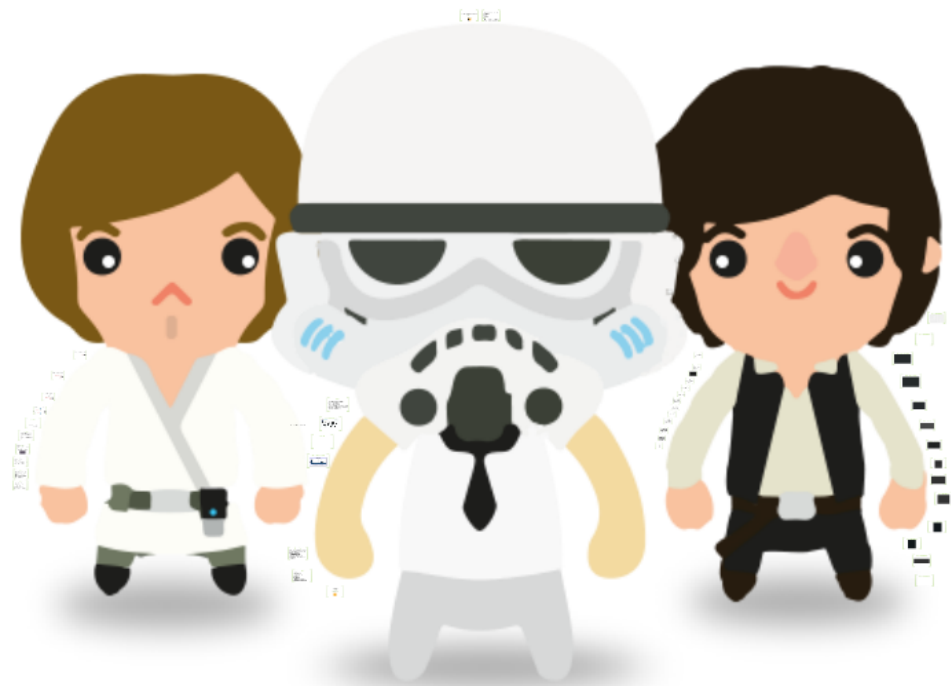




**MAY
THE
PLNOG
BE WITH
YOU**

PLNOG 2014
03-04.11.2014 WARSZAWA



**MAY
THE
PLNOG
BE WITH
YOU**

PLNOG 2014
03-04.111.2014 WARSZAWA

Ile kosztuje DDoS – z perspektywy cyberprzestępcy i ofiary ataku

Borys Łącki





Naszą misją jest ochrona naszych Klientów przed realnymi stratami finansowymi. Wykorzystując ponad 10 lat doświadczenia, świadczymy usługi z zakresu bezpieczeństwa IT:

- **Testy penetracyjne**
- **Audyty bezpieczeństwa**
- **Szkolenia**
- **Konsultacje**
- **Informatyka śledcza**
- **Aplikacje mobilne**

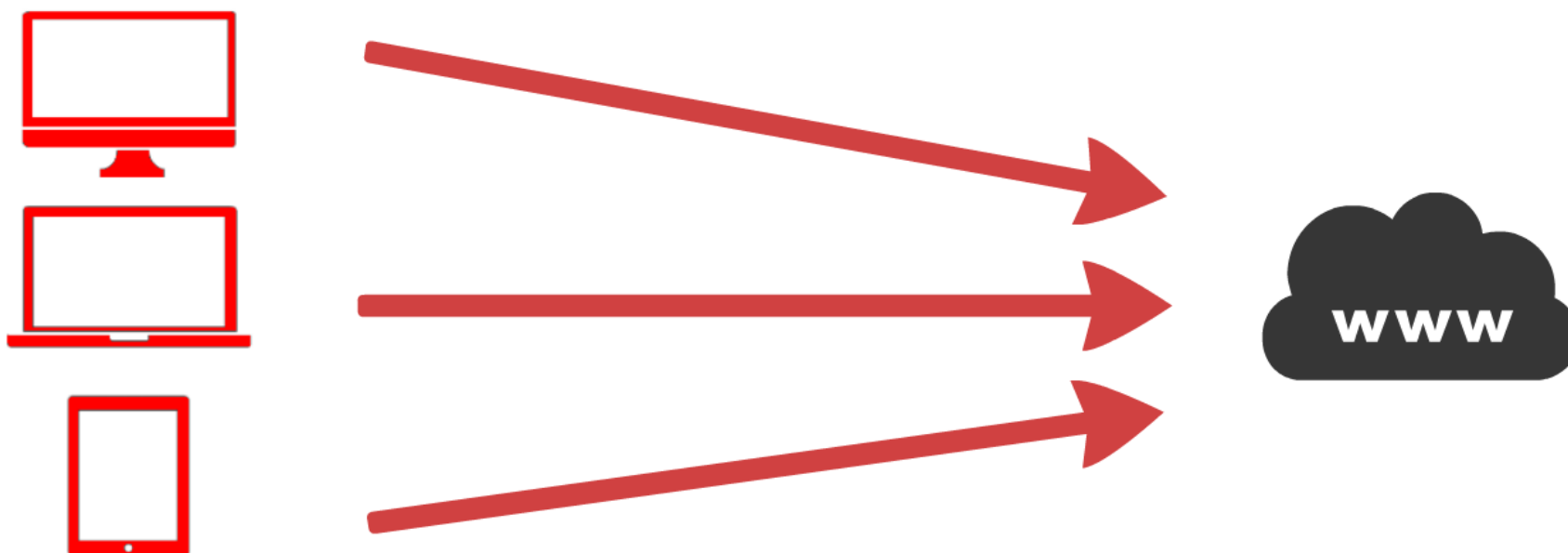
Borys Łącki

- **SECURE, Atak i Obrona, Internet Security Banking, SecureCON, SEConference, SekIT, ISSA, Open Source Security, PLNOG, (...)**
- **6 lat blogowania o cyberprzestępstwach: www.bothunters.pl**

DoS (ang. Denial of Service, odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania.

