinct target domains: 43

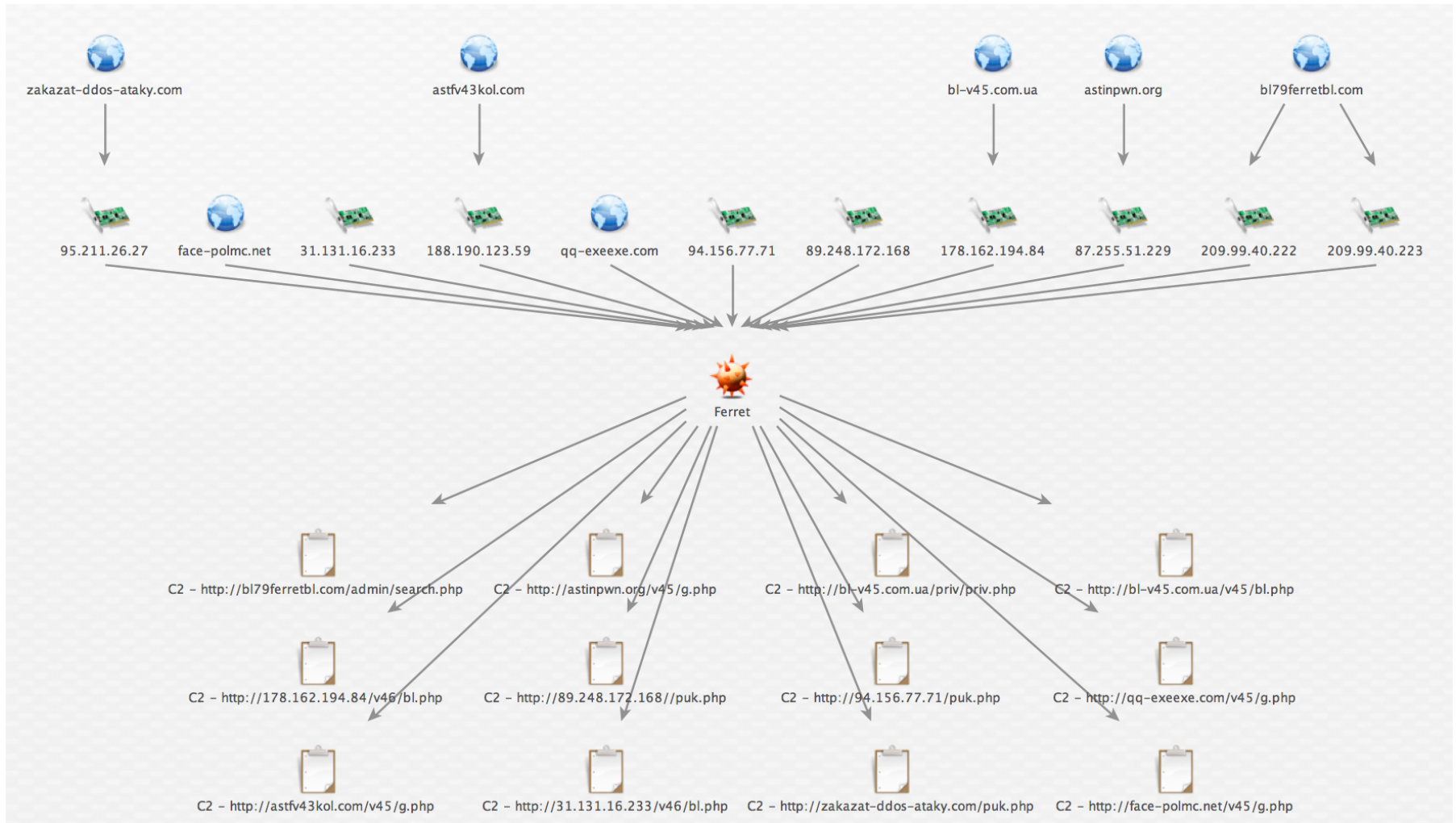
Copyleft – BlackRev – Attack Targets



A word cloud of various website URLs, likely representing attack targets. The words are arranged in a non-uniform, overlapping manner. The colors of the text vary, including shades of purple, blue, green, and brown. The background is a solid light green.

skriptomaniya.ru
webcamstudio.ru
vividcams.ru
divacams.ru
zakazat-ddos-kupit-ddos-ddos-service.biz
kharkovforum.com
hak-club.ru
top-ddos.in
bolasonic.com
passionstudio.ru
miami-studio.com
155ihbar.com
oberegi-runi.ru

Copyleft – Ferret



Copileft – Ferret

02/03/2014, 22:19 # 18

Copileft

Windows v.3.51 (NT)

Last Activity:
1 week ago

Register: 05.01.2013

Posts: 127

Thanked total: 223
for this post: 1

443666329

copileft@xep.li

Re: Complex for testing resistance to DDoS

Long time use this bot, from the earliest versiyay, very pleased with the vehicle.
Everything exactly as described above in the description.
Several times I needed something which revision (chips)
Generally recommend a decent product!

