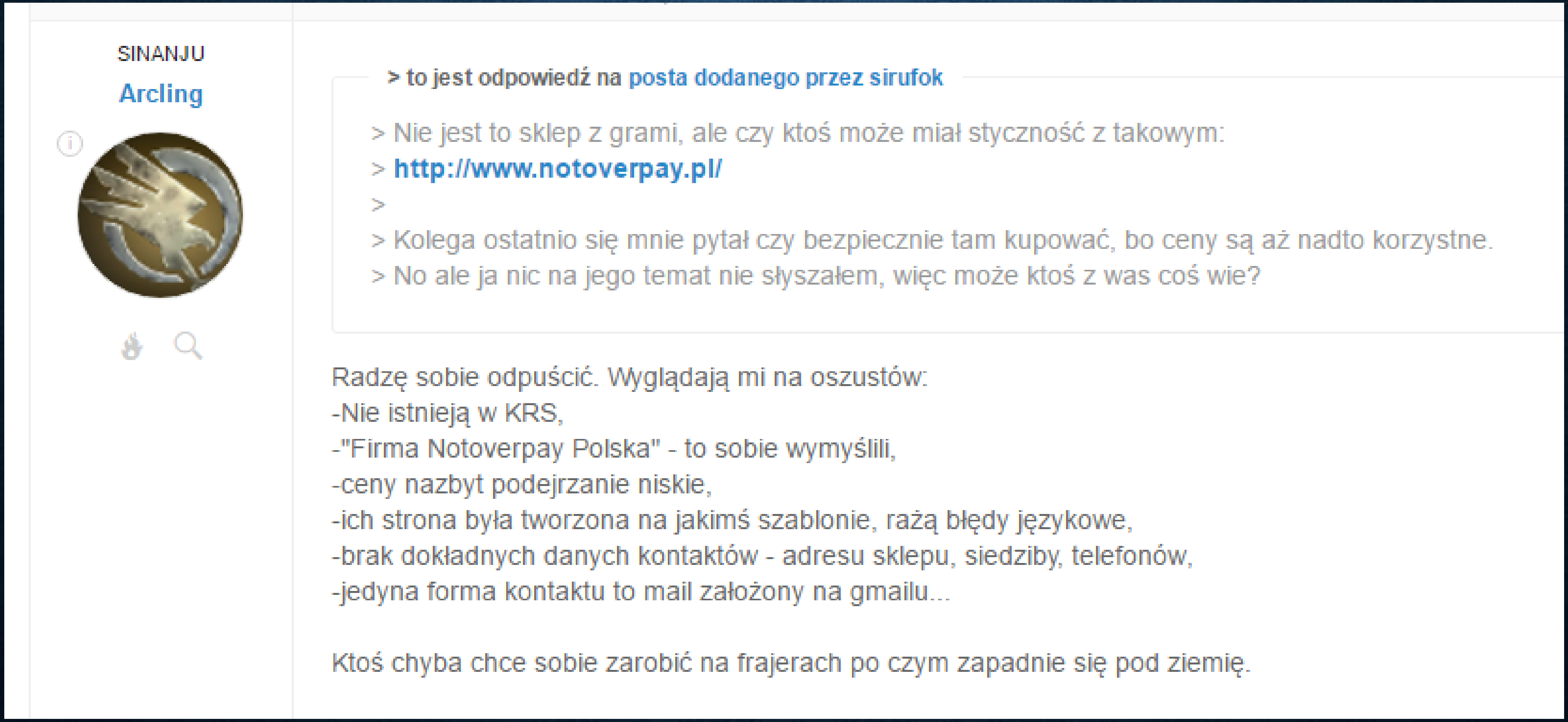
The Life Story of an IPT – Inept Persistent Threat Actor

Adam Haertlé, BadCyber.com

@badcybercom

@adamhaertle

„Company does not exist, prices are way too low, typos and language errors, no contact data…”



SINANJU

Arcling

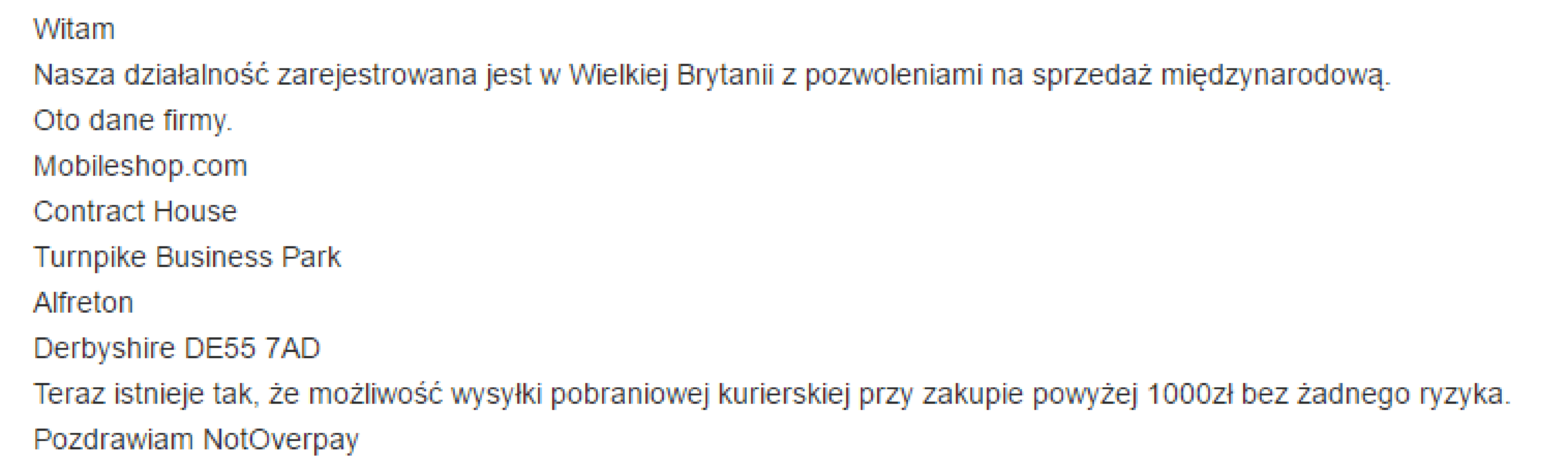
> to jest odpowiedź na posta dodanego przez sirufok

> Nie jest to sklep z grami, ale czy ktoś może miał styczność z takowym:
> http://www.notoverpay.pl/
>
> Kolega ostatnio się mnie pytał czy bezpiecznie tam kupować, bo ceny są aż nadto korzystne.
> No ale ja nic na jego temat nie słyszałem, więc może ktoś z was coś wie?

Radzę sobie odpuścić. Wyglądają mi na oszustów:
-Nie istnieją w KRS,
-"Firma Notoverpay Polska" - to sobie wymyślili,
-ceny nazbyt podejrzanie niskie,
-ich strona była tworzona na jakimś szablonie, rażą błędy językowe,
-brak dokładnych danych kontaktów - adresu sklepu, siedziby, telefonów,
-jedyna forma kontaktu to mail założony na gmailu...

Ktoś chyba chce sobie zarobić na frajerach po czym zapadnie się pod ziemię.

„We are a serious company registered in UK with licence for international sales, no risk!”



Witam

Nasza działalność zarejestrowana jest w Wielkiej Brytanii z pozwoleniami na sprzedaż międzynarodową.

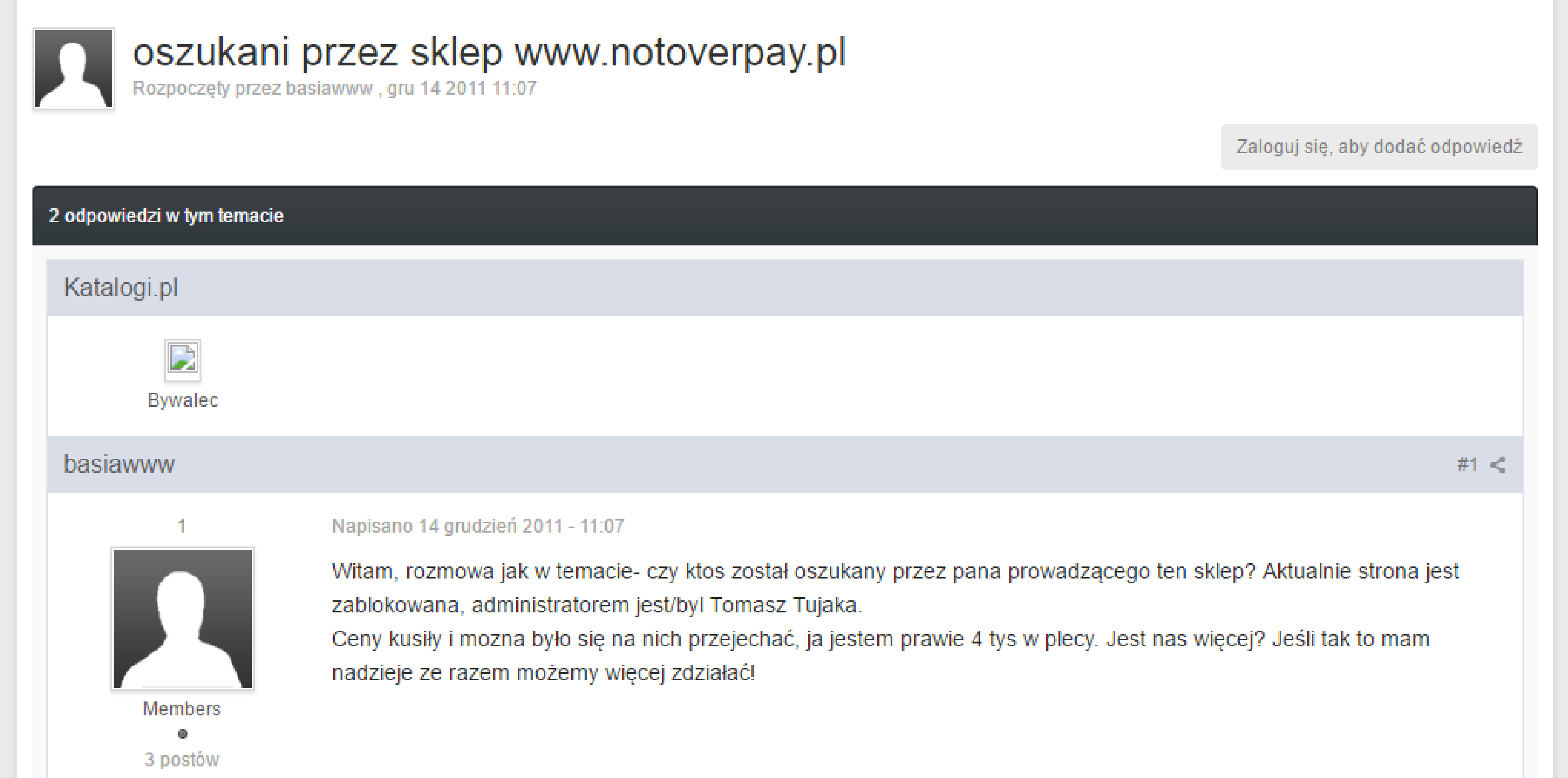
Oto dane firmy.

Mobileshop.com
Contract House
Turnpike Business Park
Alfreton
Derbyshire DE55 7AD

Teraz istnieje tak, że możliwość wysyłki pobraniowej kurierskiej przy zakupie powyżej 1000zł bez żadnego ryzyka.

Pozdrawiam NotOverpay

„I lost 1k EUR and the website administrator’s name was Tomasz Tujaka”



oszukani przez sklep www.notoverpay.pl

Rozpoczęty przez basiawww , gru 14 2011 11:07

Zaloguj się, aby dodać odpowiedź

2 odpowiedzi w tym temacie

Katalogi.pl

Bywalec

basiawww

#1

1

Napisano 14 grudzień 2011 - 11:07

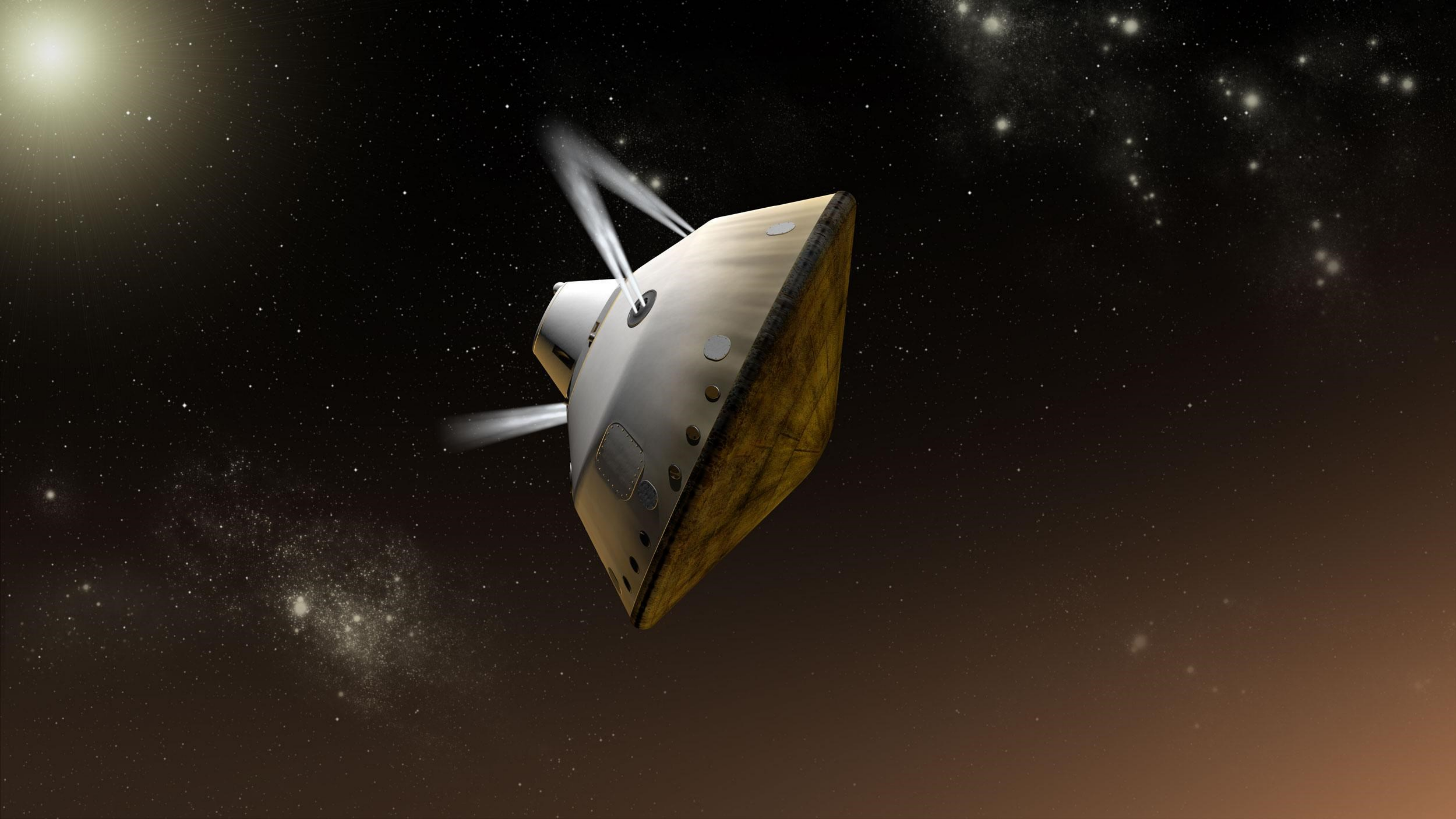
Witam, rozmowa jak w temacie- czy ktos został oszukany przez pana prowadzącego ten sklep? Aktualnie strona jest zablokowana, administratorem jest/byl Tomasz Tujaka.

Ceny kusiły i mozna było się na nich przejechać, ja jestem prawie 4 tys w plecy. Jest nas więcej? Jeśli tak to mam nadzieje ze razem możemy więcej zdziałać!

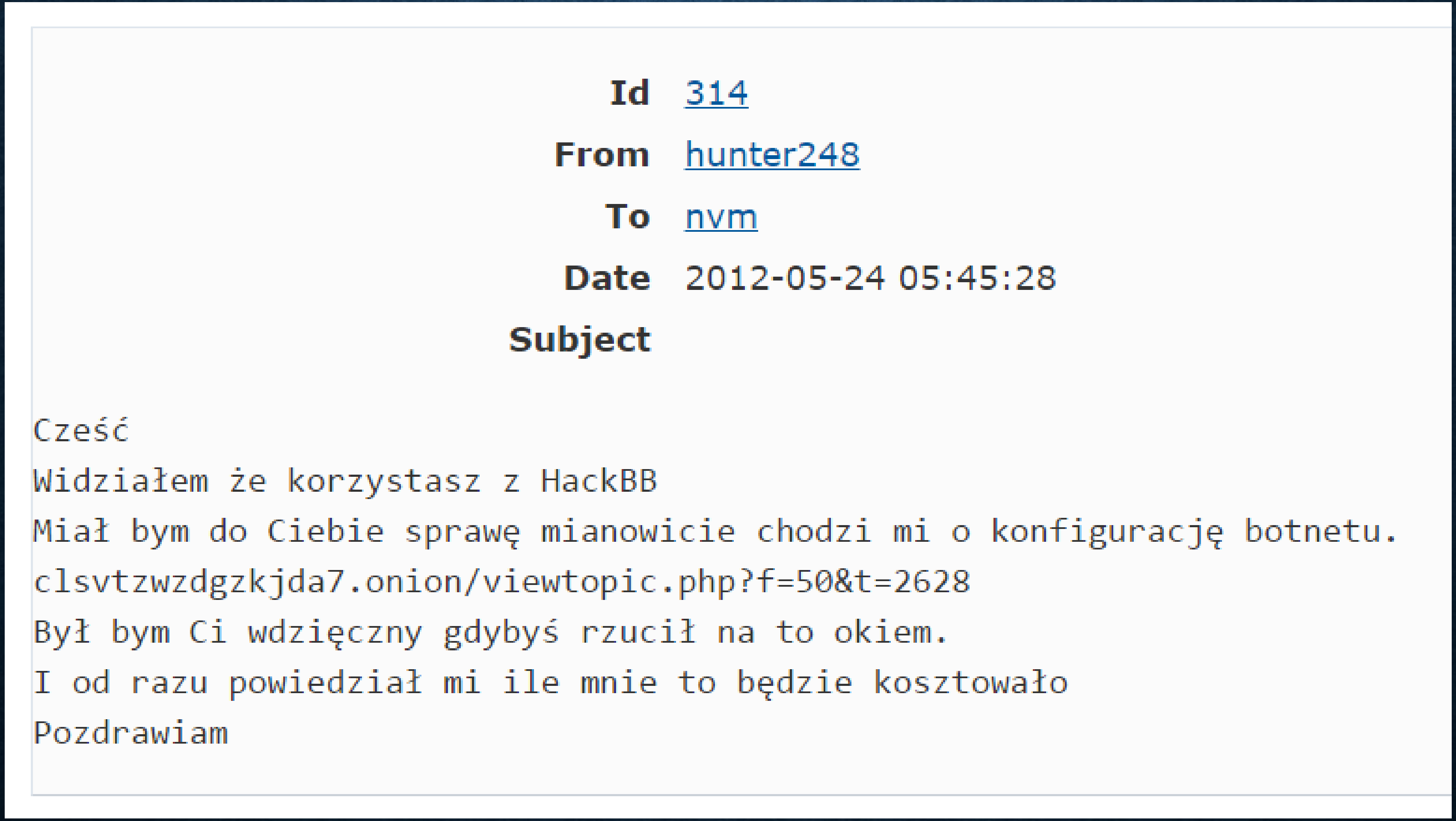
Members

•

3 postów



,,Please help me with botnet setup. How much would it cost?’’



Id 314

From hunter248

To nvm

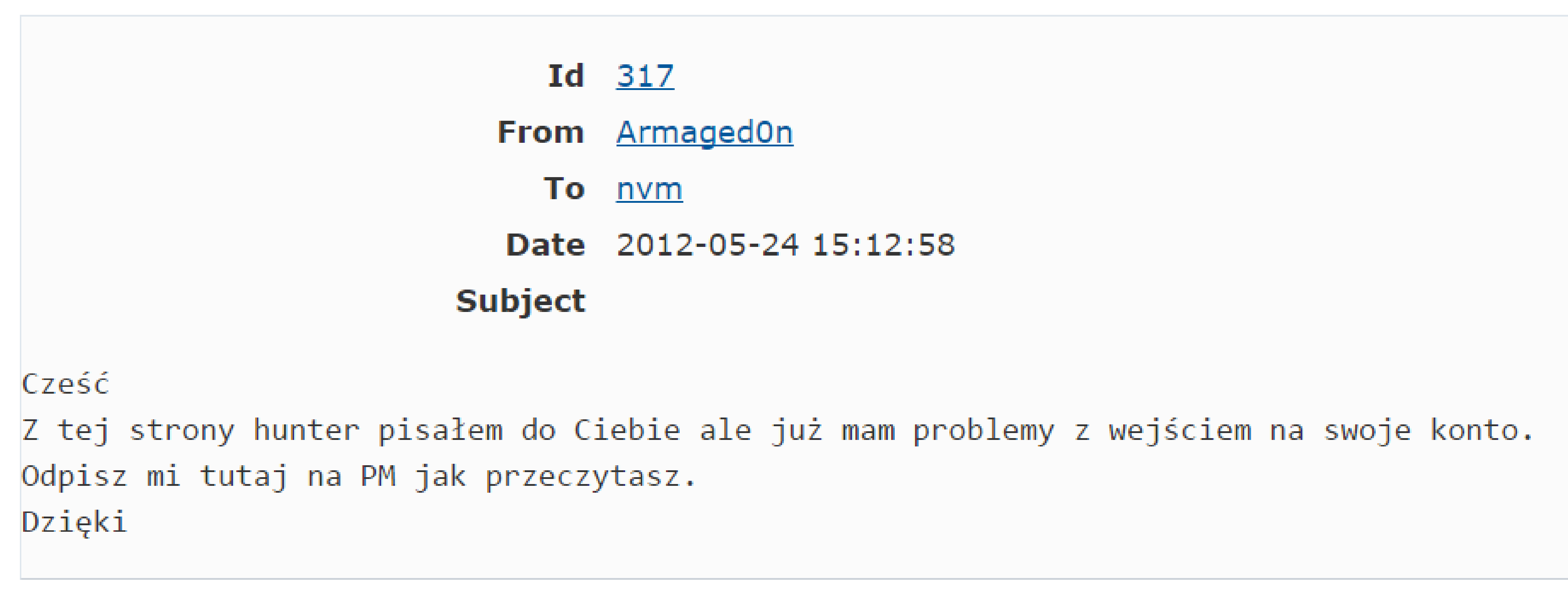
Date 2012-05-24 05:45:28

Subject

Cześć
Widziałem że korzystasz z HackBB
Miał bym do Ciebie sprawę mianowicie chodzi mi o konfigurację botnetu.
clsvtzwzdgzkjda7.onion/viewtopic.php?f=50&t=2628
Był bym Ci wdzięczny gdybyś rzucił na to okiem.
I od razu powiedział mi ile mnie to będzie kosztowało
Pozdrawiam

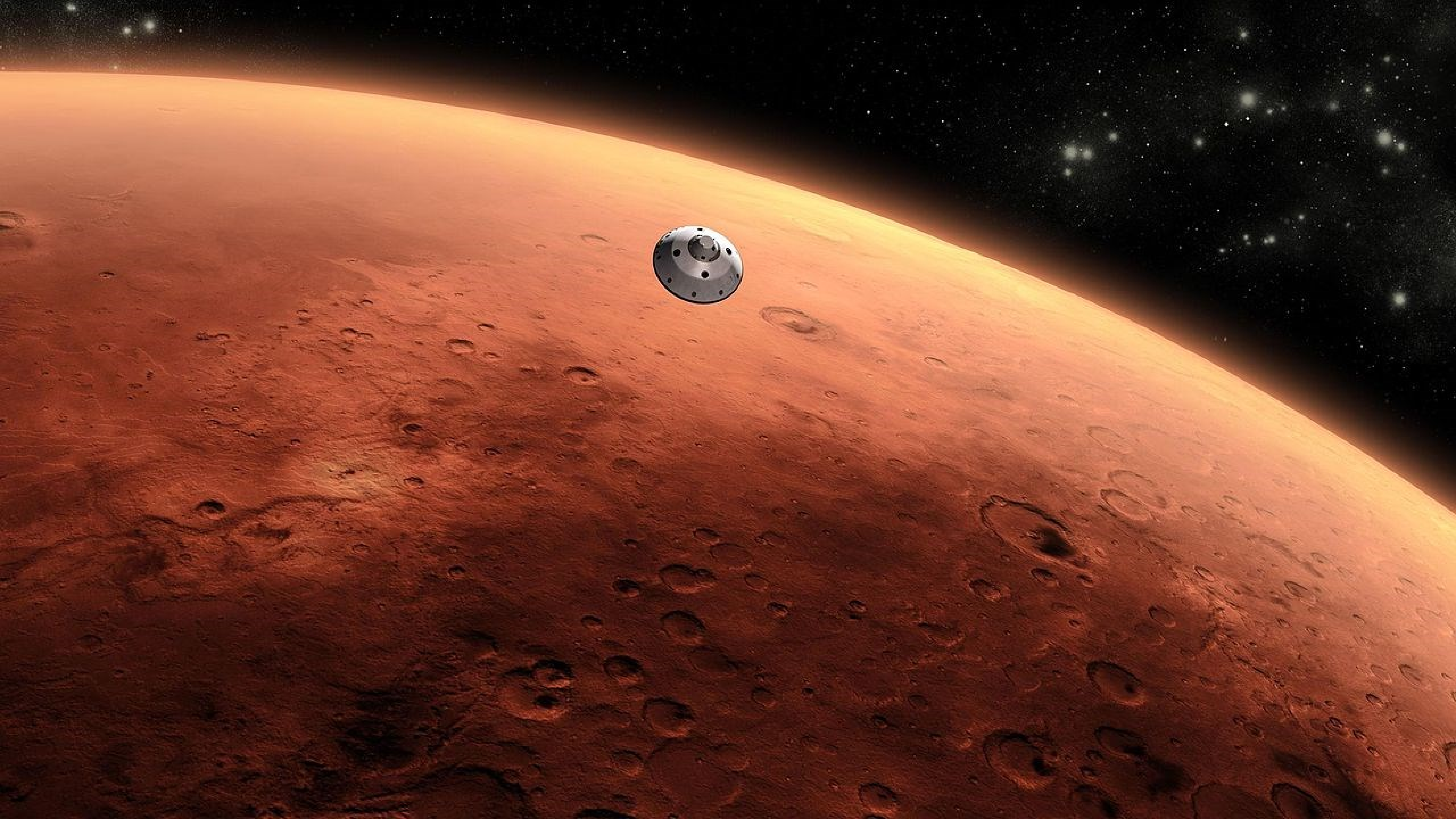
„This is hunter, lost access to my account”

Signed: Armaged0n

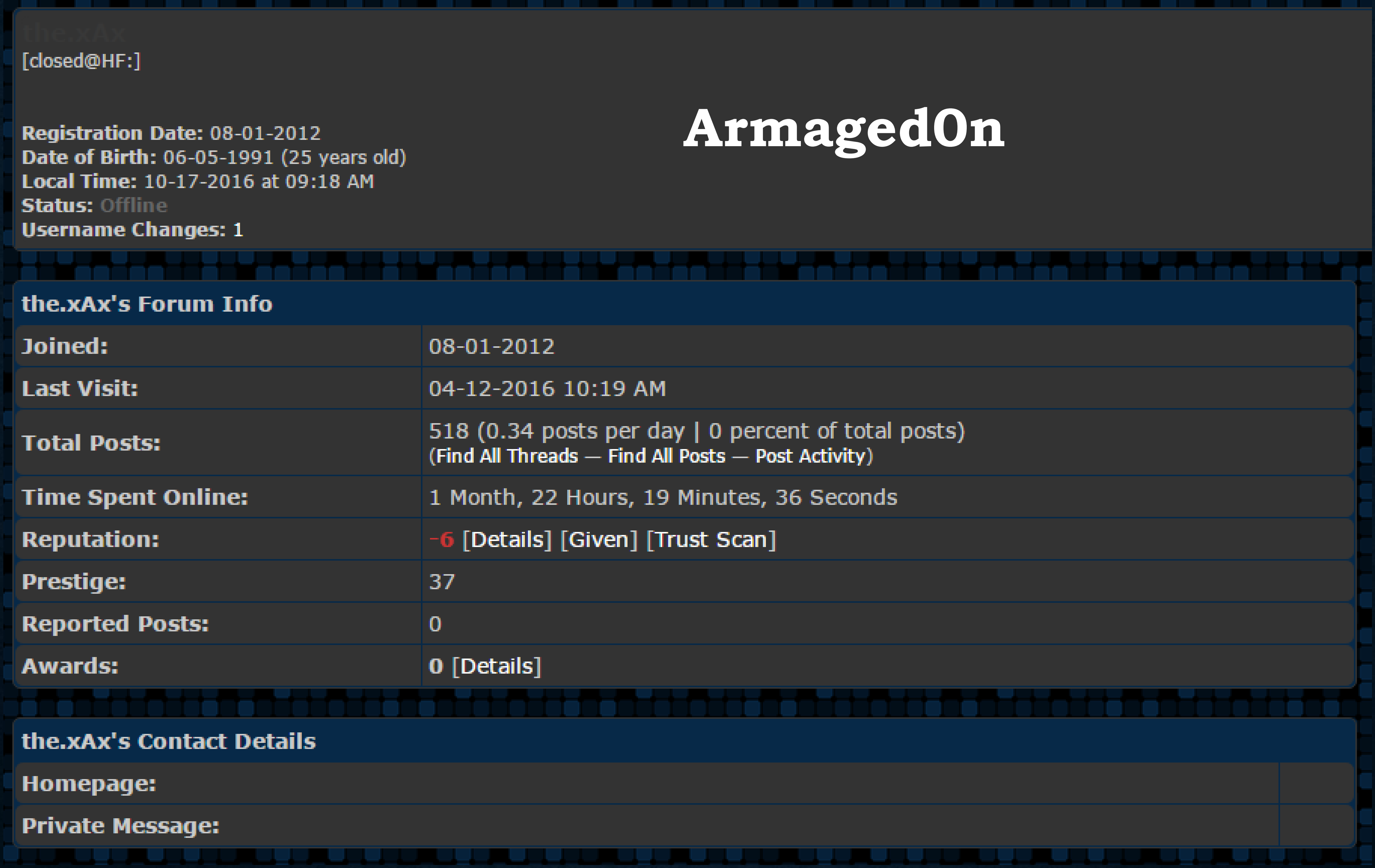


Id	317
From	Armaged0n
To	nvm
Date	2012-05-24 15:12:58
Subject	

Cześć
Z tej strony hunter pisałem do Ciebie ale już mam problemy z wejściem na swoje konto.
Odpisz mi tutaj na PM jak przeczytasz.
Dzięki



Armaged0n



the.xAx
[closed@HF:]

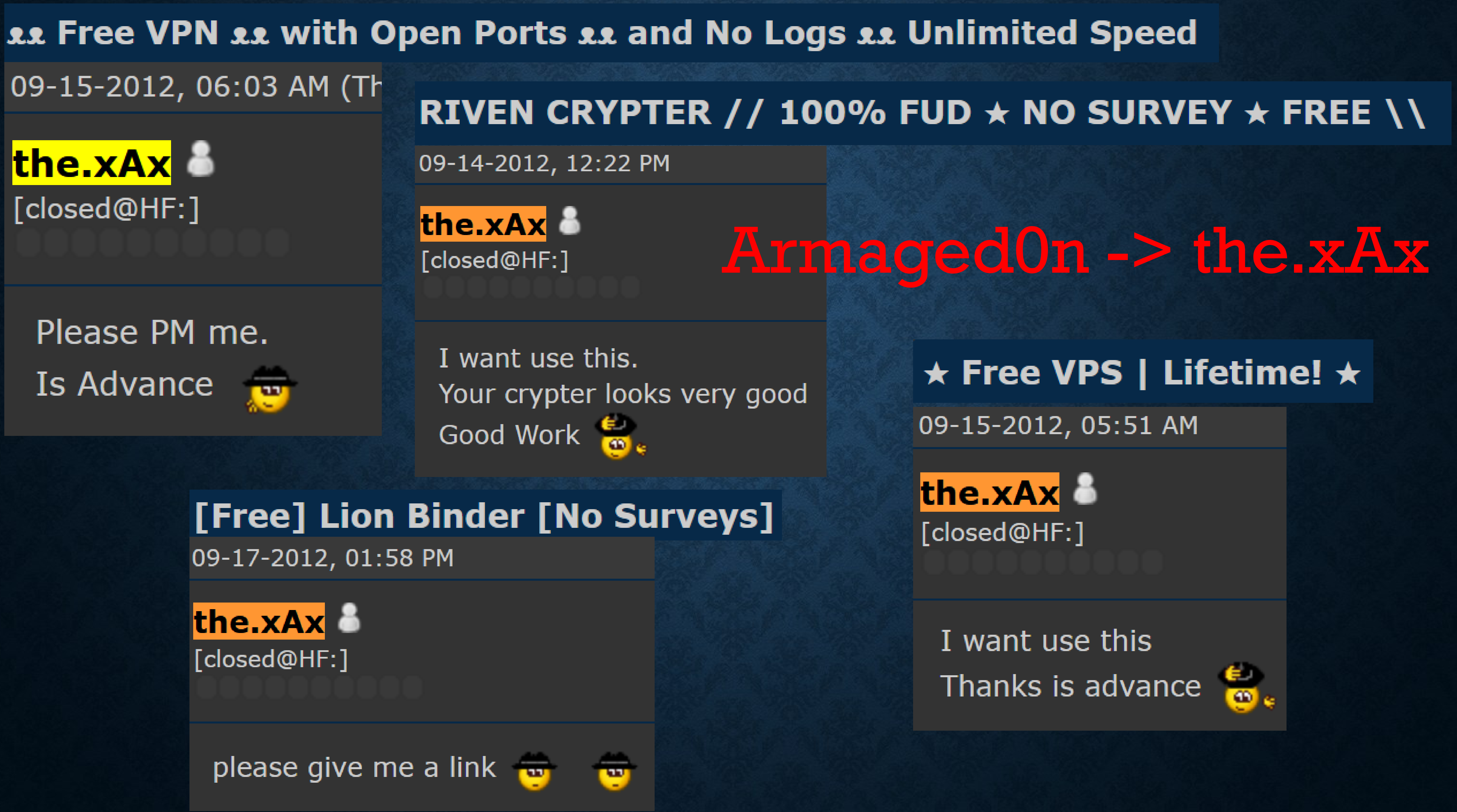
Registration Date: 08-01-2012
Date of Birth: 06-05-1991 (25 years old)
Local Time: 10-17-2016 at 09:18 AM
Status: Offline
Username Changes: 1

the.xAx's Forum Info

Joined:	08-01-2012
Last Visit:	04-12-2016 10:19 AM
Total Posts:	518 (0.34 posts per day | 0 percent of total posts) (Find All Threads — Find All Posts — Post Activity)
Time Spent Online:	1 Month, 22 Hours, 19 Minutes, 36 Seconds
Reputation:	-6 [Details] [Given] [Trust Scan]
Prestige:	37
Reported Posts:	0
Awards:	**0** [Details]

the.xAx's Contact Details

Homepage:	
Private Message:	



ஐஐ Free VPN ஐஐ with Open Ports ஐஐ and No Logs ஐஐ Unlimited Speed

09-15-2012, 06:03 AM (Th

the.xAx

[closed@HF:]

Please PM me.

Is Advance

RIVEN CRYPTER // 100% FUD ★ NO SURVEY ★ FREE \\

09-14-2012, 12:22 PM

the.xAx

[closed@HF:]

I want use this.

Your crypter looks very good

Good Work

Armaged0n -> the.xAx

★ Free VPS | Lifetime! ★

09-15-2012, 05:51 AM

the.xAx

[closed@HF:]

I want use this

Thanks is advance

[Free] Lion Binder [No Surveys]

09-17-2012, 01:58 PM

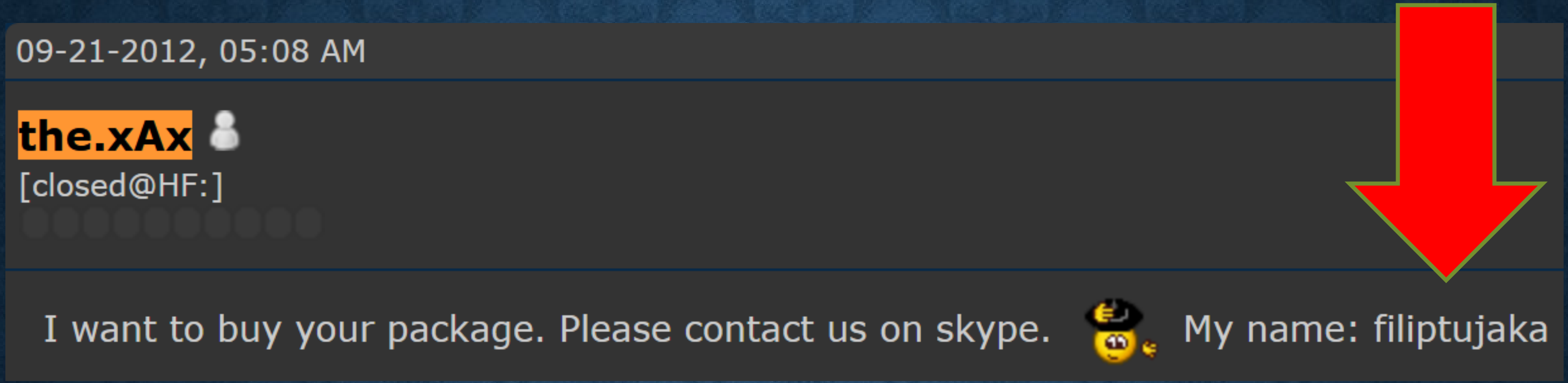
the.xAx

[closed@HF:]

please give me a link

INPUT
STO
RCL
DSP
PRT
EXIT
CLR
ENTER
Investment
Value at Year end
339 970
373 967
804 029
1 296 731
1 859 317
2 499 808
3 227 076
4 050 935
R 28 331
Investment
Value at Year end
424 963
446 211
468 522
491 948
516 545
542 372
569 491
467 459
1 005 037
1 620 915
2 324 149
3 124 764
4 033 850
5 063 675
R 35 414
Start at monthly
Can we do this?