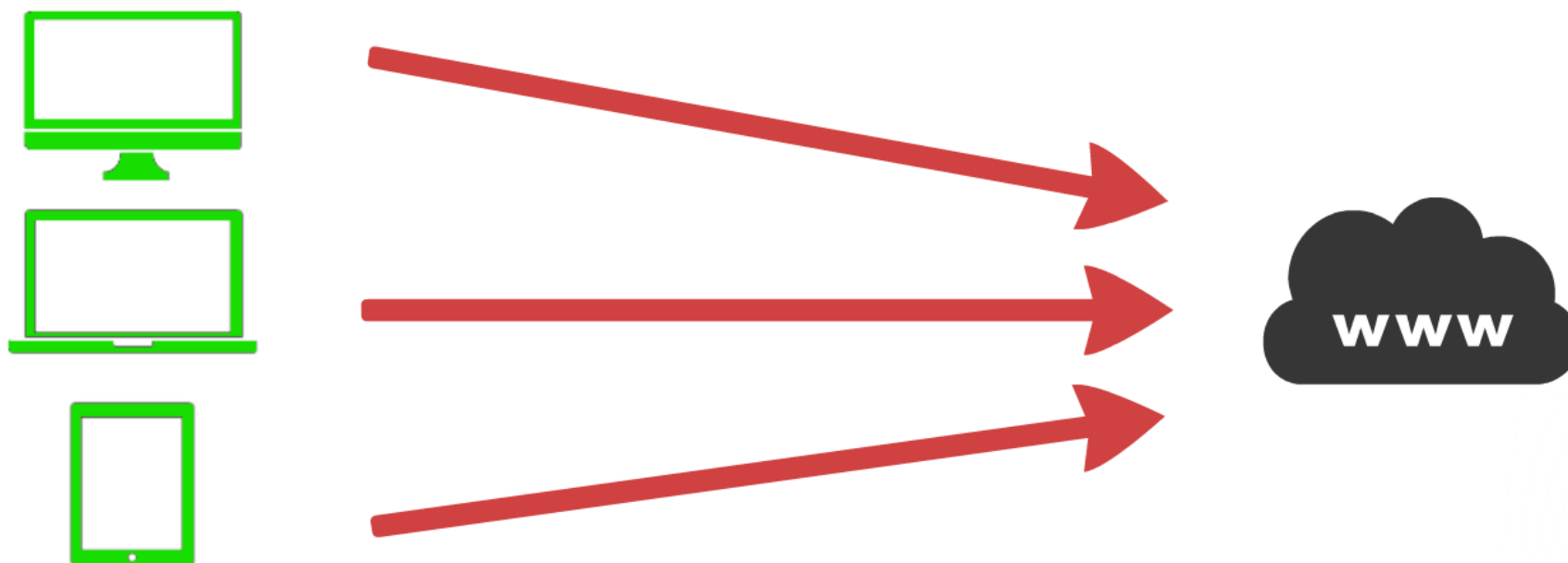


DDoS (ang. Distributed Denial of Service – rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie)