Long time use this bot, from the earliest [versions],
very pleased with the vehicle.

The dispute on the forum - this is the same as the Olym...
...dolbaeby

Last edited Copileft; 02/03/2014 at 22:27.

Copyleft – Ferret C2s

- Version updates
 - /priv/priv.php
 - /v46/bl.php
 - /v45/bl.php
 - /v45/g.php
- Filename patterns
 - g.php
 - bl.php
 - bl-v45.com.ua
 - bl79ferretbl.com
 - puk.php

Copyleft – Ferret – BladeRunner

- First logged attack: August 11, 2014
- Last logged attack: August 22, 2014
- Distinct target domains: 14

Copyleft – Ferret – BladeRunner

www.urbanlocker.com

erius.net cw2dw.net

direct-market.ru

shara-pro.com

prodw.org

tealer.fr

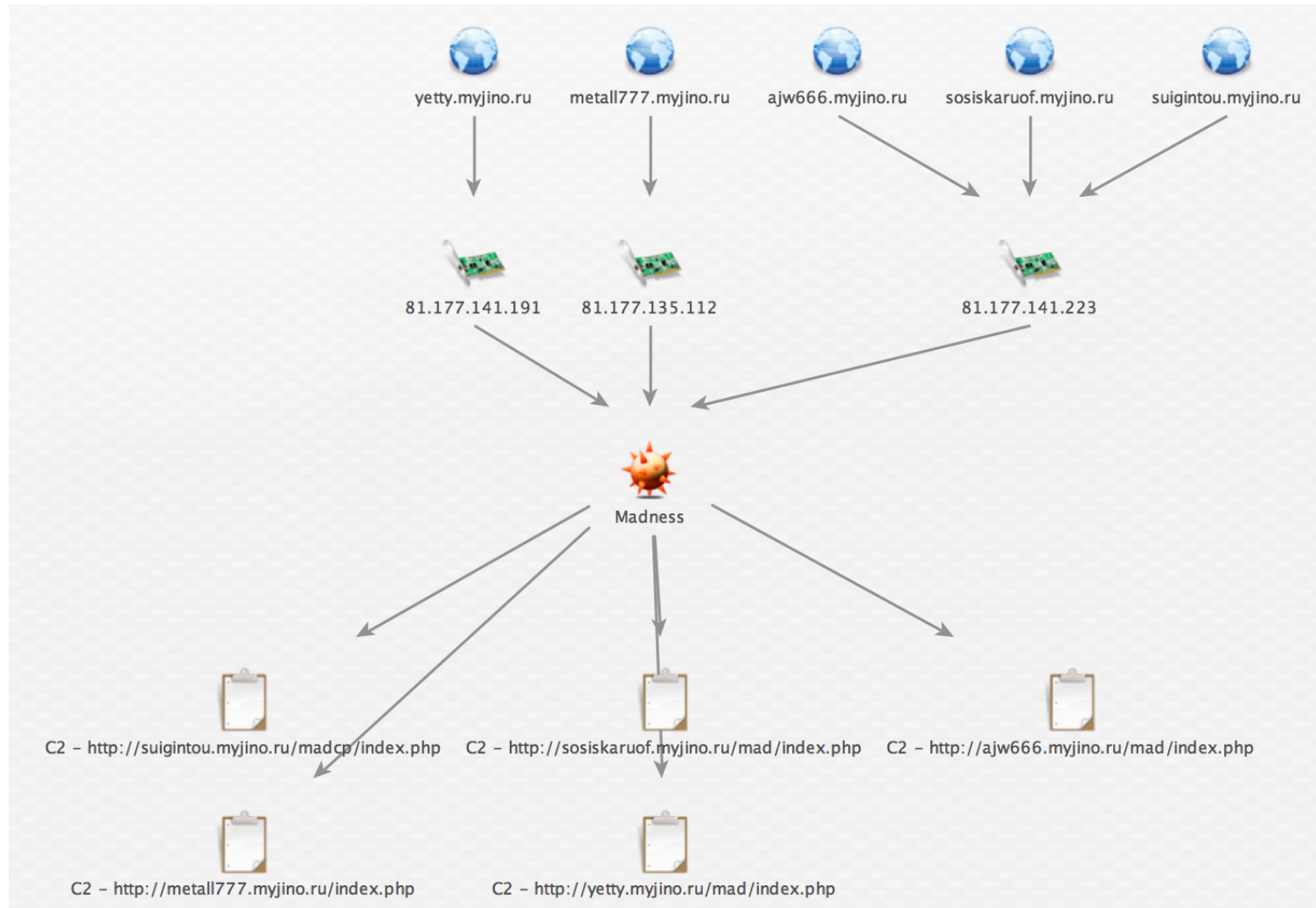
dcard.ws

investment-service.ru

www.almajd.ps

wyborcza.pl

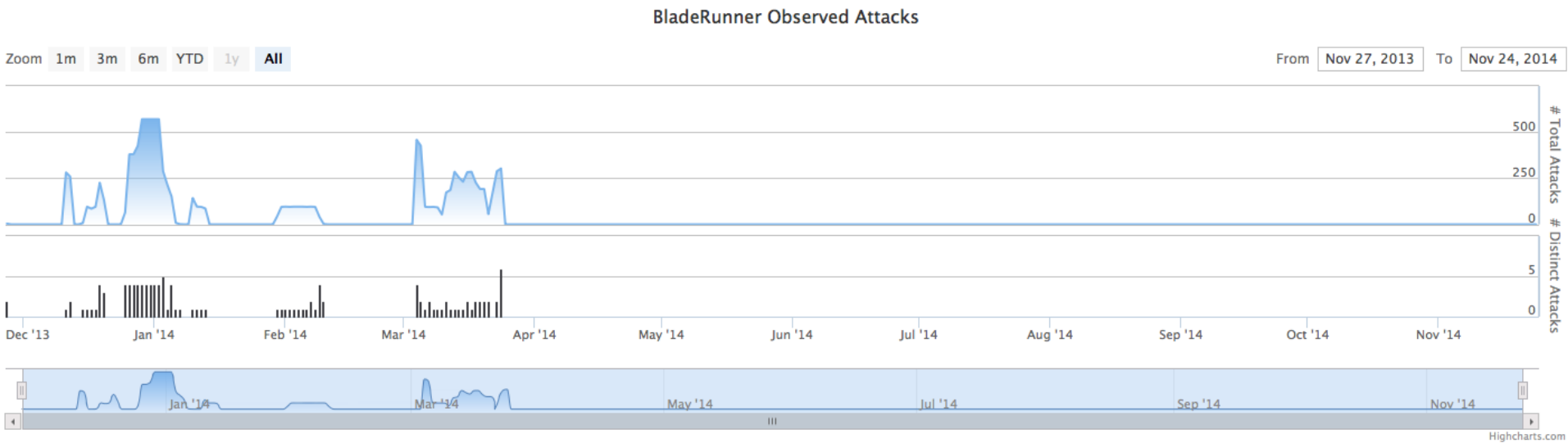
Copyleft – Madness



Copyleft – Madness

- First logged attack: October 29, 2013
- Last logged attack: March 24, 2014
- Distinct target domains: 40