Botnet Setup - FULL PACKAGE (Athena & IRC spot)



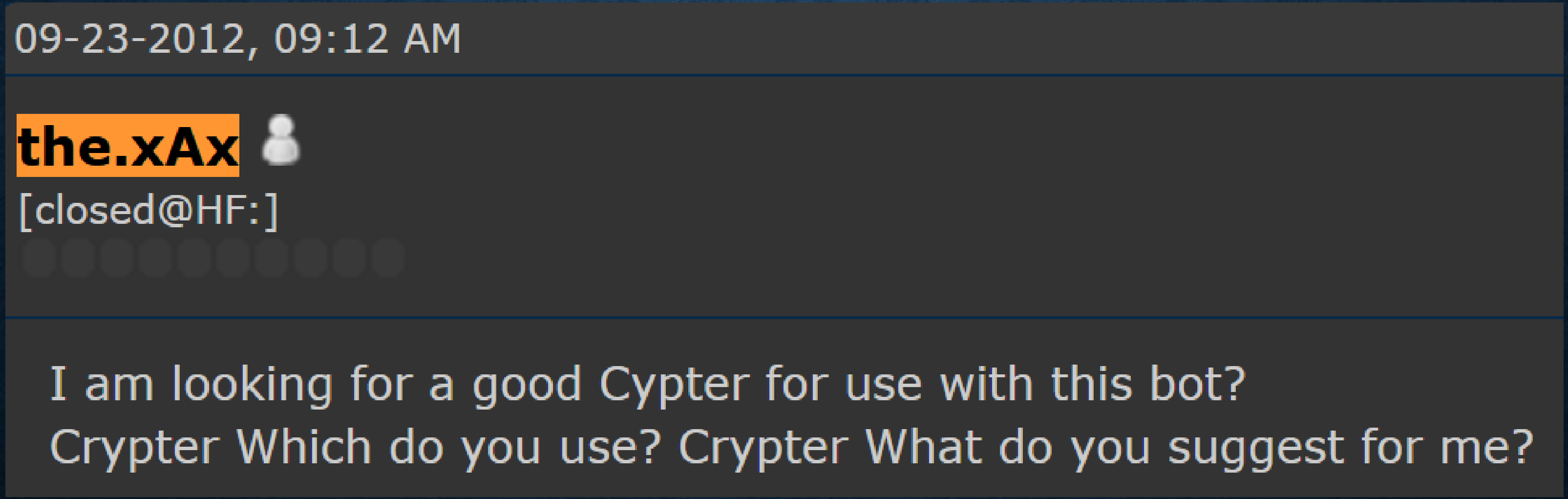
09-21-2012, 05:08 AM

the.xAx

[closed@HF:]

I want to buy your package. Please contact us on skype. My name: filiptujaka

Crypter for Athena IRC Botnet

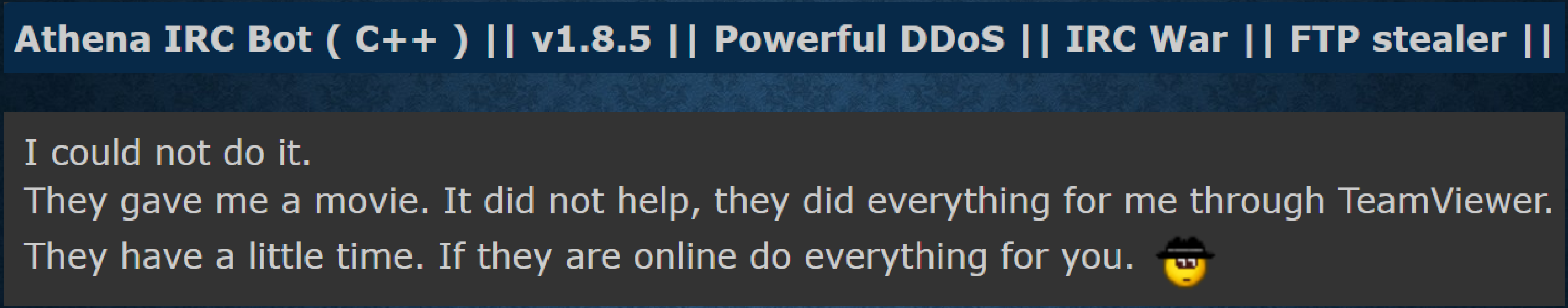


09-23-2012, 09:12 AM

the.xAx

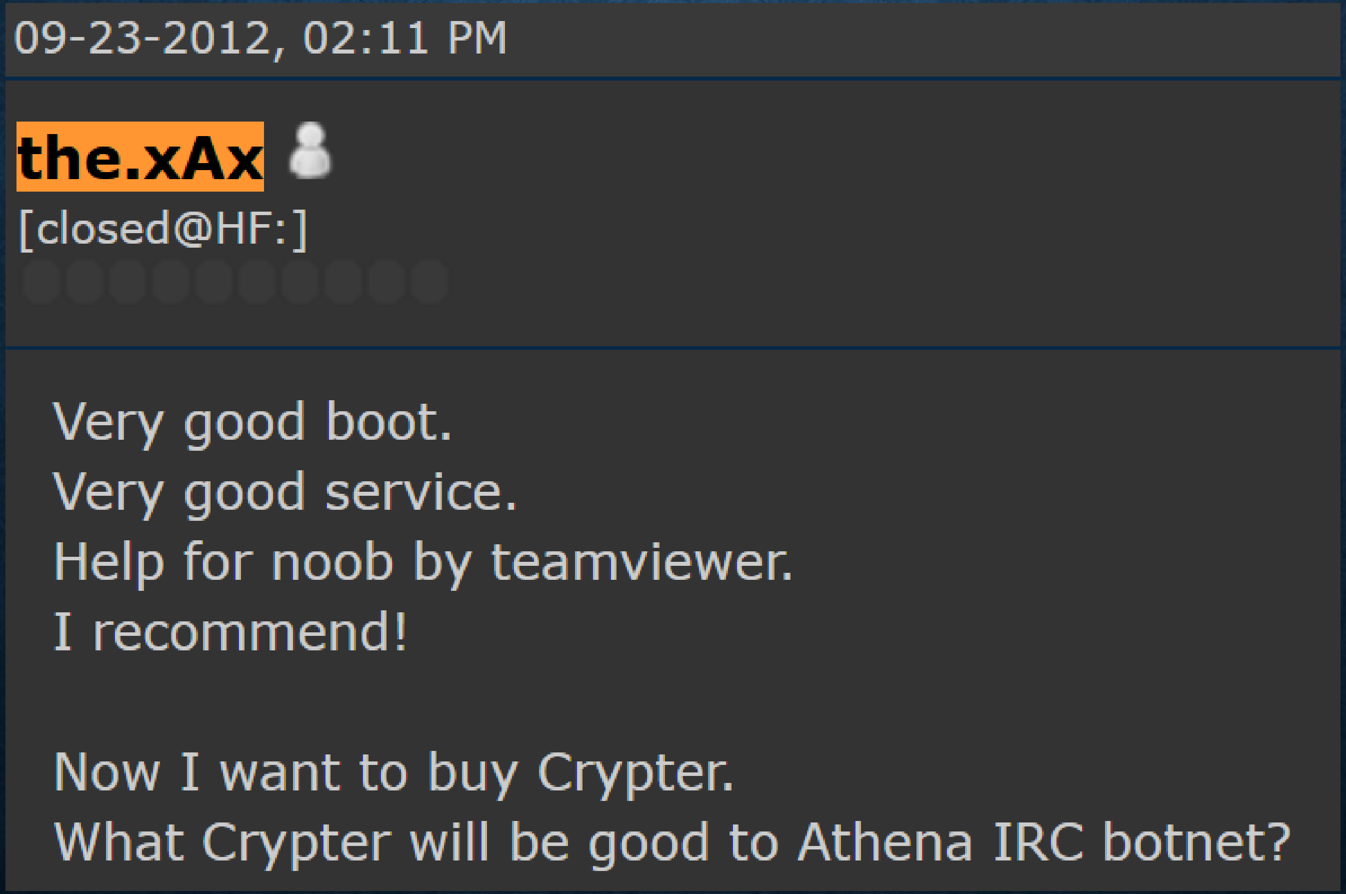
[closed@HF:]

I am looking for a good Cypter for use with this bot?
Crypter Which do you use? Crypter What do you suggest for me?



Athena IRC Bot (C++) || v1.8.5 || Powerful DDoS || IRC War || FTP stealer ||

I could not do it.
They gave me a movie. It did not help, they did everything for me through TeamViewer.
They have a little time. If they are online do everything for you.



09-23-2012, 02:11 PM

the.xAx
[closed@HF:]

Very good boot.
Very good service.
Help for noob by teamviewer.
I recommend!

Now I want to buy Crypter.
What Crypter will be good to Athena IRC botnet?

Dear User Kaspersky Lab says a bilion computers is threaned by a virus attack.

The attack can be performer by a vulnerability we doscovered in most popular browsers (including Mozilla Firefox, Google Chrome, Opera). Thousand of computers all around the world have been hacked over the last few hours.

To check if your browser is vulnerable please visit http://safe-browser.tk.

In case its needed install the updates!

Best regards Kaspersky Lab

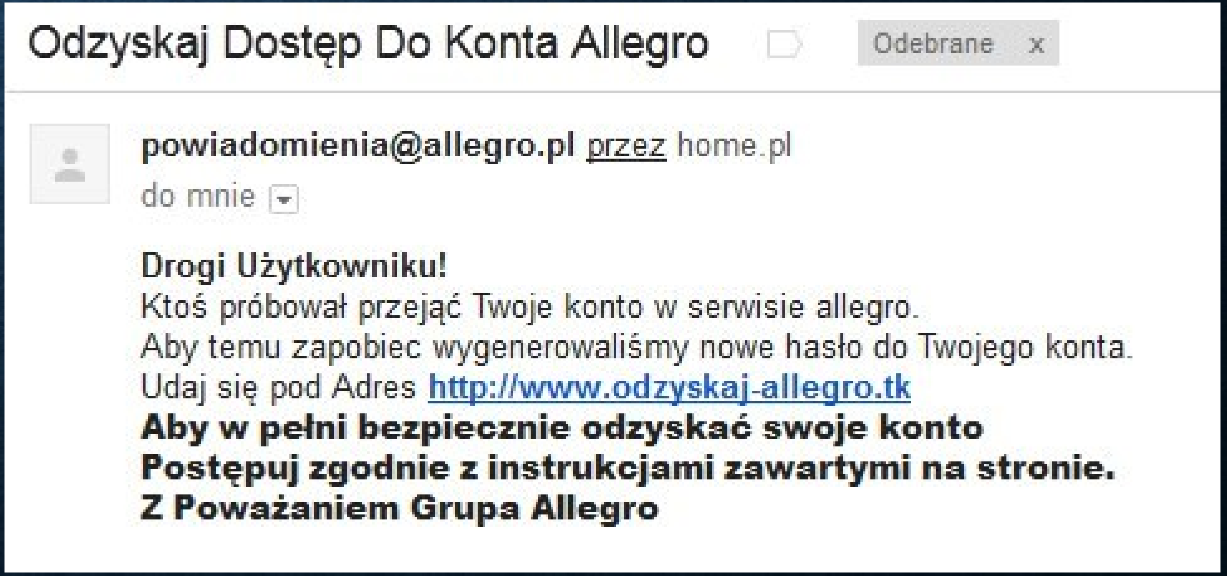
Dear User!

Someone tried to take over your Allegro account. We created a new password to block the attacker. You can recover it by going to

http://www.recover-allegro.tk

To securely recover your account follow the instructions.

Best regards Allegro Group

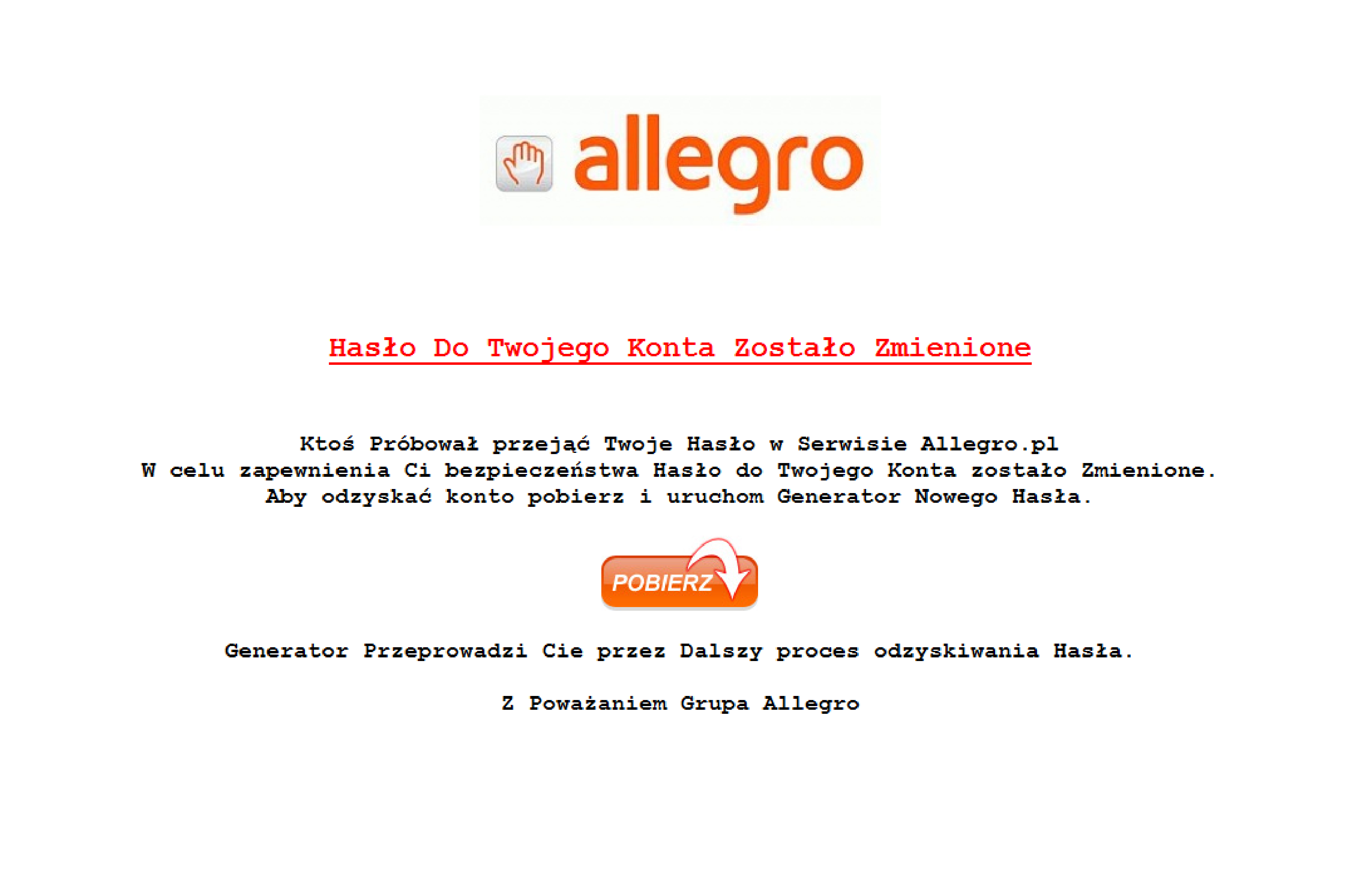


Odzyskaj Dostęp Do Konta Allegro

powiadomienia@allegro.pl przez home.pl
do mnie

Drogi Użytkowniku!
Ktoś próbował przejąć Twoje konto w serwisie allegro.
Aby temu zapobiec wygenerowaliśmy nowe hasło do Twojego konta.
Udaj się pod Adres http://www.odzyskaj-allegro.tk
Aby w pełni bezpiecznie odzyskać swoje konto
Postępuj zgodnie z instrukcjami zawartymi na stronie.
Z Poważaniem Grupa Allegro

„Download New Password Generator”

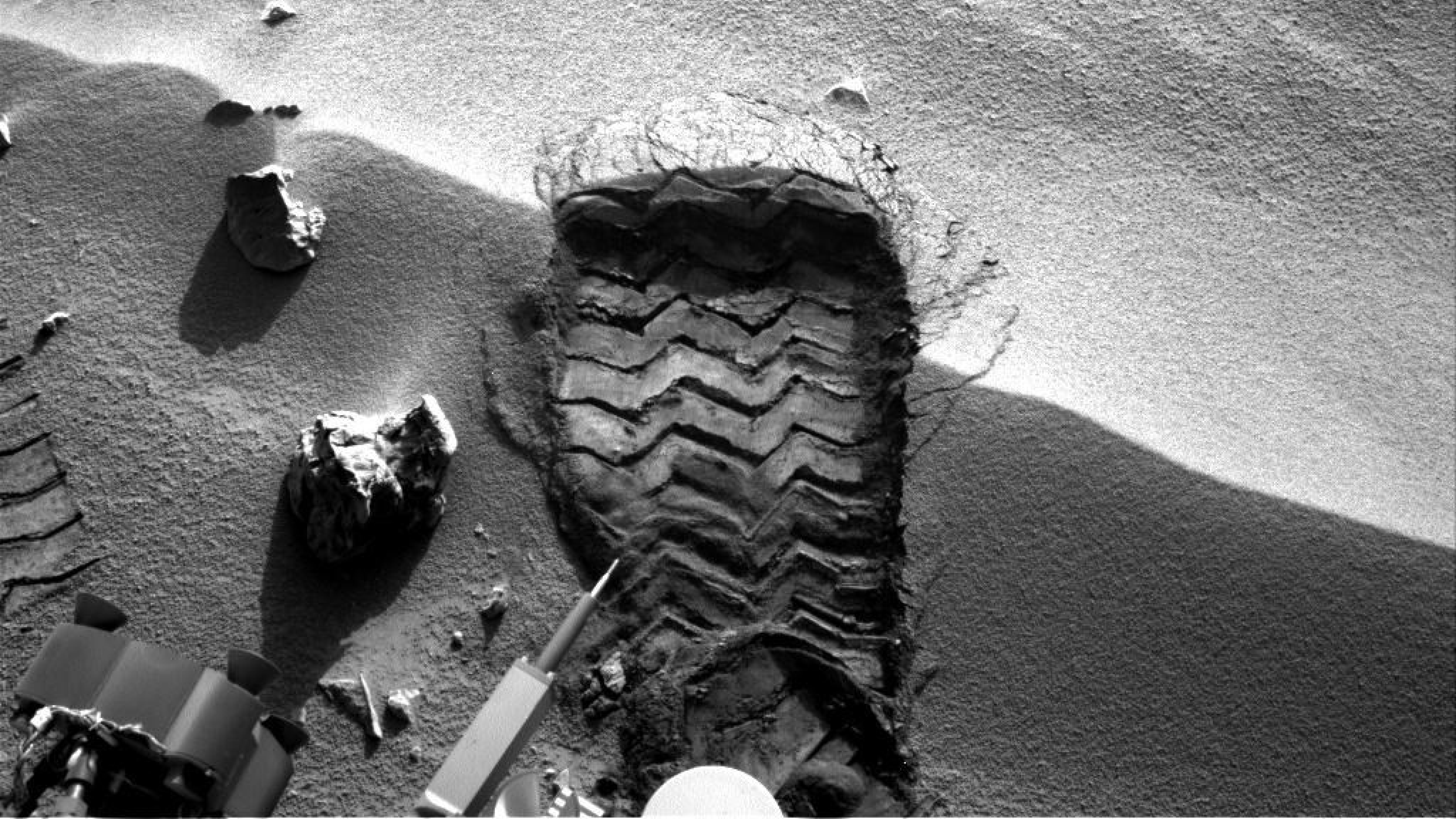


Hasło Do Twojego Konta Zostało Zmienione

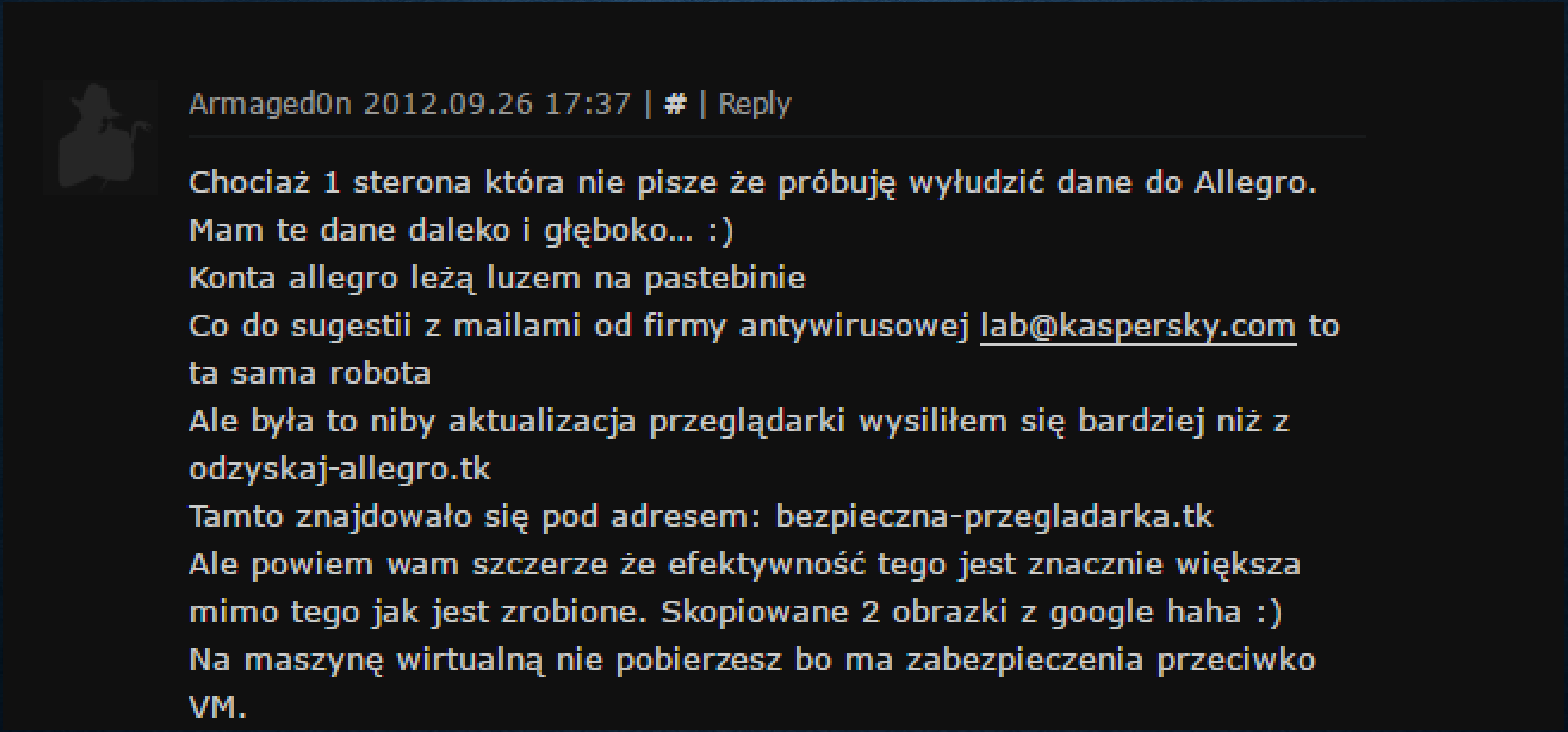
Ktoś Próbował przejąć Twoje Hasło w Serwisie Allegro.pl
W celu zapewnienia Ci bezpieczeństwa Hasło do Twojego Konta zostało Zmienione.
Aby odzyskać konto pobierz i uruchom Generator Nowego Hasła.

Generator Przeprowadzi Cie przez Dalszy proces odzyskiwania Hasła.

Z Poważaniem Grupa Allegro



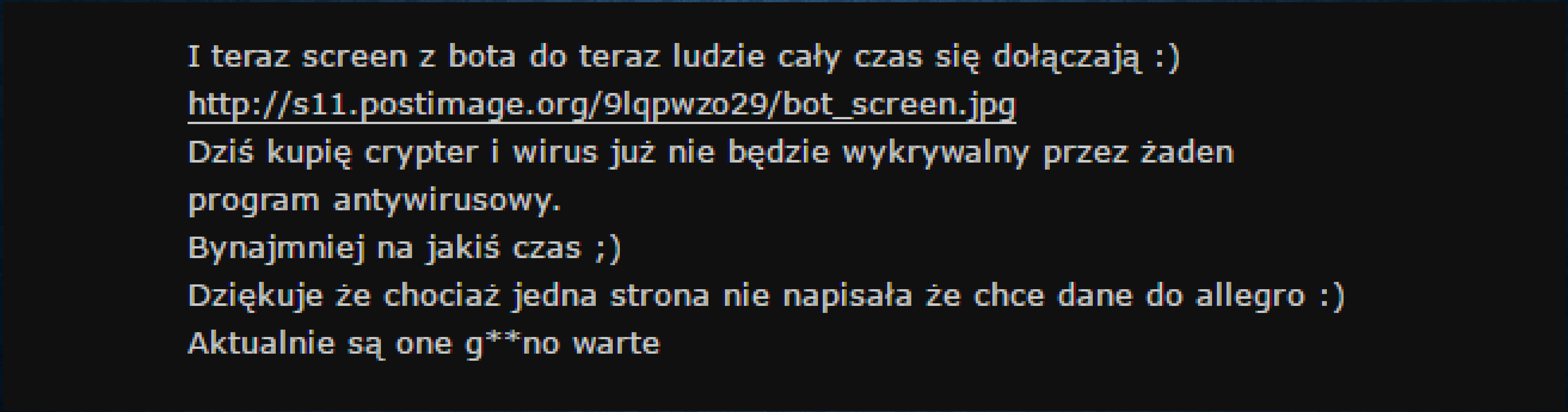
„Kaspersky and Allegro was my job. Just copied two pictures from Google.”



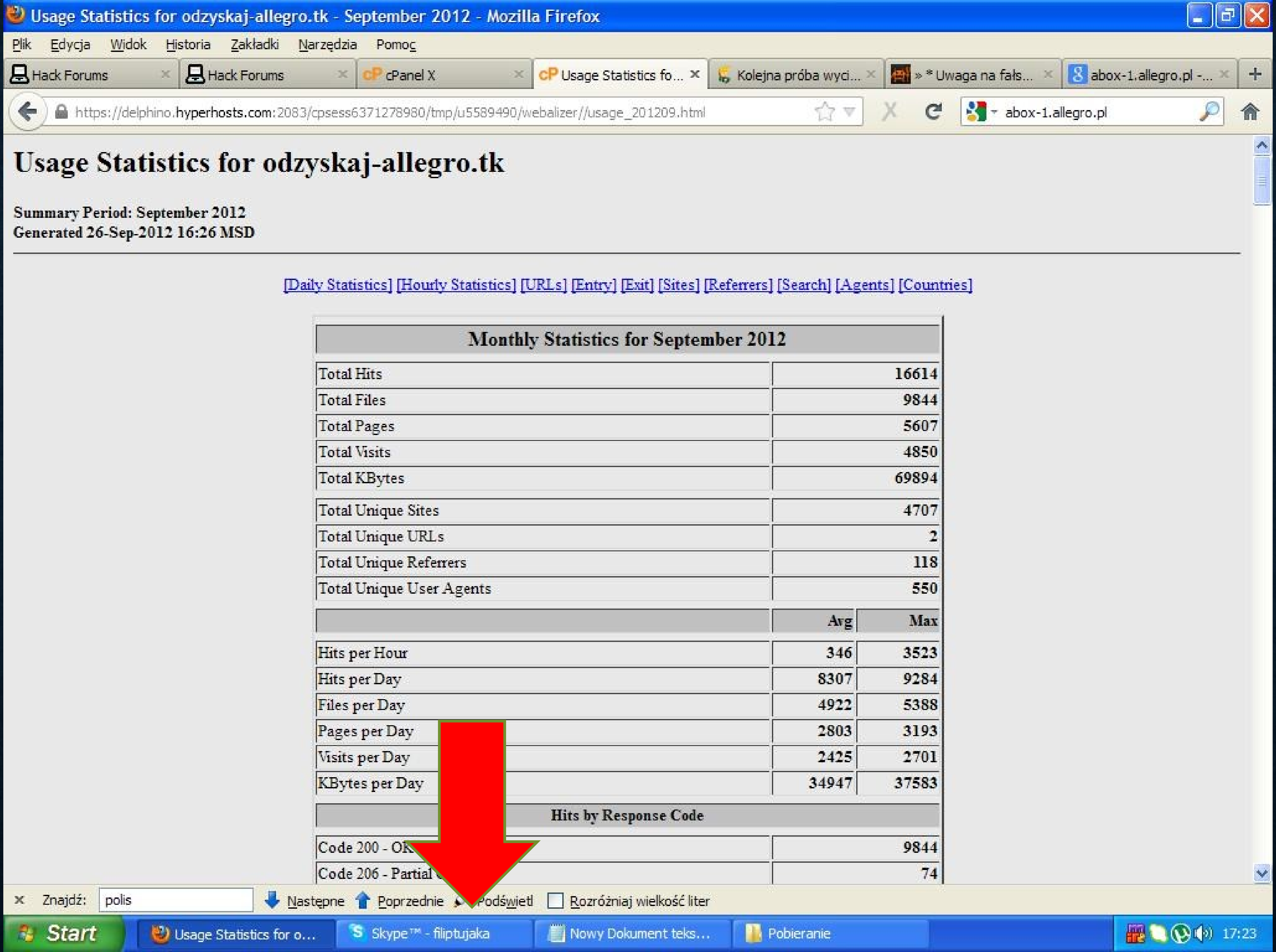
Armaged0n 2012.09.26 17:37 | # | Reply

Chociaż 1 sterona która nie pisze że próbuję wyłudzić dane do Allegro.
Mam te dane daleko i głęboko... :)
Konta allegro leżą luzem na pastebinie
Co do sugestii z mailami od firmy antywirusowej lab@kaspersky.com to ta sama robota
Ale była to niby aktualizacja przeglądarki wysiliłem się bardziej niż z odzyskaj-allegro.tk
Tamto znajdowało się pod adresem: bezpieczna-przegladarka.tk
Ale powiem wam szczerze że efektywność tego jest znacznie większa mimo tego jak jest zrobione. Skopiowane 2 obrazki z google haha :)
Na maszynę wirtualną nie pobierzesz bo ma zabezpieczenia przeciwko VM.

„Screen from my bot, people keep joining. I’ll buy a crypter today to avoid AV.”



I teraz screen z bota do teraz ludzie cały czas się dołączają :)
http://s11.postimage.org/9lqpwzo29/bot_screen.jpg
Dziś kupię crypter i wirus już nie będzie wykrywalny przez żaden program antywirusowy.
Bynajmniej na jakiś czas ;)
Dziękuje że chociaż jedna strona nie napisała że chce dane do allegro :)
Aktualnie są one g**no warte

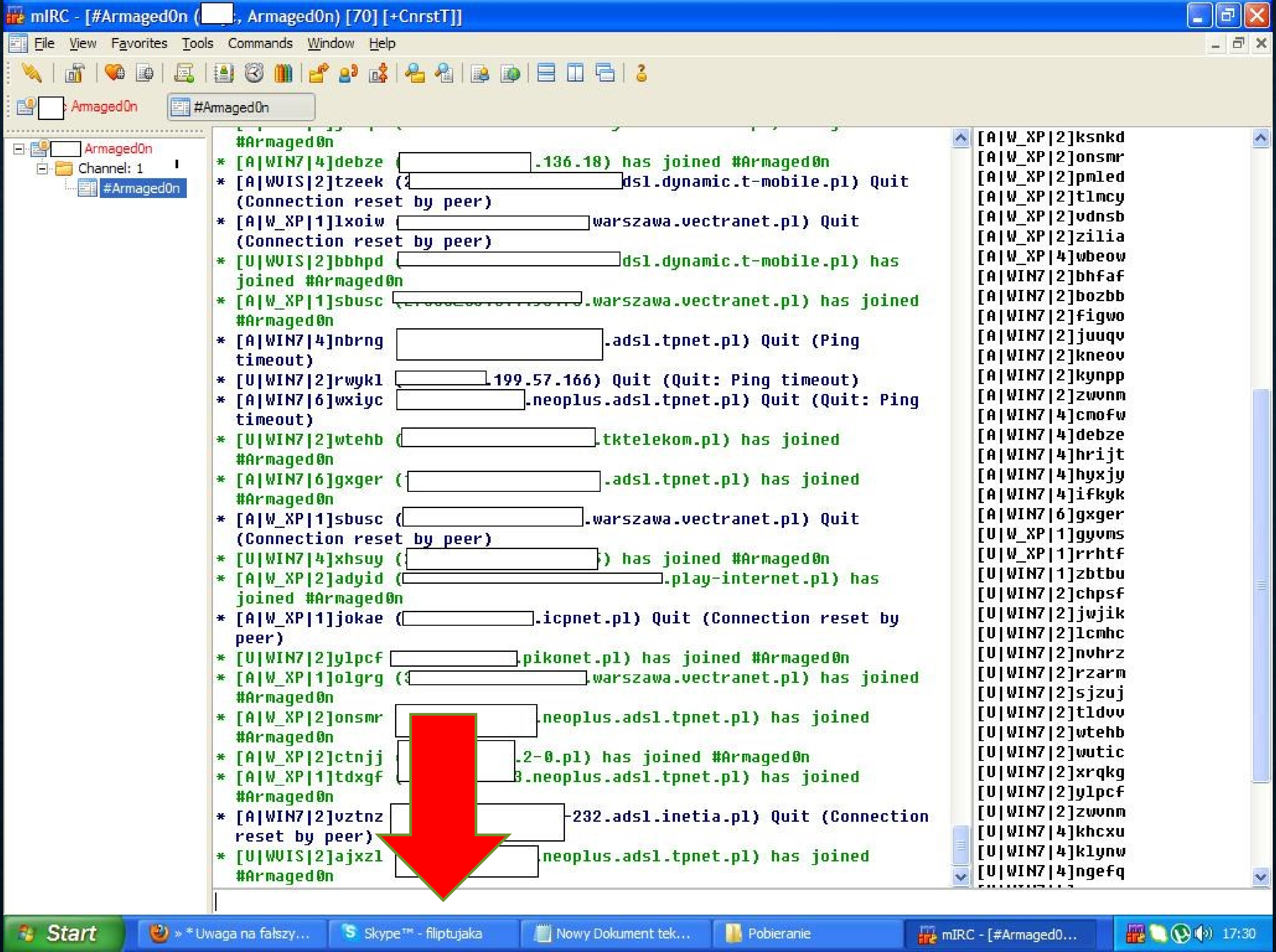


Usage Statistics for odzyskaj-allegro.tk

Summary Period: September 2012
Generated 26-Sep-2012 16:26 MSD

[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

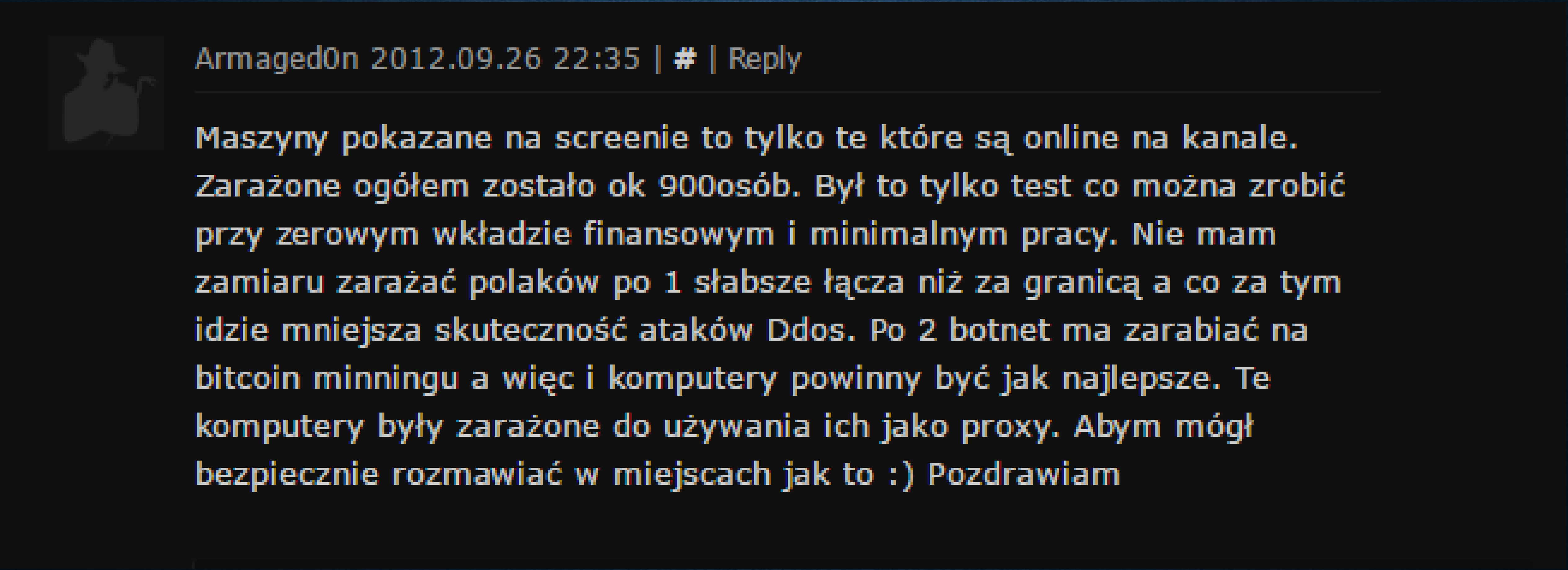
Monthly Statistics for September 2012		
Total Hits		16614
Total Files		9844
Total Pages		5607
Total Visits		4850
Total KBytes		69894
Total Unique Sites		4707
Total Unique URLs		2
Total Unique Referrers		118
Total Unique User Agents		550
	Avg	Max
Hits per Hour	346	3523
Hits per Day	8307	9284
Files per Day	4922	5388
Pages per Day	2803	3193
Visits per Day	2425	2701
KBytes per Day	34947	37583
Hits by Response Code		
Code 200 - OK		9844
Code 206 - Partial		74



```
#Armaged0n
* [A|WIN7|4]debze ([redacted].136.18) has joined #Armaged0n
* [A|WVIS|2]tzeek ([redacted]dsl.dynamic.t-mobile.pl) Quit
(Connection reset by peer)
* [A|W_XP|1]lxoiw ([redacted]warszawa.vectranet.pl) Quit
(Connection reset by peer)
* [U|WVIS|2]bbhpd ([redacted]dsl.dynamic.t-mobile.pl) has
joined #Armaged0n
* [A|W_XP|1]sbusc [redacted].warszawa.vectranet.pl) has joined
#Armaged0n
* [A|WIN7|4]nbrng [redacted].adsl.tpnet.pl) Quit (Ping
timeout)
* [U|WIN7|2]rwykl [redacted].199.57.166) Quit (Quit: Ping timeout)
* [A|WIN7|6]wxiyc [redacted].neoplus.adsl.tpnet.pl) Quit (Quit: Ping
timeout)
* [U|WIN7|2]wtehb ([redacted].tktelekom.pl) has joined
#Armaged0n
* [A|WIN7|6]gxger ([redacted].adsl.tpnet.pl) has joined
#Armaged0n
* [A|W_XP|1]sbusc ([redacted].warszawa.vectranet.pl) Quit
(Connection reset by peer)
* [U|WIN7|4]xhsuy ([redacted]) has joined #Armaged0n
* [A|W_XP|2]adyid ([redacted].play-internet.pl) has
joined #Armaged0n
* [A|W_XP|1]jokae ([redacted].icpnet.pl) Quit (Connection reset by
peer)
* [U|WIN7|2]ylpcf [redacted].pikonet.pl) has joined #Armaged0n
* [A|W_XP|1]olgrg ([redacted].warszawa.vectranet.pl) has joined
#Armaged0n
* [A|W_XP|2]onsmr [redacted].neoplus.adsl.tpnet.pl) has joined
#Armaged0n
* [A|W_XP|2]ctnjj [redacted].2-0.pl) has joined #Armaged0n
* [A|W_XP|1]tdxgf [redacted]3.neoplus.adsl.tpnet.pl) has joined
#Armaged0n
* [A|WIN7|2]vztnz [redacted]-232.adsl.inetia.pl) Quit (Connection
reset by peer)
* [U|WVIS|2]ajxzl [redacted].neoplus.adsl.tpnet.pl) has joined
#Armaged0n
```

```
[A|W_XP|2]ksnkd
[A|W_XP|2]onsmr
[A|W_XP|2]pmled
[A|W_XP|2]tlmcy
[A|W_XP|2]vdnsb
[A|W_XP|2]zilia
[A|W_XP|4]wbeow
[A|WIN7|2]bhfaf
[A|WIN7|2]bozbb
[A|WIN7|2]figwo
[A|WIN7|2]juuqv
[A|WIN7|2]kneov
[A|WIN7|2]kynpp
[A|WIN7|2]zwvnm
[A|WIN7|4]cmofw
[A|WIN7|4]debze
[A|WIN7|4]hrijt
[A|WIN7|4]hyxjy
[A|WIN7|4]ifkyk
[A|WIN7|6]gxger
[U|W_XP|1]gyvms
[U|W_XP|1]rrhtf
[U|WIN7|1]zbtbu
[U|WIN7|2]chpsf
[U|WIN7|2]jwjik
[U|WIN7|2]lcmhc
[U|WIN7|2]nvhrz
[U|WIN7|2]rzarm
[U|WIN7|2]sjzuj
[U|WIN7|2]tldvv
[U|WIN7|2]wtehb
[U|WIN7|2]wutic
[U|WIN7|2]xrqkg
[U|WIN7|2]ylpcf
[U|WIN7|2]zwvnm
[U|WIN7|4]khcxu
[U|WIN7|4]klynw
[U|WIN7|4]ngefq
```