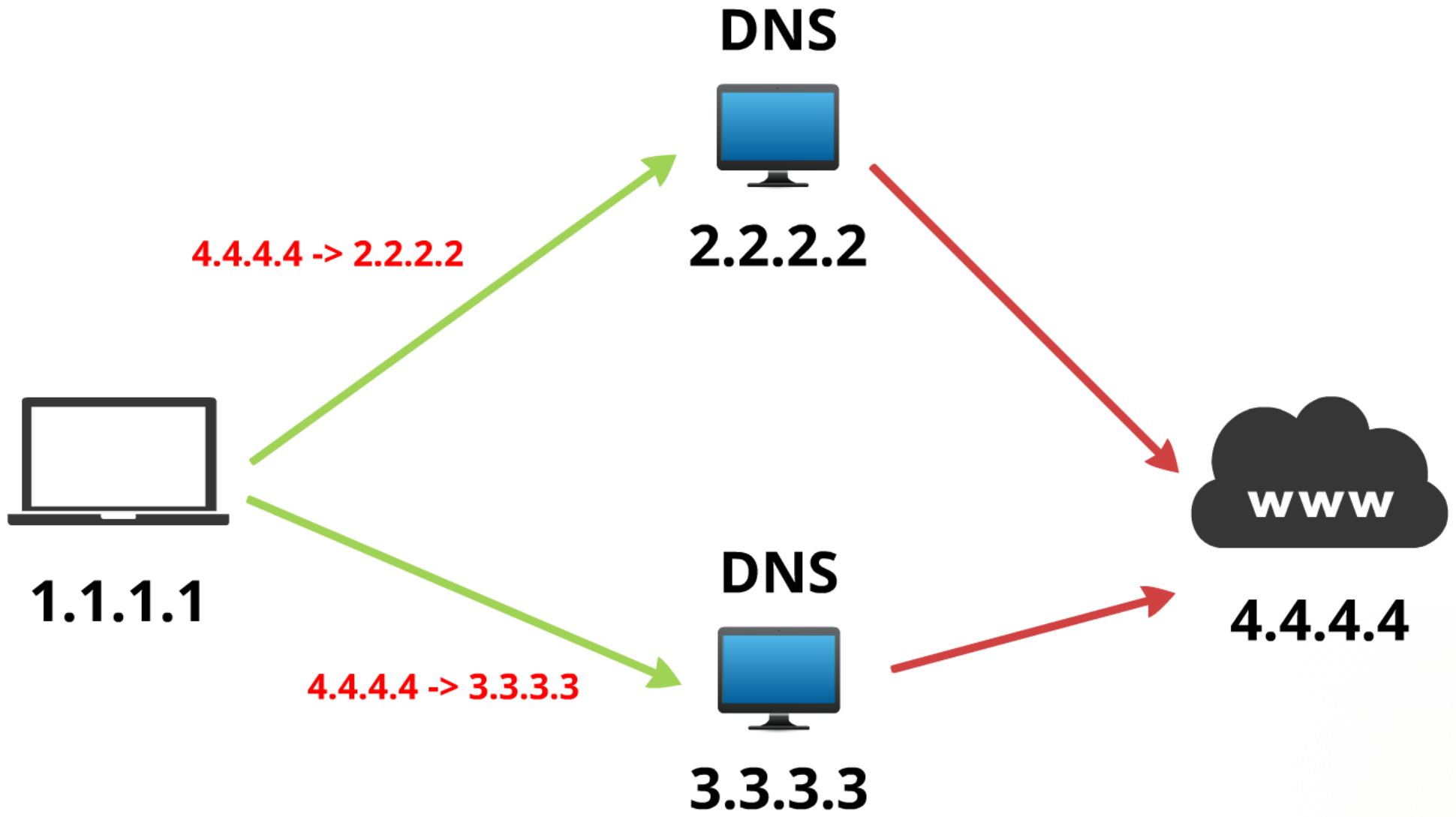


DRDoS (ang. Distributed Reflected Denial of Service) - jedna z nowszych odmian ataku odmowy dostępu DoS.

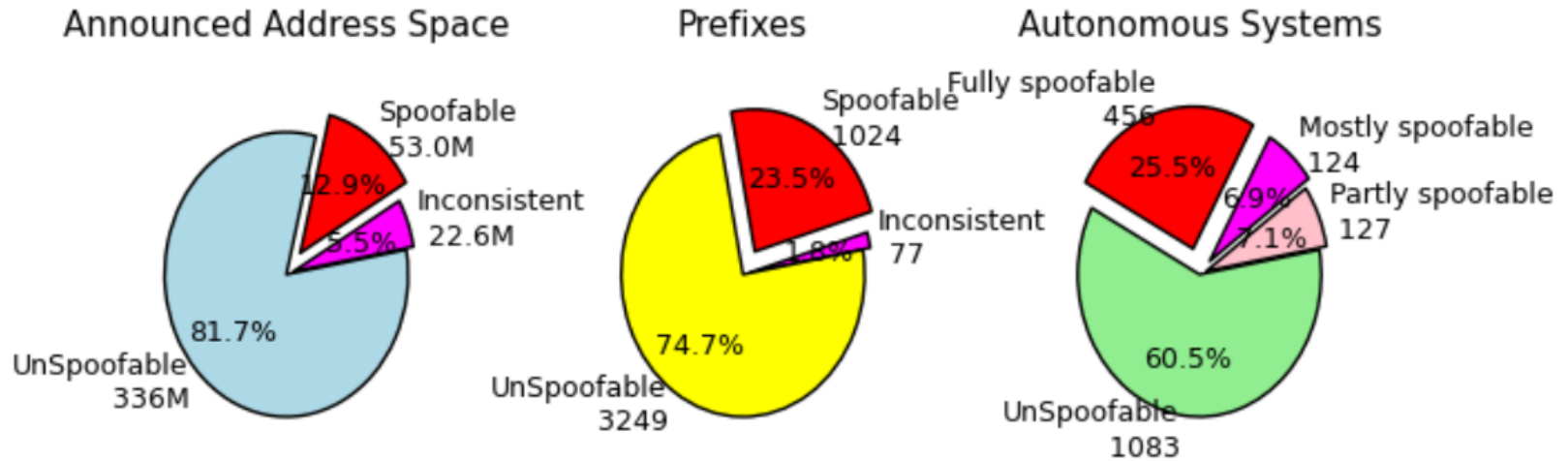
Polega na generowaniu specjalnych pakietów, których adres źródłowy jest fałszywy - jest nim adres ofiary. Następnie duża liczba takich pakietów jest wysyłana do sieci.



DRDoS (ang. Distributed Reflected Denial of Service)



Statystyki



Open Resolver Project - DNS

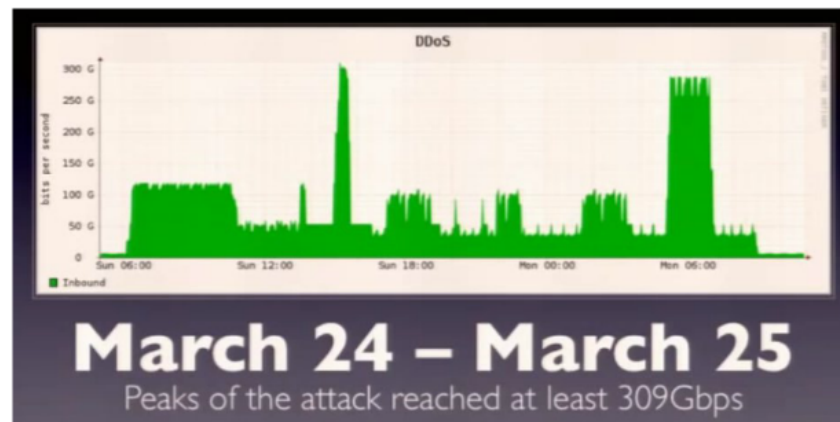
2014-02-23 - **25 510 460**

Statystyki

- **2012 - 65 Gbps**
- **2013 - 160 Gbps / 120 Mpps**
- **2013 - 309 Gbps / Spamhaus**
DNS
- **2014.02 - 350 Gbps / OVH**
- **2014.02 - 400 Gbps / CloudFlare**
NTP

Spamhaus

- **309 Gbps - 28 minut**
- 30956 open DNS resolvers ~ 0.1%
- 3 sieci - spoof IP
- 1 laptop, 5-7 przejętych serwerów
- 9 Gbps zapytań = 300 Gbps odpowiedzi



201?