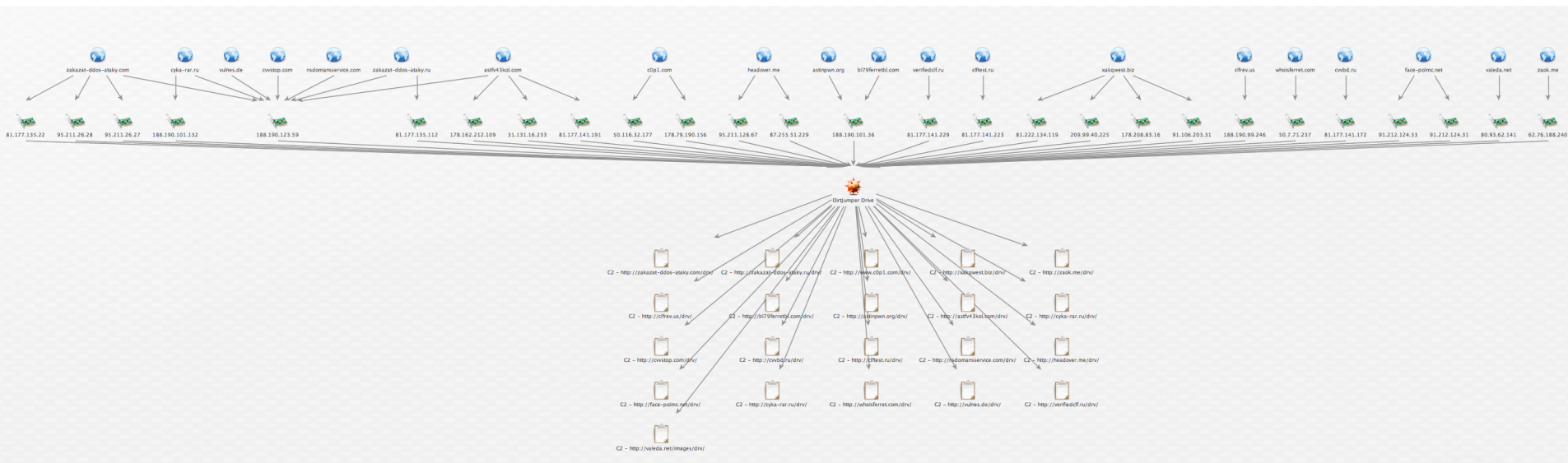
Copyleft – Madness



Copyleft – Madness – BladeRunner

unionmebel-spb.ru happy-hack.ru
evil-hack.ru dle-news.ru
fuckav.ru
www.bmw43club.ru drom.ru
chat-white.ru
apachan.net bhf.su olinepw.ru
novacidade.net swlan.ru
vremyachudes.no-ip.org it-kirov.org
bmwclub43.ru
forum.3xplr3.com smix.biz
elenamizulina.ru
m.chat-white.ru kino-reliz.com
lazycraft.ru bmw43club.ru
vremyachudes.ru vremyachudes.com

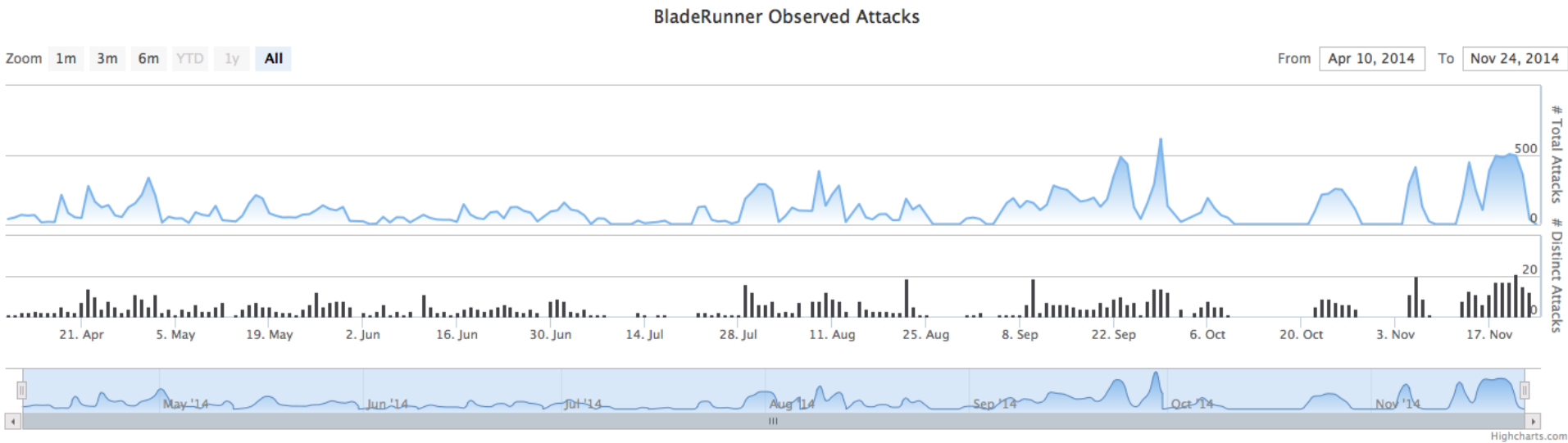
Copyleft – DirtJumper Drive



Copyleft – DirtJumper Drive – BladeRunner

- First logged attack: June 28, 2013
- Last logged attack: November 22, 2014
- Distinct target domains: 1669

Copyleft – DirtJumper Drive – BladeRunner



Copyleft – DirtJumper Drive – BladeRunner



Copyleft – C2 Patterns

- DirtJumper Drive
 - /drv/
- Copyleft
 - clfrev.us
 - clftest.ru
 - verifiedclf.ru

Crabby Krabeg

Krabeg – Ad

• Krabeg

Posted on June 28, 2012 - 22:51

DDoSSer



Members
2 posts

Offered DDOS services on the various sites, servers, and other Internet resources.

DDoS-attack (from the English. **Distributed Denial of Service** - distributed attack of the "denial of service").

The attack on a computer system in order to bring it to failure, that is, to create conditions under which legitimate users of the system can not access the provided system resources (servers), or the access is difficult.