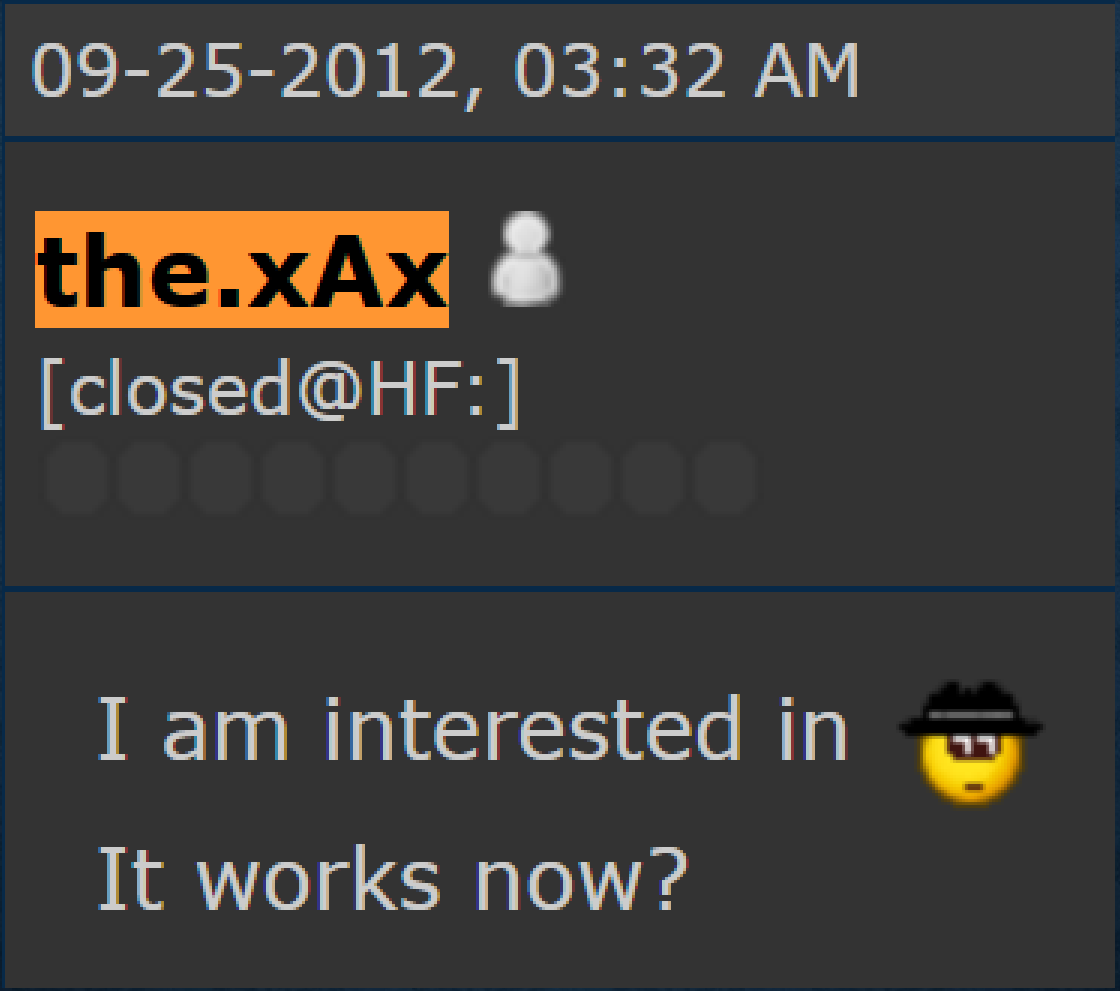
„900 infections. I'll mine bitcoin with it and use it as proxy to talk in places like this."



Armaged0n 2012.09.26 22:35 | # | Reply

Maszyny pokazane na screenie to tylko te które są online na kanale. Zarażone ogółem zostało ok 900osób. Był to tylko test co można zrobić przy zerowym wkładzie finansowym i minimalnym pracy. Nie mam zamiaru zarażać polaków po 1 słabsze łącza niż za granicą a co za tym idzie mniejsza skuteczność ataków Ddos. Po 2 botnet ma zarabiać na bitcoin minningu a więc i komputery powinny być jak najlepsze. Te komputery były zarażone do używania ich jako proxy. Abym mógł bezpiecznie rozmawiać w miejscach jak to :) Pozdrawiam

cheapMiner | Bitcoin Miner | Autobuy | Coded in C | No Dependencies | Builder | 1$



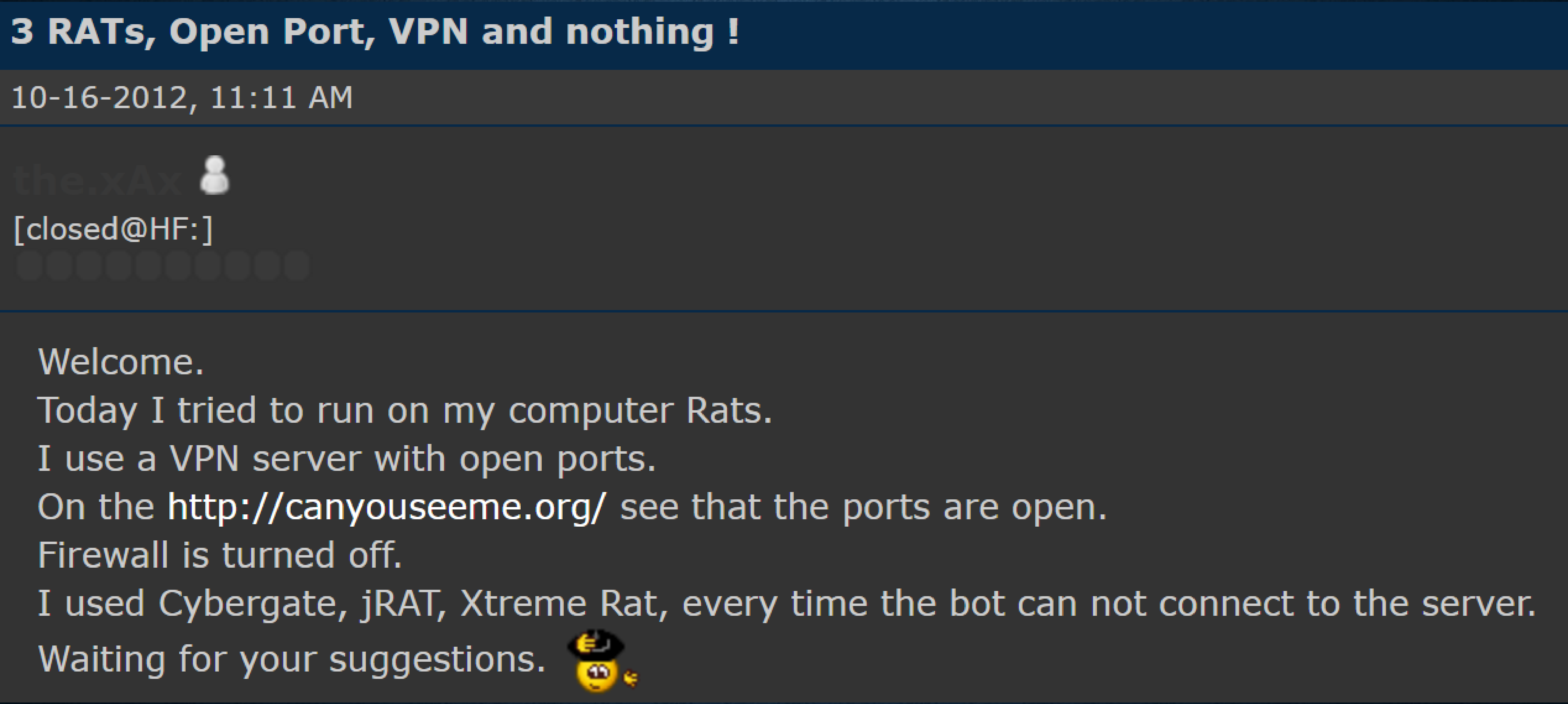
09-25-2012, 03:32 AM

the.xAx

[closed@HF:]

I am interested in

It works now?



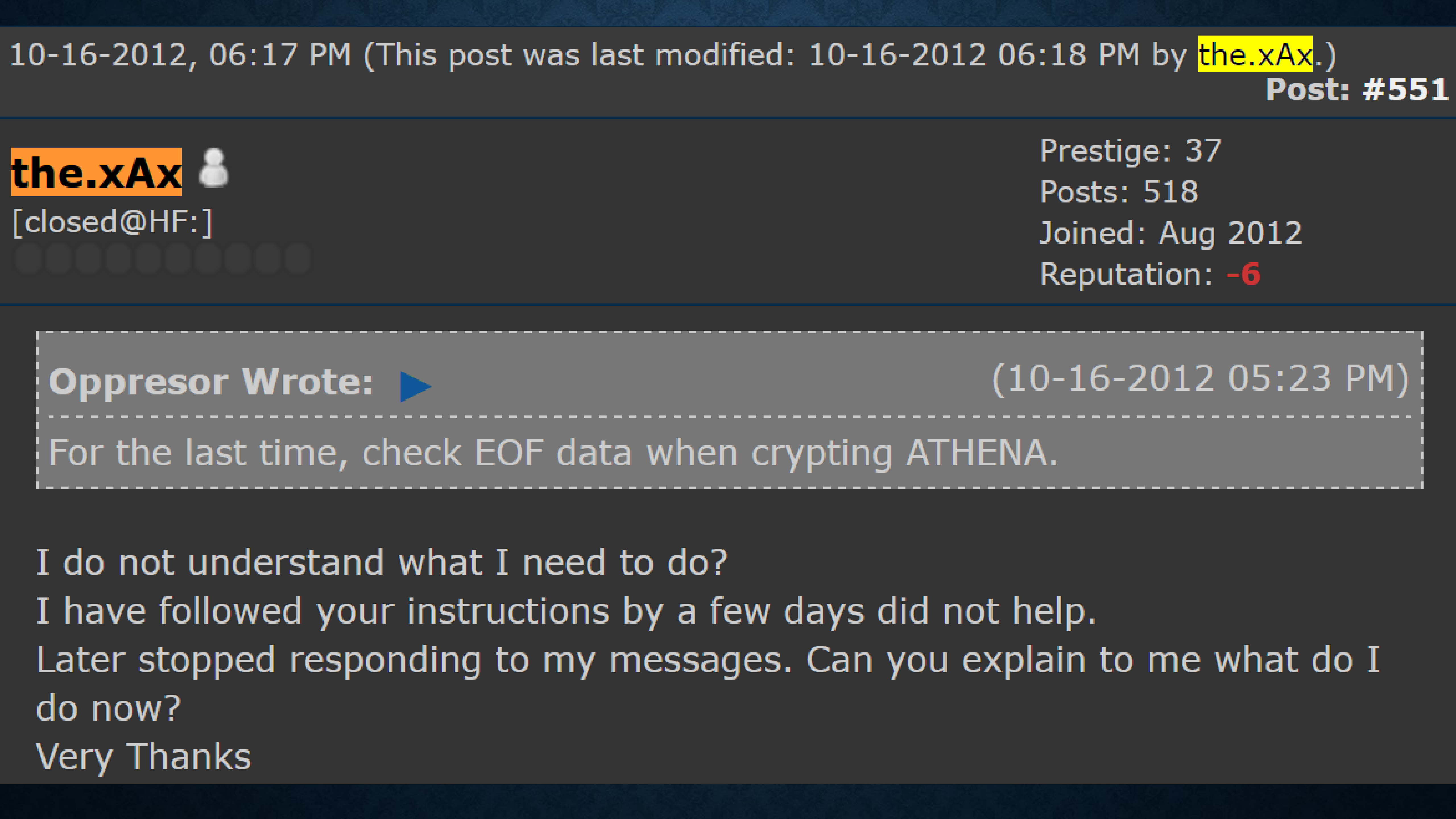
3 RATs, Open Port, VPN and nothing !

10-16-2012, 11:11 AM

the.xAx

[closed@HF:]

Welcome.
Today I tried to run on my computer Rats.
I use a VPN server with open ports.
On the http://canyouseeme.org/ see that the ports are open.
Firewall is turned off.
I used Cybergate, jRAT, Xtreme Rat, every time the bot can not connect to the server.
Waiting for your suggestions.



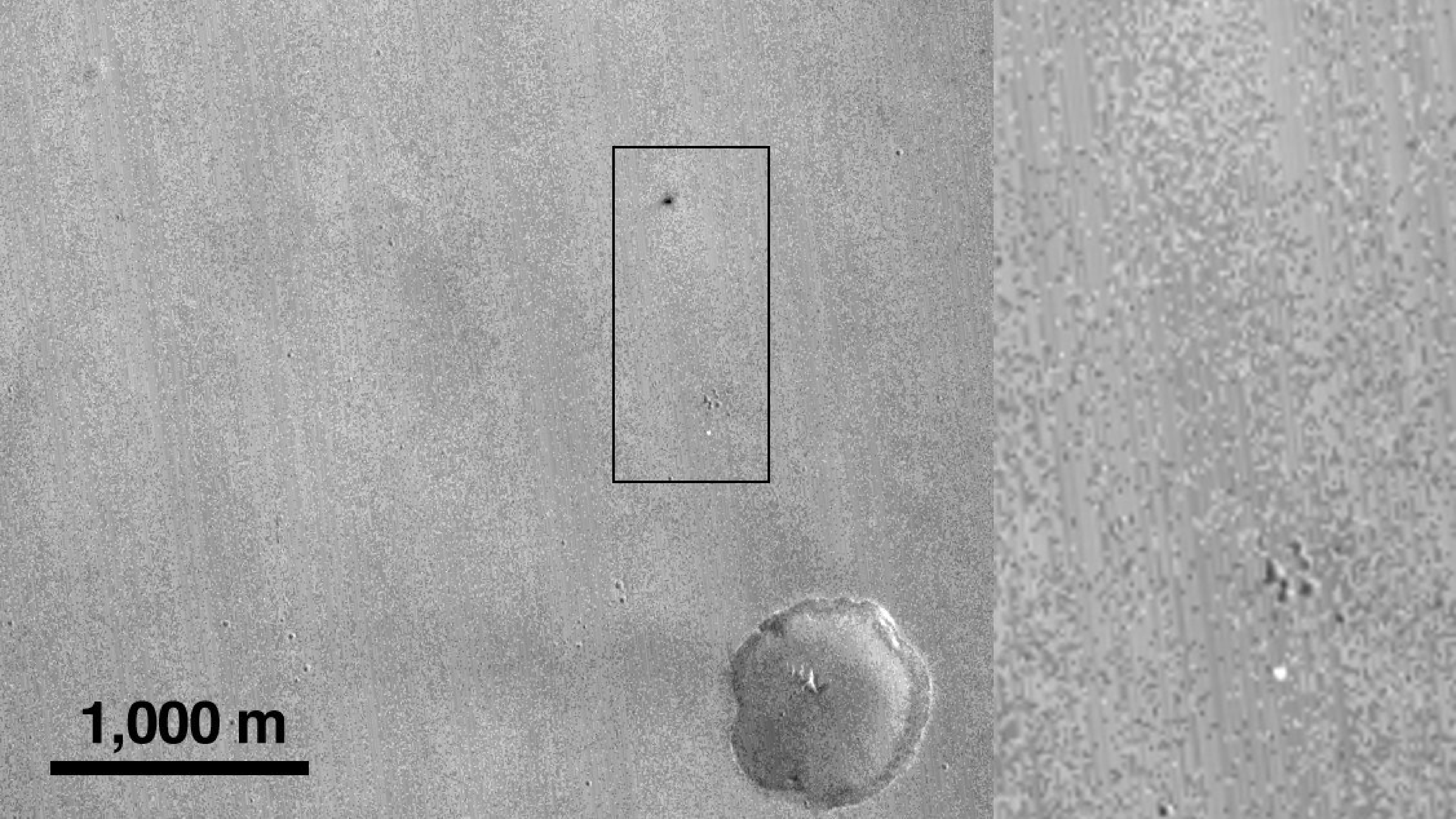
10-16-2012, 06:17 PM (This post was last modified: 10-16-2012 06:18 PM by the.xAx.)
Post: #551

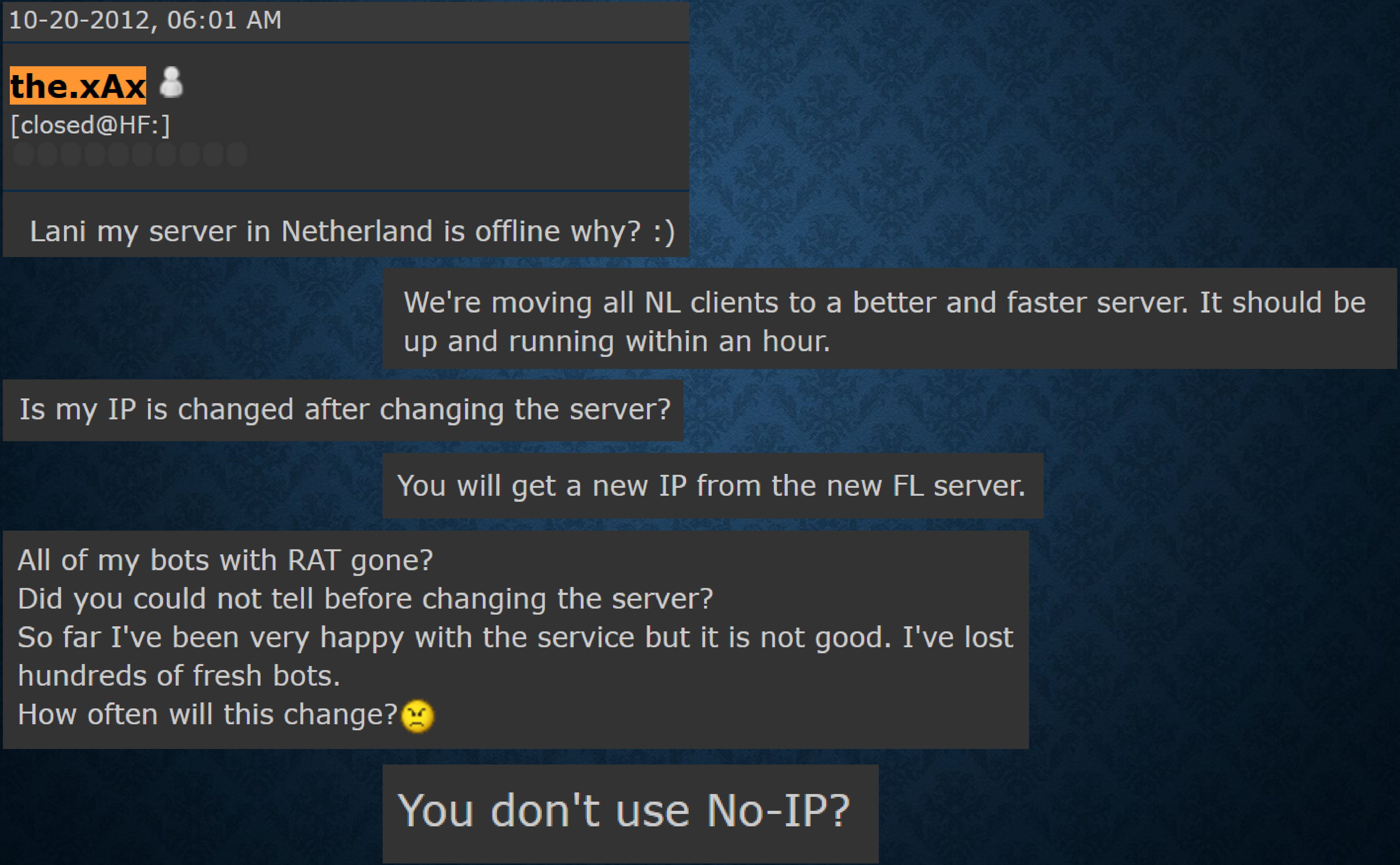
the.xAx
[closed@HF:]

Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

> **Oppresor Wrote:** ▶ (10-16-2012 05:23 PM)
>
> For the last time, check EOF data when crypting ATHENA.

I do not understand what I need to do?
I have followed your instructions by a few days did not help.
Later stopped responding to my messages. Can you explain to me what do I do now?
Very Thanks


1,000 m



10-20-2012, 06:01 AM

the.xAx

[closed@HF:]

Lani my server in Netherland is offline why? :)

We're moving all NL clients to a better and faster server. It should be up and running within an hour.

Is my IP is changed after changing the server?

You will get a new IP from the new FL server.

All of my bots with RAT gone?
Did you could not tell before changing the server?
So far I've been very happy with the service but it is not good. I've lost hundreds of fresh bots.
How often will this change?😠

You don't use No-IP?

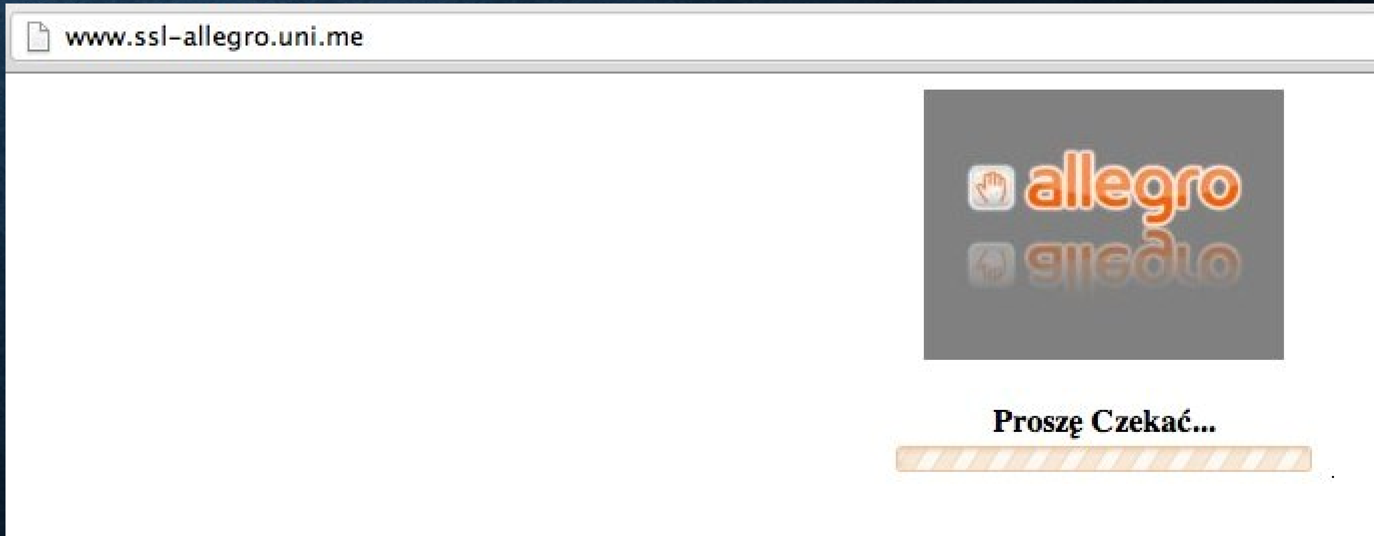
Dear User!

Probably someone tried to take over your Allegro account. We locked your account. You can recover it by going to

http://www.ssl-allegro.uni.me/

To securely recover your account follow the instructions.

Best regards Allegro Group



www.ssl-allegro.uni.me

Proszę Czekać...

Dear User!

Probably someone tried to take over your PayPal account. We locked your account. You can recover it by going to

http://ssl-paypal.tk

To securely recover your account follow the instructions.

Best regards PayPal Group

This is an automated message.

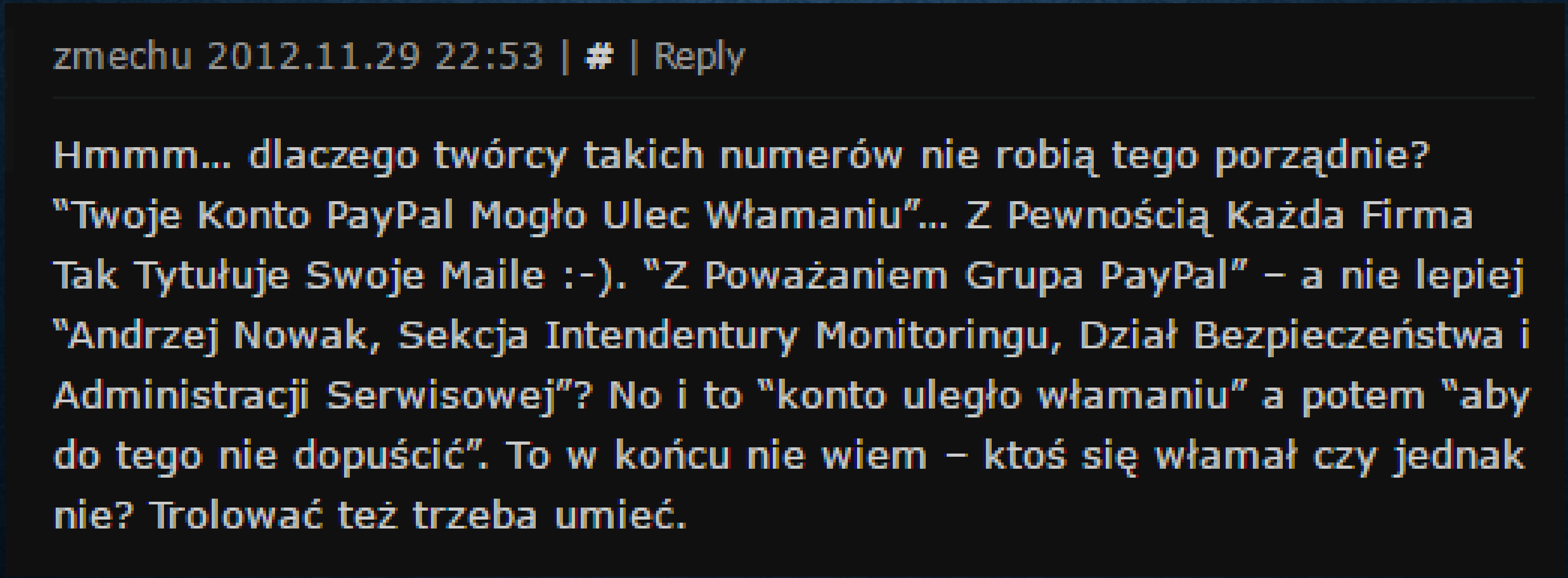
Your Facebook account was hacked. To stop the attack we locked your account. You can recover it safely only by going to

http://pass-facebook.tk/

Please wait for your new password to be created.

Andrew Jones, Stewardship Monitoring Section, Security and Server Administration Department Facebook.pl

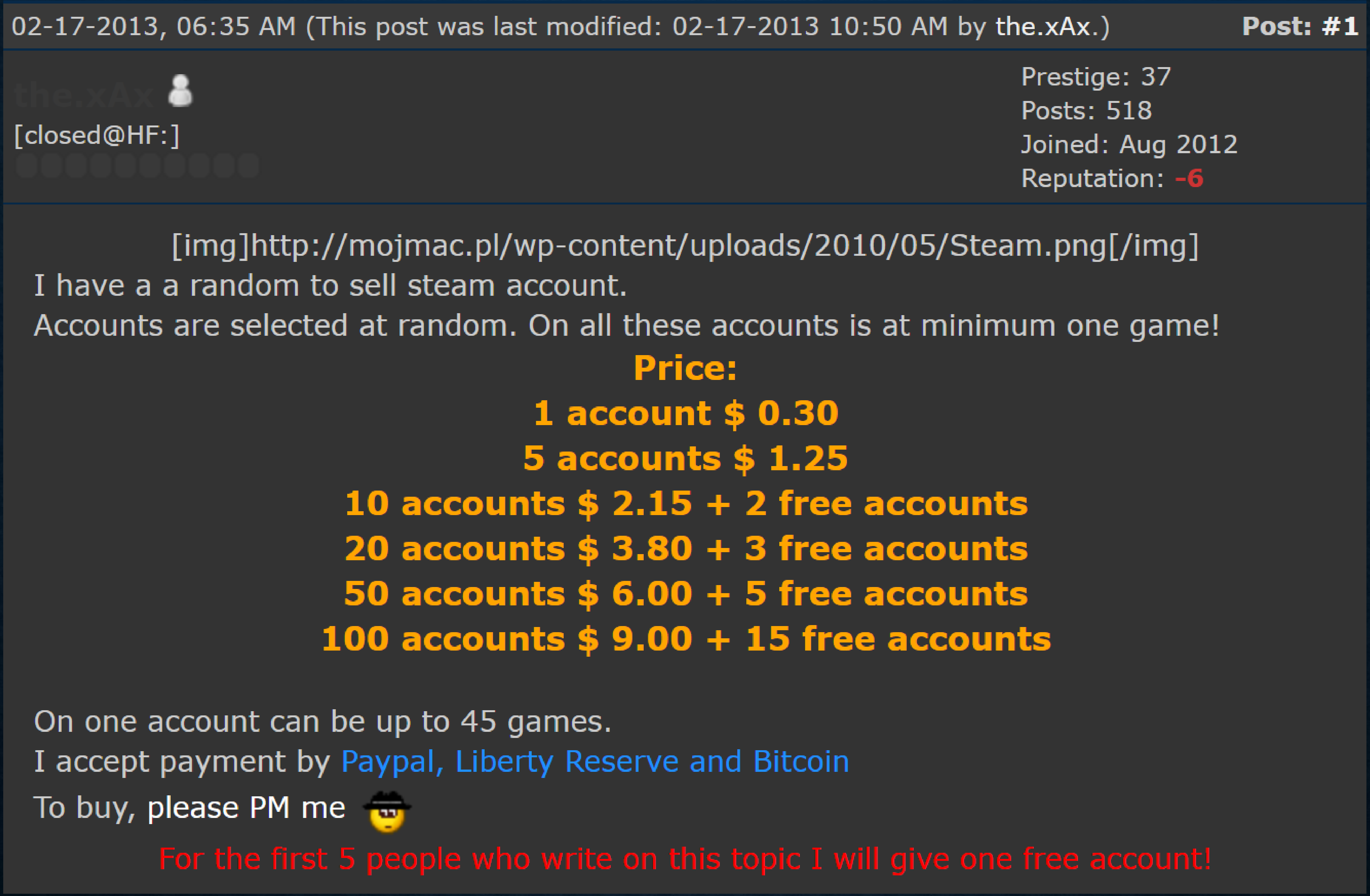
Why can’t the scammers do their job properly? „Best Regards PayPal Group’’ – why not rather use something like „Andrew Smith, Stewardship Monitoring Section, Security and Server Administration Department’’?



zmechu 2012.11.29 22:53 | # | Reply

Hmmm… dlaczego twórcy takich numerów nie robią tego porządnie? "Twoje Konto PayPal Mogło Ulec Włamaniu"… Z Pewnością Każda Firma Tak Tytułuje Swoje Maile :-). "Z Poważaniem Grupa PayPal" – a nie lepiej "Andrzej Nowak, Sekcja Intendentury Monitoringu, Dział Bezpieczeństwa i Administracji Serwisowej"? No i to "konto uległo włamaniu" a potem "aby do tego nie dopuścić". To w końcu nie wiem – ktoś się włamał czy jednak nie? Trolować też trzeba umieć.

P29640429118
50
EURO
50



02-17-2013, 06:35 AM (This post was last modified: 02-17-2013 10:50 AM by the.xAx.) **Post: #1**

the.xAx

[closed@HF:]

Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

[img]http://mojmac.pl/wp-content/uploads/2010/05/Steam.png[/img]

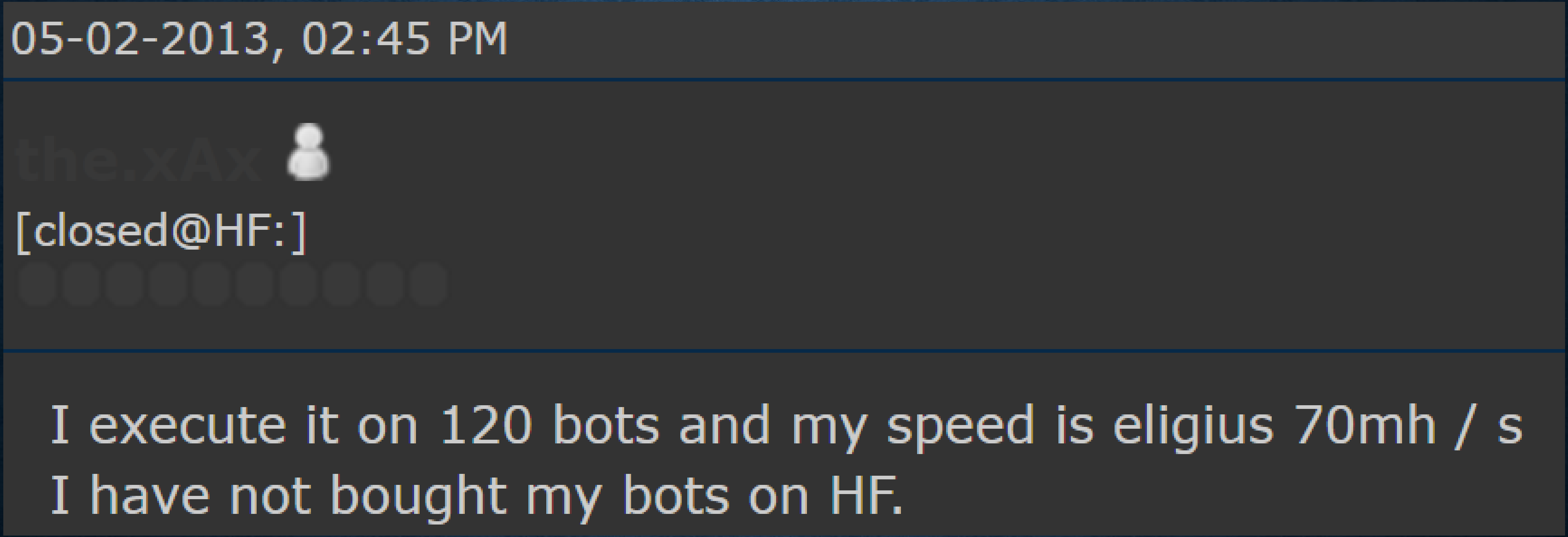
I have a a random to sell steam account.
Accounts are selected at random. On all these accounts is at minimum one game!