- ~ 8% open DNS resolvers
- 100 sieci - spoof IP
- 1 laptop, 200-400 przejętych serwerów
- 280 Gbps zapytań = **12 Tbps**
odpowiedzi

DrDoS

- **SNMP** - Simple Network Management Protocol - **600 X**
- **NTP** - Network Time Protocol - **43 X**
- **CHARGEN** - Character Generator Protocol - **17 X**
- **DNS** - Domain Name System - **53 X**
- **(Quake 3, Steam, BitTorrent, SSDP, NetBios, QOTD, Kad, ...)**

DrDoS

- ; <<>> **DiG <<>> @ns1.cisco.com axfr cisco.com**
- (...)
- zzz-dns.cisco.com. 86400 IN NS bxb-vm2.cisco.com.
- zzz-s3.cisco.com. 86400 IN A 10.86.41.33
- zzz-s3-priv.cisco.com. 86400 IN A 10.86.41.34
- cisco.com. 86400 IN SOA edns-aln1-1-l.
postmaster.cisco.com. 12445597 7200 1800 864000 86400
- ;; Query time: 176665 msec
- ;; SERVER: 72.163.5.201#53(72.163.5.201)
- ;; WHEN: Sat **Sep 14 16:35:38 2013**
- XFR size: 1808339 records (messages 1222, **bytes 62561398**)

Botnet

- **2012-2013 - > 8 000 000 - Bamital**
- **2012 - 109 000 - Kelihos**
- **2012 - > 3 000 000 - Virut**
- **2013.02 - ~ 500 000 - Microsoft - ZeroAccess**
- **2013.09 - ~ 500 000 - Symantec - ZeroAccess**
- **2013.09 - ~ 2 000 000 - TOR**

Botnet PL - 2014.01.19



[Piotr Kijewski](#)