Service Features:

- Complete anonymity
- Service without the mediation
- Reasonable prices for excellent quality
- Continuous monitoring of the targeted purpose
- Pre Paid test before ordering (from \$ 5)
- Different types of attacks, including the different protocols and ports
- Refunds in case of failure or cancellation

The prices of the service:

- **5 \$** - per hour
 - **\$ 40** - per night
 - from **\$ 250** - per week
- (The price depends on the targeted goals)

Payment Methods:

- WebMoney
- Yandex Money

Contacts:

- ICQ: **455-00-85**

Passed Inspection:

- shopworld.biz - Passed audits (3 pcs.)

Krabeg – Details

- ICQ: 4550085
- Jabber: 4550085@qip.ru

Krabeg – Stelios Blacklisting

09/24/2013, 15:19 # 6

Krabeg
DDoSSer

September 24, 2013

maverick = stelios = Kyd, rats, fraudsters !!!

Hidden text (you must login to your account or sign up and have 5 message (s)):
You do not have sufficient rights to see the hidden data contained here.

Join Date: 17-06-2012
Posts: 103
Thanks: 43
4550085

Mavrusha you stupid deer, where did you see me somebody threw? Nowhere, because I do not throw, but what are you saw on Google, well, you yourself read it? Stupid asshole. But you threw the Moor and, well, it has long been known to all, in fact, you're just a couple of days ago, threw a chela on the headstock, the site could not keep, and refused to return the money, though the site was a very weak, this suggests that you do not have even 200 bots, you just show-off their scatter and you can, all that zapezdyvaya 20Gb power there 🐼

Quote:

Message from the **Log from Blackman (neighing)**

[09/23/2013 14:59:36] <[Links visible only to registered users. Зарегистрироваться...]> Ddos nado?

[09/23/2013 15:05:34] <Horsemen of the Apocalypse> no Stelios

[09/23/2013 15:07:30] <[Links visible only to registered users. Зарегистрироваться...]> Ve tut?

[09/23/2013 15:08:16] <[Links visible only to registered users. Зарегистрироваться...]> Ya maverick

[09/23/2013 15:08:55] <[Links visible only to registered users. Зарегистрироваться...]> Ve ahueli?

[09/23/2013 15:08:59] <[Links visible only to registered users. Зарегистрироваться...]> Mamka ebal

[09/23/2013 15:09:00] <[Links visible only to registered users. Зарегистрироваться...]> Rot toptal

[09/23/2013 15:14:26] <[Links visible only to registered users. Зарегистрироваться...]> Ale?

[09/23/2013 15:14:40] <[Links visible only to registered users. Зарегистрироваться...]> Lox ebani

Mavrushchka just smear from DDOS can not do zaddosit because by any means trying to eliminate competitors by fakes.

pastebin.ru/VS781gsR
pastebin.com/6pSfnk
These pages are removed from Google.

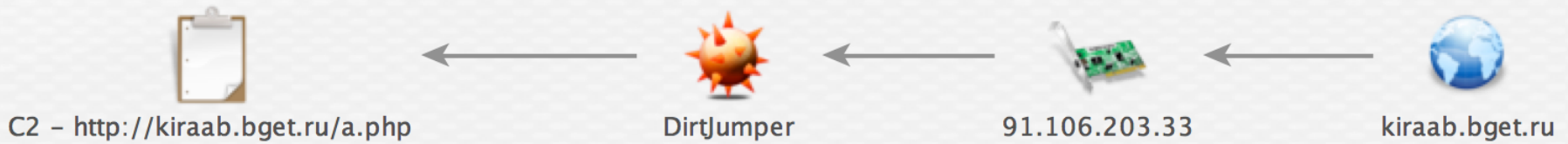
That IP of worm which all this dirt muddies:
91.121.166.108 (Courtesy admin pastebina)