Price:

1 account $ 0.30
5 accounts $ 1.25
10 accounts $ 2.15 + 2 free accounts
20 accounts $ 3.80 + 3 free accounts
50 accounts $ 6.00 + 5 free accounts
100 accounts $ 9.00 + 15 free accounts

On one account can be up to 45 games.
I accept payment by Paypal, Liberty Reserve and Bitcoin
To buy, please PM me

For the first 5 people who write on this topic I will give one free account!



05-02-2013, 02:45 PM

the.xAx

[closed@HF:]

I execute it on 120 bots and my speed is eligius 70mh / s
I have not bought my bots on HF.

Dear User!

We detected a series of logins to your iPKO bank account from abroad. Incorrect passwords were used. In order to guarantee the highest security available we locked temporarily your account.

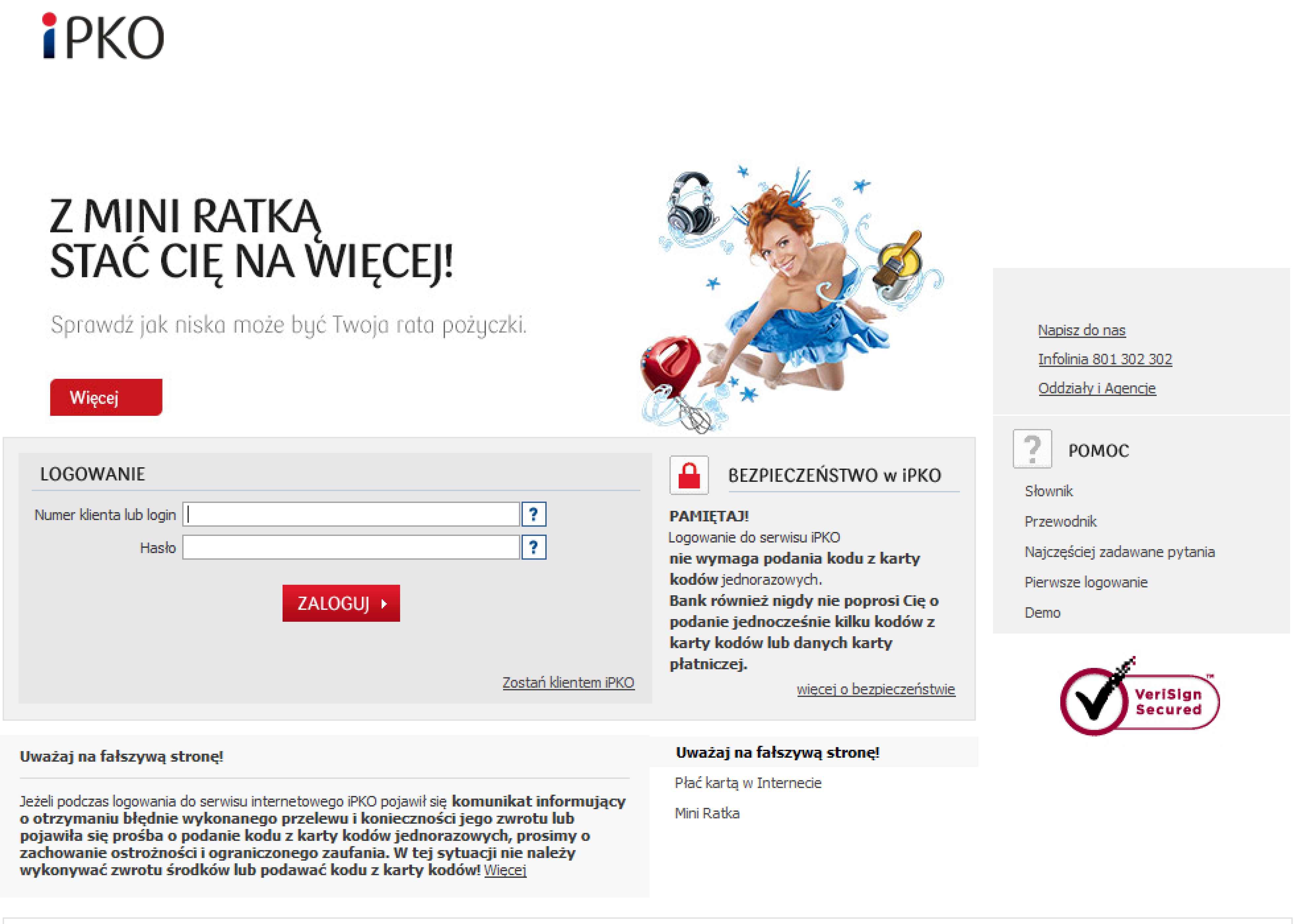
In order for you to safely recover access to your account we created a dedicated website at:

www.verify-ipko.cu.cc

After logging in your identity will be verified to recover access to your account.

Kind regards Andrew Jones

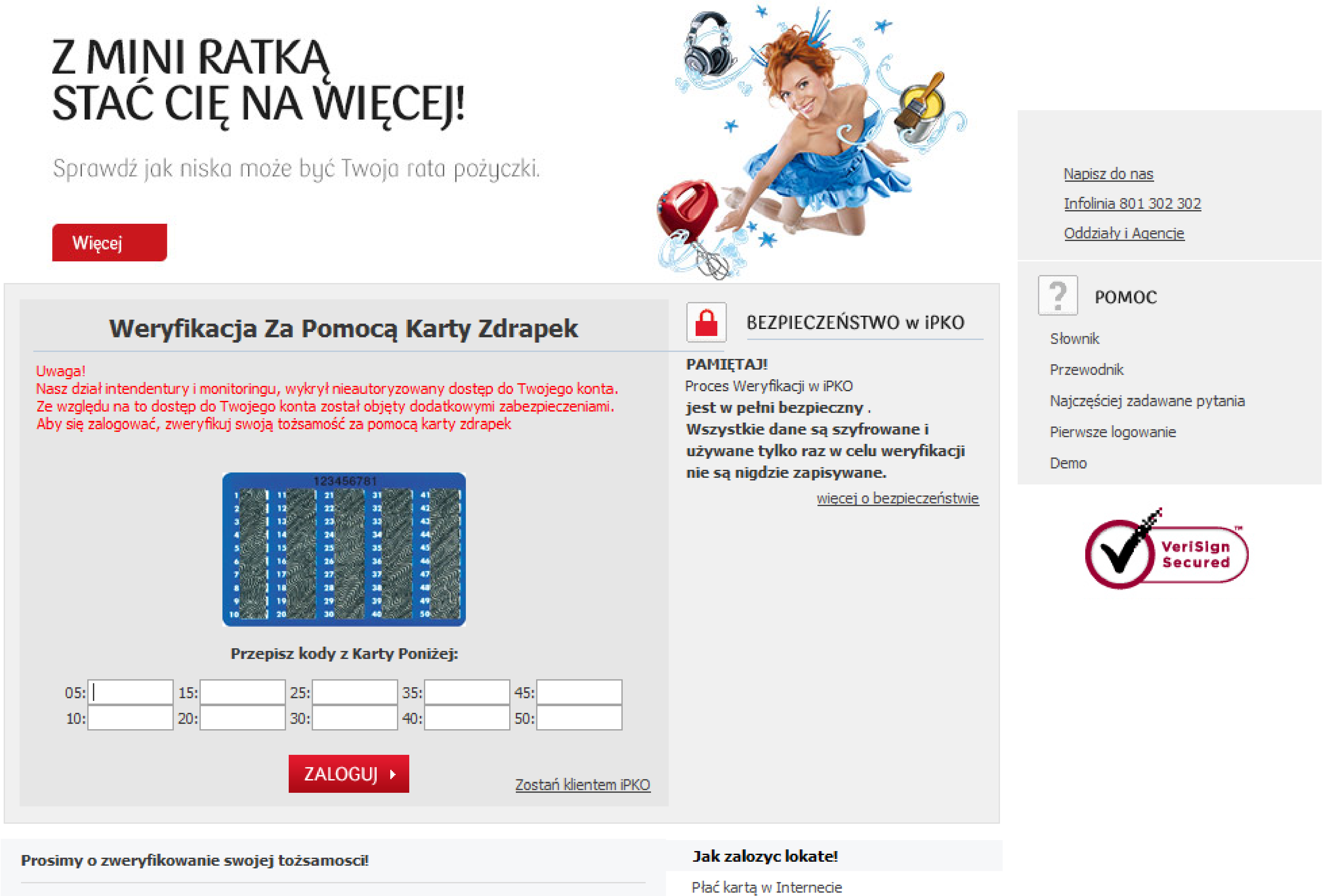
Stewardship Monitoring Section, bank PKO BP



PAMIĘTAJ!
Logowanie do serwisu iPKO **nie wymaga podania kodu z karty kodów** jednorazowych. **Bank również nigdy nie poprosi Cię o podanie jednocześnie kilku kodów z karty kodów lub danych karty płatniczej.**

Uważaj na fałszywą stronę!

Jeżeli podczas logowania do serwisu internetowego iPKO pojawił się **komunikat informujący o otrzymaniu błędnie wykonanego przelewu i konieczności jego zwrotu lub pojawiła się prośba o podanie kodu z karty kodów jednorazowych, prosimy o zachowanie ostrożności i ograniczonego zaufania. W tej sytuacji nie należy wykonywać zwrotu środków lub podawać kodu z karty kodów!** Więcej



Z MINI RATKĄ
STAĆ CIĘ NA WIĘCEJ!

Sprawdź jak niska może być Twoja rata pożyczki.

Więcej

Napisz do nas

Infolinia 801 302 302

Oddziały i Agencje

Weryfikacja Za Pomocą Karty Zdrapek

Uwaga!
Nasz dział intendentury i monitoringu, wykrył nieautoryzowany dostęp do Twojego konta.
Ze względu na to dostęp do Twojego konta został objęty dodatkowymi zabezpieczeniami.
Aby się zalogować, zweryfikuj swoją tożsamość za pomocą karty zdrapek

Przepisz kody z Karty Poniżej:

05: ___ 15: ___ 25: ___ 35: ___ 45: ___
10: ___ 20: ___ 30: ___ 40: ___ 50: ___

ZALOGUJ ▸

Zostań klientem iPKO

BEZPIECZEŃSTWO w iPKO

PAMIĘTAJ!
Proces Weryfikacji w iPKO
jest w pełni bezpieczny .
Wszystkie dane są szyfrowane i używane tylko raz w celu weryfikacji nie są nigdzie zapisywane.

więcej o bezpieczeństwie

POMOC

Słownik

Przewodnik

Najczęściej zadawane pytania

Pierwsze logowanie

Demo

VeriSign Secured

Prosimy o zweryfikowanie swojej tożsamosci!

Jak zalozyc lokate!

Płać kartą w Internecie

ARMAGEDON SPAM SERVICE

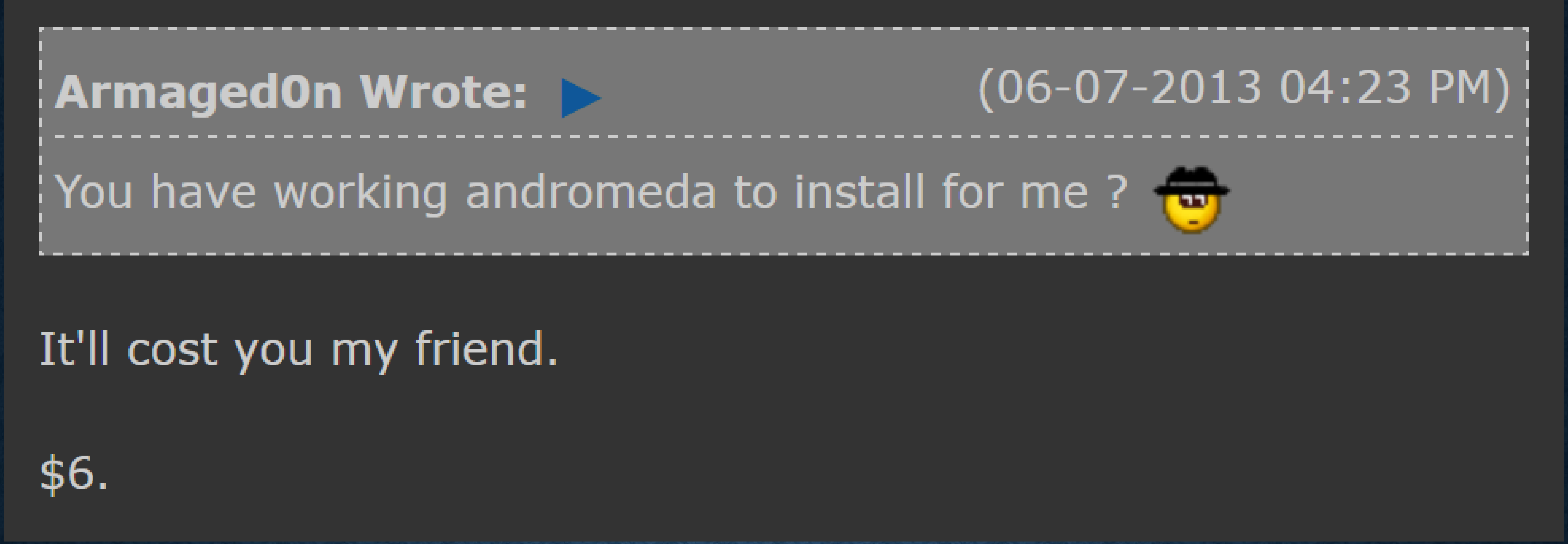
PAYMENT METHOD:

bitcoin

WebMoney

BTC e

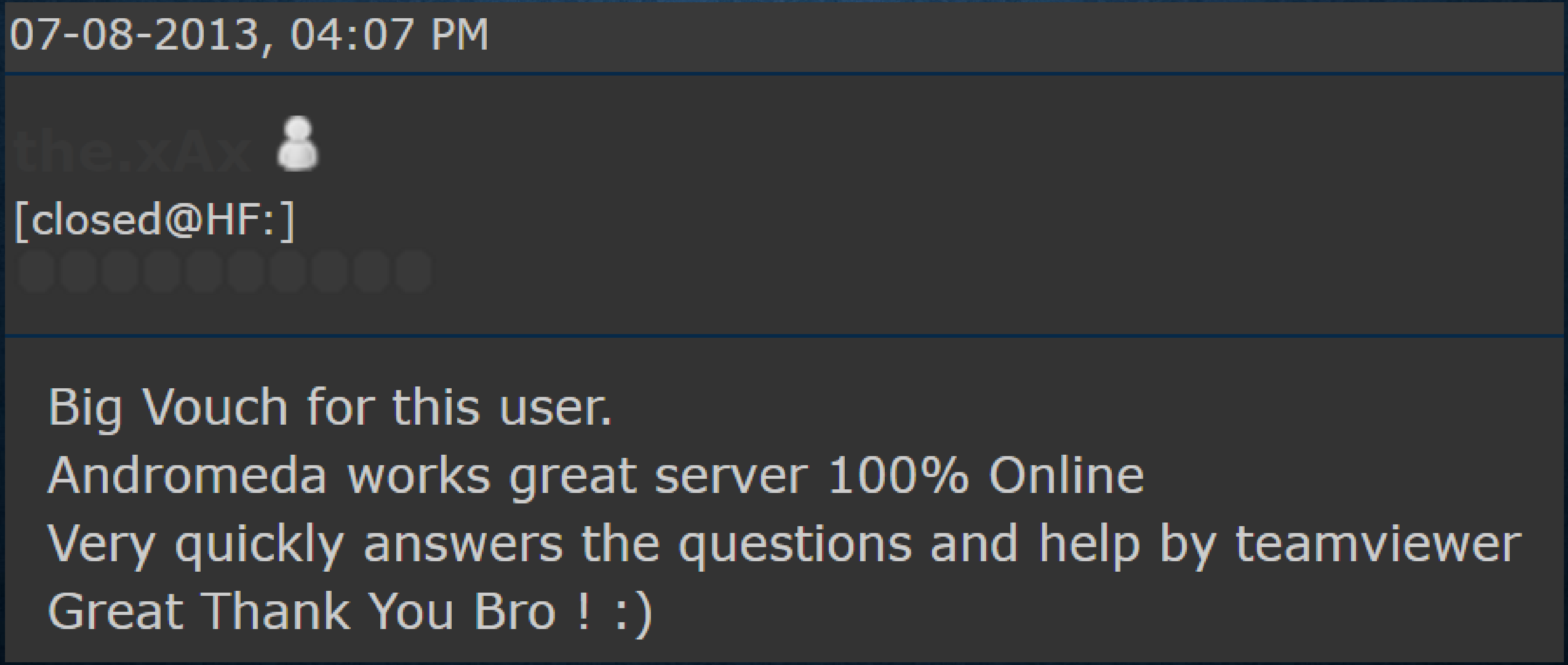
litecoin



> **Armaged0n Wrote:** ▶ (06-07-2013 04:23 PM)
>
> You have working andromeda to install for me ?

It'll cost you my friend.

$6.

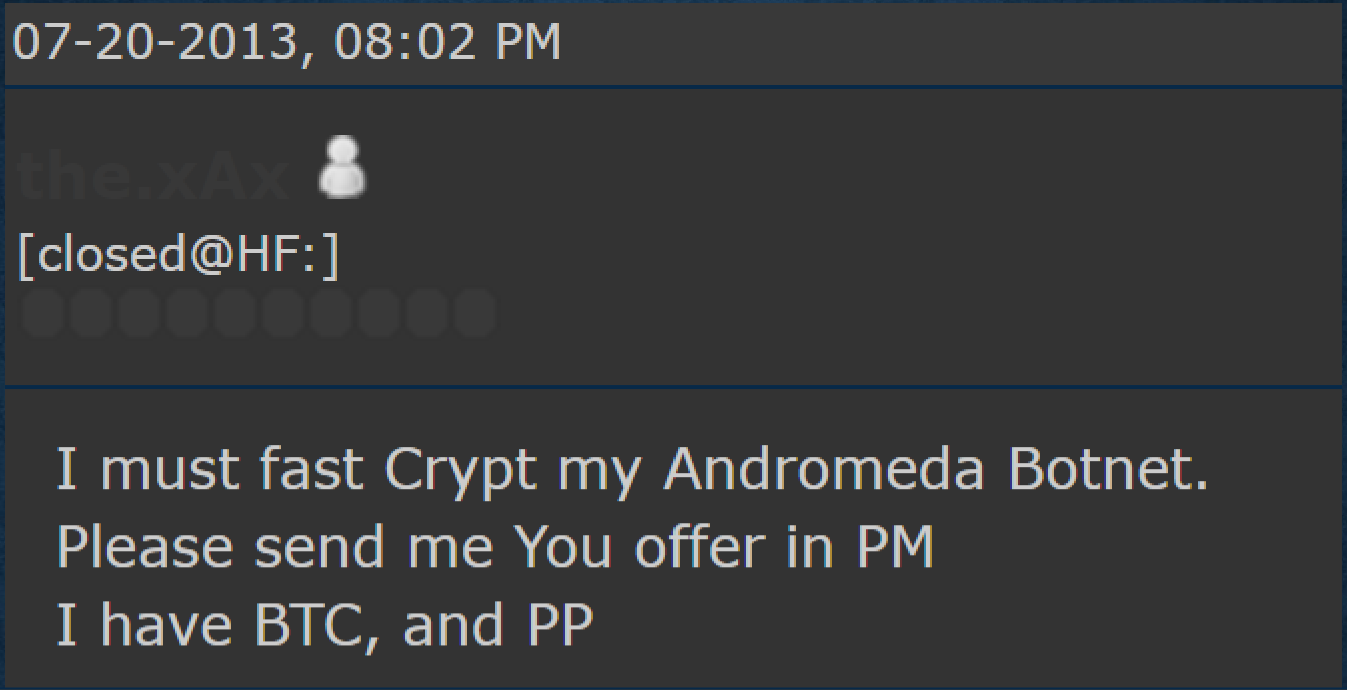


07-08-2013, 04:07 PM

the.xAx

[closed@HF:]

Big Vouch for this user.
Andromeda works great server 100% Online
Very quickly answers the questions and help by teamviewer
Great Thank You Bro ! :)

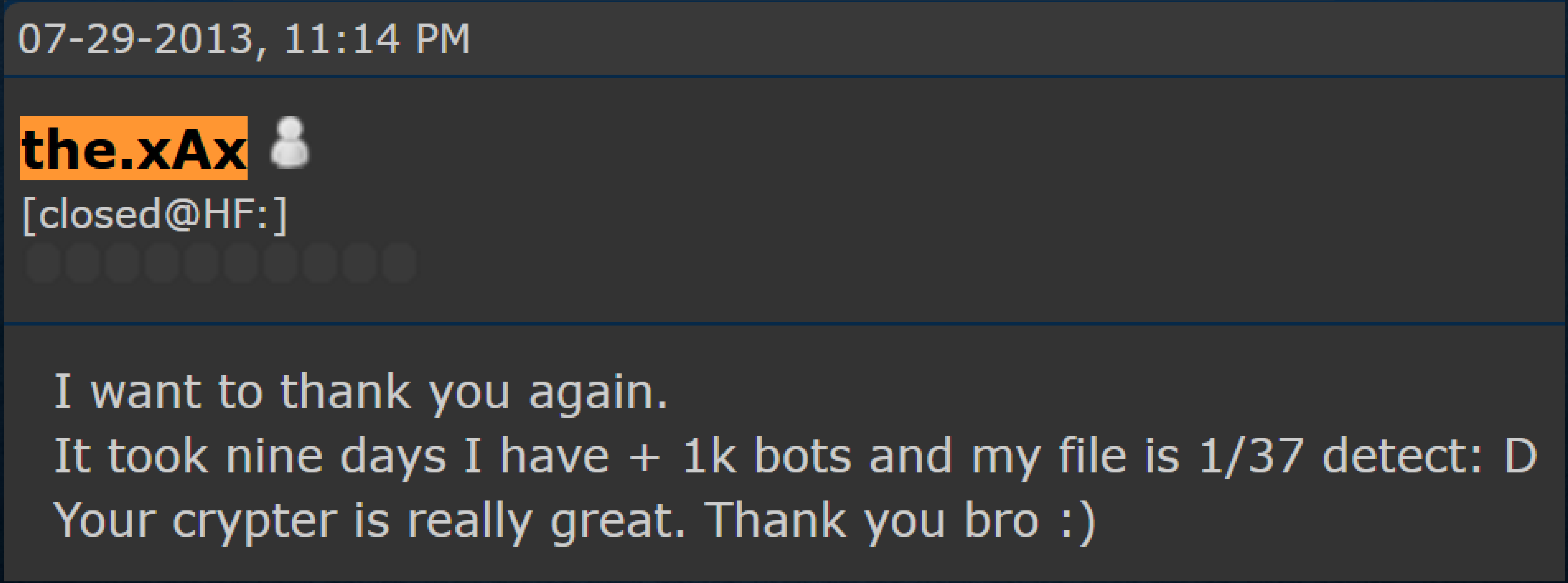


07-20-2013, 08:02 PM

the.xAx

[closed@HF:]

I must fast Crypt my Andromeda Botnet.
Please send me You offer in PM
I have BTC, and PP

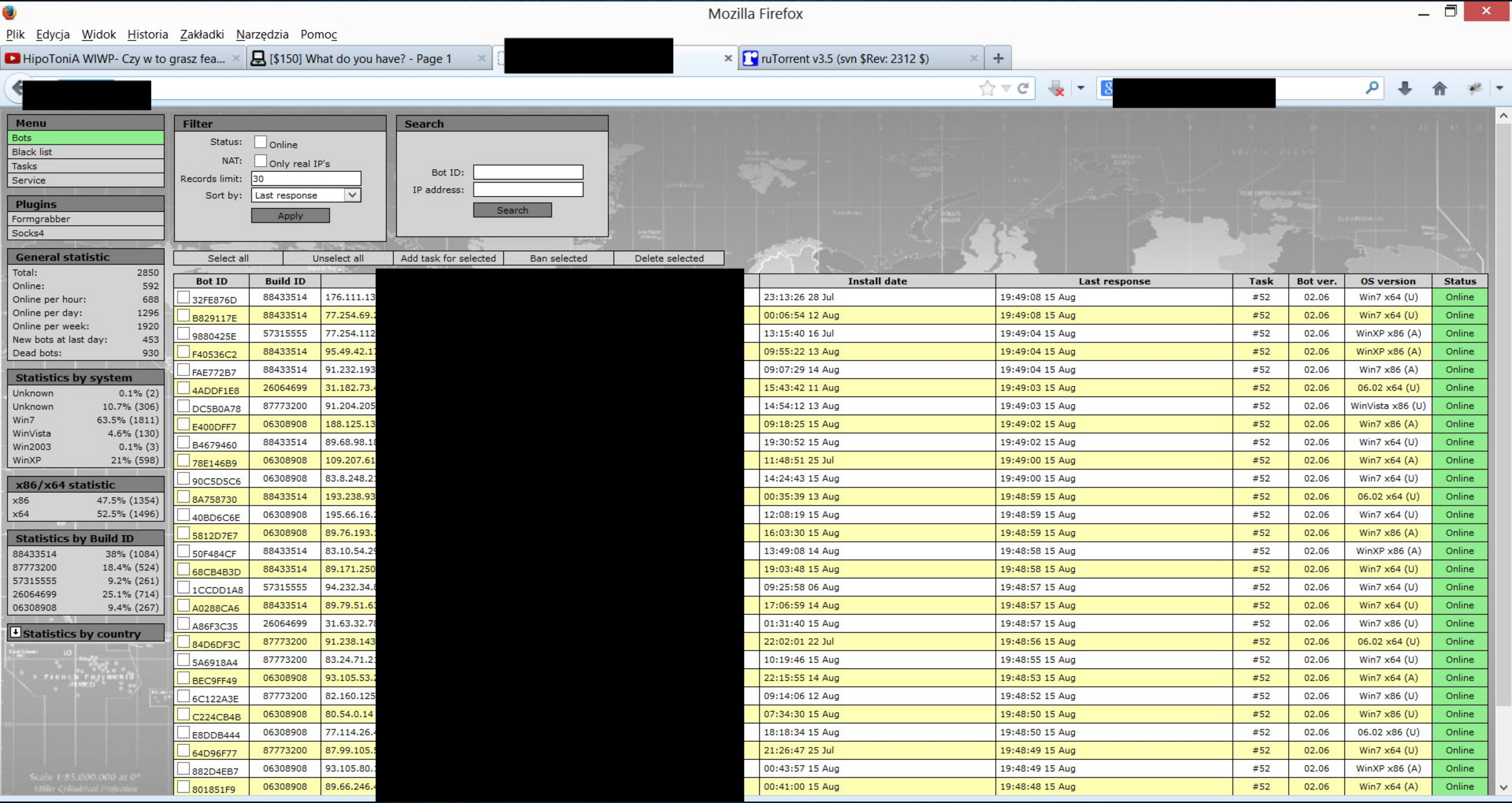


07-29-2013, 11:14 PM

the.xAx

[closed@HF:]

I want to thank you again.
It took nine days I have + 1k bots and my file is 1/37 detect: D
Your crypter is really great. Thank you bro :)


Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
HipoToniA WIWP- Czy w to grasz fea...
[$150] What do you have? - Page 1
[redacted]
ruTorrent v3.5 (svn $Rev: 2312 $)
[redacted]
[redacted]

Menu

- Bots
- Black list
- Tasks
- Service

Plugins

- Formgrabber
- Socks4

Filter

Status: □ Online

NAT: □ Only real IP's

Records limit: 30

Sort by: Last response

Apply

Search

Bot ID:

IP address:

Search

General statistic

Total:	2850
Online:	592
Online per hour:	688
Online per day:	1296
Online per week:	1920
New bots at last day:	453
Dead bots:	930

Statistics by system

Unknown	0.1% (2)
Unknown	10.7% (306)
Win7	63.5% (1811)
WinVista	4.6% (130)
Win2003	0.1% (3)
WinXP	21% (598)

x86/x64 statistic

x86	47.5% (1354)
x64	52.5% (1496)

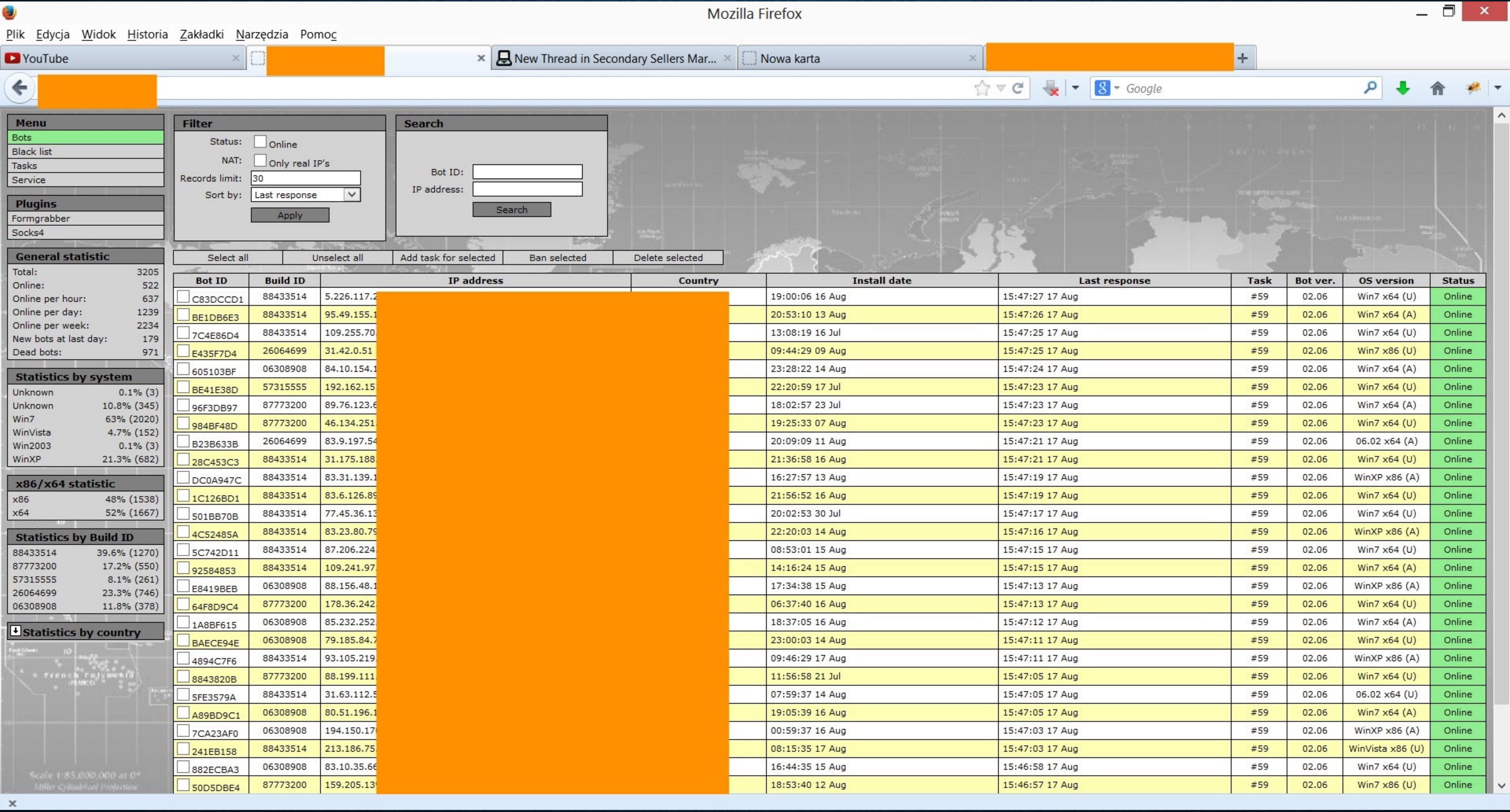
Statistics by Build ID

88433514	38% (1084)
87773200	18.4% (524)
57315555	9.2% (261)
26064699	25.1% (714)
06308908	9.4% (267)

Statistics by country

Select all | Unselect all | Add task for selected | Ban selected | Delete selected

Bot ID	Build ID			Install date	Last response	Task	Bot ver.	OS version	Status
□ 32FE876D	88433514	176.111.13	[redacted]	23:13:26 28 Jul	19:49:08 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ B829117E	88433514	77.254.69.	[redacted]	00:06:54 12 Aug	19:49:08 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 9880425E	57315555	77.254.112	[redacted]	13:15:40 16 Jul	19:49:04 15 Aug	#52	02.06	WinXP x86 (A)	Online
□ F40536C2	88433514	95.49.42.1	[redacted]	09:55:22 13 Aug	19:49:04 15 Aug	#52	02.06	WinXP x86 (A)	Online
□ FAE772B7	88433514	91.232.193	[redacted]	09:07:29 14 Aug	19:49:04 15 Aug	#52	02.06	Win7 x86 (A)	Online
□ 4ADDF1E8	26064699	31.182.73.	[redacted]	15:43:42 11 Aug	19:49:03 15 Aug	#52	02.06	06.02 x64 (U)	Online
□ DC5B0A78	87773200	91.204.205	[redacted]	14:54:12 13 Aug	19:49:03 15 Aug	#52	02.06	WinVista x86 (U)	Online
□ E400DFF7	06308908	188.125.13	[redacted]	09:18:25 15 Aug	19:49:02 15 Aug	#52	02.06	Win7 x86 (A)	Online
□ B4679460	88433514	89.68.98.1	[redacted]	19:30:52 15 Aug	19:49:02 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 78E146B9	06308908	109.207.61	[redacted]	11:48:51 25 Jul	19:49:00 15 Aug	#52	02.06	Win7 x64 (A)	Online
□ 90C5D5C6	06308908	83.8.248.2	[redacted]	14:24:43 15 Aug	19:49:00 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 8A758730	88433514	193.238.93	[redacted]	00:35:39 13 Aug	19:48:59 15 Aug	#52	02.06	06.02 x64 (U)	Online
□ 40BD6C6E	06308908	195.66.16.	[redacted]	12:08:19 15 Aug	19:48:59 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 5812D7E7	06308908	89.76.193.	[redacted]	16:03:30 15 Aug	19:48:59 15 Aug	#52	02.06	Win7 x86 (A)	Online
□ 50F484CF	88433514	83.10.54.2	[redacted]	13:49:08 14 Aug	19:48:58 15 Aug	#52	02.06	WinXP x86 (A)	Online
□ 68CB4B3D	88433514	89.171.250	[redacted]	19:03:48 15 Aug	19:48:58 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 1CCDD1A8	57315555	94.232.34.	[redacted]	09:25:58 06 Aug	19:48:57 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ A0288CA6	88433514	89.79.51.6	[redacted]	17:06:59 14 Aug	19:48:57 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ A86F3C35	26064699	31.63.32.7	[redacted]	01:31:40 15 Aug	19:48:57 15 Aug	#52	02.06	Win7 x86 (U)	Online
□ 84D6DF3C	87773200	91.238.143	[redacted]	22:02:01 22 Jul	19:48:56 15 Aug	#52	02.06	06.02 x64 (U)	Online
□ 5A6918A4	87773200	83.24.71.2	[redacted]	10:19:46 15 Aug	19:48:55 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ BEC9FF49	06308908	93.105.53.	[redacted]	22:15:55 14 Aug	19:48:53 15 Aug	#52	02.06	Win7 x64 (A)	Online
□ 6C122A3E	87773200	82.160.125	[redacted]	09:14:06 12 Aug	19:48:52 15 Aug	#52	02.06	Win7 x86 (U)	Online
□ C224CB4B	06308908	80.54.0.14	[redacted]	07:34:30 15 Aug	19:48:50 15 Aug	#52	02.06	Win7 x86 (U)	Online
□ E8DDB444	06308908	77.114.26.	[redacted]	18:18:34 15 Aug	19:48:50 15 Aug	#52	02.06	06.02 x86 (U)	Online
□ 64D96F77	87773200	87.99.105.	[redacted]	21:26:47 25 Jul	19:48:49 15 Aug	#52	02.06	Win7 x64 (U)	Online
□ 882D4EB7	06308908	93.105.80.	[redacted]	00:43:57 15 Aug	19:48:49 15 Aug	#52	02.06	WinXP x86 (A)	Online
□ 801851F9	06308908	89.66.246.	[redacted]	00:41:00 15 Aug	19:48:48 15 Aug	#52	02.06	Win7 x64 (A)	Online


Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
YouTube
[redacted]
New Thread in Secondary Sellers Mar...
Nowa karta
[redacted]
[redacted]
Google

Menu
- Bots
- Black list
- Tasks
- Service

Plugins
- Formgrabber
- Socks4

Filter

Status: □ Online
NAT: □ Only real IP's
Records limit: 30
Sort by: Last response
Apply

Search

Bot ID:
IP address:
Search

General statistic	
Total:	3205
Online:	522
Online per hour:	637
Online per day:	1239
Online per week:	2234
New bots at last day:	179
Dead bots:	971

Statistics by system	
Unknown	0.1% (3)
Unknown	10.8% (345)
Win7	63% (2020)
WinVista	4.7% (152)
Win2003	0.1% (3)
WinXP	21.3% (682)