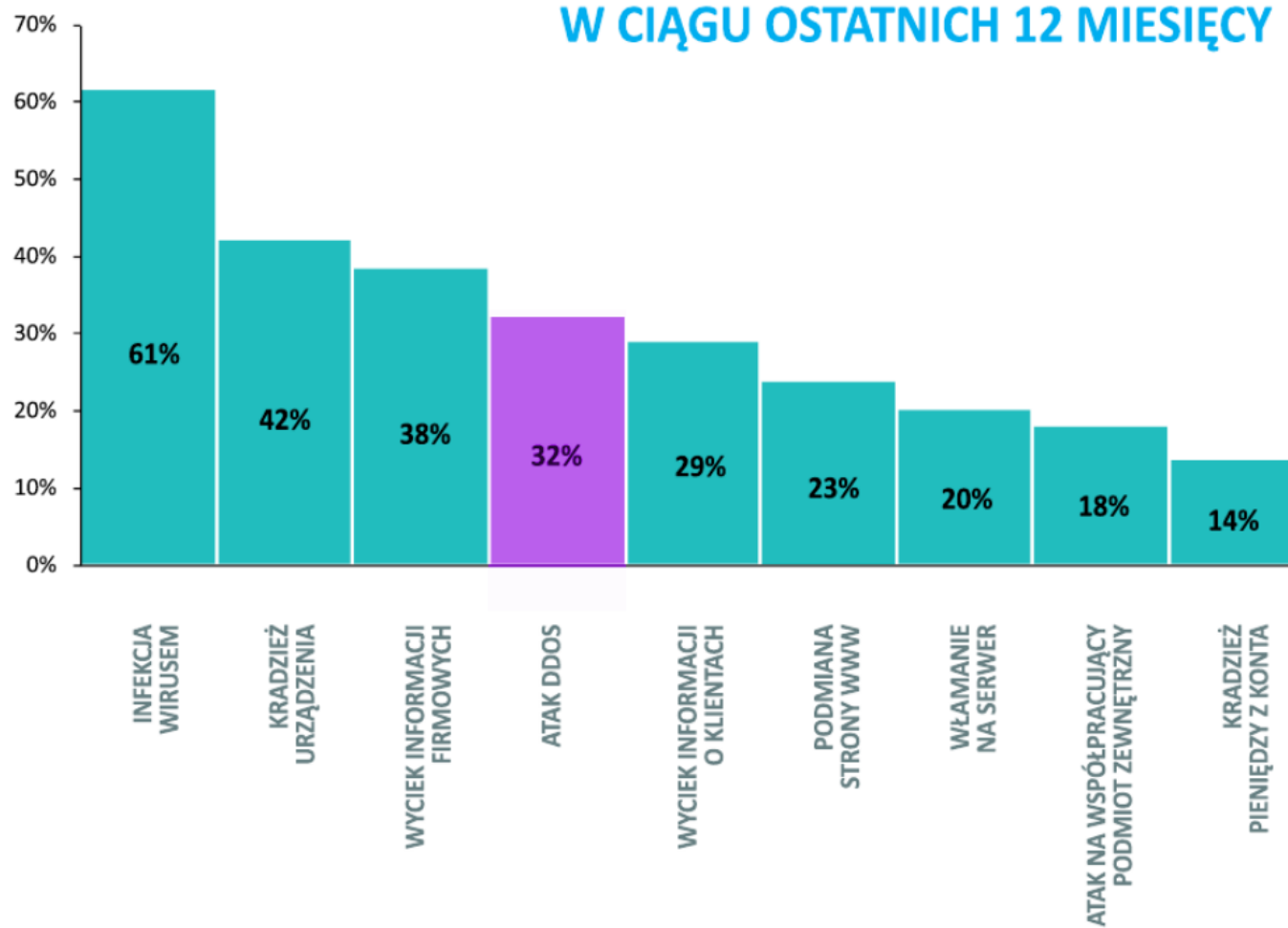
@piotrkijewski

+ Obserwuj

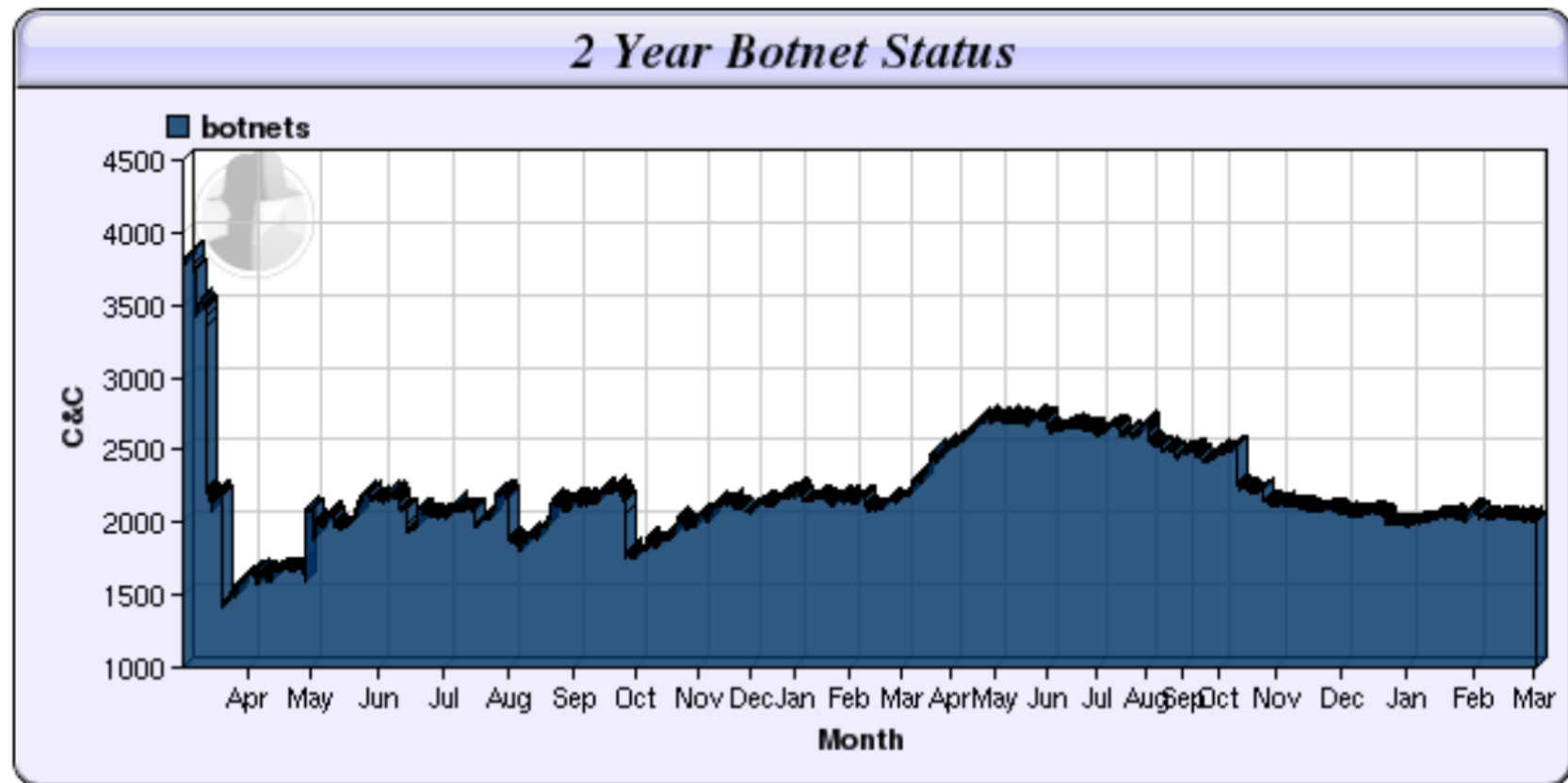
Top botnet population in Poland
(daily size estimate, infected hosts):
Conficker 46k Sality 24k
Zeroaccess 19k Virut 15k Zeus/
Citadel 12k

DDoS PL

RODZAJE INCYDENTÓW W CIĄGU OSTATNICH 12 MIESIĘCY



ShadowServer - 2014.02



DDoS - Koszty

- **operacyjne IT**
- **BOK**
- **reputacja - Klienci aktualni i potencjalni**
- **kary umowne (SLA)**
- **wydajność pracowników**
- **biznes**

DDoS - Koszty

Szacunkowo

- **DC 100 m2**
8 500\$ - 201 000\$ (średnio 46 000\$) / 1 h
- **10 000\$ - 50 000\$ / 1h**

DDoS - Koszty



Lost 500k during DDOS attack!

1 reply

[s3k] James



14 posts

0 votes

I had 500k when I was playing and I remember syncing. I've always had this problem with syncing but yes I did sync so then it said no message received for 10 sec so I was like "I synced so I should be good" then I realized server wasn't going back up for a while then I waited next day nope nothing then I read forums it said we had a DDos attack. Then today I finally log on after waiting all night literally just to play altis life. Then first thing I was going to do is get my truck and go to the airport garage. Once my truck spawned I pressed U but it wouldn't unlock so then admin said server was going to restart in 2 min. So then I decided to get a ride to the airport and boom my hummingbird was there then that's when I realized I should check if I have my money too nope I was missing 500k. So then when server restated I checked my garage and my truck was gone. So that is what brought me here please fix this because I like this server better then any other altis life servers. Thanks in advance.

[↪](#) Posted Feb 22, 14 · OP

0 votes

[s3k] James



14 posts

0 votes

I got my comp THANKS!

[↪](#) Posted Sat at 18:19 · OP

0 votes

DDoS - Koszty

"ujęto 6 osób z Hong Kongu, które szantażowały firmy zajmujące się handlem złotem, srebrem, papierami wartościowymi. 15 firm zapłaciło od 15 do 50 tysięcy złotych za "spokój". Jedna z firm zapłaciła w tym okresie 26 razy!"

DDoS - Koszty

"when HKeX under DDoS attack, all the HK stock market trading also halted. The cost is uncountable."

DDoS - Koszty

"a popular E-commerce website told Prolexic it had calculated that it lost 1 000\$ per second when it was brought down by DDoS"

DDoS - Koszty

"European gaming company, which was experiencing a series of DDoS attacks that caused significant losses in revenue. By then, the company had already experienced costly downtime, amounted to anywhere from £80,000 to £160,000 in lost revenue"

DDoS - Koszty

Online Gaming - "It was DDoS attack during peak hours. It was long lasting around 3 month. As the result, they loss 50% of customers and they fired their CEO"

DDoS - Koszty

"A DDoS attack that shut down the site of popular battery retailer for several hours resulted in losses of 40 000 \$"

DDoS - Koszty

"The parties had agreed that the direct losses as a result of the attack on the website were less than \$5,000 but Koch Industries had argued that it hired a consulting group to protect its Web sites at a cost of approximately \$183,000."