Please check this IP on 81.177.6.1

And here's another info botnet Stelios (Moor):
81.177.6.12

Krabeg – kiraab.bget.ru

- **kiraab.bget.ru** → **Krabeg**

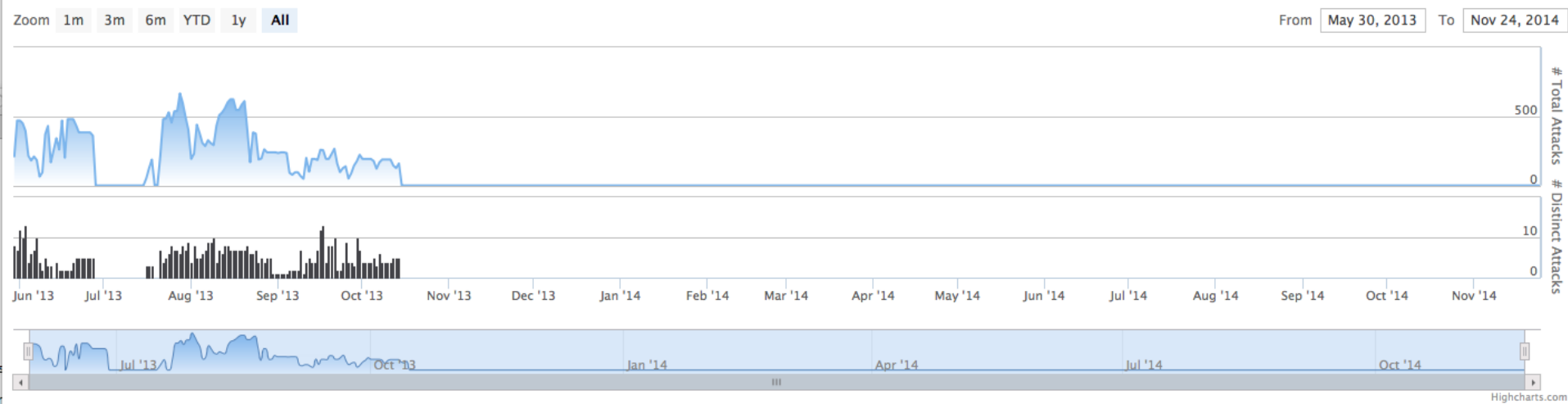


Krabeg – kiraab.bget.ru – BladeRunner

- First logged attack: May 30, 2013
- Last logged attack: October 14, 2013
- Distinct target domains: 119

Krabeg – kiraab.bget.ru – BladeRunner

BladeRunner Observed Attacks



Krabeg – kiraab.bget.ru – BladeRunner

forum.ruscams.com azpolitika.com
forum.kidal.org forum.allods2.eu
groza.ru
glosstime.ru ruscams.com
xn--80ackogdggscq.xn--plai atvision.net allods2.ru\r forum.antichat.ru
zar-par.ru www.alloder.ru www.skorobudu.com
incraft.ru invedit.ucoz.ru hqindex.org
4pda.ru
oprор.myjino.ru pplist.ru baginya.org
pastebin.ru allods2.eu utronews.ru
nocorruption.net hack-sell.su\r plexpert.ru
science.az
wow-extrim.ru
argumentua.com\r

Krabeg – San Wells Blacklisting

08/10/2014, 5:46 # 1 (Permalink)

Krabeg ▾
Beginner

Avatar Krabeg

Krabeg offline
Join Date: 17-06-2012
Posts: 8
Reputation: 0
ICQ: 4550085

San Wells bred / Icq 35993512 bred / Icq 660975608 bred

And so, the 5 th, this month, me in ICQ tapped "man" and would like to order a website, here is communication on ICQ:

Quote:

Message from the **(early conversation on ICQ):**
35993512 (17:33:48 5/08/2014)
need ddos

Krabeg (17:34:21 5/08/2014)
Hi

35993512 (17:34:32 5/08/2014)
Hi

35993512 (17:34:37 5/08/2014)
already ordered
(Why bother knocking if you are already booked, writes the type of DDoS needed a minute longer needed)

Krabeg (17:34:40 5/08/2014)
ca.

And now this "man" again decided to contact me:

Quote:

Message from **(today's talk on ICQ):**
35993512 (02:53:55 10/08/2014)
Hi

35993512 (02:53:57 10/08/2014)
here?

Krabeg (02:54:23 10/08/2014)
here

35993512 (02:54:31 10/08/2014)
Again we must

35993512 (02:55:07 10/08/2014)
san-wells. ***

35993512 (02:55:10 10/08/2014)
can?