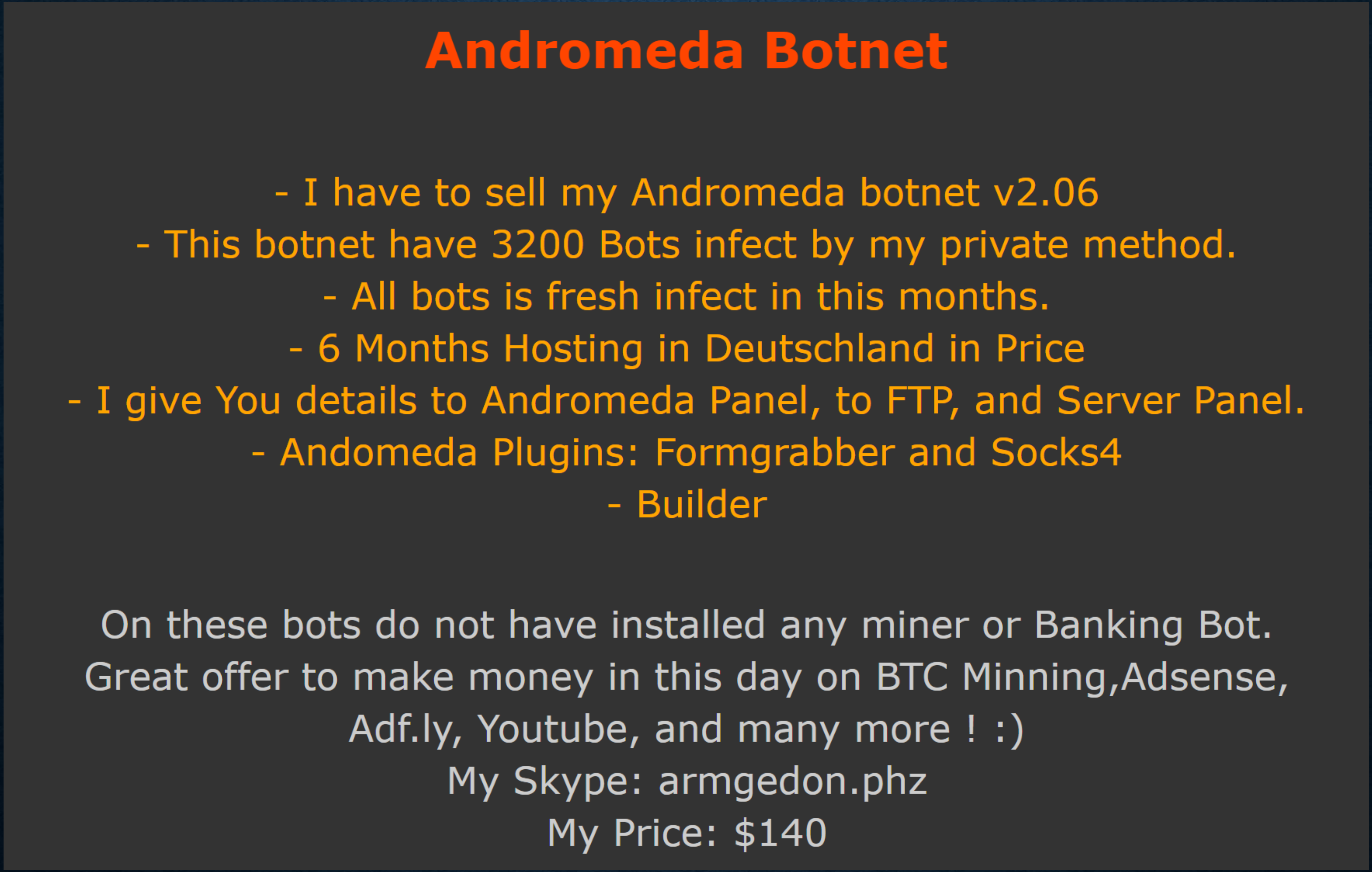
x86/x64 statistic	
x86	48% (1538)
x64	52% (1667)

Statistics by Build ID	
88433514	39.6% (1270)
87773200	17.2% (550)
57315555	8.1% (261)
26064699	23.3% (746)
06308908	11.8% (378)

Statistics by country

Select all | Unselect all | Add task for selected | Ban selected | Delete selected

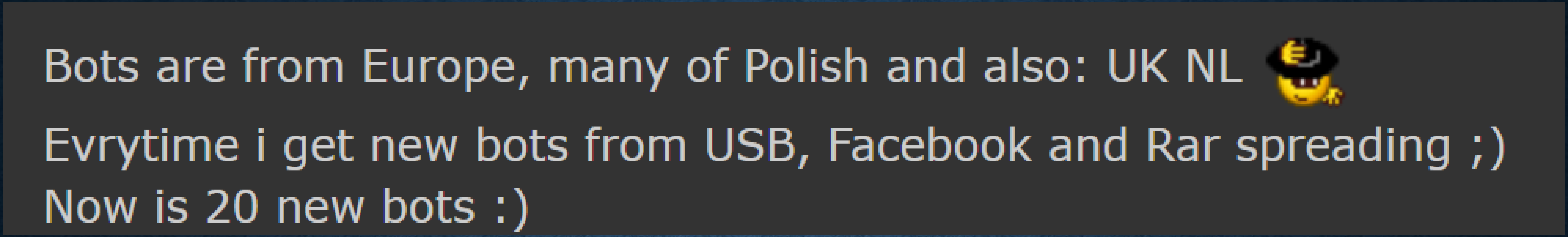
Bot ID	Build ID	IP address	Country	Install date	Last response	Task	Bot ver.	OS version	Status
□ C83DCCD1	88433514	[redacted]	[redacted]	19:00:06 16 Aug	15:47:27 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ BE1DB6E3	88433514	[redacted]	[redacted]	20:53:10 13 Aug	15:47:26 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ 7C4E86D4	88433514	[redacted]	[redacted]	13:08:19 16 Jul	15:47:25 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ E435F7D4	26064699	[redacted]	[redacted]	09:44:29 09 Aug	15:47:25 17 Aug	#59	02.06	Win7 x86 (U)	Online
□ 605103BF	06308908	[redacted]	[redacted]	23:28:22 14 Aug	15:47:24 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ BE41E38D	57315555	[redacted]	[redacted]	22:20:59 17 Jul	15:47:23 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 96F3DB97	87773200	[redacted]	[redacted]	18:02:57 23 Jul	15:47:23 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ 984BF48D	87773200	[redacted]	[redacted]	19:25:33 07 Aug	15:47:23 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ B23B633B	26064699	[redacted]	[redacted]	20:09:09 11 Aug	15:47:21 17 Aug	#59	02.06	06.02 x64 (A)	Online
□ 28C453C3	88433514	[redacted]	[redacted]	21:36:58 16 Aug	15:47:21 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ DC0A947C	88433514	[redacted]	[redacted]	16:27:57 13 Aug	15:47:19 17 Aug	#59	02.06	WinXP x86 (A)	Online
□ 1C126BD1	88433514	[redacted]	[redacted]	21:56:52 16 Aug	15:47:19 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 501BB70B	88433514	[redacted]	[redacted]	20:02:53 30 Jul	15:47:17 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 4C52485A	88433514	[redacted]	[redacted]	22:20:03 14 Aug	15:47:16 17 Aug	#59	02.06	WinXP x86 (A)	Online
□ 5C742D11	88433514	[redacted]	[redacted]	08:53:01 15 Aug	15:47:15 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 92584853	88433514	[redacted]	[redacted]	14:16:24 15 Aug	15:47:15 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ E8419BEB	06308908	[redacted]	[redacted]	17:34:38 15 Aug	15:47:13 17 Aug	#59	02.06	WinXP x86 (A)	Online
□ 64F8D9C4	87773200	[redacted]	[redacted]	06:37:40 16 Aug	15:47:13 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 1A8BF615	06308908	[redacted]	[redacted]	18:37:05 16 Aug	15:47:12 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ BAECE94E	06308908	[redacted]	[redacted]	23:00:03 14 Aug	15:47:11 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 4894C7F6	88433514	[redacted]	[redacted]	09:46:29 17 Aug	15:47:11 17 Aug	#59	02.06	WinXP x86 (A)	Online
□ 8843820B	87773200	[redacted]	[redacted]	11:56:58 21 Jul	15:47:05 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 5FE3579A	88433514	[redacted]	[redacted]	07:59:37 14 Aug	15:47:05 17 Aug	#59	02.06	06.02 x64 (U)	Online
□ A89BD9C1	06308908	[redacted]	[redacted]	19:05:39 16 Aug	15:47:05 17 Aug	#59	02.06	Win7 x64 (A)	Online
□ 7CA23AF0	06308908	[redacted]	[redacted]	00:59:37 16 Aug	15:47:03 17 Aug	#59	02.06	WinXP x86 (A)	Online
□ 241EB158	88433514	[redacted]	[redacted]	08:15:35 17 Aug	15:47:03 17 Aug	#59	02.06	WinVista x86 (U)	Online
□ 882ECBA3	06308908	[redacted]	[redacted]	16:44:35 15 Aug	15:46:58 17 Aug	#59	02.06	Win7 x64 (U)	Online
□ 50D5DBE4	87773200	[redacted]	[redacted]	18:53:40 12 Aug	15:46:57 17 Aug	#59	02.06	Win7 x86 (U)	Online



Andromeda Botnet

- I have to sell my Andromeda botnet v2.06
- This botnet have 3200 Bots infect by my private method.
- All bots is fresh infect in this months.
- 6 Months Hosting in Deutschland in Price
- I give You details to Andromeda Panel, to FTP, and Server Panel.
- Andomeda Plugins: Formgrabber and Socks4
- Builder

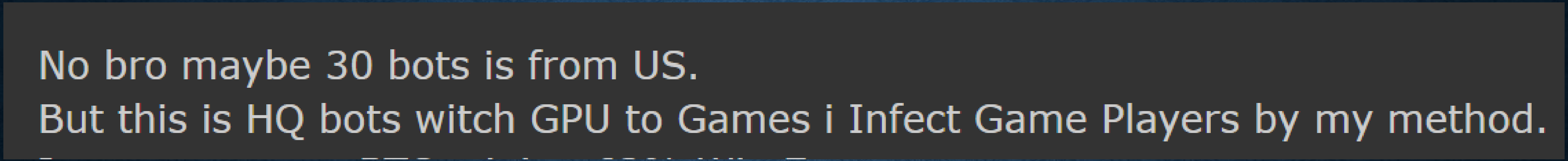
On these bots do not have installed any miner or Banking Bot.
Great offer to make money in this day on BTC Minning,Adsense,
Adf.ly, Youtube, and many more ! :)
My Skype: armgedon.phz
My Price: $140



Bots are from Europe, many of Polish and also: UK NL

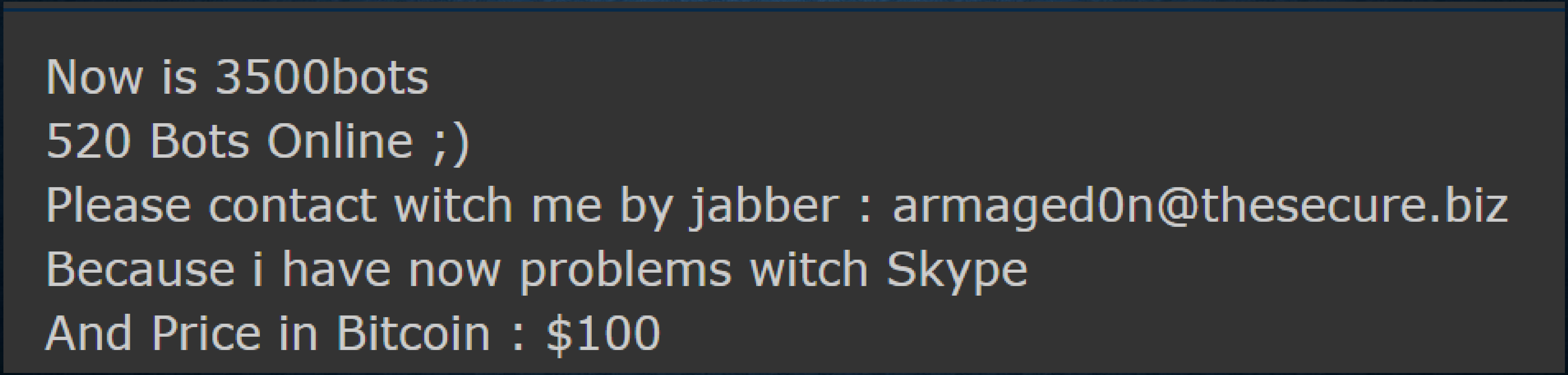
Evrytime i get new bots from USB, Facebook and Rar spreading ;)

Now is 20 new bots :)



No bro maybe 30 bots is from US.

But this is HQ bots witch GPU to Games i Infect Game Players by my method.



Now is 3500bots

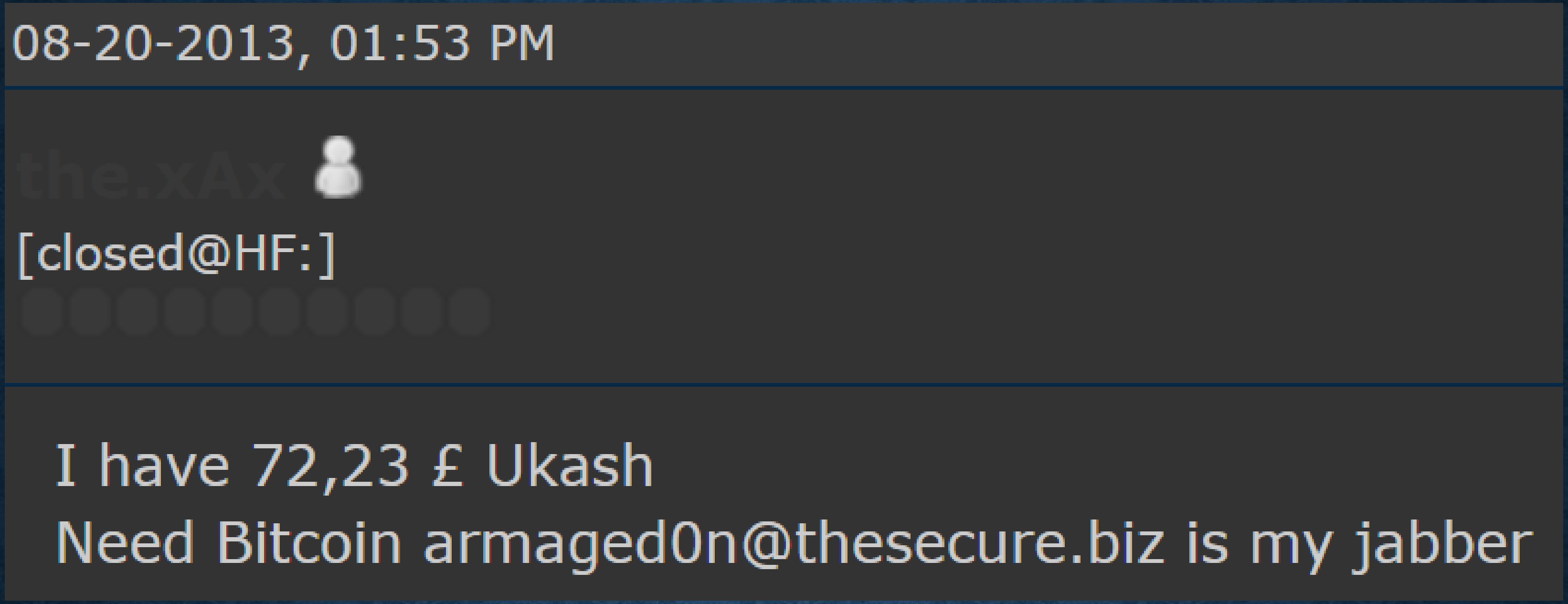
520 Bots Online ;)

Please contact witch me by jabber : armaged0n@thesecure.biz

Because i have now problems witch Skype

And Price in Bitcoin : $100

ROADSTER

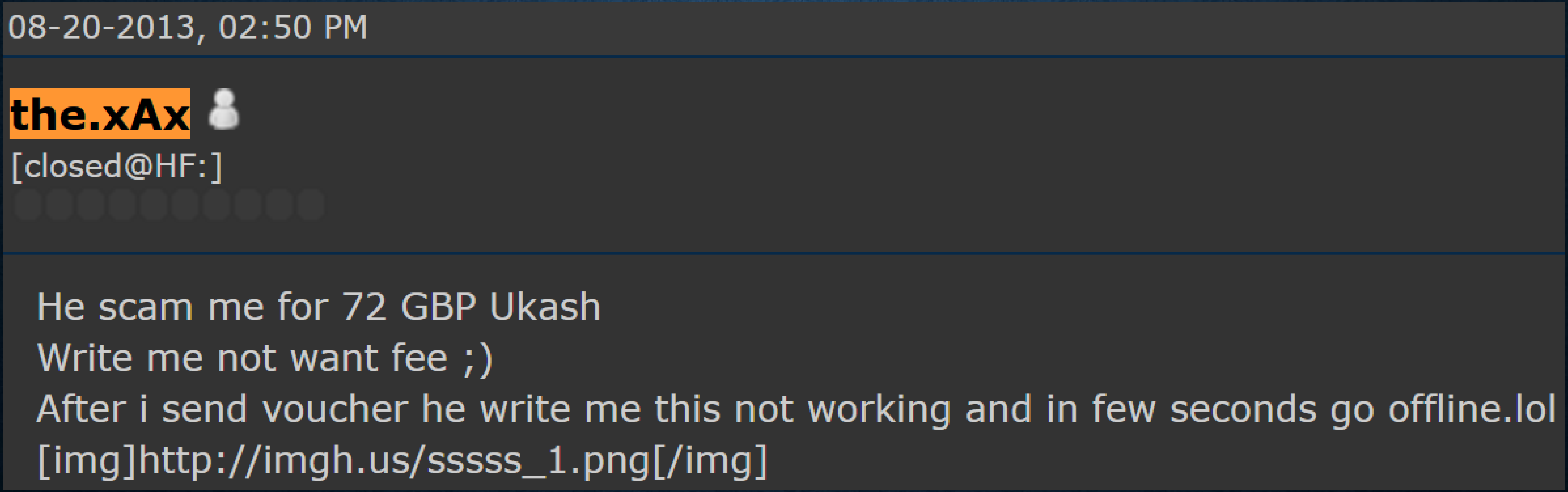


08-20-2013, 01:53 PM

the.xAx

[closed@HF:]

I have 72,23 £ Ukash
Need Bitcoin armaged0n@thesecure.biz is my jabber

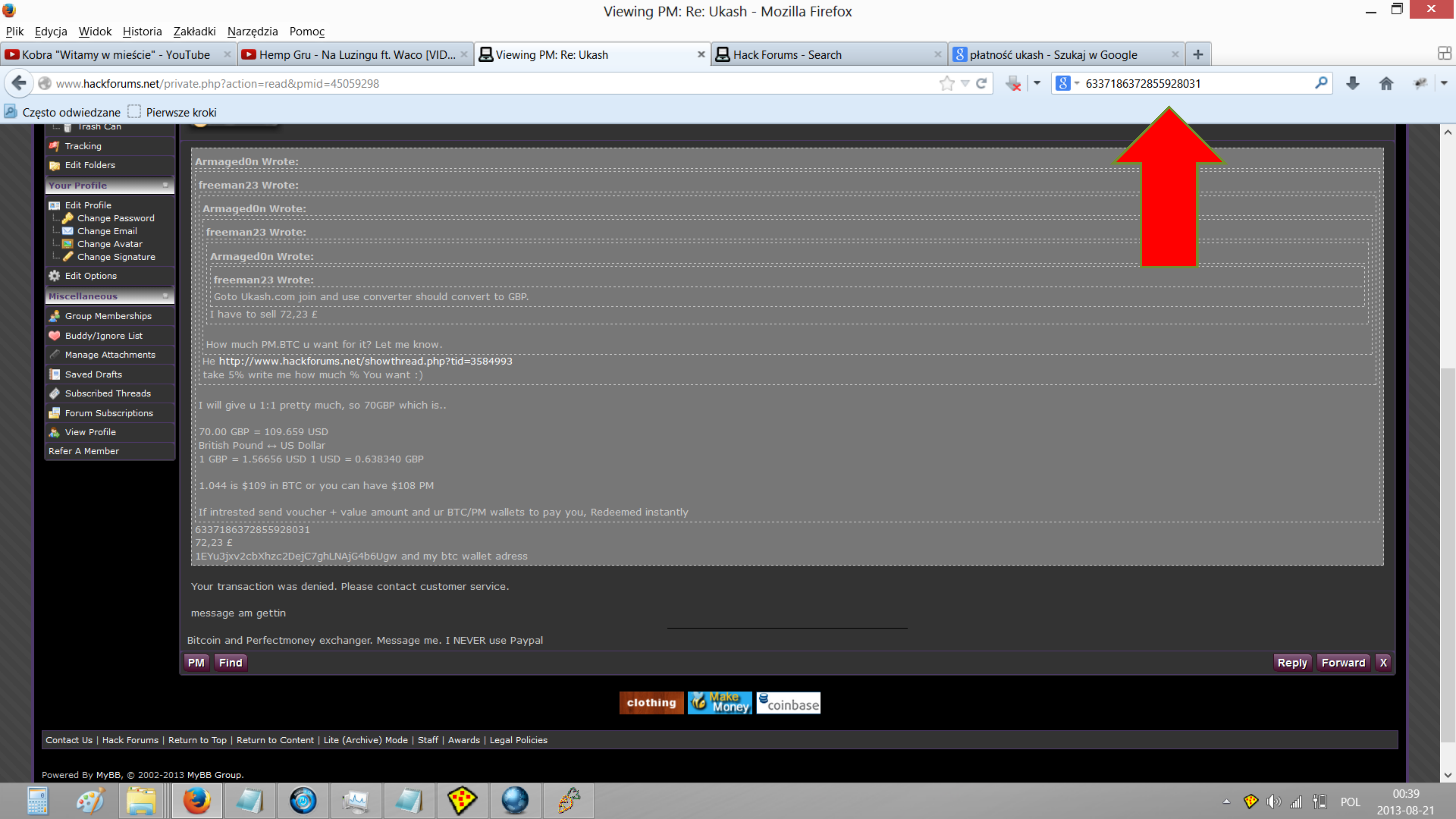


08-20-2013, 02:50 PM

the.xAx

[closed@HF:]

He scam me for 72 GBP Ukash
Write me not want fee ;)
After i send voucher he write me this not working and in few seconds go offline.lol
[img]http://imgh.us/sssss_1.png[/img]



Armaged0n Wrote:

> freeman23 Wrote:
>
>> Armaged0n Wrote:
>>
>>> freeman23 Wrote:
>>>
>>>> Armaged0n Wrote:
>>>>
>>>>> freeman23 Wrote:
>>>>>
>>>>> Goto Ukash.com join and use converter should convert to GBP.
>>>>
>>>> I have to sell 72,23 £
>>>
>>> How much PM.BTC u want for it? Let me know.
>>
>> He http://www.hackforums.net/showthread.php?tid=3584993
>> take 5% write me how much % You want :)
>
> I will give u 1:1 pretty much, so 70GBP which is..
>
> 70.00 GBP = 109.659 USD
> British Pound ↔ US Dollar
> 1 GBP = 1.56656 USD 1 USD = 0.638340 GBP
>
> 1.044 is $109 in BTC or you can have $108 PM
>
> If intrested send voucher + value amount and ur BTC/PM wallets to pay you, Redeemed instantly

6337186372855928031
72,23 £
1EYu3jxv2cbXhzc2DejC7ghLNAjG4b6Ugw and my btc wallet adress

Your transaction was denied. Please contact customer service.

message am gettin

Bitcoin and Perfectmoney exchanger. Message me. I NEVER use Paypal

PM
Find
Reply
Forward
X
clothing
Make Money
coinbase
Contact Us | Hack Forums | Return to Top | Return to Content | Lite (Archive) Mode | Staff | Awards | Legal Policies
Powered By MyBB, © 2002-2013 MyBB Group.
POL
00:39
2013-08-21

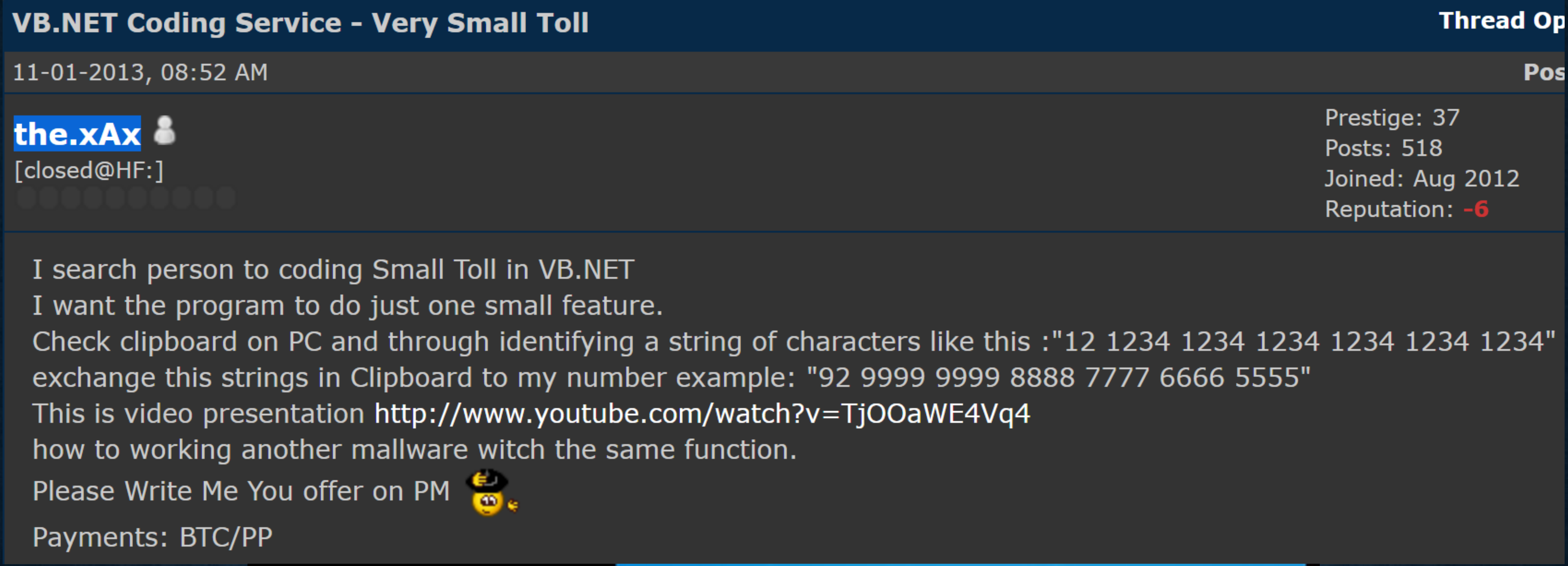
Hello,

Your service is inder the DDoS attack by a polish group 2Pac Team. We have access to 150k bots, 18k polish computers which can be used for DDoS. We have DDoSed some major companies in PL.

We will stop the attack for 600 EUR transferred to our account. This really is a moderate amount of money. Once we get the money, the attacks will stop. Let us know when you are ready for the transfer, we'll send you the details.

Best regards 2Pac Team

P29640429118
50
EURO
EYPΩ
50



VB.NET Coding Service - Very Small Toll

11-01-2013, 08:52 AM

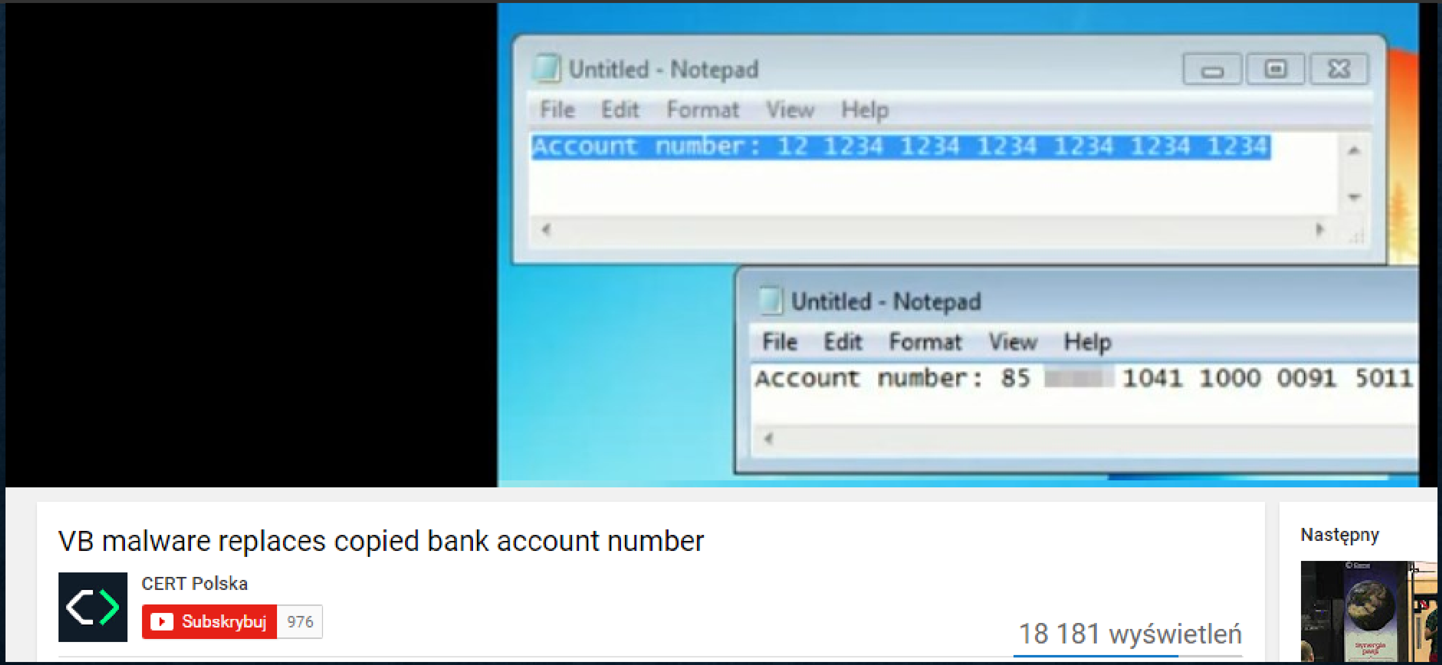
the.xAx

[closed@HF:]

Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

I search person to coding Small Toll in VB.NET
I want the program to do just one small feature.
Check clipboard on PC and through identifying a string of characters like this :"12 1234 1234 1234 1234 1234 1234"
exchange this strings in Clipboard to my number example: "92 9999 9999 8888 7777 6666 5555"
This is video presentation http://www.youtube.com/watch?v=TjOOaWE4Vq4
how to working another mallware witch the same function.
Please Write Me You offer on PM

Payments: BTC/PP



Untitled - Notepad

```
Account number: 12 1234 1234 1234 1234 1234 1234
```

Untitled - Notepad

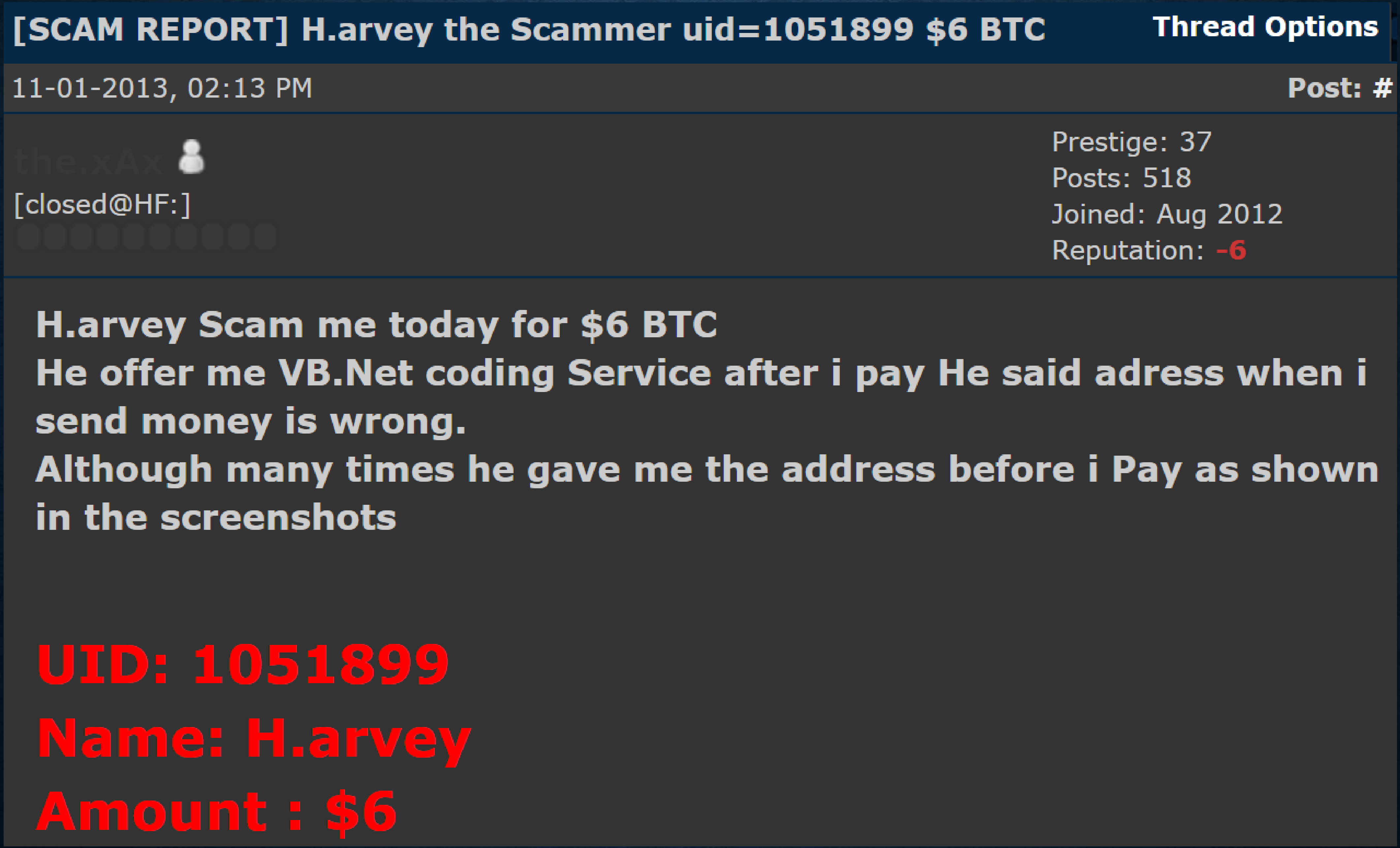
```
Account number: 85 [redacted] 1041 1000 0091 5011
```

VB malware replaces copied bank account number

CERT Polska

18 181 wyświetleń

CONTACT



[SCAM REPORT] H.arvey the Scammer uid=1051899 $6 BTC

11-01-2013, 02:13 PM

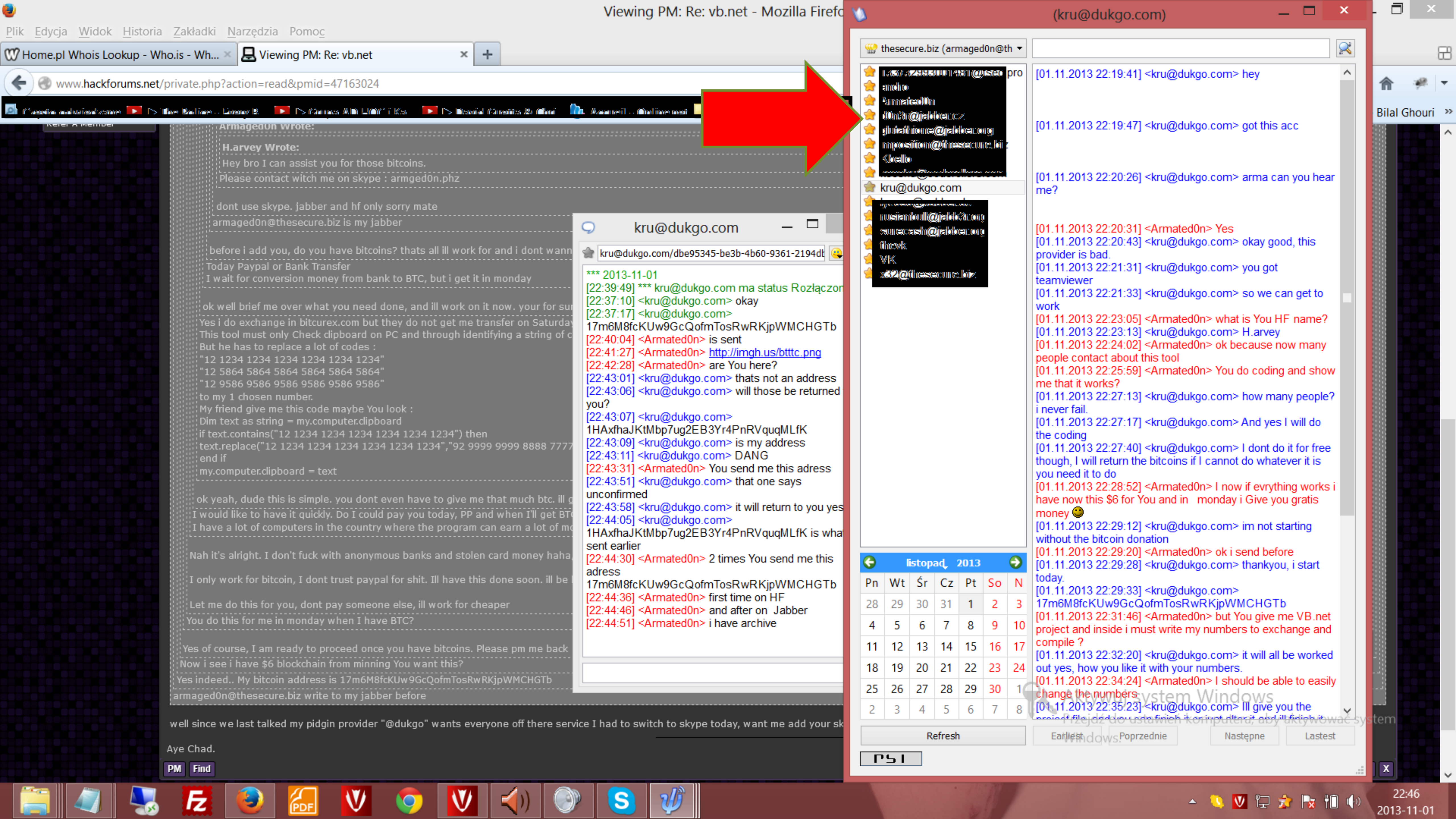
the.xAx

[closed@HF:]

Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

H.arvey Scam me today for $6 BTC
He offer me VB.Net coding Service after i pay He said adress when i send money is wrong.
Although many times he gave me the address before i Pay as shown in the screenshots

UID: 1051899
Name: H.arvey
Amount : $6


Viewing PM: Re: vb.net - Mozilla Firefo
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
Home.pl Whois Lookup - Who.is - Wh...
Viewing PM: Re: vb.net
www.hackforums.net/private.php?action=read&pmid=47163024
Bilal Ghouri
(kru@dukgo.com)
thesecure.biz (armaged0n@th
pro
kru@dukgo.com
listopad 2013
Pn Wt Śr Cz Pt So N
Refresh
Earliest
Poprzednie
Następne
Lastest
22:46
2013-11-01

[redacted]

Armaged0n Wrote:

H.arvey Wrote:

Hey bro I can assist you for those bitcoins.