DDoS - Koszty

Kampania kwietniowa (2013)

"W sumie w ostatnich dwóch miesiącach mieliśmy do czynienia z około 4 atakami DDOS, które skutkowały dłuższą niedostępnością serwisu Allegro ale tylko dla części naszych Użytkowników. Wczoraj z problemami borykało się około 20% naszych użytkowników, pozostali nie mieli problemów z dostępem do serwisu."

Grupa Allegro ~ 16 mln użytkowników

DDoS - Koszty

"Od godziny 20 obserwujemy duży atak DDoS, m.in. na nasze adresy IP. Atak wygenerował ruch przeszło dziesięciokrotnie większy niż zwykły i zapchał wszystkie nasze łącza.

Atak ma intensywność ok 60Gbps i ponad 62Mpps. Atak pochodził z ponad 257 tyś adresów źródłowych na całym świecie a celem ataku były wszystkie adresy z jednej z naszych klas IP.

Niestety ok 1/4 klientów została całkowicie pozbawiona usługi dostępu do Internetu."

DDoS - Koszty

24.12.2012

"San Francisco - Bank of the West"
> 900 000\$

DDoS - Cyberprzestępcy

HOME > PRICING >

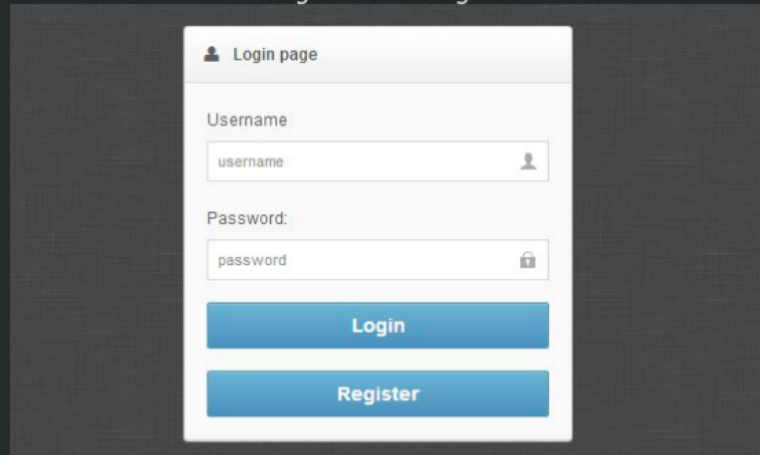
Plans and pricing Autobuy

Monthly

	Bronze	Silver	Gold	Platinum	Ultimate
Max Boot	300 seconds	450 seconds	600 seconds	1500 seconds	1 hour
Attacks	<i>unlimited</i>	<i>unlimited</i>	<i>unlimited</i>	<i>unlimited</i>	<i>unlimited</i>
50GBPS TOTAL NETWORK	✓	✓	✓	✓	✓
LAYER 4 & 7	✓	✓	✓	✓	✓
INSTANT ACTIVATION	✓	✓	✓	✓	✓
	BUY NOW £5.99	BUY NOW £9.99	BUY NOW £14.99	BUY NOW £19.99	BUY NOW £39.99

DDoS - Cyberprzestępcy

Register and Log In!!



Login page

Username
username

Password:
password

Login

Register

Once you've registered for the first time. You will choose from several packages of Boot time and Strength. I have Personally found that is important to have several Booters with medium time, rather than just 1 large DDoser (there is more flexibility, and more safety against hosting failures) + With your 2 or 3 DDosers and you will completely punish any group of people.

Silver		Gold	
Price:	\$12.99	Price:	\$24.99
Length:	31 Days	Length:	31 Days
Max Boot Time:	1200 Seconds	Max Boot Time:	3600 Seconds
Concurrent Attacks:	1 Attacks	Concurrent Attacks:	1 Attacks
Description: 1200 seconds		Description: 3600 seconds	
Buy Now!		Buy Now!	

DDoS - Cyberprzestępcy

Selling DDOSES Here! *Prices Can Be Crunched*

Each Comes With 2 Attacks! 1 PRICE!

PACKAGE 1: 1-5 Minute DDOSS \$1.00 (Comes With 2 Attacks For 1 Price!)

PACKAGE 2: 5-10 Minute DDOSS \$1.50 (Comes With 2 Attacks For 1 Price!)

PACKAGE 3: 10-20 Minute DDOSS \$2.50 (Comes With 2 Attacks For 1 Price!)

PACKAGE 4: ELITE PACKAGE: 1-20 Minute DDOSS + 1MONTH Of Service "When Available" \$8.00

TRUSTED SELLER! PAYPAL VERIFIED!

Vouch Copy **[ALREADY]** Given.

[RIGHT]Stresser:

Custom Booter

20min MAX.

Chargen, UDP, UDP-Lag, SSYN, HTTP GHP

TO ORDER: Contact Me ON Skype: kcrossey

We Will Talk About Details & Price Crunching There! (: 🤔 🤔 🤔 🤔 🤔 🤔 🤔 🤔 🤔 🤔 🤔 🤔 Thank You!

DDoS - Cyberprzestępcy

Ddos | IP Resolver | CloudFlare Down | Website IP | VPN Breaker | Service

Hello, I'm going to sell my Service!

Features:

DDOS

IP Resolver

CloudFlare (Shut Down CloudFlare on any Site) (Free Version only)

Website IP Resolver

Prices:

Ddos: 4\$/ 2 Min

IP Resolver (Steam - Skype): 2\$

CloudFlare: 7\$/ 30 Min

Website IP: 3\$

VPN Breaker: 8\$

PM/Post if you're interested

**I'm not going to use my service before getting the money in ANYWAY - ChargeBack will lead you to a ban and Ddosed

DDoS - Cyberprzestępcy

So recently i acquired a very strong, DDoser <3

Now i'm offering ddosing, Guaranteed to bring them down, Or your money back, Plus a free ddos!
I can do 2 DDos's at a time :P

Pricing:

1/3 Power: Every 300 Seconds is .50 cents!