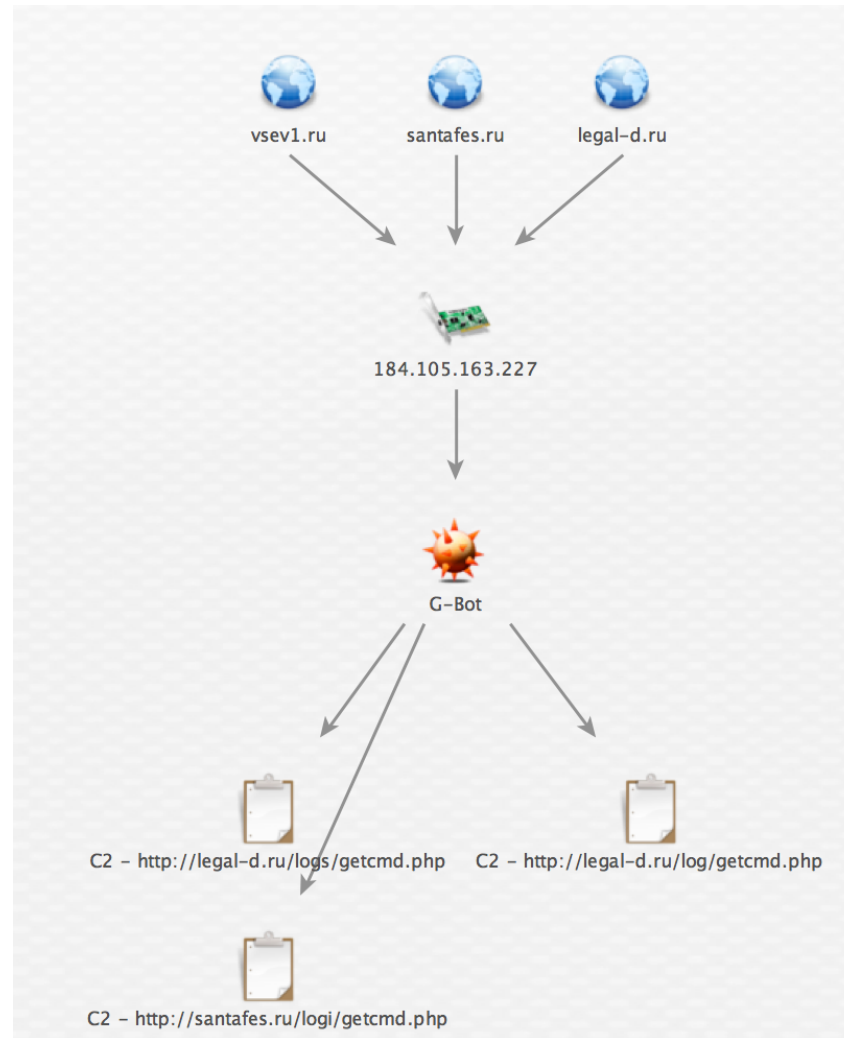
need ddos

August 10, 2014 -- san-wells.***

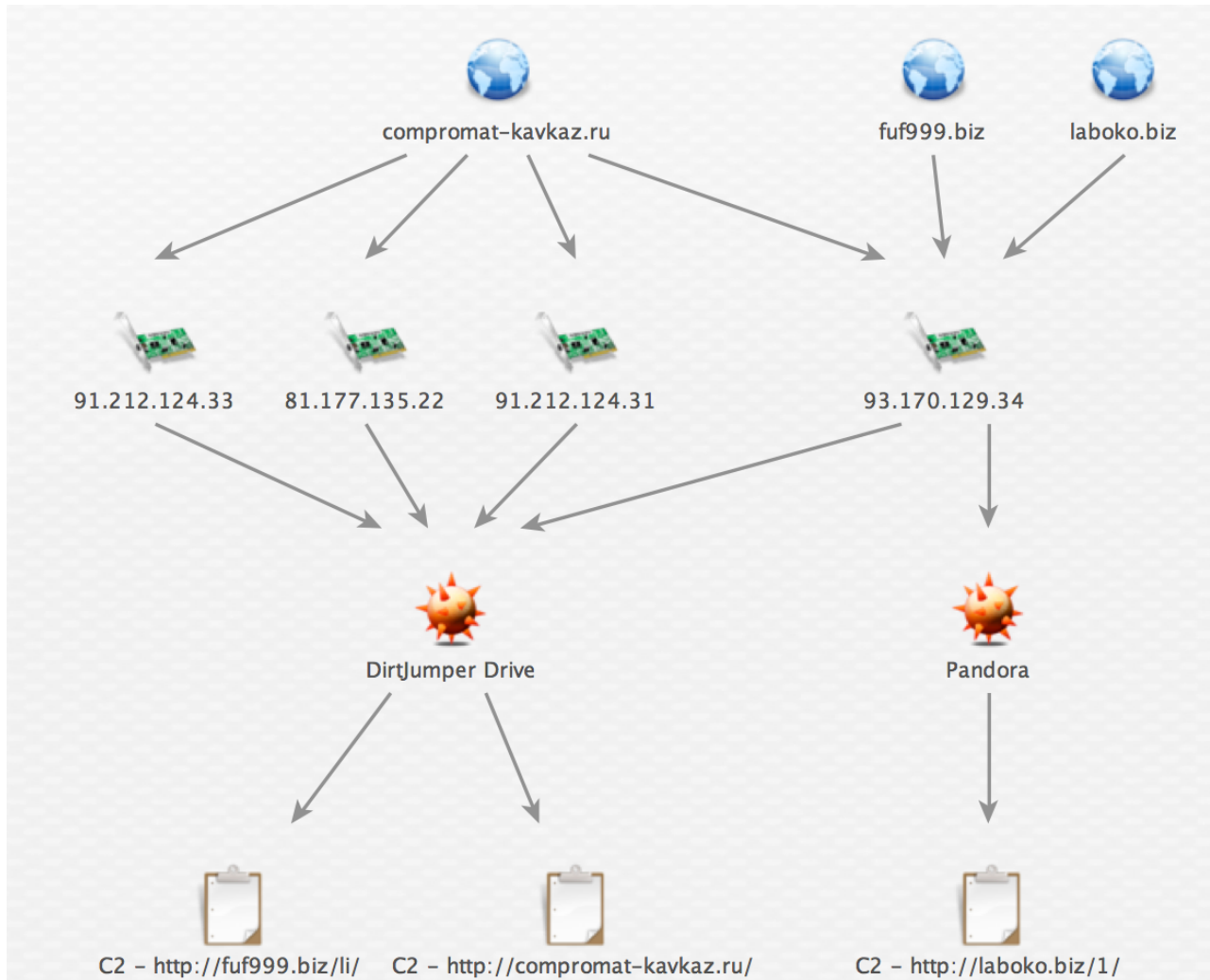
Krabeg – san-wells.ws – Attack C2s

- <http://legal-d.ru/log/getcmd.php>
- <http://santafes.ru/logi/getcmd.php>
- <http://compromat-kavkaz.ru/>

Legal D – Active Domains



Krabeg – compromat-kavkaz.ru

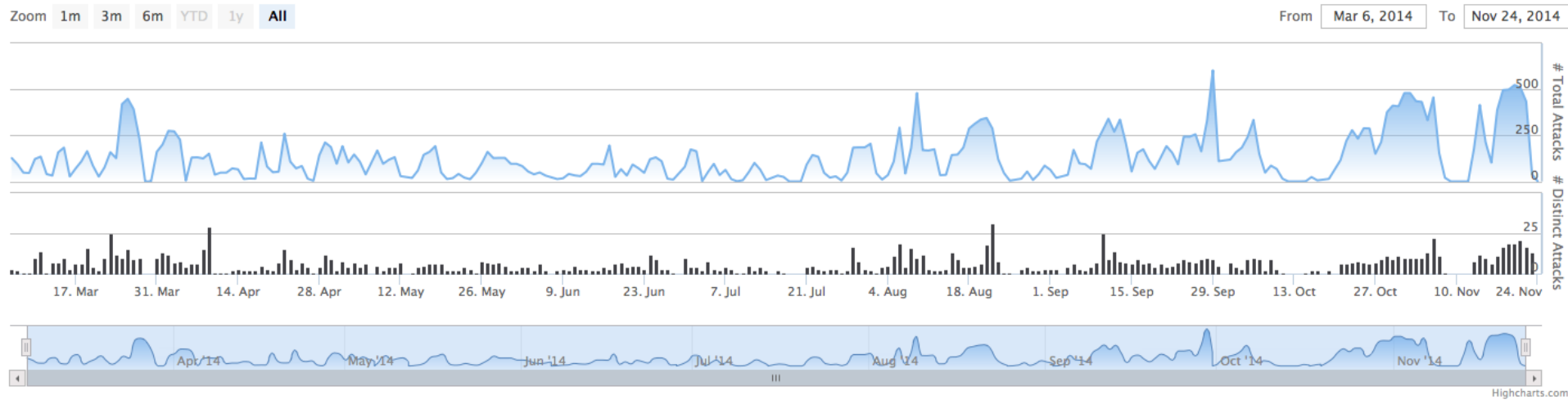


Krabeg – compromat-kavkaz.ru – BladeRunner

- First logged attack: November 25, 2013
- Last logged attack: November 22, 2014
- Distinct target domains: 767

Krabeg – compromat-kavkaz.ru – BladeRunner

BladeRunner Observed Attacks



Krabeg – compromat-kavkaz.ru – BladeRunner

www.lsresearchchems.com ifud.ws profakedocs.com
dream-supply.com
satsis.info syndication.traffichaus.com
kga.gov.ua
sharing-service.ru tic-research.com
tehnolenta.com
militarymaps.info rt.com vor.vc
news.pn www.lsrcdistribution.com
sharacom.com
shara.pro www.oneway-avia.ru
golubey.net vipshara.com

Takeaways and Future Work

- Passive Enumeration
 - Luck
 - Shaky pattern matching
 - Gut feelings
 - Incomplete information
- Active Enumerating
 - DDoS honeypots
 - Known target domains

Thanks Much !

- Questions/Comments/Feedback
- dschwarz@arbor.net