Please contact witch me on skype : armged0n.phz

dont use skype. jabber and hf only sorry mate

armaged0n@thesecure.biz is my jabber

before i add you, do you have bitcoins? thats all ill work for and i dont wann

Today Paypal or Bank Transfer
I wait for conversion money from bank to BTC, but i get it in monday

ok well brief me over what you need done, and ill work on it now. your for su

Yes i do exchange in bitcurex.com but they do not get me transfer on Saturday
This tool must only Check clipboard on PC and through identifying a string of c
But he has to replace a lot of codes :
"12 1234 1234 1234 1234 1234 1234"
"12 5864 5864 5864 5864 5864 5864"
"12 9586 9586 9586 9586 9586 9586"
to my 1 chosen number.
My friend give me this code maybe You look :

```
Dim text as string = my.computer.clipboard
if text.contains("12 1234 1234 1234 1234 1234 1234") then
text.replace("12 1234 1234 1234 1234 1234 1234","92 9999 9999 8888 7777
end if
my.computer.clipboard = text
```

ok yeah, dude this is simple. you dont even have to give me that much btc. ill g

I would like to have it quickly. Do I could pay you today, PP and when I'll get BT
I have a lot of computers in the country where the program can earn a lot of m

Nah it's alright. I don't fuck with anonymous banks and stolen card money haha,

I only work for bitcoin, I dont trust paypal for shit. Ill have this done soon. ill be

Let me do this for you, dont pay someone else, ill work for cheaper

You do this for me in monday when I have BTC?

Yes of course, I am ready to proceed once you have bitcoins. Please pm me back

Now i see i have $6 blockchain from minning You want this?

Yes indeed.. My bitcoin address is 17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb

armaged0n@thesecure.biz write to my jabber before

well since we last talked my pidgin provider "@dukgo" wants everyone off there service I had to switch to skype today, want me add your sk

Aye Chad.

PM Find

kru@dukgo.com

kru@dukgo.com/dbe95345-be3b-4b60-9361-2194dt

```
*** 2013-11-01
[22:39:49] *** kru@dukgo.com ma status Rozłączor
[22:37:10] <kru@dukgo.com> okay
[22:37:17] <kru@dukgo.com>
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[22:40:04] <Armated0n> is sent
[22:41:27] <Armated0n> http://imgh.us/btttc.png
[22:42:28] <Armated0n> are You here?
[22:43:01] <kru@dukgo.com> thats not an address
[22:43:06] <kru@dukgo.com> will those be returned
you?
[22:43:07] <kru@dukgo.com>
1HAxfhaJKtMbp7ug2EB3Yr4PnRVquqMLfK
[22:43:09] <kru@dukgo.com> is my address
[22:43:11] <kru@dukgo.com> DANG
[22:43:31] <Armated0n> You send me this adress
[22:43:51] <kru@dukgo.com> that one says
unconfirmed
[22:43:58] <kru@dukgo.com> it will return to you yes
[22:44:05] <kru@dukgo.com>
1HAxfhaJKtMbp7ug2EB3Yr4PnRVquqMLfK is wha
sent earlier
[22:44:30] <Armated0n> 2 times You send me this
adress
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[22:44:36] <Armated0n> first time on HF
[22:44:46] <Armated0n> and after on  Jabber
[22:44:51] <Armated0n> i have archive
```

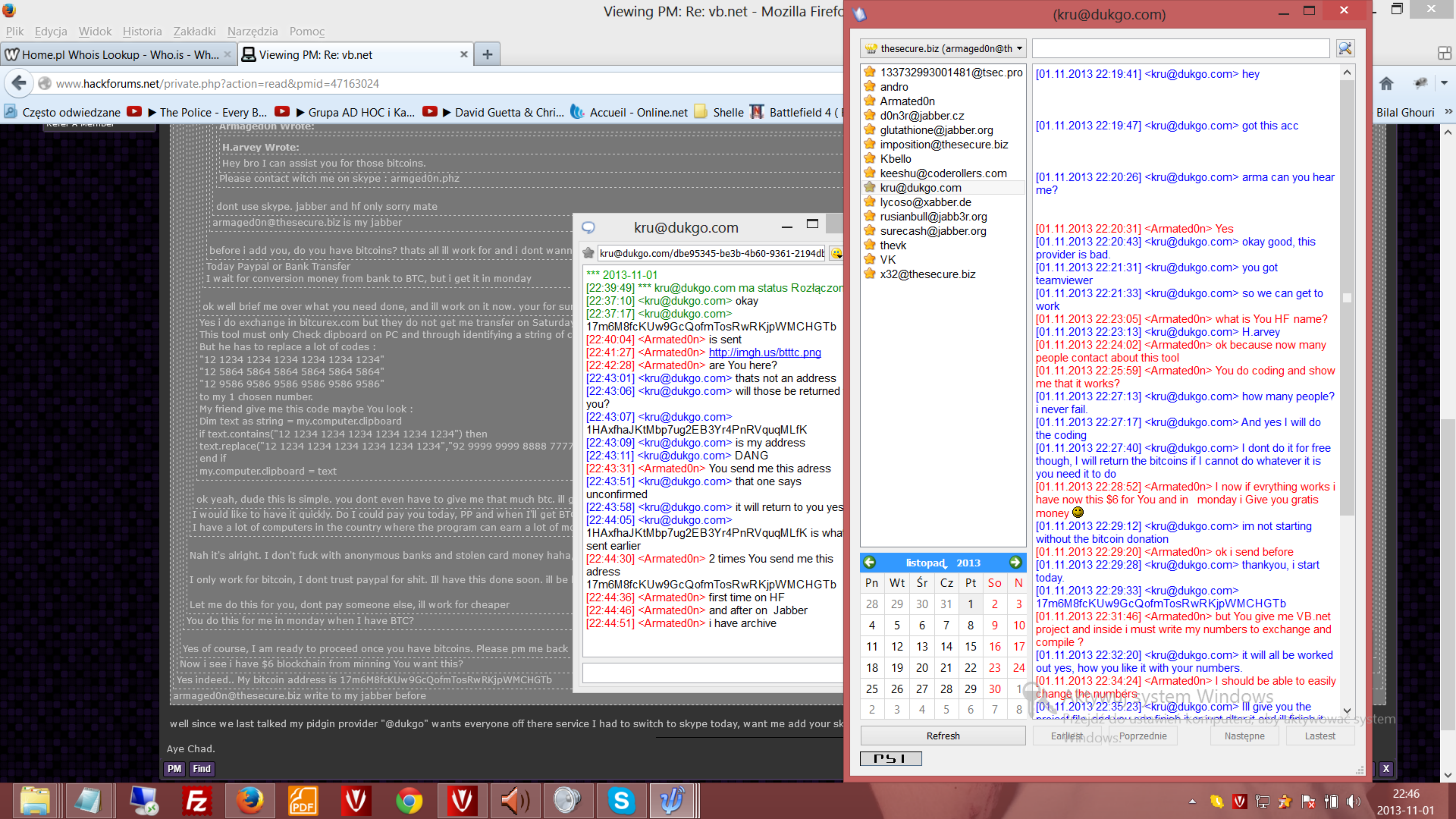
[redacted]

kru@dukgo.com

[redacted]

Pn	Wt	Śr	Cz	Pt	So	N
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

```
[01.11.2013 22:19:41] <kru@dukgo.com> hey
[01.11.2013 22:19:47] <kru@dukgo.com> got this acc
[01.11.2013 22:20:26] <kru@dukgo.com> arma can you hear
me?
[01.11.2013 22:20:31] <Armated0n> Yes
[01.11.2013 22:20:43] <kru@dukgo.com> okay good, this
provider is bad.
[01.11.2013 22:21:31] <kru@dukgo.com> you got
teamviewer
[01.11.2013 22:21:33] <kru@dukgo.com> so we can get to
work
[01.11.2013 22:23:05] <Armated0n> what is You HF name?
[01.11.2013 22:23:13] <kru@dukgo.com> H.arvey
[01.11.2013 22:24:02] <Armated0n> ok because now many
people contact about this tool
[01.11.2013 22:25:59] <Armated0n> You do coding and show
me that it works?
[01.11.2013 22:27:13] <kru@dukgo.com> how many people?
i never fail.
[01.11.2013 22:27:17] <kru@dukgo.com> And yes I will do
the coding
[01.11.2013 22:27:40] <kru@dukgo.com> I dont do it for free
though, I will return the bitcoins if I cannot do whatever it is
you need it to do
[01.11.2013 22:28:52] <Armated0n> I now if evrything works i
have now this $6 for You and in  monday i Give you gratis
money ☺
[01.11.2013 22:29:12] <kru@dukgo.com> im not starting
without the bitcoin donation
[01.11.2013 22:29:20] <Armated0n> ok i send before
[01.11.2013 22:29:28] <kru@dukgo.com> thankyou, i start
today.
[01.11.2013 22:29:33] <kru@dukgo.com>
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[01.11.2013 22:31:46] <Armated0n> but You give me VB.net
project and inside i must write my numbers to exchange and
compile ?
[01.11.2013 22:32:20] <kru@dukgo.com> it will all be worked
out yes, how you like it with your numbers.
[01.11.2013 22:34:24] <Armated0n> I should be able to easily
change the numbers
[01.11.2013 22:35:23] <kru@dukgo.com> Ill give you the
project file and you can finish it or just alter it and ill finish it
```


Viewing PM: Re: vb.net - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
Home.pl Whois Lookup - Who.is - Wh...
Viewing PM: Re: vb.net
www.hackforums.net/private.php?action=read&pmid=47163024
Często odwiedzane
The Police - Every B...
Grupa AD HOC i Ka...
David Guetta & Chri...
Accueil - Online.net
Shelle
Battlefield 4 (
Bilal Ghouri
PM
Find

Armaged0n Wrote:

H.arvey Wrote:

Hey bro I can assist you for those bitcoins.

Please contact witch me on skype : armged0n.phz

dont use skype. jabber and hf only sorry mate

armaged0n@thesecure.biz is my jabber

before i add you, do you have bitcoins? thats all ill work for and i dont wann

Today Paypal or Bank Transfer
I wait for conversion money from bank to BTC, but i get it in monday

ok well brief me over what you need done, and ill work on it now. your for su

Yes i do exchange in bitcurex.com but they do not get me transfer on Saturday
This tool must only Check clipboard on PC and through identifying a string of c
But he has to replace a lot of codes :
"12 1234 1234 1234 1234 1234 1234"
"12 5864 5864 5864 5864 5864 5864"
"12 9586 9586 9586 9586 9586 9586"
to my 1 chosen number.
My friend give me this code maybe You look :

```
Dim text as string = my.computer.clipboard
if text.contains("12 1234 1234 1234 1234 1234 1234") then
text.replace("12 1234 1234 1234 1234 1234 1234","92 9999 9999 8888 7777
end if
my.computer.clipboard = text
```

ok yeah, dude this is simple. you dont even have to give me that much btc. ill g

I would like to have it quickly. Do I could pay you today, PP and when I'll get BTC
I have a lot of computers in the country where the program can earn a lot of mo

Nah it's alright. I don't fuck with anonymous banks and stolen card money haha,

I only work for bitcoin, I dont trust paypal for shit. Ill have this done soon. ill be

Let me do this for you, dont pay someone else, ill work for cheaper

You do this for me in monday when I have BTC?

Yes of course, I am ready to proceed once you have bitcoins. Please pm me back

Now i see i have $6 blockchain from minning You want this?

Yes indeed.. My bitcoin address is 17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb

armaged0n@thesecure.biz write to my jabber before

well since we last talked my pidgin provider "@dukgo" wants everyone off there service I had to switch to skype today, want me add your sk

Aye Chad.

kru@dukgo.com

kru@dukgo.com/dbe95345-be3b-4b60-9361-2194db

```
*** 2013-11-01
[22:39:49] *** kru@dukgo.com ma status Rozłączon
[22:37:10] <kru@dukgo.com> okay
[22:37:17] <kru@dukgo.com>
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[22:40:04] <Armated0n> is sent
[22:41:27] <Armated0n> http://imgh.us/btttc.png
[22:42:28] <Armated0n> are You here?
[22:43:01] <kru@dukgo.com> thats not an address
[22:43:06] <kru@dukgo.com> will those be returned
you?
[22:43:07] <kru@dukgo.com>
1HAxfhaJKtMbp7ug2EB3Yr4PnRVquqMLfK
[22:43:09] <kru@dukgo.com> is my address
[22:43:11] <kru@dukgo.com> DANG
[22:43:31] <Armated0n> You send me this adress
[22:43:51] <kru@dukgo.com> that one says
unconfirmed
[22:43:58] <kru@dukgo.com> it will return to you yes
[22:44:05] <kru@dukgo.com>
1HAxfhaJKtMbp7ug2EB3Yr4PnRVquqMLfK is wha
sent earlier
[22:44:30] <Armated0n> 2 times You send me this
adress
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[22:44:36] <Armated0n> first time on HF
[22:44:46] <Armated0n> and after on  Jabber
[22:44:51] <Armated0n> i have archive
```

(kru@dukgo.com)

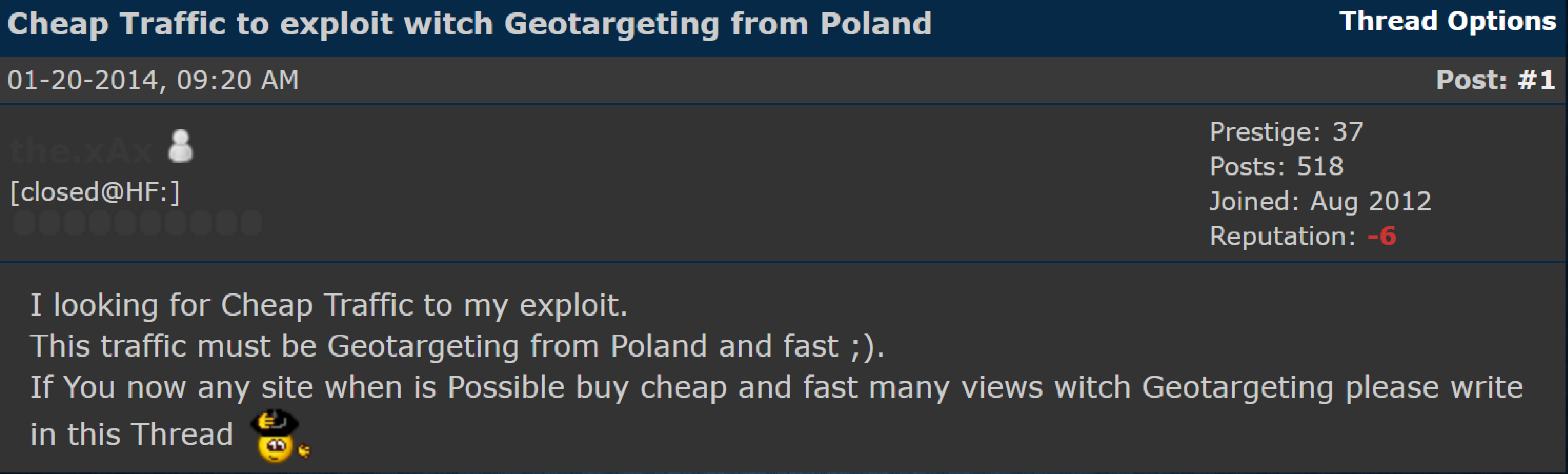
Pn	Wt	Śr	Cz	Pt	So	N
28	29	30	31	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	1
2	3	4	5	6	7	8

```
[01.11.2013 22:19:41] <kru@dukgo.com> hey

[01.11.2013 22:19:47] <kru@dukgo.com> got this acc

[01.11.2013 22:20:26] <kru@dukgo.com> arma can you hear
me?

[01.11.2013 22:20:31] <Armated0n> Yes
[01.11.2013 22:20:43] <kru@dukgo.com> okay good, this
provider is bad.
[01.11.2013 22:21:31] <kru@dukgo.com> you got
teamviewer
[01.11.2013 22:21:33] <kru@dukgo.com> so we can get to
work
[01.11.2013 22:23:05] <Armated0n> what is You HF name?
[01.11.2013 22:23:13] <kru@dukgo.com> H.arvey
[01.11.2013 22:24:02] <Armated0n> ok because now many
people contact about this tool
[01.11.2013 22:25:59] <Armated0n> You do coding and show
me that it works?
[01.11.2013 22:27:13] <kru@dukgo.com> how many people?
i never fail.
[01.11.2013 22:27:17] <kru@dukgo.com> And yes I will do
the coding
[01.11.2013 22:27:40] <kru@dukgo.com> I dont do it for free
though, I will return the bitcoins if I cannot do whatever it is
you need it to do
[01.11.2013 22:28:52] <Armated0n> I now if evrything works i
have now this $6 for You and in   monday i Give you gratis
money ☺
[01.11.2013 22:29:12] <kru@dukgo.com> im not starting
without the bitcoin donation
[01.11.2013 22:29:20] <Armated0n> ok i send before
[01.11.2013 22:29:28] <kru@dukgo.com> thankyou, i start
today.
[01.11.2013 22:29:33] <kru@dukgo.com>
17m6M8fcKUw9GcQofmTosRwRKjpWMCHGTb
[01.11.2013 22:31:46] <Armated0n> but You give me VB.net
project and inside i must write my numbers to exchange and
compile ?
[01.11.2013 22:32:20] <kru@dukgo.com> it will all be worked
out yes, how you like it with your numbers.
[01.11.2013 22:34:24] <Armated0n> I should be able to easily
change the numbers
[01.11.2013 22:35:23] <kru@dukgo.com> Ill give you the
```



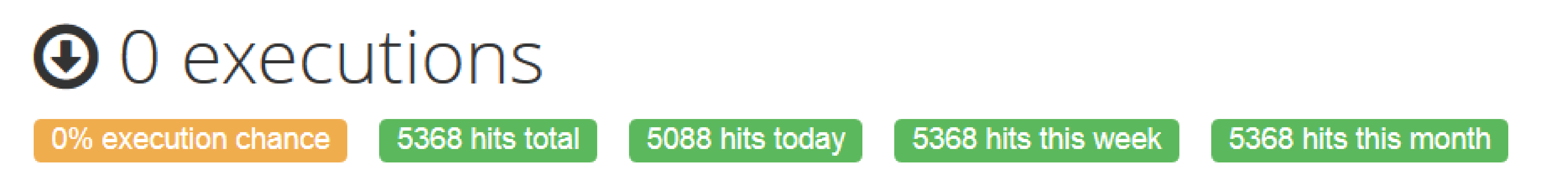
Cheap Traffic to exploit witch Geotargeting from Poland Thread Options

01-20-2014, 09:20 AM Post: #1

the.xAx
[closed@HF:]

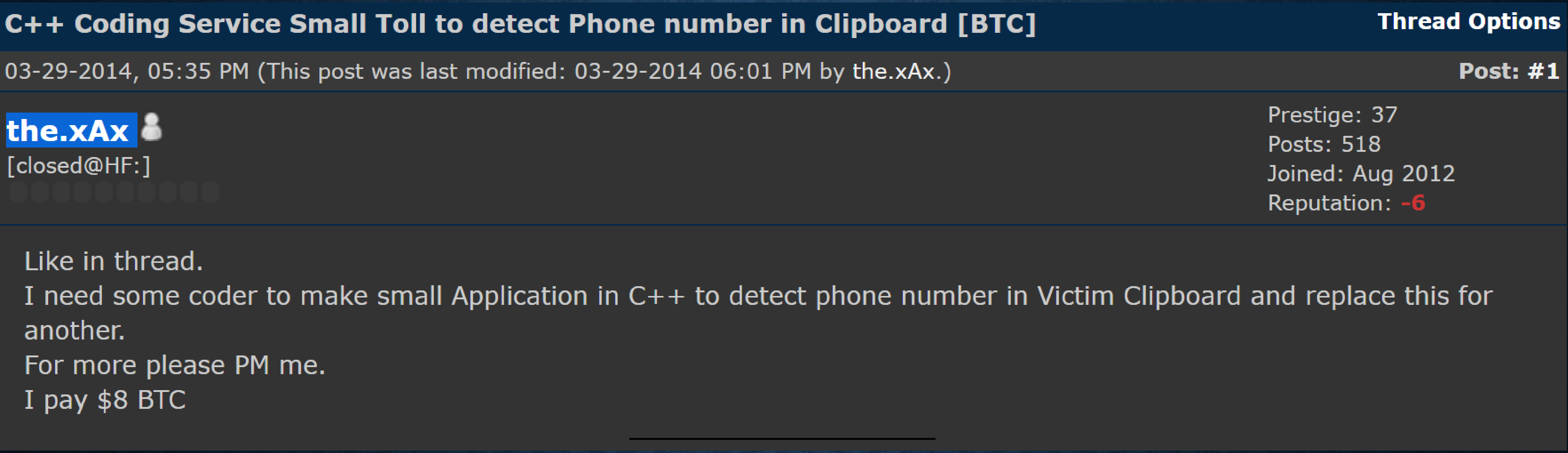
Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

I looking for Cheap Traffic to my exploit.
This traffic must be Geotargeting from Poland and fast ;).
If You now any site when is Possible buy cheap and fast many views witch Geotargeting please write in this Thread



0 executions

0% execution chance | 5368 hits total | 5088 hits today | 5368 hits this week | 5368 hits this month



C++ Coding Service Small Toll to detect Phone number in Clipboard [BTC]

Thread Options

03-29-2014, 05:35 PM (This post was last modified: 03-29-2014 06:01 PM by the.xAx.)

Post: #1

the.xAx

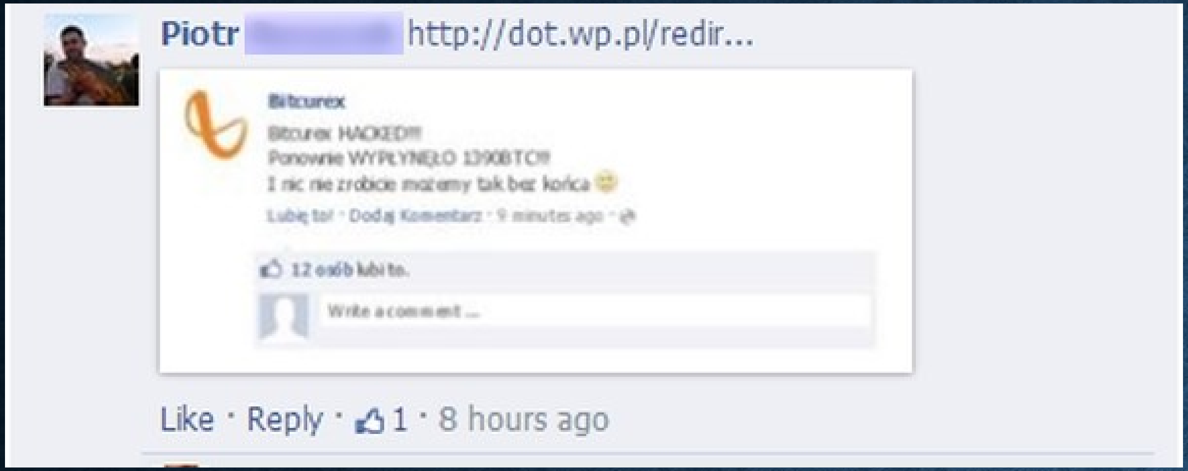
[closed@HF:]

Prestige: 37
Posts: 518
Joined: Aug 2012
Reputation: -6

Like in thread.
I need some coder to make small Application in C++ to detect phone number in Victim Clipboard and replace this for another.
For more please PM me.
I pay $8 BTC

CERT.PL

We have observed a simple VBKlip app created in .NET framework. It is distributed using existing botnet Infrastructure (ex. Andromeda). The malware itself is simplistic– it checks the clipboard for the presence of a string of numbers in the format of a bank account numer and swaps it with another numer, hardcoded in the binary.



Piotr [redacted] http://dot.wp.pl/redir...

Bitcurex

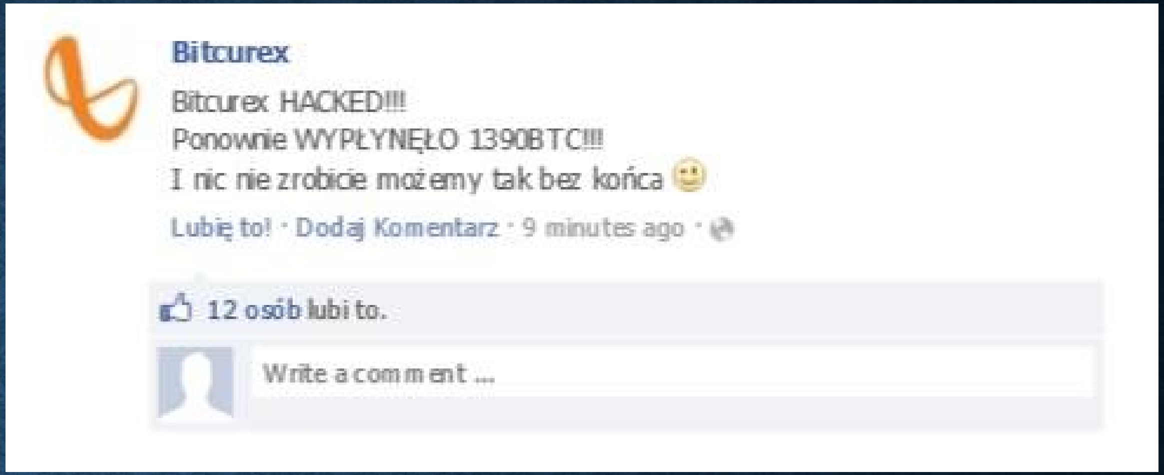
Bitcurex HACKED!!!
Ponownie WYPŁYNEŁO 1390BTC!!!
I nic nie zrobicie możemy tak bez końca 🙂

Lubię to! · Dodaj Komentarz · 9 minutes ago ·

12 osób lubi to.

Write a comment ...

Like · Reply · 1 · 8 hours ago



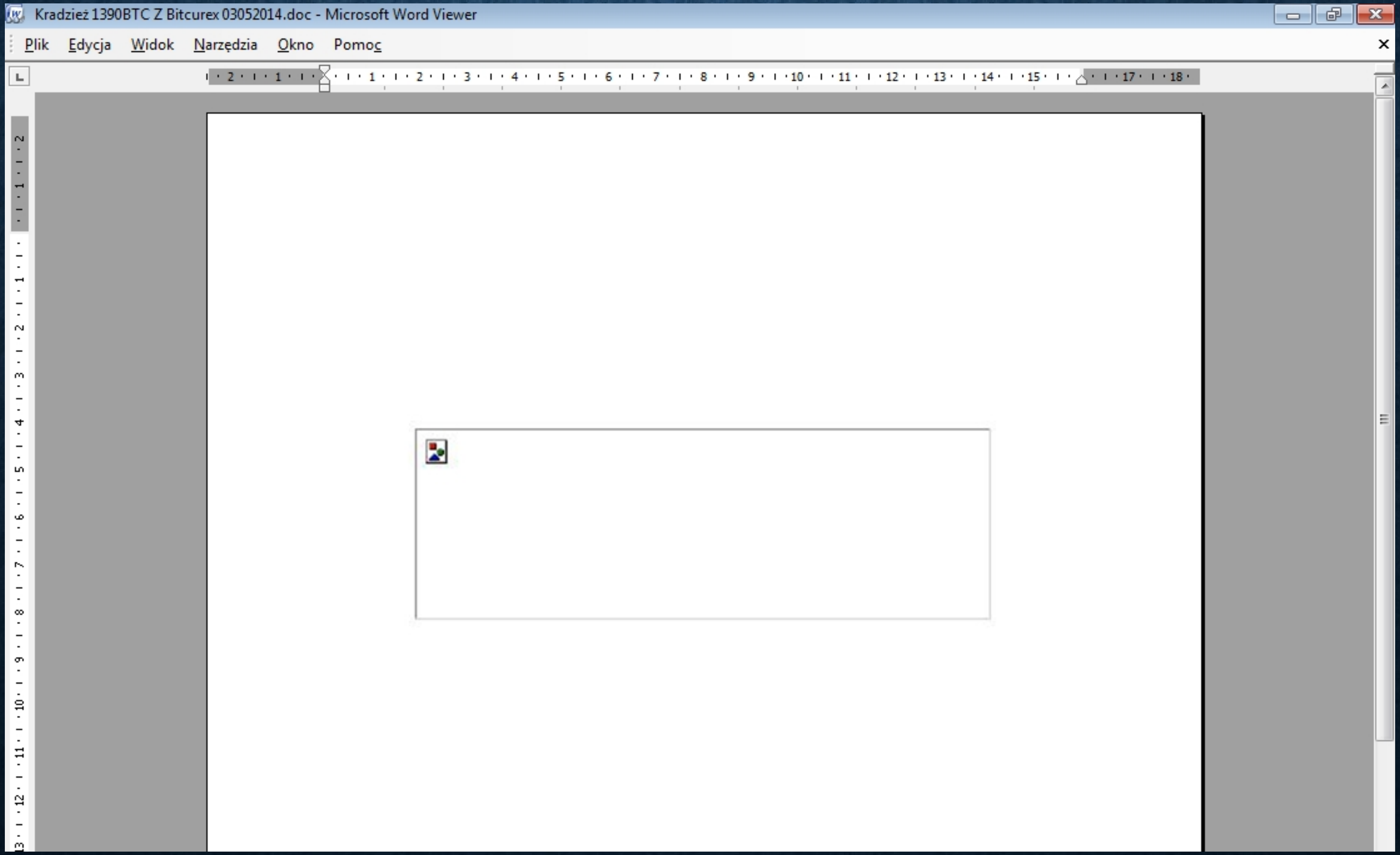
Bitcurex

Bitcurex HACKED!!!
Ponownie WYPŁYNEŁO 1390BTC!!!
I nic nie zrobicie możemy tak bez końca 🙂

Lubię to! · Dodaj Komentarz · 9 minutes ago ·

12 osób lubi to.

Write a comment ...



Kradzież 1390BTC Z Bitcurex 03052014.doc - Microsoft Word Viewer

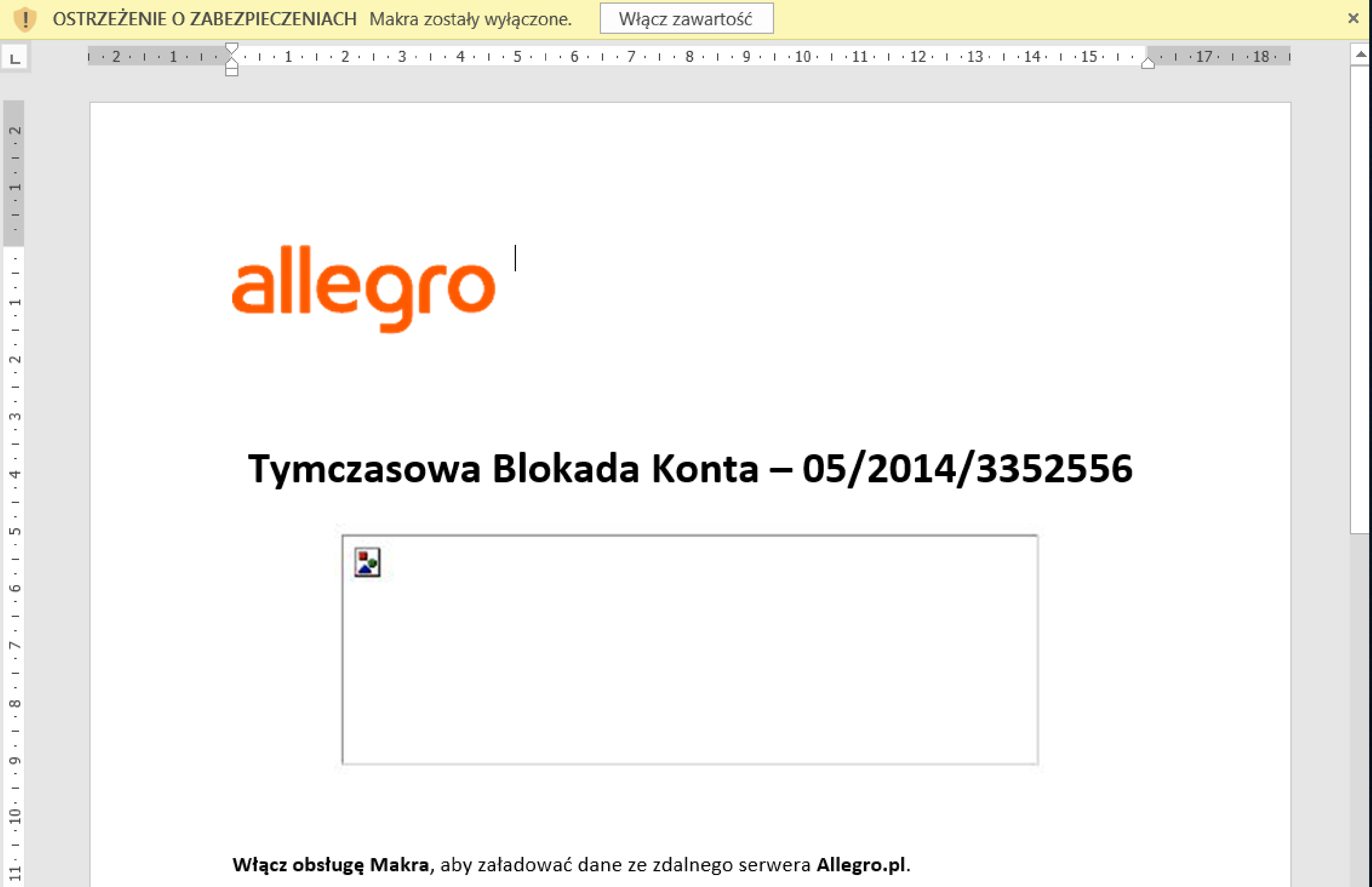
Dear User!

You Allegro account will be soon locked because your auction [real live auction title here] contains forbidden elements in its description.