Max Power: Every 300 Seconds is .75 cents

Monthly:

1/3 Power for a month, Max of 1000 Seconds per ddos, 2 ddos per hour
10 dollars

Max Power for a month, Max of 1000 Seconds per DDos, 2 ddos per hour
15 dollars

To purchase:

Add Afitz200 On skype

You pay first, Money back if does not go down!

Current sales/promotions:

None

DDoS - Cyberprzestępcy

Our current power is 5Gbps average, 20Gbps network!

Monthly	Lifetime	Addons	
100 Seconds MONTHLY Price: \$2.99 We accept PayPal & Bitcoin!	180 Seconds MONTHLY Price: \$4.99 We accept PayPal & Bitcoin!	500 Second MONTHLY Price: \$9.99 We accept PayPal & Bitcoin!	1500 Seconds MONTHLY Price: \$14.99 We accept PayPal & Bitcoin!
3500 Seconds MONTHLY Price: \$19.99 We accept PayPal & Bitcoin!	7200 Second MONTHLY Price: \$29.99 We accept PayPal & Bitcoin!	10800 Seconds MONTHLY Price: \$49.99 We accept PayPal & Bitcoin!	30k Seconds MONTHLY Price: \$69.99 We accept PayPal & Bitcoin!

DDoS - Cyberprzestępcy

The image shows a screenshot of a website offering DDoS attack services. It features three main product cards arranged horizontally. Each card has a dark background with white text. The first card is for 'Life Gold', the second for 'Solo Diamond', and the third for 'Dual Diamond'. Each card lists a price in USD, duration in days, stress time in seconds, and the number of concurrent attacks. Below each card are two buttons: a red one for 'Pay with Paypal' and a white one with a Bitcoin icon for 'Pay with Bitcoin'. A 'Check price in BTC' link is also present. At the bottom right, there is a dark grey chat bubble with a speech icon and the text 'Live Support' and a plus sign.

Package Name	Description	Price (USD)	Length (days)	Stress time (seconds)	Concurrent attacks
Life Gold	Power Gold for life!	100.00	3650	3600	1
Solo Diamond	Destroy all with Power Platinum!	60.00	31	7200	1
Dual Diamond	2 Concurrents!	90.00	31	7200	2

Payment options: [Pay with Paypal](#), [Pay with Bitcoin](#), [Check price in BTC](#)

Live Support

DDoS - Cyberprzestępcy

TYPES OF ATTACKS

- JUNO SYNTAX
- SLICE SYNTAX
- STREAM TCP PACKET STORM
- TALK SYNTAX
- TCP SYNTAX
- UDP SYNTAX
- BANG SYNTAX
- FUCK SYNTAX
- FUCK4 SYNTAX
- HTTP SYNTAX
- DESTROY SYNTAX
- SKYPE SYNTAX
- 5TD SYNTAX
- TTY SYNTAX
- V2 SYNTAX




ALL OF THE BOT PACKAGES WILL RUN ALL OF THE ATTACKS MENTIONED ABOVE


PRICES


REGULAR PACK MAINLY FOR HOME CONNECTIONS OR GAMESERVERS	ADVANCED PACK FOR HIGHLY PROTECTED SITES / CLOUDFLARE
15 BOTS - \$75	20 BOTS - \$160
30 BOTS - \$145	40 BOTS - \$300
40 BOTS - \$200	60 BOTS - \$450
	80 BOTS - \$600
	100 BOTS - \$750


WE RUN THE IRC NETWORK. EACH CUSTOMER WILL HAVE A DIFFERENT
IP TO CONNECT TO, AND A PRIVATE CHANNEL

PAYMENT AND CONTACT

PayPal    WebMoney

Perfect Money 

MoneyGram 
Money Transfer

WESTERN 

DDoS - Cyberprzestępcy

FEATURES

CLOUDFLARE RESOLVER ✓

IP LOOKUP ✓

AUTOBUY ✓

IP GRABBER ✓

WEBSITE RESOLVER ✓

DEDICATED SUPPORT ✓

FRIENDS AND ENEMIES ✓

DEDICATED SERVERS ✓

100% UPTIME ✓

UNTRACEABLE ✓

CHEAP ✓

DDoS - Cyberprzestępcy

1 MONTH	1 MONTH	1 MONTH
600 SECONDS	1000 SECONDS	1400 SECONDS
\$2.99	\$4.99	\$6.99
3 MONTHS	3 MONTH	3 MONTH
600 SECONDS	1000 SECONDS	1400 SECONDS
\$4.99	\$9.99	\$12.99
LIFETIME	LIFETIME	LIFETIME
600 SECONDS	1000 SECONDS	1400 SECONDS
\$14.99	\$24.99	\$49.99

DDoS - Cyberprzestępcy

GETSMACKED

SMACK YOUR ENEMIES OFFLINE

INTRODUCTION



GetSmacked is not you're regular booter. We are here to bring a product that exceeds the expectations of our customers. GetSmacked is ran by professionals who know what they are doing in this field, what that means for the customer is very *little* downtime, everything is self maintained by us, so you don't need to worry about anything! We have *many staff* members on hand at any given point to offer a very quick reply by our *ticket system*, should you need assistance with anything.

First time purchasing a booter? NO PROBLEM!

If you are unsure or confused on any aspects of how to use GetSmacked, you can open a support ticket at any moment and we will be glad to assist you with any confusion you may have, we try to make this as user-friendly as possible so you don't need to worry about a thing!