You can find details of your infingement in the attached document Allegro-05-2014-52556.doc

Best regards Andrew Jones,

Stewardship Monitoring Section, Allegro

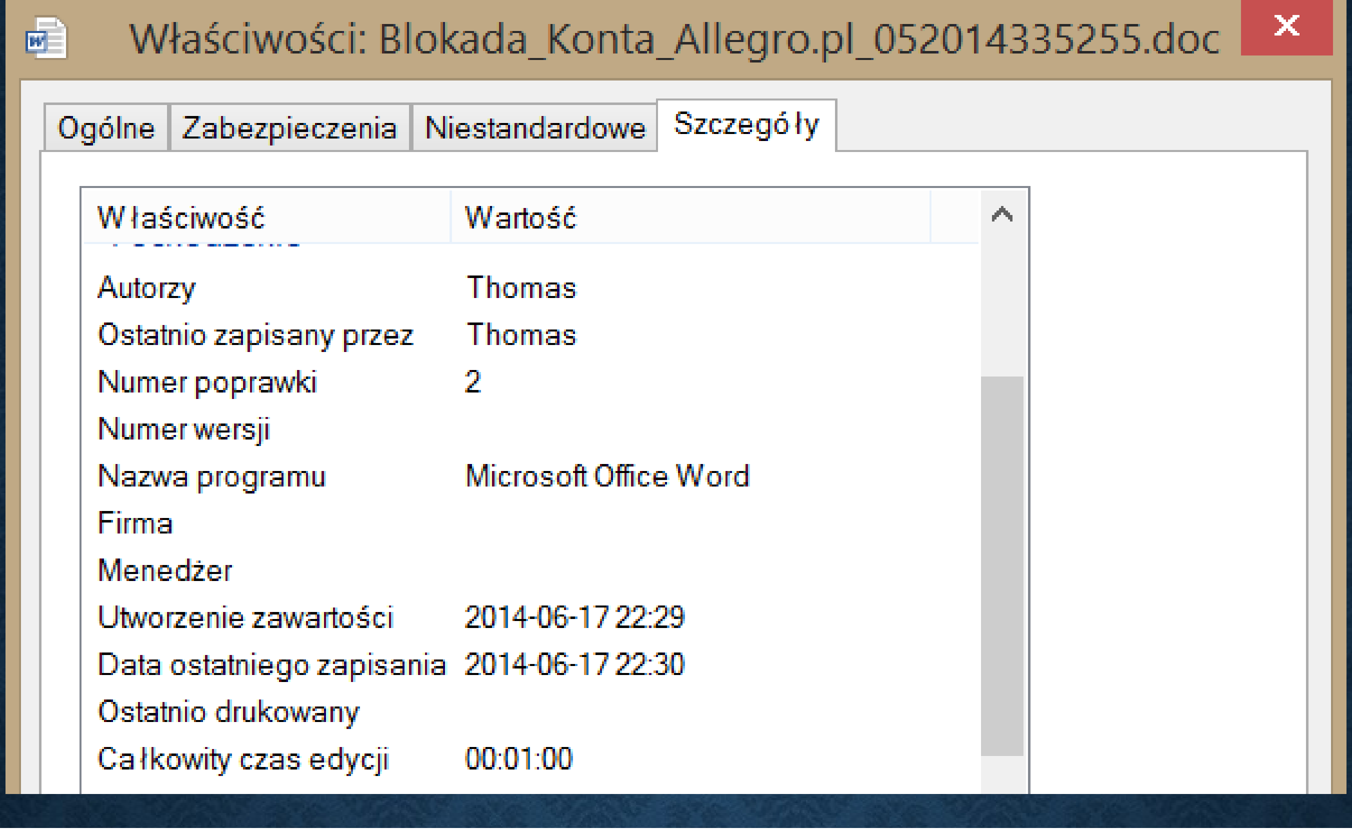


OSTRZEŻENIE O ZABEZPIECZENIACH Makra zostały wyłączone.

allegro

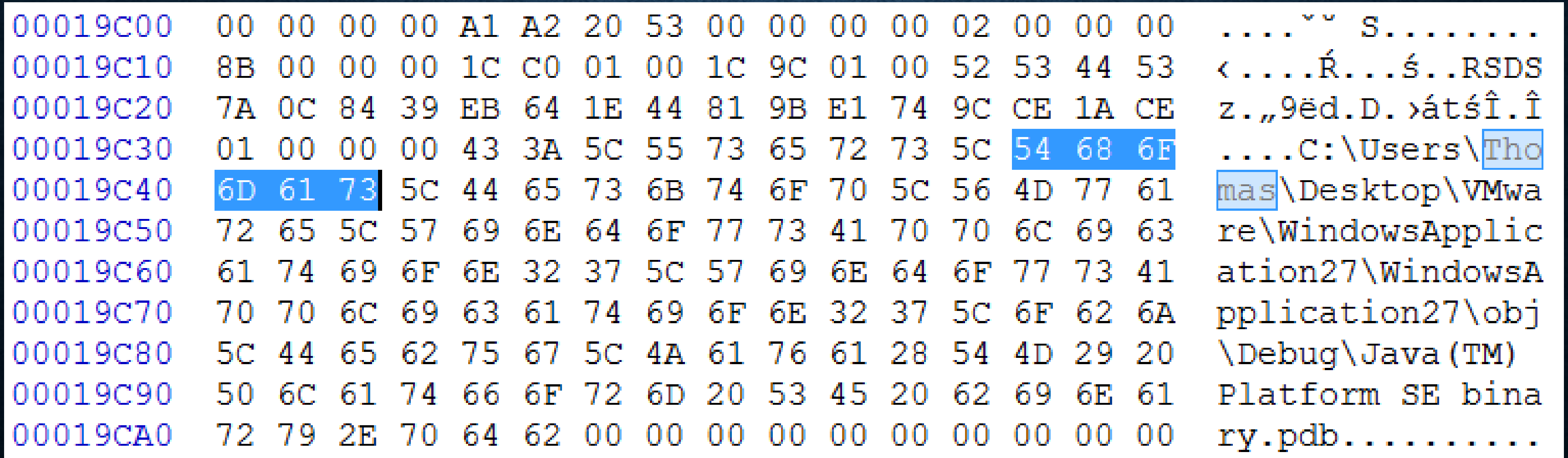
Tymczasowa Blokada Konta – 05/2014/3352556

Włącz obsługę Makra, aby załadować dane ze zdalnego serwera **Allegro.pl**.

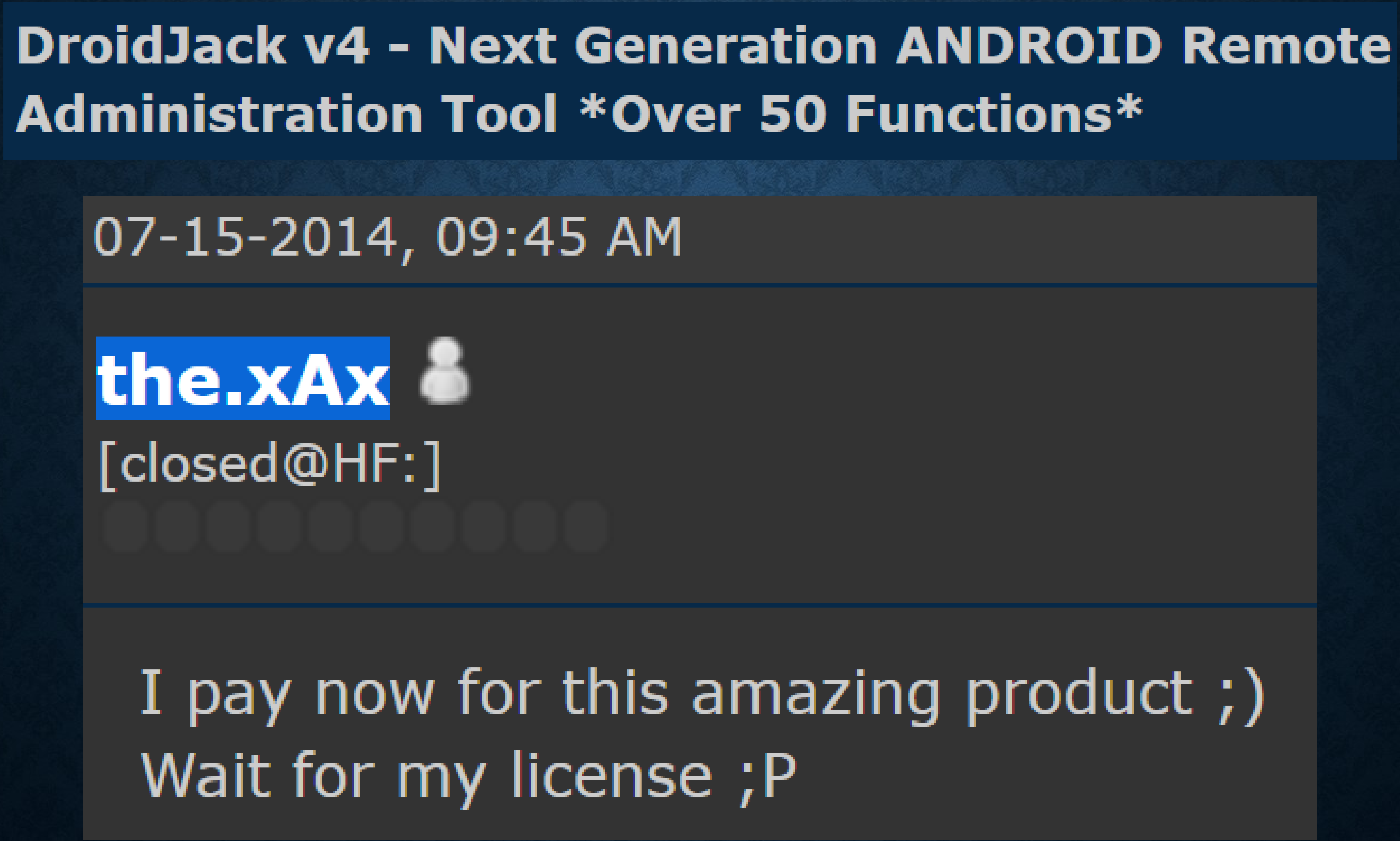


Właściwości: Blokada_Konta_Allegro.pl_052014335255.doc

Właściwość	Wartość
Autorzy	Thomas
Ostatnio zapisany przez	Thomas
Numer poprawki	2
Numer wersji	
Nazwa programu	Microsoft Office Word
Firma	
Menedżer	
Utworzenie zawartości	2014-06-17 22:29
Data ostatniego zapisania	2014-06-17 22:30
Ostatnio drukowany	
Całkowity czas edycji	00:01:00



```
00019C00  00 00 00 00 A1 A2 20 53 00 00 00 00 02 00 00 00  ....ˇ˘ S........
00019C10  8B 00 00 00 1C C0 01 00 1C 9C 01 00 52 53 44 53  ‹....Ŕ...ś..RSDS
00019C20  7A 0C 84 39 EB 64 1E 44 81 9B E1 74 9C CE 1A CE  z.„9ëd.D.›átśÎ.Î
00019C30  01 00 00 00 43 3A 5C 55 73 65 72 73 5C 54 68 6F  ....C:\Users\Tho
00019C40  6D 61 73 5C 44 65 73 6B 74 6F 70 5C 56 4D 77 61  mas\Desktop\VMwa
00019C50  72 65 5C 57 69 6E 64 6F 77 73 41 70 70 6C 69 63  re\WindowsApplic
00019C60  61 74 69 6F 6E 32 37 5C 57 69 6E 64 6F 77 73 41  ation27\WindowsA
00019C70  70 70 6C 69 63 61 74 69 6F 6E 32 37 5C 6F 62 6A  pplication27\obj
00019C80  5C 44 65 62 75 67 5C 4A 61 76 61 28 54 4D 29 20  \Debug\Java(TM)
00019C90  50 6C 61 74 66 6F 72 6D 20 53 45 20 62 69 6E 61  Platform SE bina
00019CA0  72 79 2E 70 64 62 00 00 00 00 00 00 00 00 00 00  ry.pdb..........
```



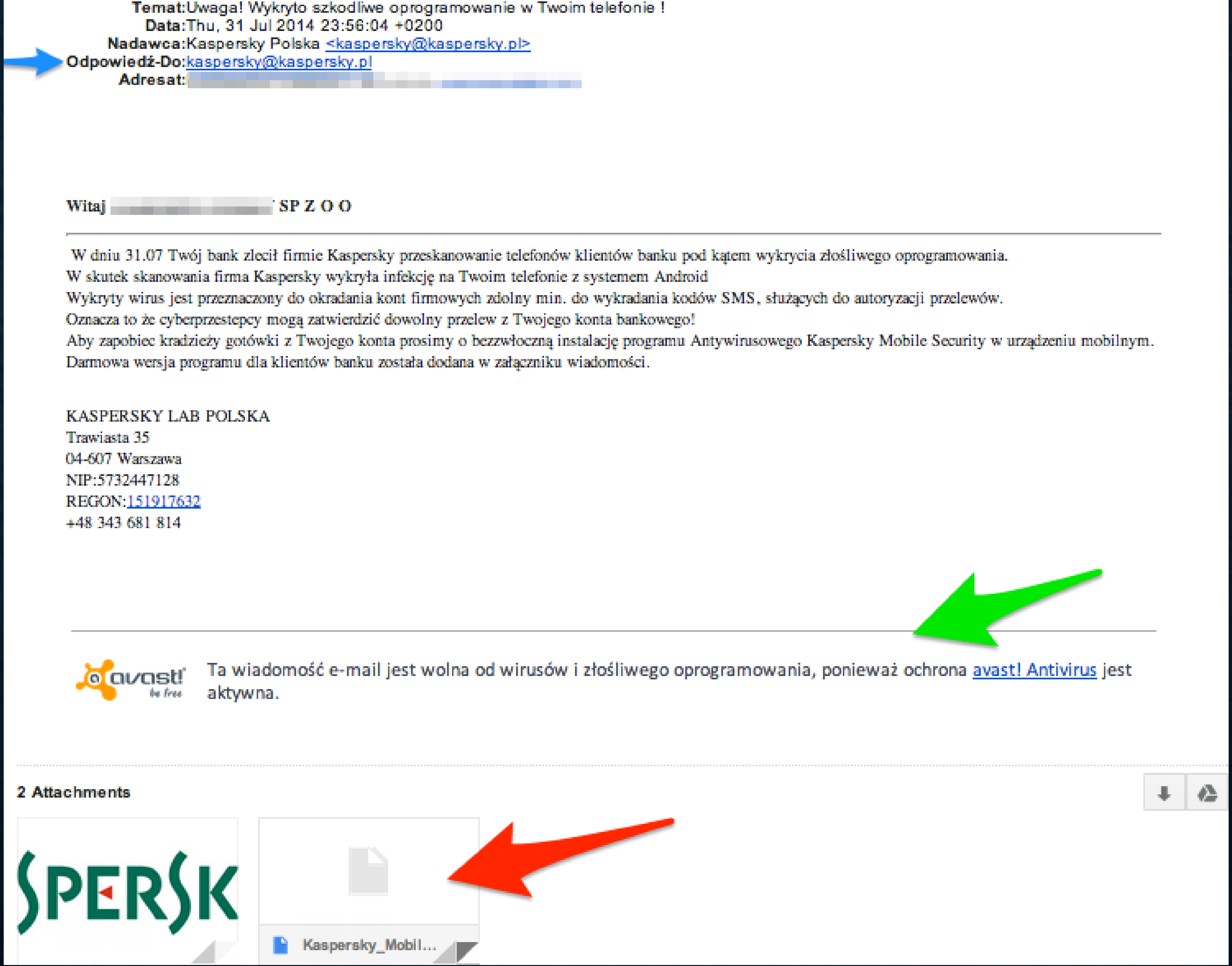
DroidJack v4 - Next Generation ANDROID Remote Administration Tool *Over 50 Functions*

07-15-2014, 09:45 AM

the.xAx

[closed@HF:]

I pay now for this amazing product ;)
Wait for my license ;P



Temat: Uwaga! Wykryto szkodliwe oprogramowanie w Twoim telefonie !
Data: Thu, 31 Jul 2014 23:56:04 +0200
Nadawca: Kaspersky Polska <kaspersky@kaspersky.pl>
Odpowiedź-Do:kaspersky@kaspersky.pl
Adresat:[redacted]

Witaj [redacted] SP Z O O

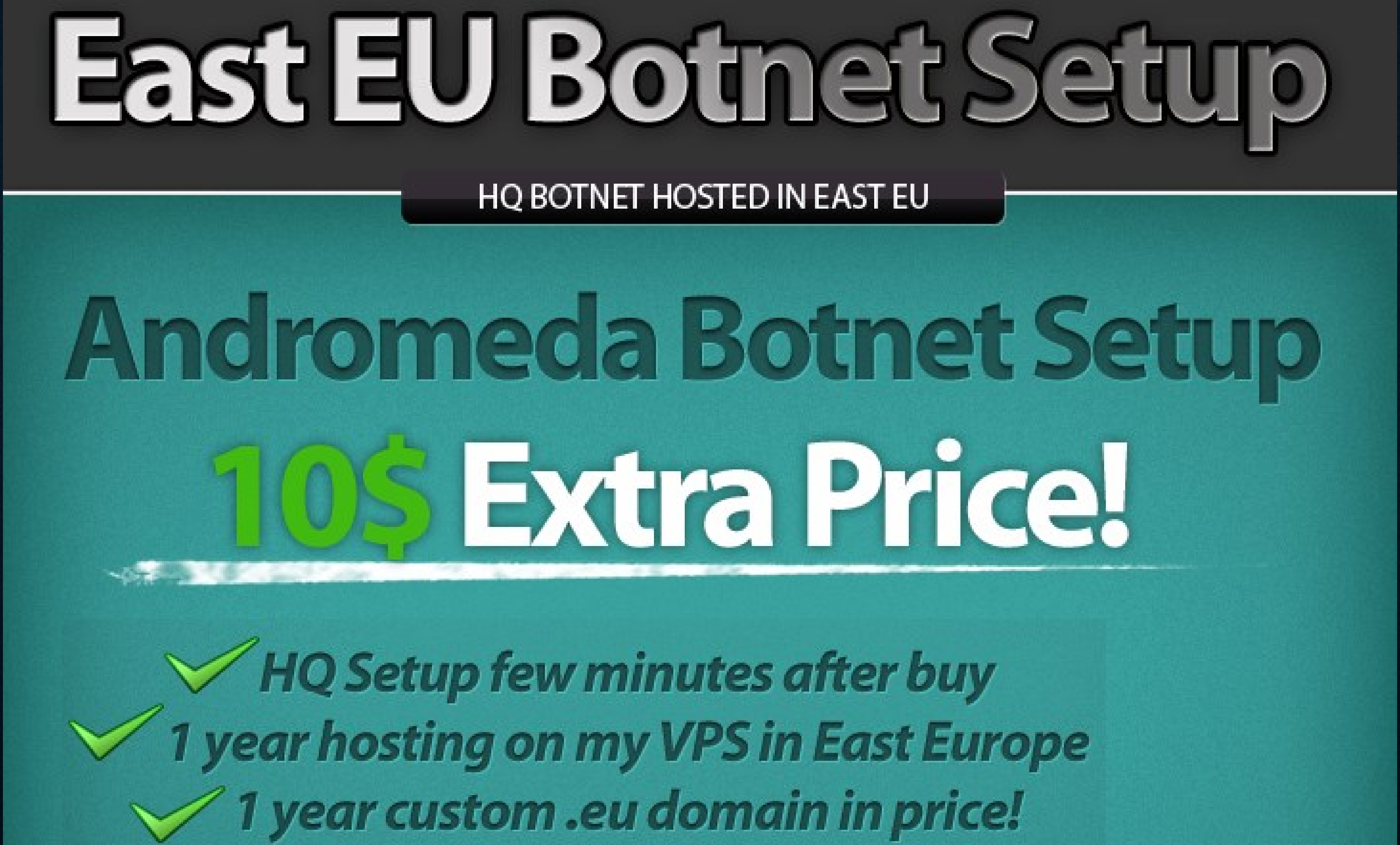
W dniu 31.07 Twój bank zlecił firmie Kaspersky przeskanowanie telefonów klientów banku pod kątem wykrycia złośliwego oprogramowania.
W skutek skanowania firma Kaspersky wykryła infekcję na Twoim telefonie z systemem Android
Wykryty wirus jest przeznaczony do okradania kont firmowych zdolny min. do wykradania kodów SMS, służących do autoryzacji przelewów.
Oznacza to że cyberprzestepcy mogą zatwierdzić dowolny przelew z Twojego konta bankowego!
Aby zapobiec kradzieży gotówki z Twojego konta prosimy o bezzwłoczną instalację programu Antywirusowego Kaspersky Mobile Security w urządzeniu mobilnym.
Darmowa wersja programu dla klientów banku została dodana w załączniku wiadomości.

KASPERSKY LAB POLSKA
Trawiasta 35
04-607 Warszawa
NIP:5732447128
REGON:151917632
+48 343 681 814

Ta wiadomość e-mail jest wolna od wirusów i złośliwego oprogramowania, ponieważ ochrona avast! Antivirus jest aktywna.

2 Attachments

Kaspersky_Mobil...



East EU Botnet Setup

HQ BOTNET HOSTED IN EAST EU

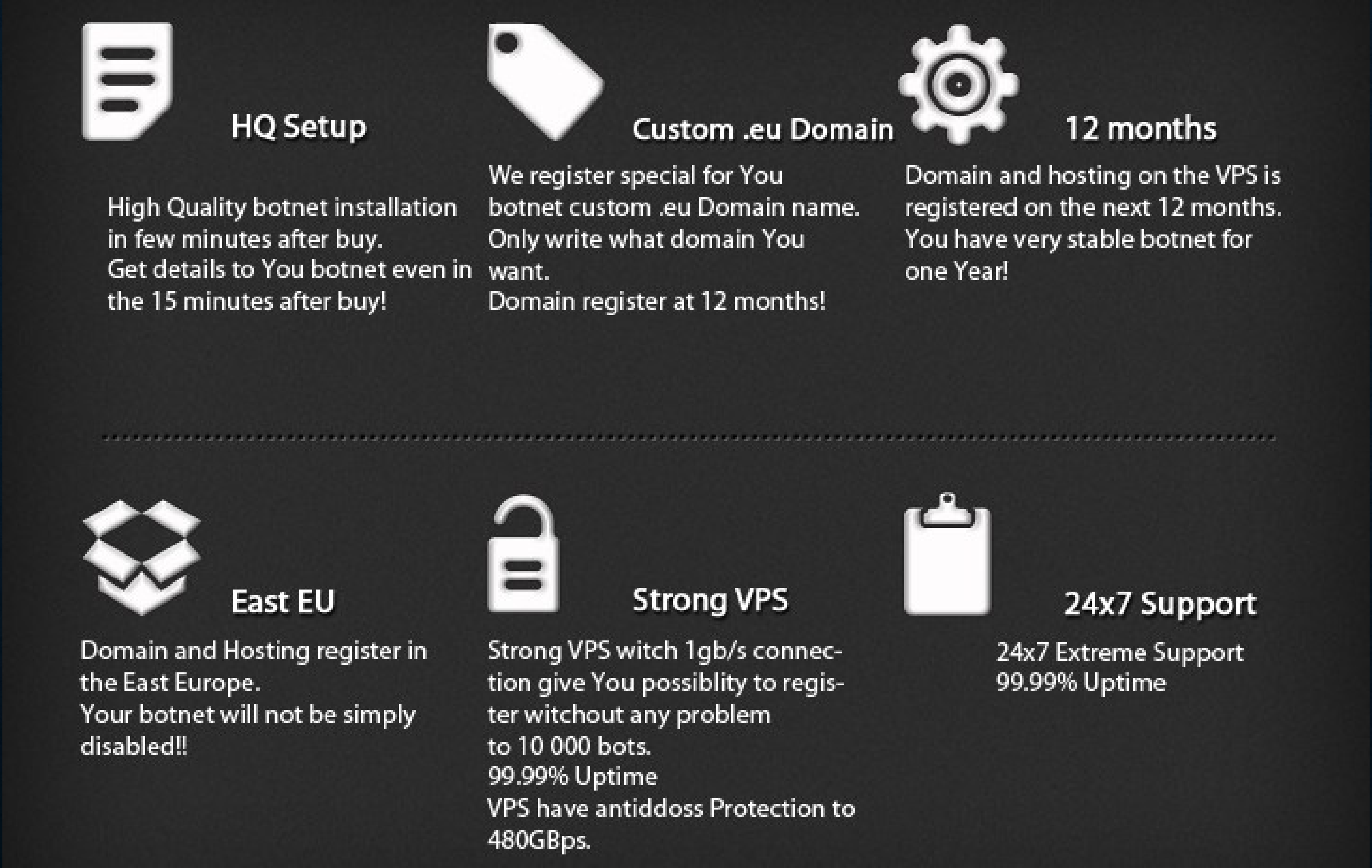
Andromeda Botnet Setup

10$ Extra Price!

✓ *HQ Setup few minutes after buy*

✓ *1 year hosting on my VPS in East Europe*

✓ *1 year custom .eu domain in price!*



HQ Setup

High Quality botnet installation in few minutes after buy.
Get details to You botnet even in the 15 minutes after buy!

Custom .eu Domain

We register special for You botnet custom .eu Domain name.
Only write what domain You want.
Domain register at 12 months!

12 months

Domain and hosting on the VPS is registered on the next 12 months.
You have very stable botnet for one Year!

East EU

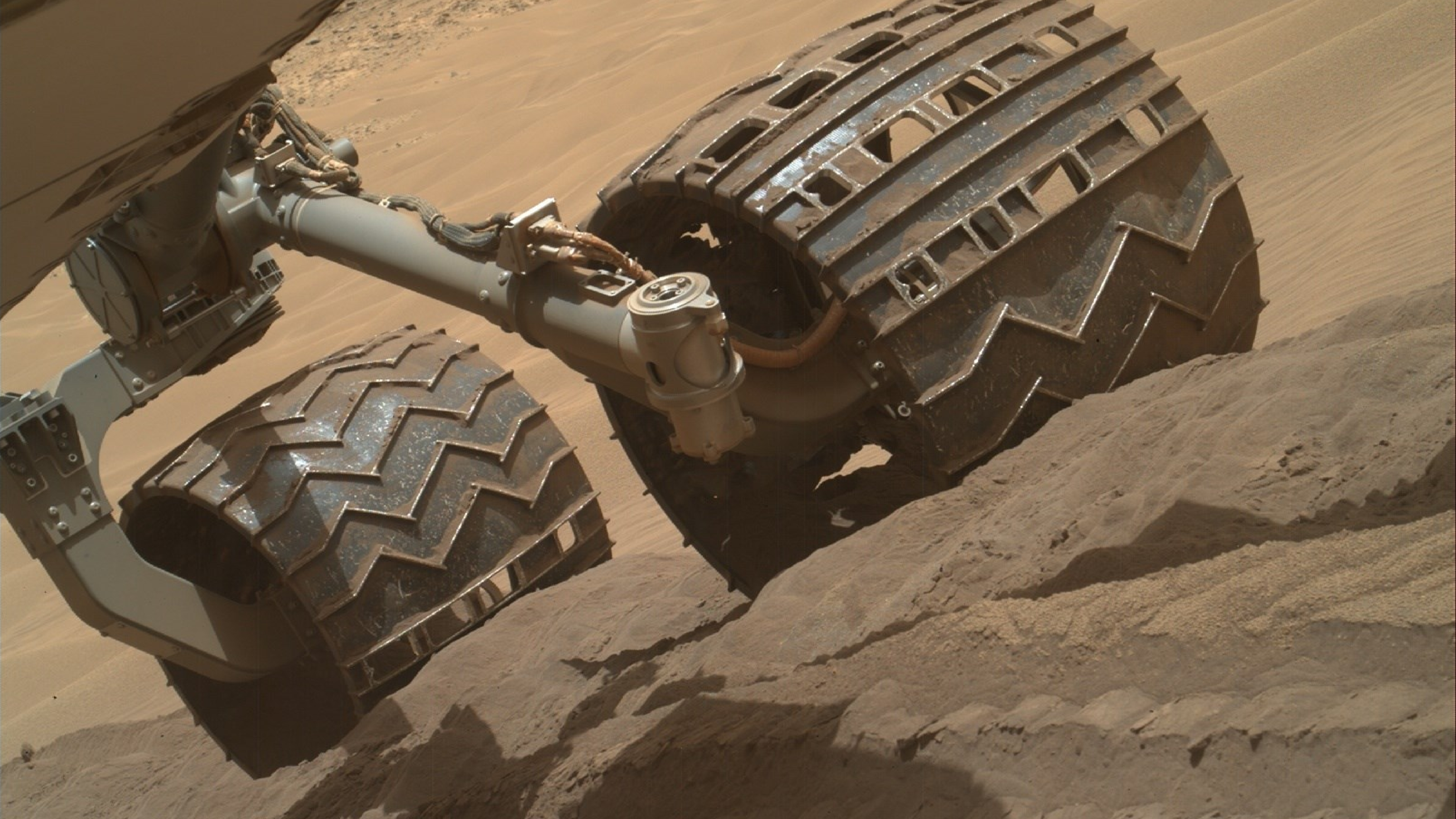
Domain and Hosting register in the East Europe.
Your botnet will not be simply disabled!!

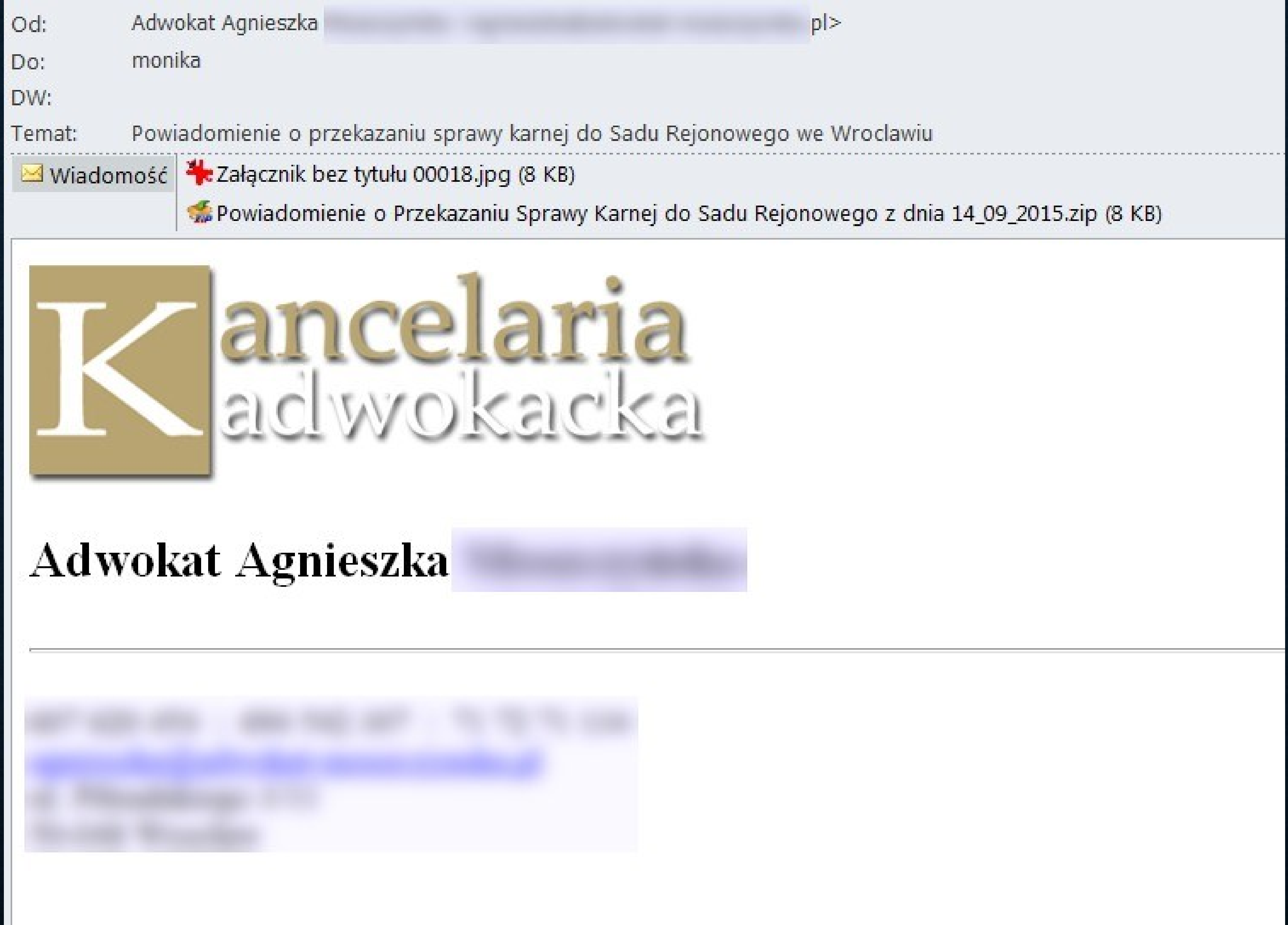
Strong VPS

Strong VPS witch 1gb/s connection give You possiblity to register witchout any problem
to 10 000 bots.
99.99% Uptime
VPS have antiddoss Protection to 480GBps.

24x7 Support

24x7 Extreme Support
99.99% Uptime





Od: Adwokat Agnieszka [redacted]pl>

Do: monika

DW:

Temat: Powiadomienie o przekazaniu sprawy karnej do Sadu Rejonowego we Wroclawiu

Wiadomość

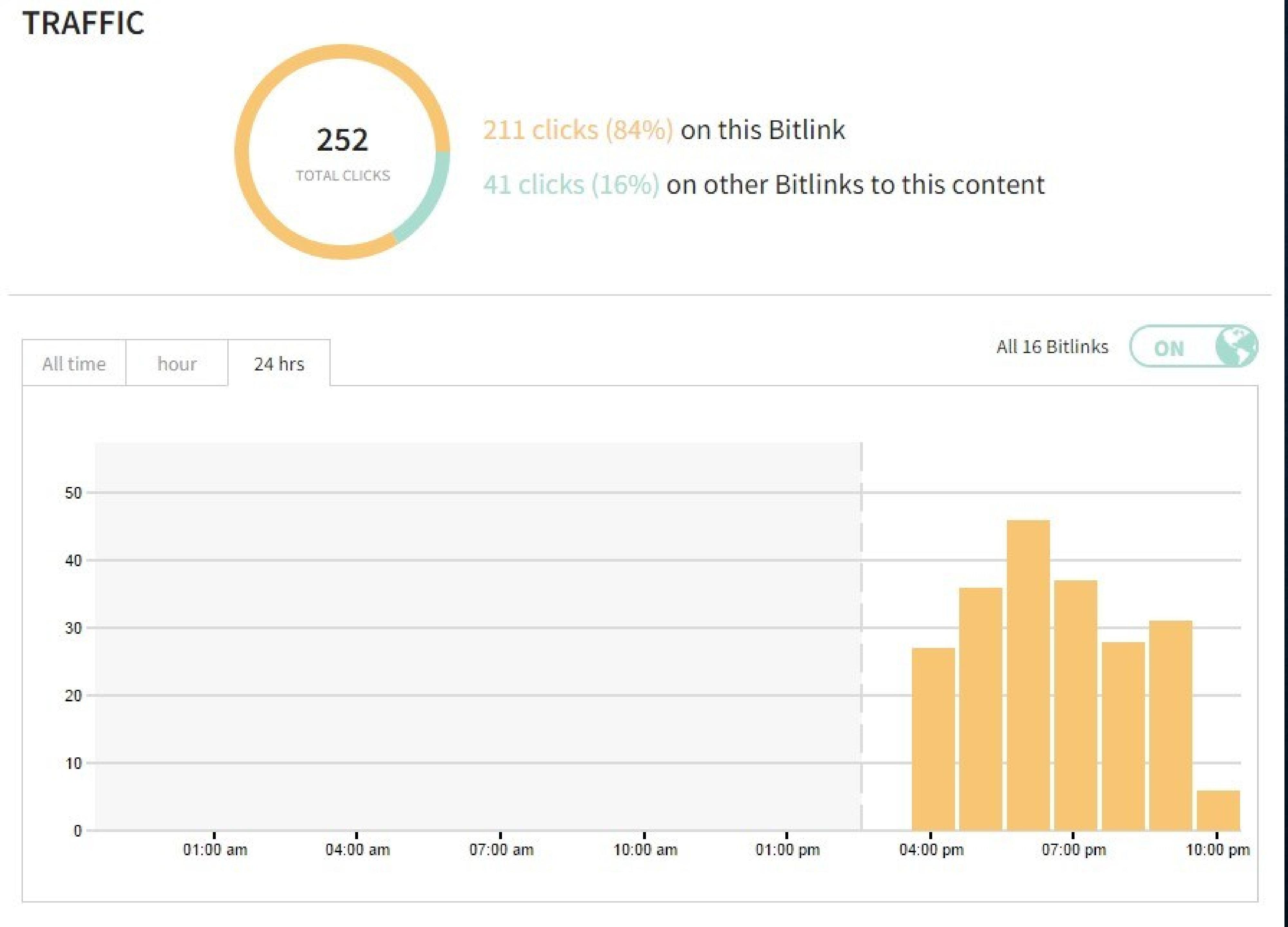
Załącznik bez tytułu 00018.jpg (8 KB)

Powiadomienie o Przekazaniu Sprawy Karnej do Sadu Rejonowego z dnia 14_09_2015.zip (8 KB)

Kancelaria
adwokacka

Adwokat Agnieszka [redacted]

[redacted]



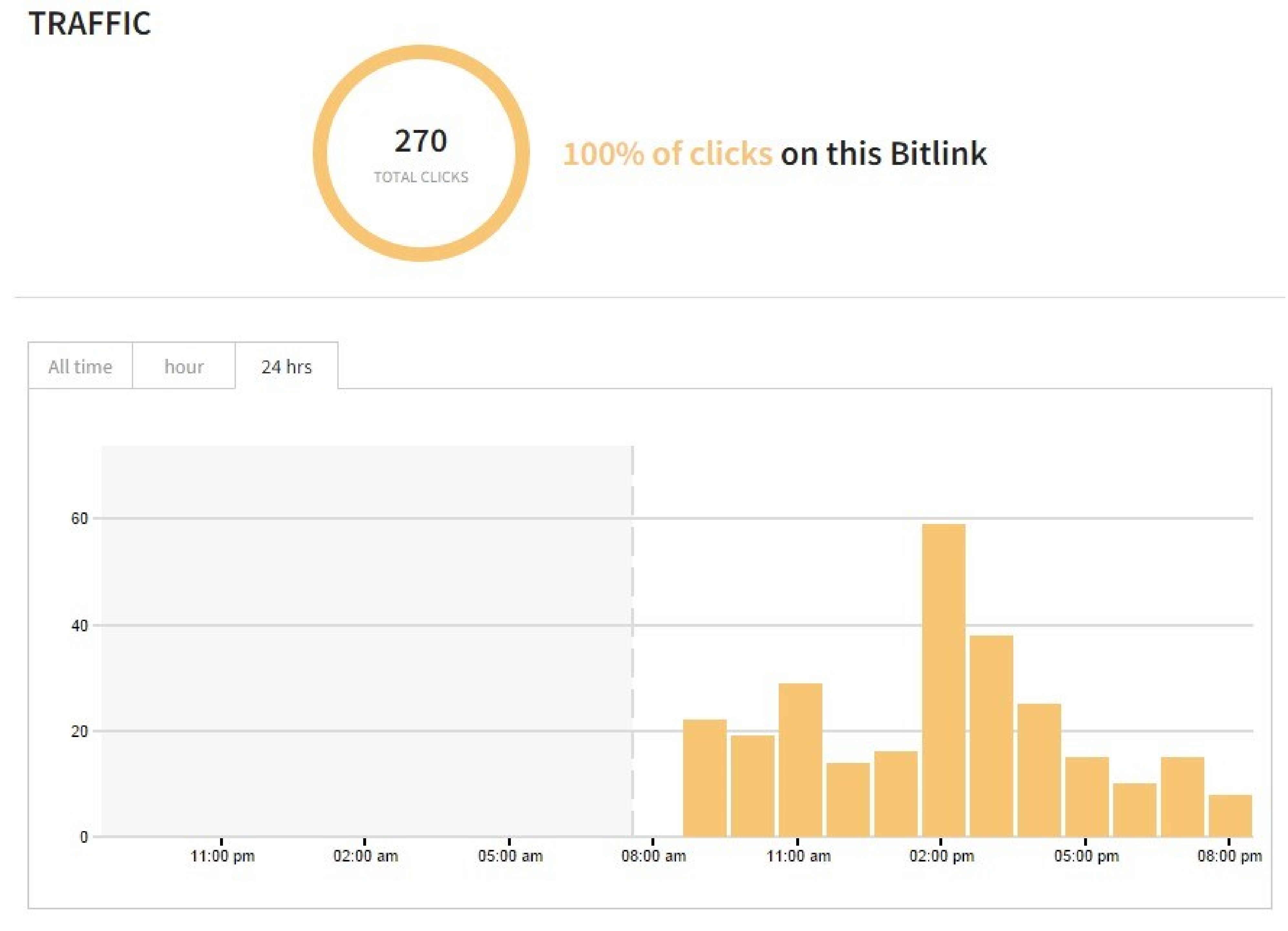
TRAFFIC

252

TOTAL CLICKS

211 clicks (84%) on this Bitlink

41 clicks (16%) on other Bitlinks to this content



TRAFFIC

270

TOTAL CLICKS

100% of clicks on this Bitlink

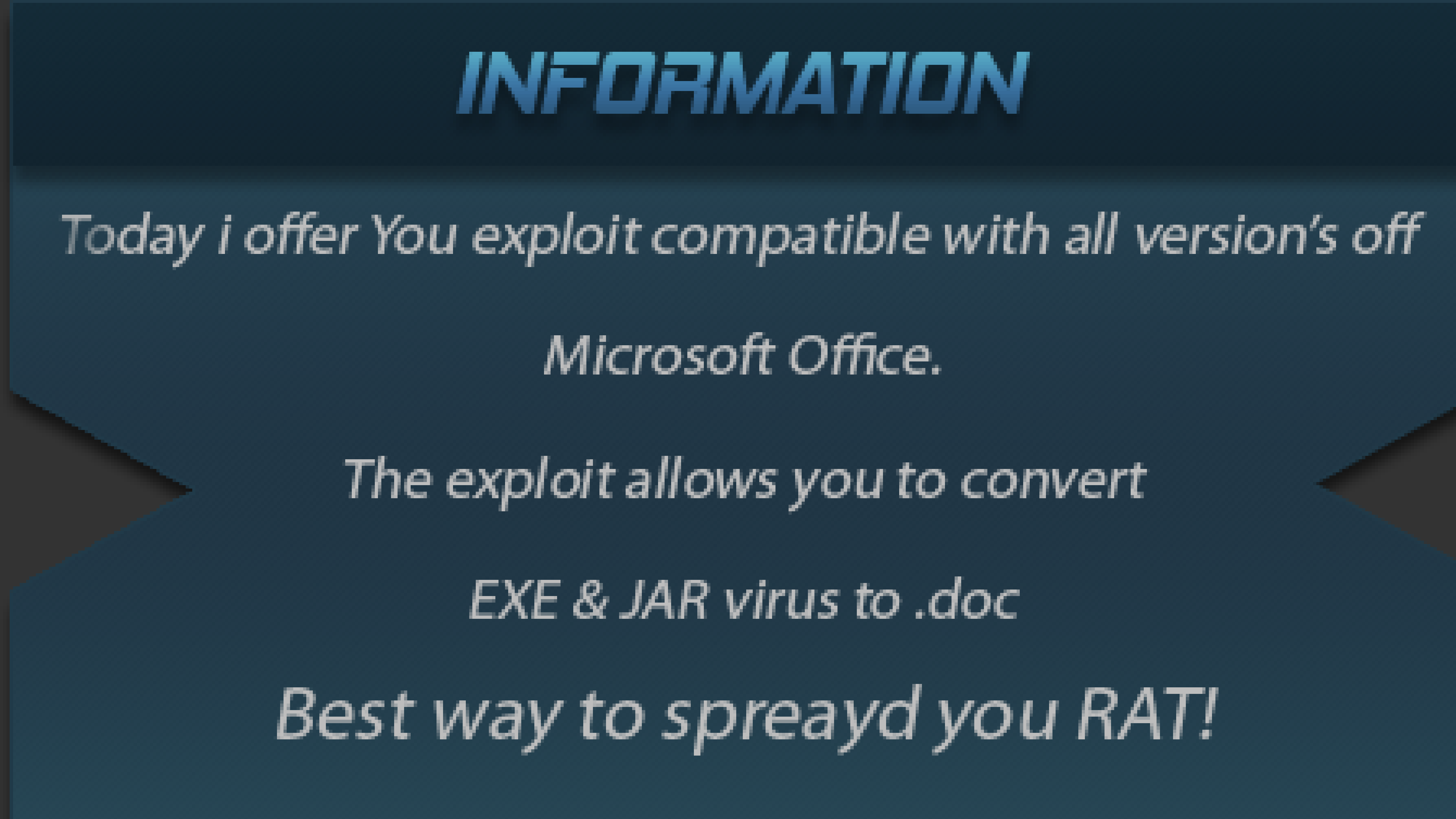
RE: I was expecting someone speaking russian

Thomas: it's obvious it's me, I keep using the same spam servers, they already wrote about it on z3s

Thomas: we have to end spam runs, it's a tragedy because of Adam and the publicity he gets us, 50k emails and only 1k infections

Thomas: it used to be 10%, cert is hunting us 24/7

RE: I don't know why I'm waisting my time on this



INFORMATION

Today i offer You exploit compatible with all version's off Microsoft Office.