FEATURES

- ✓ UDP
- ✓ HTTP POST
- ✓ STEAM RESOLVER
- ✓ DEDICATED SERVERS
- ✓ SSYN
- ✓ RUDY
- ✓ CLOUDFLARE RESOLVER
- ✓ STOP ATTACK
- ✓ HOME (Unique)
- ✓ SOURCE
- ✓ SKYPE BETA RESOLVER
- ✓ AUTO BUY
- ✓ HTTP GET
- ✓ ARME
- ✓ HOST to IP
- ✓ TICKET SUPPORT
- ✓ HTTP HEAD
- ✓ CUSTOM SOURCE
- ✓ 24Hour BOOT TIME (SS.00 - Home)
- ✓ HIGH UPTIME

DDoS - Cyberprzestępcy

PURCHASING

STARTING AT ONLY!
\$2.00

- ✓ 7200 Seconds Boot Time
- ✓ 1 Concurrent Boots
- ✓ 6 Months Membership
- ✓ Full Customer Support


★ WHEN YOU BUY A PLAN (NOT INCLUDING TRIAL) YOU WILL BE ABLE TO USE OUR HOME METHOD. THIS METHOD ALLOWS YOU TO BOOT A HOME CONNECTION FOR UP TO 24 HOURS. ★


FOR COMPLETE LIST OF PRICES & PACKAGES, PLEASE VISIT OUR WEBSITE:
WWW.GETSMACK.DE


PayPal bitcoin

WE CURRENTLY ACCEPT PAYMENTS THROUGH
PAYPAL & BITCOINS ONLY

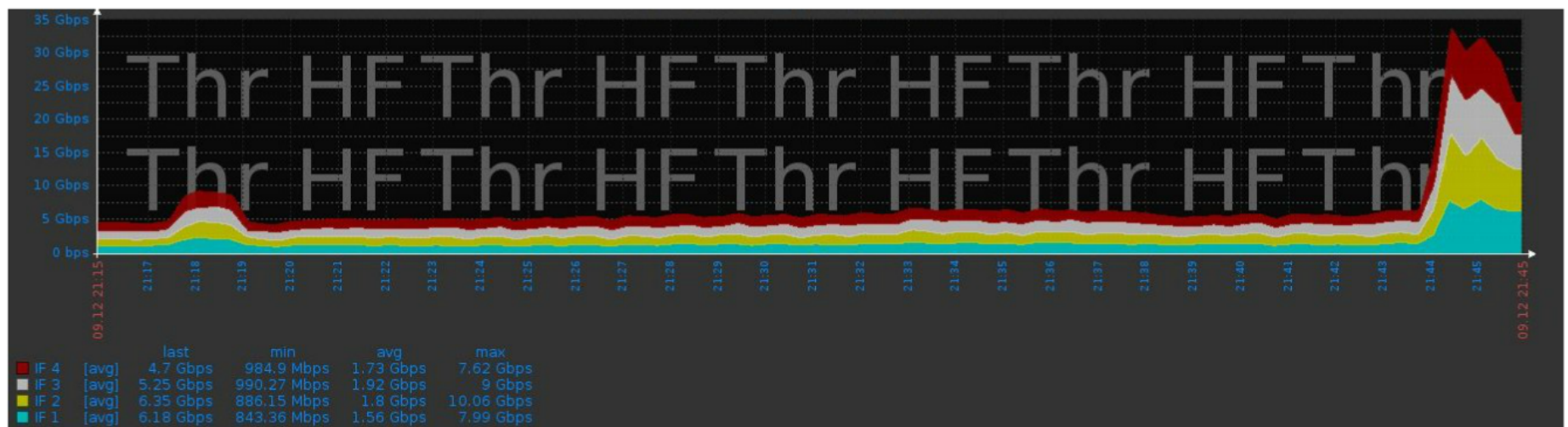
PURCHASING

 **SKYPE SUPPORT**
FROFROSTORM (JUST MESSAGE ME)

 **PRIVATE MESSAGE**
FROSTORM (JUST MESSAGE ME)

 **TICKET SUPPORT**
WWW.GETSMACK.DE (JUST FILE A TICKET)

DDoS - Cyberprzestępcy



DDoS - Cyberprzestępcy

Xtreme

70 - Linux Bots
12 - Attack Methods
Power - 10-12 Gbps (7mpps)
Concurrent Attacks - No
Recommended -
Home Conections/VPNS/
SITES/GAME SERVERS/
Protected sites

Monthly Price
\$450

Quaterly Price
\$650

Semi-Anualy Price
\$800

Lifetime Price
\$1000

Xtreme Fire

90 - Linux Bots
12 - Attack Methods
Power - 15-16 Gbps (10mpps)
Concurrent Attacks - No
Recommended -
Home Conections/VPNS/
SITES/GAME SERVERS/
Protected sites

Monthly Price
\$500

Quaterly Price
\$950

Semi-Anualy Price
\$1000

Lifetime Price
\$1200

Lifetime packages will have Lifetime warranty of replacement of bots. Monthly packages will have monthly warranty of Bots replacement warranty. We do provide tests before testing. Please reach us on skype for testing ips.s

DDoS - Obrona

- **DNS/NTP/SNMP/CHARGEN/(...) - ACL/OFF/Rate limit**
- **Plan działania (IT, PR, BOK, Odpowiedzialność)**
- **Komunikacja wewnętrzna**
- **Komunikacja z ISP/CERT/(...)**
- **Aktualizacje bezpieczeństwa**
- **Segmentacja usług/IP (DNS, CDN)**
- **no IP Spoofing**
- **WANGUARD, Arbor Networks, Prolexic, F5 CloudFlare, (...)**

URL

<http://krebsonsecurity.com/>

<http://openresolverproject.org/>

<http://pl.wikipedia.org/wiki/DDoS>

<http://pl.wikipedia.org/wiki/DoS>

<http://pl.wikipedia.org/wiki/DRDoS>

<https://code.google.com/p/dns-check/>

<http://atak-obrona.pl/>

<https://www.cloudflare.com/>

<https://www.shadowserver.org>

<http://www.arbornetworks.com/>

<http://www.ponemon.org/>

<http://www.prolexic.com/>

<http://www.spidersweb.pl/2013/04/allegro-ataki-ddos.html>

http://www.internetsociety.org/sites/default/files/01_5.pdf

<http://www.team-cymru.org/>



Dziękuję za uwagę

Borys Łacki

b.lacki@logicaltrust.net