The exploit allows you to convert EXE & JAR virus to .doc

Best way to spreayd you RAT!

FEATURE

- 100% private ✓
- Bulk Mailer Gratis! ✓
- Free Crypting ✓
- Best price on HF ✓
- Works on X32 and X64 ✓
- Any Mallware Compatible ✓

- ✓ 30kb stub size!
- ✓ All Office Version!
- ✓ Ease of use
- ✓ Stable
- ✓ Team Viewer Support
- ✓ Spread on E-mails, Facebook, etc!

PRICE

MACRO

2/34 AV!
Best Price!

ONLY $39!

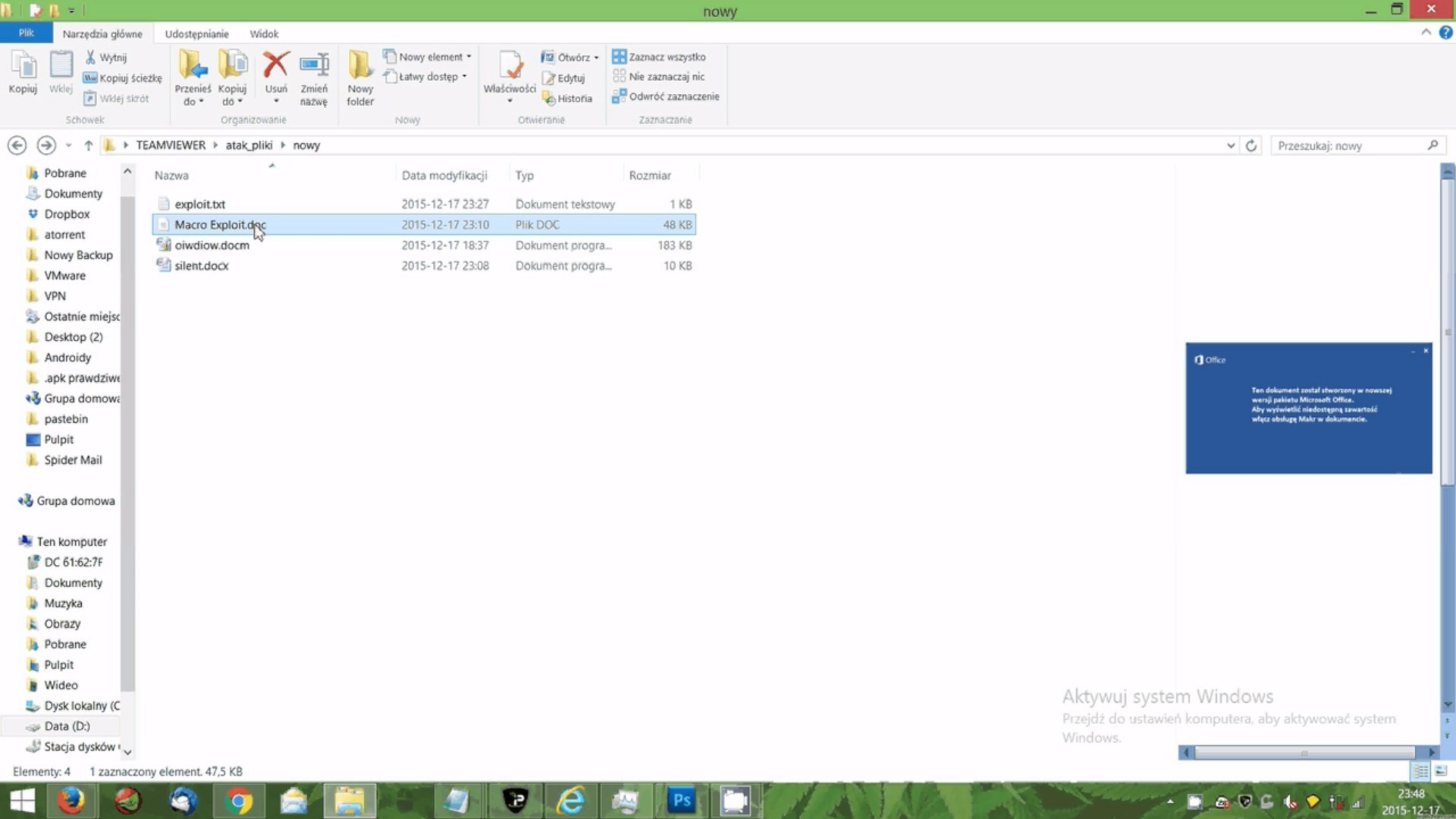
GET IT NOW!

SILENT

1/34 AV
100% silent

ONLY $399!

GET IT NOW!

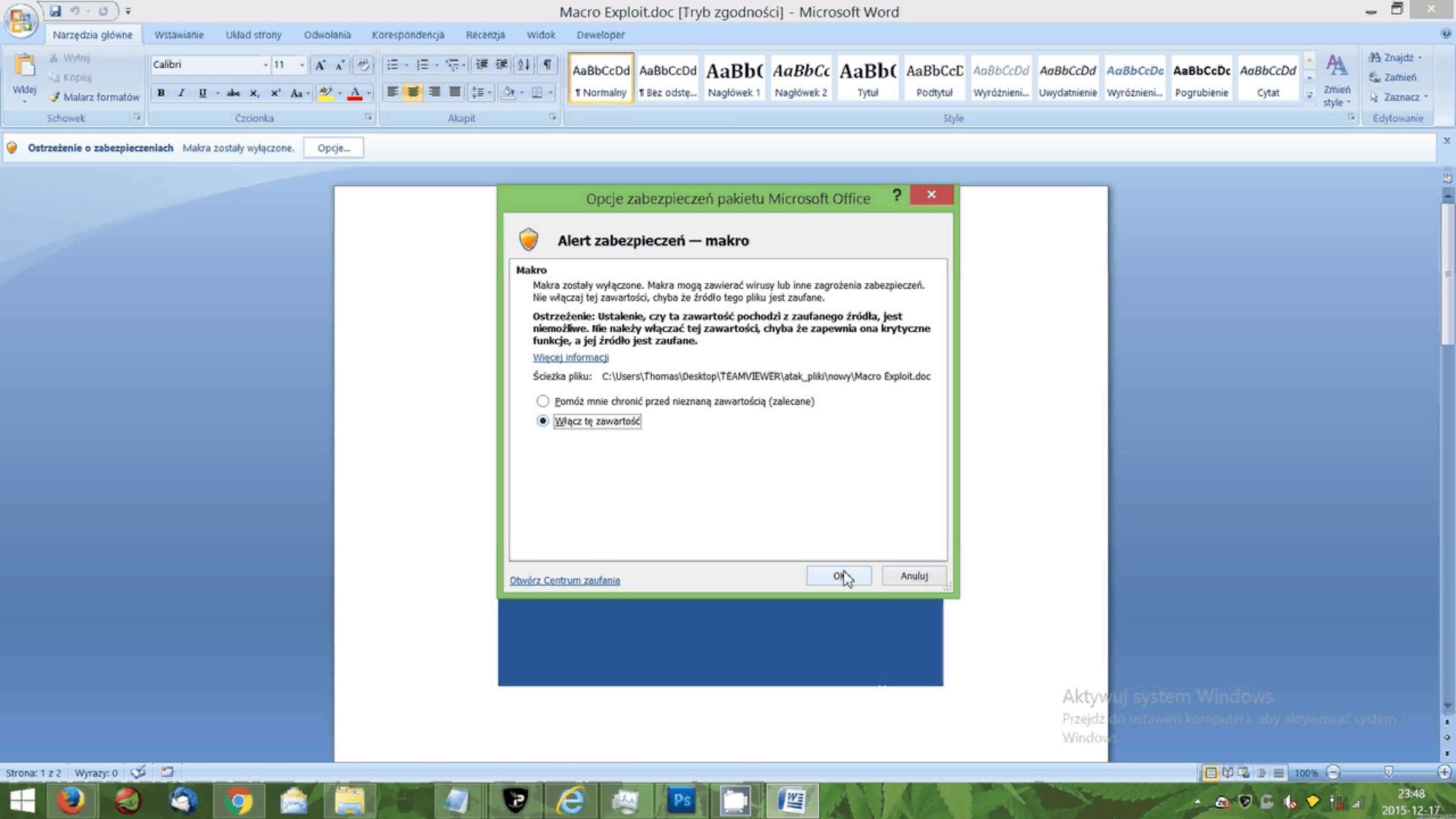


Nazwa	Data modyfikacji	Typ	Rozmiar
exploit.txt	2015-12-17 23:27	Dokument tekstowy	1 KB
Macro Exploit.doc	2015-12-17 23:10	Plik DOC	48 KB
oiwdiow.docm	2015-12-17 18:37	Dokument progra...	183 KB
silent.docx	2015-12-17 23:08	Dokument progra...	10 KB

Office

Ten dokument został stworzony w nowszej wersji pakietu Microsoft Office.
Aby wyświetlić niedostępną zawartość włącz obsługę Makr w dokumencie.

Elementy: 4 1 zaznaczony element. 47,5 KB



Ostrzeżenie o zabezpieczeniach Makra zostały wyłączone. Opcje...

Opcje zabezpieczeń pakietu Microsoft Office

Alert zabezpieczeń — makro

Makro

Makra zostały wyłączone. Makra mogą zawierać wirusy lub inne zagrożenia zabezpieczeń. Nie włączaj tej zawartości, chyba że źródło tego pliku jest zaufane.

Ostrzeżenie: Ustalenie, czy ta zawartość pochodzi z zaufanego źródła, jest niemożliwe. Nie należy włączać tej zawartości, chyba że zapewnia ona krytyczne funkcje, a jej źródło jest zaufane.

Więcej informacji

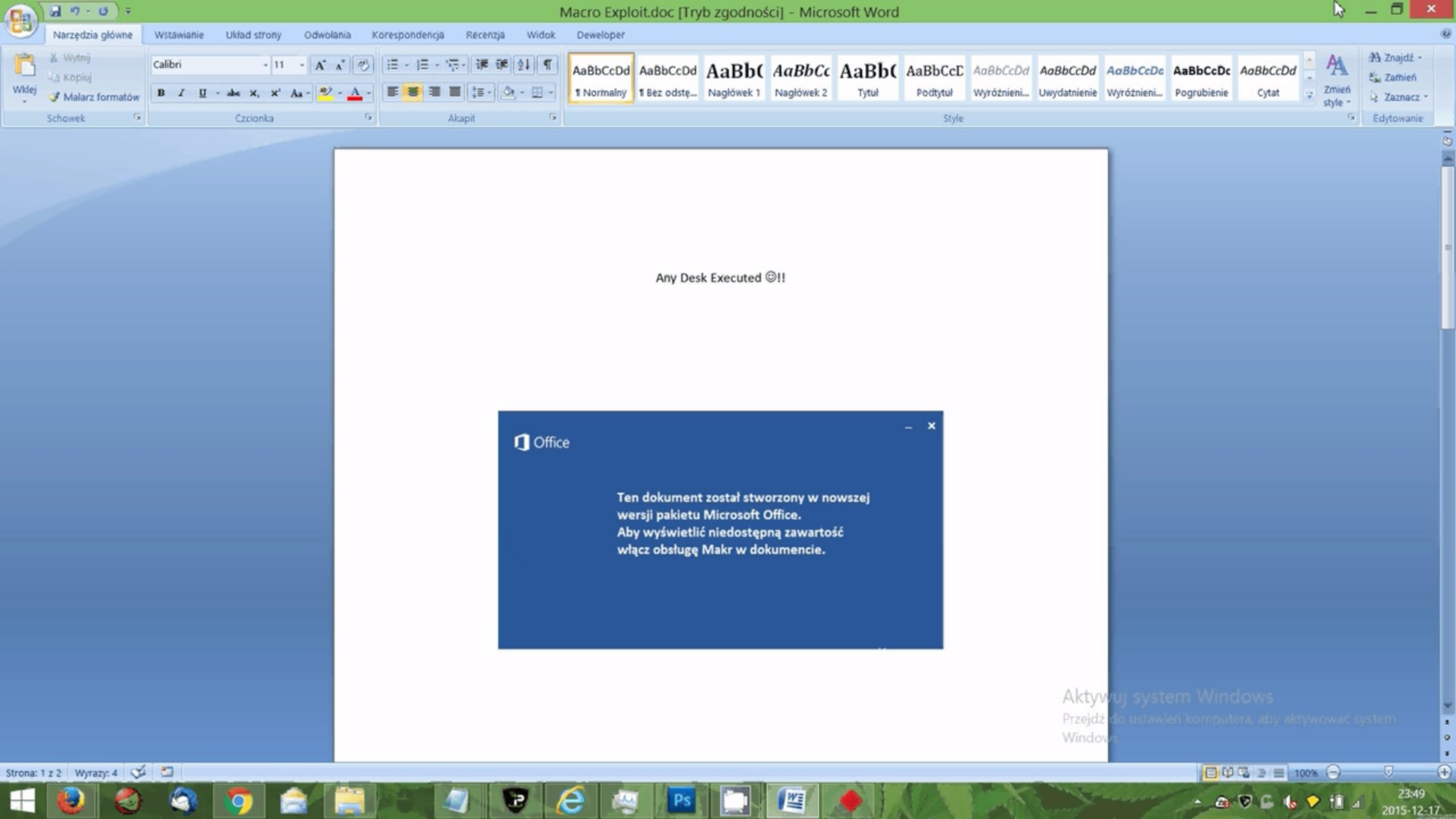
Ścieżka pliku: C:\Users\Thomas\Desktop\TEAMVIEWER\atak_pliki\nowy\Macro Exploit.doc

○ Pomóż mnie chronić przed nieznaną zawartością (zalecane)

● Włącz tę zawartość

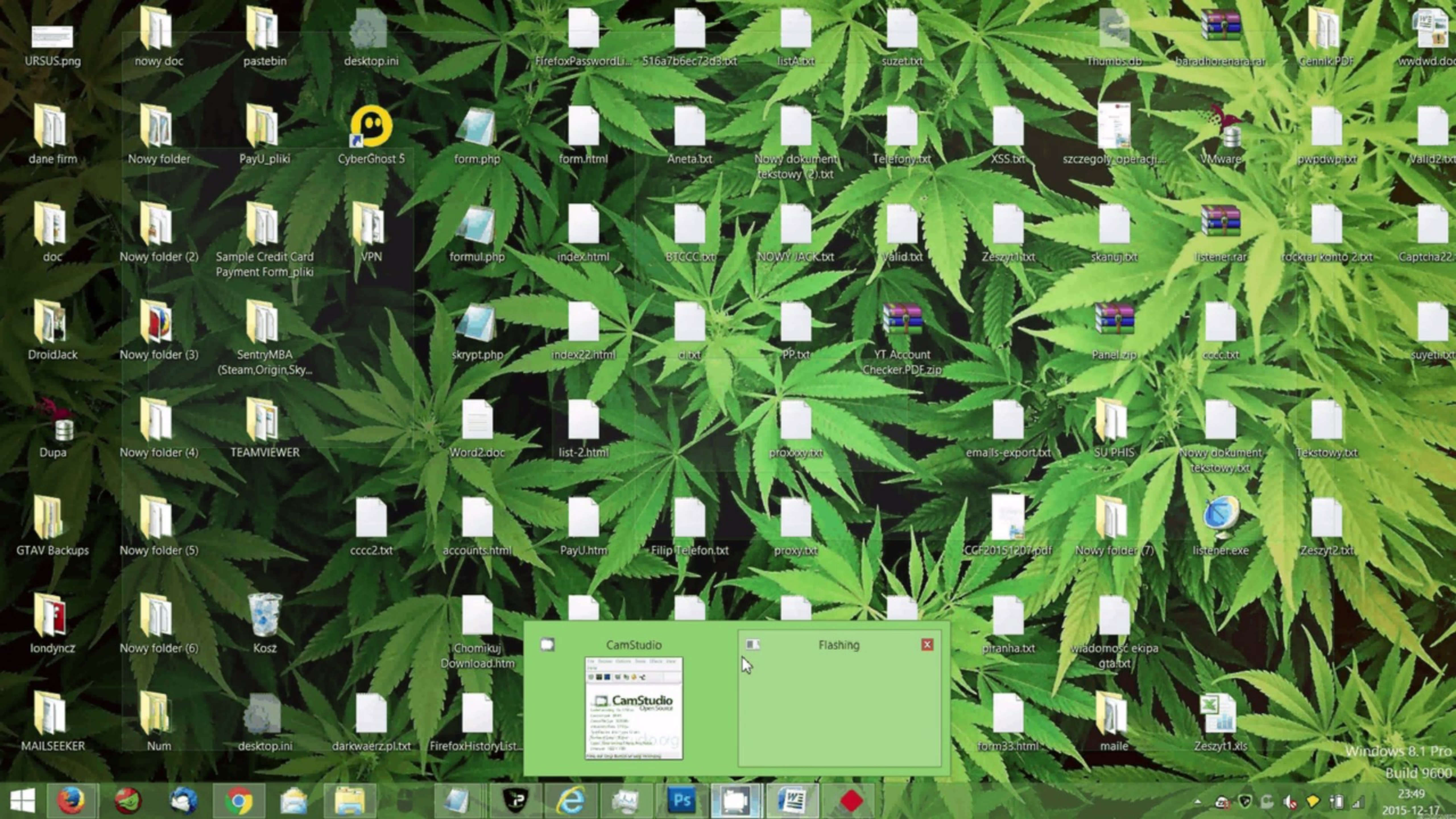
Otwórz Centrum zaufania

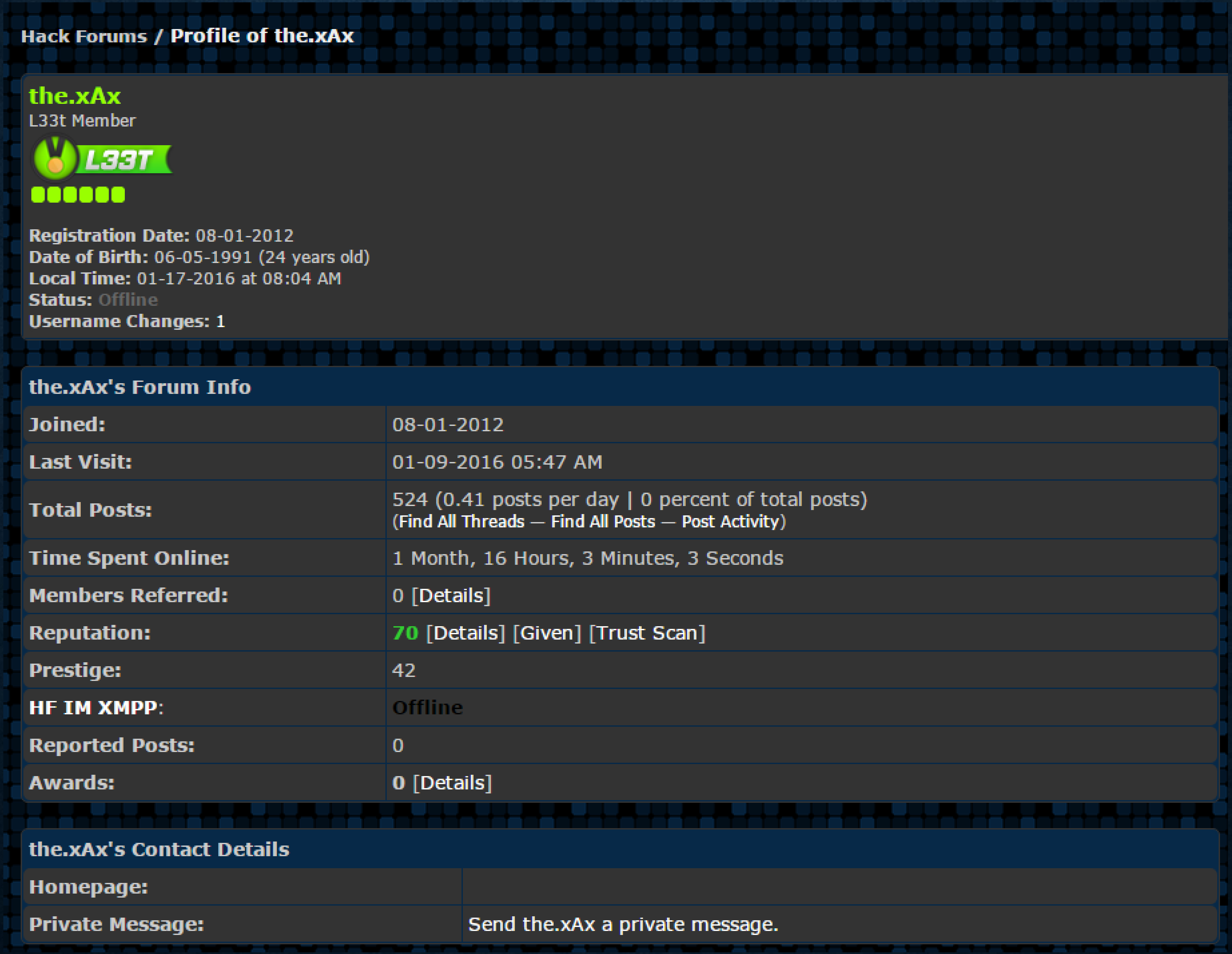
OK Anuluj



Any Desk Executed ☺!!

Ten dokument został stworzony w nowszej wersji pakietu Microsoft Office.
Aby wyświetlić niedostępną zawartość włącz obsługę Makr w dokumencie.


URSUS.png
nowy doc
pastebin
desktop.ini
FirefoxPasswordLi...
516a7b6ec73d3.txt
listA.txt
suzet.txt
Thumbs.db
baradhorenara.rar
Cennik.PDF
wwdwd.doc
dane firm
Nowy folder
PayU_pliki
CyberGhost 5
form.php
form.html
Aneta.txt
Nowy dokument tekstowy (2).txt
Telefony.txt
XSS.txt
szczegoly_operacji...
VMware
pwpdwp.txt
Valid2.txt
doc
Nowy folder (2)
Sample Credit Card Payment Form_pliki
VPN
formul.php
index.html
BTCCC.txt
NOWY JACK.txt
Valid.txt
Zeszyt1.txt
skanuj.txt
listener.rar
rocktar konto 2.txt
Captcha22...
DroidJack
Nowy folder (3)
SentryMBA (Steam,Origin,Sky...
skrypt.php
index22.html
d.txt
PP.txt
YT Account Checker.PDF.zip
Panel.zip
cccc.txt
suyeti.txt
Dupa
Nowy folder (4)
TEAMVIEWER
Word2.doc
list-2.html
proxxxy.txt
emails-export.txt
SU PHIS
Nowy dokument tekstowy.txt
Tekstowy.txt
GTAV Backups
Nowy folder (5)
cccc2.txt
accounts.html
PayU.htm
Filip Telefon.txt
proxy.txt
CCF20151207.pdf
Nowy folder (7)
listener.exe
Zeszyt2.txt
londyncz
Nowy folder (6)
Kosz
Chomikuj Download.htm
CamStudio
CamStudio Open Source
Flashing
piranha.txt
wiadomosc ekipa gta.txt
MAILSEEKER
Num
desktop.ini
darkwaerz.pl.txt
FirefoxHistoryList...
form33.html
maile
Zeszyt1.xls
Windows 8.1 Pro
Build 9600
23:49
2015-12-17



Hack Forums / **Profile of the.xAx**

the.xAx

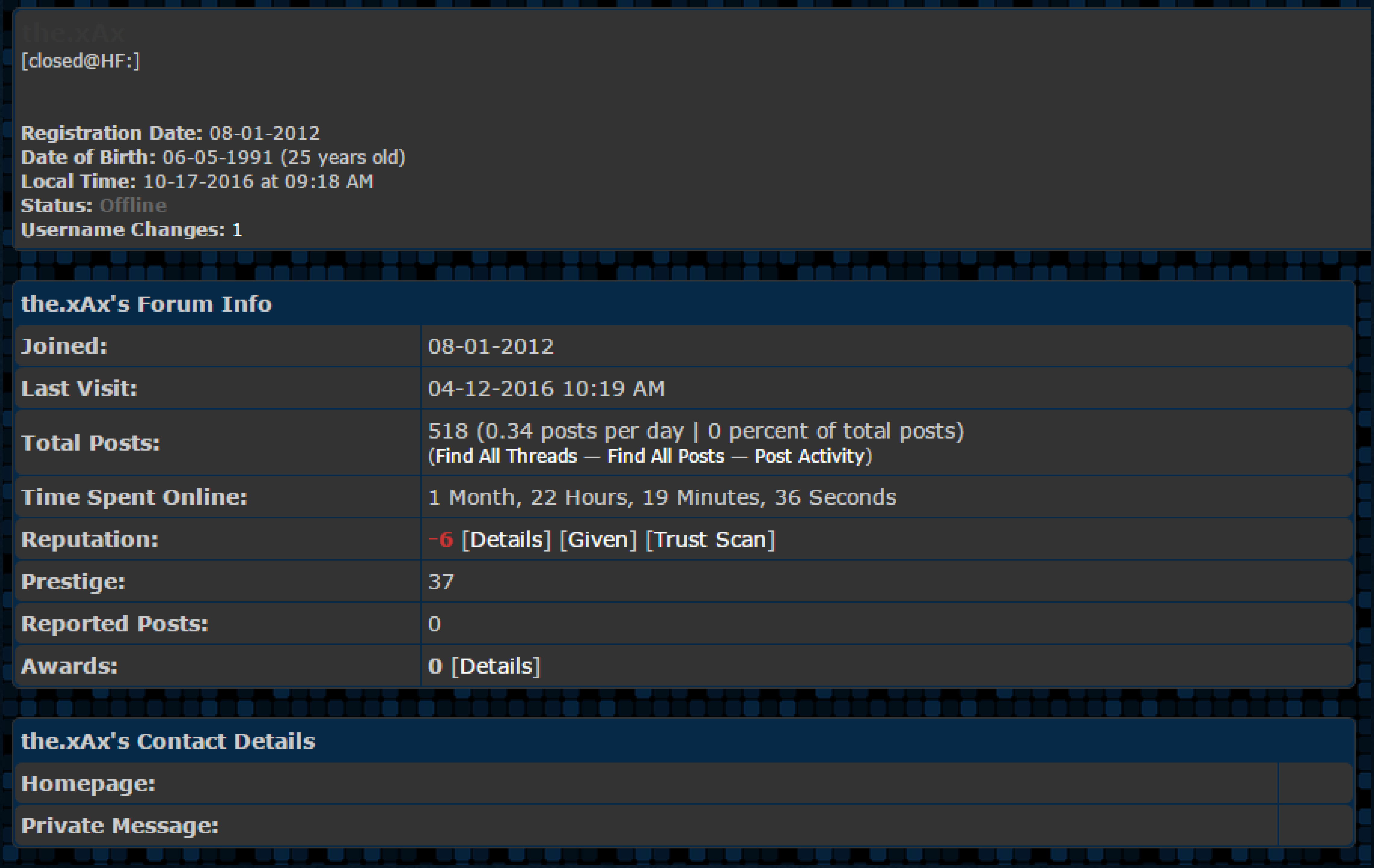
L33t Member

L33T

Registration Date: 08-01-2012
Date of Birth: 06-05-1991 (24 years old)
Local Time: 01-17-2016 at 08:04 AM
Status: Offline
Username Changes: 1

the.xAx's Forum Info	
Joined:	08-01-2012
Last Visit:	01-09-2016 05:47 AM
Total Posts:	524 (0.41 posts per day | 0 percent of total posts) (Find All Threads — Find All Posts — Post Activity)
Time Spent Online:	1 Month, 16 Hours, 3 Minutes, 3 Seconds
Members Referred:	0 [Details]
Reputation:	**70** [Details] [Given] [Trust Scan]
Prestige:	42
HF IM XMPP:	**Offline**
Reported Posts:	0
Awards:	**0** [Details]

the.xAx's Contact Details	
Homepage:	
Private Message:	Send the.xAx a private message.



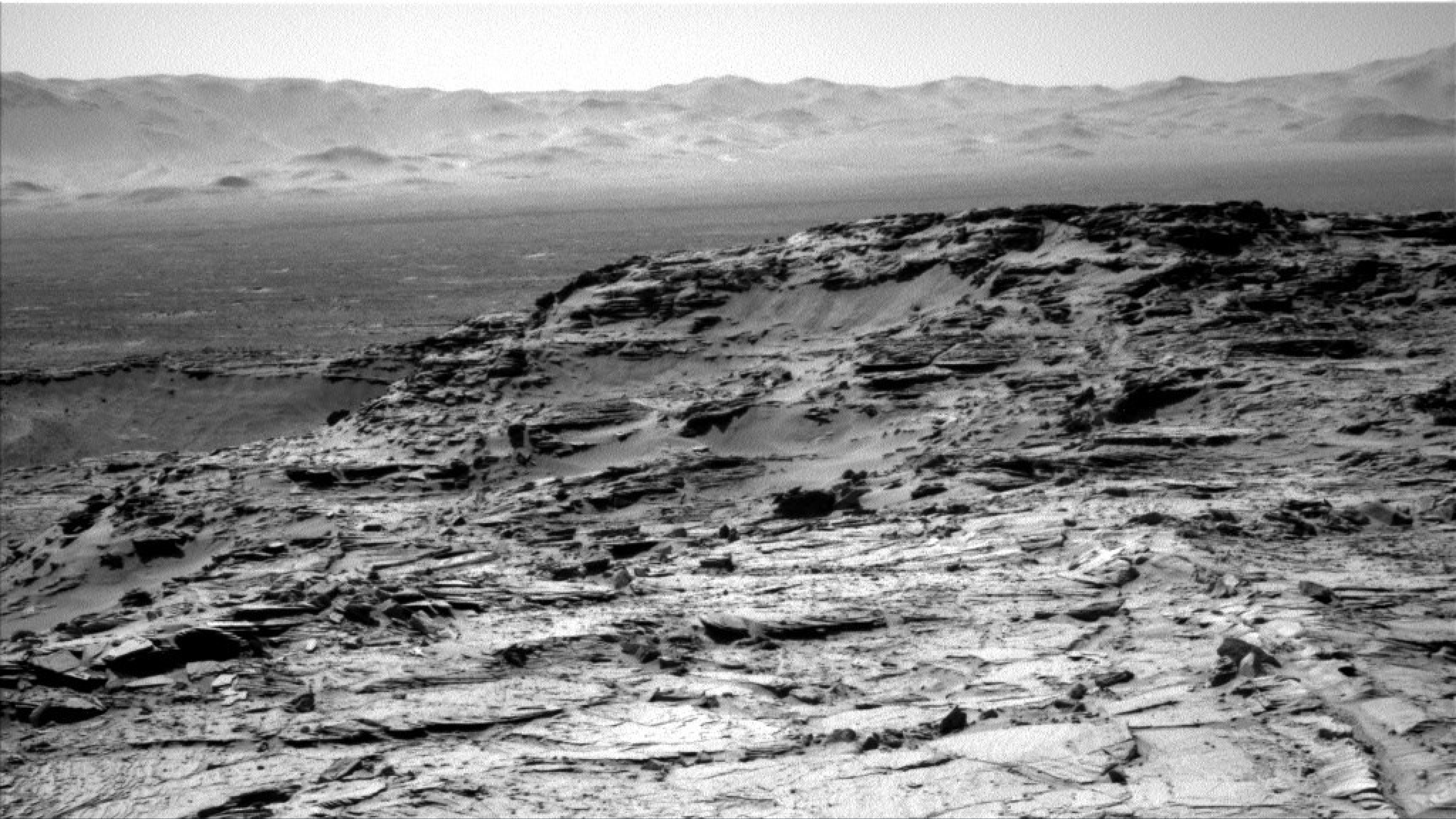
the.xAx

[closed@HF:]

Registration Date: 08-01-2012
Date of Birth: 06-05-1991 (25 years old)
Local Time: 10-17-2016 at 09:18 AM
Status: Offline
Username Changes: 1

the.xAx's Forum Info	
Joined:	08-01-2012
Last Visit:	04-12-2016 10:19 AM
Total Posts:	518 (0.34 posts per day | 0 percent of total posts) (Find All Threads — Find All Posts — Post Activity)
Time Spent Online:	1 Month, 22 Hours, 19 Minutes, 36 Seconds
Reputation:	-6 [Details] [Given] [Trust Scan]
Prestige:	37
Reported Posts:	0
Awards:	**0** [Details]

the.xAx's Contact Details	
Homepage:	
Private Message:	



Zierikzee
E311
A16
N65
A4
A17
A27
A2
Domburg
Kamperland
Steenbergen
Etten-Leur
Breda
Tilburg
A58
Roosendaal
A58
Middelburg
Goes
Bergen op Zoom
A58
Hilvarenbeek
Essen
A58
Vlissingen
A58
Breskens
A4
Hoogstraten
Ve
N62
nokke-Heist
Terneu
A12
Brass
E34
Damme
Sch
Antwerpia
Lommel
gia
Eeklo
Mol
Lokeren
Heist-op-den-Berg
E40
Gandawa
Heusden-Zolder
E17
N9
E19
N10
Merelbeke
Wetteren
Dendermonde
E314
Deinze
Aarschot
Diest
E313
A12
E314
Hasselt
E40

2017?

Spam, lots of spam

Vjw0rm (JS RAT)

Vortex / Flotera (ransomware)

PDF – JS – HTA – EXE – AutoIt - .NET - Payload

THANKS

CERT.PL >_

QUESTIONS?

BadCyber

BadCyber.com

@badcybercom

@adamhaertle